TransNexus

Advocates for Rural Broadband

Get ready for STIR/SHAKEN

2022-12-13

Presenters

Jim Dalton
TransNexus, Inc.
Chief Executive Officer

Alec Fenichel
TransNexus, Inc.
Chief Technology Officer

The SIP School

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'

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

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

Agenda

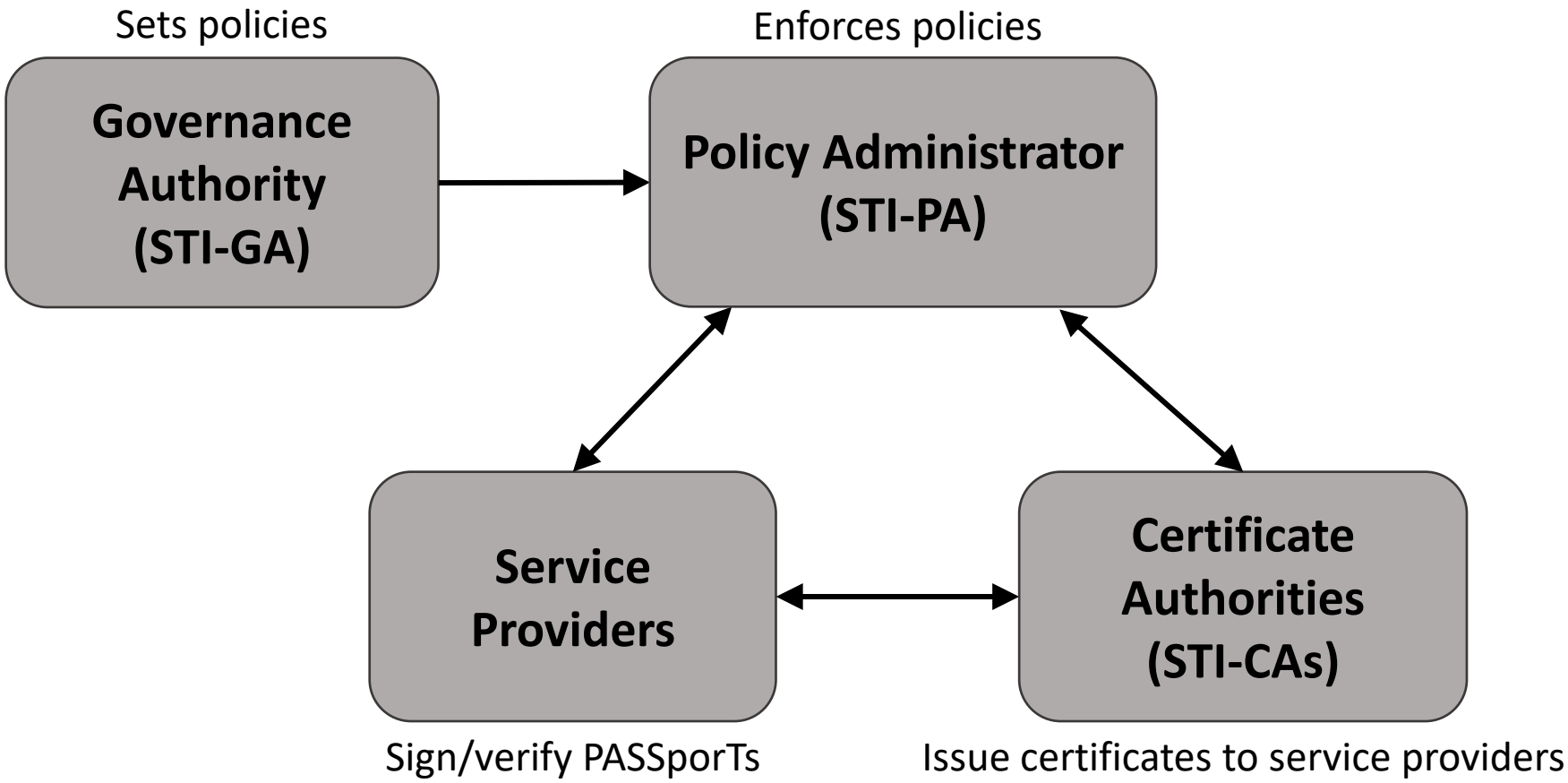
- SHAKEN overview
- Non-IP out-of-band SHAKEN
- Non-IP in-band SHAKEN
- Integration
- Questions and answers

SHAKEN overview

What does SHAKEN do?

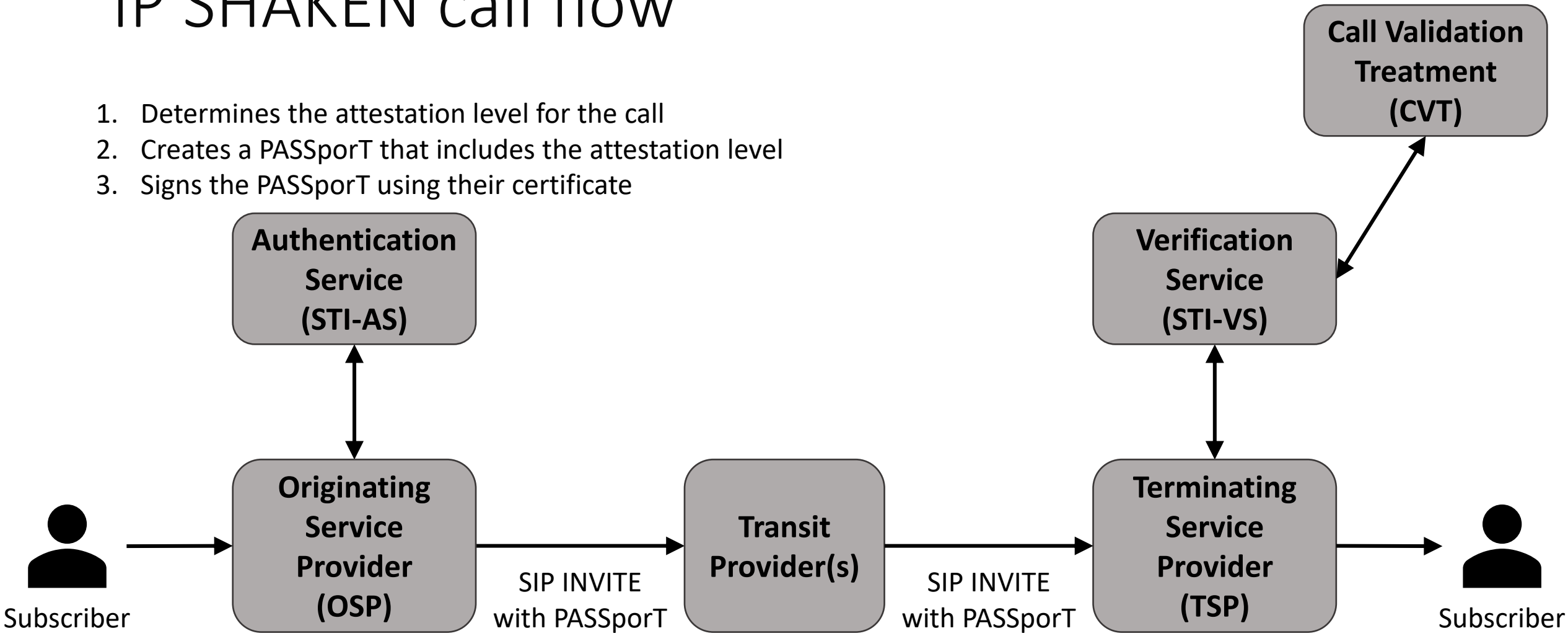
- Identifies the service provider who originated the call
- Allows the service provider to attest
  - If they know the end-user who placed the call
  - If they know the end-user is authorized to use the calling number
- Does not directly indicate whether a call is wanted versus unwanted
- Provides information to the Call Validation Treatment (CVT) which determines whether a call is wanted versus unwanted

SHAKEN ecosystem



IP SHAKEN call flow

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



Attestation levels

- A – Full attestation
  - Is responsible for the origination of the call onto the IP based service provider voice network.
  - 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
  - Is responsible for the origination of the call onto the IP-based service provider voice network.
  - Has a direct authenticated relationship with the customer and can identify the customer.
  - Has NOT established a verified association with the telephone number used for the call.
- C – Gateway attestation
  - Has no relationship with the initiator of the call (e.g., international gateways).

SIP INVITE with PASSporT

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
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1NTEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V41ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-EScb9otFNDxOCTjerg ;info=<https://cert.example.org/passport.pem>;ppt="shaken"
Content-Length: 122

v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
s=-
c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv

Decoded PASSporT

Header


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


Signature


```
_V41ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0re
lYset-EScb9otFNDxOCTjerg
```


Payload


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

Certificate

-----BEGIN CERTIFICATE-----
MIIC8zCCApmgAwIBAgIQaP0LzopRzU51HiJ77zNgjzAKBggqhkjOPQQDAjBnMQsw
CQYDVQQGEwJVUzEZMBcGA1UEChMQVHJhbnNOZXh1cywgSW5jLjEPMA0GA1UECxMG
U0hBS0VOMSwwKgYDVQQDEyNUcmFuc05leHVzLCBJbmMuIFNIQUtFTiBJc3N1aW5n
IENBMzAeFw0yMjA3MDcyMDA5NTFaFw0yMjA3MTQyMDA5NTBaMFAxCzAJBgNVBAYT
AlVTMRowGAYDVQQKExFBc3N1cmFuY2UgVGVsZWNvbTEPMA0GA1UECxMGU0hBS0VO
MRQwEgYDVQQDEwtTSEFLRU4gNTE4SjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IA
BNWJ/aw7x2dfCbEsYMww8uWpEklQhsa3S2sgoN3wTsj9H4FF20YmAztvCmxYqaV6
r90/0OeTVujyLl7OaHpYrN+jggE8MIIBODAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB
/wQEAwIAgDAdBgNVHQ4EFgQUNl9OGRW3XhxGc9i3QbRFccD8qYwwHwYDVR0jBBgw
FoAUu5beMRLN05aZhKQ2MGA811KBfScwFwYDVR0gBBAwDjAMBgpghkgBhv8JAQED
MIGmBgNVHR8EgZ4wgZswgZigOqA4hjZodHRwczovL2F1dGhlbnRpY2F0ZS1hcGku
aWNvbmVjdGl2LmNvbS9kb3dubG9hZC92MS9jcmyiWqRYMFYxFDASBgNVBAcMC0Jy
aWRnZXdhdGVyMQswCQYDVQQIDAJOSjETMBEGA1UEAwwKU1RJLVBBIENSTDELMAkG
A1UEBhMCVVMxDzANBgNVBAoMBlNUSS1QQTAWBggrBgEFBQcBGgQKMAigBhYENTE4
SjAKBggqhkjOPQQDAgNIADBFAiB89BGf1siNx0kPkbQ/Jr2t63JaUpDfd1Y2ciCy
D5y+KAIhAJtWZai36eBbb/cRXwpwFgRh2BdOcc/fY4Ves863zQzX
-----END CERTIFICATE-----

Parsed certificate

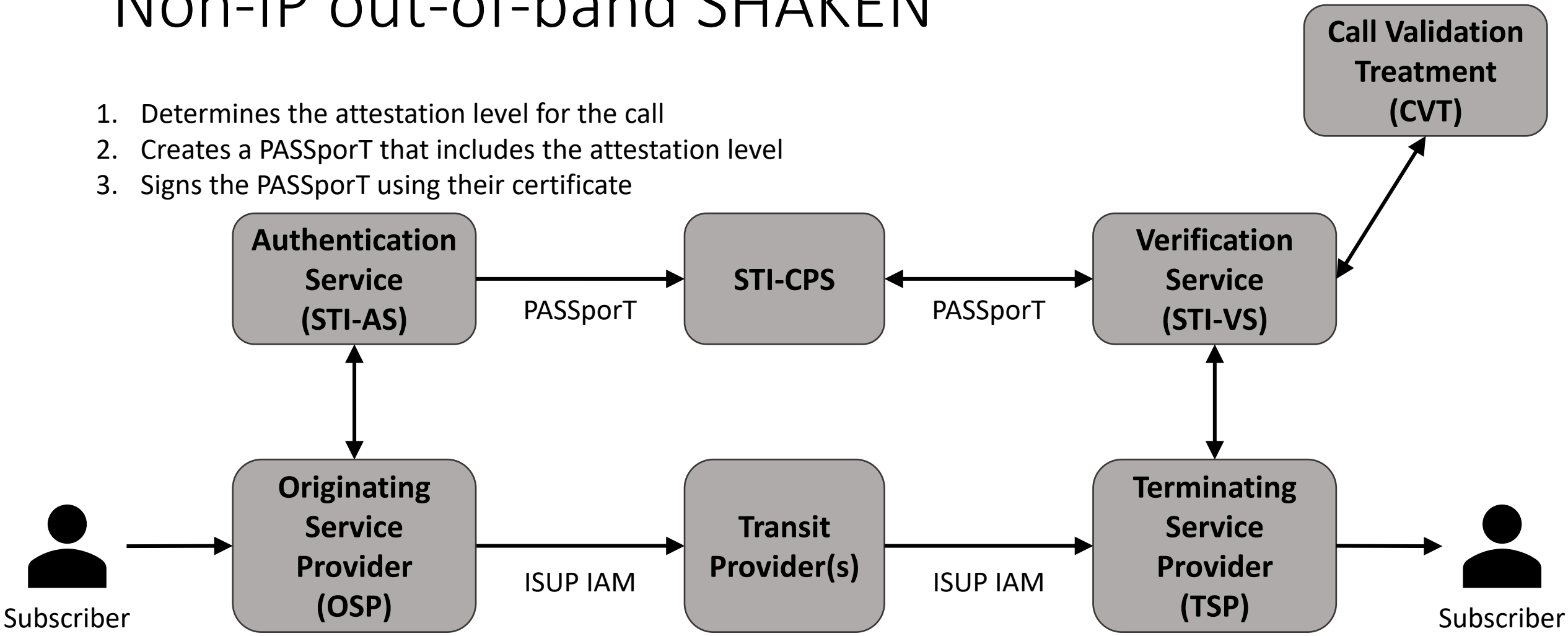
Version: 3
Serial Number: 68:fd:0b:ce:8a:51:cd:4e:75:1e:22:7b:ef:33:60:8f
Signature Algorithm: ecdsa-with-SHA256
Issuer: C=US, O=TransNexus, Inc., OU=SHAKEN, CN=TransNexus, Inc. SHAKEN Issuing CA3
Subject: C=US, O=Assurance Telecom, OU=SHAKEN, CN=SHAKEN 518J
Validity:
  Not Before: Jul 7 20:09:51 2022 GMT
  Not After: Jul 14 20:09:50 2022 GMT
X509v3 extensions:
  TN Auth List:
    Service Provider Code: 518J
  Basic Constraints: critical
    CA: FALSE
  Key Usage: critical
    Digital Signature
  Subject Key Identifier:
    36:5F:4E:19:15:B7:5E:1C:46:73:D8:B7:41:B4:45:71:C0:FC:A9:8C
  Authority Key Identifier:
    BB:96:DE:31:12:CD:D3:96:99:84:A4:36:30:60:3C:D7:52:81:7D:27
  Certificate Policies:
    Policy: 2.16.840.1.114569.1.1.3
  CRL Distribution Points:
    Full Name:
      URI: https://authenticate-api.iconectiv.com/download/v1/crl
    CRL Issuer:
      Directory Name: L=Bridgewater, ST=NJ, CN=STI-PA CRL, C=US, O=STI-PA

TransNexus®

Non-IP out-of-band SHAKEN

Non-IP out-of-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



STI-CPS API endpoints

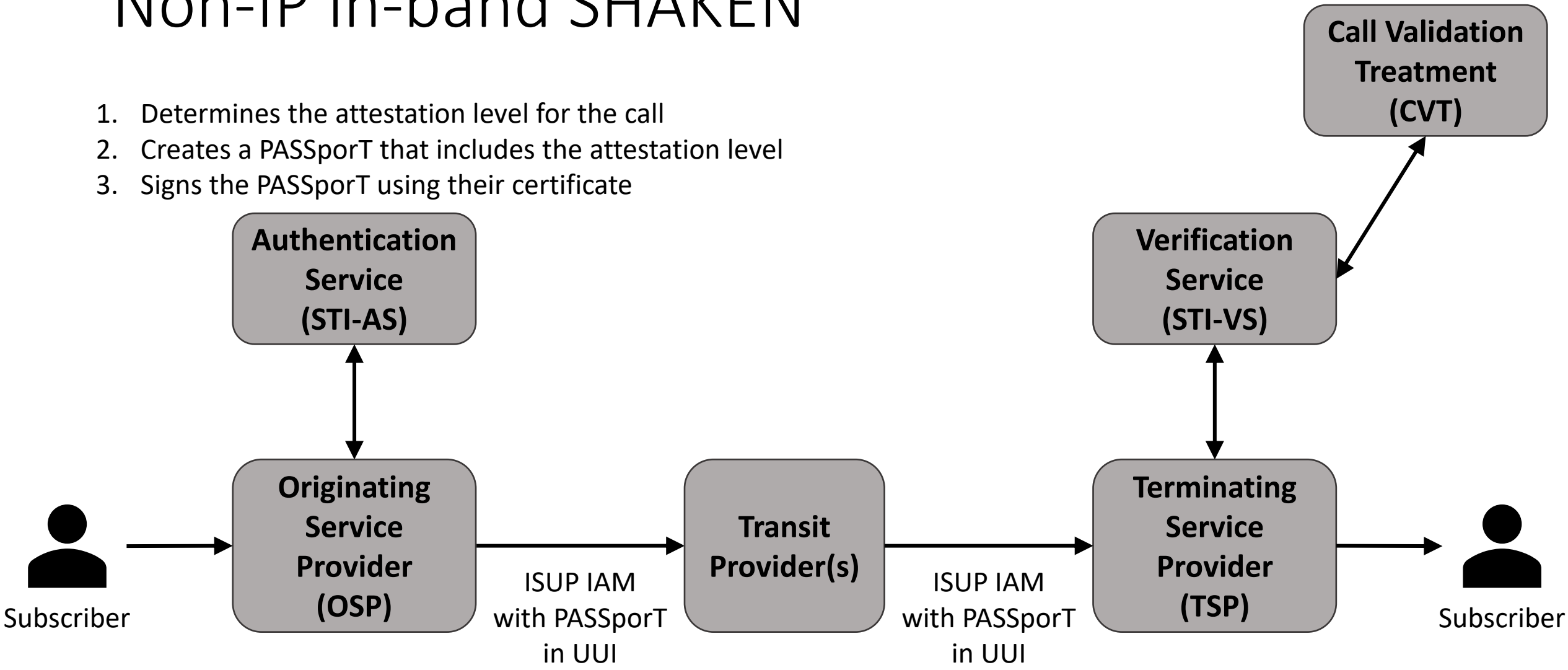
Path	Method	Description	Authentication	Request Body	Successful Response Code	Successful Response Body
/health	GET	Check STI-CPS health	None	N/A	200	{ "status": 200, "message": "OK" }
/passports/DEST/ORIG	POST	Publish PASSporT(s)	JWT signed by SHAKEN certificate	{ "passports": ["…"] }	201	{ "status": 201, "message": "Created" }
/passports/DEST/ORIG	GET	Retrieve PASSporT(s)	JWT signed by SHAKEN certificate	N/A	200	{ "tokens": ["…"] "passports": ["…"] }

TransNexus®

Non-IP in-band SHAKEN

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



TransNexus

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

TransNexus

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

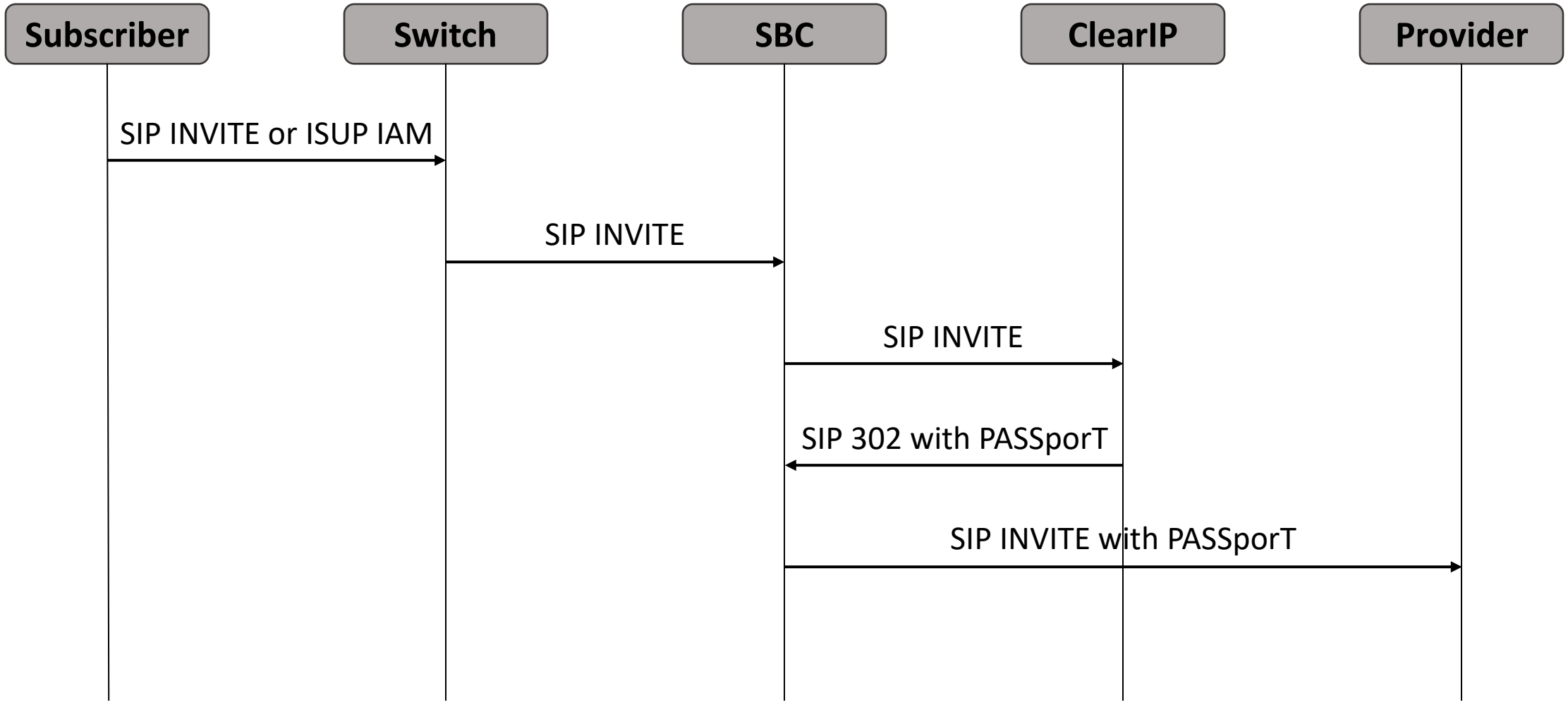
TransNexus®

Integration

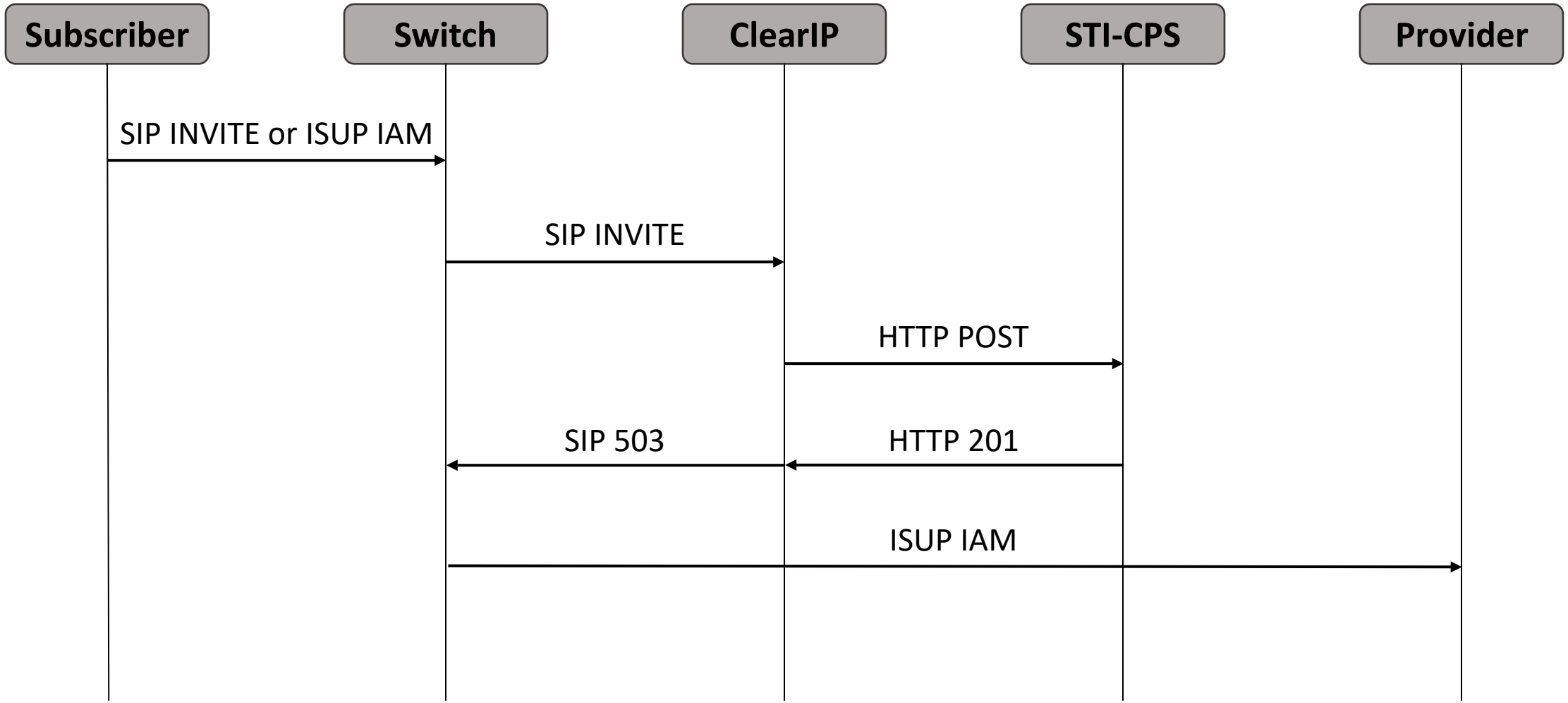
STI-AS integration

- SIP redirect
  - SIP INVITE
  - SIP 302 response with Identity header (plain or embedded) for in-band
  - SIP 503 response for OOB
- SIP proxy
  - SIP INVITE
  - SIP INVITE with Identity header
- 3GPP TS 24.229 HTTP API
  - HTTP POST with attestation level and origid
  - HTTP 200 with PASSporT

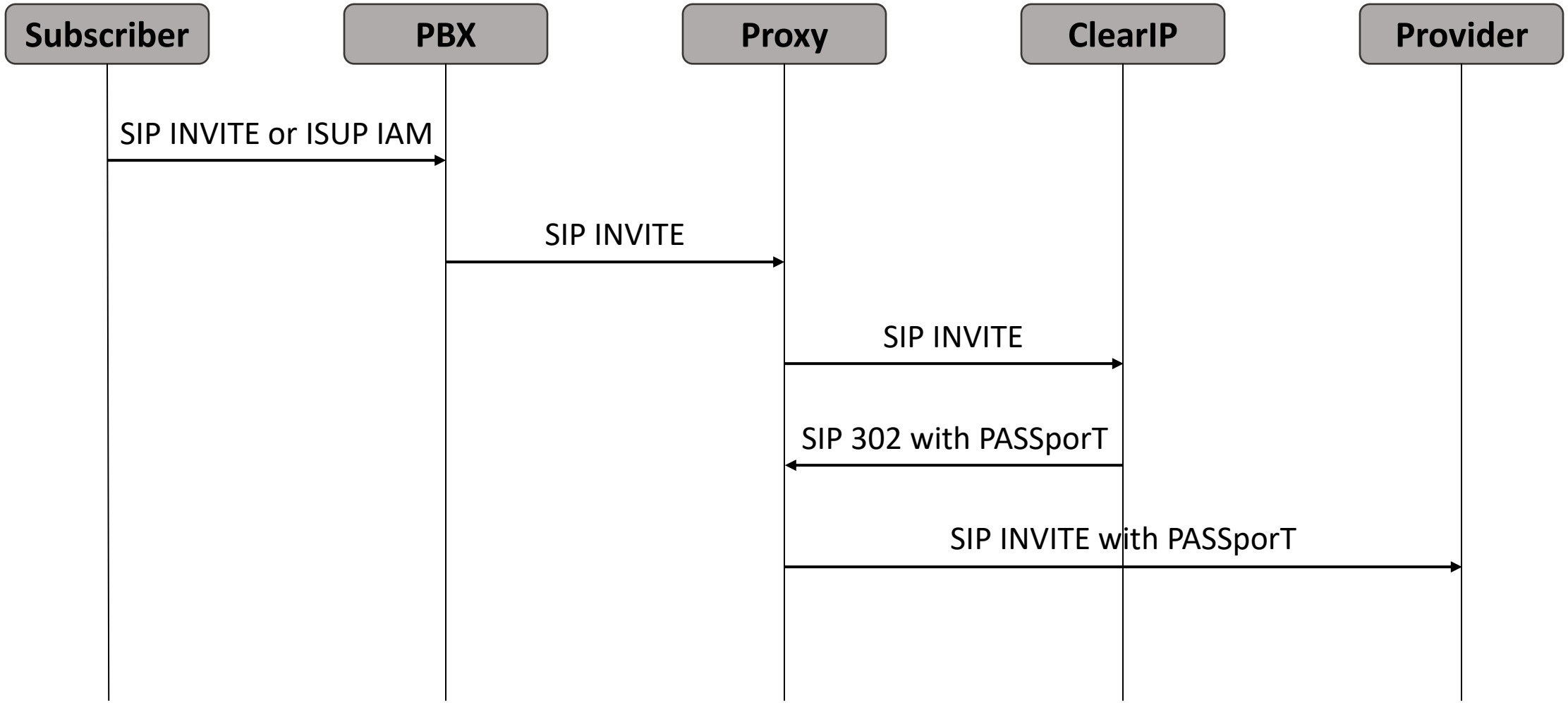
STI-AS integration with SIP 302 for in-band



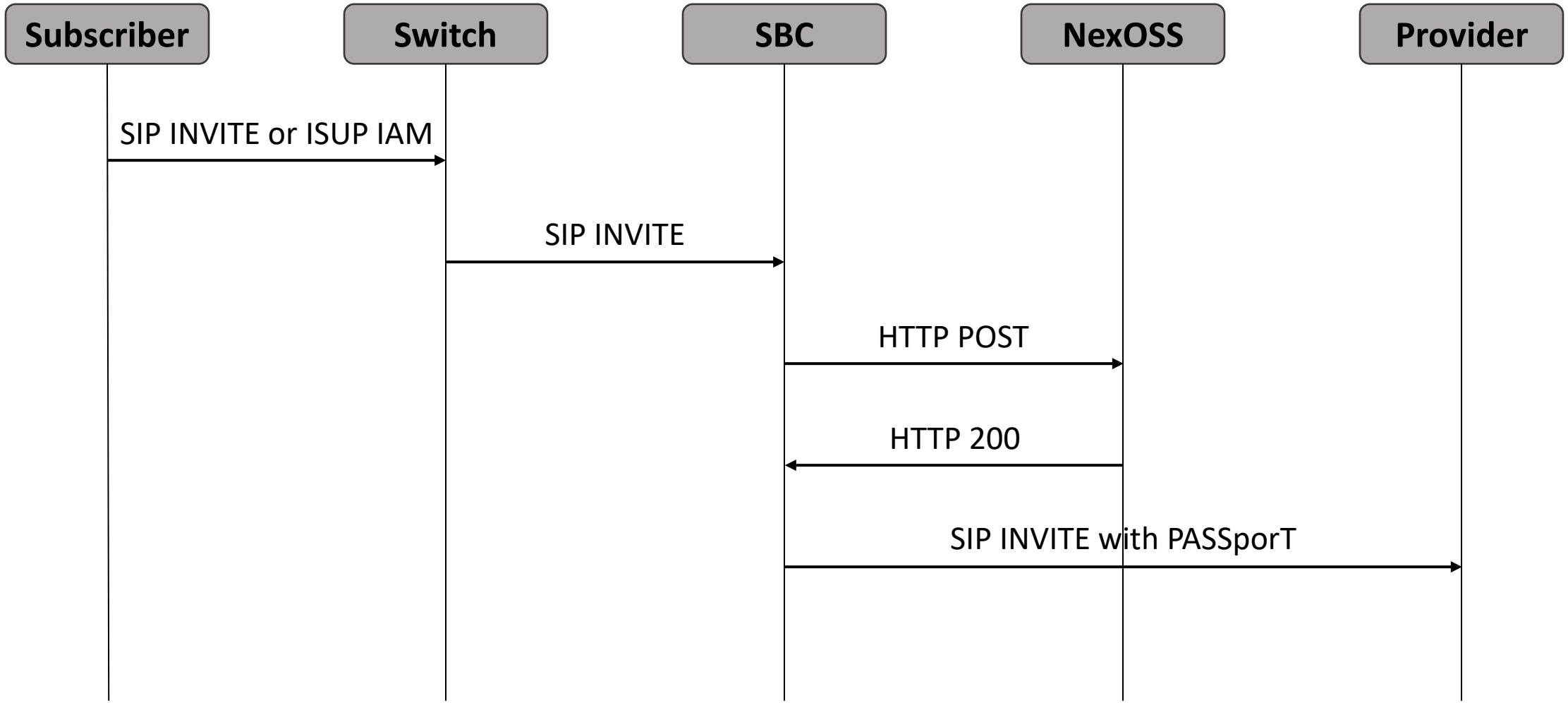
STI-AS integration with SIP 503 for OOB



STI-AS integration with SIP proxy



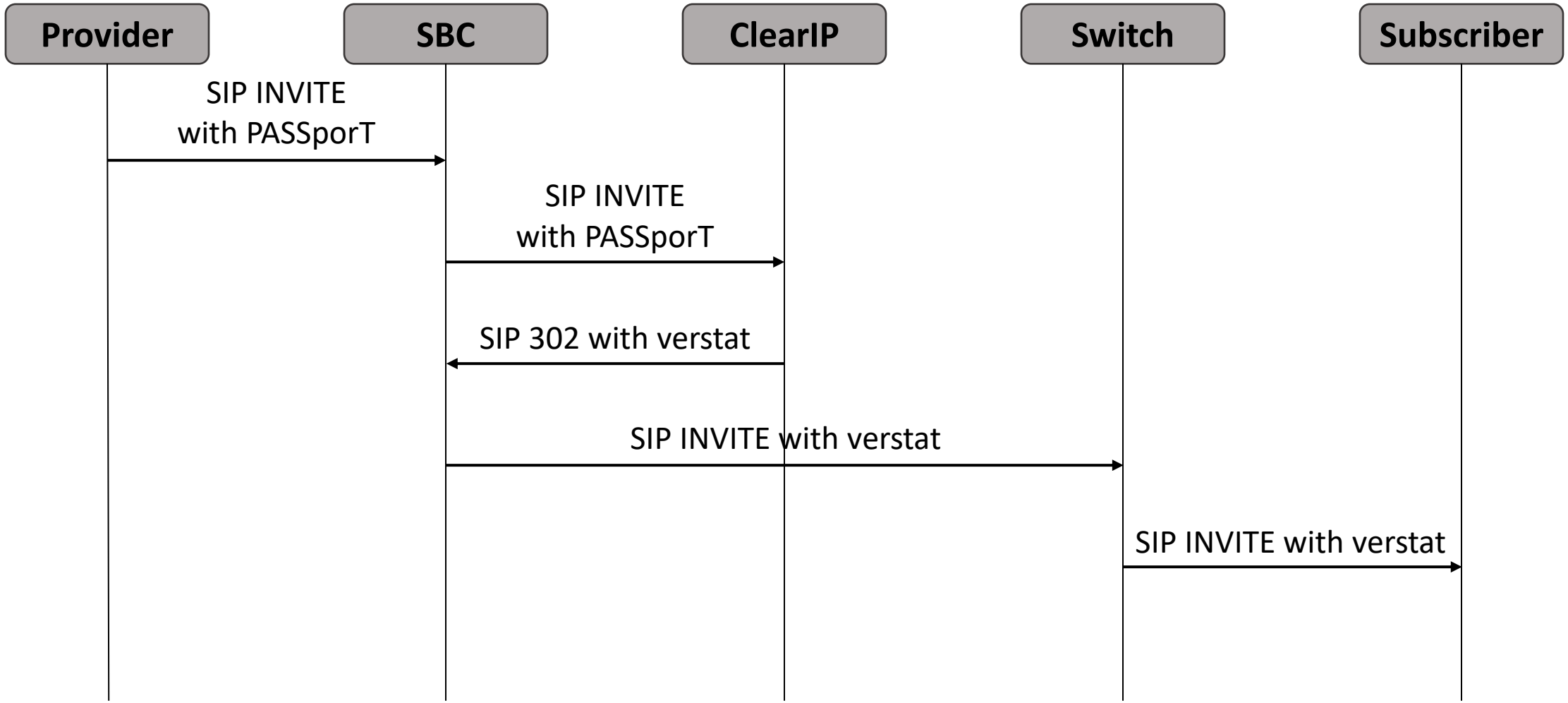
STI-AS integration with HTTP



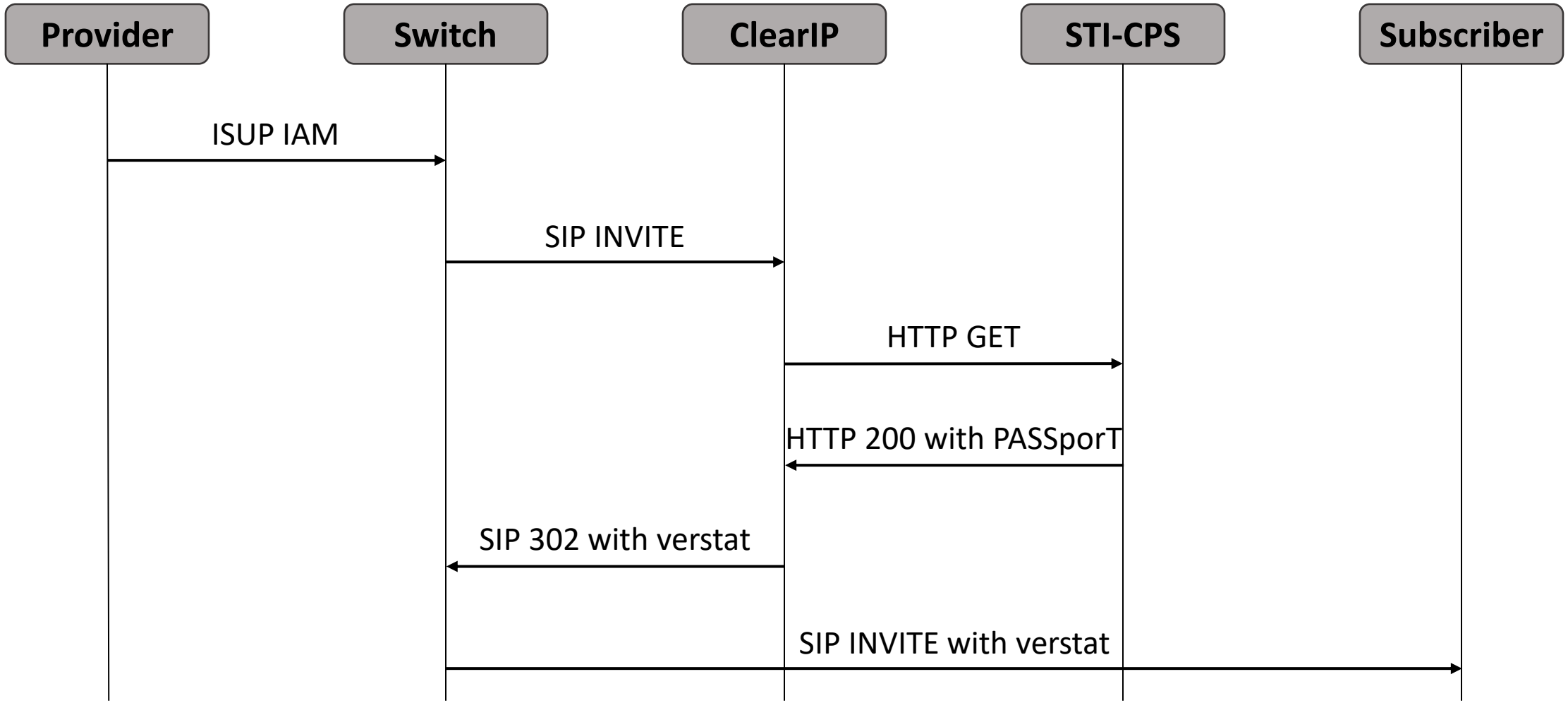
STI-VS integration

- SIP redirect
  - SIP INVITE
  - SIP 302 response with P-Asserted-Identity header including verstat (plain or embedded)
- SIP proxy
  - SIP INVITE
  - SIP INVITE with P-Asserted-Identity header including verstat
- 3GPP TS 24.229 HTTP API
  - HTTP POST with PASSporT
  - HTTP 200 with verstat

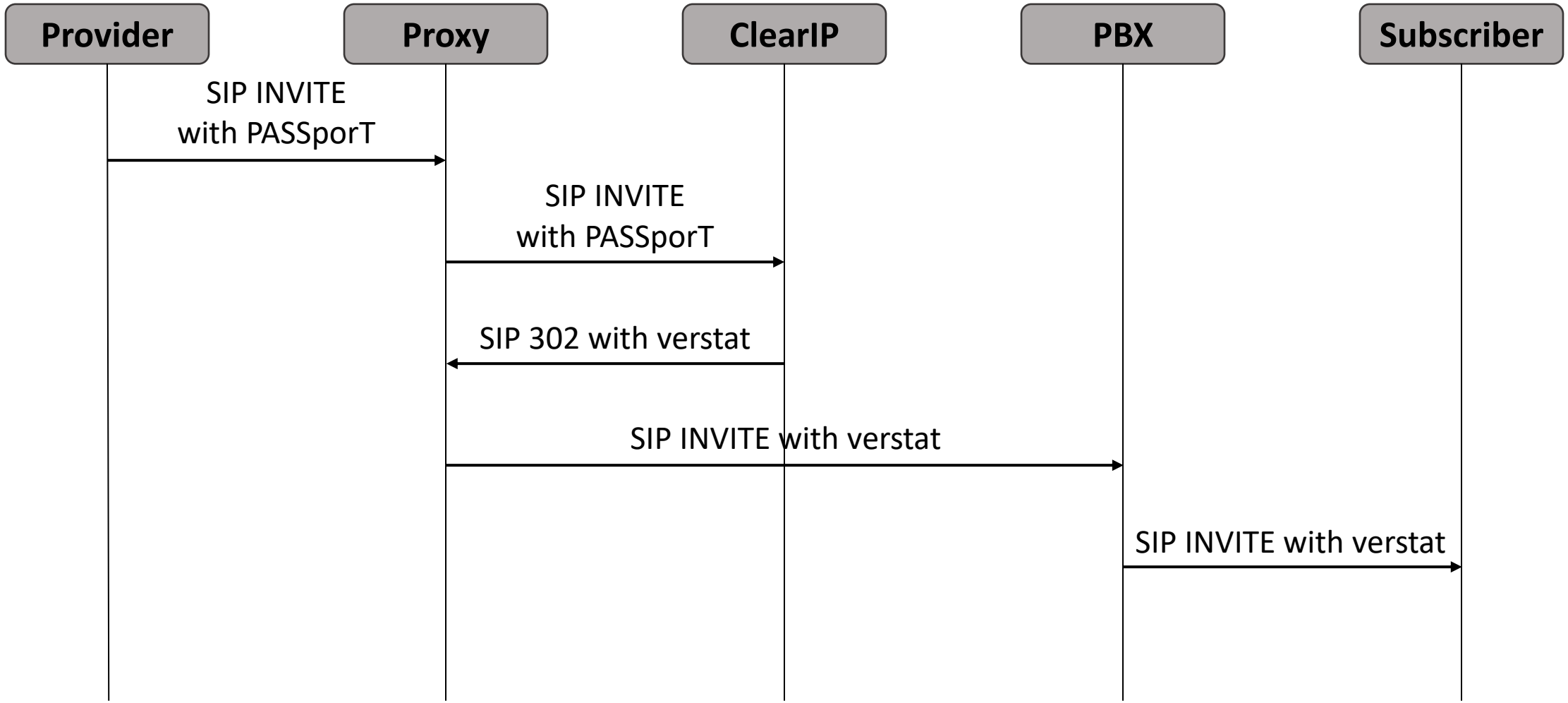
STI-VS integration with SIP 302 for in-band



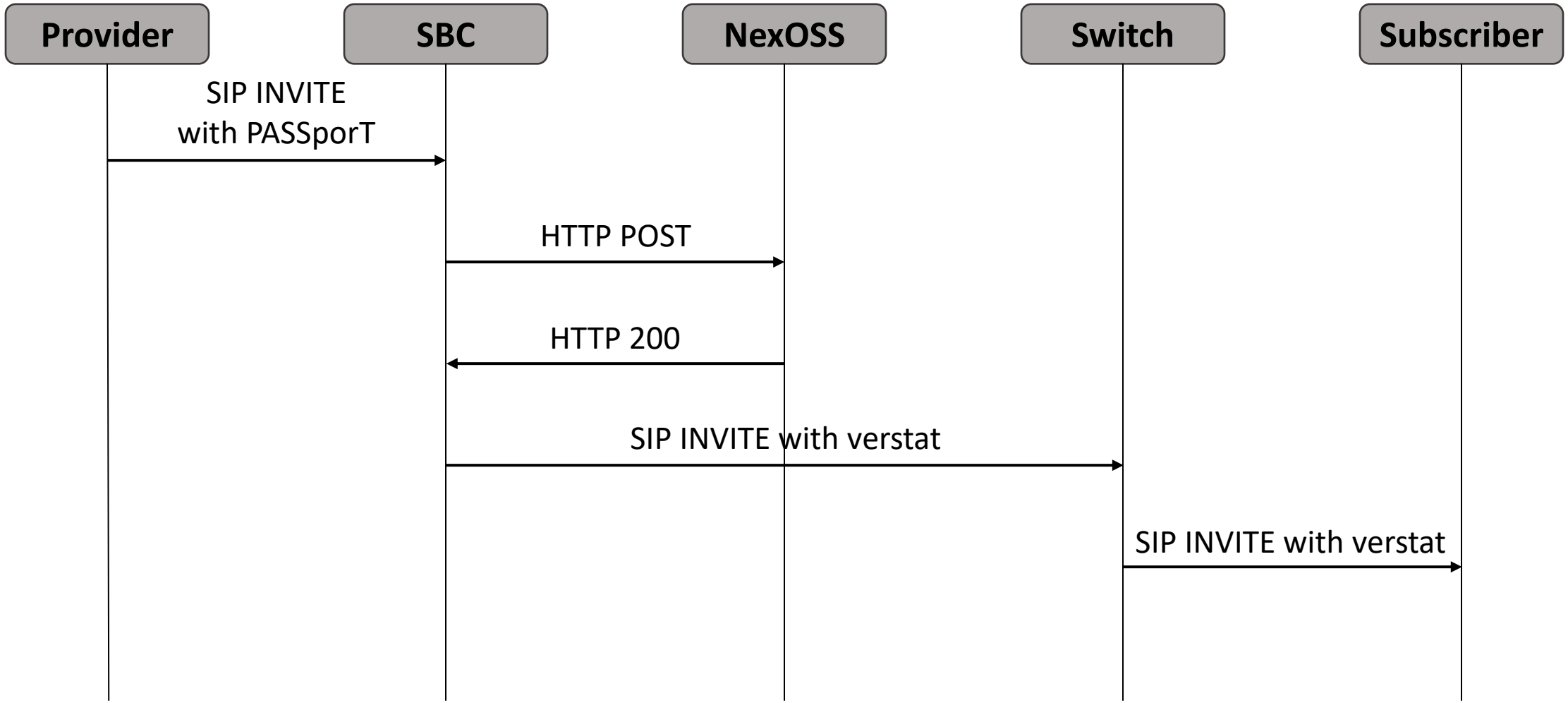
STI-VS integration with SIP 302 for OOB



STI-VS integration with SIP proxy



STI-VS integration with SIP proxy



Questions and answers

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