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

12-3-2019

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.

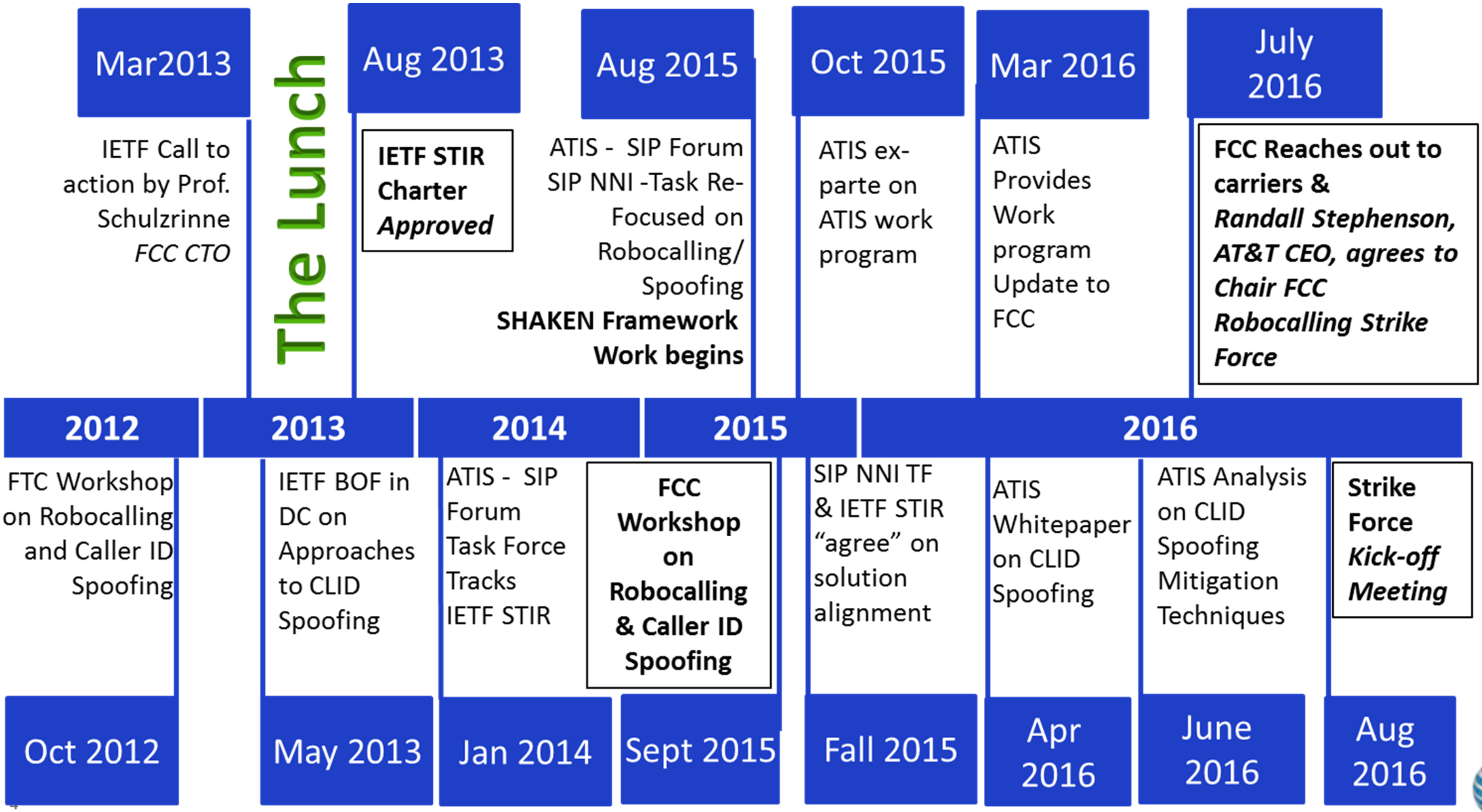
- **Robo-Calling**

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.

We know how we got here

- Robocalls & Spoofing is the #1 complaint to the FCC and FTC.
  - https://consumercomplaints.fcc.gov/hc/en-us/articles/204009760-Consumer-Complaint-Charts-and-Data-Overview
- Robocalls & Spoofing is the #1 complaint to the CRTC in Canada
- Robocalls & Spoofing is the # 1 complaint to OFCOM and the UK ICO
  - https://ico.org.uk/action-weve-taken/nuisance-calls-and-messages/
- There have been 6-8 different bills in Congress looking at this. Hearings you name it.
  - FCC FTC CRTC [CA] OFCOM [UK] have held workshops. I wrote one of the reports.
  - http://stakeholders.ofcom.org.uk/binaries/market-data-research/Ofcom_VoIP_RPKI_Report.pdf
  - US Congress had endless hearings.
  - https://energycommerce.house.gov/hearings-and-votes/hearings/modernizing-telephone-consumer-protection-act
- The PSTN is undergoing a radical transition
  - With VoLTE IP based voice will be 75% of the market in 3 years in the US.
- Existing PSTN Class 5 TDM/SS7 equipment is at or near End of Life [EOL] and cannot be modified.
- All IP Interconnection now a reality US CA EU

Robocalling/ Spoofing Timeline (1-2)



Mar2013

IETF Call to action by Prof. Schulzrinne *FCC CTO*

The Lunch

Aug 2013

IETF STIR Charter *Approved*

Aug 2015

ATIS - SIP Forum SIP NNI -Task Re-Focused on Robocalling/ Spoofing

SHAKEN Framework Work begins

Oct 2015

ATIS ex-parte on ATIS work program

Mar 2016

ATIS Provides Work program Update to FCC

July 2016

FCC Reaches out to carriers & *Randall Stephenson, AT&T CEO, agrees to Chair FCC Robocalling Strike Force*

2012 **2013** **2014** **2015** **2016**

Oct 2012

FTC Workshop on Robocalling and Caller ID Spoofing

May 2013

IETF BOF in DC on Approaches to CLID Spoofing

Jan 2014

ATIS - SIP Forum Task Force Tracks IETF STIR

Sept 2015

FCC Workshop on Robocalling & Caller ID Spoofing

Fall 2015

SIP NNI TF & IETF STIR "agree" on solution alignment

Apr 2016

ATIS Whitepaper on CLID Spoofing

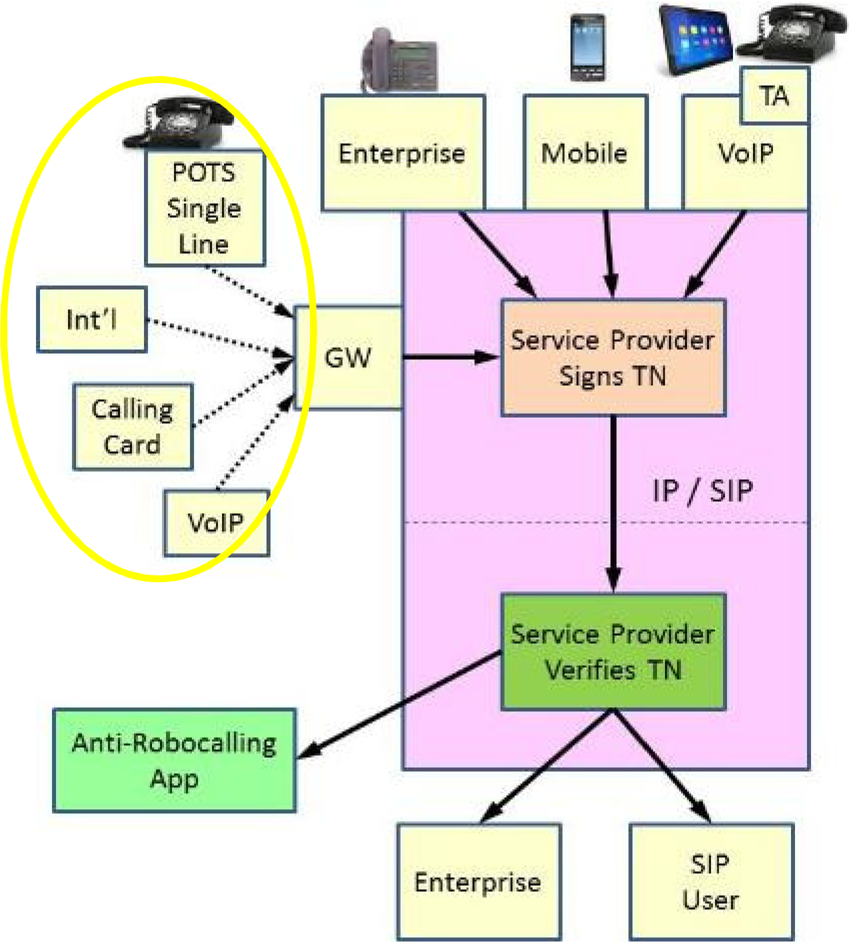
June 2016

ATIS Analysis on CLID Spoofing Mitigation Techniques

Aug 2016

Strike Force *Kick-off Meeting*

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 SIP network cannot be verified.
  - Domestic SIP only
  - No support for TDM

Certificate Attestation Policy Indication

A. **Full Attestation:** The signing provider:

- is responsible for the origination of the call onto the IP based service provider voice network
- has a direct authenticated relationship with the customer and can identify the customer
- has established a verified association with the telephone number used for the call.

Note: The legitimacy of the telephone number(s) the originator of the call can use is subject to signer specific policy

B. **Partial Attestation:** The signing provider:

- is responsible for the origination of the call onto the telephone network
- has a direct authenticated relationship with the customer and can identify the customer
- has NOT established a verified association with the telephone number being used for the call

Note: Each customer will have a unique identifier, The unique identifier also provides a reliable mechanism to identify the customer for forensic analysis or legal action where appropriate.

C. **Gateway Attestation:** The signing provider:

- is the entry point of the call onto the telephone network
- has no relationship to the initiator of the call (e.g., international gateways).

Note: The signature will provide a unique identifier of the node. (The signer is not asserting anything other than “this is the point where the call entered my network”.)

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"
}
```

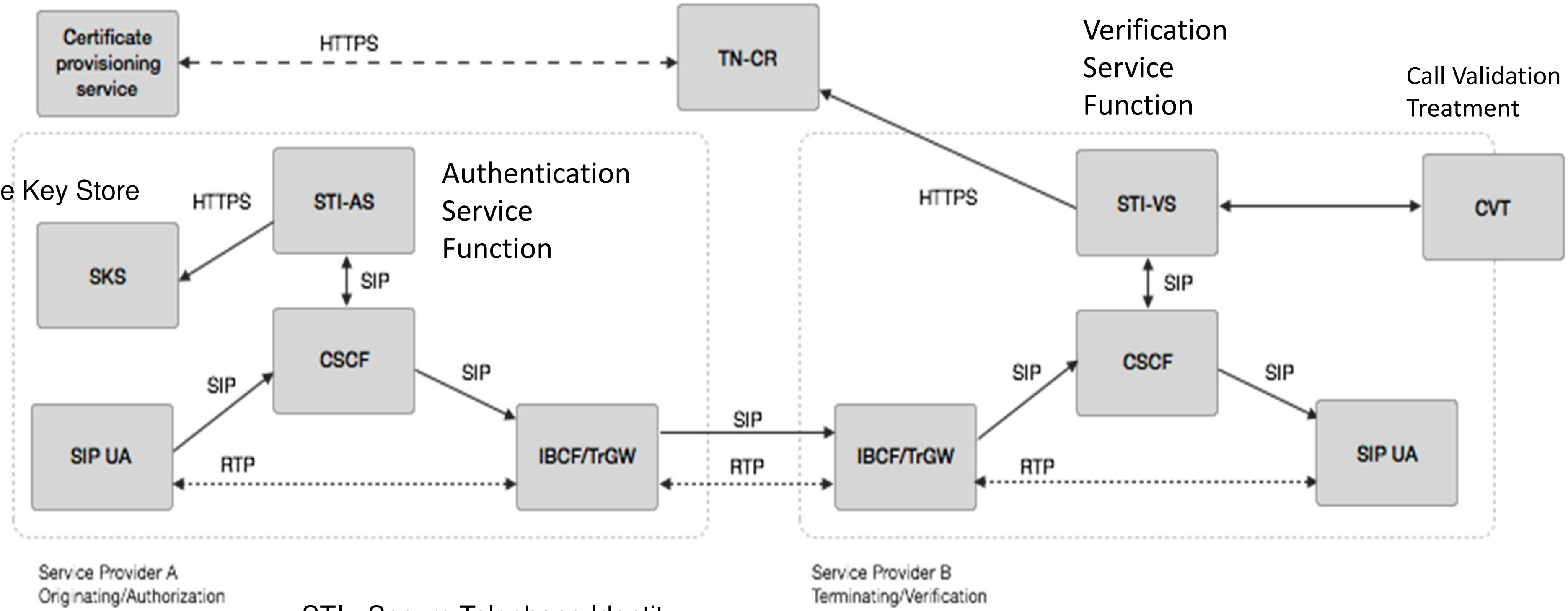
Payload

```
{
                "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
- Carrier Customer/Access Carrier
- Entry Gateway

SHAKEN reference architecture



TN Certificate Repository

Secure Key Store

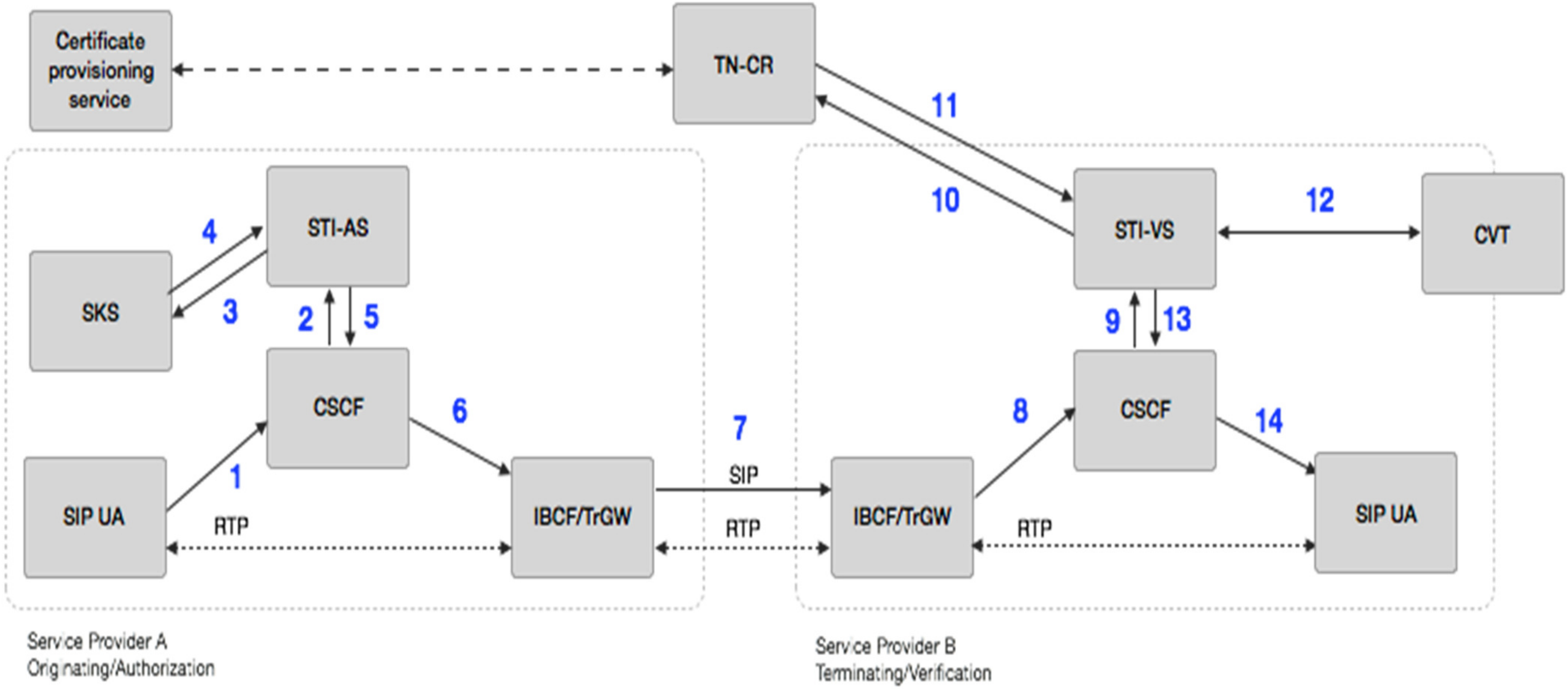
Authentication Service Function

Verification Service Function

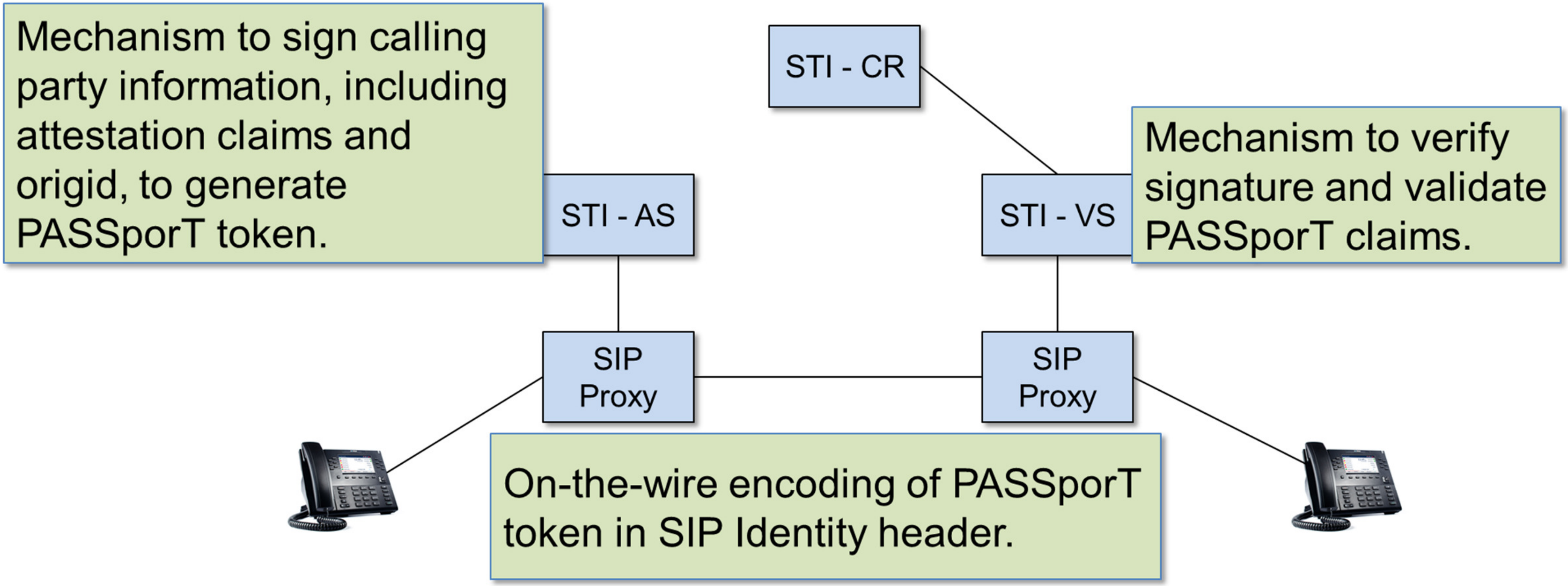
Call Validation Treatment

STI - Secure Telephone Identity

STIR/SHAKEN Basic Call Flow



Phase 1: ATIS-100074 SHAKEN Specification



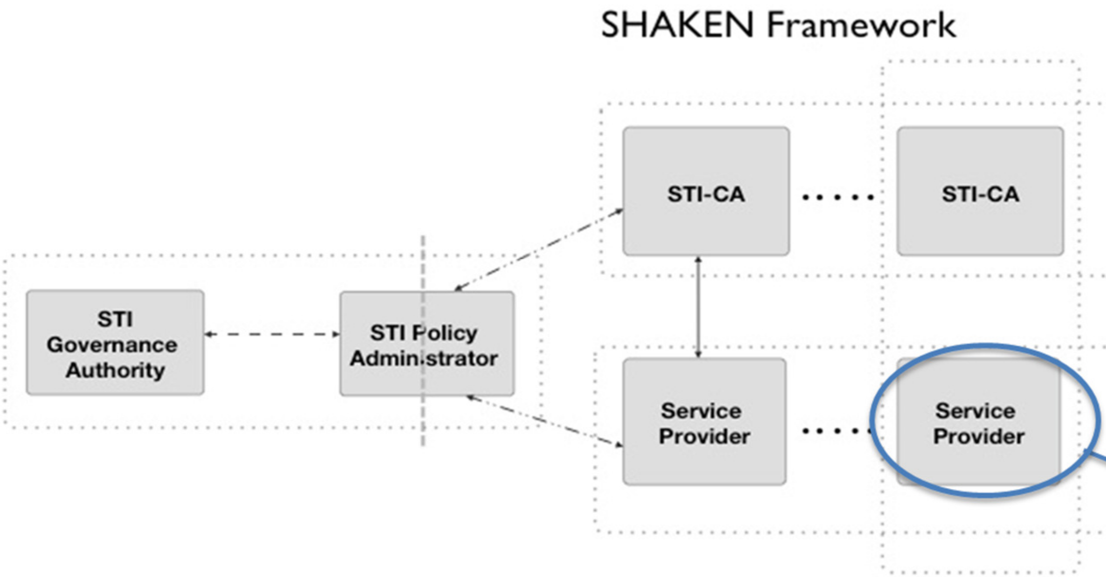
Mechanism to sign calling party information, including attestation claims and origid, to generate PASSporT token.

Mechanism to verify signature and validate PASSporT claims.

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

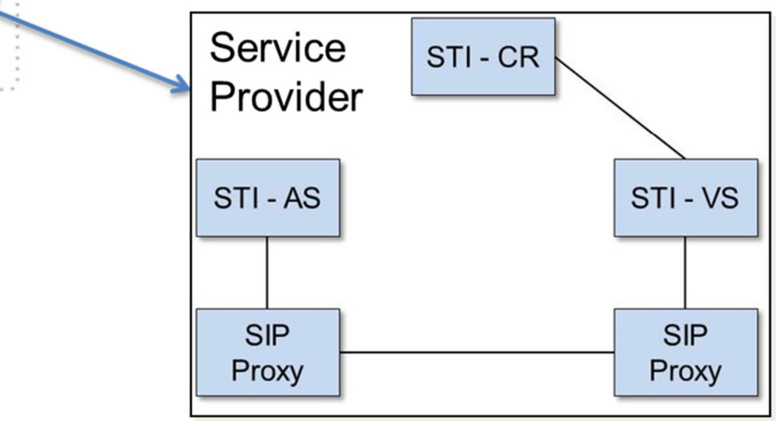
ATIS-1000074: Signature based Handling of Asserted information using ToKENs (i.e., SHAKEN)

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 (2-2)

2017

Feb July

- ATIS-1000074 -Signature-based Handling of Asserted information using toKENs (SHAKEN)
- ATIS launches testbed to advance mitigation of unwanted robocalling and caller ID fraud
- ATIS-1000080.v002, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management

2018

May Aug Nov

- ATIS-100081, TR on Framework for Display of Verified Caller ID
- ATIS-1000082, TR on SHAKEN APIs for a Centralized Signing and Signature Validation Server
- Industry groups select ATIS as the STI-GA. The GA was officially launched
- The GA is up and running
- ATIS testbed findings validate SHAKEN protocols effectiveness in mitigating unwanted robocalling
- Request for Proposal (RFP) issued for Secure Telephony Policy Administrator (STI-PA) role

2019

Feb Aug Dec

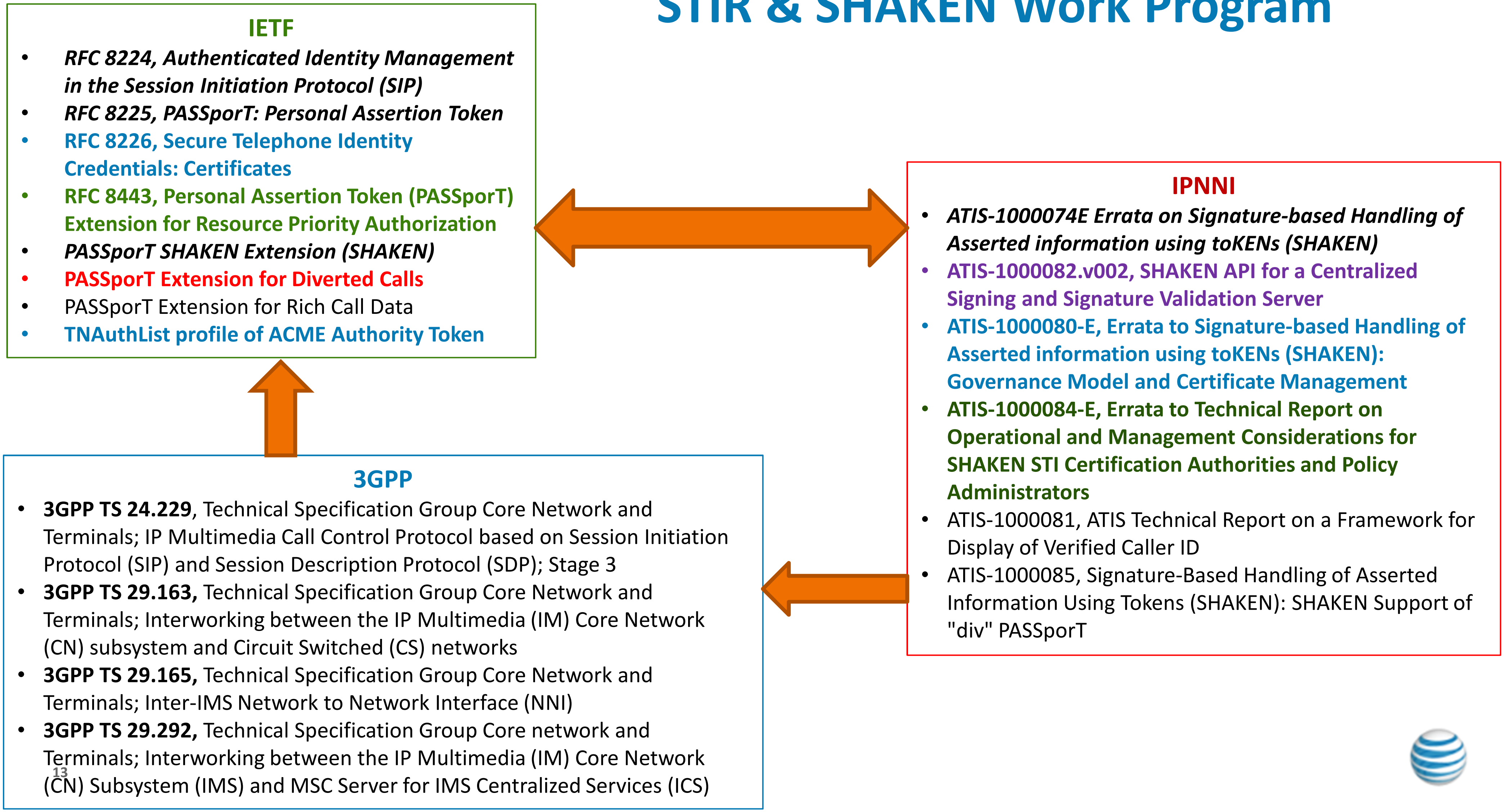
- ATIS-1000085, SHAKEN Support of "div" PASSporT

  ATIS-1000084-E, Errata to Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrator

  ATIS-1000080-E, Errata to Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management

  ATIS-1000074-E, Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN)
- STI-GA executes contract with iConnectv as STI-PA
- ATIS-1000080.v002, (SHAKEN): Governance Model and Certificate Management
- Target to have the STI-PA operational

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
- **TNAuthList profile of ACME Authority Token**

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

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)

IPNNI Active Documents

Signature-based Handling of Asserted information using toKENs (SHAKEN)	ATIS-1000074.v003	IPNNI-2019-00130R003
Verification Token Use Cases	IPNNI-2017-00020R000	Living Document
ATIS Technical Report on a Framework for SHAKEN Attestation and Origination Identifier	IPNNI-2019-00003R006	PTSC-LB-246
Robo-Metrics	IPNNI-2018-00083R001	
SHAKEN Roadmap	IPNNI-2019-00140R000	
SHAKEN Delegate Certificates	IPNNI-2019-00129R000	
SHAKEN Calling Name and Rich Call Data Handling Procedures	IPNNI-2019-00024R001	
Best Current Practices on the protection of STIR/SHAKEN data between service providers and from service providers to enterprises	IPNNI-2019-00055R000	
Considerations for Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)	IPNNI-2019-00056R013	PTSC-LB-242_d
Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements	IPNNI-2019-00075R005	
Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange	IPNNI-2019-00102R004	
ATIS Standard on Signature-based Handling of SIP RPH Assertion using Tokens	IPNNI-2019-00132R000	PTSC Issue S0150

Thank you.

AT&T Proprietary (Internal Use Only) Not for use or disclosure outside the AT&T companies except under written agreement.