Out-of-Band SHAKEN Deployment – Everything You Need to Know

Alec Fenichel
Senior Software Architect
TransNexus

Agenda

- About TransNexus
- Out-of-Band SHAKEN Overview
- STI-OOBS
- STI-CPS API
- TransNexus STI-CPS Architecture
- Demonstration
- Questions and Answers

About TransNexus

- Software for the telecommunications industry since 1997
- Solutions for
  - STIR/SHAKEN
  - Robocall mitigation
  - Robocall prevention
  - TDoS prevention
  - Toll and toll-free fraud prevention
  - Jurisdictional least cost routing
  - Analytics and reporting
- STI-PA approved SHAKEN vendor
- STI-PA approved SHAKEN Certificate Authority (STI-CA)
- Active ATIS contributor
  - ATIS/SIP Forum IP-NNI Task Force
  - PTSC Non-IP Call Authentication Task Force

Out-of-Band SHAKEN Overview

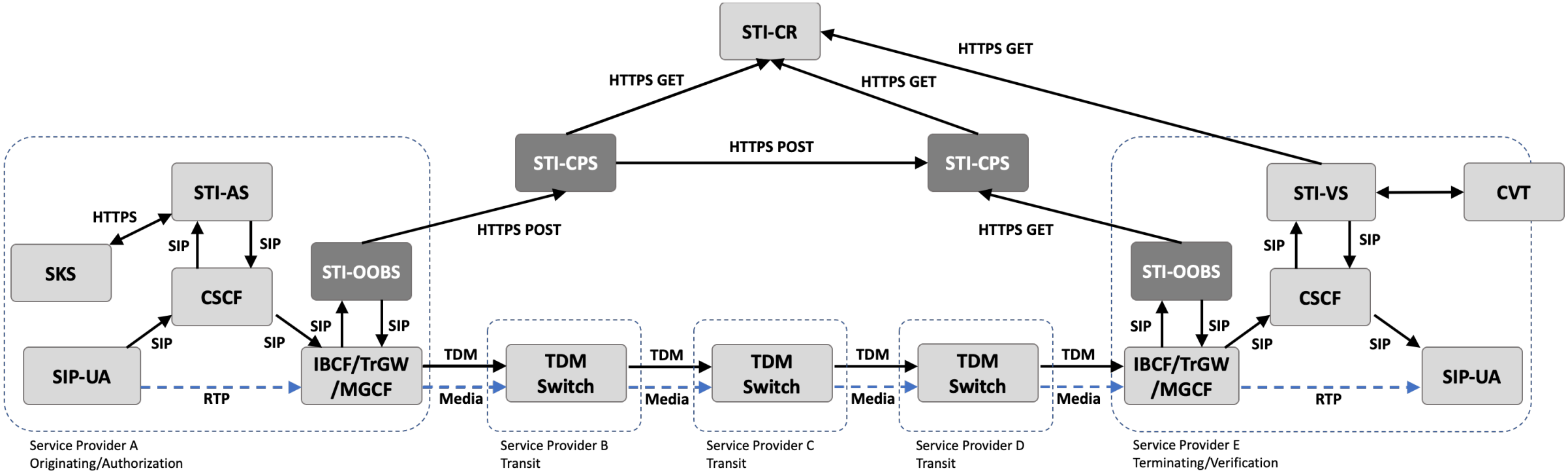
Out-of-Band SHAKEN History

- July 2013: *Secure Caller-ID Fallback Mode* proposed in IETF
- July 2017: *STIR Out of Band Architecture and Use Cases* proposed in IETF
- May 2019: TransNexus customers using Out-of-Band STIR in production
- March 2020: *Out-of-Band STIR for Service Providers* proposed in IETF
- May 2020: *SHAKEN: Out-of-Band PASSporT Transmission Involving TDM Networks* proposed in PTSC Non-IP Call Authentication Task Force
- December 2020: TransNexus customers using Out-of-Band SHAKEN in production
- July 2021: *SHAKEN: Out-of-Band PASSporT Transmission Involving TDM Networks (ATIS-1000096)* published

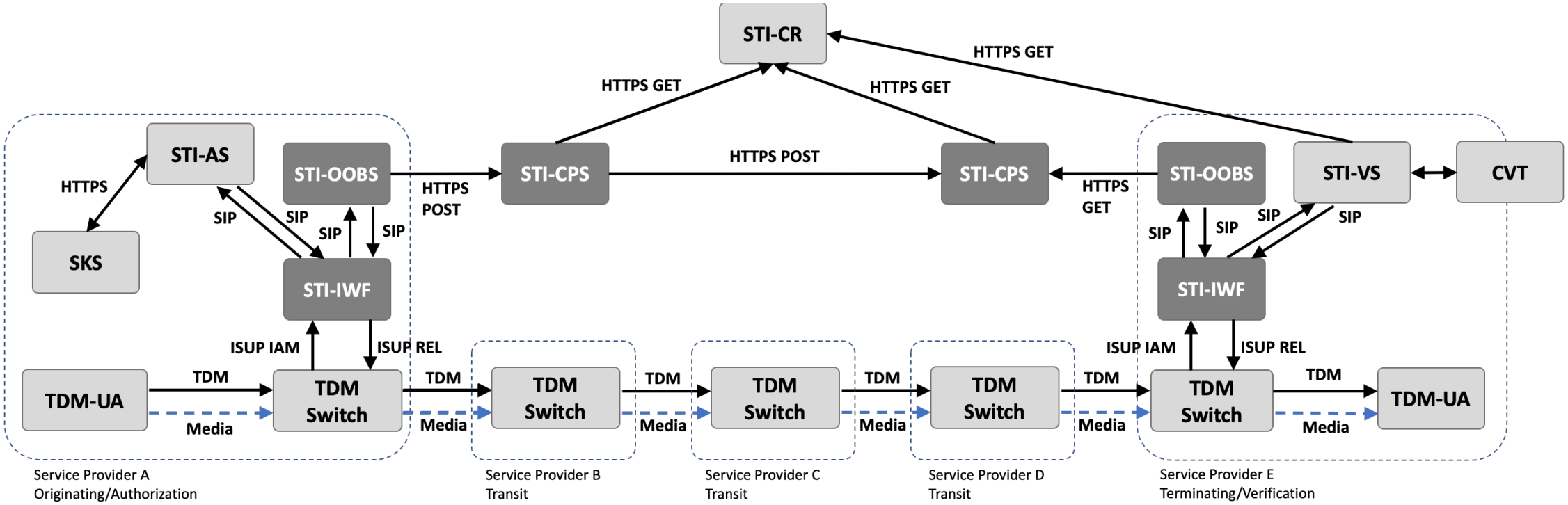
Out-of-Band SHAKEN

- SHAKEN, as defined in ATIS-1000074, only works for SIP end-to-end calls
- Out-of-Band SHAKEN enables SHAKEN for calls that use TDM interconnects
- The normal SHAKEN PASSporT is transported over the internet for the portions of the call flow that use TDM
- Leverages the existing SHAKEN trust model
- Easy to implement
- No new requirements for VoIP service providers with SIP interconnects
- Currently used in production by more than 50 service providers

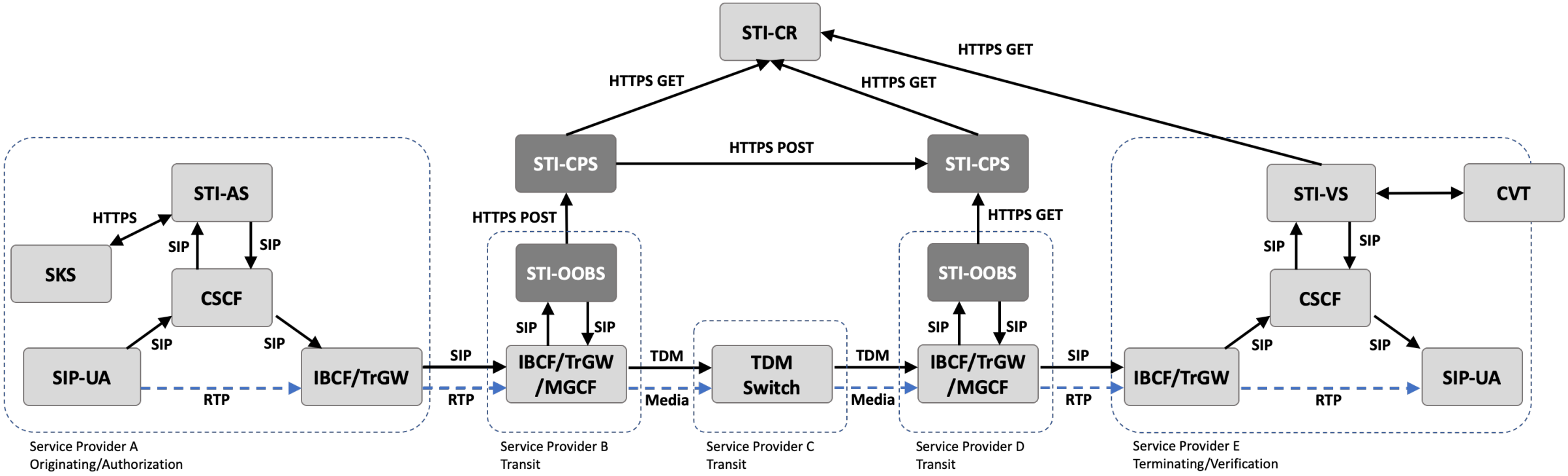
Out-of-Band SHAKEN Call Flow 1



Out-of-Band SHAKEN Call Flow 2



Out-of-Band SHAKEN Call Flow 3



STI-OOBS

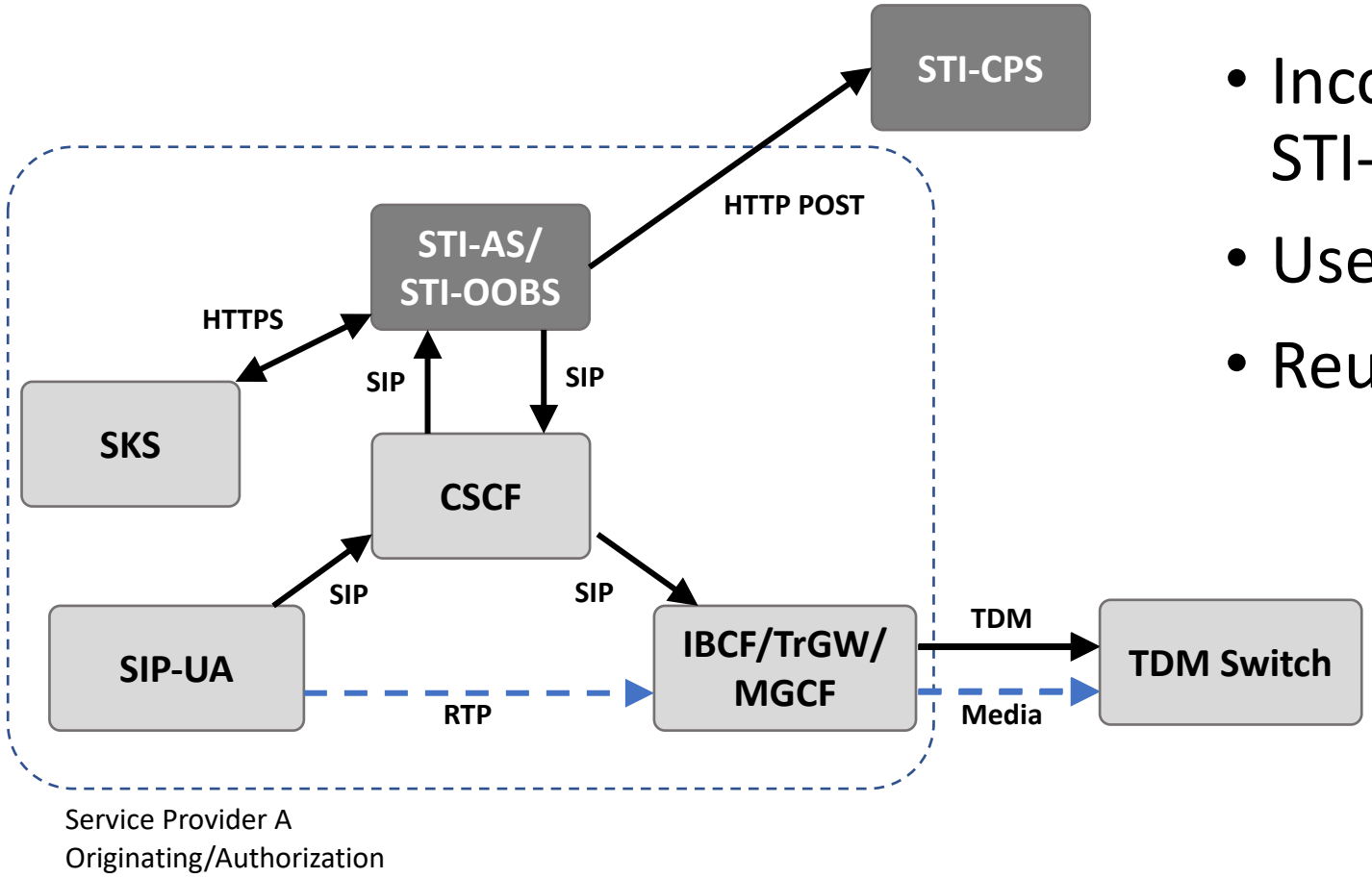
STI-OOBS Publish Logic

- Receive a request (SIP or HTTP)
- Generate an STI-CPS authentication token
  - Base PASSporT with additional claims
  - Signed by SHAKEN certificate
- Publish PASSporT(s) to the STI-CPS
  - HTTP POST
  - Authentication Bearer token
  - JSON request body
  - JSON response body

STI-OOBS Retrieve Logic

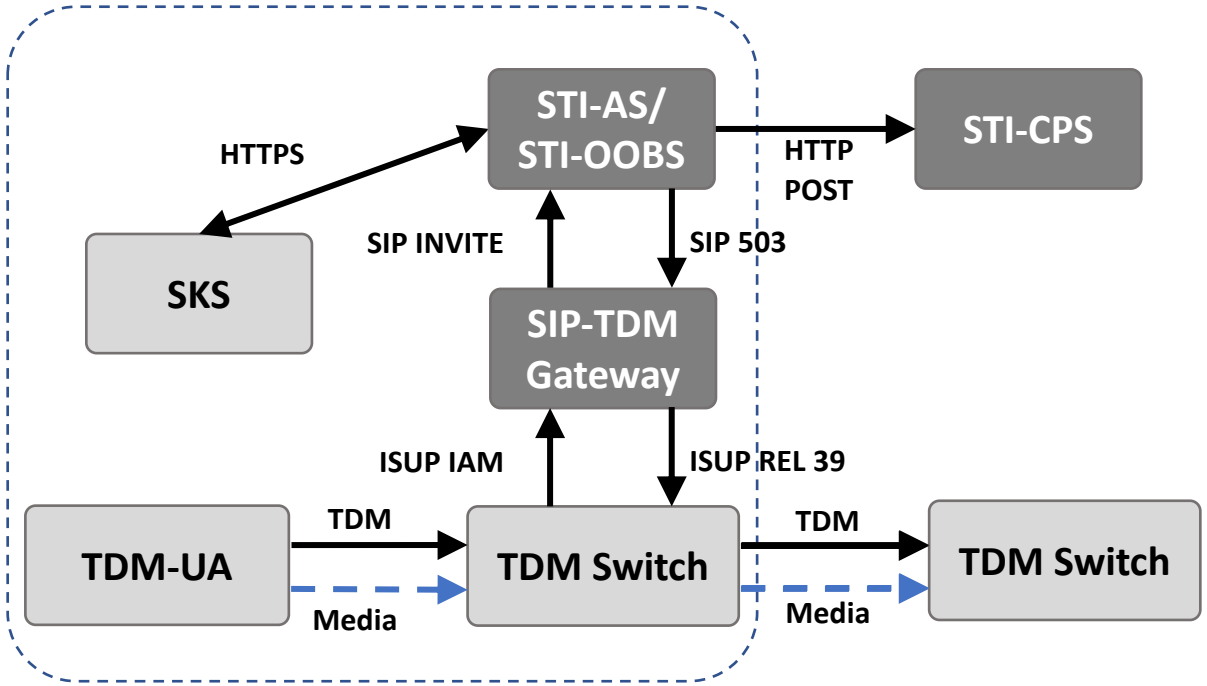
- Receive a request (SIP or HTTP)
- Generate an STI-CPS authentication token
  - Base PASSporT with additional claims
  - Signed by SHAKEN certificate
- Retrieve PASSporT(s) from the STI-CPS
  - HTTP GET
  - Authentication Bearer token
  - JSON response body
- Return PASSporT(s) (SIP or HTTP)

STI-OOBS Recommendations



- Incorporate the STI-OOBS into the STI-AS/STI-VS
- Use asynchronous publish requests
- Reuse TCP connections

STI-IWF Recommendations



- Use an off-the-shelf SIP-to-TDM gateway
- Set the SIP-to-TDM gateway trunk as the first route in the switches routing table

STI-CPS API

STI-CPS API

- RESTful API
  - JSON request body
  - JSON response body
- Three endpoints
  - Health Check
  - Publish PASSporT(s)
  - Retrieve PASSporT(s)
- JSON Web Token (JWT) authentication
  - Base PASSporT with additional claims
  - Signed by SHAKEN certificate

STI-CPS Health Check Request

```
GET /health HTTP/1.1
Host: cps.example.com
Content-Length: 0
```

STI-CPS Health Check Response

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 29

{
  "status": 200,
  "message": "OK"
}
```

STI-CPS Publish Authentication Token

Header


```
{
  "alg": "ES256",
  "x5u": "https://certificates.example.com/example.crt"
}
```


Payload


```
{
  "iat": 1608048420,
  "dest": {
    "tn": [
      "19032469103"
    ]
  },
  "orig": {
    "tn": "12013776051"
  },
  "sub": "1234",
  "iss": "1234",
  "aud": "cps.example.com",
  "action": "publish",
  "passports": "sha256-YO4Hq/xE6mkCeuPoYYck5Pt6vACmfbzNfdi6aeq95dA=",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059"
}
```

STI-CPS Publish Request

```
POST /passports/19032469103/12013776051 HTTP/1.1
Host: cps.example.com
Content-Type: application/json
Content-Length: 423
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUuY3J0In0.eyJpYXQiOjE
2MDgwNDg0MjAsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOiJzaGEyNTYtWU80SHEveEU2bWtDZXVQb1lZY2s1UHQ2dkFDbW
Ziek5mZGk2YWVxOTVkQT0iLCJzdWIiOiIxMjM0IiwiaXNzIjoiMTIzNCIsImF1ZCI6ImNwcy5leGFtcGxlLmNvbSIsImp0aSI6ImViY
2JkN2YyLWI3OGItNDAxOS1iZjgzLTMyYzI1MTdlNjA1OSIsImRlc3QiOnsidG4iOlsiMTkwMzI0NjkxMDMiXX0sIm9yaWciOnsidG4i
OiIxMjAxMzc3NjA1MSJ9fQ.1_Nty37vqW0aEHn7y5k9Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXRhtXCM6IcBm6rIsTW5BDEg
6SwbBQ

{
  "passports": [
    "eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0aWZpY2F0ZX
    MuZXhhbXBsZS5jb20vZXhhbXBsZS5jcnQifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwiaW
    F0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzFjLTkwN
    2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNKBRmHcx-YZ3DjPgBe4Mvqq9N-
    bThN1_HTWeSvbruAyet26fetRL1_bn1g"
  ]
}
```

STI-CPS Publish Response

```
HTTP/1.1 201 Created
Content-Type: application/json
Content-Length: 34

{
  "status": 201,
  "message": "Created"
}
```

STI-CPS Retrieve Authentication Token

Header


```
{
  "alg": "ES256",
  "x5u": "https://certificates.example.com/example.crt"
}
```


Payload


```
{
  "iat": 1608048420,
  "dest": {
    "tn": [
      "19032469103"
    ]
  },
  "orig": {
    "tn": "12013776051"
  },
  "sub": "1234",
  "iss": "1234",
  "aud": "cps.example.com",
  "action": "retrieve",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059"
}
```

STI-CPS Retrieve Request

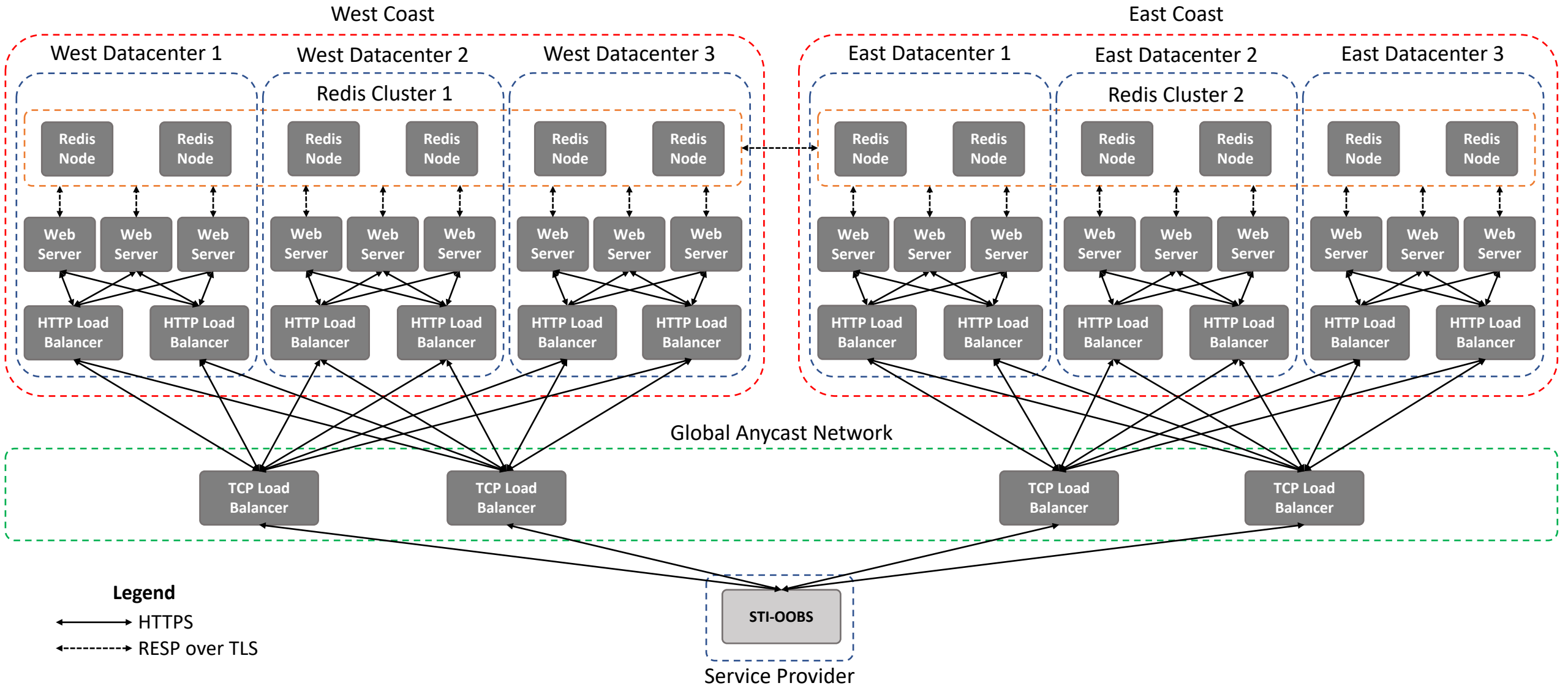
```
GET /passports/19032469103/12013776051 HTTP/1.1
Host: cps.example.com
Content-Length: 0
Authorization: Bearer
eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUuY3J0In0.eyJpY
XQiOjE2MDgwNDg0NDQsImFjdGlvbiI6InJldHJpZXZlIiwic3ViIjoiMTIzNCIsImlzcyI6IjEyMzQiLCJhdWQiOiJjcHMuZX
hhbXBsZS5jb20iLCJqdGkiOiJiODBlMTAyMy04ZGM0LTQ2NWQtYTFhYS1mMDhlODhmODkyNjUiLCJkZXN0Ijp7InRuIjpbIjE
5MDMyNDY5MTAzIl19LCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifX0.k3S9oNyj9B8olbgaObL-
eqdnCAB_sZaBOSuzfo8R7PDyqEBUOVvm-pFzG24giW8ztlg6339TerVQRGUQNhx9HQ
```

STI-CPS Retrieve Response

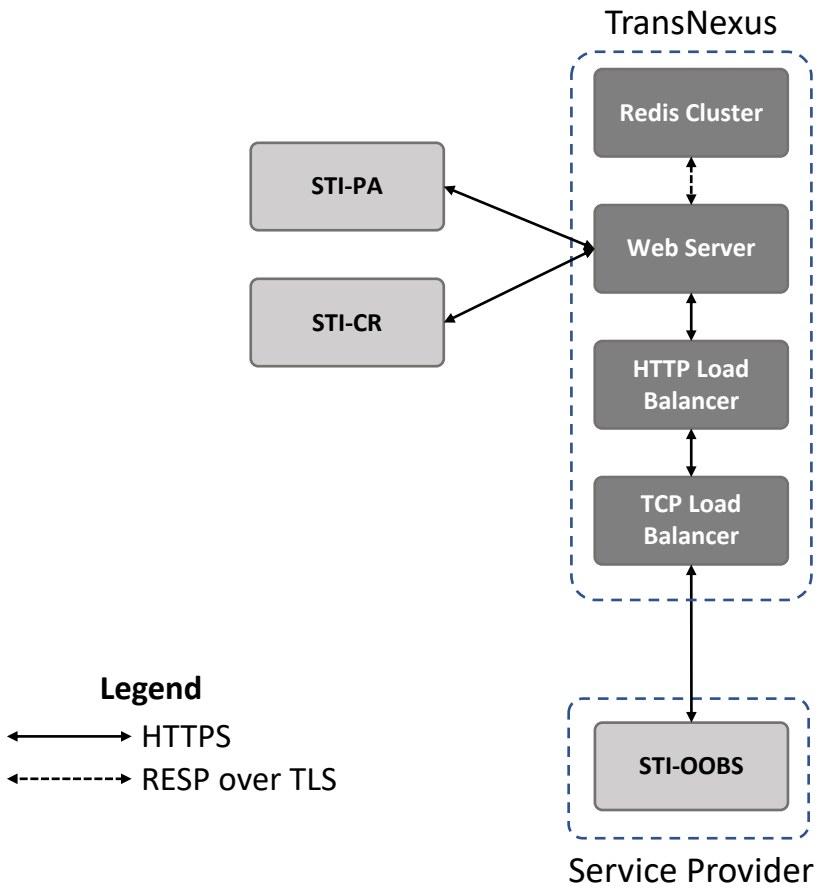
```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 958

{
  "passports": [
    "eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0aWZpY2F0ZX
    MuZXhhbXBsZS5jb20vZXhhbXBsZS5jcnQifQ.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwiaW
    F0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzFjLTkwN
    2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNKBRmHcx-YZ3DjPgBe4Mvqq9N-
    bThN1_HTWeSvbruAyet26fetRL1_bn1g"
  ],
  "tokens": [
    "eyJhbGciOiJFUzI1NiIsIng1dSI6Imh0dHBzOi8vY2VydGlmaWNhdGVzLmV4YW1wbGUuY29tL2V4YW1wbGUuY3J0In0.eyJpYX
    QiOjE2MDgwNDg0MjAsImFjdGlvbiI6InB1Ymxpc2giLCJwYXNzcG9ydHMiOiJzaGEyNTYtWU80SHEveEU2bWtDZXVQb1lZY2s1U
    HQ2dkFDbWZiek5mZGk2YWVxOTVkQT0iLCJzdWIiOiIxMjM0IiwiaXNzIjoiMTIzNCIsImF1ZCI6ImNwcy5leGFtcGxlLmNvbSIs
    Imp0aSI6ImViY2JkN2YyLWI3OGItNDAxOS1iZjgzLTMyYzI1MTdlNjA1OSIsImRlc3QiOnsidG4iOlsiMTkwMzI0NjkxMDMiXX0
    sIm9yaWciOnsidG4iOiIxMjAxMzc3NjA1MSJ9fQ.1_Nty37vqW0aEHn7y5k9Da9vXO_FvWSMGY6xOh6U_7RbGOSm0H9BK_xTqXR
    htXCM6IcBm6rIsTW5BDEg6SwbBQ"
  ]
}
```

TransNexus STI-CPS Architecture

TransNexus STI-CPS Architecture



TransNexus STI-CPS Web Server Processing



- Publish request
  - Receive HTTP POST request
  - Verify authentication token
  - Put PASSporT(s) into the Redis cluster
    - Key: Calling/called number pair
    - Value: PASSporT(s) and authentication token in a JSON object
  - Return HTTP 201
- Retrieve request
  - Receive HTTP GET request
  - Verify authentication token
  - Get PASSporT(s) from the Redis cluster
    - Key: Calling/called number pair
  - Return HTTP 200 with JSON object
- Two-tier STI-CR cache
  - Web server – per process
  - Redis – shared
  - Least Recently Used (LRU)

Demonstration

Open Source Source Code

- https://github.com/TransNexus/sti-oobs-sample (130 lines of code)
- Generates a PASSporT (line 21 - 42)
- Generates an STI-CPS publish authentication token (line 44 - 68)
- Publishes the PASSporT to an STI-CPS using an HTTP POST (line 70 - 86)
- Generates an STI-CPS retrieve authentication token (line 88 - 111)
- Retrieves the PASSporT from an STI-CPS using an HTTP GET (line 113 - 123)

Questions and Answers

Learn More

- ATIS-1000096
- ATIS-1000097
- TransNexus STI-CPS
- STI-OOBS Sample
- Out-of-Band SHAKEN Whitepaper
- SHAKEN Information Hub

Contact Us

- TransNexus
  - https://transnexus.com
  - info@transnexus.com
  - + 1 (404) 526-6060
- Alec Fenichel
  - alec.fenichel@transnexus.com
  - +1 (407) 760-0036