

A Resp Orgs Role in SHAKEN: What You Need to Know

October 2021

CONFIDENTIAL & PROPRIETARY INFORMATION OF SOMOS, INC.
The information contained in this document is confidential and proprietary to Somos, Inc. and is intended for the express use of the intended recipients. Any unauthorized release of this information is prohibited and punishable by law.
Somos, Somos and Design, 4 Quarters Design, SMS/800, RouteLink, SMS800 TFN Registry Design, TSS Registry Design, TFN Identity Design and RealNumber Design are trademarks of Somos.
Copyright © 2021 Somos, Inc. All rights reserved.
CONFIDENTIAL

Your Presenter



MICHAEL FAIN

Senior System Engineer

Somos



Agenda

- SHAKEN Overview
- SHAKEN Governance
- Registering a Resp Org
- Obtaining an SPC Token
- Resp Org Certificate Acquisition
- Using a Delegate Certificate
- References

SOMOS®

What is SHAKEN?

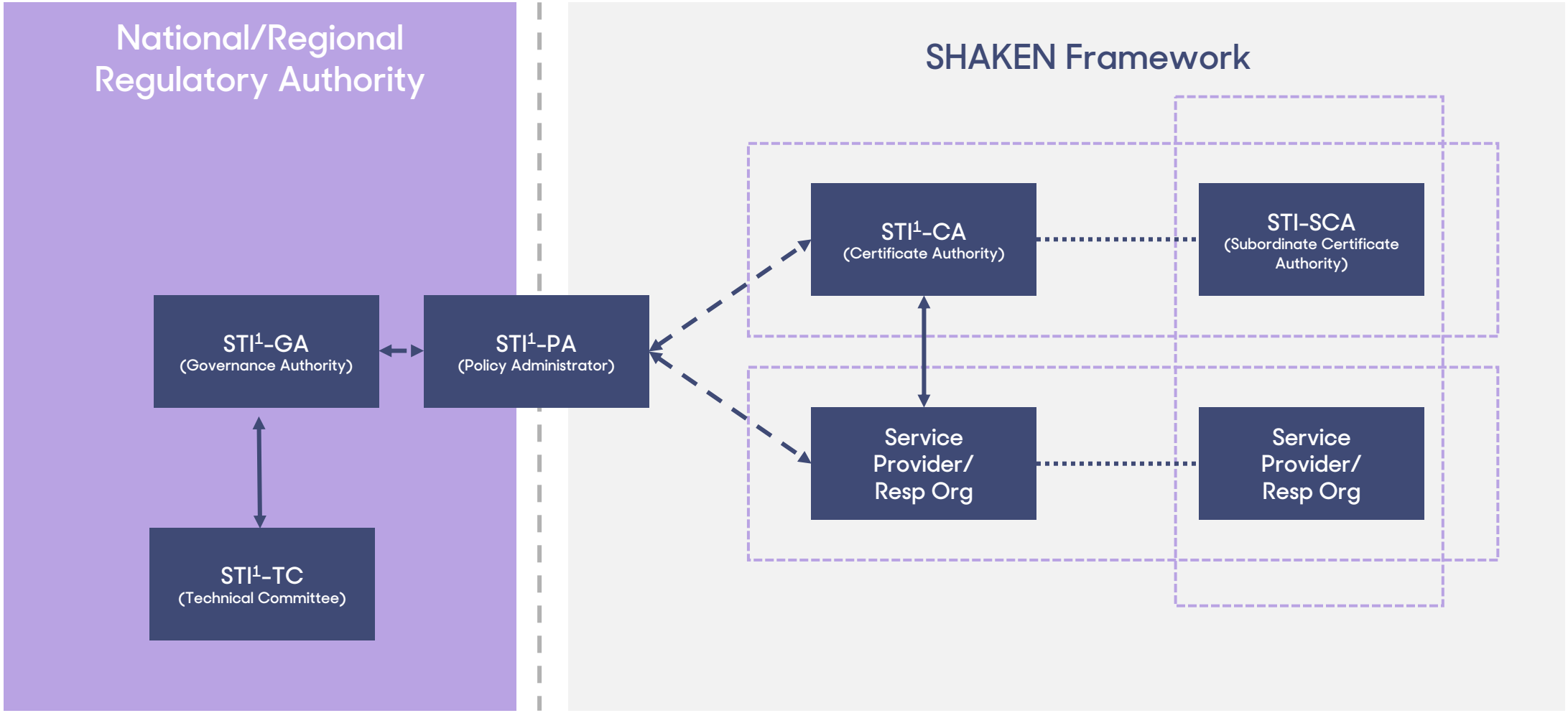
Spoofed robocalls have undermined the trust in the PSTN. Industry technical experts developed the SHAKEN Framework to reignite trust in the calls across the PSTN.

STIR/SHAKEN is built on verifiable Trust

- STIR is Secure Telephony Identity revisitied
- The FCC entrusted the Secure Telephone Identity Governance Authority (STI-GA) to set the governance rules
- The STI-GA trusts the Secure Telephone Identity Policy Administrator (STI-PA) to onboard Certificate Authorities, Service Providers and Responsible Organizations (Resp Orgs)
- The STI-PA is the trust anchor of the SHAKEN framework
- The Originating Service Providers (OSPs) set attestation levels, based on trust and information on the originating number



Governance Architecture



ATIS-1000080: Governance Model for Certificate Management

[1] *STI – Secure Telephone Identity*

SOMOS®

What is SHAKEN?

The Importance of Know Your Customer

- The key to trust is the need to implement Know Your Customer (KYC) to trust that customer's will not generate illegal robocalls
- Calls carry an indication of their attestation from the OSP to the Terminating Service Provider (TSP)
- Network call processing has added aspects such as PASSporT headers, certificates and public/private keys

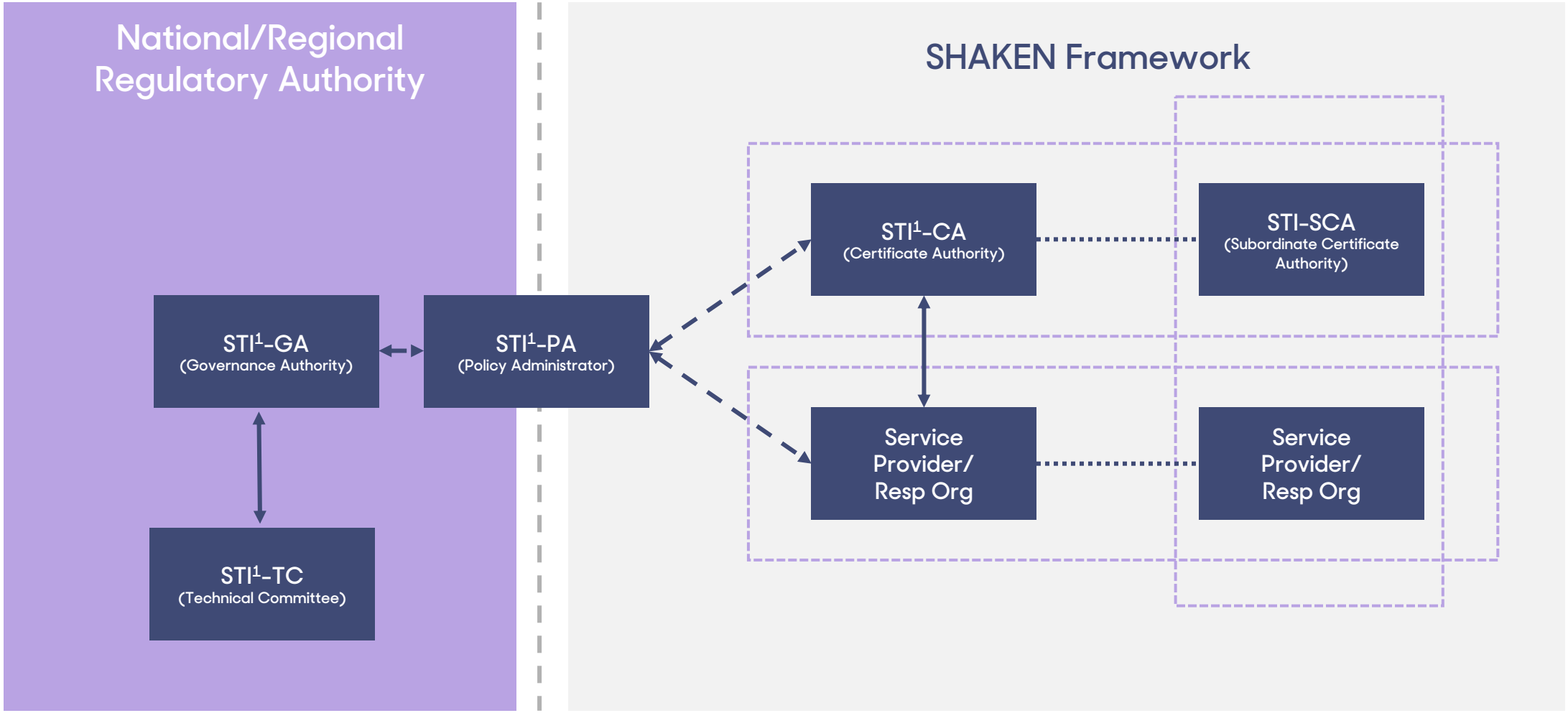


Governance

SOMOS®

* This presentation is based on information from the STI Governance Organization.

Governance Architecture

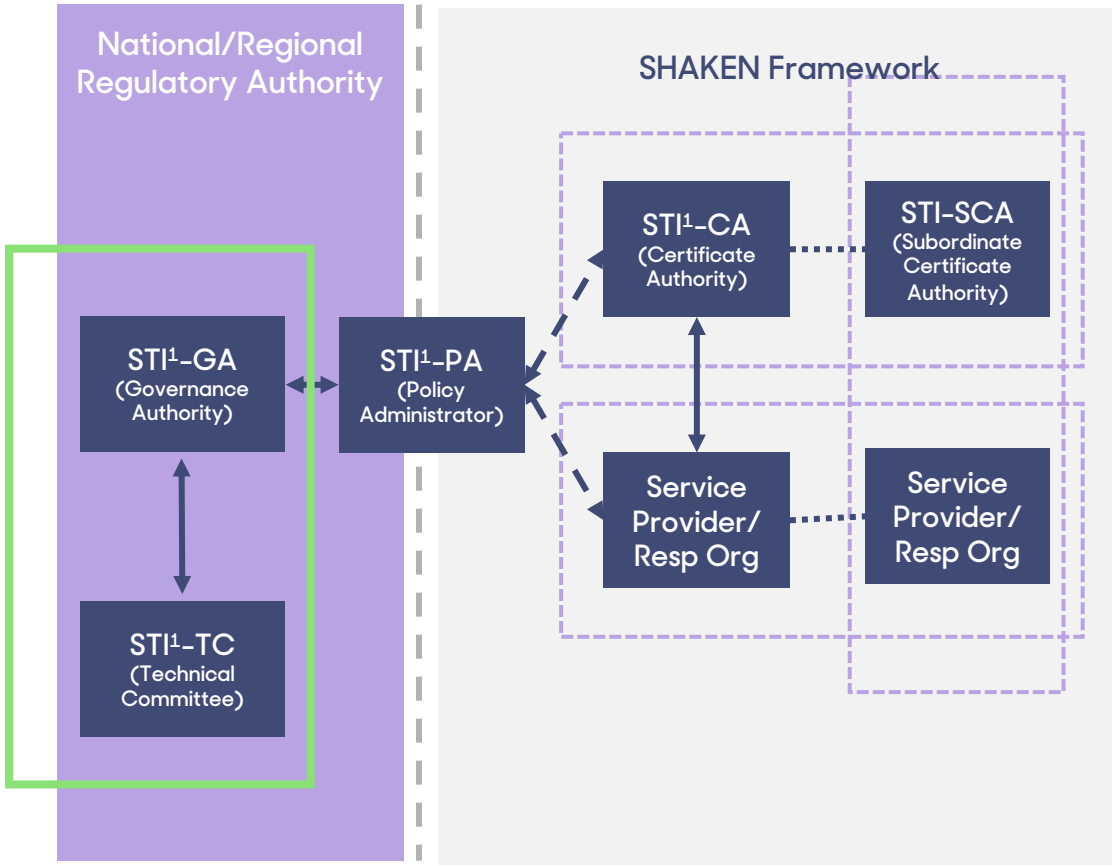


ATIS-1000080: Governance Model for Certificate Management

[1] *STI – Secure Telephone Identity*

SOMOS®

SHAKEN Governance: The STI-GA



ATIS-1000080: Governance Model for Certificate Management

[1] *STI – Secure Telephone Identity*

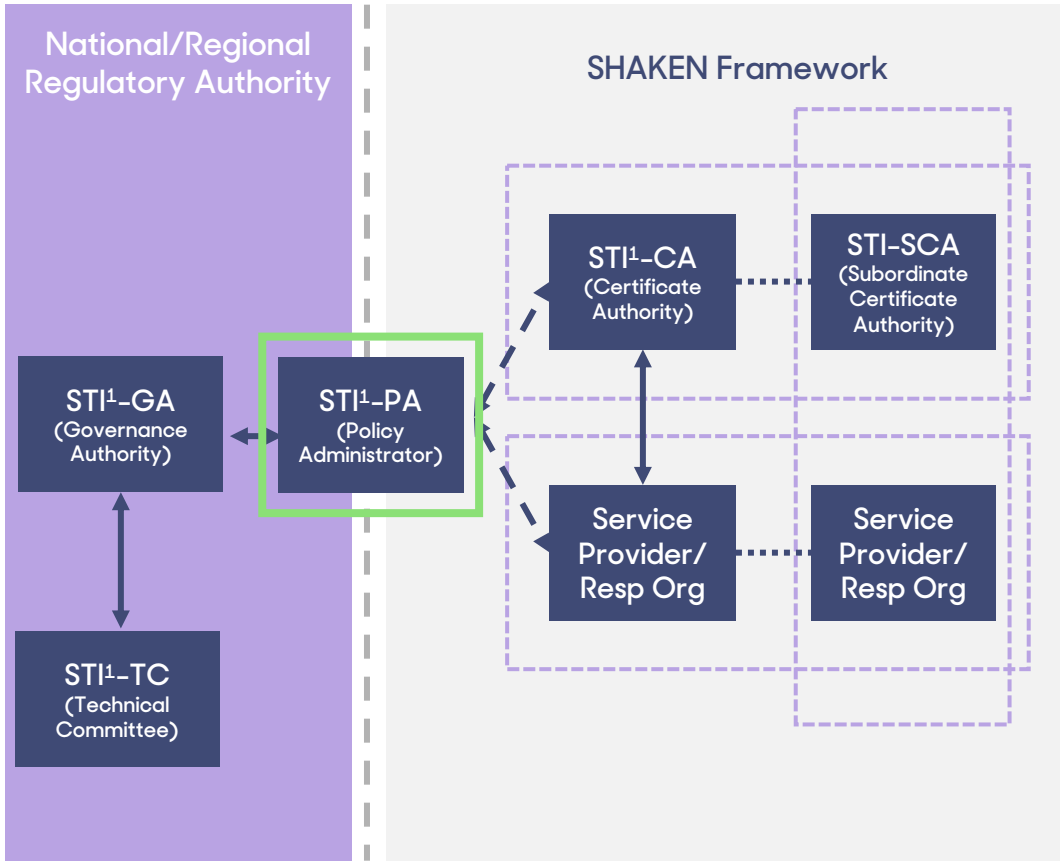
- An independent industry group based on the NANC Working Group recommendation and the FCC agreement with it
- Supported by ATIS
- Defines the policies and procedures governing the STI-PA
- Defines policies and procedures of the STI-CA's, Service Providers and TNSP/Resp Orgs

The STI-GA Technical Committee

- Reviews requests to change the STI-GA Policy
- Advises the STI-GA on technical matters

SOMOS®

SHAKEN Governance: The STI-PA



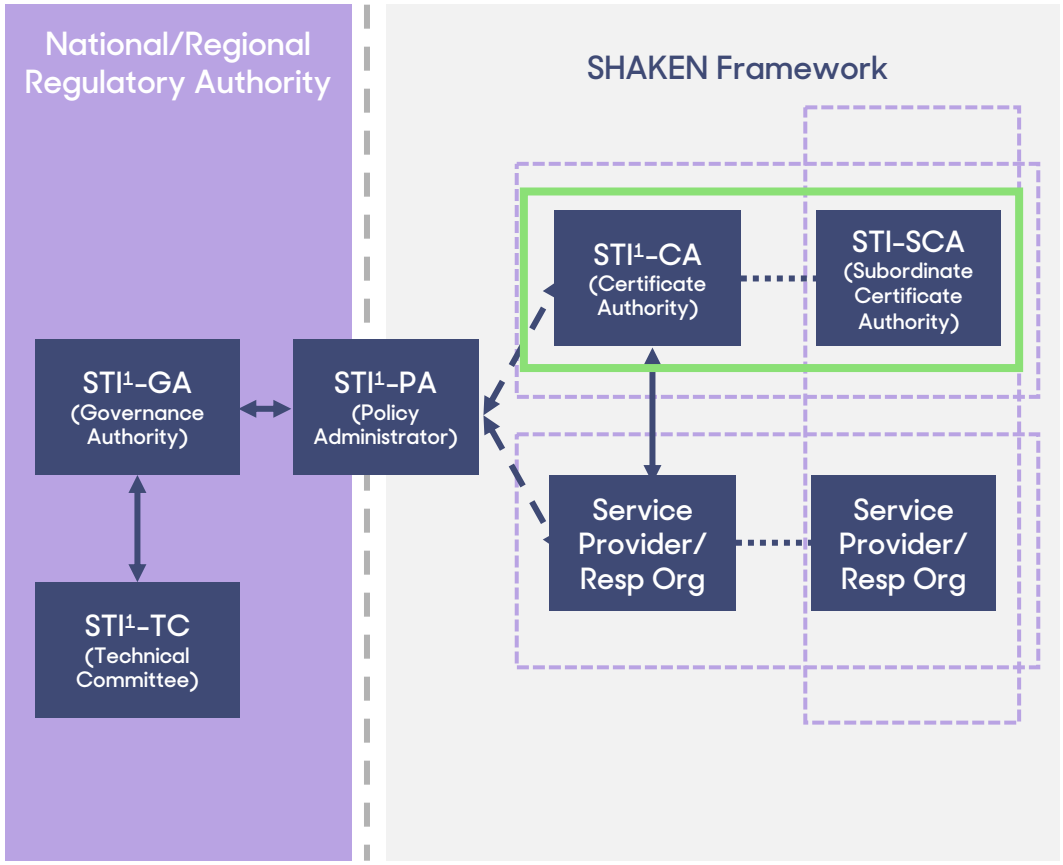
ATIS-1000080: Governance Model for Certificate Management

- A separate group under the direction and oversight of the STI-GA and iconectiv was selected to fill this role
- Authorizes/registers Certificate Authorities and maintains the STI-CA list
- Registers, administers and maintains the TNSP/Resp Org Token validation list of acquired tokens and the active list of Service Providers
- Maintains and updates the CRL (Certificate Revocation List)

[1] *STI – Secure Telephone Identity*

SOMOS®

SHAKEN Governance: The STI-CA and STI-SCA



ATIS-1000080: Governance Model for Certificate Management

[1] STI – Secure Telephone Identity

The STI-CA

- Serve as the Root/Intermediate CA for all STI Certificates
- The Root Certificates are like Public Key Infrastructure (PKI) public root certificates used by web browsers
- The Root Certificates are used in call verification, distributed to the verification service (STI-VS) of all end-entity Service Providers via STI-PA URL

The STI-SCA (Secure Telephony Identity Subordinate Certificate Authority)

- Subordinate of the Root/Intermediate CAs
- Provide CA (delegate) certificates to VoIP entities

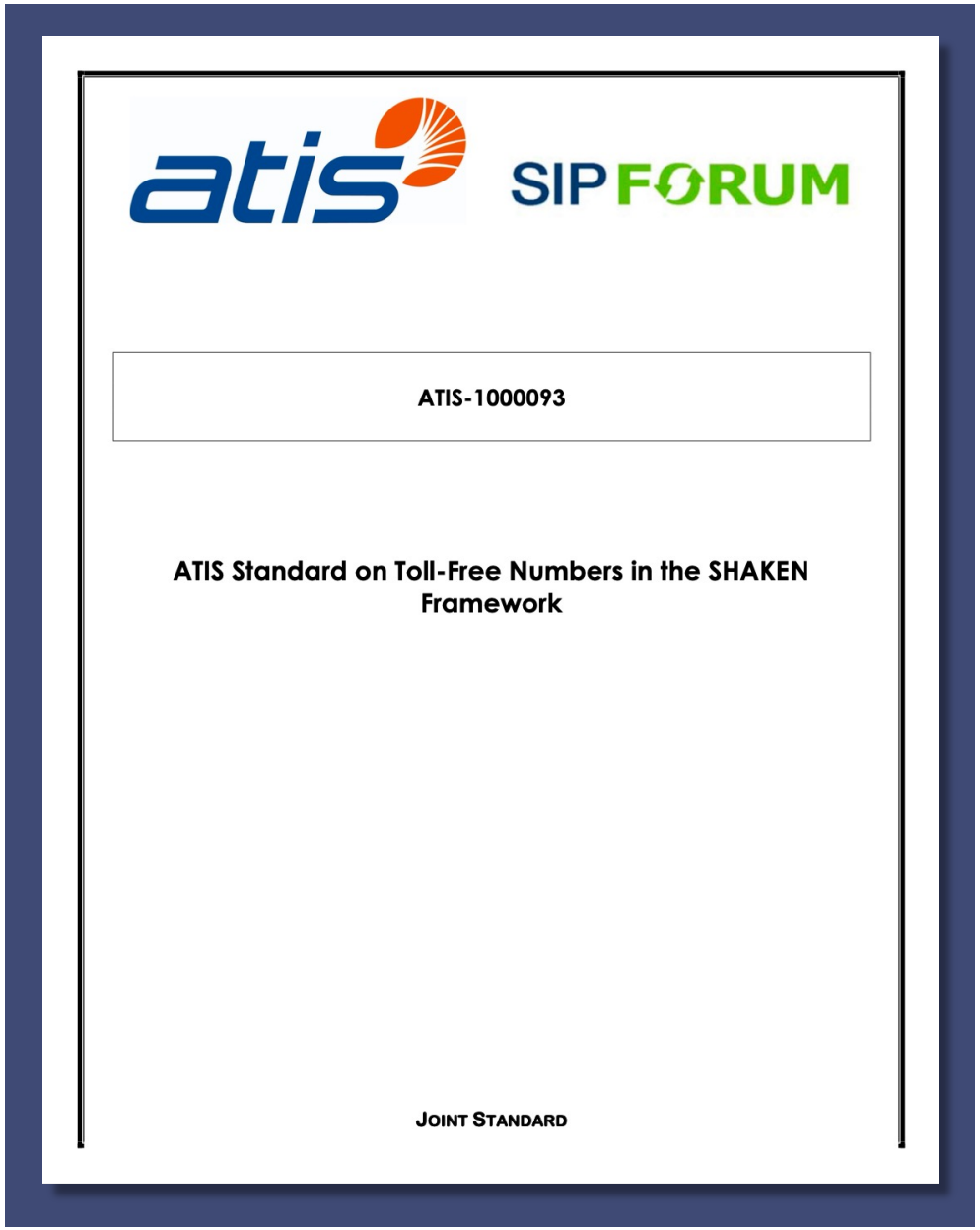
SOMOS®

Resp Org Actions

SOMOS®

Businesses rely on calls using Toll-Free Numbers (TFNs) as the calling party number and it is important to have their calls processed appropriately through the SHAKEN framework.

ATIS-1000093 was developed as the ATIS standard for using Toll-Free Numbers in the SHAKEN framework.



SOMOS®

4 Key Steps to Register a Resp Org with the STI-PA



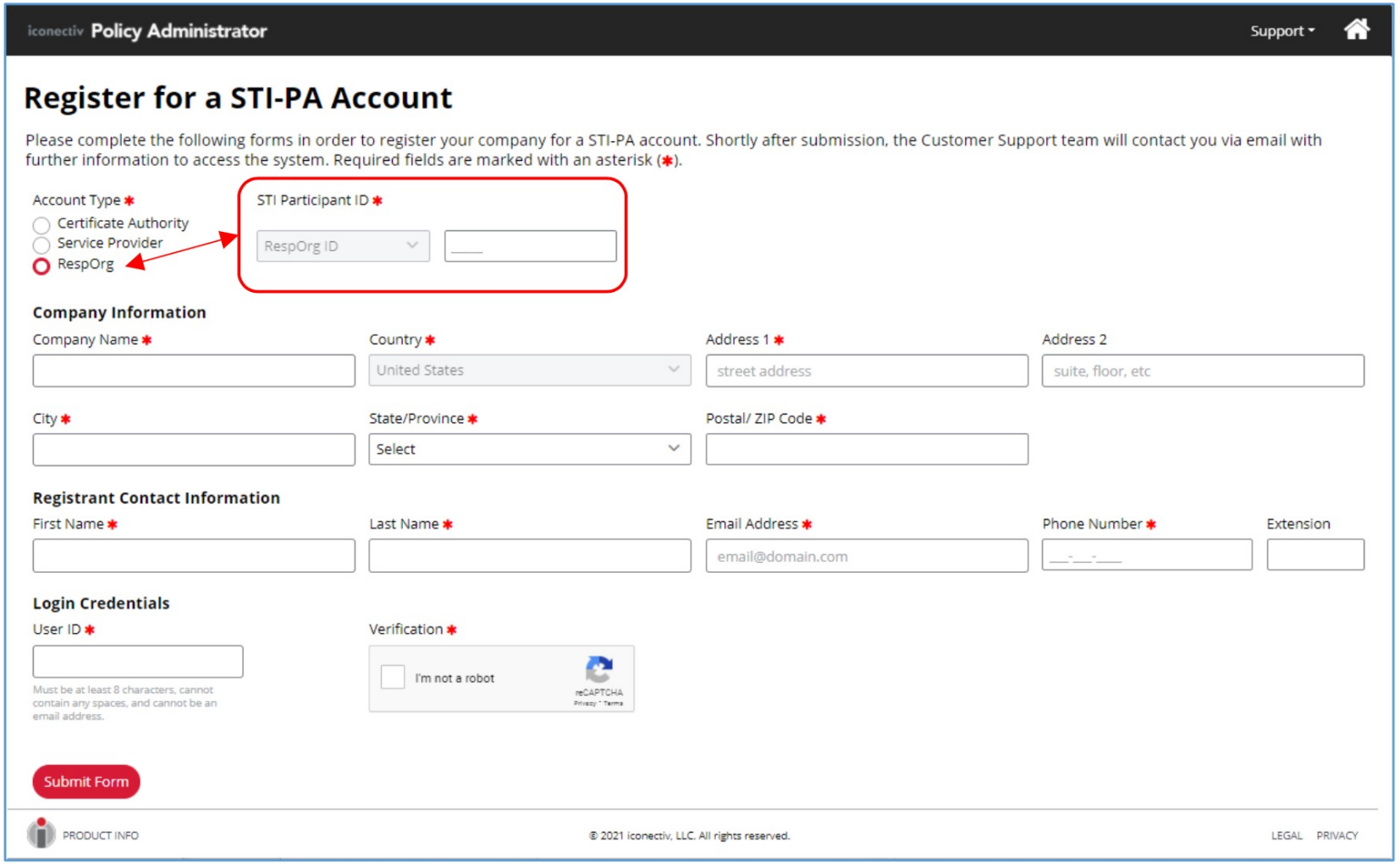
SOMOS®

1. Registration

2. Activation

3. Annual Fee

4. Tokens



- Provide basic company setup with the STI-PA (including your Resp Org ID, contact info, etc.)
- Verify company email address

1. Registration

2. Activation

3. Annual Fee

4. Tokens



Create a system User ID & Password



Review and agree to account level agreement and annual fee agreement

1. Registration

2. Activation

3. Annual Fee

4. Tokens



Current (most recent calendar year) annual Toll-Free revenue data



Funding methodology can be found in the STI-GA Policy Decision Binder

1. Registration

2. Activation

3. Annual Fee

4. Tokens



After the Resp Org completes the STI-PA steps to activate the account, additional credentials are created to obtain the SPC token using RESTful API via instructions from STI-PA.



Additional information related to SPC tokens can be found in ATIS-1000080

Resp Org Certificate Acquisition from STI-CA

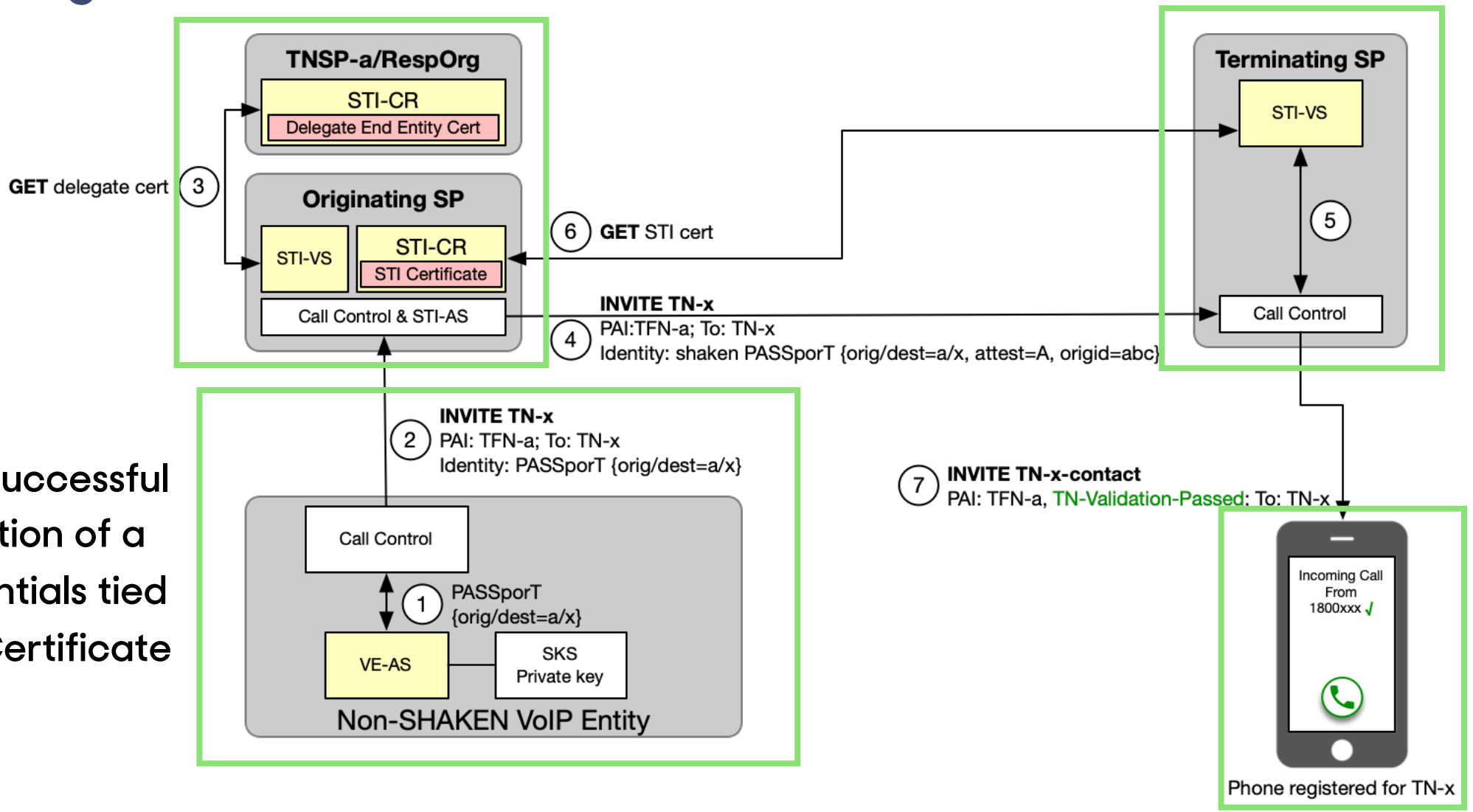
- Resp Org selects an STI-CA and creates an account to obtain certificates and follows the STI-CA implementation procedures
- Delegate certificates chain to the STI-CA root certificate
- Resp Orgs will perform the KYC for their customers and the numbers provided to their customers
- Resp Orgs may obtain any number of certificates with one token and will need to establish a delegation plan

List of Certificate Authorities (as of 10/2021)	
GBSD Technologies	Public
Metaswitch	Public
NetNumber	Public
Neustar	Public
PeeringHub	Public
Ribbon	Public
Sansay	Public
TransNexus	Public
Comcast	*Private*
T-Mobile	*Private*

SOMOS®

Using Delegate Certificate for Toll-Free Number

Overview of a successful signing/verification of a TFN with credentials tied to a Delegate Certificate



References

References
ATIS-1000074v002, Signature-based Handling of Asserted information using toKENs (SHAKEN) [1]
ATIS-1000080v003, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management [1]
ATIS-1000092, Signature-based Handling of Asserted information using toKENs (SHAKEN): Delegate Certificate [1]
ATIS-1000093, ATIS Standard on Toll-Free Numbers in the SHAKEN Framework [1]
IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [2]
IETF RFC 8224, Authenticated Identity Management in the Session Initiated Protocol [2]
IETF RFC 8225, Personal Assertion Token (PASSporT) [2]
IETF RFC 8226, Secure Telephone Identity Credentials: Certificates [2]
STI-CA list website, https://authenticate.iconectiv.com/approved-certification-authorities
STI-GA website, https://sti-ga.atis.org
STI-PA website, https://authenticate.iconectiv.com/
FCC Robocall Mitigation Database (RMD), https://fccprod.servicenowservices.com/rmd?id=rmd_welcome

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < www.atis.org >.
[2] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

SOMOS®

The System is Now Available!

Get Started Today!

Access the system by navigating to the Policy Administrator website:

https://authenticate.iconectiv.com/

Have questions?
Email us at: SHAKEN@somos.com

Reignite Trust

Acronyms and Abbreviations

Acronyms and Abbreviations	
ATIS	Alliance for Telecommunications Industry Solutions
CATA WG	Call Authentication Trust Anchor Working Group
CP	Certificate Policy
CRL	Certificate Revocation List
KMS	Key Management Server
KYC	Know Your Customer
NANC	North American Numbering Council
OSP	Originating Service Provider
PASSporT	Personal Assertion Token
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
Resp Org	Responsible Organization
SHAKEN	Signature-based Handling of Asserted information using toKENs
SKS	Secure Key Store
SP	Service Provider
SPC	Service Provider Code

Acronyms and Abbreviations	
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-GA	Secure Telephone Identity Governance Authority
STI-PA	Secure Telephone Identity Policy Administrator
STI-SCA	Secure Telephone Identity Subordinate Certification Authority
STI-TC	Secure Telephone Identity Technical Committee
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TFN	Toll-Free Number
TNSP	Telephone Number Service Provider
TSP	Terminating Service Provider
URL	Uniform Resource Locator
VE-AS	VoIP Entity Authentication Service

SOMOS®