

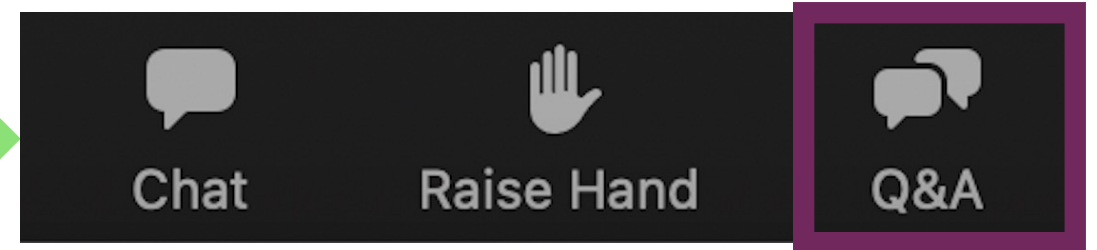


Third-Party Certificates: Learn Why You Need to Make This Your First Priority

September 7, 2023

Zoom Webinar Control Panel

Submit your questions using the Q&A feature and our moderator will address your questions live.



Your
Moderator



Joel Bernstein
Vice President, Regulatory
& Public Policy

Today we will cover:



1. In-Depth Overview of Certificates
2. Moderated Panel Discussion
3. Q&A

David
Hancock



PKI Security Analyst
Somos

Benefits of Delegate Certificates

- Provide a way for Service Providers to indicate verified association between the user of a telephone number and that telephone number
- This association is sometimes difficult to achieve in complex call scenarios
- Enable cryptographic proof of the association carried in the call signaling, which can be verified at the terminating service provider network and indicated to the calling party that this user is authorized to use that number
- With this additional verification, the goal is for users to be more willing to answer their calls

Acronyms and Definitions

- SP – VoIP Service Provider (specifically, a shaken-approved Service Provider)
- OSP – Originating SP
- TSP – Terminating SP
- CPaaS -- Communications Platform as a Service (typically not shaken-approved)
- OCN – Operating Company Number
- VoIP Entity – a VoIP entity such as an Enterprise SIP-PBX that is not shaken-approved

Comparing STI and Delegate Certificates

STI certificates and delegate certificates are the same in that the certificate credentials are used to sign PASSporTs that cryptographically demonstrate the caller's authority to use the calling TN

STI certificate
TNAuthList: 1234

Per ATIS-1000080, STI Certificates:

- Are issued to a shaken-approved OSP
- Contain a TNAuthList extension that identifies the OCN assigned to the OSP certificate holder

As a result of the FCC TRACED Act, there are currently there over 1200 shaken-approved OSPs authorized to obtain STI certificates

Delegate certificate
TNAuthList: 18005551212

Per ATIS-1000092, delegate certificates:

- Are issued to a non-shaken-approved VoIP Entities
- Contain a TNAuthList extension that identifies the set of (1 or more) TNs that the certificate credentials are authorized to sign

Although there is currently no FCC mandate w.r.t. support of delegate certificates, they do play a role in improving the security and accuracy of delivering verifiable calling TN information during call setup.

SHAKEN Can Easily Support These Call Scenarios

Call scenarios where:

- OSP has direct authenticated relationship with originating entity
- OSP assigns calling TN to originating entity

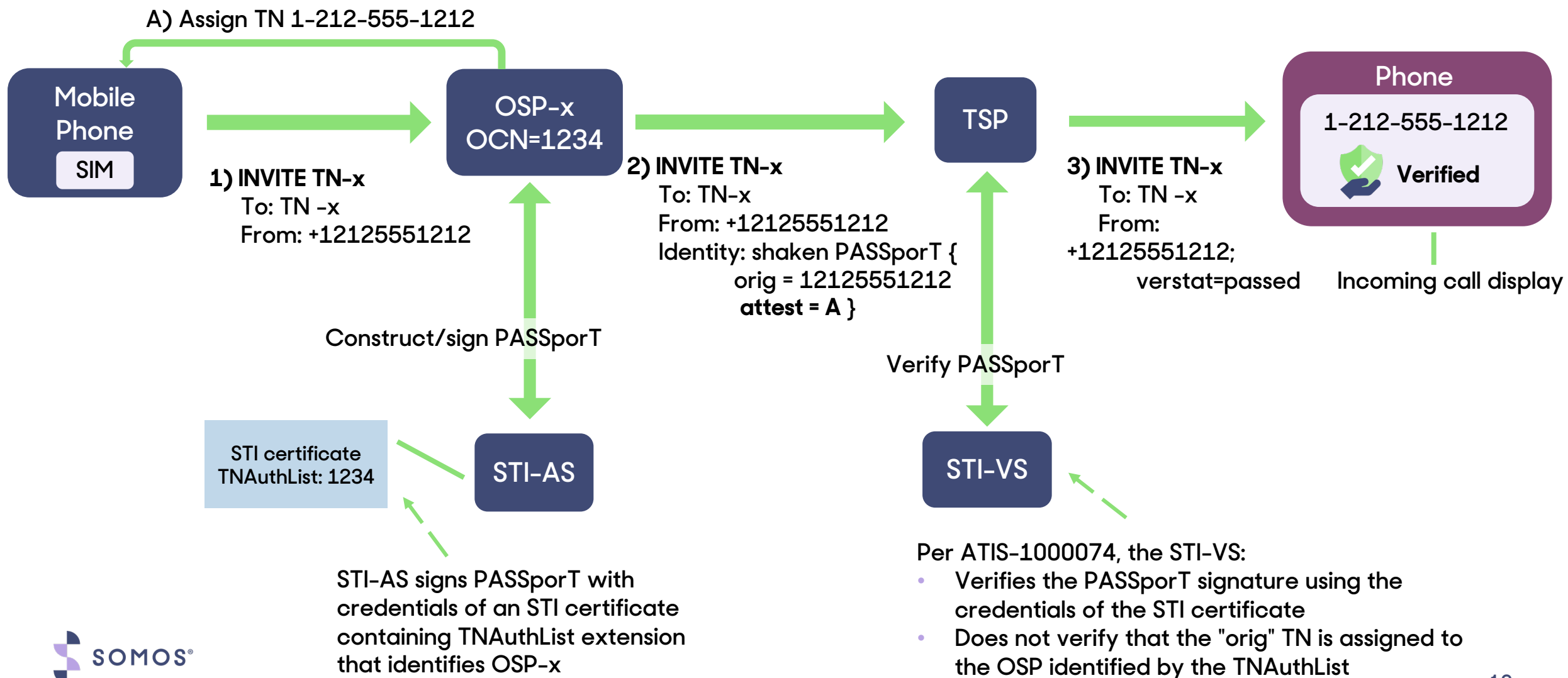
(E.g., calls originations from mobile phone)

Apply SHAKEN attestation criteria

SHAKEN "A" Attestation Criteria from ATIS-1000074	Status
OSP is responsible for the origination of call onto the voice network	yes
OSP has a direct authenticated relationship with the customer	yes
OSP has established a verified association with the calling TN	yes

Result:
OSP can
confidently
assert attest= A

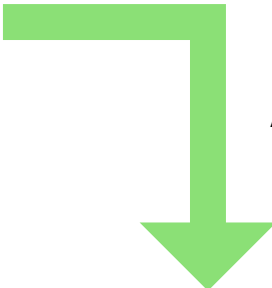
Example of "Easy" Call Scenario



Certain Call Scenarios Are More Challenging for SHAKEN

Call scenarios where:

- OSP does not have direct authenticated relationship with originating entity, and/or
- OSP has not assigned calling TN to originating entity



Apply SHAKEN attestation criteria

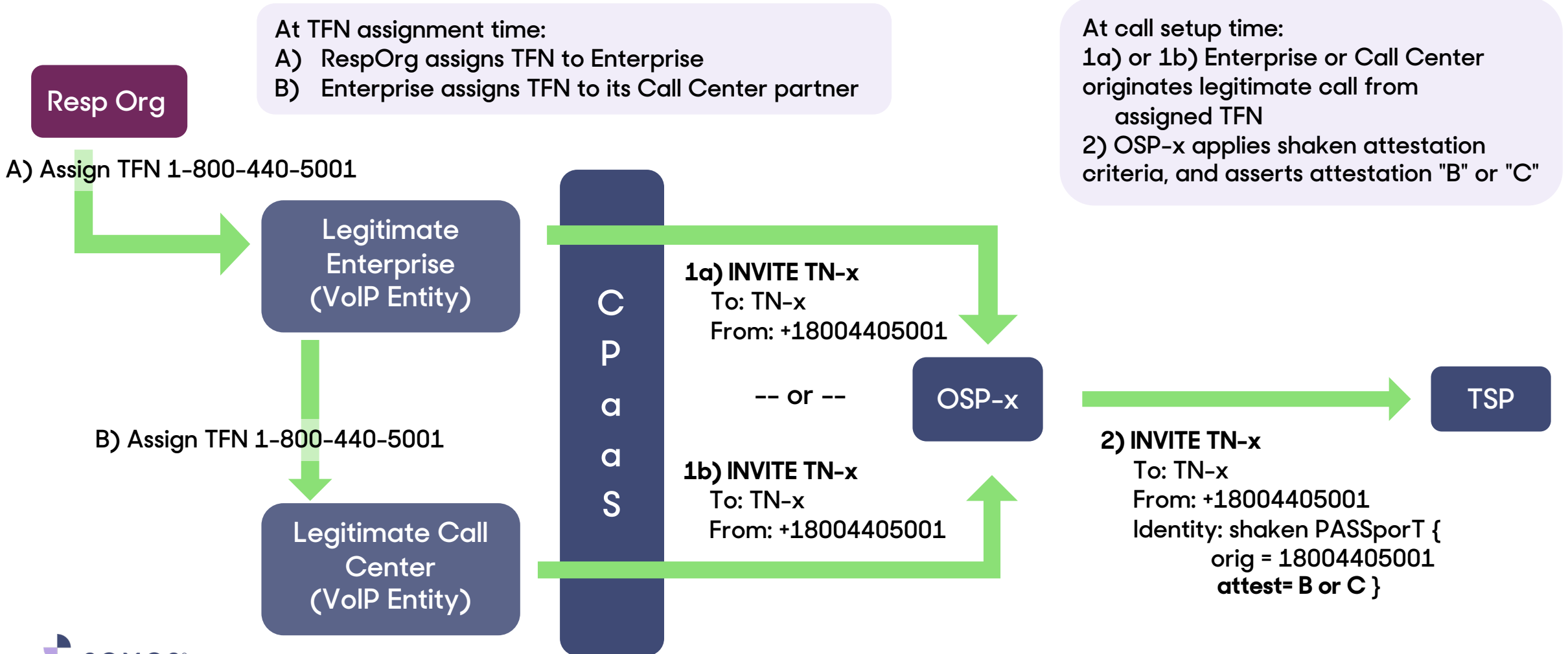
SHAKEN "A" Attestation Criteria from ATIS-1000074	Status
Is responsible for the origination of call onto the voice network	yes
Has a direct authenticated relationship with the customer	no
Has established a verified association with the calling TN	no



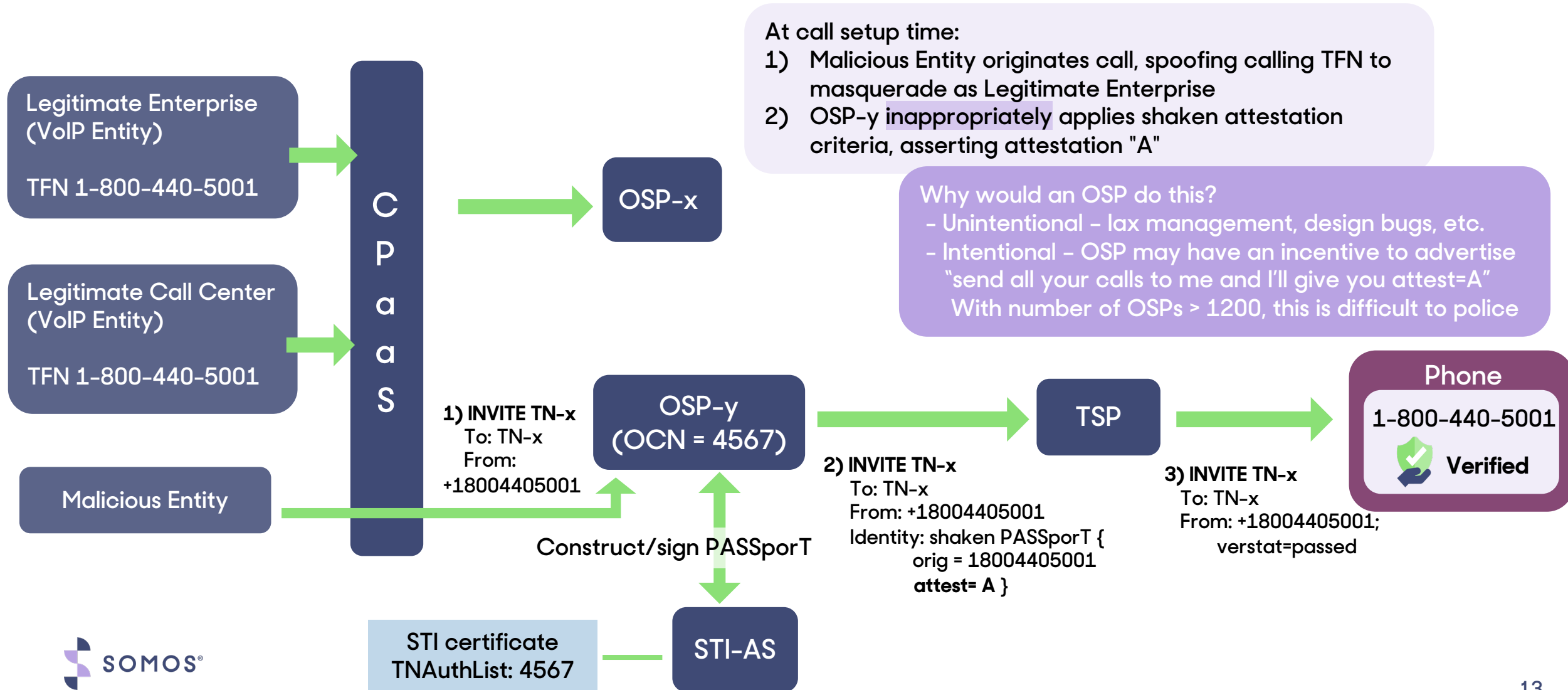
Result:

OSP asserts attest = B or C, even though these could be legit calls that deserve an attest=A

Example of a "Challenging" (for SHAKEN) Call Scenario



Worse Yet – Sometimes the OSP Guesses, and Guesses Wrong

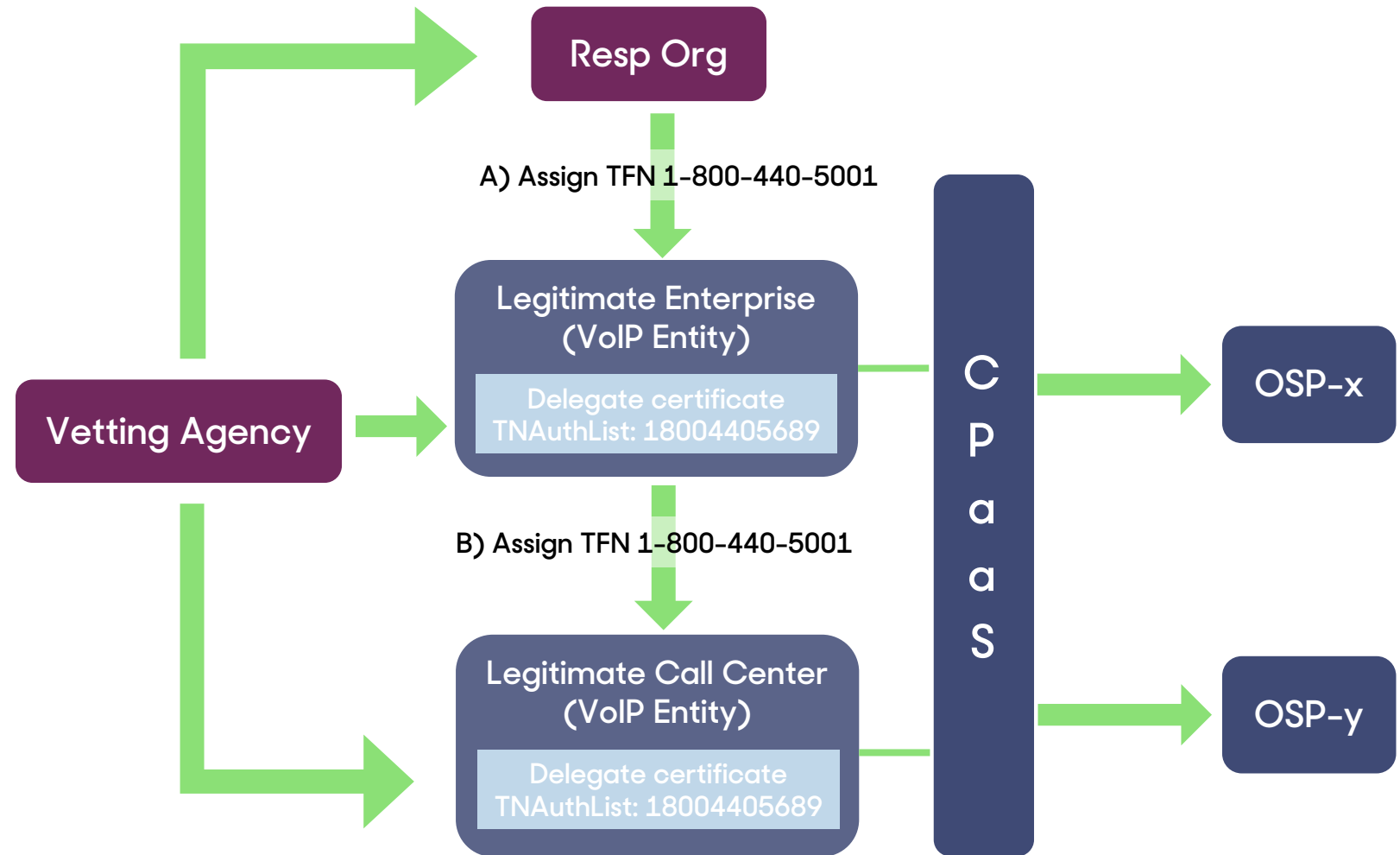


Solution: Vetting Agency Issues Delegate Certificates to VoIP Entities

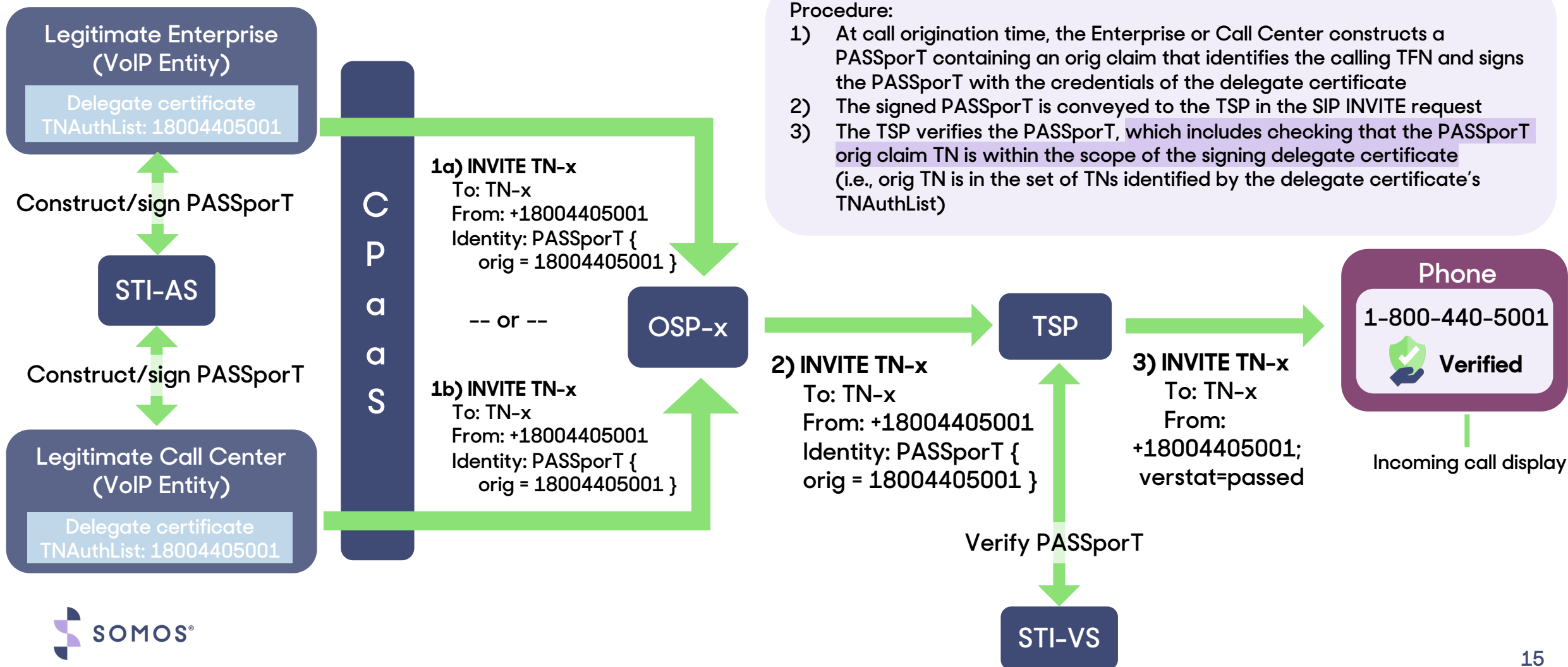
Vetting Agency interacts with Resp Org, Enterprise and Call Center to verify that:

- All three are legitimate and reputable entities
- The Resp Org has authority over the TFN and has assigned the TFN to the Enterprise, who has in turn assigned the TFN to the Call Center

Once verified, the Vetting Agency issues a delegate certificate to the Enterprise and to the Call Center that gives them the authority to sign PASSporTs for the assigned TFN



Using Delegate Certificates During Call Setup



Welcome Panelists!



Glenn Richards

Communications Practice
Group Leader



Chris Shipley

Executive Director,
Public Policy



Heather Barrows

VP, Operations

Questions?

Have additional
questions regarding
today's webinar?

Contact a Somos team
member today:

connect@somos.com



SOMOS®