

The Non-IP Call Authentication Standards (Out-of-Band SHAKEN)

Alec Fenichel
Chief Technology Officer
TransNexus

Agenda

- Non-IP Call Authentication Task Force
- Comparison of Out-of-Band SHAKEN standards
 - Call Flows
 - STI-CPS API
- Questions and Answers

Non-IP Call Authentication Task Force

- Standards

- *ATIS-1000095 – Extending STIR/SHAKEN over TDM*
- *ATIS-1000096 – Out-of-Band PASSporT Transmission Involving TDM Networks*
- *ATIS-1000105 – Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM*
- *ATIS-10001XX – STI-CPS Discovery for Out-of-Band PASSporT Transmission Involving TDM Networks*

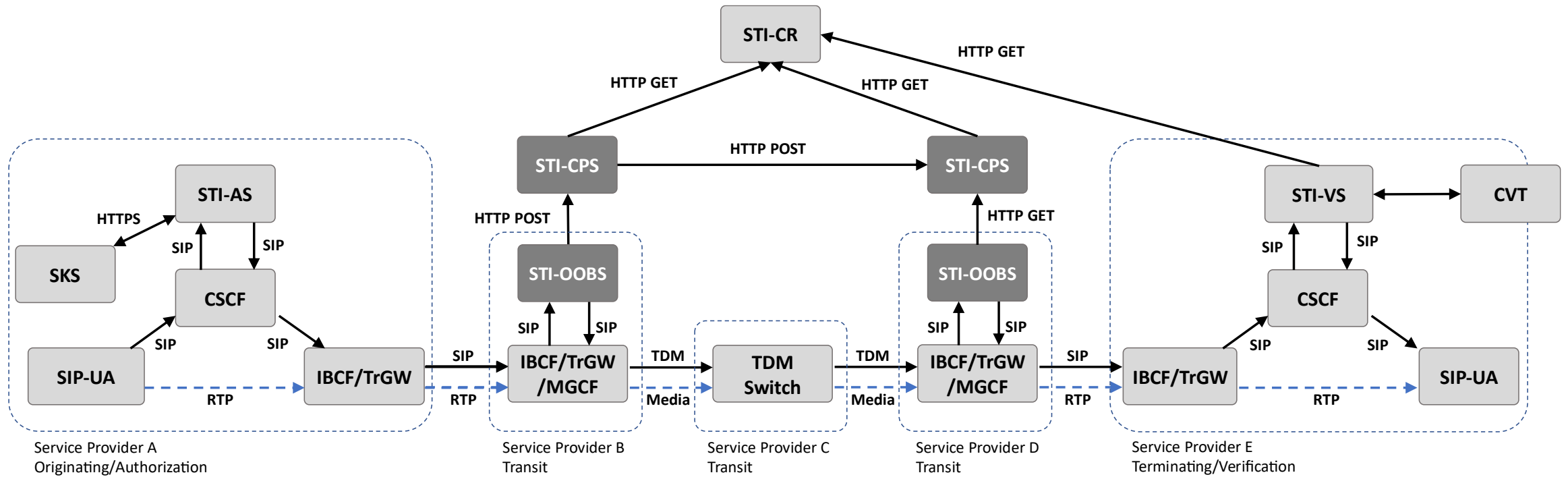
- *Technical Reports*

- *ATIS-1000097 – Alternatives for Call Authentication for Non-IP Traffic*
- *ATIS-1000106 – Viability of Non-IP Call Authentication Standards*

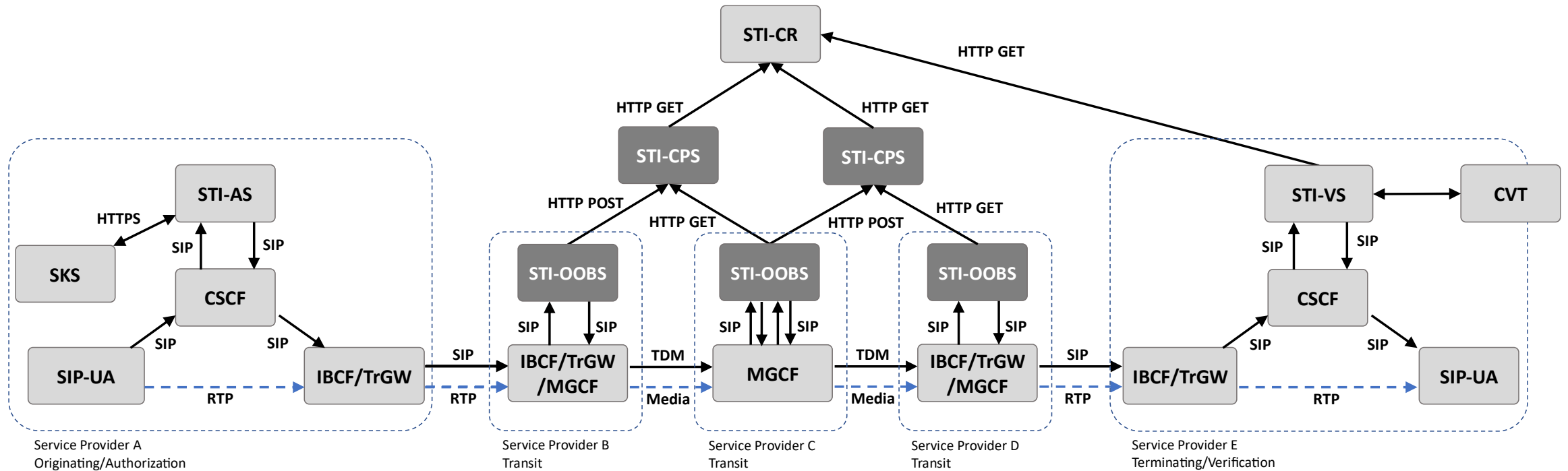
Out-of-Band SHAKEN

- SHAKEN, as defined in ATIS-1000074, only works for SIP end-to-end calls
- Out-of-Band SHAKEN enables SHAKEN for calls that use non-IP interconnects
- The SHAKEN PASSporT is transported over the internet for the portions of the call flow that use non-IP
- Leverages the existing SHAKEN trust model
- Multiple standards
 - ATIS-1000096 – Broadcast
 - *ATIS-1000105* – Hop-by-Hop
 - *ATIS-10001XX* – Discovery

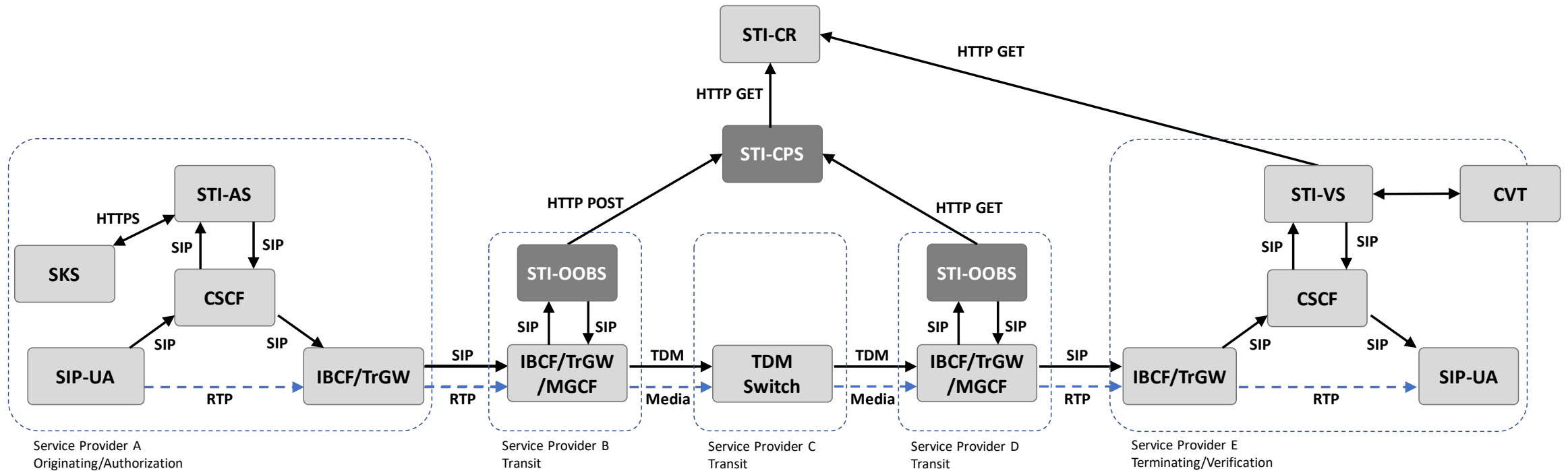
Call Flow 1 – Broadcast



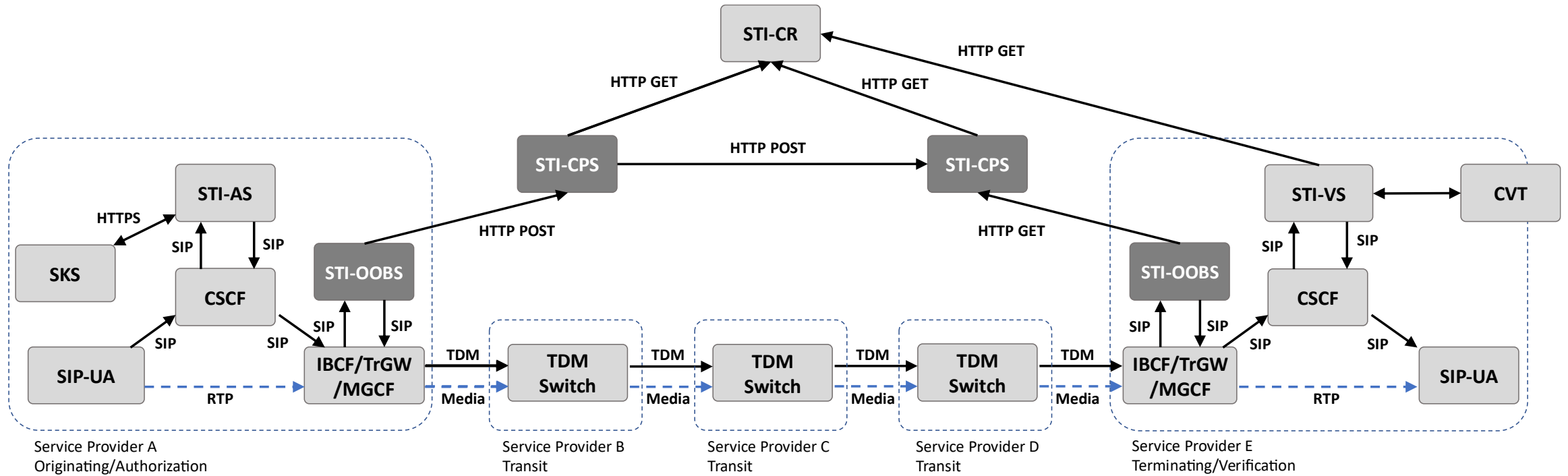
Call Flow 1 – Hop-by-Hop



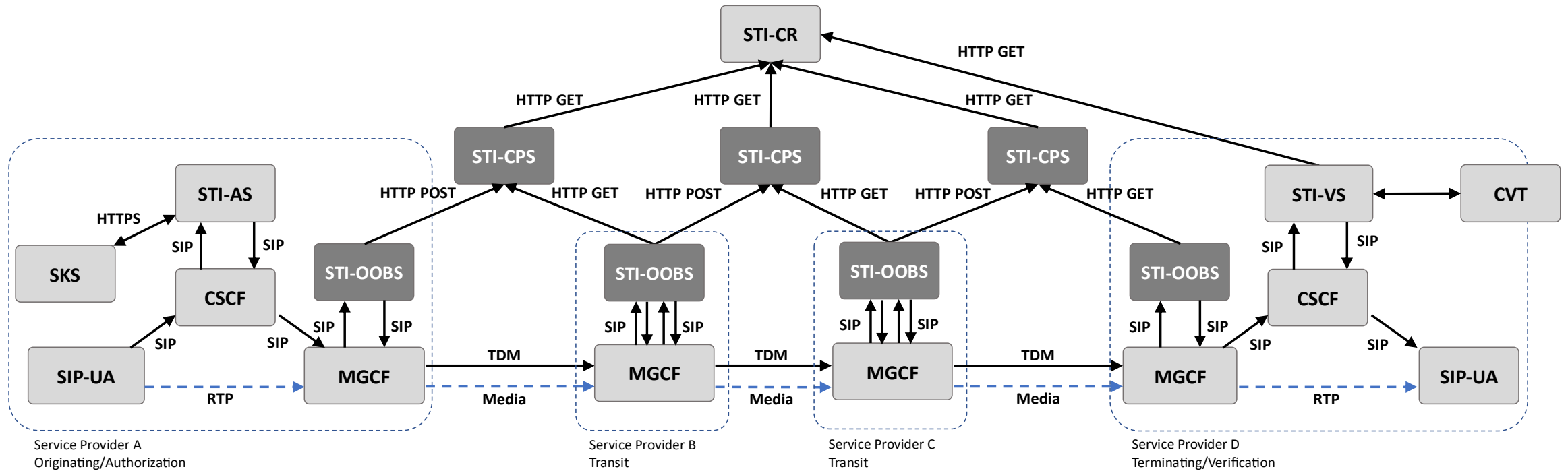
Call Flow 1 – Discovery



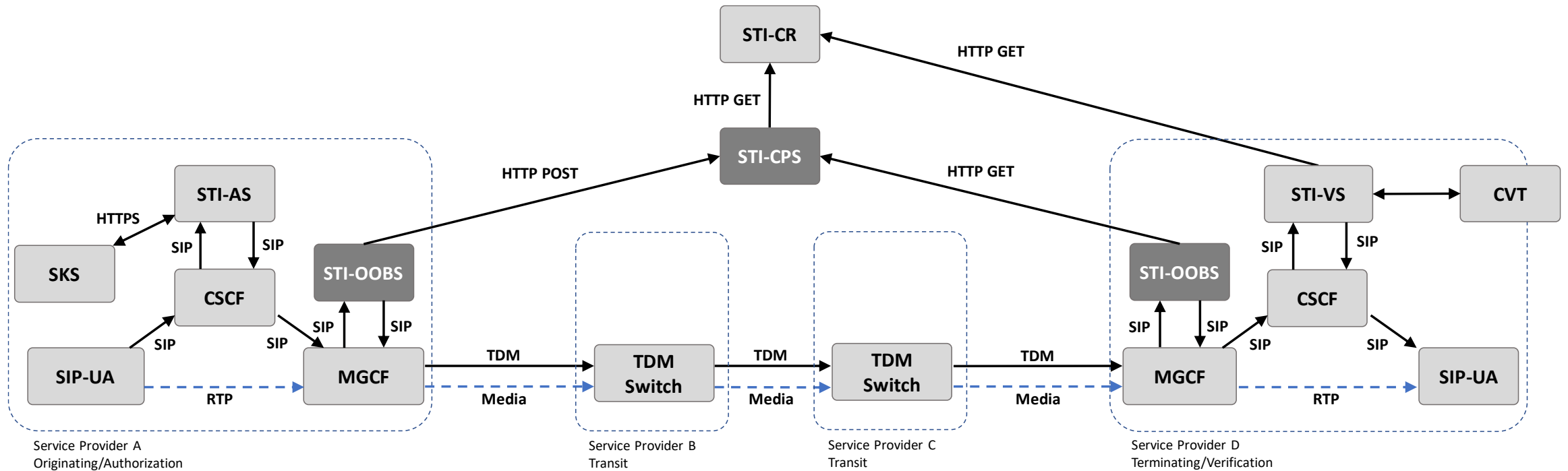
Call Flow 2 – Broadcast



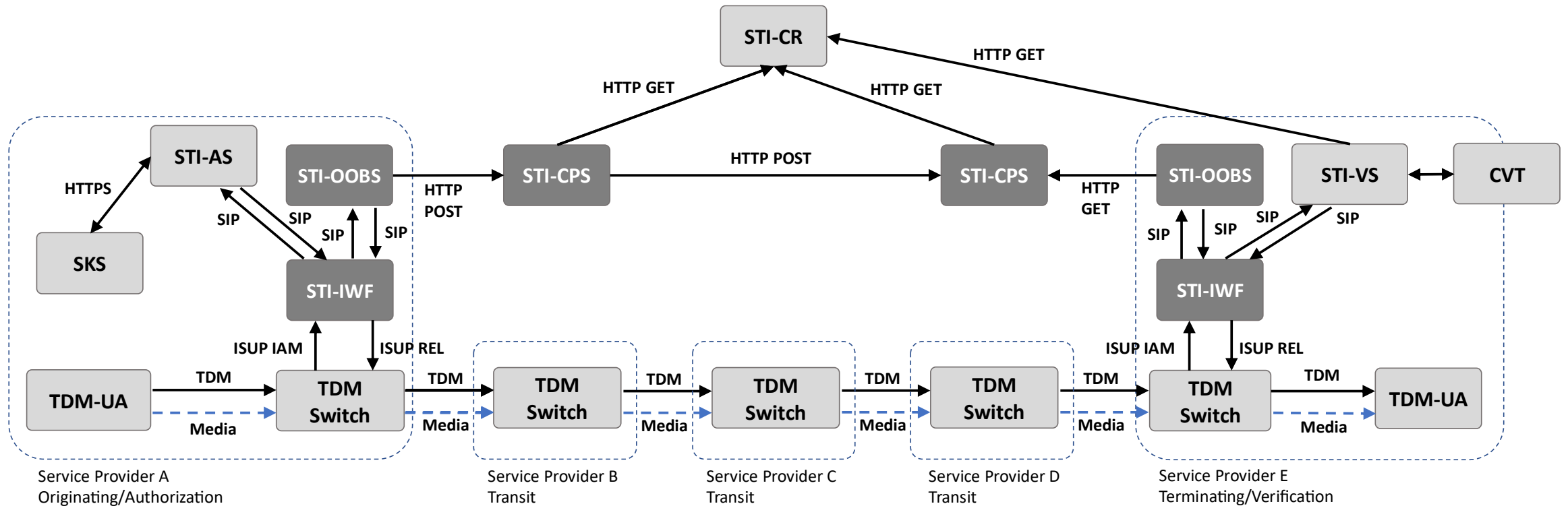
Call Flow 2 – Hop-by-Hop



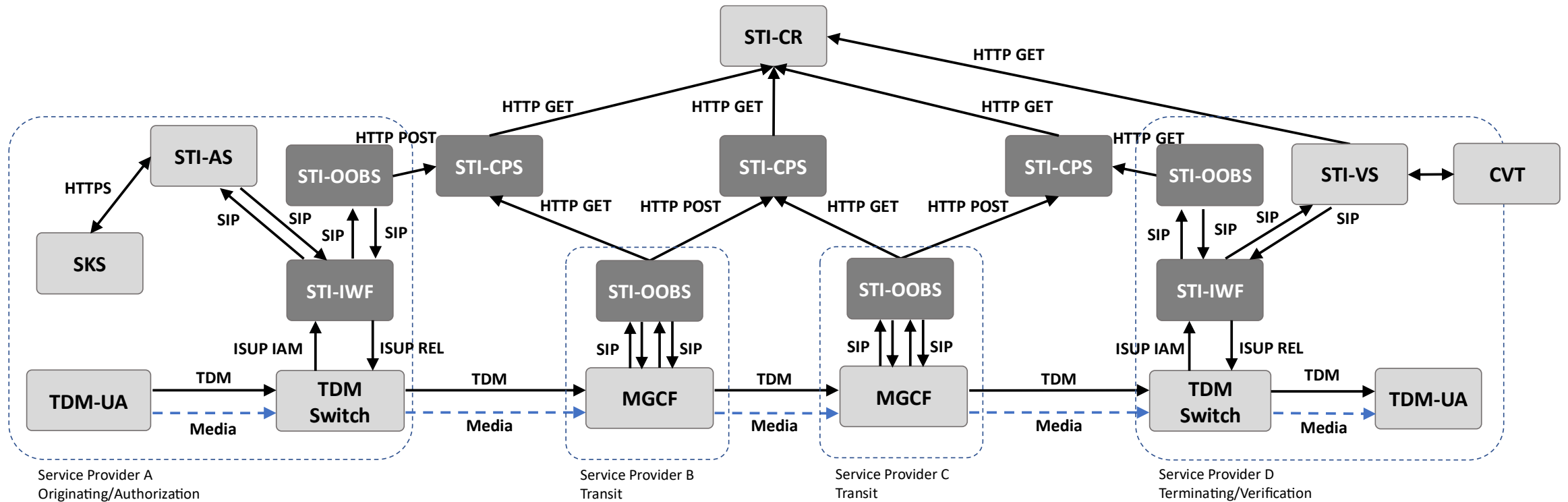
Call Flow 2 – Discovery



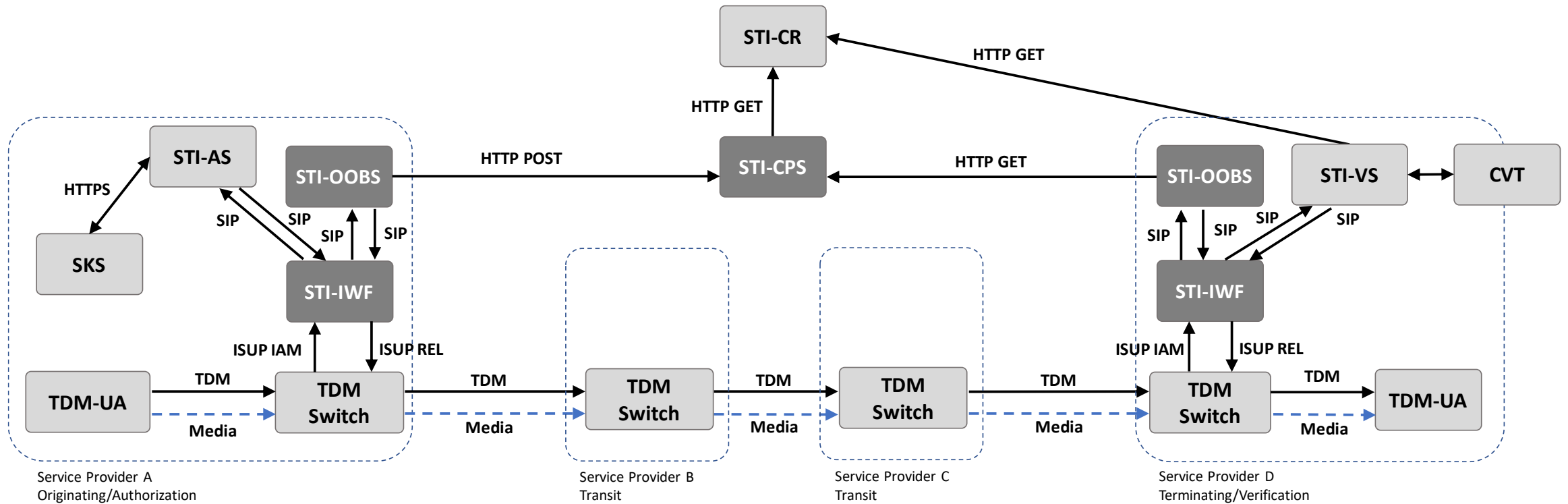
Call Flow 3 – Broadcast



Call Flow 3 – Hop-by-Hop



Call Flow 3 – Discovery



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
 - Signed with SHAKEN certificate

Health Check Request

GET /health HTTP/1.1

Host: cps.example.com

Content-Length: 0

Health Check Response

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 29

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


Publish Authentication – Broadcast

```
{  
  "iat": 1608048420,  
  "action": "publish",  
  "passports": "sha256-YO4Hq/xE6mkCeUPoYYck5Pt6vACmfbzNfdi6aeq95dA=",  
  "sub": "1234",  
  "iss": "1234",  
  "aud": "cps.example.com",  
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",  
  "dest": {  
    "tn": [  
      "19032469103"  
    ]  
  },  
  "orig": {  
    "tn": "12013776051"  
  }  
}
```

Publish Authentication – Hop-by-Hop

```
{
  "iat": 1608048420,
  "exp": 1608048425,
  "action": "publish",
  "passports": "sha256-YO4Hq/xE6mkCeUPoYYck5Pt6vACmfbzNfdi6aeq95dA=",
  "spc": "1234",
  "iss": "1234",
  "aud": "cps.example.com",
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",
  "dest": {
    "tn": [
      "19032469103"
    ]
  },
  "orig": {
    "tn": "12013776051"
  }
}
```

Publish Authentication – Discovery

```
{  
  "iat": 1608048420,  
  "exp": 1608048425,  
  "action": "publish",  
  "passports": "sha256-YO4Hq/xE6mkCeUPoYYck5Pt6vACmfbzNfdi6aeq95dA=",  
  "iss": "1234",  
  "aud": "cps.example.com",  
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",  
  "dest": {  
    "tn": [  
      "19032469103"  
    ]  
  },  
  "orig": {  
    "tn": "12013776051"  
  }  
}
```

Publish Request – Broadcast

POST /passports/19032469103/12013776051 HTTP/1.1

Content-Type: application/json

Content-Length: 31

Host: cps.example.com

Authorization: Bearer [TOKEN_HERE](#)

```
{"passports":["PASSPORT\_HERE
```

Publish Request – Hop-by-Hop

POST /passports/**1234**/19032469103/12013776051 HTTP/1.1

Content-Type: application/json

Content-Length: 31

Host: cps.example.com

Authorization: Bearer **TOKEN_HERE**

{"passports":["**PASSPORT_HERE**"]}

Publish Request – Discovery

POST /passports/19032469103/12013776051 HTTP/1.1

Content-Type: application/json

Content-Length: 31

Host: cps.example.com

Authorization: Bearer **TOKEN_HERE**

{"passports":["PASSPORT_HERE"]}

Publish Response

HTTP/1.1 201 Created

Content-Type: application/json

Content-Length: 34

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

Retrieve Authentication – Broadcast

```
{  
  "iat": 1608048420,  
  "action": "retrieve",  
  "sub": "4321",  
  "iss": "4321",  
  "aud": "cps.example.com",  
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",  
  "dest": {  
    "tn": [  
      "19032469103"  
    ]  
  },  
  "orig": {  
    "tn": "12013776051"  
  }  
}
```


Retrieve Authentication – Hop-by-Hop

```
{  
  "iat": 1608048420,  
  "action": "retrieve",  
  "spc": "1234",  
  "iss": "4321",  
  "aud": "cps.example.com",  
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",  
  "dest": {  
    "tn": [  
      "19032469103"  
    ]  
  },  
  "orig": {  
    "tn": "12013776051"  
  }  
}
```

Retrieve Authentication – Discovery

```
{  
  "iat": 1608048420,  
  "action": "retrieve",  
  "iss": "4321",  
  "aud": "cps.example.com",  
  "jti": "ebcbd7f2-b78b-4019-bf83-32c2517e6059",  
  "dest": {  
    "tn": [  
      "19032469103"  
    ]  
  },  
  "orig": {  
    "tn": "12013776051"  
  }  
}
```

Retrieve Request – Broadcast

GET /passports/19032469103/12013776051 HTTP/1.1

Content-Length: 0

Host: cps.example.com

Authorization: Bearer [TOKEN_HERE](#)

Retrieve Request – Hop-by-Hop

GET /passports/1234/19032469103/12013776051 HTTP/1.1

Content-Length: 0

Host: cps.example.com

Authorization: Bearer [TOKEN_HERE](#)

Retrieve Request – Discovery

GET /passports/19032469103/12013776051 HTTP/1.1

Content-Length: 0

Host: cps.example.com

Authorization: Bearer [TOKEN_HERE](#)

Retrieve Response – Broadcast

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 55

```
{"tokens":["TOKEN_HERE"],"passports":["PASSPORT_HERE"]}
```

Retrieve Response – Hop-by-Hop

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 52

```
{"token":"TOKEN_HERE","passports":["PASSPORT_HERE"]}
```

Retrieve Response – Discovery

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 52

```
{"token":"TOKEN_HERE","passports":["PASSPORT_HERE"]}
```


Questions and Answers

- Contact us
 - <https://transnexus.com>
 - info@transnexus.com
 - +1 (404) 526-6060