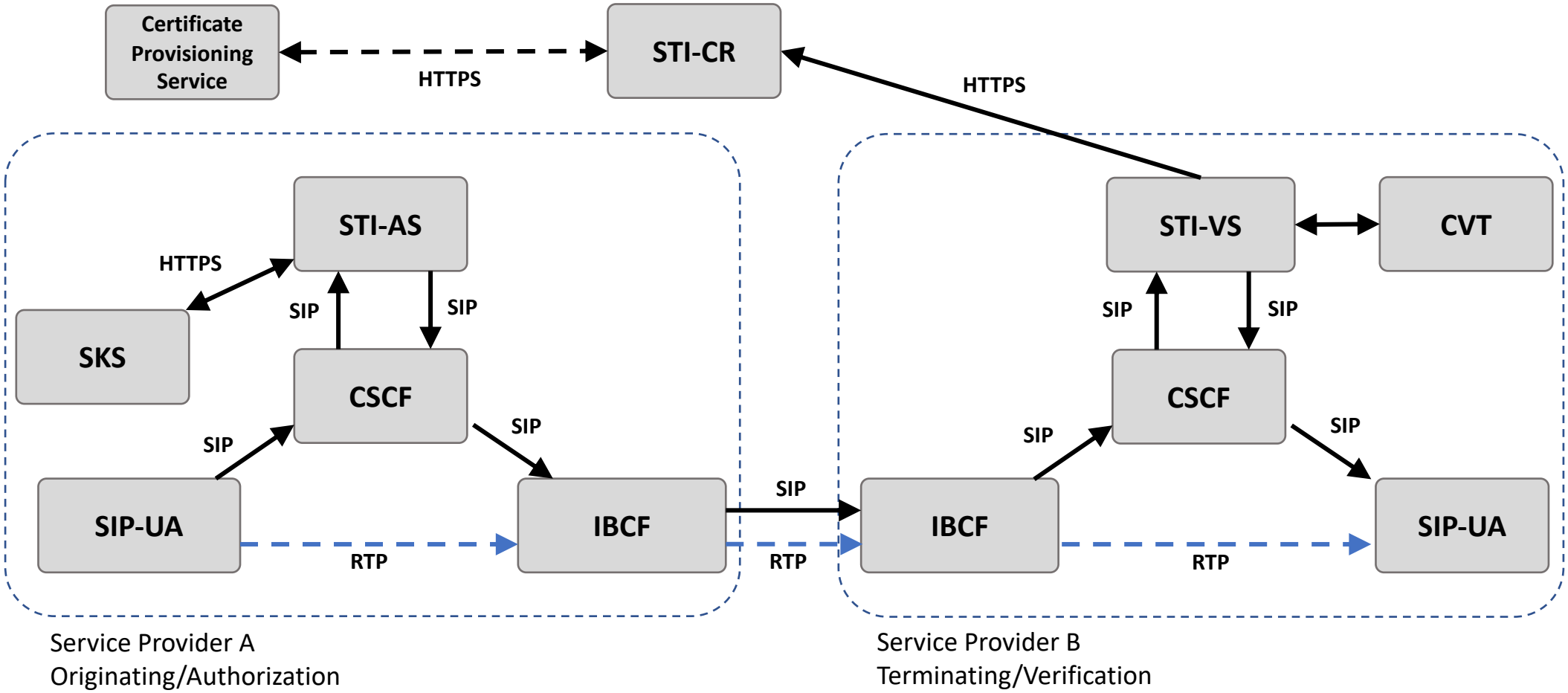
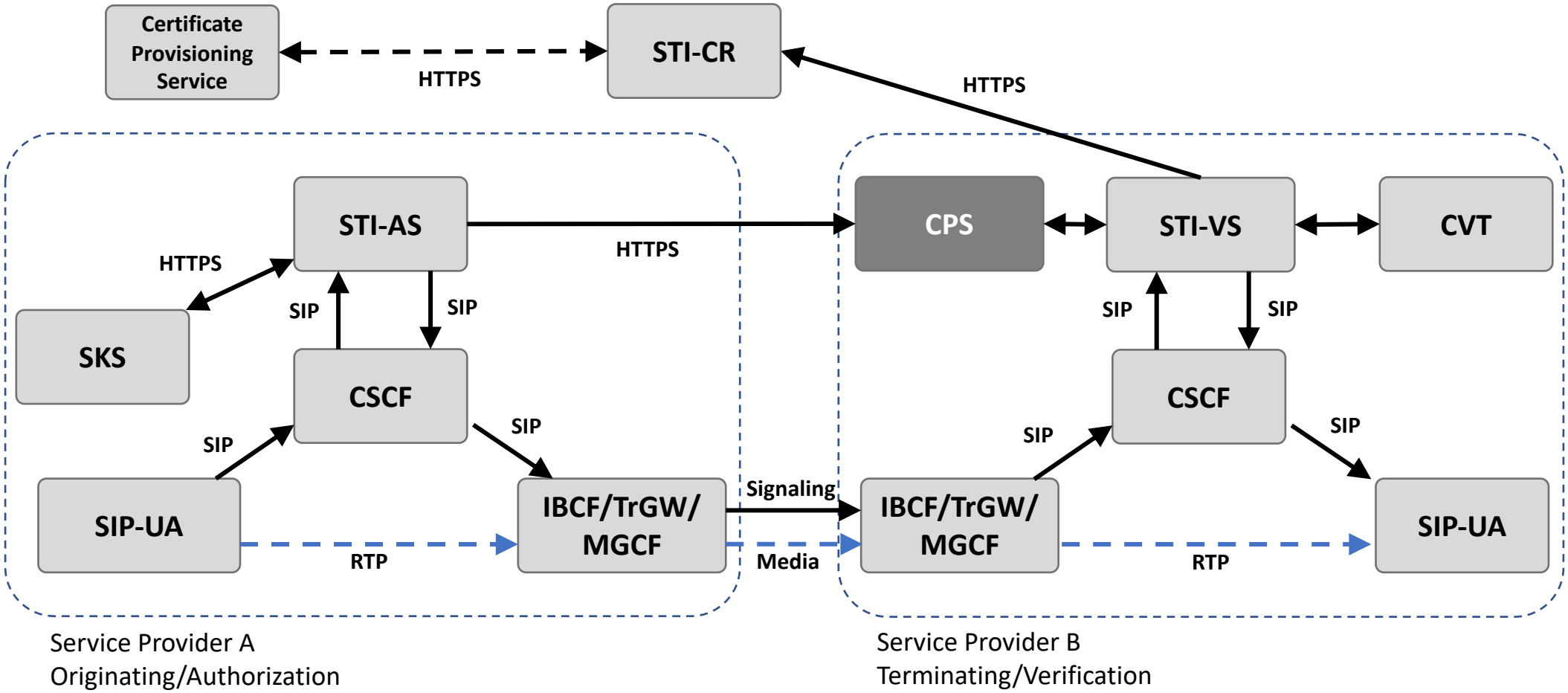
How to Build a Call Placement Service (CPS) for Out-of-Band SHAKEN

Alec Fenichel
Senior Software Architect
TransNexus

SHAKEN Call Flow



Out-of-Band SHAKEN Call Flow



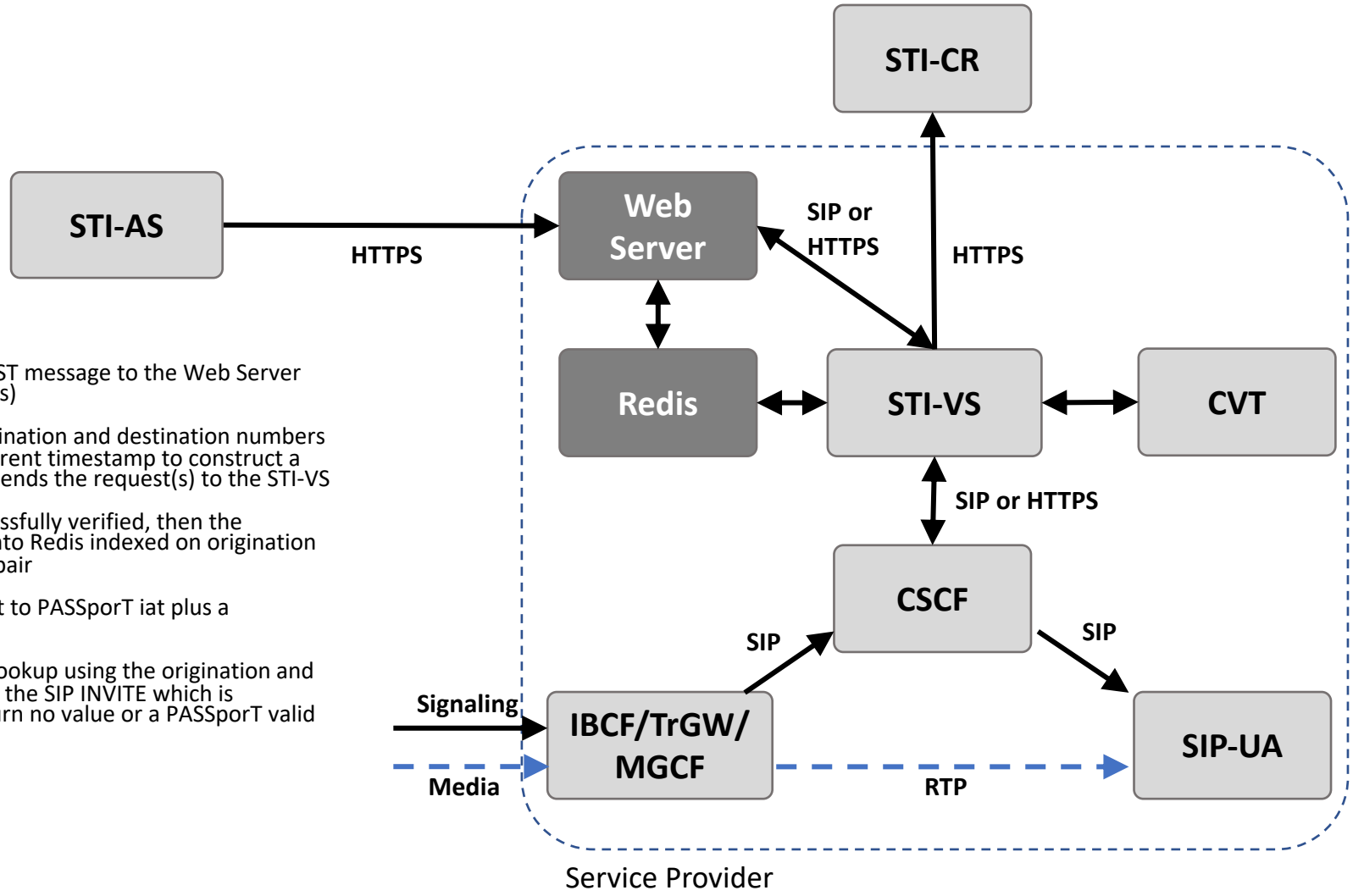
CPS Requirements

- Accept PASSporT(s) from an STI-AS via an HTTPS POST
  - Requires a **web server**
- Store PASSporT(s) until call arrives
  - Requires a **database**
- Verify PASSporT(s) before persisting
  - Requires communication with the STI-VS using HTTP or SIP
- Provide PASSporT(s) to STI-VS when call arrives
  - Requires integration with the STI-VS

Open Source CPS Components

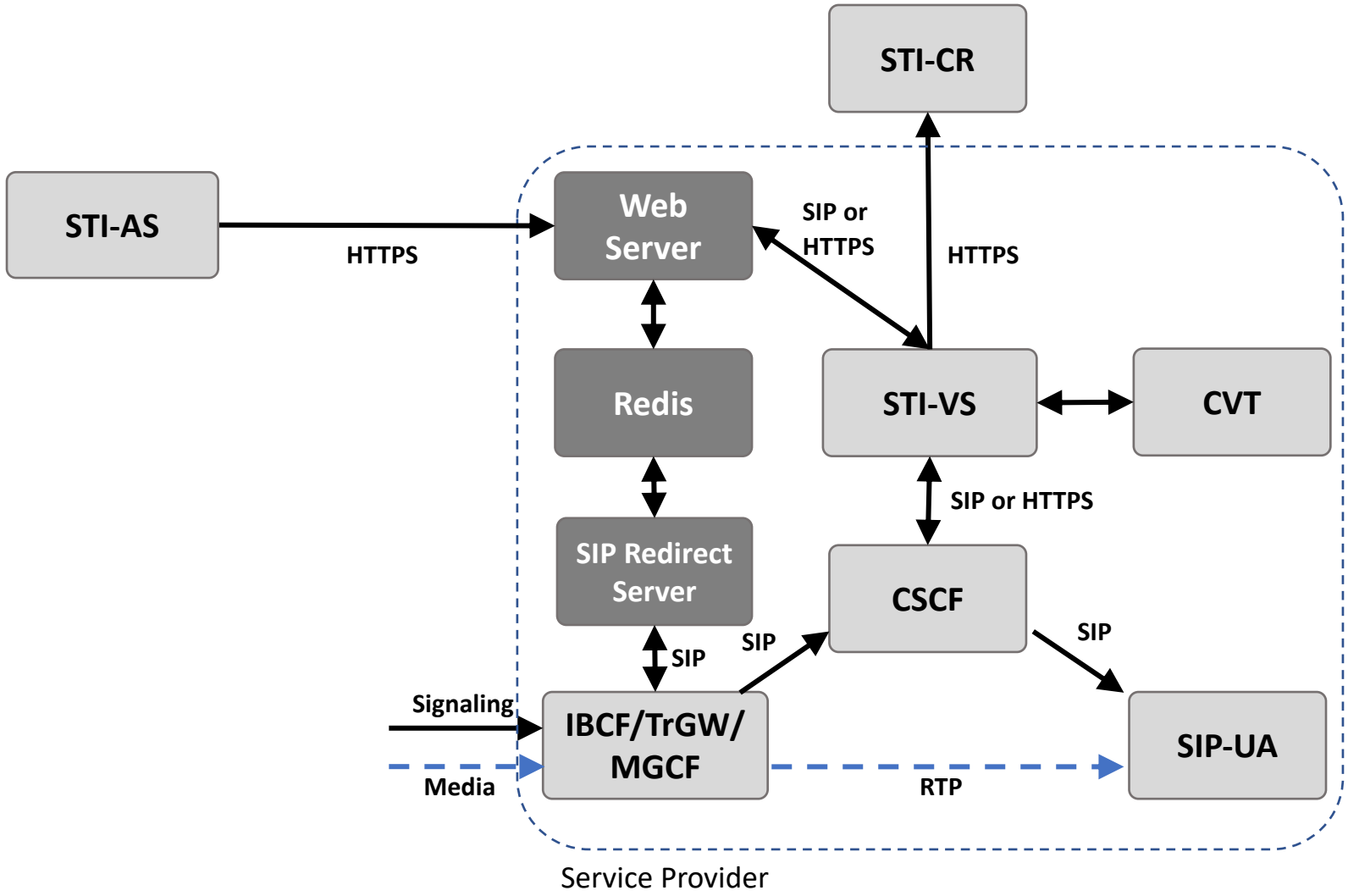
- Web Server
  - https://github.com/TransNexus/call-placement-service
  - Developed using Node.js
  - Supports HTTP STI-VS interface (defined in ATIS-1000082)
  - SIP STI-VS interface in development
  - Integrates with Redis
- Database
  - Redis

Open Source CPS Deployment

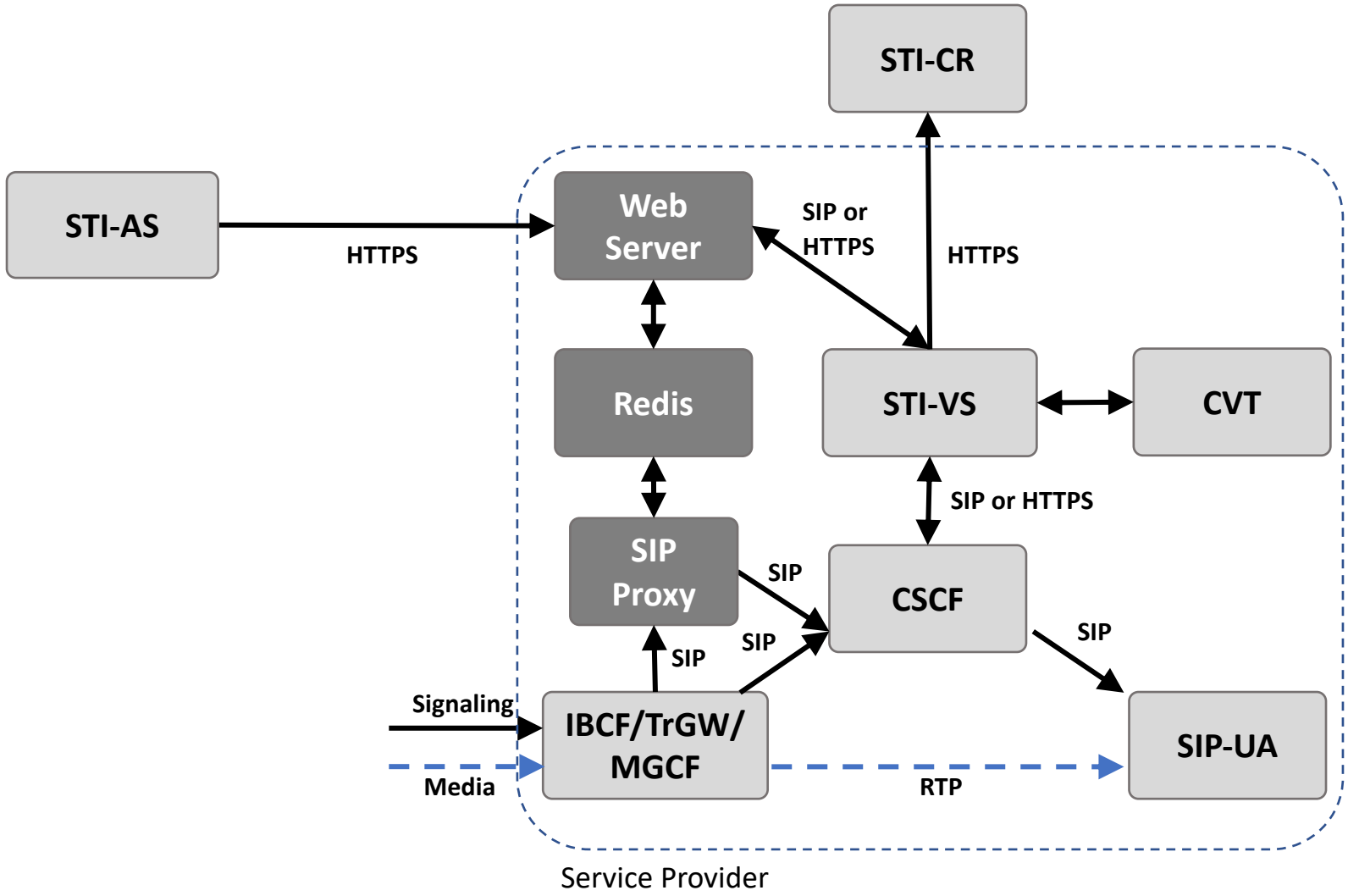


1. STI-AS sends an HTTP POST message to the Web Server containing the PASSporT(s)
2. Web Server uses the origination and destination numbers from the URL and the current timestamp to construct a verification request and sends the request(s) to the STI-VS
3. If all PASSporTs are successfully verified, then the PASSporTs are inserted into Redis indexed on origination and destination number pair
4. Redis key expiration is set to PASSporT iat plus a configurable freshness
5. STI-VS performs a Redis lookup using the origination and destination number from the SIP INVITE which is guaranteed to either return no value or a PASSporT valid for that call

Open Source CPS Deployment: SIP Redirect



Open Source CPS Deployment: SIP Proxy



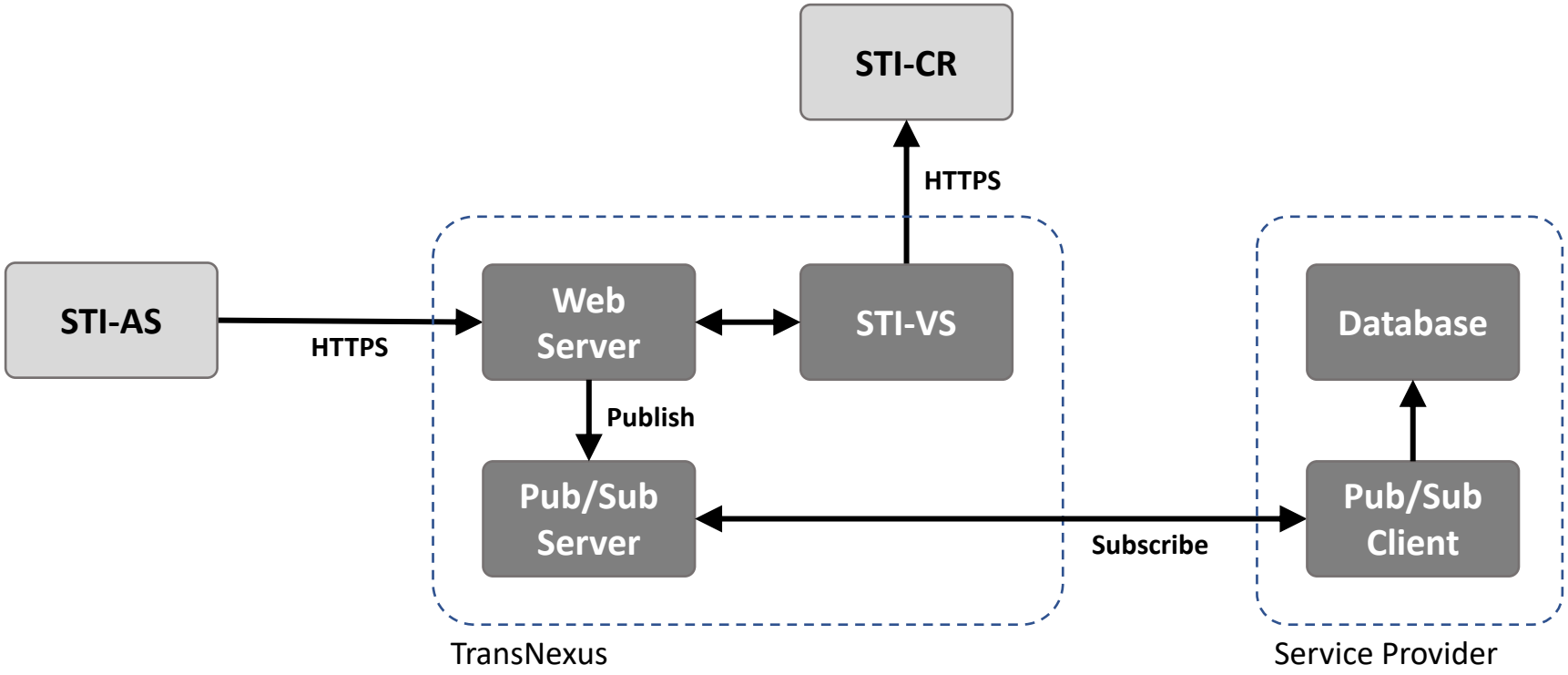
Open Source CPS Components

- Web Server
  - https://github.com/TransNexus/call-placement-service
  - Developed using Node.js
  - Supports HTTP STI-VS interface (defined in ATIS-1000082)
  - SIP STI-VS interface in development
  - Integrates with Redis
- Database
  - Redis
- SIP Redirect Server or SIP Proxy
  - Kamailio
  - OpenSIPS

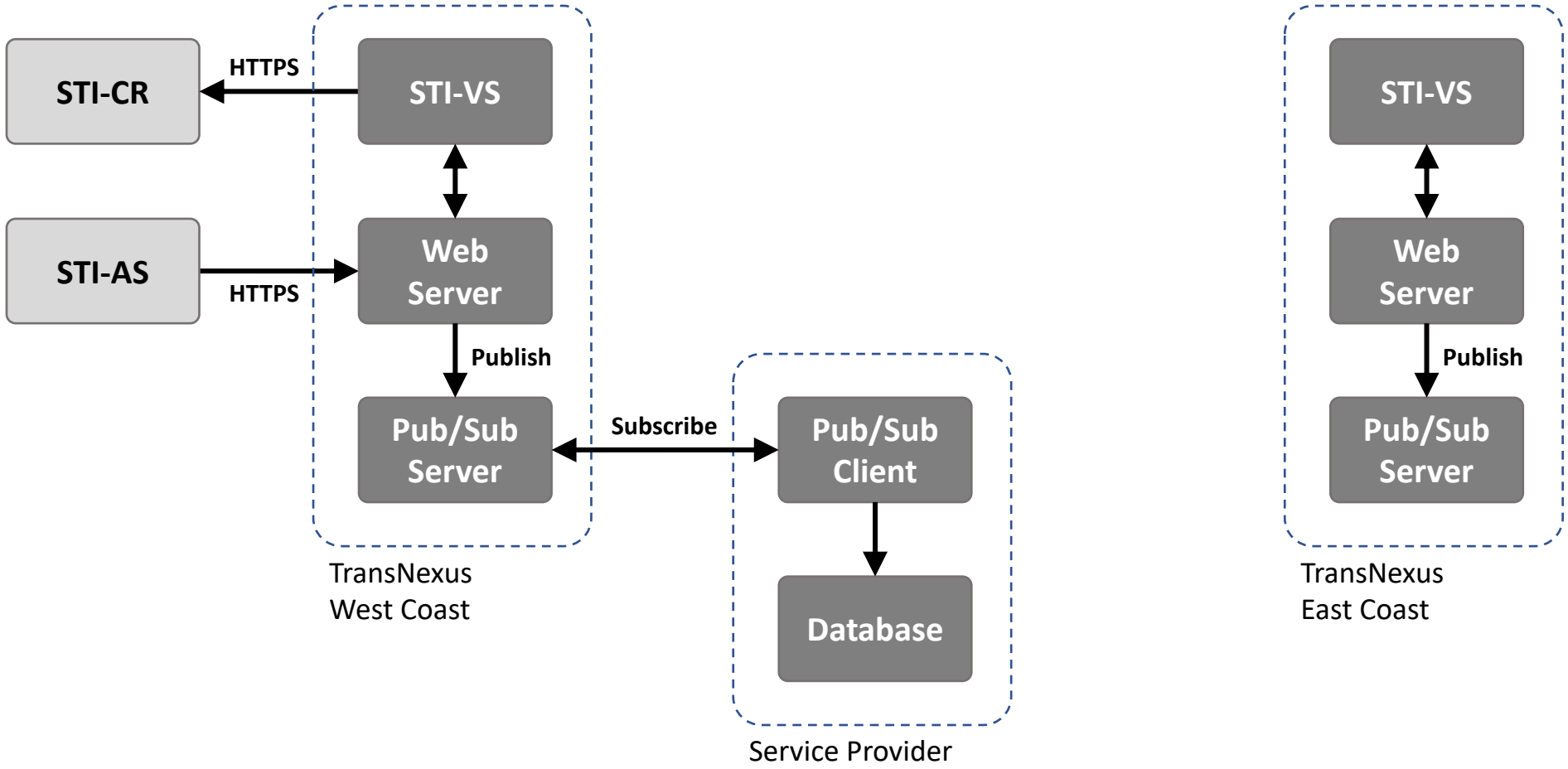
Announcing TransNexus CPS

- Managed CPS as a service
- Publish/subscribe model
- Redundant – 6 active data centers with anycast routing
- Scalable – tested at over 1 million HTTP POSTs / second
- Available starting today
- Completely free

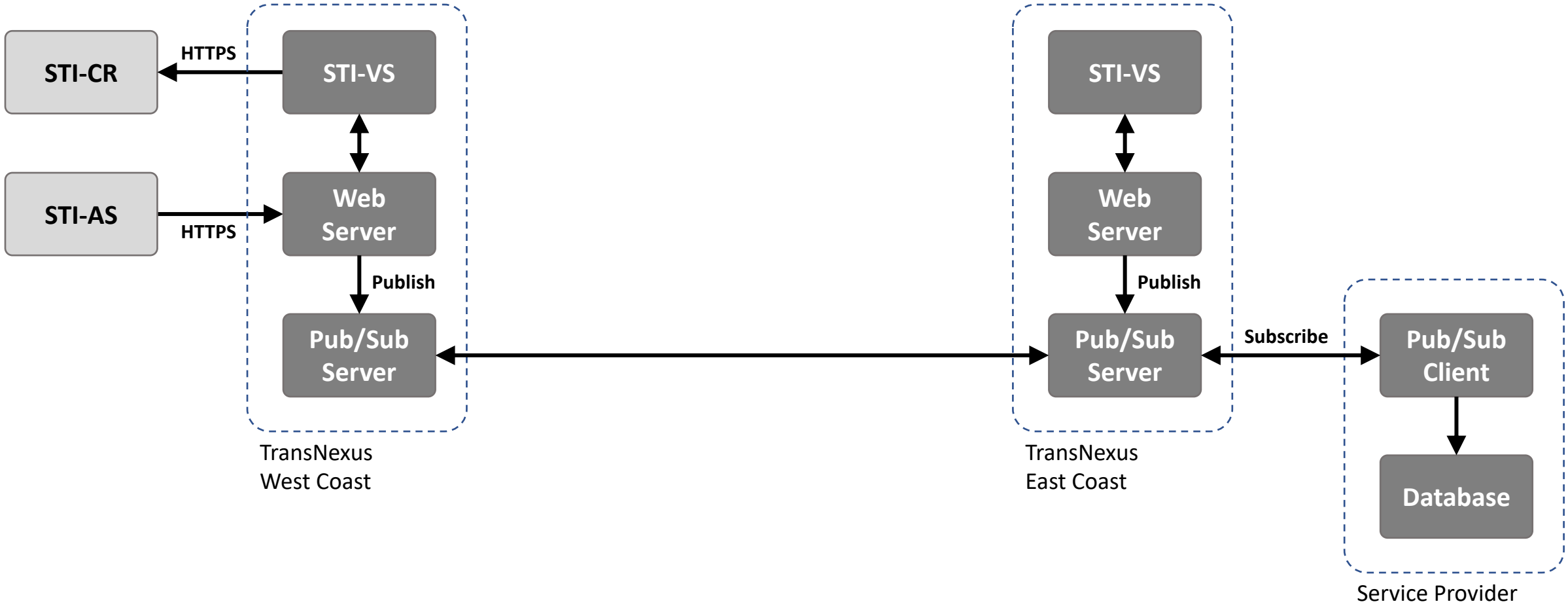
TransNexus CPS Architecture



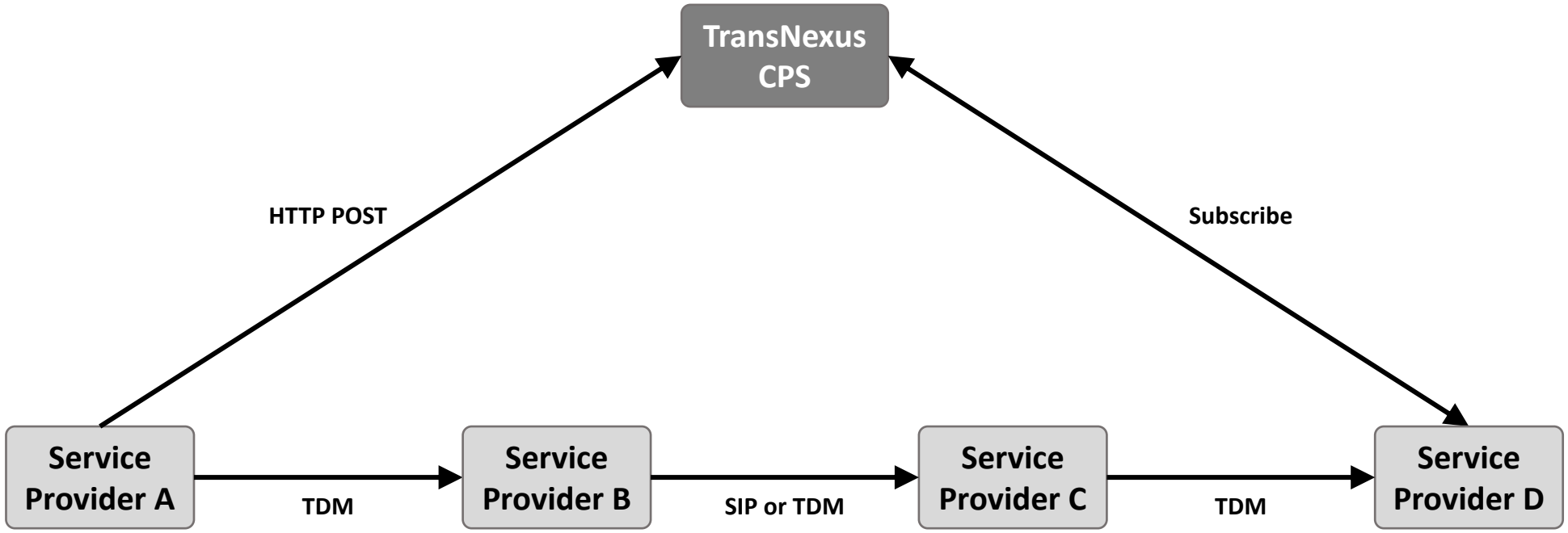
TransNexus CPS Geographic Message Routing



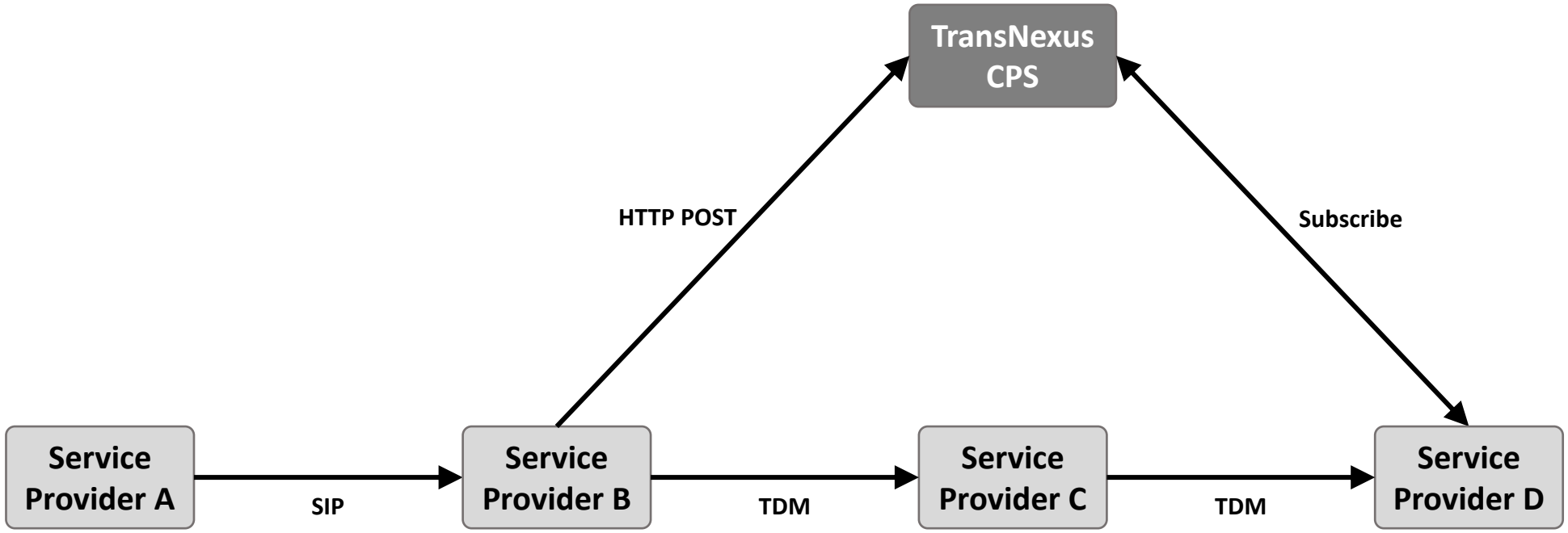
TransNexus CPS Geographic Message Routing



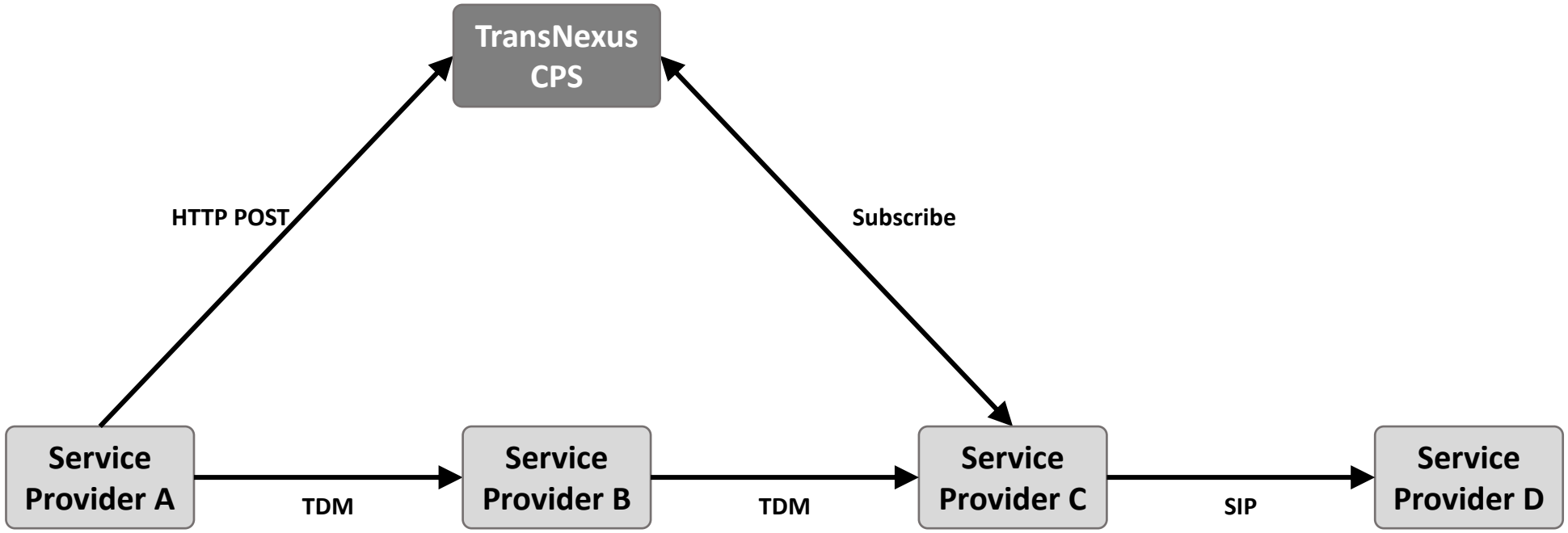
TransNexus CPS Standard Call Flow



TransNexus CPS Transit POST Call Flow



TransNexus CPS Transit Subscribe Call Flow



TransNexus CPS Publish

- Anyone can send PASSporTs via an HTTP POST
- PASSports are verified before being published
- All PASSporTs from the HTTP POST are published in a single message
- HTTP POST URL format:

  `https://cps.transnexus.com/DEST_SPC/DEST_NUMBER/ORIG_SPC/ORIG_NUMBER`

TransNexus CPS Subject and Message Format

Subject:

```
DEST_SPC.DEST_NUMBER.ORIG_SPC.ORIG_NUMBER
```

Message:

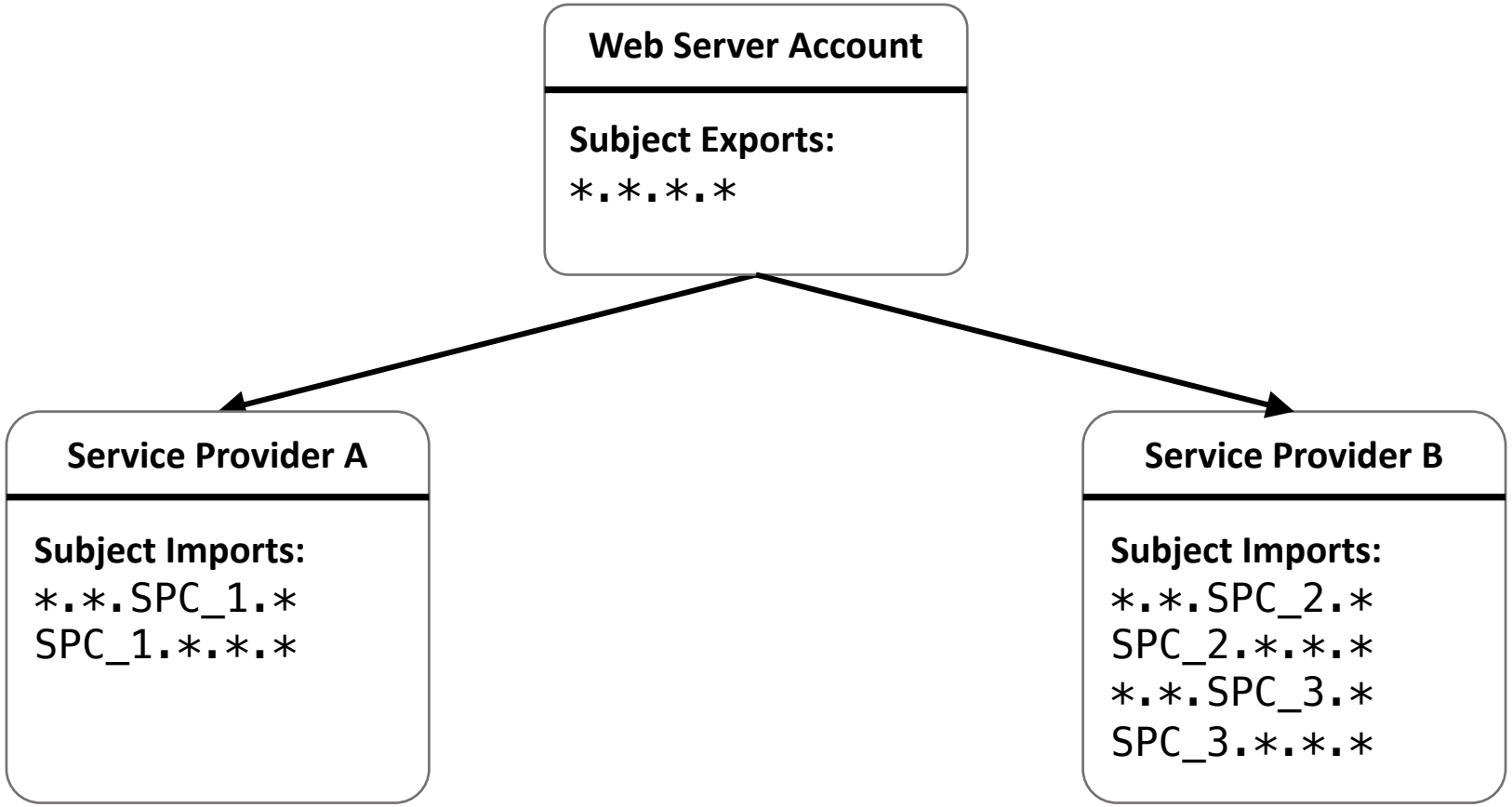
```
{
  "ip": "HTTP_POST_SOURCE_IP",
  "passports": [
    {
      "passport": "PASSPORT_1",
      "certificates": [ "PEM_SHAKEN_CERTIFICATE", "PEM_INTERMEDIATE_CERTIFICATE", "PEM_ROOT_CERTIFICATE" ]
    },
    {
      "passport": "PASSPORT_2",
      "certificates": [ "PEM_SHAKEN_CERTIFICATE", "PEM_INTERMEDIATE_CERTIFICATE", "PEM_ROOT_CERTIFICATE" ]
    }
  ]
}
```

TransNexus CPS Registration

- Only STI-PA approved service providers can register
- Registration requires an SPC token
- Multiple SPC tokens can be provided
- Service providers only receive messages if the subject DEST_SPC or ORIG_SPC matches one their SPCs
- Authentication uses NKEYs and JWTs
- Service providers supply their public NKEY during registration
- Behind the scenes TransNexus CPS issues an account JWT the defines the service providers permissions

TransNexus CPS Account Isolation

Subject: `DEST_SPC.DEST_NUMBER.ORIG_SPC.ORIG_NUMBER`



TransNexus CPS Subscribe

- A user NKEY pair must first be created
- Service providers authorize users by creating a user JWT that specifies the user's permissions and then service providers sign the JWT with their account NKEY
- User permissions can allow subscribing to to all subjects (within the account) or a subset:
  - Subscribe to all

```
*.*.*.*
```

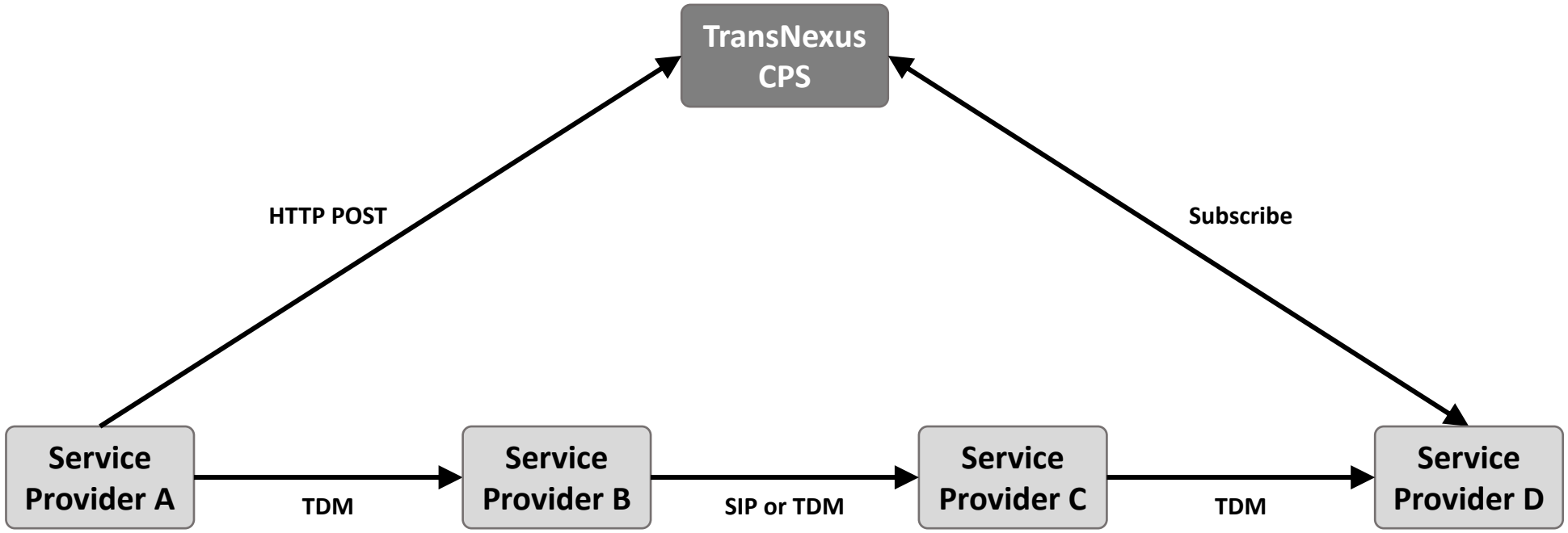
  - Subscribe to specific SPC

```
1234.*.*.*
*.*.1234.*
```

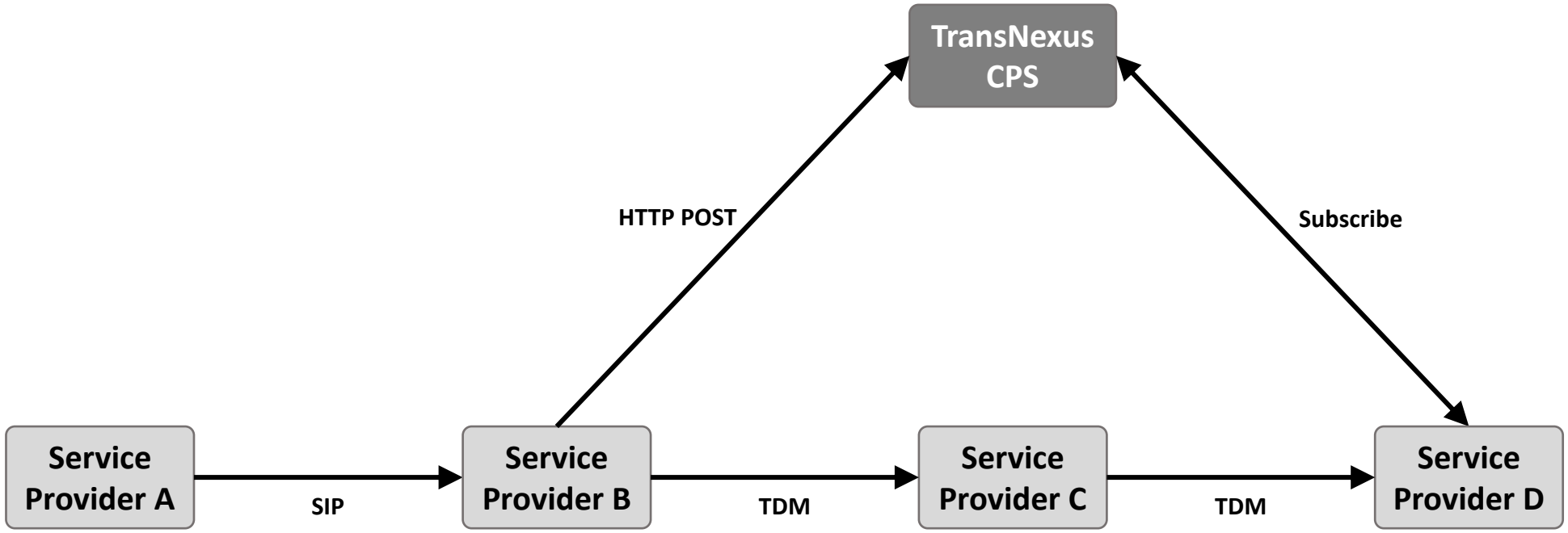
  - Subscribe to specific number

```
*.14045266060.*.*
*.*.*.14045266060
```

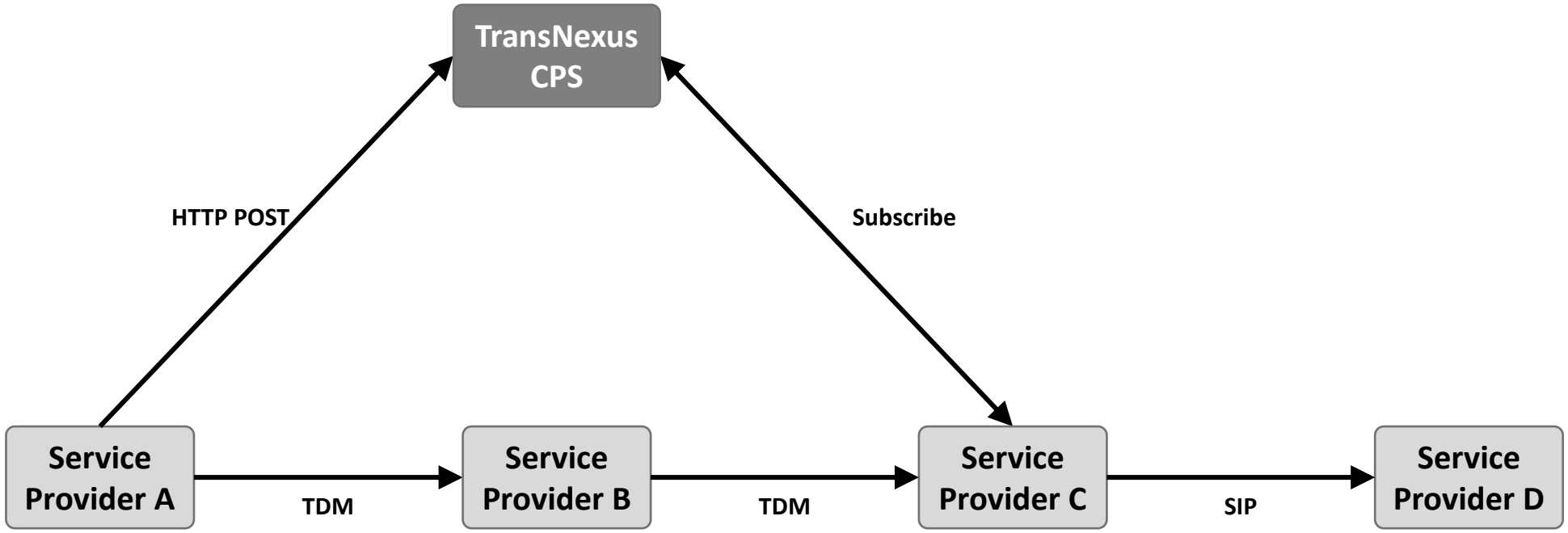
TransNexus CPS Standard Call Flow



TransNexus CPS Transit POST Call Flow



TransNexus CPS Transit Subscribe Call Flow



TransNexus CPS Transit Subscribe Method 1

- Service Provider D registers with TransNexus CPS
- Service Provider D issues user credentials for Service Provider C that can be optionally restricted to specific subjects:

```
SERVICE_PROVIDER_D_SPC.*.*.*
SERVICE_PROVIDER_D_SPC.*.SEVICE_PROVIDER_A_SPC.*
```

- Service Provider C subscribes to TransNexus CPS
- Service Provider A POSTs the PASSporT to TransNexus CPS
- Service Provider C receives the PASSporT

TransNexus CPS Transit Subscribe Method 2

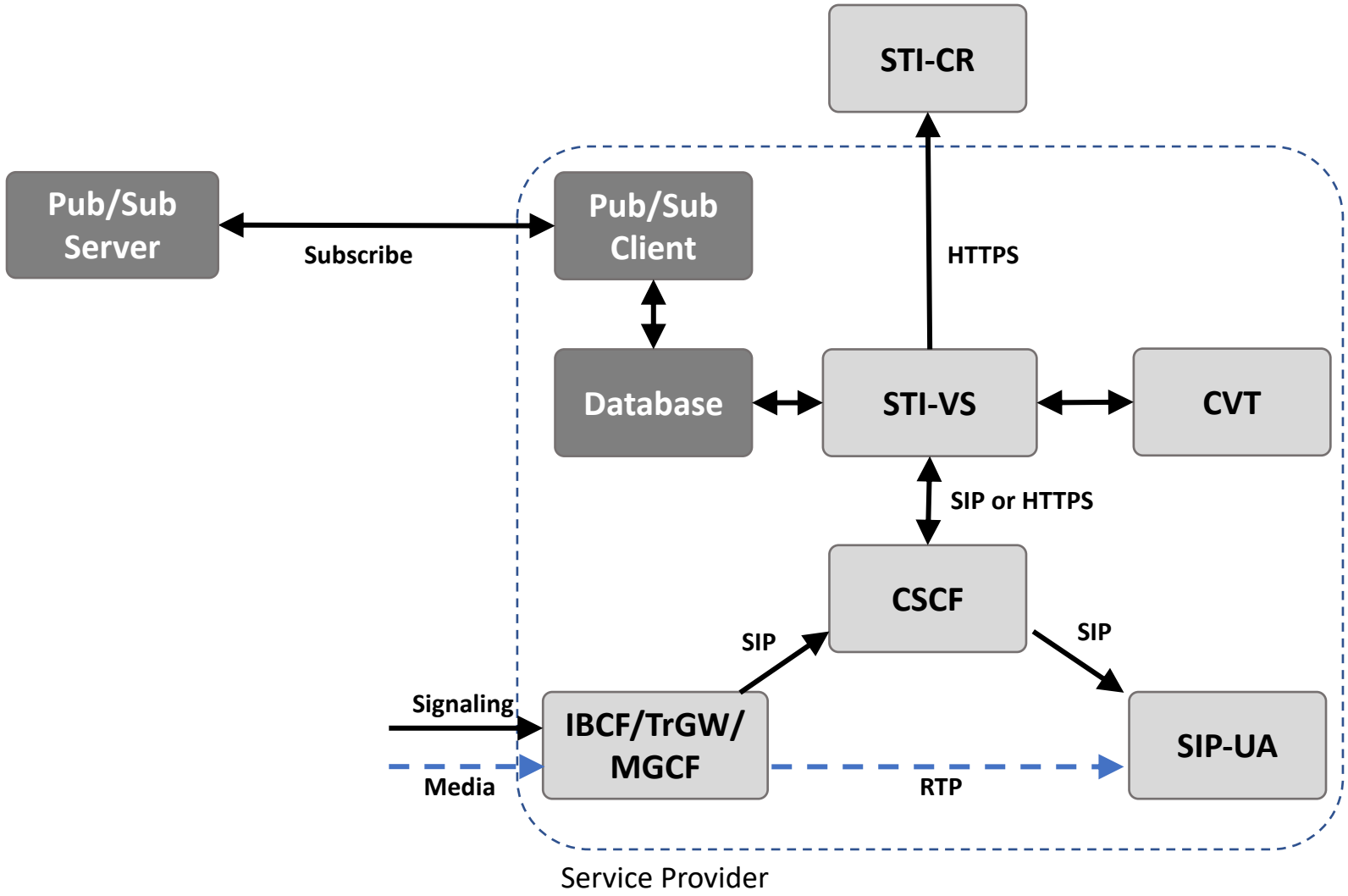
- Service Provider A registers with TransNexus CPS
- Service Provider A issues user credentials for Service Provider C that can be optionally restricted to specific subjects:

`*.*.SEVICE_PROVIDER_A_SPC.*`

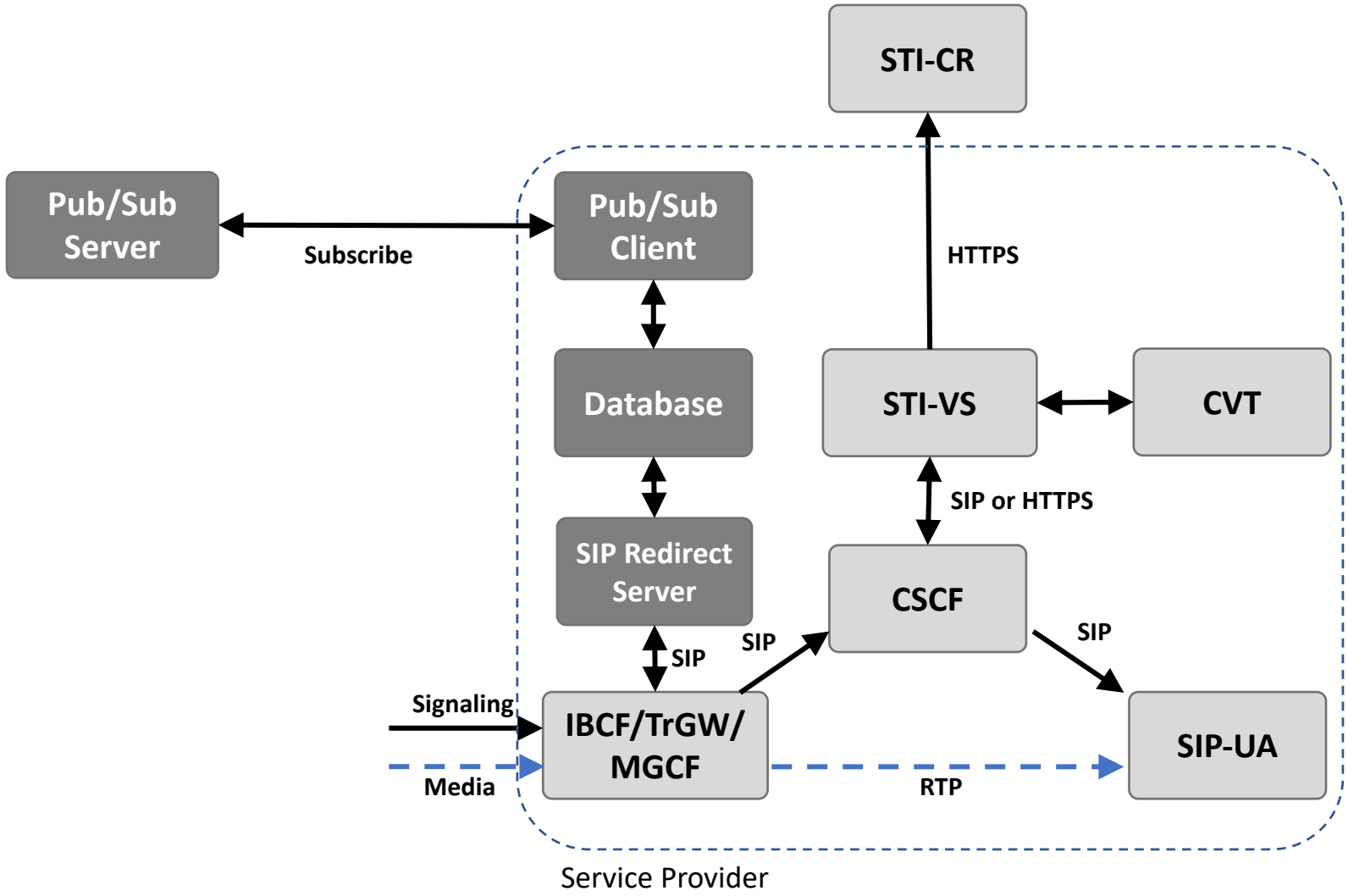
`SERVICE_PROVIDER_D_SPC.*.SEVICE_PROVIDER_A_SPC.*`

- Service Provider C subscribes to TransNexus CPS
- Service Provider A POSTs the PASSporT to TransNexus CPS
- Service Provider C receives the PASSporT

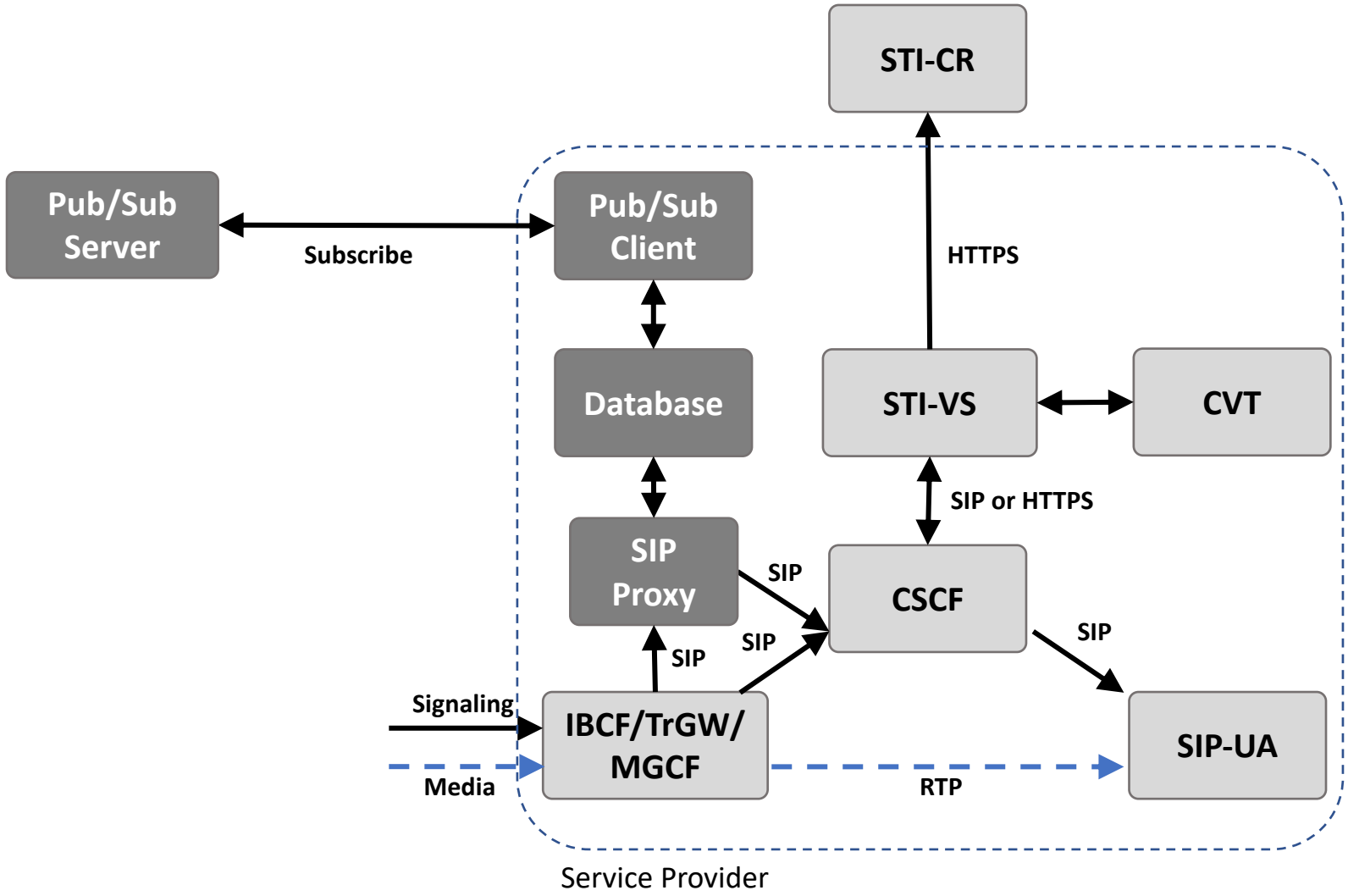
TransNexus CPS Deployment



TransNexus CPS Deployment: SIP Redirect



TransNexus CPS Deployment: SIP Proxy



TransNexus®

TransNexus CPS

- Managed CPS as a service
- Publish/subscribe model
- Redundant – 6 active data centers with anycast routing
- Scalable – tested at over 1 million HTTP POSTs / second
- Available starting today
- Completely free
- Client: https://github.com/TransNexus/transnexus-cps-client
- Email me for a copy of the presentation: alec.fenichel@transnexus.com