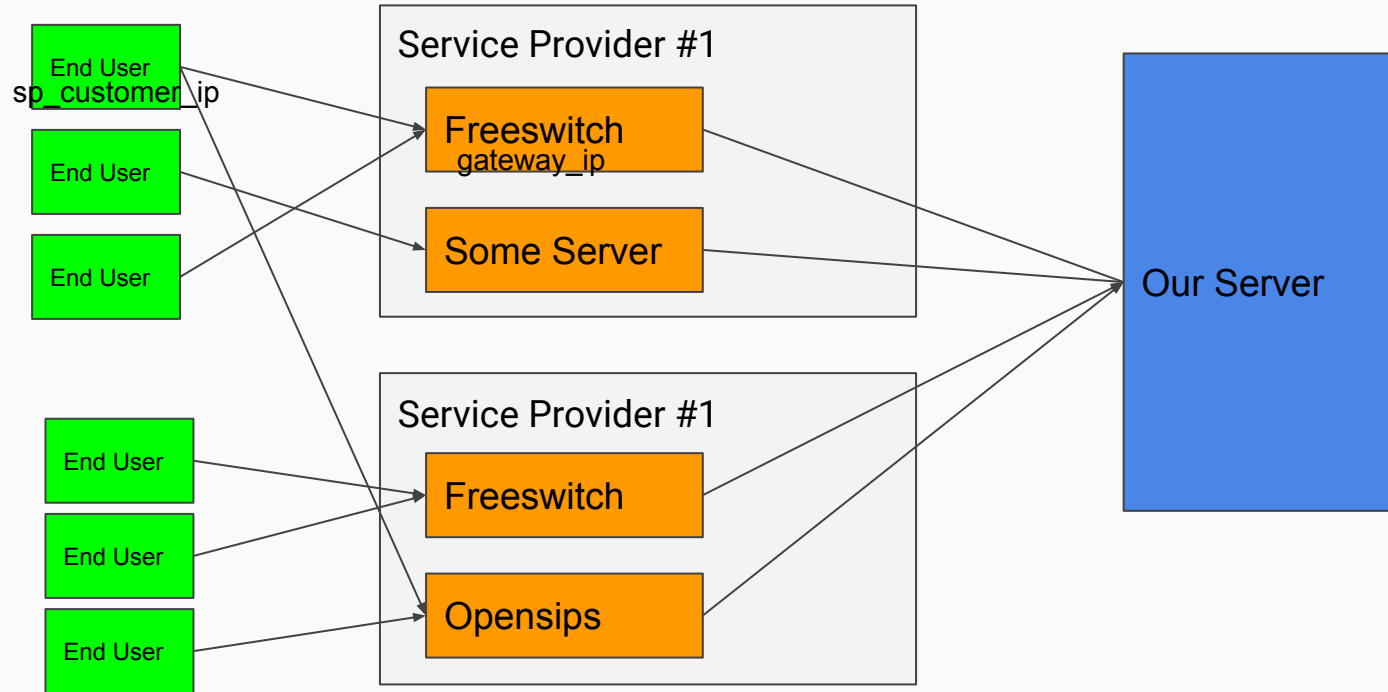


SIP and HTTP engine for AS and VS

Architecture

End Users that send traffic
to Service Providers



Purpose

The purpose is to implement HTTP and SIP interface.

There are the following interface:

- HTTP - Implement as in https://drive.google.com/file/d/15XrL4vvd2RmXVI-PftX44_iJDWLJICS/view?usp=sharing
- SIP-INVITE to SIP-INVITE
- SIP-INVITE to SIP-302

For each interface, there are two services:

- Authentication
- Verification

Content of token

```
{
  "header": {
    "alg": "ES256",
    "ppt": "shaken",
    "typ": "passport",

    "x5u": "https://certificates.peeringhub.io/4a871c06-e0b5-4cb9-8347-43126bd86c85/646b1be373f16eaf8753799e3499032a.crt"
  },
  "payload": {
    "attest": "A",
    "dest": {
      "tn": [
        "15806392239"
      ]
    },
    "iat": 1584993422,
    "orig": {
      "tn": "14077600036"
    },
    "origid": "4aec94e2-508c-4c1c-907b-3737bac0a80e",
    "rcd": {
      "icn": "https://peeringhub.io/logo.png",
      "inf": "https://peeringhub.io",
      "nam": "Alec Fenichel"
    }
  },
  "signature": "uTelvGauTvmVFCiDHFEjacv4ItOCiEFtiLjSnKZXUAOfi8Y-VfxRgwgw20inGWHfuOr646WlftiL3LhZqPy0Ng"
}
```

Sample code

← → ↺ opensips.org/docs/modules/3.1.x/stir_shaken.html#func_stir_shaken_auth

STIR/SHAKEN MODULE

Table of Contents

1. Admin Guide

1.1. Overview

1.2. Dependencies

1.2.1. OpenSIPS Modules

1.2.2. External Libraries or Applications

1.3. Exported Parameters

1.3.1. `auth_date_freshness` (integer)

1.3.2. `verify_date_freshness` (integer)

1.3.3. `ca_list` (string)

1.3.4. `ca_dir` (string)

1.3.5. `crl_list` (string)

1.3.6. `crl_dir` (string)

1.4. Exported Functions

1.4.1. `stir_shaken_auth`(`attest`, `origid`, `cert`, `pkey`, `x5u`, [`orig`], [`dest`])

1.4.2. `stir_shaken_verify`(`cert`, `err`)

1.4.3. `stir_shaken_check`()

1.4.4. `stir_shaken_check_cert`()

Authorization /
Signing

Verification

Sample code for AS and VS

<https://github.com/signalwire/libstirshaken/tree/master/examples>

- https://github.com/signalwire/libstirshaken/blob/master/examples/stir_shaken_as_passport.c
- https://github.com/signalwire/libstirshaken/blob/master/examples/stir_shaken_vs.c

Secsipidx opensource

- <https://github.com/asipto/secsipidx>

HTTP

Specification

The API and Error Code is here :

https://drive.google.com/file/d/15XrL4vvd2RmXVI-PfltX44_iJDWLJlCS/view?usp=sharing

The code for signing and verification can be found in:

https://opensips.org/docs/modules/3.1.x/stir_shaken.html#func_stir_shaken_auth

<https://github.com/signalwire/libstirshaken/commit/af9ba3b423afe0ccb64aad0163d1a3dd065d268b>

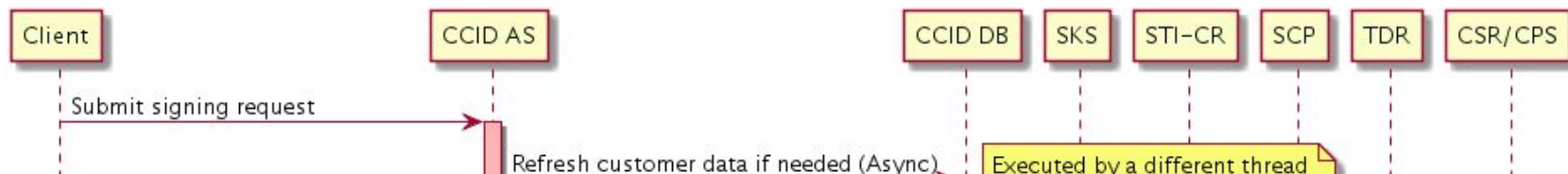
Additional Restful Interface to implement

STI-AS: <https://docs.ccid.neustar.biz/ccid/authn/docs/api-guide.html>

STI-VS: <https://docs.ccid.neustar.biz/ccid/verify/docs/api-guide.html>

Player

protocol.



Client	People who call our api
CCID DB	Our Postgres DB
SKS	This is where we store keys , either in disk or DB but need a secure place.
STI-CR	This is another project we are needing to develop
SCP	We can return the list of valid OCN from DB
TDR	Internal logging within this project
CPS	Internal logging within this project

AS

The CCID AS provides three categories of API entry points:

- Generates SIP Identity headers

Four different API entry points are defined for SIP Identity header creation:

- Accepts requests in JSON format and produces responses in JSON format
- Accepts SIP INVITE messages and produces responses in JSON format
- Accepts SIP INVITE messages and produces responses in SIP format
- Accepts SIP INVITE messages and produces responses in JSON format for SIP proxies

- Gets certificates for verifying SIP Identity headers

This API entry point is to return the certificate of a customer that does not provide a public accessible URL for fetching its certificate.

- Gets a list of all potential errors generated

This API entry point is to return a list of all potential errors that could be generated by the CCID AS for SIP Identity header creation.

VS

- Verifies SIP Identity headers

Four different API entry points are defined for SIP Identity header verification:

- Accepts requests in JSON format and produces responses in JSON format
- Accepts SIP INVITE messages and produces responses in JSON format
- Accepts SIP INVITE messages and produces responses in SIP format
- Accepts SIP INVITE messages and produces responses in JSON format for SIP proxies

- Performs CNAM queries

Two different API entry points are defined to return the CNAM data for a specific telephone number:

- Accepts a GET request with telephone number as a URL path parameter
- Accepts a POST request in JSON format with the "from" attribute

- Performs ESNAM queries

Two different API entry points are defined to return the ESNAM data for a specific telephone number:

- Accepts a GET request with telephone number as a URL path parameter
- Accepts a POST request in JSON format with the "from" attribute

- Gets a list of all potential errors generated

This API entry point is to return a list of all potential errors that could be generated by the CCID VS for SIP Identity header verification.

Signing Server

8.1.1 Functional Behavior

Used to create the PASSporT signature with private key certificate.

The Authenticator sends a signingRequest including the following to the SHAKEN Signing Service:

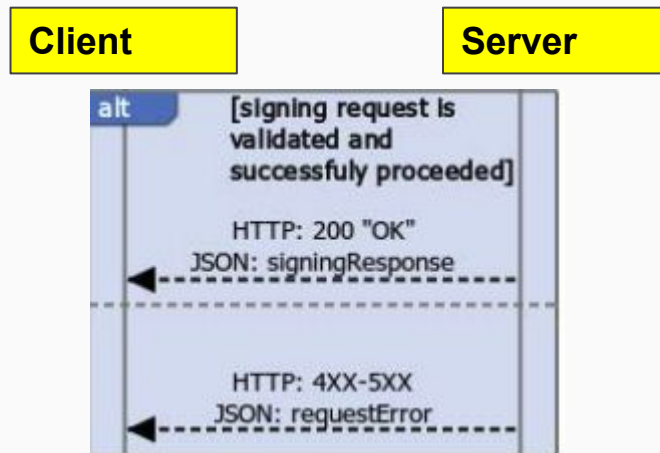
1. The "orig" parameter is populated using the PAI field if present, otherwise using the From header field in the SIP Invite.
2. The "dest" parameter is populated using the To header field in the SIP Invite.
3. The "iat" parameter is populated using the "Date" header field in the SIP Invite. If there is no "Date" header field in the SIP Invite, a Date header field is added to the SIP INVITE.
4. The "origid" parameter is determined as described in ATIS-1000074 for the "origid" field in the PASSporT.
5. The "attest" parameter is determined as described in ATIS-1000074 for the "attest" field in the PASSporT.
6. The signingRequest is then sent to the SHAKEN Signing Service.

The SHAKEN Signing Service performs the following steps:

1. Validate the incoming signing request parameters in terms of parameter's type and format.
2. Validate the "iat" parameter value in terms of "freshness": the request with "iat" value with time different by more than one minute from the current time will be rejected.
3. Normalize to the canonical form the received telephony numbers if needed (remove visual separators and leading "+").
4. Build SHAKEN PASSport protected JWT header (with "ppt" SHAKEN extension).
5. Build SHAKEN PASSporT JWT payload by keeping lexicographic order and removing space and line breaking characters.
6. Generate PASSporT signature with appropriate certificate private key.
7. Build Full Form of PASSporT.
8. Build SIP "Identity" header value by using identity digest from the previous step and add "info" parameter with angle bracketed URI used to acquire the public key of certificate used during PASSporT signing.
9. If successfully signed, build and send "signingResponse" to the Authenticator, otherwise send error.

Upon receipt of the signingResponse, the Authenticator uses the "identity" parameter in the response to populate the SIP Identity header field and forwards the request. If no identity parameter is received in a response, the Authenticator forwards the request without adding a SIP Identity header field.

Signing



Signing Service - Request

8.1.3 Request (POST)

The used resource is: `http://{serverRoot}/stir/v1/signing`.

Name	Description
serverRoot	Server base URL: hostname+port+base path Hostname contains the Global FQDN of Signing Service.

8.1.3.1 Request Body

Parameter	Data Type	Required?	Brief description
Signing Request	signingRequest	Yes	Contains the JSON structure of the signing request (PASSporT payload claims).

Request Sample

```
POST /stir/v1/signing HTTP/1.1
Host: stir.example.com
Accept: application/json
X-InstanceID : de305d54-75b4-431b-adb2-eb6b9e546014
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: ...
{
  "signingRequest": {
```

```
    ATIS-1000082
```

```
    12
```

```
    "attest": "A",
    "orig": {
      "tn": "12155551212"
    },
    "dest": {
      "tn": [
        "12355551212"
      ]
    },
    "iat": 1443208345,
    "origid": "de305d54-75b4-431b-adb2-eb6b9e546014"
  }
}
```

Request Sample (Success)

HTTP/1.1 200 OK

X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836

Content-Type: application/json

Content-Length: ...

{

```
"signingResponse": {
```

```
"identity": "eyJhbGciOiJFUzI1NiIsInR5cCI6Imluc3Nwb3J0IiwicHB0Ijoic2hha2VuliwieDV1ljoiaHR0cDovL2NlcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydCJ9eyJhdHRLc3QiOiJBliwiZGVzdCl6eyJ0bil6lisxMjE1NTU1MTIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyl6eyJ0bil64oCdKzEyMTU1NTUxMjEyln0slm9yaWdpZCI6IjEyM2U0NTY3LUU4OWltMTJkMy1hNDU2LTQyNyJ1NTQ0MDAwMCJ9._28kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWl4g75mnq9Tj2IW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;info=<https://cert.example2.net/example.cert>"
```

}

}

Verification Server

Verification Service - Response

Response body is returned as JSON object (Content-Type: application/json).

Parameter	Data Type	Required?	Brief description
Signing Response	signingResponse	Yes	Contains the JSON structure of the signing response (SIP Identity header field value).

Requet Sample (Failure)

HTTP/1.1 400 Bad Request

X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836

Content-Type: application/json

Content-Length: ...

```
{  
  "requestError": {  
    "serviceException": {
```

PH-1000082

13

```
    "messageId": "SVC4001"
```

```
    "text": "Error: Missing mandatory parameter '%1'",
```

```
    "variables": ["iat"]
```

```
  }
```

```
}
```

```
}
```

Response Code

Response code	Service/Policy Exception	Reason /Description
200	N/A	Successful signing.
400	SVC4000	Missing JSON body in the request.
400	SVC4001	Missing mandatory parameter.
406	SVC4002	Not supported body type is specified in Accept HTTP header.
415	SVC4004	Received unsupported message body type in Content-Type HTTP header.
400	SVC4005	Invalid parameter value.
400	SVC4006	Failed to parse JSON body.
411	SVC4007	Missing mandatory Content-Length header.
405	POL4050	Method Not Allowed: Invalid HTTP method used (all methods except POST will be rejected for the specific resource URL).
500	POL5000	The POST request failed due to internal signing server problem.

INVITE-INVITE

Spec

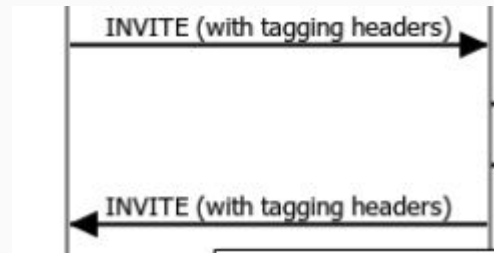
https://drive.google.com/file/d/147JlnwaDNCM_QUeZKKLDB9DxxfM2hKdE/view?usp=sharing

- I will provide data source API for determine if a caller-id is robo number
- I will provide data source api for CNAME

Signing Service

Client

Server



SIP Invite (signing)

SIP INVITE sent to Neustar SIP Proxy:

INVITE sip:+18097399997@dest.imscore.myorg.com:5060;transport=tcp;user=phone SIP/2.0

To: <sip:+18097399997@dest.imscore.myorg.com>

From: <sip:+18097399996@dest.imscore.myorg.com>;tag=h7g4EsbG_323fa4d5-1cd67b3a-2c-a69235a0-4a9d6304-715

Call-ID: 3b5bc958-1143f101-2c-593b4690-56052abf-715

CSeq: 1 INVITE

Max-Forwards: 68

Content-Length: 697

Via: SIP/2.0/TCP

192.19.98.50:5060;branch=z9hG4bKc882b446524d968c4528b58ebf4977bck555555yaaaaacaaaaafn3olla3Zqkv7y0ynrt
s3kgtxhqaabqaaaaabaaaaaa

Via: SIP/2.0/UDP 192.19.99.164:5060;branch=z9hG4bKg3Zqkv7if71dm5h3g7ten2n3uo3pfcotu

Via: SIP/2.0/TCP [fd06:0:0:2622::5]:6100;branch=z9hG4bK-2c-ac24-140cc73d-6f57a160

Route: <sip:192.21.151.196:5060;lr;call=orig>

Route: <sip:3Zqkv72ceamGaaaaaaaabebp@192.19.98.50:5060;lr>

Record-Route: <sip:3Zqkv7@srbhpp-scscf-01.dest.imscore.myorg.com:5060;maddr=192.19.98.50;lr>

Record-Route: <sip:192.19.99.164;transport=udp;lr>

Contact: <sip:302221001813278@[fd06:0:0:2622:0:0:5]:6100;transport=tcp;EriBindingId=1551715365091847;eribind-generated-at=192.19.99.164;q=1.0;+g.3gpp.access-type="cellular";+sip.instance="urn:gsma:imei:3022210-014132-

8>";+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmmtel";+g.3gpp.smsip

Content-Type: application/sdp

Allow: INVITE, BYE, CANCEL, ACK, PRACK, UPDATE, INFO, REFER, NOTIFY, MESSAGE

Accept: application/sdp

Accept: application/3gpp-ims+xml

Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmmtel"

Supported: 100rel, replaces, timer

P-Asserted-Identity: <sip:+18097399996@dest.imscore.myorg.com>

P-Asserted-Identity: tel:+18097399996

Proxy-Authorization: Digest

uri="sip:+18097399997@dest.imscore.myorg.com:5060;transport=tcp;user=phone",response="",nonce="",realm="",usern

ame="302221001813278@dest.imscore.myorg.com"

P-Visited-Network-ID: dest.imscore.myorg.com

P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=302221d6e11d0d200

SIP INVITE Response

INVITE sip:+18097399997@dest.imscore.myorg.com:5060;transport=tcp;user=phone SIP/2.0
Via: SIP/2.0/TCP
192.19.98.50:5060;branch=z9hG4bKc882b446524d968c4528b58ebf4977bck555555yaaaaacaaaaafn3olla3Zqkv7y0ynrt
s3kgtxhqaaaaabqaaaaabaaaaaa
Via: SIP/2.0/UDP 192.19.99.164:5060;branch=z9hG4bKg3Zqkv7if71dm5h3g7ten2n3uo3pfcotu
Via: SIP/2.0/TCP [fd06:0:0:2622::5]:6100;branch=z9hG4bK-2c-ac24-140cc73d-6f57a160
Max-Forwards: 67
Route: <sip:3Zqkv72ceamGaaaaaaaabebp@192.19.98.50:5060;lr>
Record-Route: <sip:3Zqkv7@srbhpp-scscf-01.dest.imscore.myorg.com:5060;maddr=192.19.98.50;lr>
Record-Route: <sip:192.19.99.164;transport=udp;lr>
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6ImNoYWtlbWVlbnR5cCIsInBhc3Nwb3J0IiwieDV1IjoiaHR0cDovLzE3Mi4yMS4xMjQuMTQvY2NpZC9hdXRobi92Mi9jZXJ0cy8xMTAwMSJ9.eyJhdHRlc3QiOiJBIiwieGVzdCI6eyJ0bil6WyIxODA5NzM5OTk5NyJdfSwiaWF0IjoxNTUzMDE1NzAxLCJvcmluIjpw7InRuljoiMTgwOTczOTk5OTYifSwib3JpZ2lkjoiNTQyZDk4YTgtOWVIMi00NGFILtkwZmUtNTQyNzBhYTU4MTkyIn0.LIRJJ_y01S5ym52GnfXyqwlPeweM1vLdPQLLPXpgWI8qDGU
WxOVFuJ1ecKs4XNgE232gYV-
qq4I91cPt3yg;info=<http://192.21.124.14/ccid/authn/v2/certs/11001>;alg=ES256;ppt="shaken"

Contact:

<sip:302221001813278@[fd06:0:0:2622:0:0:5]:6100;transport=tcp;EriBindingId=1551715365091847;eribind-generated-at=192.19.99.164>;q=1.0;+g.3gpp.accessstype="cellular";+sip.instance="urn:gsma:imei:3022210-014132-8>;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel";+g.3gpp.smsip
To: <sip:+18097399997@dest.imscore.myorg.com>
From: <sip:+18097399996@dest.imscore.myorg.com>;tag=h7g4Esbg_323fa4d5-1cd67b3a-2c-a69235a0-4a9d6304-715
Call-ID: 3b5bc958-1143f101-2c-593b4690-56052abf-715
CSeq: 1 INVITE
Session-Expires: 1800
Min-SE: 900
Accept: application/sdp, application/3gpp-ims+xml
Allow: INVITE, BYE, CANCEL, ACK, PRACK, UPDATE, INFO, REFER, NOTIFY, MESSAGE
Content-Type: application/sdp
Date: Tue, 19 Mar 2019 17:15:01 GMT
From: Authenticated Identity

Verification Service

SIP INVITE (Verification)

INVITE sip:+18097399997@dest.imscore.myorg.com SIP/2.0
To: <sip:+18097399997@dest.imscore.myorg.com>
From: sip:+18097399996@dest.imscore.myorg.com;tag=p65541t1553015701m100955c232359s3_2771535783-1904181461
Call-ID: p65541t1553015701m100955c232359s4
CSeq: 1 INVITE
Max-Forwards: 61
Content-Length: 694
Via: SIP/2.0/TCP
192.19.98.50:5060;branch=z9hG4bK90114face61c37bdc220ee15775ebc8k555555yaaaaacaaaaafgpfnnq3Zqkv7ye2tf2mzvsngnqaaaaabqaaaaabaaaaaa
Via: SIP/2.0/UDP
192.19.98.50:5060;branch=z9hG4bK90114face61c37bdc220ee15775ebc8k555555yaaaaacaaaaafib2ggi3Zqkv7ae2tf2m004qhfeaaaaabqaaaaaaq
Via: SIP/2.0/TCP 192.19.98.56:5082;branch=z9hG4bK2771535766-1861616012
Route: <sip:192.21.151.197:5060;lr;call=term_reg>
Route: <sip:3Zqkv72ceamGaaaaaaaabkhffya7@192.19.98.50:5060;lr>
Record-Route: <sip:3Zqkv7@srhbpp-scsf-01.dest.imscore.myorg.com:5060;maddr=192.19.98.50;lr>
Record-Route: <sip:3Zqkv7@srhbpp-scsf-01.dest.imscore.myorg.com:5060;maddr=192.19.98.50;lr>
Contact:
<sip:p65541t1553015701m100955c232359s3@192.19.98.56:5082;transport=tcp>;+g.3gpp.accesstype="cellular";+sip.ims
tance="urn:gsma:imei:3022210-014132-8>;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmmtel";+g.3gpp.smsip

Content-Type: application/sdp
Allow: REGISTER, REFER, NOTIFY, SUBSCRIBE, PRACK, UPDATE, INFO, INVITE, ACK, OPTIONS, CANCEL, BYE
Accept: application/sdp
Accept: application/3gpp-ims+xml
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmmtel";explicit;require
Supported: timer, 100rel, replaces
P-Asserted-Identity: <sip:+18097399996@dest.imscore.myorg.com>
P-Asserted-Identity: tel:+18097399996
P-Visited-Network-ID: dest.imscore.myorg.com
P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=302221d6e11d0d200
Min-SE: 900
Session-Expires: 1800
Date: Tue, 19 Mar 2019 17:15:01 GMT

P-Charging-Vector: icid-value=srbhpp-sbg-01-pcsf-sgc01.dest.imscore.myorg.com-1553-15700-995869;icid-generated-at=srbhpp-sbg-01-pcsf-sgc01.dest.imscore.myorg.com;orig-icid=dest.imscore.myorg.com;charging-info="(P-

SIP INVITE (response)

INVITE sip:+18097399997@dest.imscore.myorg.com SIP/2.0
Via: SIP/2.0/UDP 192.21.151.197:5060;branch=z9hG4bK-524287-1---9a001c13d627972f;rport
Via: SIP/2.0/TCP
192.19.98.50:5060;branch=z9hG4bK90114face61c37bdc220ee15775ebc8k555555yaaaaacaaaaafgpfnnq3Zqkv7ye2tf
2mzvsngnqaaaaabqaaaaabaaaaaa
Via: SIP/2.0/UDP
192.19.98.50:5060;branch=z9hG4bKec4cfe7409766cd8ef88ac2178723ebk555555yaaaaacaaaaafib2ggi3Zqkv7ae2tf2
m004qhfeaaaaabqaaaaaaq
Via: SIP/2.0/TCP 192.19.98.56:5082;branch=z9hG4bK2771535766-1861616012
Max-Forwards: 60
Route:
<sip:3Zqkv72ceamGaaaaaaaabkhffya7%26%269xsCMxJm1K0ZycaSaaaaadbaysip%3A%2B18097399997%40ims.mn
c221.mcc302.3gppnetwork.orgqHCn8aeaeaymdrHma@192.19.98.50:5060;lr>
Record-Route:
<sip:3Zqkv7%20caqmGaaaaacaaaaYCMxJm1K0Zyaaaaaesip%3A%2B18097399997%40ims.mnc221.mcc302.3gppnetw
ork.org@srbhpp-scscf-01.dest.imscore.myorg.com:5060;maddr=192.19.98.50;lr>
Record-Route:
<sip:3Zqkv7%20caqmGaaaaacaaaaalCMxJnA9a5saaaaagsip%3A%2B18097399996%40ims.mnc221.mcc302.3gppnetwo
rk.org@srbhpp-scscf-01.dest.imscore.myorg.com:5060;maddr=192.19.98.50;lr>
Contact:
<sip:p65541t1553015701m100955c232359s3@192.19.98.56:5082;transport=tcp>;+g.3gpp.accesstype="cellular";+sip.ins
tance="<urn:gsma:imei:3022210-014132-8>";+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-
service.ims.icsi.mmTel";+g.3gpp.smsip

To: <sip:+18097399997@dest.imscore.myorg.com>

From: <sip:+18097399996;verstat=TN-Validation-
Passed@dest.imscore.myorg.com>;tag=p65541t1553015701m100955c232359s3_2771535783-1904181461

Call-ID: p65541t1553015701m100955c232359s4

CSeq: 1 INVITE

Session-Expires: 1800

Min-SE: 900

Accept: application/sdp, application/3gpp-ims+xml

Allow: REGISTER, REFER, NOTIFY, SUBSCRIBE, PUBLISH, UPDATE, INFO, INVITE, ACK, OPTIONS, CANCEL, BYE

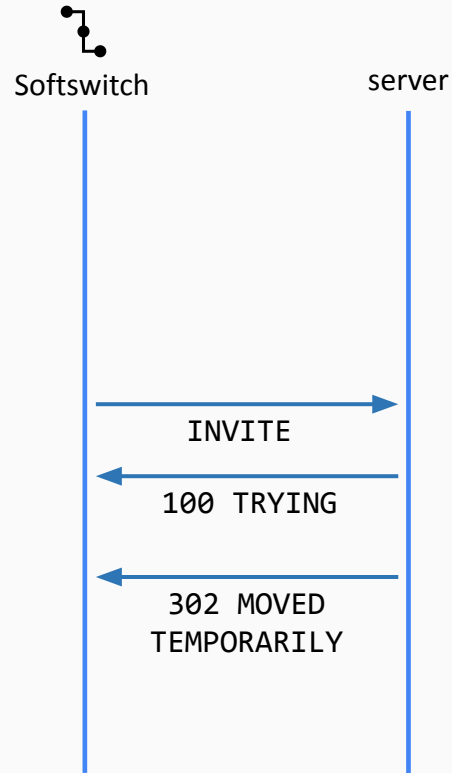
INVITE-302

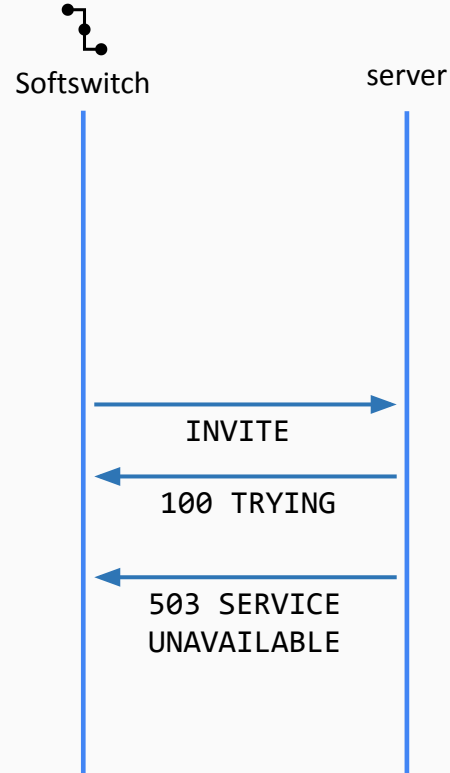
Specification

<https://drive.google.com/file/d/1i0difT1URbJUoiS3g1PXGH3rmShagW1c/view?usp=sharing>

Signing

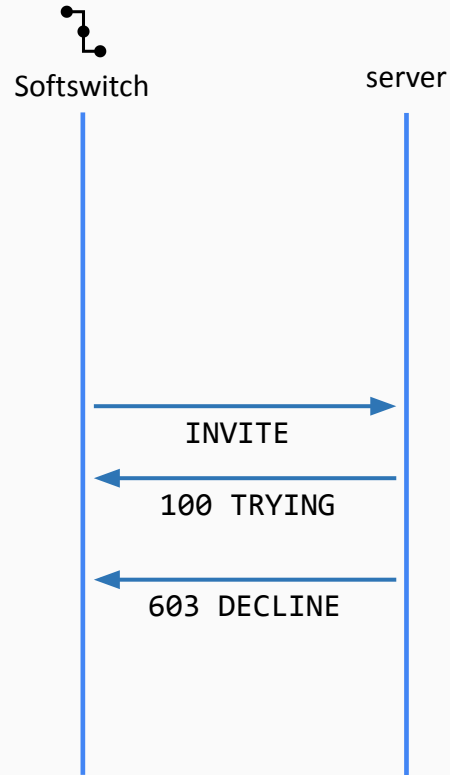
302 – Allow call and provide routes
503 – Allow call
603 – Block call





- 302 – Allow call and provide routes
- 503 – Allow call
- 603 – Block call

302 – Allow call and provide routes
503 – Allow call
603 – Block call



SIP/2.0 302 Moved Temporarily

Via: SIP/2.0/TLS

sip.clearip.com:5061;branch=z9hG4bK358c.edfa81f701a43bbcd7703fda294adc00.0;j=e48e54d2;received=:ffff:10.0.

12.110

Via: SIP/2.0/TCP

35.153.225.168;received=18.205.222.129;rport=48249;branch=z9hG4bKDX75tK7N4NpmH

To:

<sip:15806392239@sip.clearip.com;transport=tcp>;tag=fb7120b6-e8bb-447a-884c-8a4b20007c22

From: "SIPp" <sip:14077600036@35.153.225.168>;tag=pc04epeFaHB8c

Call-ID: 4dd659ee-e7e3-1238-a5b5-124662f73474

CSeq: 17942919 INVITE

Identity:

eyJhbGciOiJFUzI1NilsInBwdCI6InNoYWtlbilsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6

Ly9jZXJ0aWZpY2F0ZXMuY2x1YXJp

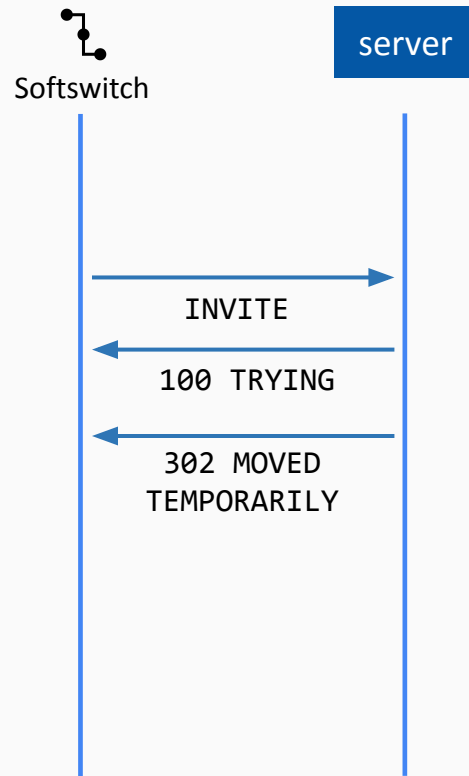
cC5jb20vNGE4NzFjMDYtZTBiNS00Y2I5LTgzNDctNDMxMjZiZDg2Yzg1LzY0NmIxYmUzNzN

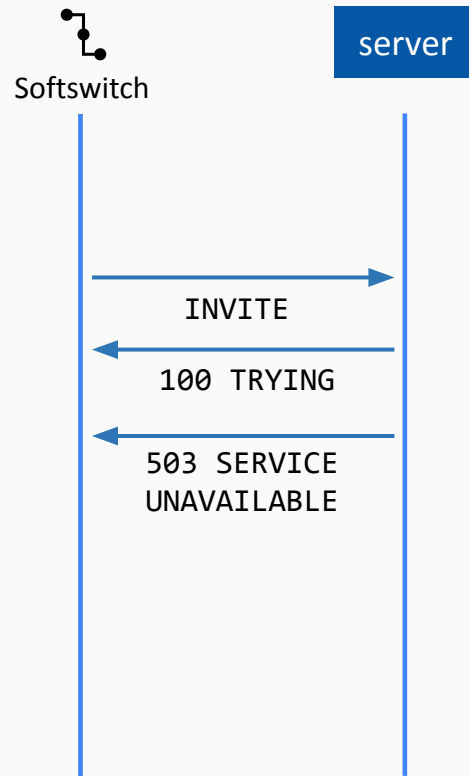
mMTZlYWY4NzUzNzk5ZTM0OTkwMzJhLmNy

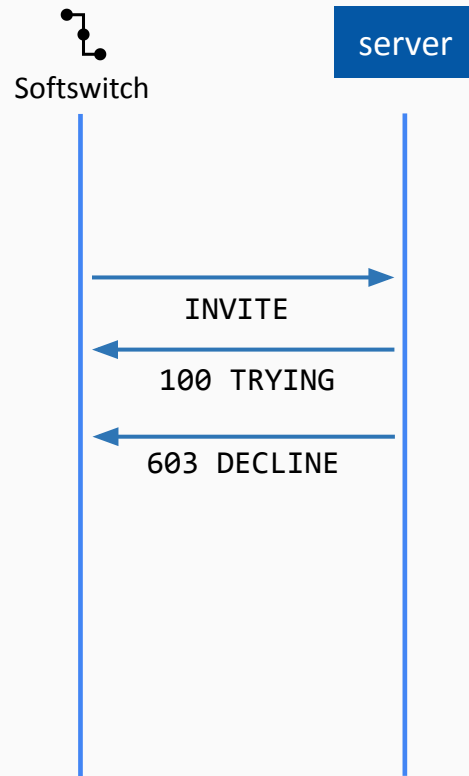
dCJ9.eyJhdHRlc3QiOiJBIiwieGZVzdCI6eyJ0bil6WylxNTgwNjM5MjZiZDg2Yzg1LzY0NmIxYmUzNzN

OTkzNDYtZTM0OTkwMzJhLmNyMTQwNzNz

Verification







INVITE sip:19292674904@sip.clearip.com;transport=tcp SIP/2.0
Via: SIP/2.0/TLS
sip.clearip.com:5061;branch=z9hG4bK4952.1dd5f51f5ed2a8663706e25c981390d9.0;j=e223036;
Via: SIP/2.0/TCP 192.168.1.200;received=52.207.147.53;branch=z9hG4bK608v79ym4K9a
Max-Forwards: 65
From: "SIPp" <sip:12013776051@192.168.1.200>;tag=veZegpp02jNgH
To: <sip:19292674904@sip.clearip.com;transport=tcp>
Call-ID: 2bde27dd-e78a-1237-dfa0-12ab5f1d9310
CSeq: 3850029 INVITE
Contact: <sip:mod_sofia@192.168.1.200:5060;transport=tcp>
User-Agent: FreeSWITCH-mod_sofia/1.6.19~64bit
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO, UPDATE, REGISTER, REFER,
NOTIFY
Supported: timer, path, replaces
Allow-Events: talk, hold, conference, refer
Content-Type: application/sdp
Content-Disposition: session
Content-Length: 222
P-Source-Device: 82.76.23.41
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCl6InNoYWtlbilsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9JZ
9fyw;info=<https://certificates.clearip.com/4a871c06-e0b5-4cb9-8347-
43126bd86c85/3360a7703b037d9a4b0b0218ffefb6fb.crt>;alg=ES256;ppt=shaken
X-Fs-Support: update_display,send_info
Remote-Party-Id: "SIPp"
<sip:12013776051@192.168.1.200>;party=calling;screen=yes;privacy=off
X-Real-Ip: 52.207.147.53
v=0
o=FreeSWITCH 1556776908 1556776909 IN IP4 192.168.1.200
s=FreeSWITCH
c=IN IP4 192.168.1.200
t=0 0
m=audio 30734 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000

SIP/2.0 302 Moved Temporarily

Via: SIP/2.0/TLS

sip.clearip.com:5061;branch=z9hG4bK4952.1dd5f51f5ed2a8663706e25c981390d9.0;i=e223036;

Via: SIP/2.0/TCP 192.168.1.200;received=52.207.147.53;branch=z9hG4bK608v79yrm4K9a

To: <sip:19292674904@sip.clearip.com;transport=tcp>;tag=addfba15-606b-43f7-a0c0-bc265c636147

From: "SIPp" <sip:12013776051@192.168.1.200>;tag=veZegpp02jNgH

Call-ID: 2bde27dd-e78a-1237-dfa0-12ab5f1d9310

CSeq: 3850029 INVITE

P-Asserted-Identity: "[V]Alice" <sip:12013776051;verstat=TN-Validation-Passed@192.168.1.200>

Contact: <sip:19292674904@sip.clearip.com>;q=0.99

Reason: SIP;cause=302;text="no-fraud-detected"

Content-Length: 0

SIP/2.0 302 Moved Temporarily

Via: SIP/2.0/TLS

sip.clearip.com:5061;branch=z9hG4bK4952.1dd5f51f5ed2a8663706e25c981390d9.0;i=e223036;

Via: SIP/2.0/TCP 192.168.1.200;received=52.207.147.53;branch=z9hG4bK608v79yrm4K9a

To: <sip:19292674904@sip.clearip.com;transport=tcp>;tag=addfba15-606b-43f7-a0c0-bc265c636147

From: "SIPp" <sip:12013776051@192.168.1.200>;tag=veZegpp02jNgH

Call-ID: 2bde27dd-e78a-1237-dfa0-12ab5f1d9310

CSeq: 3850029 INVITE

P-Asserted-Identity: "[V]Alice" <sip:12013776051;verstat=TN-Validation-Passed@192.168.1.200>

Contact: <sip:19292674904@sip.clearip.com>;q=0.99

Reason: SIP;cause=302;text="no-fraud-detected"

Content-Length: 0

DB schema

Postgres DB schema - sp_account_uuid table

Field	Type	Description
sp_account_uuid		
active	boolean	If inactive, then we should 404 the call
started_on		
expired_on		If expired, then we should 404 the call
cps_limit		This is the request per sec allowed
as_enabled	boolean	Auth service is allowed from this sp's IP
vs_enabled	boolean	Verification service is allowed from this sp's ip
priv_key	Varchar	If null, then the default cert will be used.
pem_file_path	Varchar	Cert of this service provider
default_att_level_with_sp_ani		If the via IP is not specified in sp_customer_ip, then we use this default value. If the ANI is not one of service provider's ANI, then we use this attestation level.
Default_att_level_wo_sp_ani		If the via IP is not specified in sp_customer_ip, then we use this default value. If the ANI is one of service provider's ANI, then we use this attestation level.

Postgres DB schema - sp_gateway_ip table

Field	Type	Description
sp_gateway_ip_uuid		
sp_account_uuid		
gateway_ip		Opensips should only allow requests from this IP. Each SP can define multiple IPs.

Postgres DB schema - sp_customer table

Field	Type	Description
sp_customer_uuid		
active	boolean	If inactive, then we should send 404 back.
started_on		Before started_on, we should send 404 back.
expired_on		After expired_on, we should send 404 back.
cps_limit		Max request per second allowed for this customer.
as_enabled		This customer's IP can send AS request. The SP's as_enable must be true for this to pass.
vs_enabled		This customer's IP can send VS request. The SP's vs_enable must be true for this to pass.
include_cname	boolean	If true, sp can specify to have their customer to enable "include_cname" in the response.
include_lrn	boolean	If true, sp can specify to have their customer to enable "include_lrn" in the response. This is similar to the callfwd
include_dnc	boolean	If true,sp can specify to have dnc include in the response.

Postgres DB schema - sp_customer_ip table

Field	Type	Description
sp_customer_uuid		
customer_ip	inet	Each customer can have multiple IP address that they are allowed to send AS/Vs request to opensips. This is the actual IP sending the request of AS and VS.
orig_id	varchar	This is a orig_id representing the customer
tech_prefix		If hostname is present then IP is ignored.
att_level_with_sp_an		If the ANI is not one of service provider's ANI, then we use this attestation level.

Postgres DB schema - sp_tn table

Field	Type	Description
sp_tn		
sp_account_uuid		
tn		This is the telephone phone of the service provider. Each number should be associated to one sp.

Schema

```
CREATE TABLE sp_accounts ( sp_account_uuid uuid DEFAULT uuid_generate_v4 (), active boolean default true, started_on TIMESTAMP NOT NULL, modified_on TIMESTAMP NOT NULL, expired_on TIMESTAMP NOT NULL, cps_limit integer , as_enabled boolean default true, vs_enabled boolean default true, priv_key varchar not null, pem_file_path varchar not null, default_att_level_with_sp_ani char not null, default_att_level_wo_sp_ani char not null);
```

```
CREATE table sp_gateway_ip ( sp_gateway_ip_uuid uuid DEFAULT uuid_generate_v4 (), sp_account_uuid uuid not null, gateway_ip inet not null);
```

```
CREATE table sp_customers ( sp_customer_uuid uuid DEFAULT uuid_generate_v4 (), active boolean default true, started_on TIMESTAMP NOT NULL, modified_on TIMESTAMP NOT NULL, expired_on TIMESTAMP NOT NULL, cps_limit integer, as_enabled boolean default true , vs_enabled boolean default true );
```

```
CREATE table sp_customer_ip ( sp_customer_ip_uuid uuid DEFAULT uuid_generate_v4 (), sp_customer_uuid uuid, customer_ip inet not null, tech_prefix varchar, att_level_with_sp_ani char not null, att_level_wo_sp_ani char not null);
```

```
CREATE table sp_tn ( sp_tn_uuid uuid DEFAULT uuid_generate_v4 (), sp_account_uuid uuid, tn varchar );
```