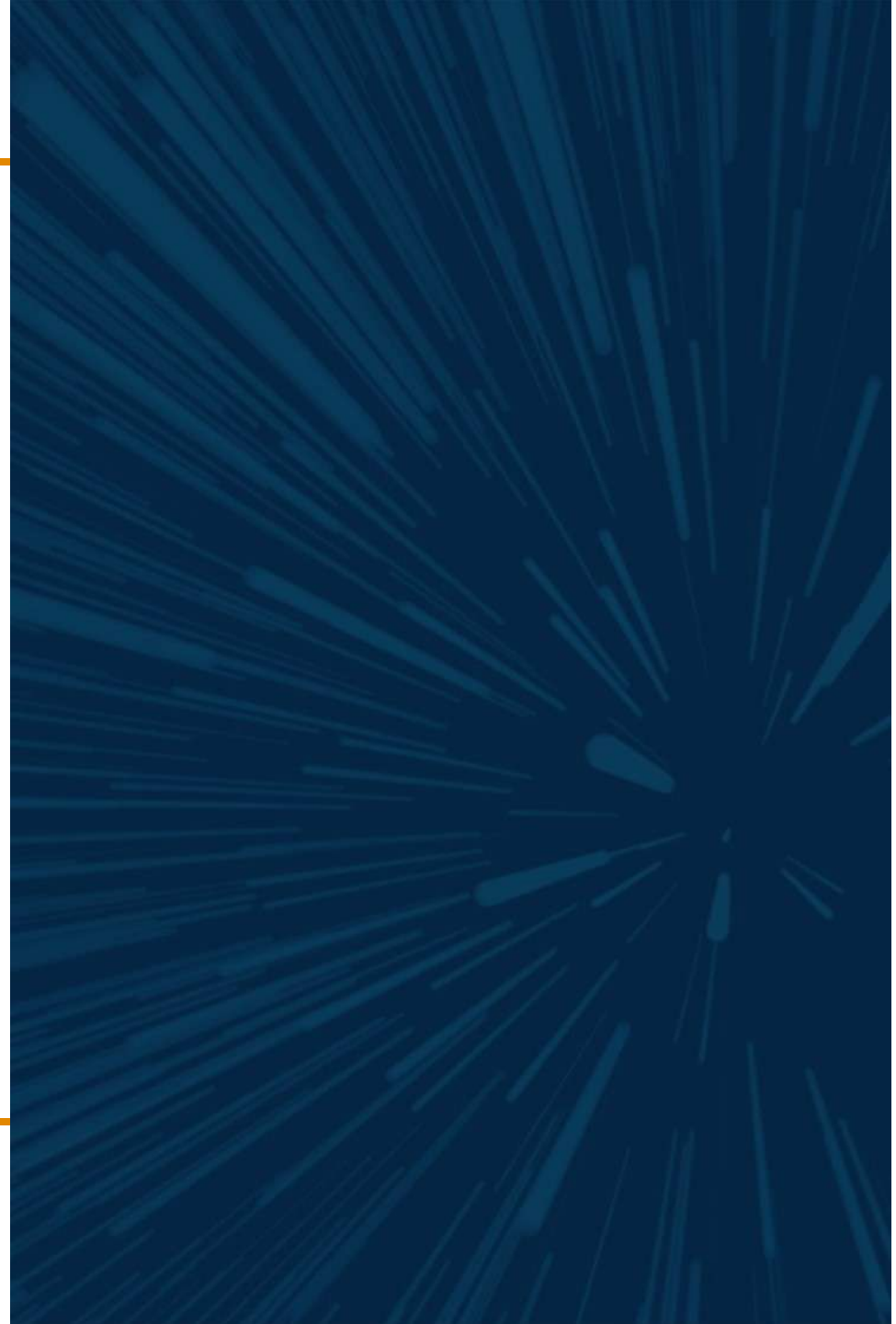
Simplifying the Full Attestation Enterprise Problem

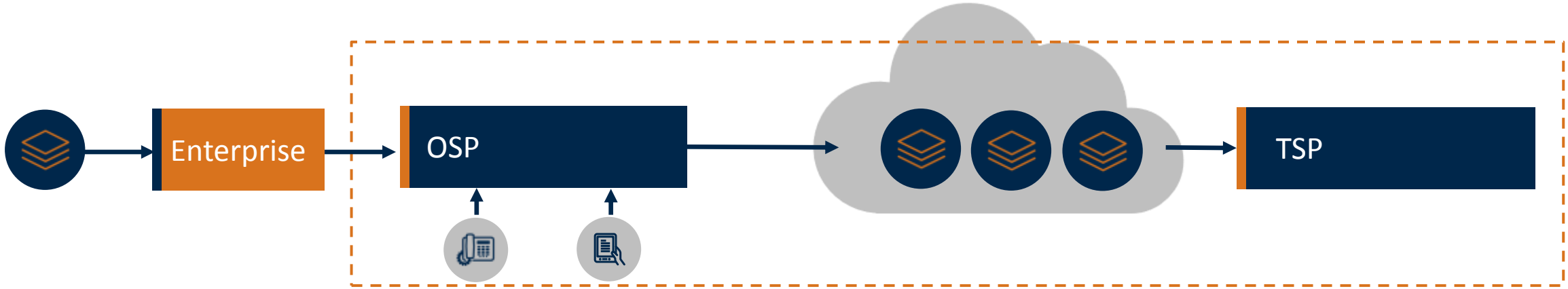
with a Central TN Database

Dr Peter Brown | STIR/SHAKEN Product Manager
4 December 2019

metaswitch



STIR/SHAKEN context



- STIR/SHAKEN creates a trust relationship between OSP and TSP
  - Regardless of the multiple entities through which the SIP traffic must pass
- An OSP's subscribers are in this circle of trust, i.e. they get A-level attestation
  - Which requires that the OSP polices its subscribers' connections
- We want to add the OSP's Enterprise Customers to this circle
  - There may be a chain of Enterprises upstream of the OSP's Customer involved in the initiation of a call

Guiding Principles

There are multiple “Central TN Database” approaches.

Here we are concerned with a database which:

- Records TNs that are assigned to Enterprises
- Is centrally administered, or is synchronized between multiple providers
- May have multiple service bureaus that provide access.

My involvement:

- Presenting a database-driven approach for consideration as an alternative to certificate-based approaches
- Driven by the demand from our carrier customers to offer a viable approach to their enterprises.

Guiding Principles: Central TN Database

Central TN Database

Enterprises:
No Network Impact

- No new Network Elements
- No software upgrades

Service Providers:
Minimal Impact

- Minimal software changes
- Minimal administration effort

Central TN Database

Interactions

Central TN Database - Definitions

OSP	Originating Service Provider
TSP	Terminating Service Provider
TNSP	TN Service Provider; service provider that owns TNs and distributes to Enterprises
Enterprise	Any non-SP organization involved in VoIP call path
Initiator Enterprise	Enterprise that is permitted to create a SIP INVITE for a TN
Enabler Enterprise	Enterprise that is permitted to pass-through a SIP INVITE for a TN

Central TN Database – Enterprise identity

Enterprise identity is a crucial element in the CTND approach

---

Enterprises must be vetted and be provided with a unique Enterprise ID

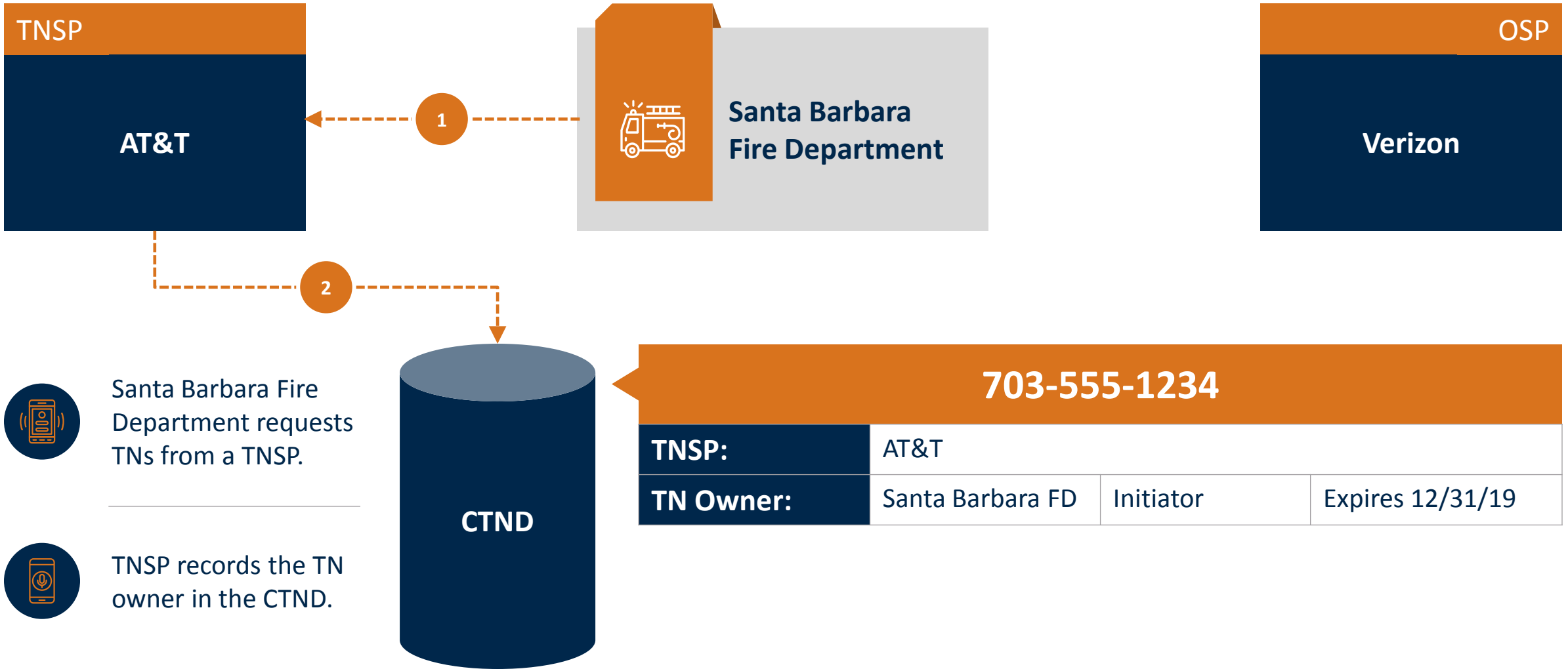
Envisage a central Enterprise ID repository from which:

- Enterprises request IDs
- OSPs & TNSPs can validate Enterprise ID interactions

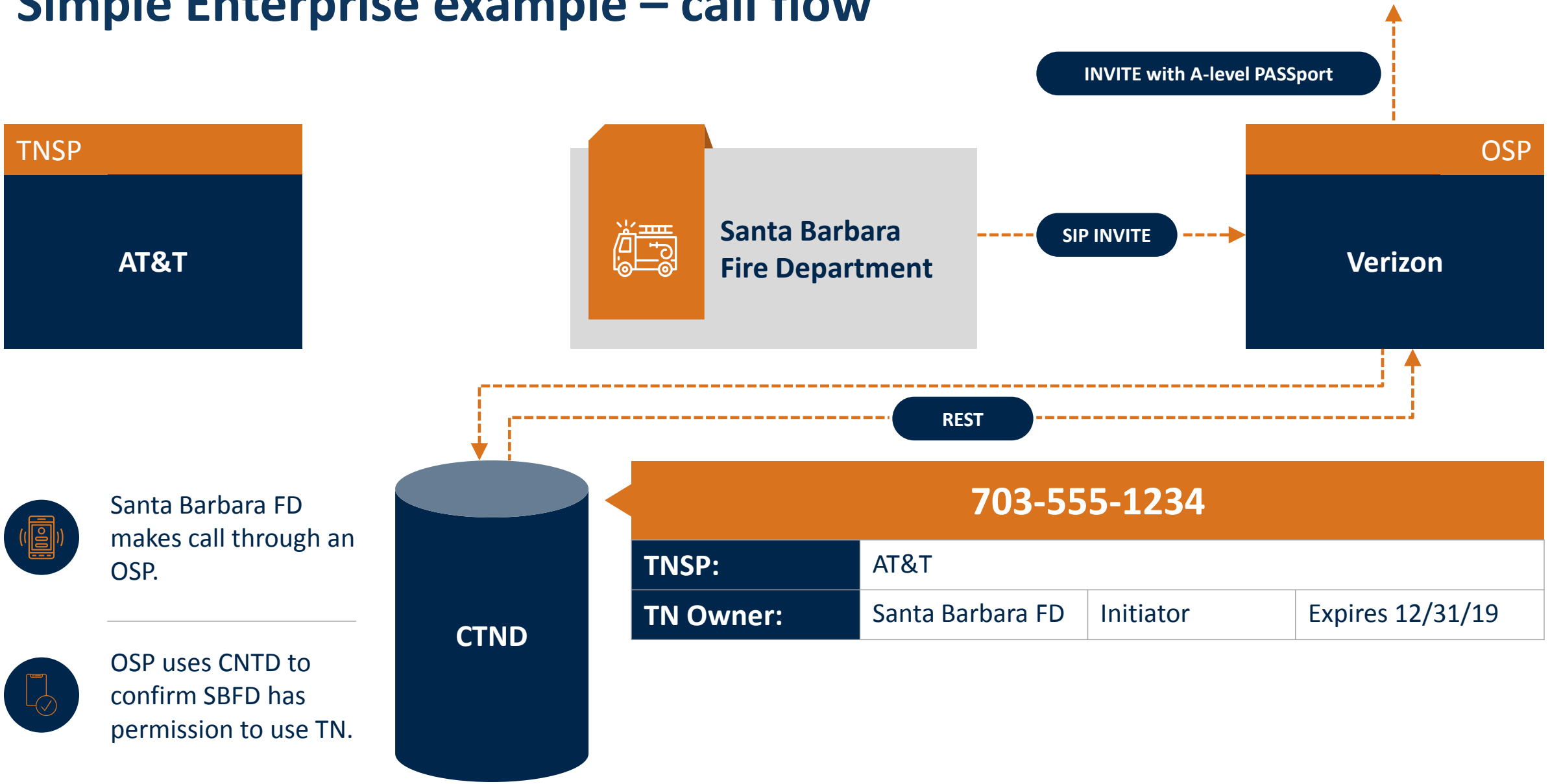
Enterprises can use their ID

- When requesting TNs from their TNSP(s)
- When establishing their connectivity with their OSP(s)
- To login to the Central TN Database to assign their TNs to other Enterprises
- Optionally, to login to the CTND to add Rich Call Data that will be used by the OSP.

Simple Enterprise example – TN assignment



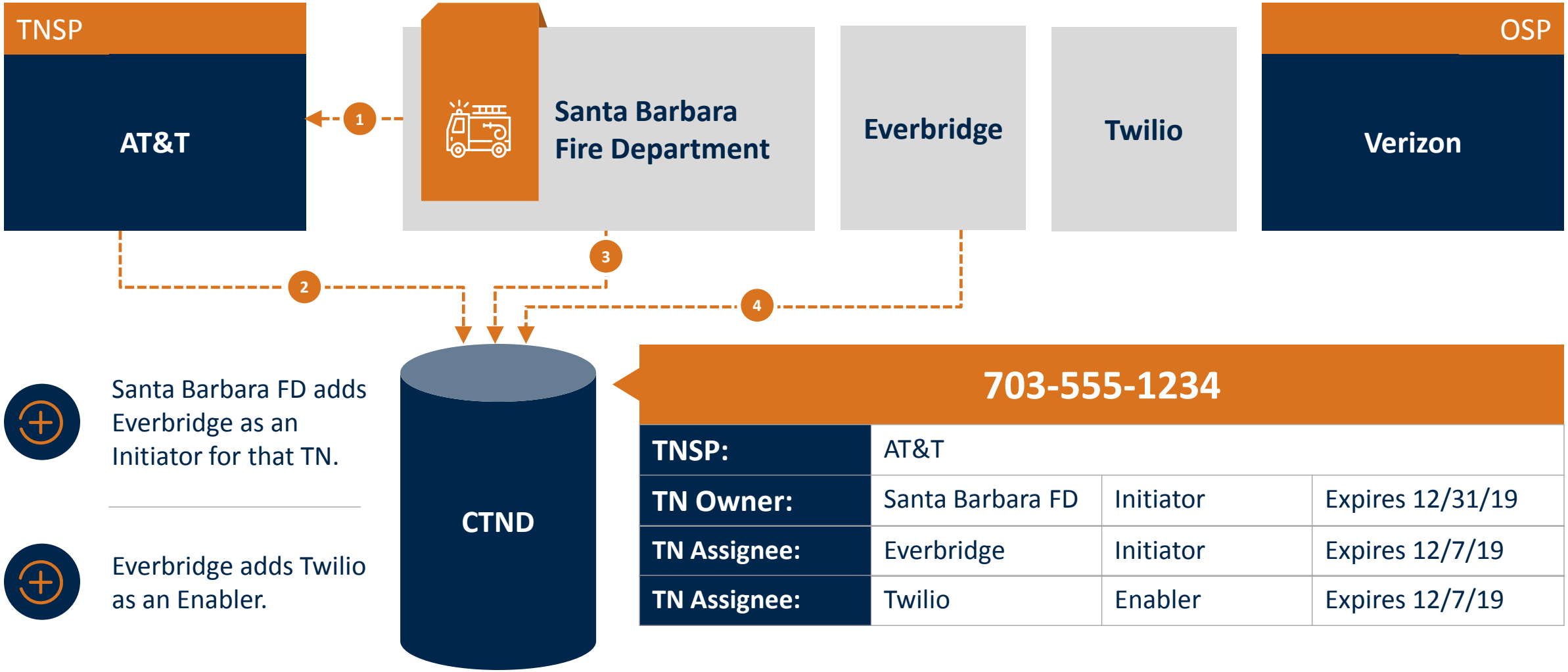
Simple Enterprise example – call flow



Santa Barbara FD makes call through an OSP.

OSP uses CNTD to confirm SBFD has permission to use TN.

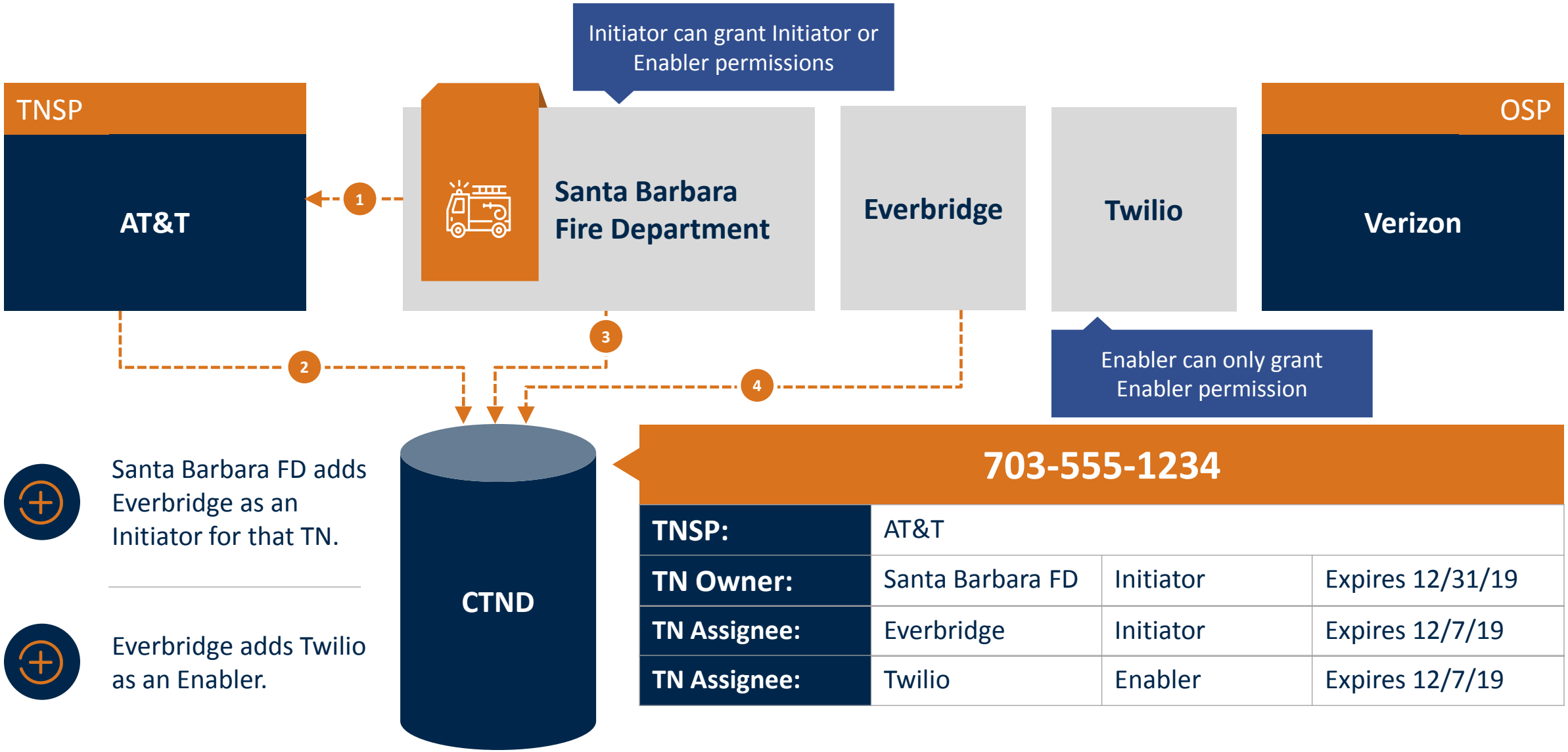
Complex Enterprise example – TN assignment



703-555-1234

TNSP:	AT&T		
TN Owner:	Santa Barbara FD	Initiator	Expires 12/31/19
TN Assignee:	Everbridge	Initiator	Expires 12/7/19
TN Assignee:	Twilio	Enabler	Expires 12/7/19

Complex Enterprise example – Permissions



Santa Barbara FD adds Everbridge as an Initiator for that TN.

Everbridge adds Twilio as an Enabler.

703-555-1234

TNSP:	AT&T		
TN Owner:	Santa Barbara FD	Initiator	Expires 12/31/19
TN Assignee:	Everbridge	Initiator	Expires 12/7/19
TN Assignee:	Twilio	Enabler	Expires 12/7/19

Complex Enterprise example – call flow

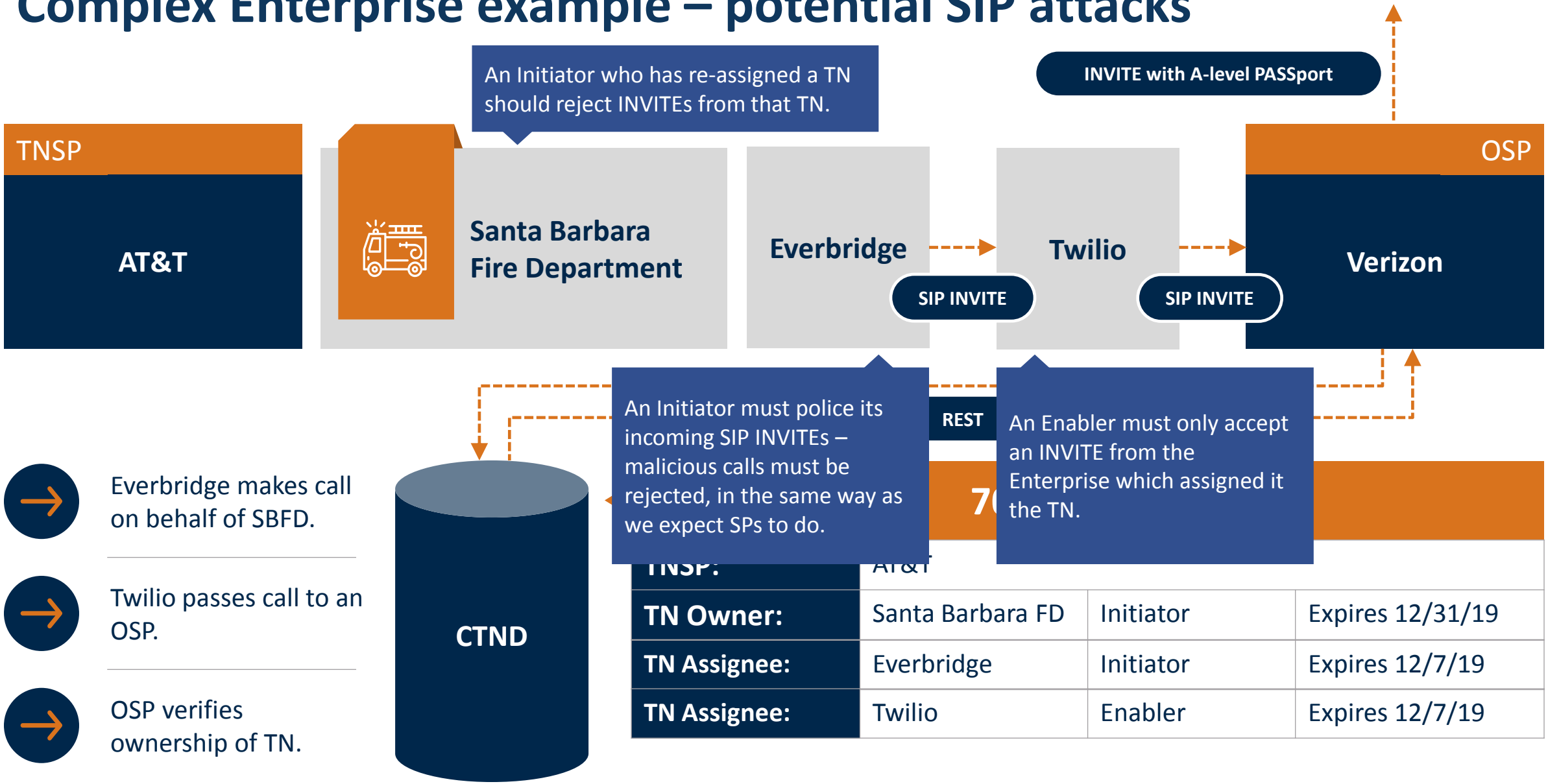
- Everbridge makes call on behalf of SBFD.
- Twilio passes call to an OSP.
- OSP verifies ownership of TN.

703-555-1234

TNSP:	AT&T		
TN Owner:	Santa Barbara FD	Initiator	Expires 12/31/19
TN Assignee:	Everbridge	Initiator	Expires 12/7/19
TN Assignee:	Twilio		

OSP knows the calling party as the last Initiator in the CTND chain. Important for traceback.

Complex Enterprise example – potential SIP attacks



TNSP:	AT&T		
TN Owner:	Santa Barbara FD	Initiator	Expires 12/31/19
TN Assignee:	Everbridge	Initiator	Expires 12/7/19
TN Assignee:	Twilio	Enabler	Expires 12/7/19

Central TN Database – Reputation check on Enterprises

Central TN Database

The Central TN Database can provide a reputation score, based on Analytics, to the OSP

- Score based on spoofing rate for calls which have been Initiated/Enabled by an Enterprise

Given a chain of custody of a TN (from the CTND), the OSP can make a decision based on its local policy using:

- The reputation of the Initiator Enterprise
- The reputations of the subsequent Enabler Enterprises
- and hence whether these entities are known to follow best practice on ensuring malicious INVITEs are rejected.

Central TN Database

Summary

Central TN Database - Summary

Central TN Database

- Stores information about TNs that have been delegated to Enterprises
- Each TN is associated with a “chain of custody” of the Enterprises by which it has been delegated
- Each of these Enterprises are classified as Initiators or Enablers to allow traceback.

TNSP

- Adds information about delegated TNs to CTND.

Enterprises

- Register with Enterprise ID database
- Use Enterprise ID in interactions with TNSPs and OSPs
- If delegating TNs to another VoIP entity, must register that delegation in the CTND
- Must police incoming INVITEs to avoid malicious attacks.

OSP

- Uses CTND information to confirm whether its Customer has the right to use a delegated TN
- Can use CTND information for traceback purposes and, potentially, to retrieve RCD information
- Optionally, can use CTND reputation information for analytics purposes.

Central TN Database - Benefits

Central TN Database

Simplicity

- Enterprises need no new hardware or software
- Enterprises are not responsible for certificates
- Carriers do not need to host subordinate CAs.

Low Friction

- Only administrative process changes in the Carrier-Enterprise and Enterprise-Enterprise relationships.
- No stacking of identity headers required.
- No requirement for Terminating SP to deploy anything other than existing STI-VS.

Q&A

peter.brown@metaswitch.com