Overview of the STIR / SHAKEN Framework and Current IPNNI Task Force Milestones

7-19-2021

Martin Dolly
Lead Member of Technical Staff
Core Network & Gov't/Regulatory Standards
ATIS – SIP Forum Co-Chair, STI-GC TC Chair,
and Director, SIP Forum
md3135@att.com

Spoofed Calls Versus Robo-Call

- **Spoofed calls**

The *Truth in Caller ID Act* prohibits spoofing, or deliberately falsifying the telephone number (TN) and/or name relayed as the caller ID information to disguise the identity of the caller ***for harmful or fraudulent purposes***. However, the law only applies to callers within the United States.

- **Robo-Calling**

A robocall is a phone call that uses a computerized autodialer to deliver a pre-recorded message, as if from a robot. Robocalls are often associated with political and telemarketing phone campaigns, but can also be used for public-service or emergency announcements.

In the Beginning & Now

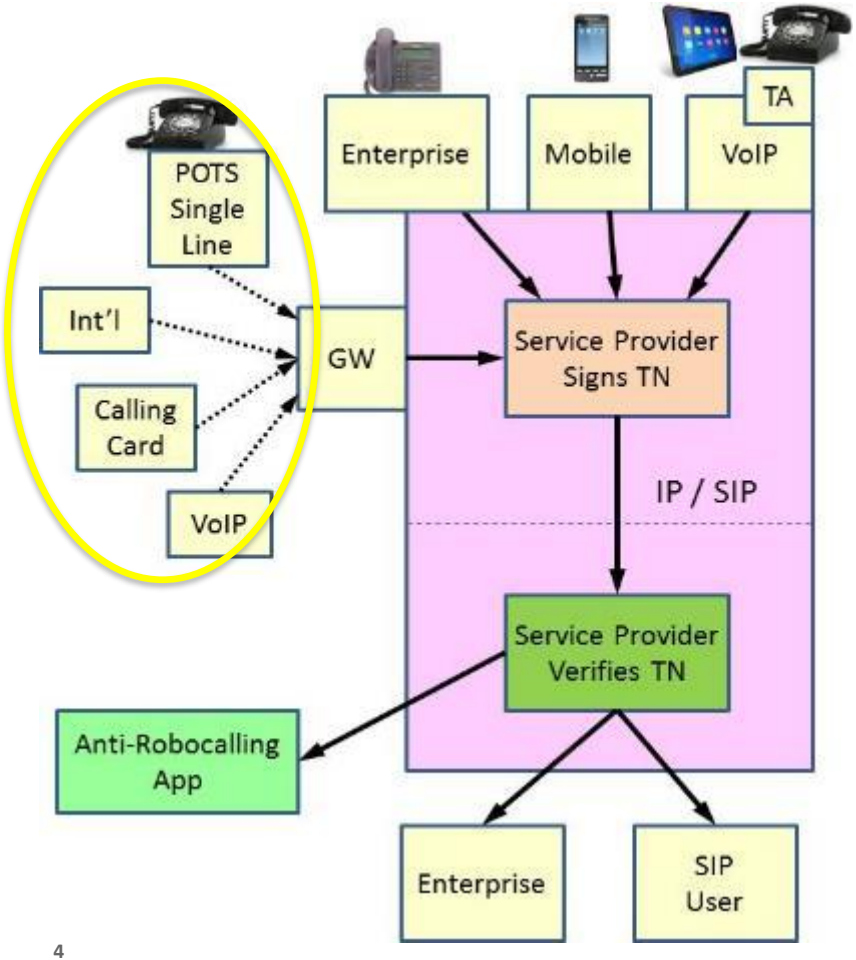
Then

- Robocalls & Spoofing is the #1 complaint to the FCC and FTC.
- Robocalls & Spoofing is the #1 complaint to the CRTC in Canada, and OFCOM in the UK
- There have been 6-8 different bills in Congress looking at this. Hearings you name it.
- The PSTN is undergoing a radical transition
- Existing PSTN Class 5 TDM/SS7 equipment is at or near End of Life [EOL] and cannot be modified.
- March 2020, FCC requires the implementation of Caller ID Authentication, such as STIR/SHAKEN
- December 2019, TRACE ACT into law
- July 2020, FCC approves new safe harbor rules to encourage blocking
- October 2020, FCC adopts new rules to combat spoofed robocalls
- I3 Forum: STIR/SHAKEN is considered the most favorable long-term approach because it has the least impact on the business and activities of the wholesale carriers and IPX providers http://i3forum.org/blog/2020/11/04/i3forum-calling-line-identification-cli-spoofing-report/

Now

- 331 SPs (up from 64, 12/20) eligible to get certificates with dozens of registrations in progress
- 9 STI-CAs {7 public and 2 private (T-Mobile and Comcast)
- ATIS STI-GA in talks with Canadian counterpart

Basic STIR/SHAKEN Limitations



- STIR can be used to validate SIP calls in real-time or to trace calls after the fact.
- GW may sign its identity for traceability purposes, without verifying calling number.
- Calls from outside USA SIP networks cannot be verified.
  - Domestic SIP only
- No support for TDM

STIR/SHAKEN Enhancements

- SHAKEN support of “div” PASSport for call redirection
- TN Registry (“Registered Caller”) for subscriber vetting, and Enterprise and Tollfree validation
- Delegated Certificates (DC) for Enterprise validation
- Toll-Free Calls in the SHAKEN Framework using DC
- SIP RPH Signing using PASSPorT Tokens (for GETS/WPS)
- SIP RPH and Priority Header Signing in Support of Emergency Calling
- Enhanced User Display (eCNAM, RCDa, RCDb, RCDc)
- Out-of-Band
- Distributed Ledger Technology
- In development:
  - Use of ISUP CPC interworking
  - Lemon Twist

STIR/SHAKEN ECOSYSTEM

Factors

- International is coming. Global standards and Governance.
- Bar for getting a CA token is lowering
- STIR/SHAKEN Enhancements
  - Delegated Certificates
  - Enhanced User Display (eCNAM, RCDa, RCDb, RCDc)
  - Tollfree
  - Out-of-Band
  - Distributed Ledger Technology

The PASSporT “shaken” extension

The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (”origid”) as described in section 5.2.4. The SHAKEN PASSporT token would have the form given in the example below:

Protected Header


```
{
        "alg":"ES256",
        "typ":"passport",
        "ppt":"shaken",
        "x5u":"https://cert.example.org/passport.cert"
}
```

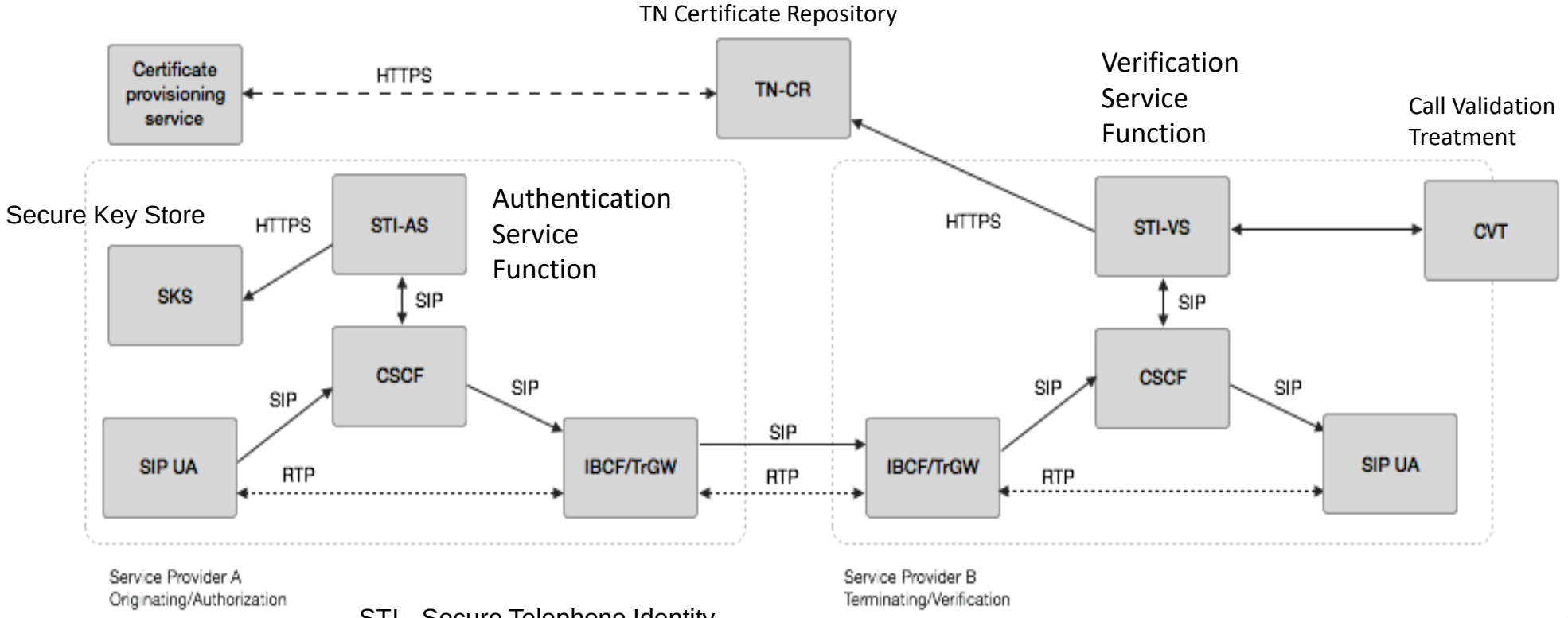

Payload


```
{
        "attest":"A",
        "dest":{"tn":["12125551213 "]},
        "iat":1443208345,
        "orig":{"tn":"12155551212"},
        "origid":"123e4567-e89b-12d3-a456-426655440000"
```


In addition to attestation, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122). The origid will identify:

- Signing Carrier or 3rd party
- Carrier Customer/Access Carrier
- Entry Gateway

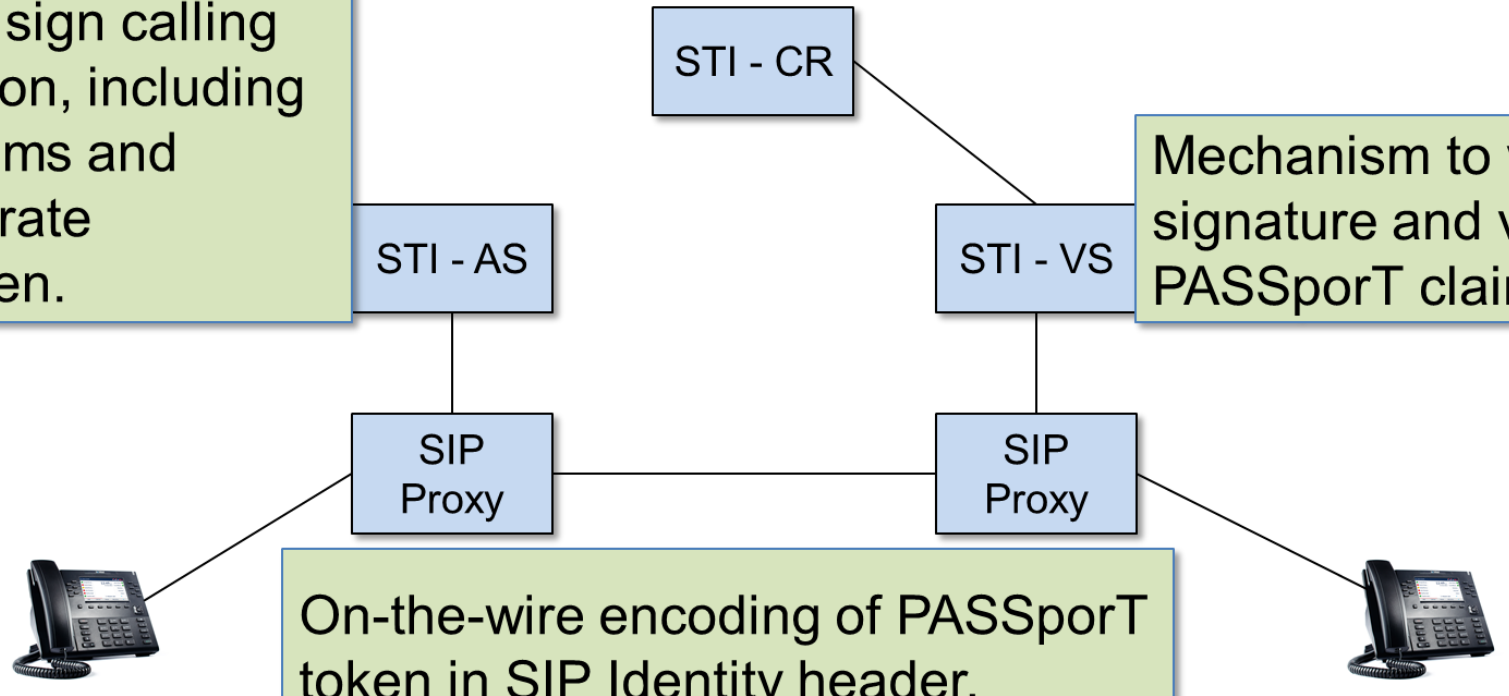
SHAKEN reference architecture (Illustrative IMS based deployment)



STI - Secure Telephone Identity

Phase 1: ATIS-100074 SHAKEN Specification

Mechanism to sign calling party information, including attestation claims and origid, to generate PASSporT token.

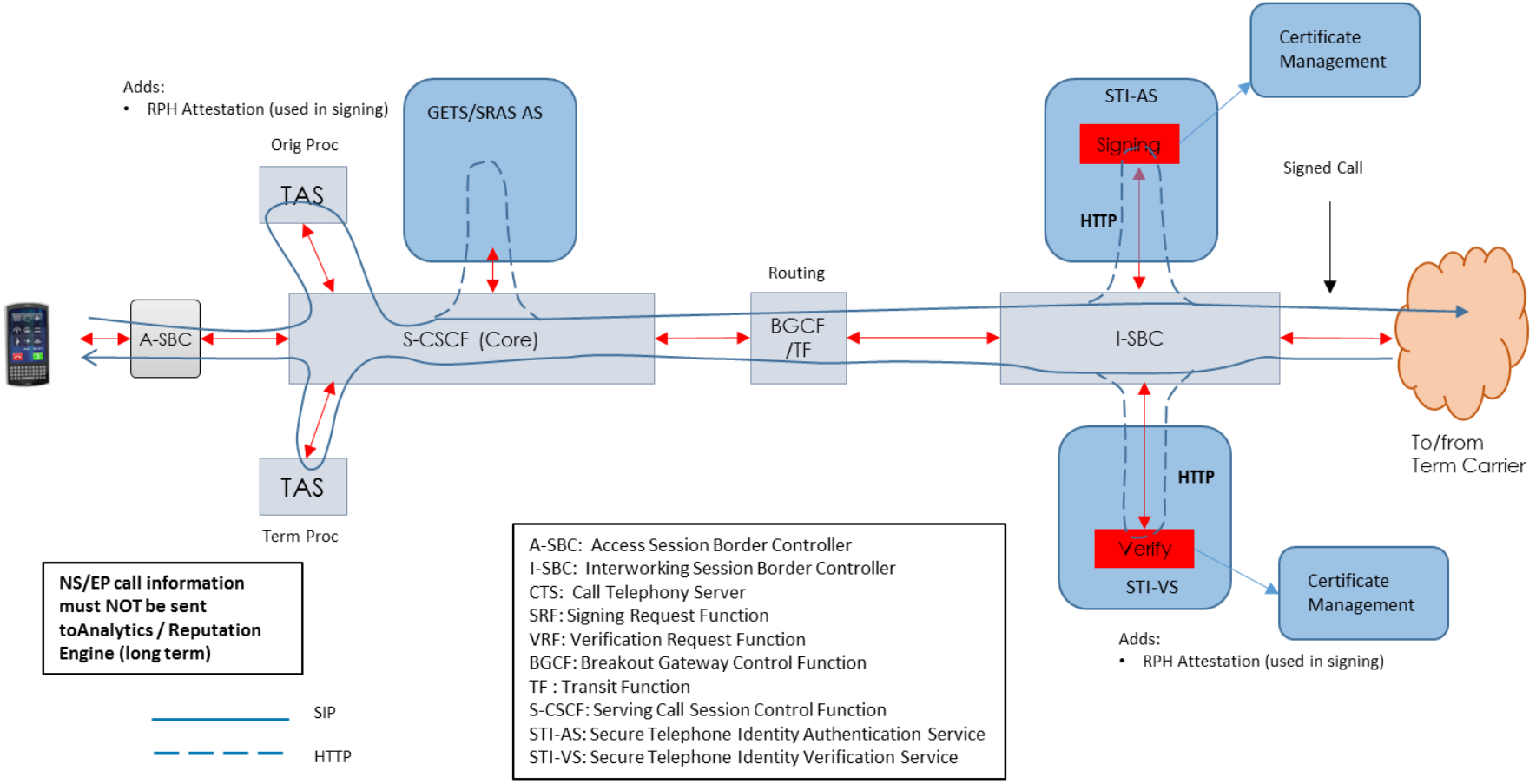


Mechanism to verify signature and validate PASSporT claims.

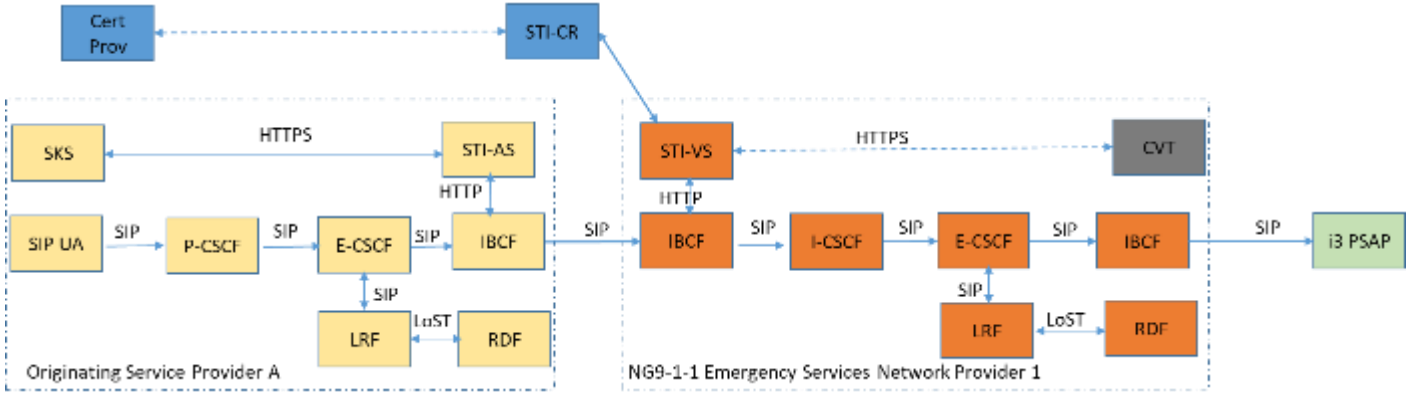
On-the-wire encoding of PASSporT token in SIP Identity header.

ATIS-1000074: Signature based Handling of Asserted information using ToKENs (i.e., SHAKEN)

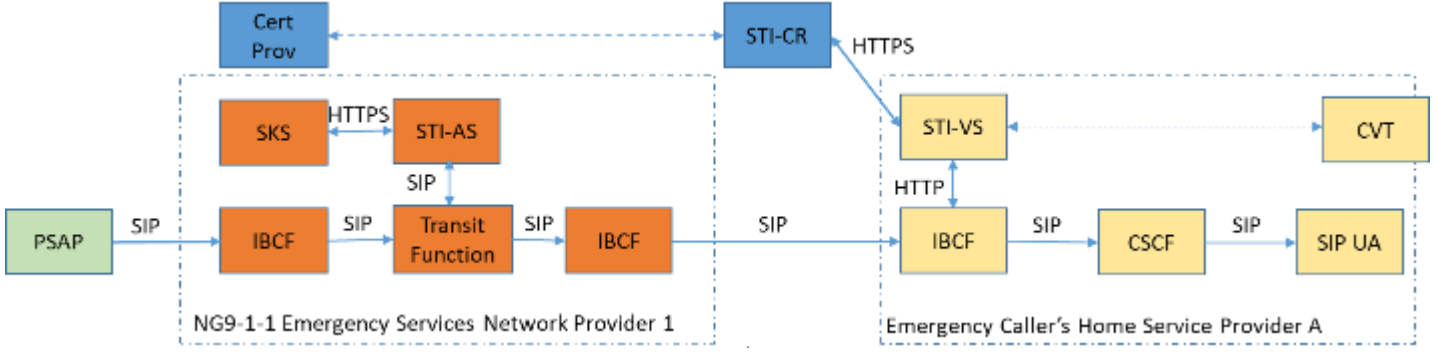
Inter-Network SHAKEN Flows (RPH)



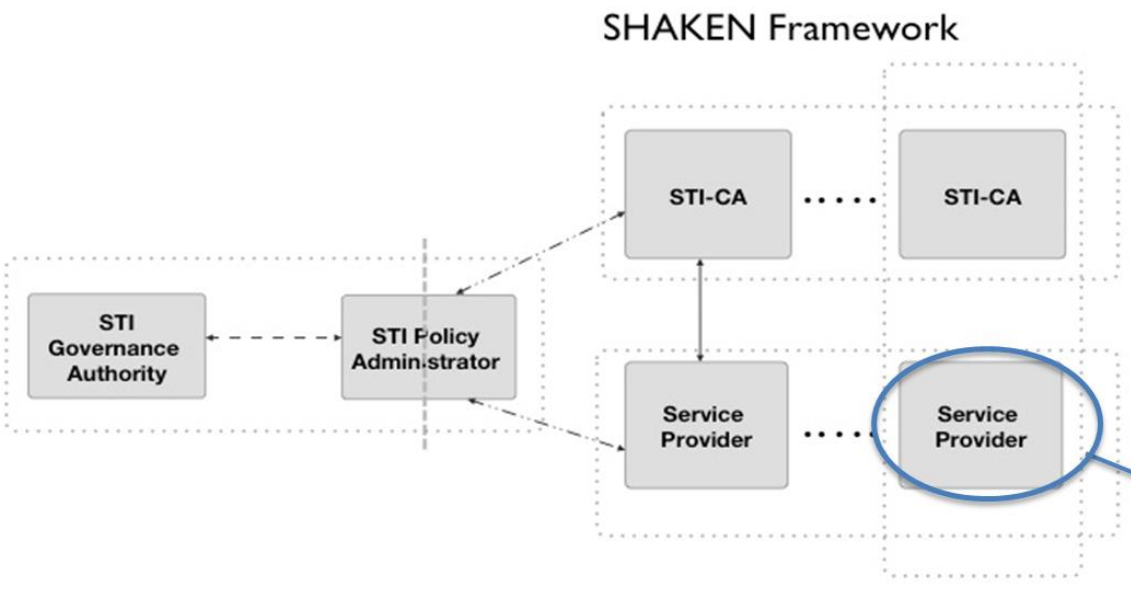
Architecture for Signing SIP RPH of Emergency Originations



Architecture for Signing SIP RPH of Callback Calls

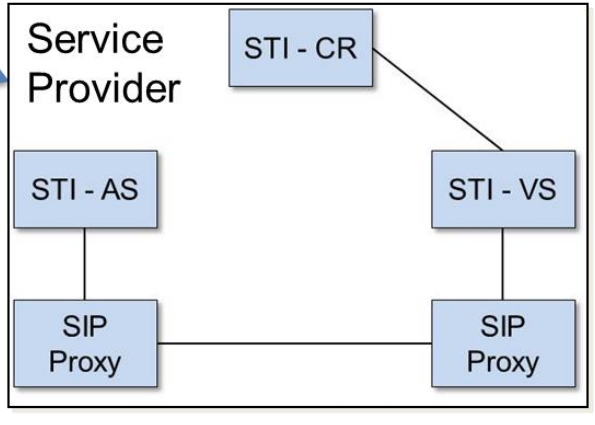


Phase 2: ATIS-1000080 SHAKEN Governance Model



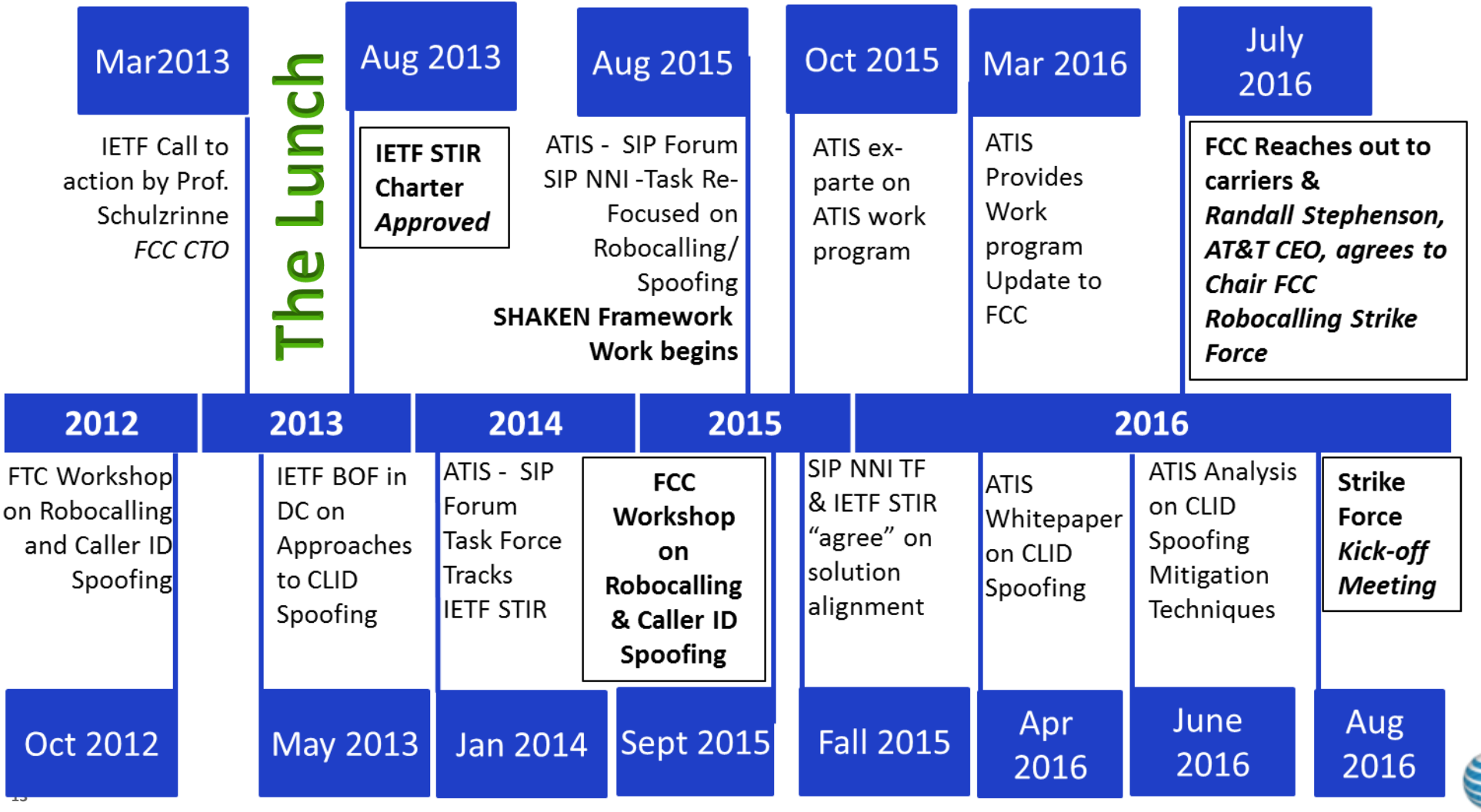
SHAKEN Governance Model and Certificate Management defines mechanism for service provider to obtain SHAKEN STI Certificates:

- Roles
- Protocols

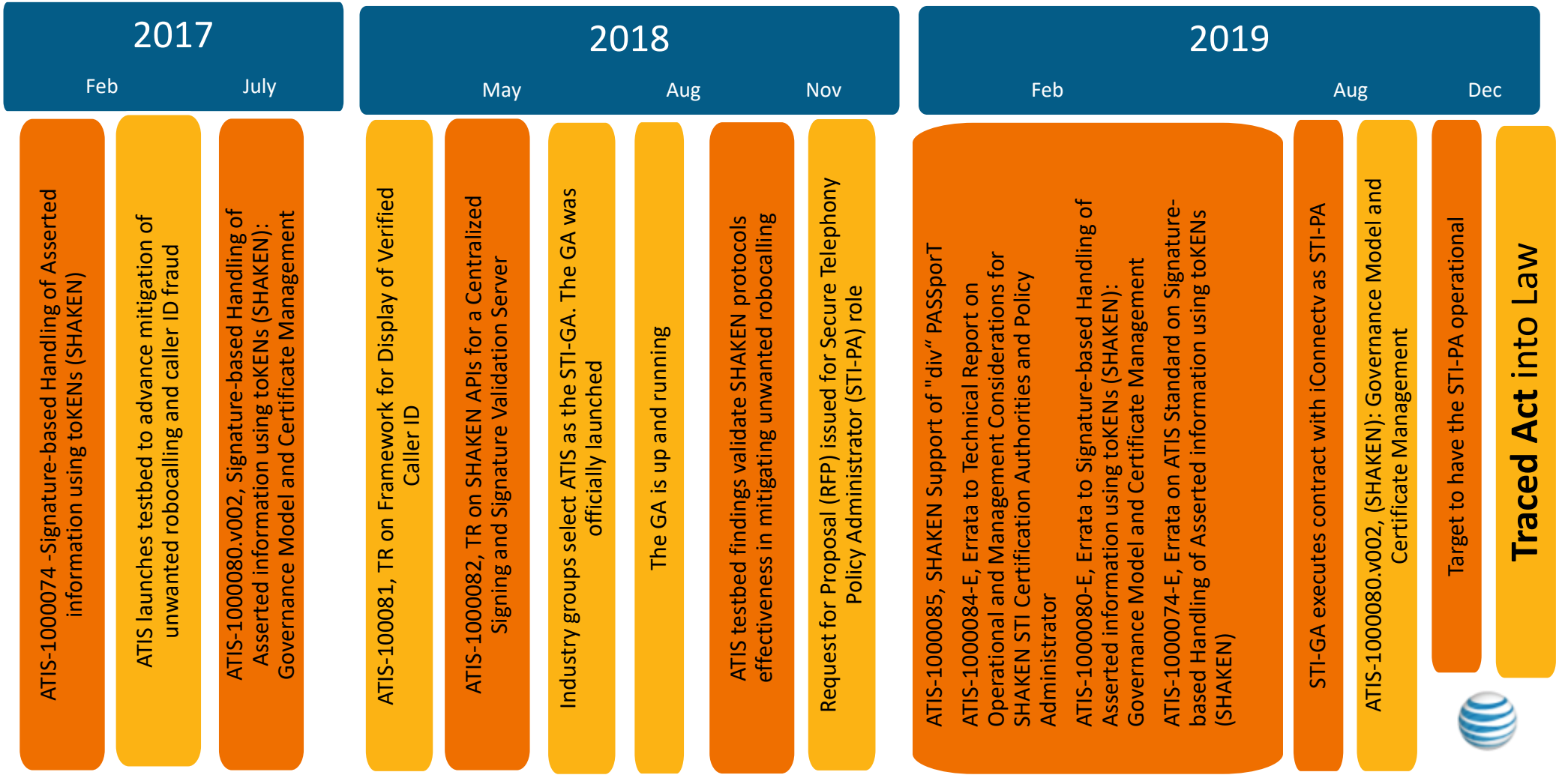


ATIS-1000080: SHAKEN: Governance Model and Certificate Management

Robocalling/ Spoofing Timeline (1-2)



Robocalling/ Spoofing Timeline (2-2)



2020: What a Year it Was…..

- **Letter Resolution and Publication of:**
  - ATIS-1000092 Signature-based Handling of Asserted information using toKENs (SHAKEN): Delegate Certificates.
  - ATIS-1000085.v002, Signature-based handling of Asserted information using toKENs (SHAKEN): SHAKEN Support of “div” PASSporT.
  - ATIS-1000080.v003, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management.
  - ATIS-1000084.v002, Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators.
  - ATIS-1000091, Mechanism for International Signature-based handling of Asserted information using toKENs (SHAKEN).
  - ATIS-1000089, Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements.
  - ATIS-1000088, A Framework for SHAKEN Attestation and Origination Identifier.
  - ATIS-1000093, ATIS Standard on Toll-Free Numbers in the SHAKEN Framework

2021: What a Year it is and not done…

- **Letter Resolution and Publication of:**
  - ATIS -10700048, Study of SHAKEN Impacts on 9-1-1 Calls and Callback
  - Calls
  - ATIS-1000098 Session Initiation Protocol (SIP) Resource-Priority Header (RPH) and Priority Header Signing in Support of Emergency Calling
  - ATIS-1000074.v002, Signature-based handling of Asserted information using
  - toKENs (SHAKEN)
  - ATIS-1000089v002, Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements.

ATIS/SIP Forum IP-NNI TF Issue Tracker can be found at :

https://access.atis.org/apps/org/workgroup/ipnni/download.php/57644/

NIPCA: OOB and CPC Interworking

STIR & SHAKEN Work Program

IETF

- ***RFC 8224, Authenticated Identity Management in the Session Initiation Protocol (SIP)***
- ***RFC 8225, PASSporT: Personal Assertion Token***
- **RFC 8226, Secure Telephone Identity Credentials: Certificates**
- **RFC 8443, Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization**
- ***PASSporT SHAKEN Extension (SHAKEN)***
- **PASSporT Extension for Diverted Calls**
- PASSporT Extension for Rich Call Data
- **Etc.**

IPNNI

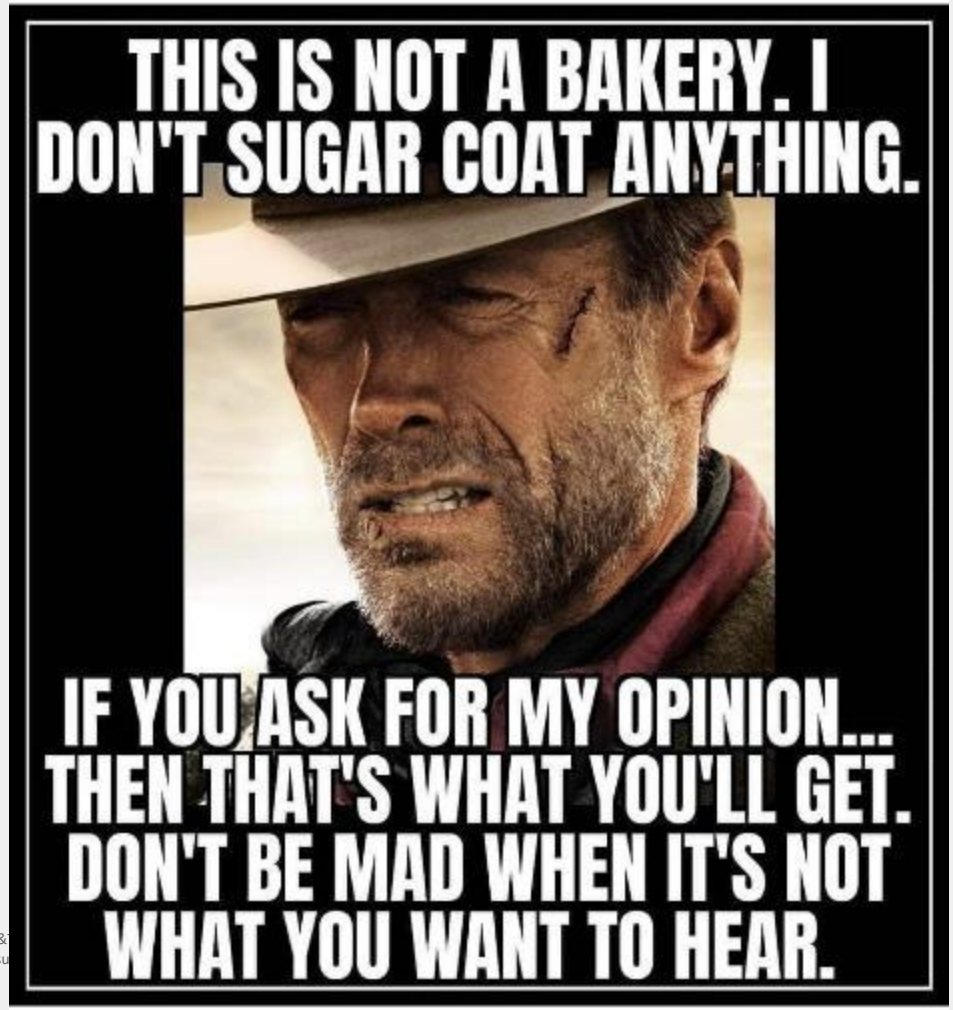
- ***ATIS-1000074E Errata on Signature-based Handling of Asserted information using toKENs (SHAKEN)***
- **ATIS-1000082.v002, SHAKEN API for a Centralized Signing and Signature Validation Server**
- **ATIS-1000080-E, Errata to Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management**
- **ATIS-1000084-E, Errata to Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators**
- ATIS-1000081, ATIS Technical Report on a Framework for Display of Verified Caller ID
- ATIS-1000085, Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): SHAKEN Support of "div" PASSporT
- Etc.

3GPP

- **3GPP TS 24.229**, Technical Specification Group Core Network and Terminals; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- **3GPP TS 29.163,** Technical Specification Group Core Network and Terminals; Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks
- **3GPP TS 29.165,** Technical Specification Group Core Network and Terminals; Inter-IMS Network to Network Interface (NNI)
- **3GPP TS 29.292,** Technical Specification Group Core network and Terminals; Interworking between the IP Multimedia (IM) Core Network (CN) Subsystem (IMS) and MSC Server for IMS Centralized Services (ICS)

PTSC Non-IP Call Authentication Task Force

Q & A



Thank you.