STIR/SHAKEN deployment made easy

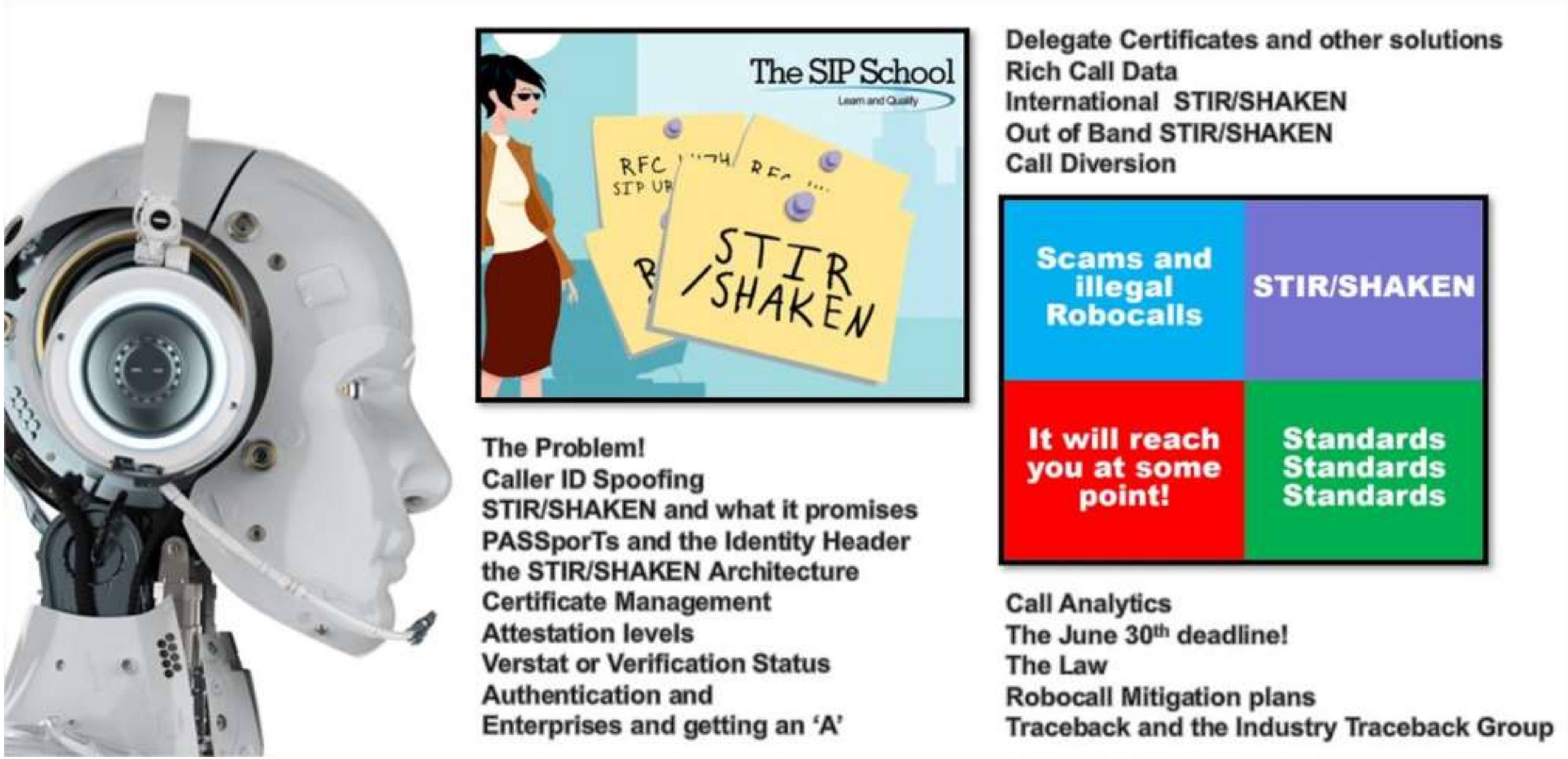
February 2, 2023

Presenters

Jim Dalton

Marc St. Onge

The SIP School



Delegate Certificates and other solutions
Rich Call Data
International STIR/SHAKEN
Out of Band STIR/SHAKEN
Call Diversion

Scams and illegal Robocalls	STIR/SHAKEN
It will reach you at some point!	Standards Standards Standards

The Problem!
Caller ID Spoofing
STIR/SHAKEN and what it promises
PASSporTs and the Identity Header
the STIR/SHAKEN Architecture
Certificate Management
Attestation levels
Verstat or Verification Status
Authentication and
Enterprises and getting an 'A'

Call Analytics
The June 30th deadline!
The Law
Robocall Mitigation plans
Traceback and the Industry Traceback Group

https://www.thesipschool.com/

Agenda

- Regulatory update
- SHAKEN overview
- Non-IP out-of-band SHAKEN
- Non-IP in-band SHAKEN
- Integration
- Conclusions, Questions and Answers

Submit questions in the Q&A panel, not in the Chat box

You will receive an e-mail with a link to the webinar and slides

Regulatory Overview

- Dec 2019 – TRACED Act is passed
- June 2021 – Large carriers implement SHAKEN on their SIP networks
- June 2021 – All service providers certify the robocall mitigation plans
  - Service providers must “know their customers” and “police their networks”
- June 2022 – Small carriers with no facilities implement SHAKEN
- June 2023 – Small carriers with facilities and international gateway providers must implement SHAKEN on their SIP Networks
- **FCC will make a decision on SHAKEN for TDM networks soon**

Go to https://transnexus.com/shaken-info-hub/#regs for links to all FCC orders on SHAKEN and Robocalls

Who needs to implement SHAKEN?

- You need to implement SHAKEN if you operate a SIP network.
  - SHAKEN on every SIP network by June 30, 2023
- You may need to implement SHAKEN if you operate a TDM network.
  - FCC decision is pending
- Fax only providers must implement SHAKEN.
- You may need to implement SHAKEN even if you have no network.
  - Managed Service Provider example:
  - Manage your customer’s VoIP PBX connection to an intermediate provider
  - Bill your customer for services you resell from the intermediate provider
- Service providers who want their calls completed.

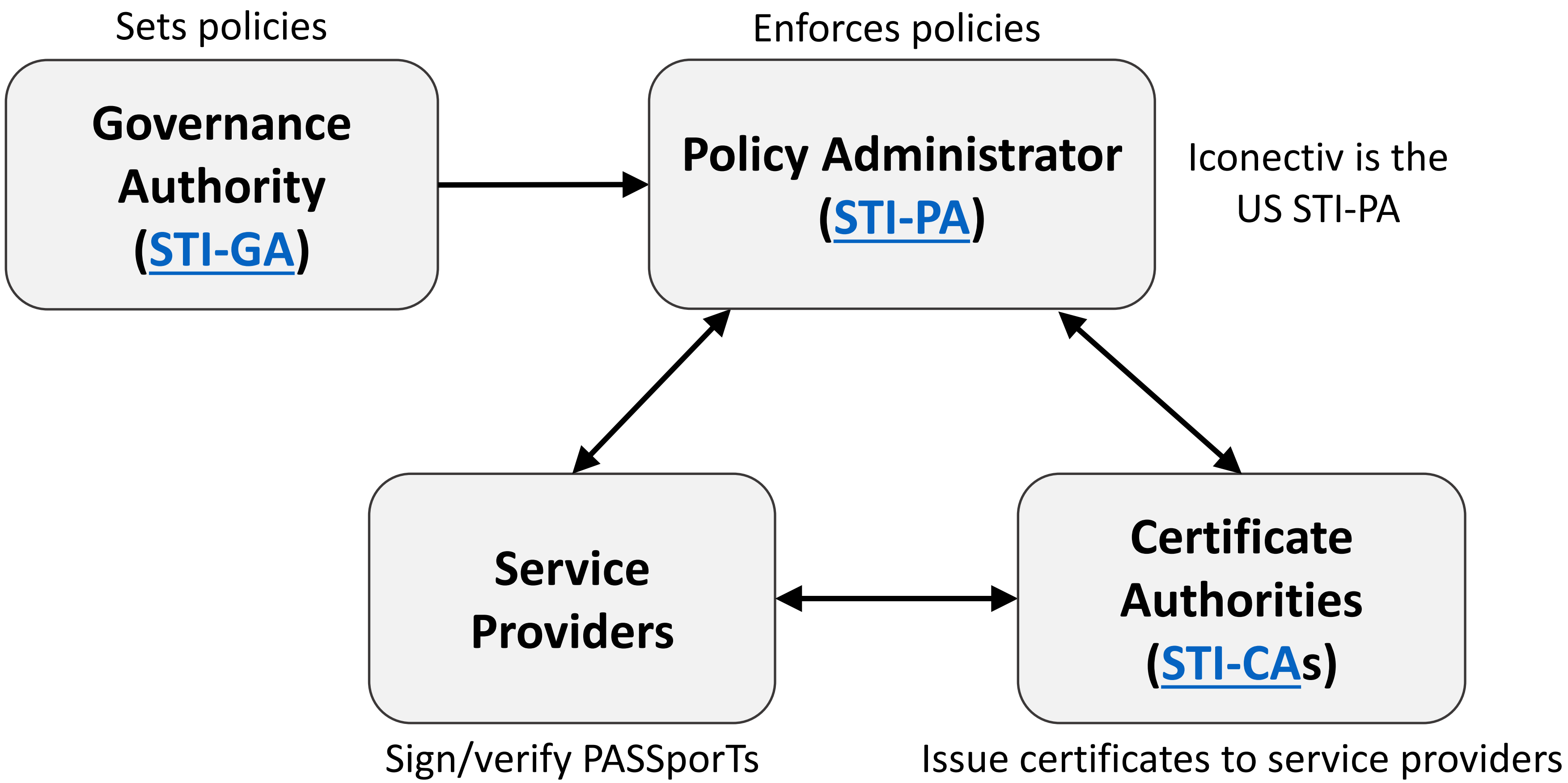
SHAKEN overview

ATIS SHAKEN Standard 1000074

What does SHAKEN do?

- Identifies the service provider who originated the call
- Allows the service provider to attest
  - If they know the end-user who placed the call
  - If they know the end-user is authorized to use the calling number
- Does not directly indicate whether a call is wanted versus unwanted
- Provides information to robocall analytics which determine whether a call is wanted versus unwanted

SHAKEN ecosystem



Sets policies

Governance Authority (STI-GA)

Enforces policies

Policy Administrator (STI-PA)

Iconectiv is the US STI-PA

Service Providers

Sign/verify PASSporTs

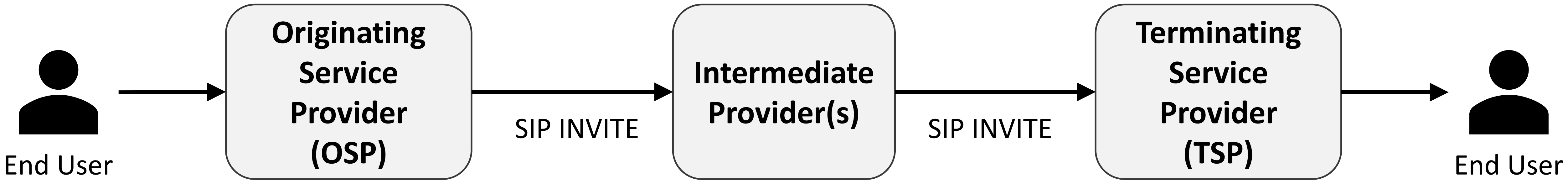
Certificate Authorities (STI-CAs)

Issue certificates to service providers

SIP call flow

Understanding Terms

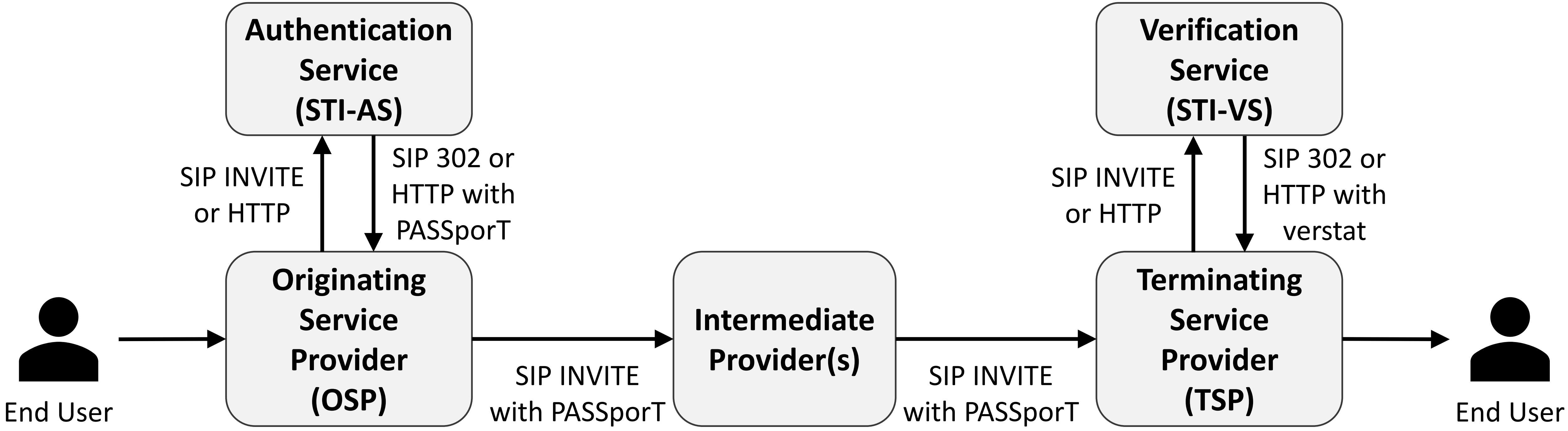
- End user – the person or enterprise using telephone service
- OSP – Provider of voice service to the calling end user
- Intermediate provider – Long distance, inter exchange carriers
- TSP – Provider of voice service to the called end user


End User
Originating Service Provider (OSP)
SIP INVITE
Intermediate Provider(s)
SIP INVITE
Terminating Service Provider (TSP)
End User

SIP call flow with SHAKEN

1. Determines the attestation level for the call
2. Creates a PASSporT that includes the attestation level
3. Signs the PASSporT using their certificate

1. Verifies PASSporT signature
2. Creates verstat parameter
3. Often combined with call analytics



Authentication Service (STI-AS)

SIP INVITE or HTTP

SIP 302 or HTTP with PASSporT

Verification Service (STI-VS)

SIP INVITE or HTTP

SIP 302 or HTTP with verstat

End User

Originating Service Provider (OSP)

SIP INVITE with PASSporT

Intermediate Provider(s)

SIP INVITE with PASSporT

Terminating Service Provider (TSP)

End User

SHAKEN Attestation = Level of Trust

- A = Full Attestation: The signing provider shall satisfy all of the following conditions:
  - Is responsible for the origination of the call
  - Has a direct authenticated relationship with the customer and can identify the customer.
  - Has established a verified association with the telephone number used for the call.
- B = Partial Attestation: Trusted relationship with the customer
  - Call from a end user trunk group
- C = Gateway Attestation: No trust
- Defined in ATIS-1000074 section 5.2.3

SIP INVITE with Identity Header

```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+12155551213@tel.example1.net>
From: "Alice"<sip:+12155551212@tel.example2.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
P-Asserted-Identity: "Alice"<sip:+12155551212@tel.example2.net>,<tel:+12155551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb
3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIx
NTU1NMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMD1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTR
TpQ5X0relYset-EScb9otFNDxOCTjerg ;info=<https://cert.example.org/passport.pem>;ppt="shaken"
Content-Length: 122
```

Decoded SHAKEN PASSporT

Header

```
{
  "alg": "ES256",
  "ppt": "shaken",
  "typ": "passport",
  "x5u": "https://cert.example.org/passport.pem"
}
```

Signature

_V41ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwG
xm3tDUTRTpQ5X0relYset-EScb9otFNDxOCTjerg

Payload

```
{
  "attest": "A",
  "dest": {
    "tn": [
      "12125551213"
    ]
  },
  "iat": 1471375418,
  "orig": {
    "tn": "12155551212"
  },
  "origid": "123e4567-e89b-12d3-a456-426655440000"
}
```

Parsed SHAKEN certificate (first 10 lines)

```
Version: 3
Serial Number: 68:fd:0b:ce:8a:51:cd:4e:75:1e:22:7b:ef:33:60:8f
Signature Algorithm: ecdsa-with-SHA256
Issuer: C=US, O=TransNexus, Inc., OU=SHAKEN, CN=TransNexus, Inc. SHAKEN Issuing CA3
Subject: C=US, O=Assurance Telecom, OU=SHAKEN, CN=SHAKEN 518J
Validity:
  Not Before: Jul  7 20:09:51 2022 GMT
  Not After: Jul 14 20:09:50 2022 GMT
X509v3 extensions:
  TN Auth List:
    Service Provider Code: 518J
```

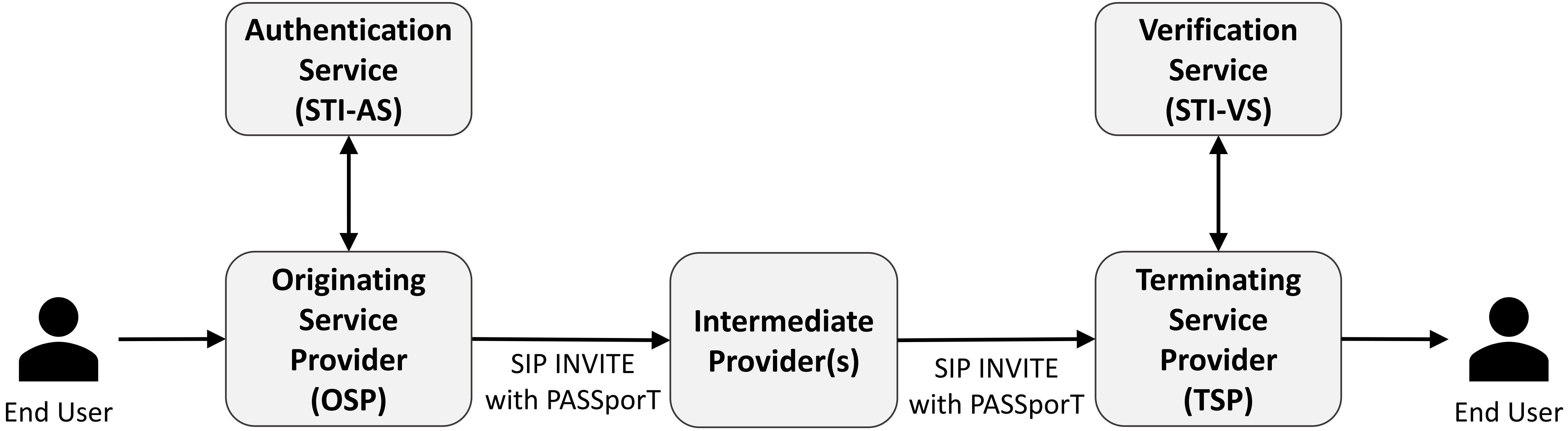
Non-IP out-of-band SHAKEN

ATIS Out-of-Band SHAKEN Standard 1000096

SIP call flow with SHAKEN

1. Determines the attestation level for the call
2. Creates a PASSporT that includes the attestation level
3. Signs the PASSporT using their certificate

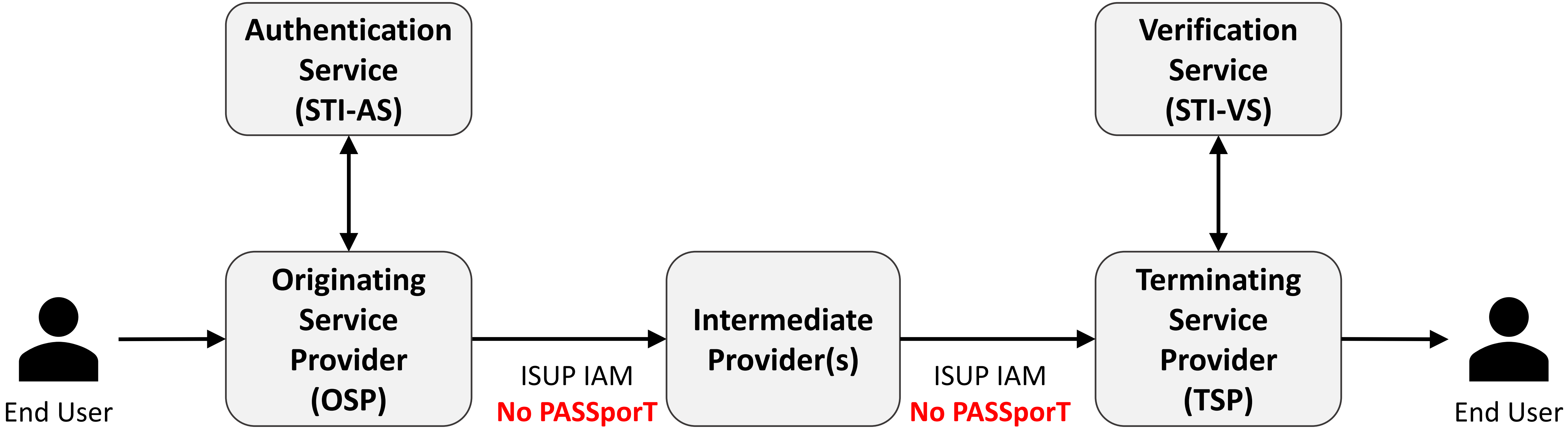
1. Verifies PASSporT signature
2. Creates verstat parameter
3. Often combined with call analytics


Authentication Service (STI-AS)
Verification Service (STI-VS)
End User
Originating Service Provider (OSP)
SIP INVITE with PASSporT
Intermediate Provider(s)
SIP INVITE with PASSporT
Terminating Service Provider (TSP)
End User

Non-SIP call, No SHAKEN

1. Determines the attestation level for the call
2. Creates a PASSporT that includes the attestation level
3. Signs the PASSporT using their certificate

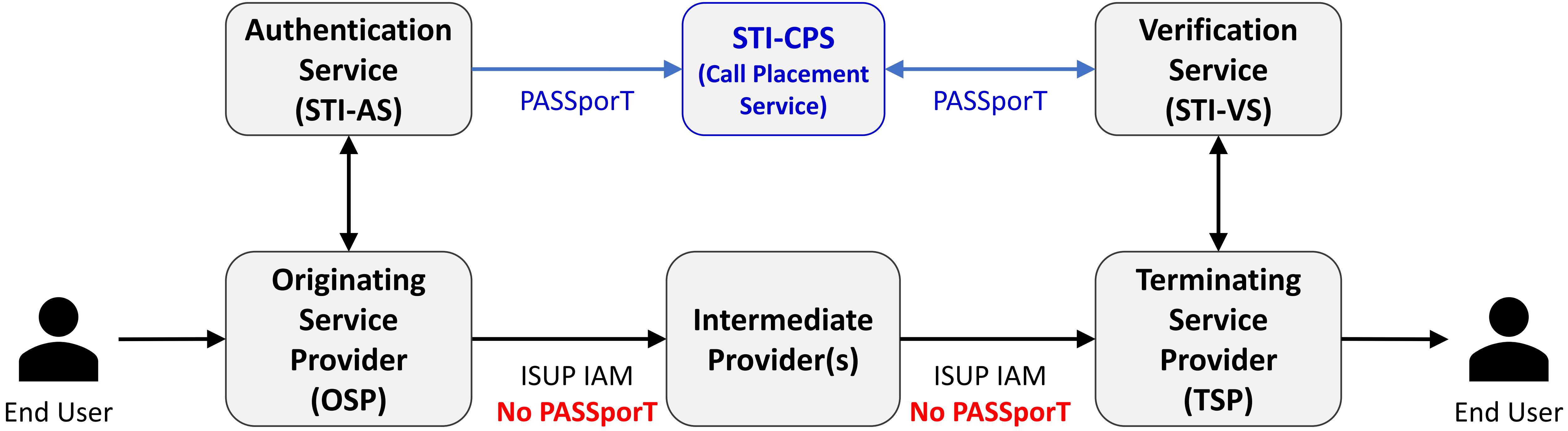
1. Verifies PASSporT signature
2. Creates verstat parameter
3. Often combined with call analytics


Authentication Service (STI-AS)
Verification Service (STI-VS)
End User
Originating Service Provider (OSP)
ISUP IAM
No PASSporT
Intermediate Provider(s)
ISUP IAM
No PASSporT
Terminating Service Provider (TSP)
End User

Non-SIP call with SHAKEN Out-of-Band

1. Determines the attestation level for the call
2. Creates a PASSporT that includes the attestation level
3. Signs the PASSporT using their certificate

1. Verifies PASSporT signature
2. Creates verstat parameter
3. Often combined with call analytics


Authentication Service (STI-AS)

PASSporT

STI-CPS (Call Placement Service)

PASSporT

Verification Service (STI-VS)

End User

Originating Service Provider (OSP)

ISUP IAM

No PASSporT

Intermediate Provider(s)

ISUP IAM

No PASSporT

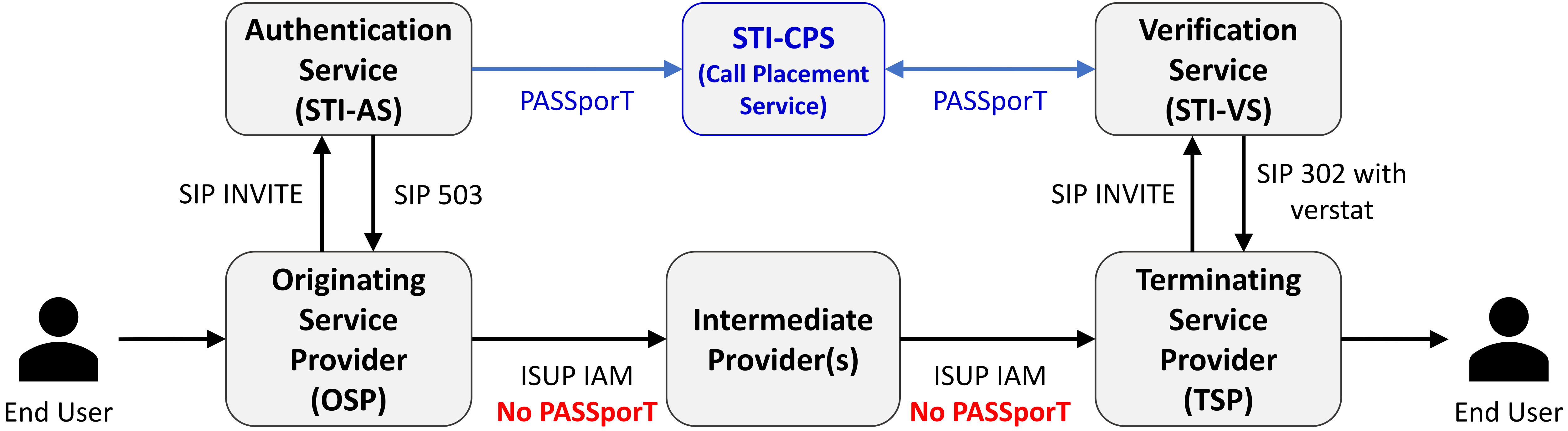
Terminating Service Provider (TSP)

End User

Non-SIP call with SHAKEN Out-of-Band

1. Determines the attestation level for the call
2. Creates a PASSporT that includes the attestation level
3. Signs the PASSporT using their certificate

1. Verifies PASSporT signature
2. Creates verstat parameter
3. Often combined with call analytics



Authentication Service (STI-AS)

PASSporT

STI-CPS (Call Placement Service)

PASSporT

Verification Service (STI-VS)

SIP INVITE

SIP 503

SIP INVITE

SIP 302 with verstat

End User

Originating Service Provider (OSP)

ISUP IAM

No PASSporT

Intermediate Provider(s)

ISUP IAM

No PASSporT

Terminating Service Provider (TSP)

End User

Out-of-Band SHAKEN

- Requires no network changes.
  - Only impacts the SHAKEN Authentication and SHAKEN Verification modules.
- Posting a PASSporT to the CPS is faster than call set-up.
- Only service providers can access the CPS
  - Posting or retrieving PASSporT requests must be signed with a SHAKEN certificate
- Supports multiple PASSporTs per call
  - DIV for forwarded calls
  - RCD for logos, images and call reason
  - RPH for emergency services

Comments to FCC on Out-of-Band SHAKEN

- Wabash was one of TransNexus's first live-production recipients of TDM SHAKEN three years ago, and has proudly been authenticating and verifying PSTN TDM calls, free from trouble or issue, since inception.

  - Wabash Communications reply comments to FCC, January 23, 2023

- Aureon has engaged TransNexus as its vendor for Out-of-Band.
  - Far easier than Non-IP In-Band
  - Vendors such as TransNexus have already developed Out-of-Band
  - Out-of-Band could reduce disputes regarding transport costs.

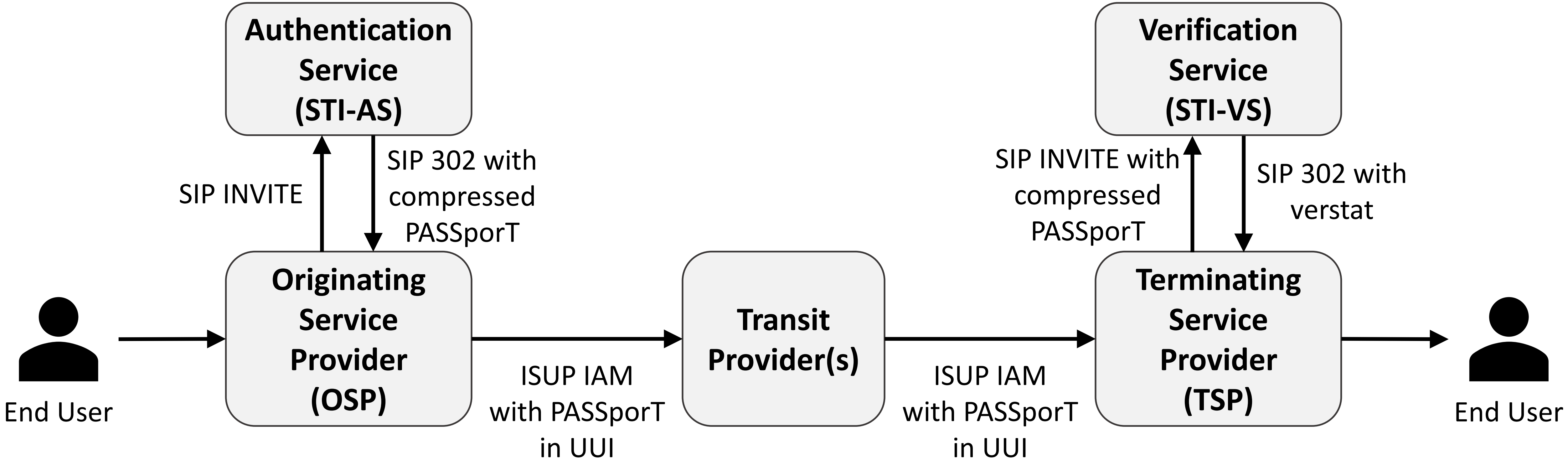
  - Aureon comments to FCC, December 12, 2022

Non-IP in-band SHAKEN

ATIS In-Band SHAKEN Standard 1000095

Non-IP in-band SHAKEN

1. Determines the attestation level for the call
2. Creates a PASSporT that includes the attestation level
3. Signs the PASSporT using their certificate


Authentication Service (STI-AS)
SIP INVITE
SIP 302 with compressed PASSporT
Verification Service (STI-VS)
SIP INVITE with compressed PASSporT
SIP 302 with verstat
End User
Originating Service Provider (OSP)
ISUP IAM with PASSporT in UUI
Transit Provider(s)
ISUP IAM with PASSporT in UUI
Terminating Service Provider (TSP)
End User

UUI = User to User Information Parameter

ISUP UUI encoding

Field	Bit positions	Value	Definition
UUI protocol discriminator	0 – 7	01001010	Per ITU Q.931, identifies UUIs intended use.
ppt/alg	8 – 13	000000	PASSporT type and algorithm.
attest	14 – 15	00 = “A” 01 = “B” 10 = “C”	Attestation level
x5u	16 – 103		ASCII encoded URL without protocol (assumes HTTPS) . Most significant bytes are padded with NULL characters (“00000000”).
iat	104 – 135		32-bit unsigned integer. Number of seconds since UNIX epoch.
origid	136 – 263		128-bit UUID
Signature	264 – 775		PASSporT signature

ISUP UUI encoding example

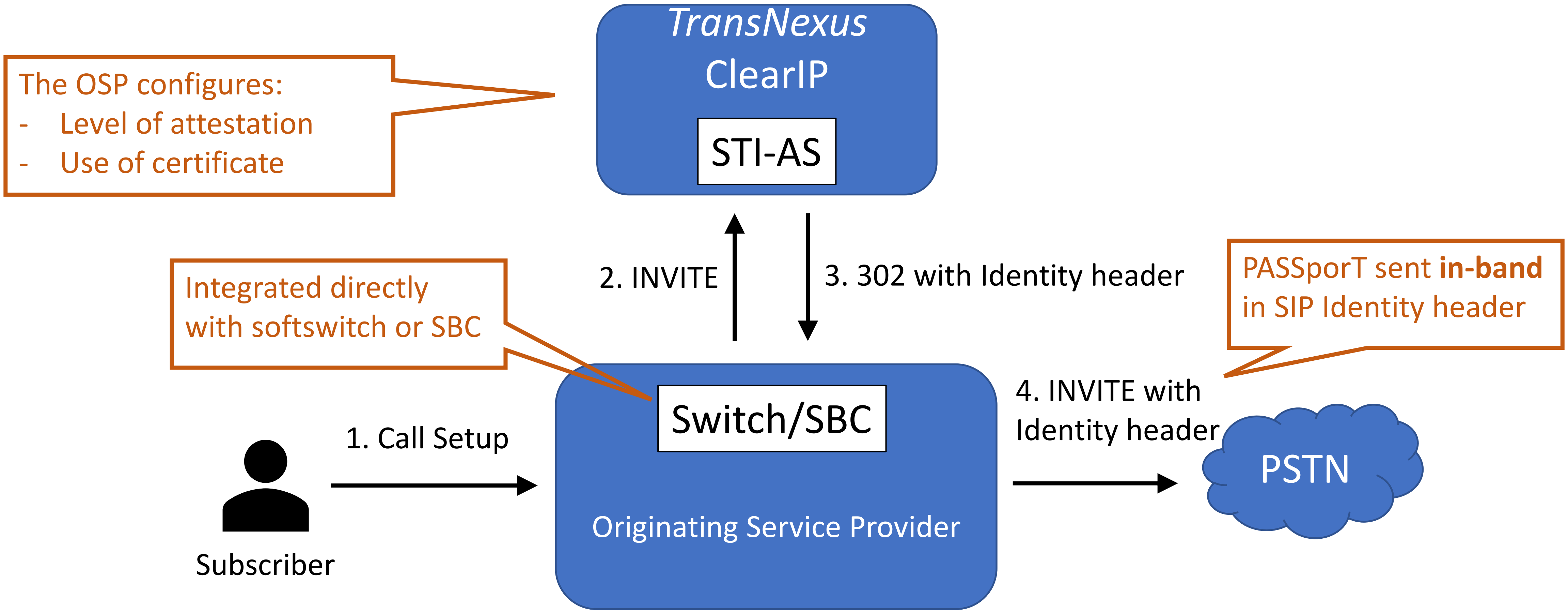
Field	Bit positions	Value
UUI protocol discriminator	0 – 7	01001010
ppt/alg	8 – 13	000000
attest	14 – 15	00
x5u (bit.ly/3odj5jb)	16 – 103	01100010 01101001 01110100 0000000001101100 01111001 00110011 01101111 01100100 01101010 00110101
iat	104 – 135	01100000 01110000 11001011 01110000
origid	136 – 263	00010010 00111110 01000101 01100111 11101000 10011011 00010010 11010011 10100100 01010110 01000010 01100110 01010101 01000100 00000000 00000000
Signature	264 – 775	11111101 01011110 00110101 01001110 00010100 01001001 11101111 10000011 00100100 10110111 00010111 10001011 00011001 10100110 01010000 00011000 00001000 10101011 11110010 10010111 00001000 10111110 01100000 01111010 00111001 00000001 00001100 10000001 00101110 00011000 10011011 10110001 01001111 11000000 01101100 01100110 11011110 11010000 11010100 01001101 00010100 11101001 01000011 10010101 11110100 10101101 11101001 01011000 10110001 11101011 01111110 00010001 00100111 00011011 11110110 10001011 01000101 00110100 00111100 01001110 00001001 00111000 11011110 10101110

Integration for SHAKEN Authentication

Three different options:

1. SIP Redirect
2. SIP Proxy
3. Restful HTTP API

STI-AS Integration Using SIP Redirect


TransNexus
ClearIP
STI-AS
2. INVITE
3. 302 with Identity header
Switch/SBC
Originating Service Provider
1. Call Setup
Subscriber
4. INVITE with Identity header
PSTN

The OSP configures:

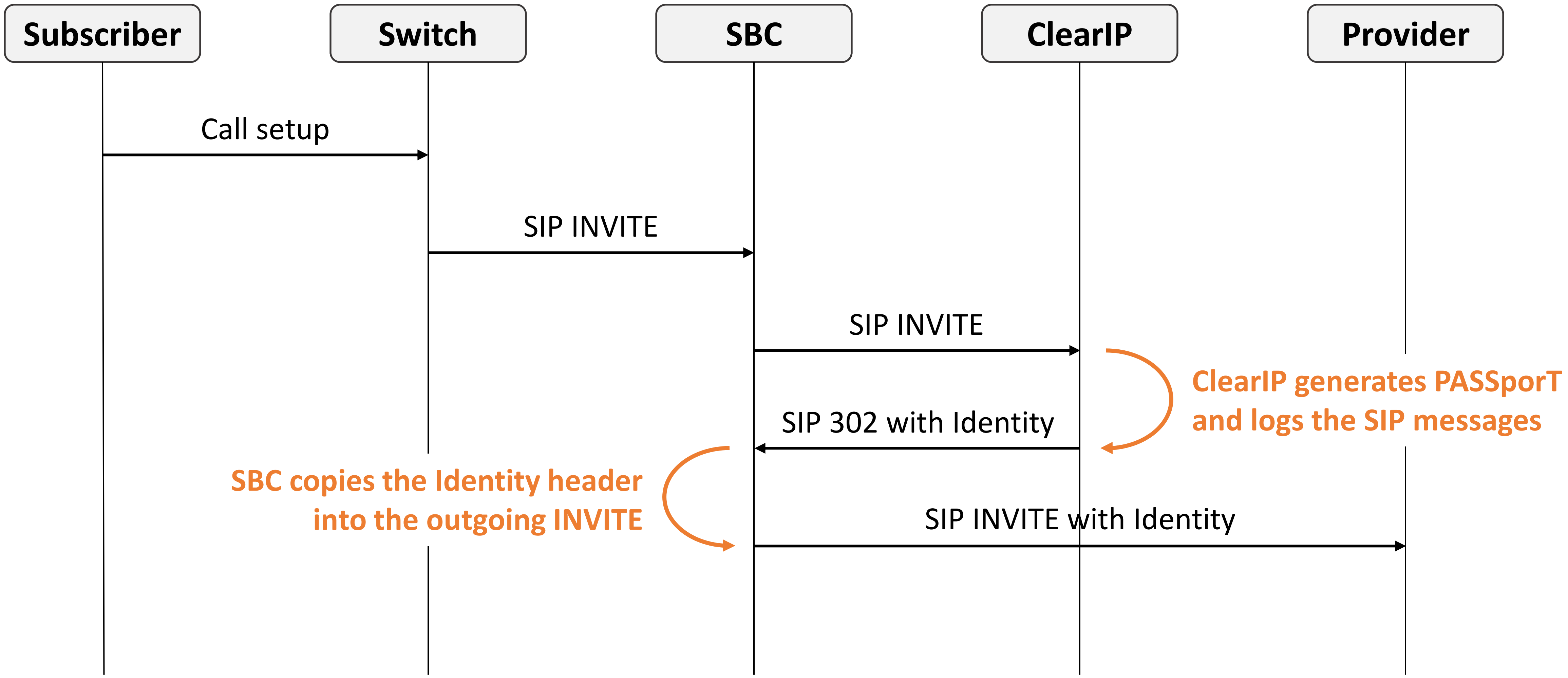
- Level of attestation
- Use of certificate

Integrated directly with softswitch or SBC

PASSporT sent **in-band** in SIP Identity header

Please find more information here: https://transnexus.com/clearip/

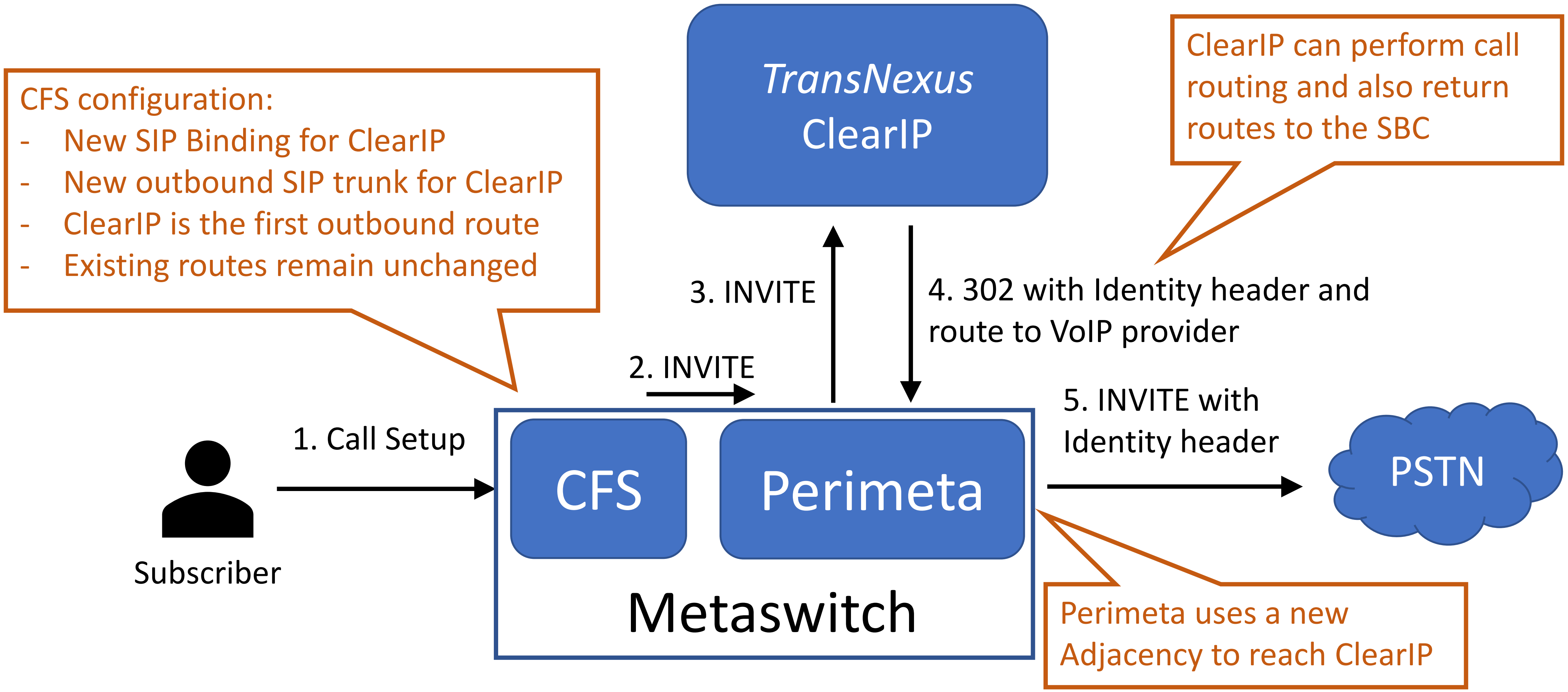
SIP Redirect Call Flow for In-Band



ClearIP generates PASSporT and logs the SIP messages

SBC copies the Identity header into the outgoing INVITE

Example: Integration with Metaswitch



CFS configuration:

- New SIP Binding for ClearIP
- New outbound SIP trunk for ClearIP
- ClearIP is the first outbound route
- Existing routes remain unchanged

TransNexus
ClearIP

ClearIP can perform call routing and also return routes to the SBC

Subscriber

1. Call Setup

2. INVITE

3. INVITE

4. 302 with Identity header and route to VoIP provider

5. INVITE with Identity header

CFS

Perimeta

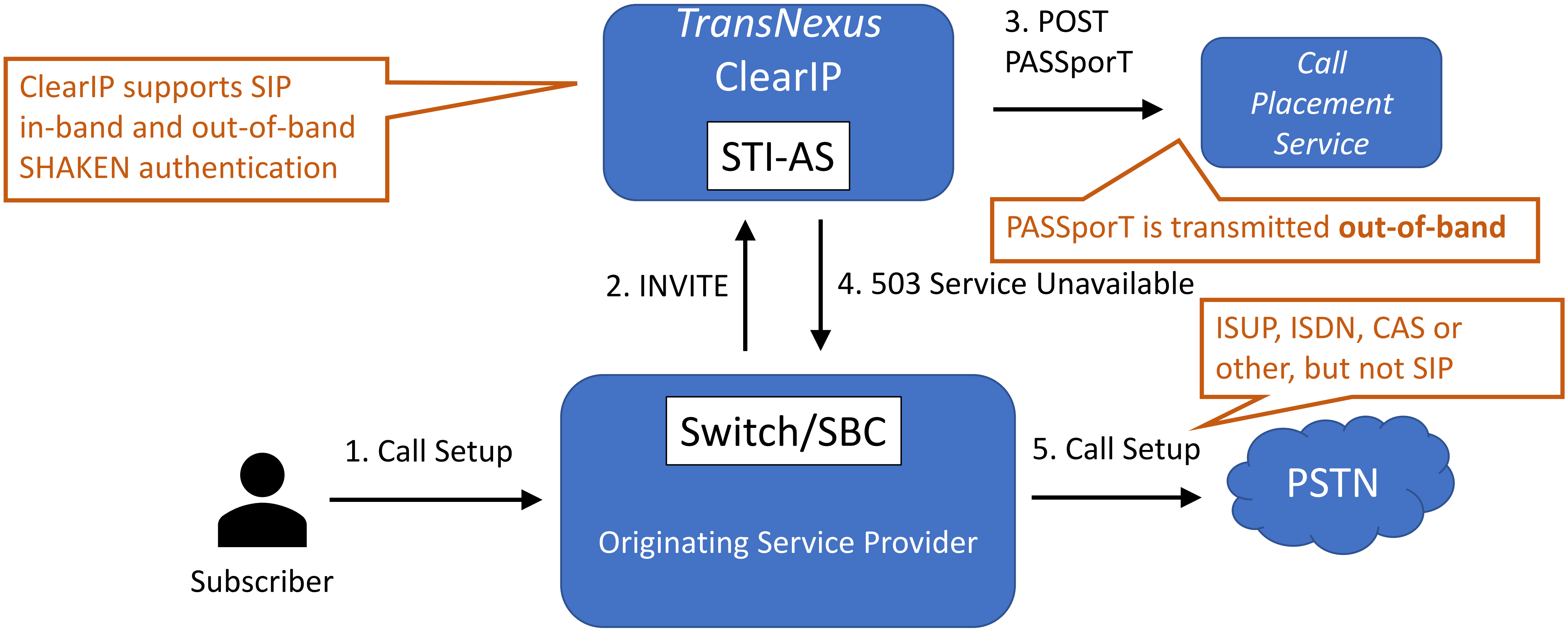
Metaswitch

PSTN

Perimeta uses a new Adjacency to reach ClearIP

Please find more information here: https://transnexus.com/docs/clearip-metaswitch-config-outbound/

STI-AS Integration for Out-of-Band



TransNexus ClearIP

STI-AS

ClearIP supports SIP in-band and out-of-band SHAKEN authentication

3. POST PASSporT

Call Placement Service

PASSporT is transmitted **out-of-band**

2. INVITE

4. 503 Service Unavailable

ISUP, ISDN, CAS or other, but not SIP

Switch/SBC

Originating Service Provider

1. Call Setup

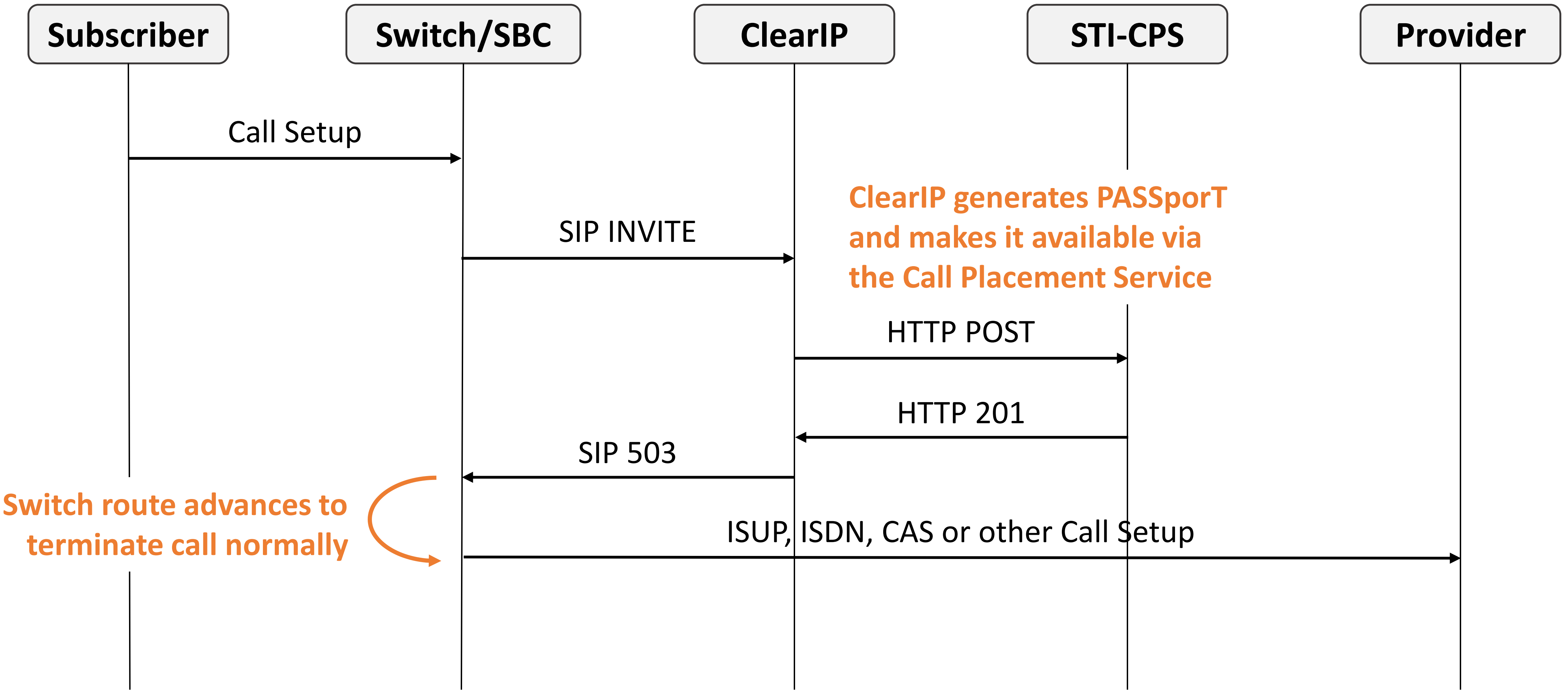
5. Call Setup

PSTN

Subscriber

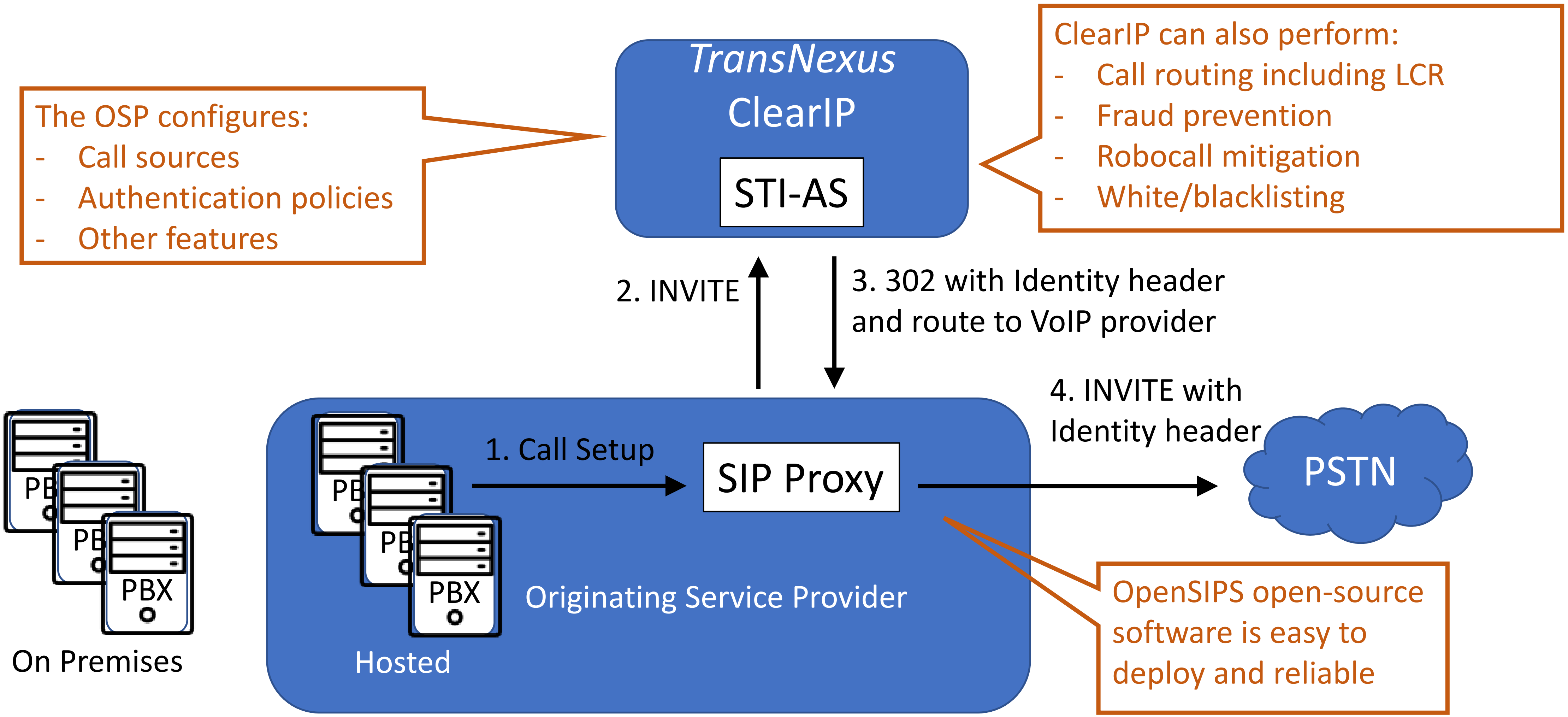
Please find more information here: https://transnexus.com/whitepapers/out-of-band-shaken/

SIP Redirect Call Flow for Out-of-Band



Subscriber
Switch/SBC
ClearIP
STI-CPS
Provider
Call Setup
SIP INVITE
ClearIP generates PASSporT and makes it available via the Call Placement Service
HTTP POST
HTTP 201
SIP 503
Switch route advances to terminate call normally
ISUP, ISDN, CAS or other Call Setup

STI-AS Integration Using SIP Proxy



The OSP configures:
- Call sources
- Authentication policies
- Other features

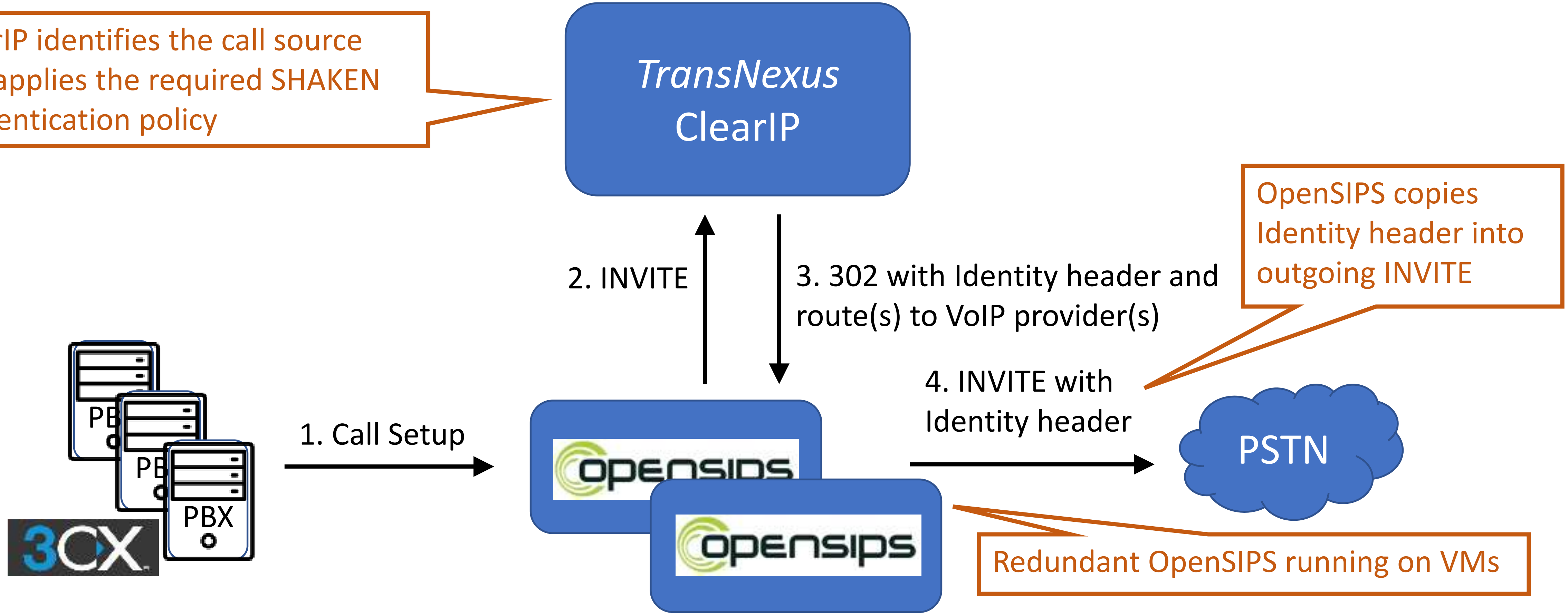
ClearIP can also perform:
- Call routing including LCR
- Fraud prevention
- Robocall mitigation
- White/blacklisting

OpenSIPS open-source software is easy to deploy and reliable

TransNexus
ClearIP
STI-AS
2. INVITE
3. 302 with Identity header and route to VoIP provider
4. INVITE with Identity header
PSTN
1. Call Setup
SIP Proxy
PBX
Originating Service Provider
Hosted
On Premises

Please find more information here: https://transnexus.com/clearip-inline-proxy/

Example: Integration for 3CX



ClearIP identifies the call source and applies the required SHAKEN authentication policy

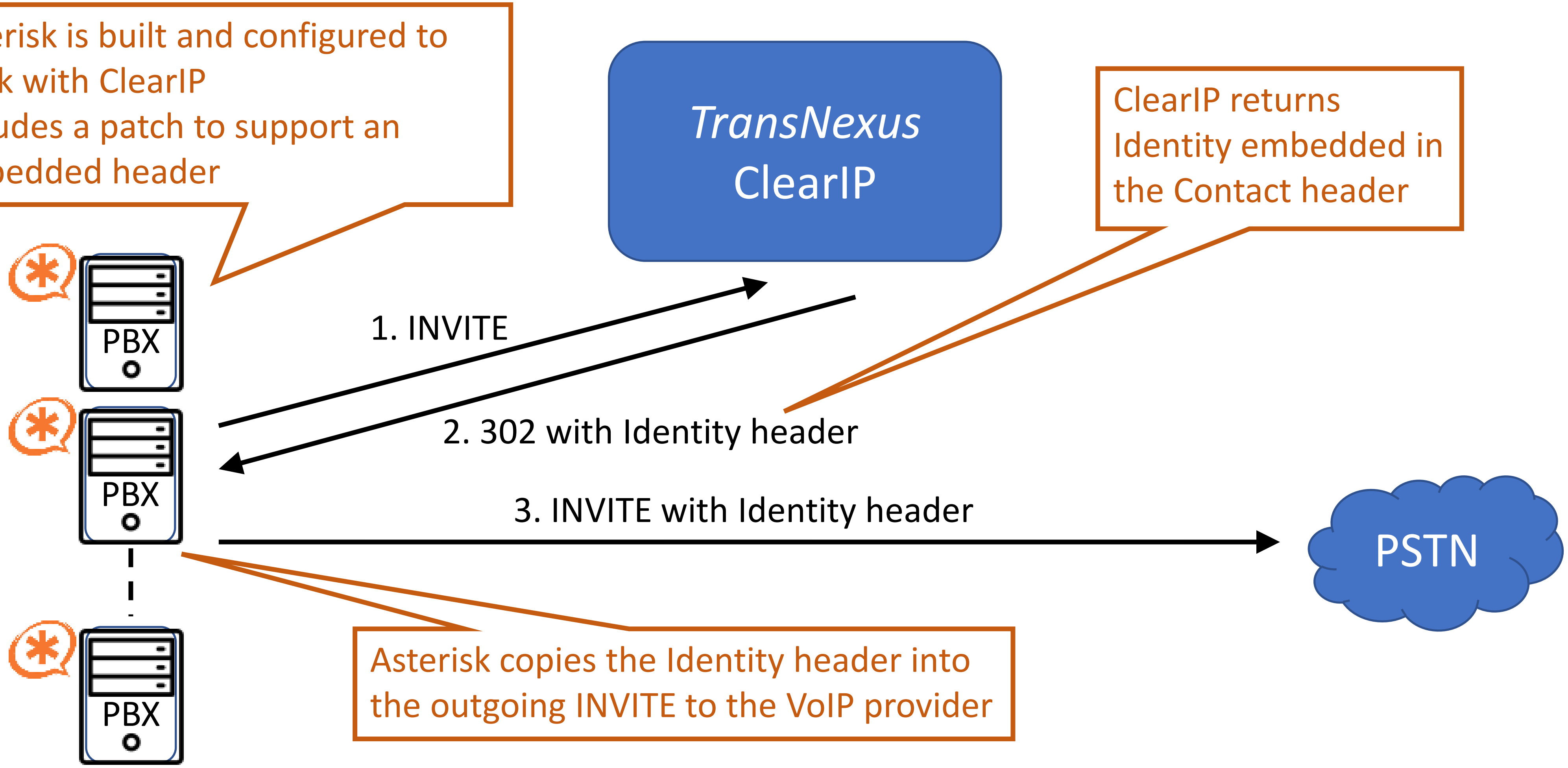
OpenSIPS copies Identity header into outgoing INVITE

Redundant OpenSIPS running on VMs

TransNexus
ClearIP
2. INVITE
3. 302 with Identity header and route(s) to VoIP provider(s)
PBX
PBX
PBX
3CX
1. Call Setup
opensips
opensips
4. INVITE with Identity header
PSTN

Please find more information here: https://transnexus.com/docs/clearip-asterisk-inline-routing-shaken/

Example: Integration for MSPs Using Asterisk



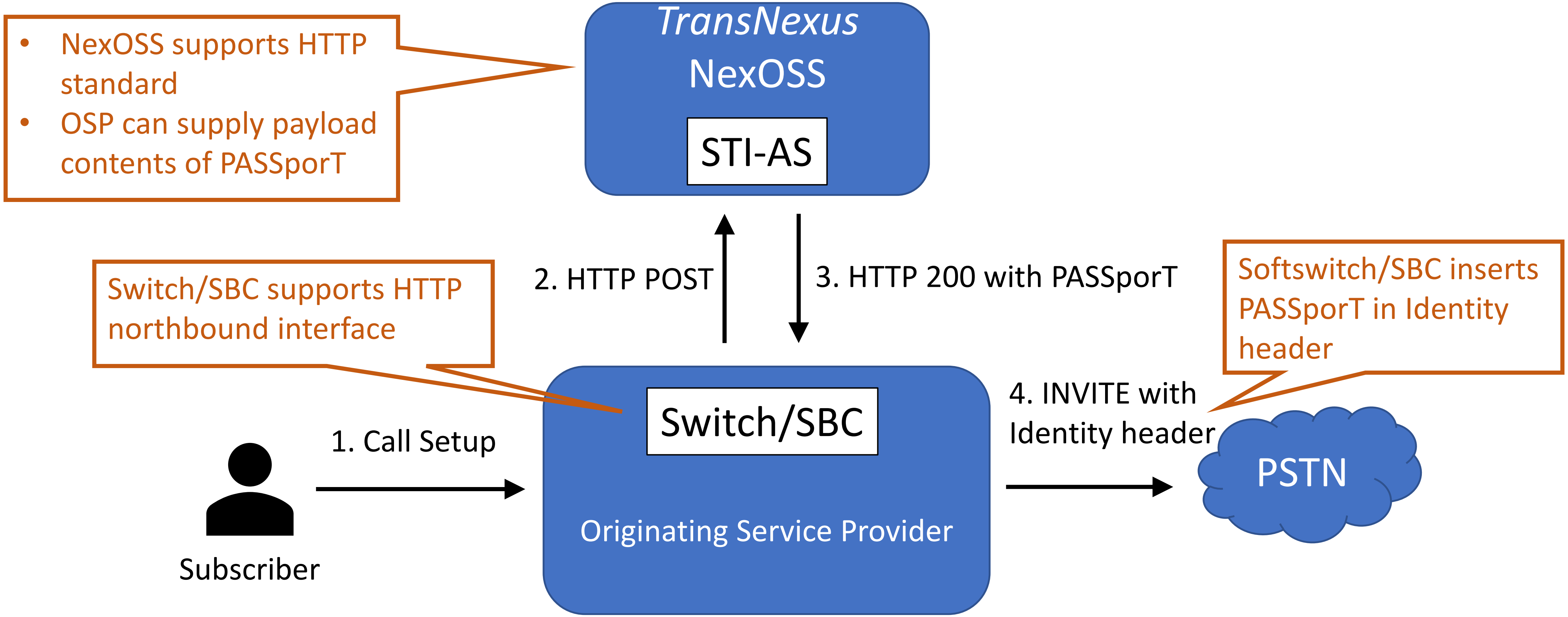
- Asterisk is built and configured to work with ClearIP
- Includes a patch to support an embedded header

ClearIP returns Identity embedded in the Contact header

Asterisk copies the Identity header into the outgoing INVITE to the VoIP provider

Please find more information here: https://transnexus.com/docs/clearip-asterisk-config-shaken-cnam/

STI-AS Integration Using HTTP



TransNexus
NexOSS
STI-AS
2. HTTP POST
3. HTTP 200 with PASSporT
Switch/SBC
Originating Service Provider
1. Call Setup
Subscriber
4. INVITE with Identity header
PSTN

- NexOSS supports HTTP standard
- OSP can supply payload contents of PASSporT

Switch/SBC supports HTTP northbound interface

Softswitch/SBC inserts PASSporT in Identity header

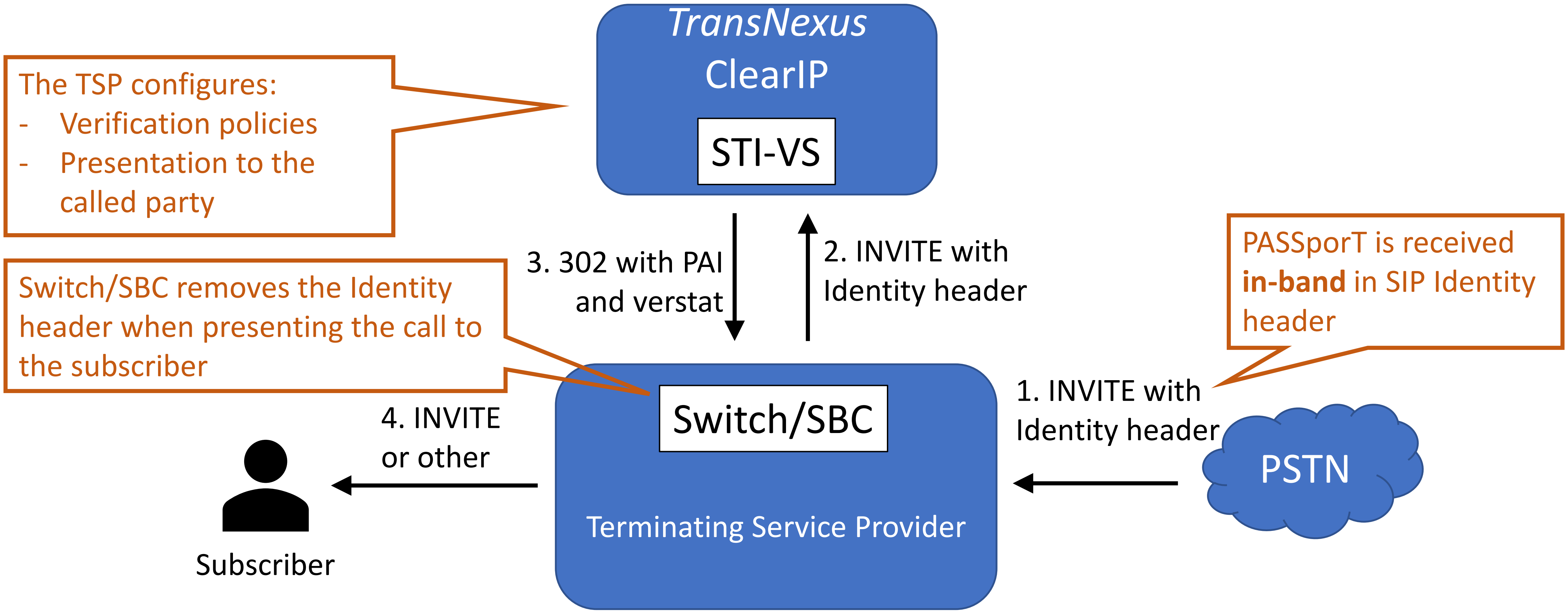
Please find more information here: https://transnexus.com/nexoss-centralized-shaken-server/

Integration for SHAKEN Verification

Three different options:

1. SIP Redirect
2. SIP Proxy
3. Restful HTTP API

STI-VS Integration Using SIP Redirect



TransNexus
ClearIP

STI-VS

The TSP configures:
- Verification policies
- Presentation to the called party

Switch/SBC removes the Identity header when presenting the call to the subscriber

3. 302 with PAI and verstat

2. INVITE with Identity header

PASSporT is received **in-band** in SIP Identity header

Switch/SBC

Terminating Service Provider

1. INVITE with Identity header

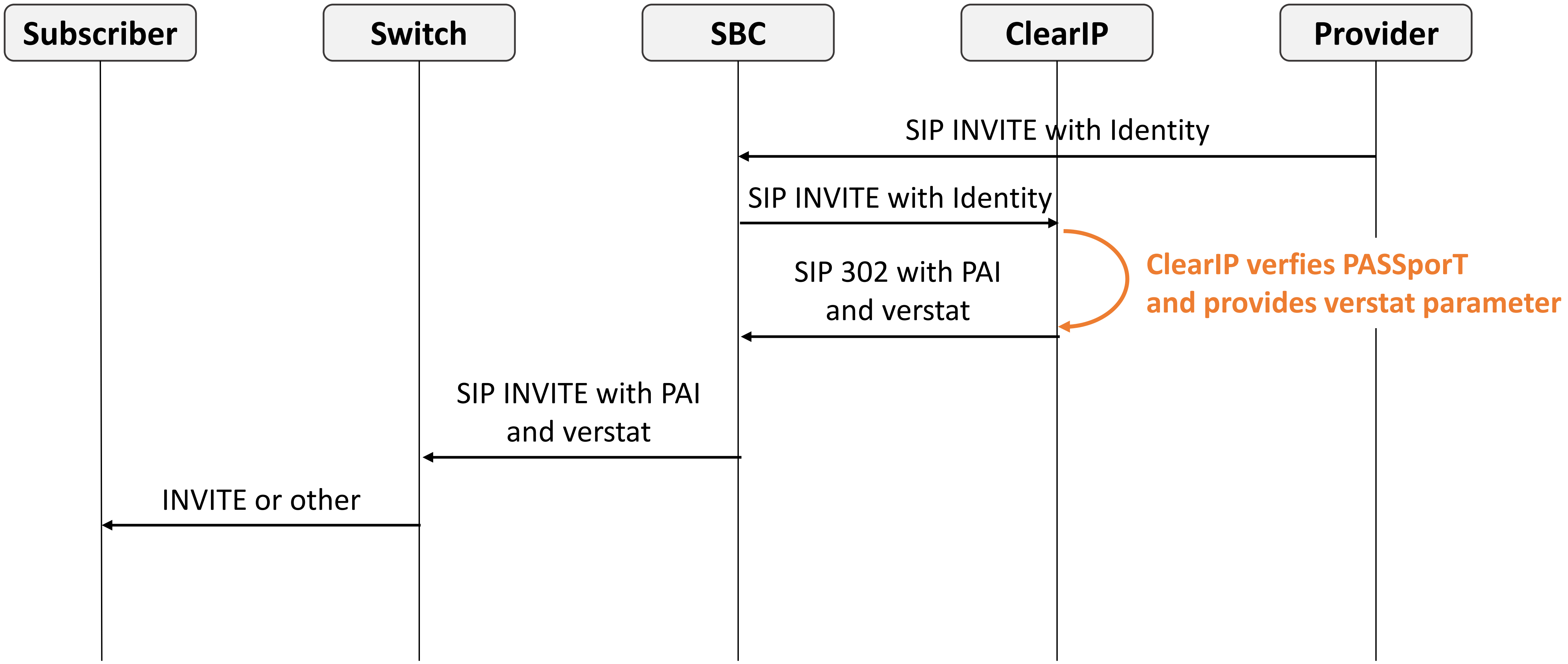
PSTN

4. INVITE or other

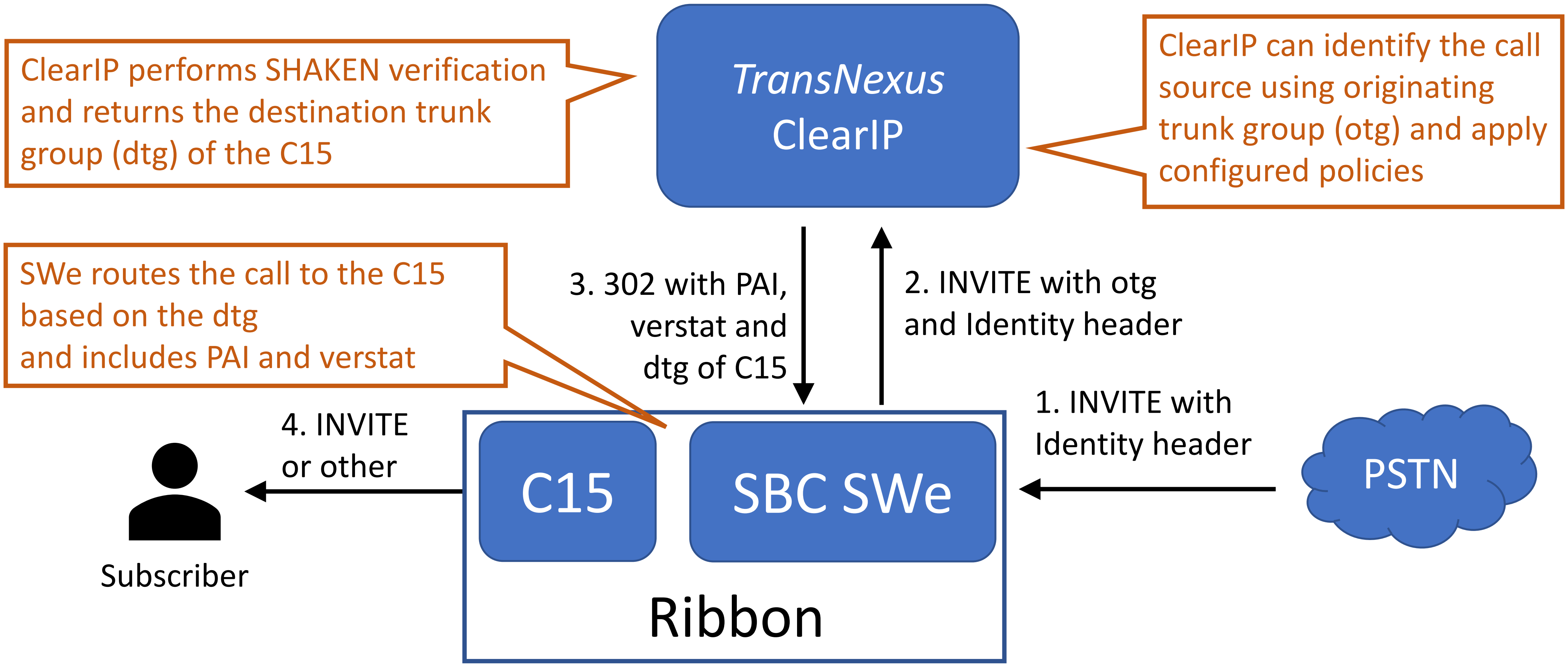
Subscriber

Please find more information here: https://transnexus.com/whitepapers/shaken-vs/

SIP Redirect Call Flow for In-Band


Subscriber
Switch
SBC
ClearIP
Provider
SIP INVITE with Identity
SIP INVITE with Identity
SIP 302 with PAI and verstat
ClearIP verfies PASSporT and provides verstat parameter
SIP INVITE with PAI and verstat
INVITE or other

Example: Integration with Ribbon Communications



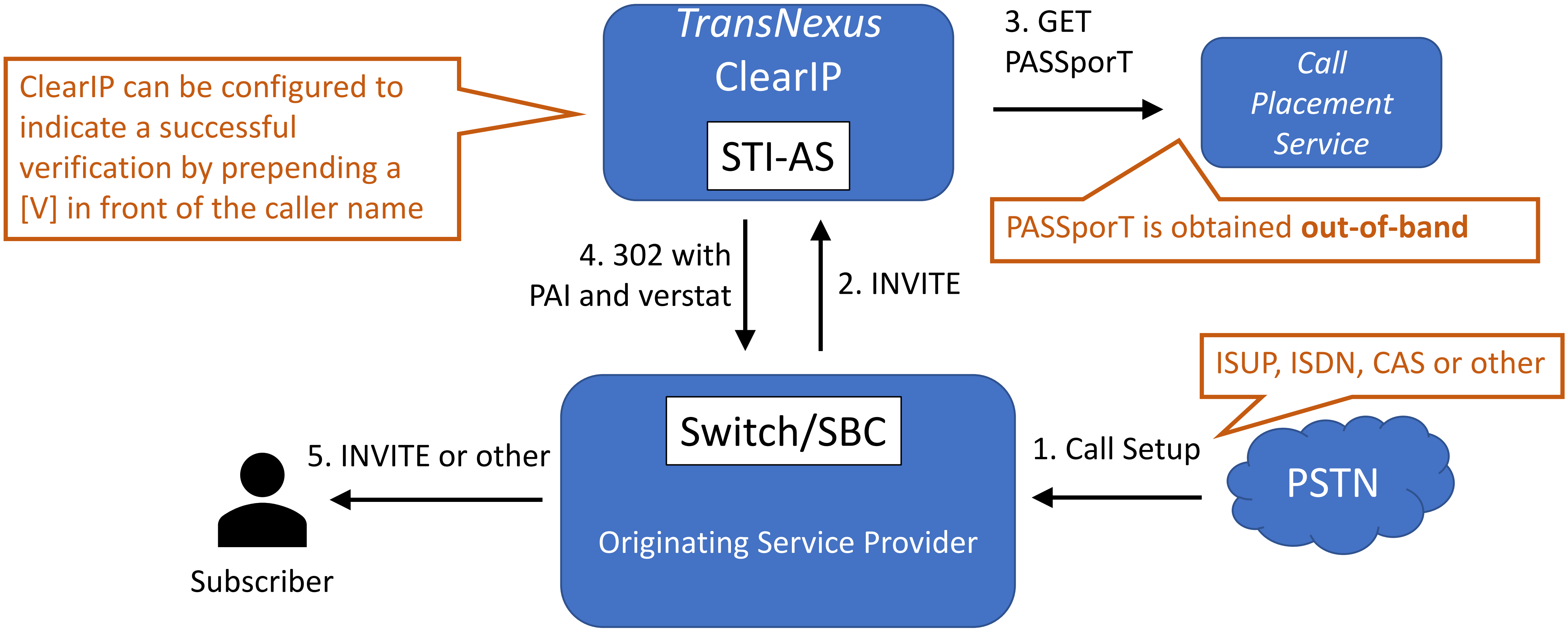
ClearIP performs SHAKEN verification and returns the destination trunk group (dtg) of the C15

ClearIP can identify the call source using originating trunk group (otg) and apply configured policies

SWe routes the call to the C15 based on the dtg and includes PAI and verstat

TransNexus
ClearIP
3. 302 with PAI, verstat and dtg of C15
2. INVITE with otg and Identity header
1. INVITE with Identity header
4. INVITE or other
C15
SBC SWe
Ribbon
PSTN
Subscriber

STI-VS Integration for Out-of-Band



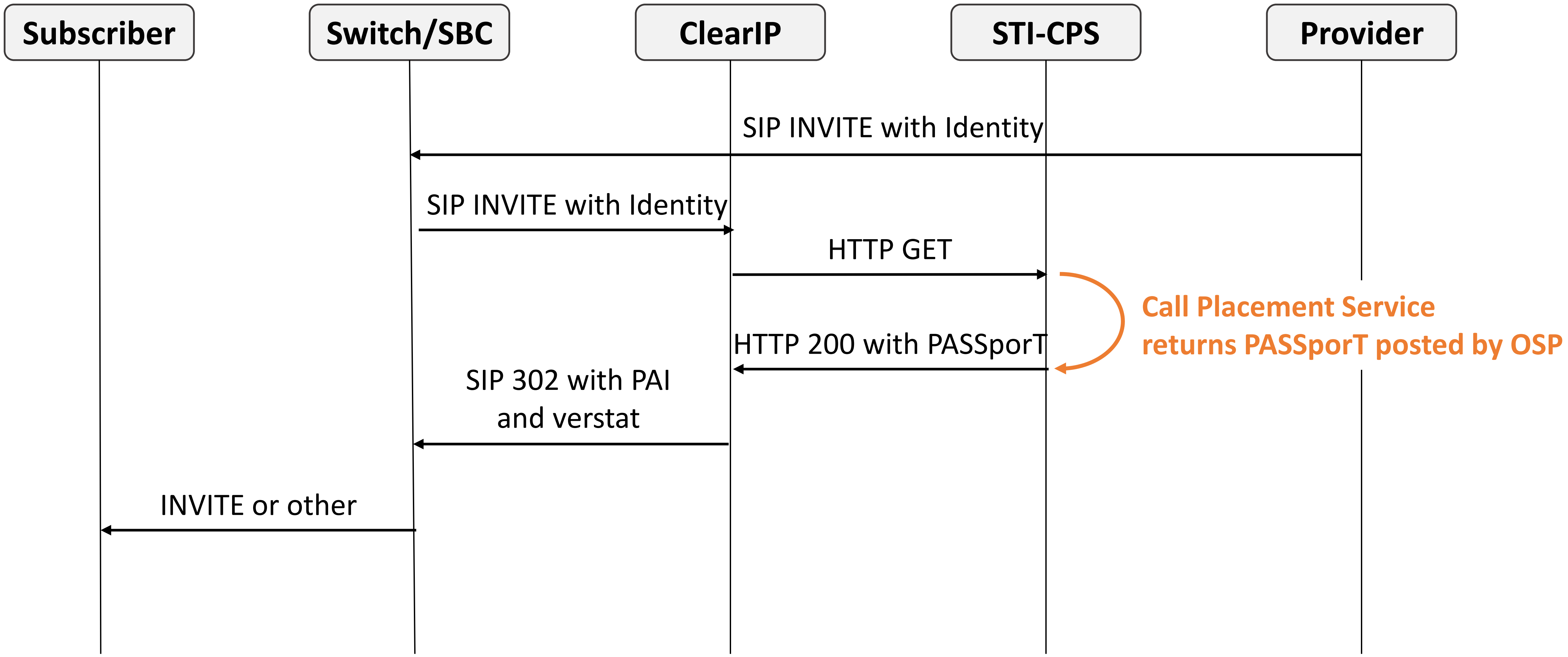
ClearIP can be configured to indicate a successful verification by prepending a [V] in front of the caller name

PASSporT is obtained **out-of-band**

ISUP, ISDN, CAS or other

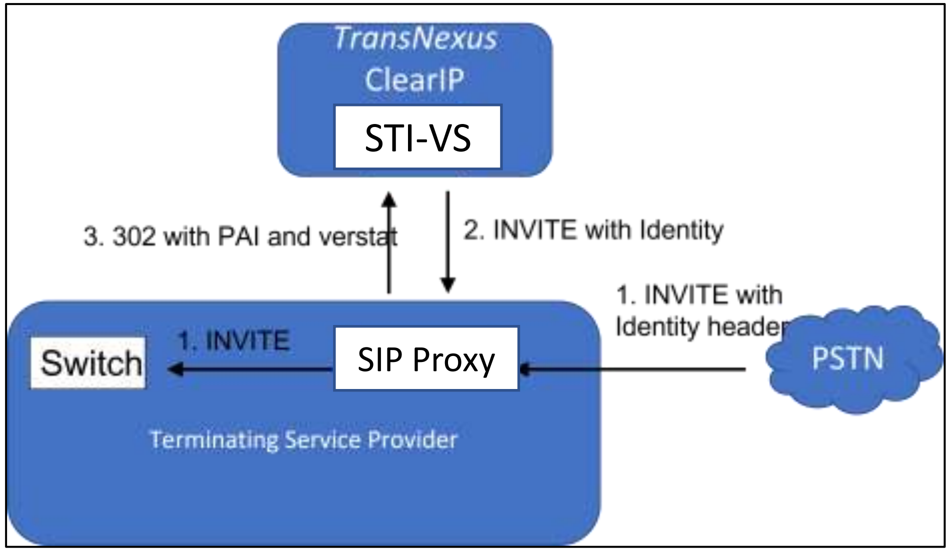
Please find more information here: https://transnexus.com/whitepapers/out-of-band-shaken/

SIP Redirect Call Flow for Out-of-Band

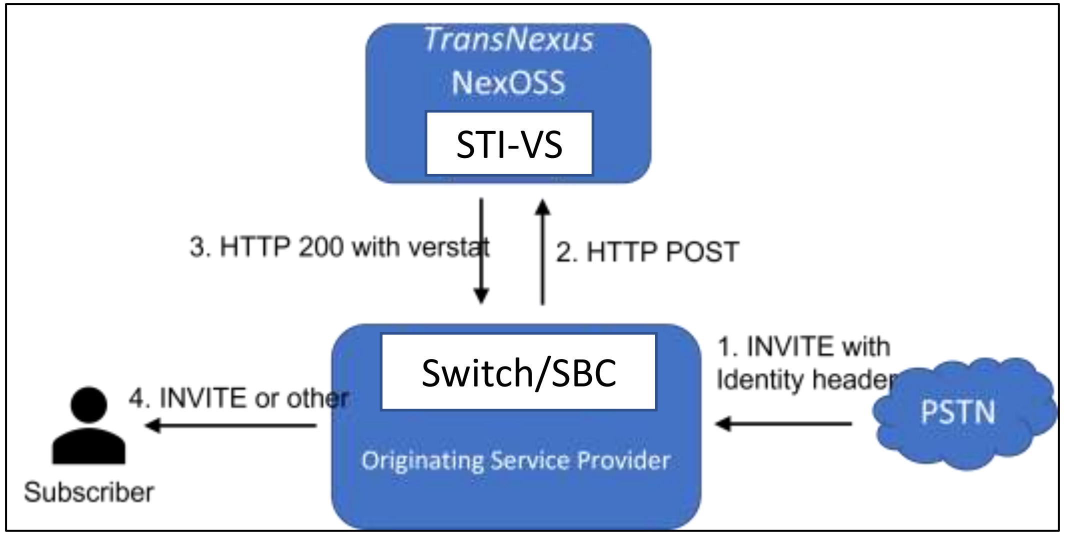


Call Placement Service returns PASSporT posted by OSP

Other STI-VS Integration Options


TransNexus
ClearIP
STI-VS
3. 302 with PAI and verstat
2. INVITE with Identity
1. INVITE with Identity header
PSTN
Switch
1. INVITE
SIP Proxy
Terminating Service Provider

SIP proxy enables any SIP network to perform SHAKEN verification



NexOSS supports an HTTP interface for SHAKEN verification

Conclusions, Questions and Answers

- Many implementation options
- Do not wait to start
  - Registration with STI-PA takes time
  - Implementation takes time
  - Backlogs are increasing
- Contact info@TransNexus.com for more information
- Presenters
  - Jim.Dalton@TransNexus.com
  - Marc.St-Onge@TransNexus.com

More resources

- Telecom glossary
- SHAKEN whitepapers
    - Understanding STIR/SHAKEN
    - Certificate management for STIR/SHAKEN
    - STIR/SHAKEN authentication service
    - STIR/SHAKEN verification service
- SHAKEN standards
    - ATIS-1000074.v003
    - ATIS-1000080.v004
- SHAKEN regulations
    - Code of Federal Regulations - Caller ID Authentication
    - TRACED Act
    - First Report and Order
    - Second Report and Order
    - Third Report and Order
    - Fourth Report and Order
    - Fifth Report and Order
- Useful tools
    - Decode PASSporT
    - Parse certificate