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

10-17-2022

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.
- **Legitimate applications for this practice**
  - Doctor that calls from cell phone but doesn’t want to share her cell number, rather make it look like it comes from her office
  - Outbound Call center represents many customers so “spoofs” appropriate number of call-back number specific to that customer

Robocalls

- Robocalls are calls that are generally initiated by applications or auto-dialers that either are fully automated playing messages to the caller, or interact with the caller, or connect the calls to humans once it's determined that a called party has picked up and is communicating with the robs-call application.

- There is legitimate uses of robocall auto-dialing applications, for example emergency alerts, like snow-day calls to alert parents/students of a school delay or closing.

- There is legitimate but less popular uses of robocalls including political, sales, and debt collection calls. Of course there is some rules that try to protect people including Do Not Call list and related rules about contacting consumers that want to opt-out of these calls.

- Then there is illegitimate uses of robocalls that are often just bulk calling consumers to defraud them using scam scenarios to get people to sign up or give personal information that can be used often with the goal to steal money

Spoofing and Robocalling

Number reputation

Because robocalling practices lead to using numbers that are assigned to others you get the problem of false reputation

Bad vs Good

We can’t tell who is good or bad, truthful vs non-truthful, even within “trusted networks”, attacks to truth are coming from all directions

Breaking Analytics

The fact is, random processes break data analytics, so any call analytics techniques that try to determine bad practices now are leading to blocking legitimate calls

Path to Truth

STIR/SHAKEN framework is intended to get us on the path to truth in the telephone network

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
- Existing PSTN Class 5 TDM/SS7 equipment is at or near End of Life [EOL] and cannot be modified.

Now

- 756 Authorized Service Providers
- 12 Approved STI-CAs
- -10 public (Only 9 are listed on the STI-PA website, because one has been really slow in getting iconectiv their logo and links to post on the website.)
- -2 private
- ATIS STI-GA signs MOU with Canadian GA
- Ireland, UK, France and India inquiring about STIR/SHAKEN
- December 2019, TRACE ACT into law
- March 2020, FCC requires the implementation of Caller ID Authentication, such as STIR/SHAKEN
- July 2020, FCC approves new safe harbor rules to encourage blocking
- October 2020, FCC adopts new rules to combat spoofed robocalls

Robocalling/ Spoofing Timeline (1-2)

2012 | 2013 | 2014 | 2015 | 2016

Oct 2012

FTC Workshop on Robocalling and Caller ID Spoofing

Mar2013

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

The Lunch

May 2013

IETF BOF in DC on Approaches to CLID Spoofing

Aug 2013

IETF STIR Charter *Approved*

Jan 2014

ATIS - SIP Forum Task Force Tracks IETF STIR

Aug 2015

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

SHAKEN Framework Work begins

Sept 2015

FCC Workshop on Robocalling & Caller ID Spoofing

Oct 2015

ATIS ex-parte on ATIS work program

Fall 2015

SIP NNI TF & IETF STIR “agree” on solution alignment

Mar 2016

ATIS Provides Work program Update to FCC

Apr 2016

ATIS Whitepaper on CLID Spoofing

June 2016

ATIS Analysis on CLID Spoofing Mitigation Techniques

July 2016

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

Aug 2016

Strike Force *Kick-off Meeting*

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
- **Traced Act** into Law

Implementation of STIR/SHAKEN

March 2020: FCC requires the implementation of Caller ID Authentication, Report and Order
September 2020: FCC approves second report and order for implementing STIR/SHAKEN
June 2021: Implementation deadline for large providers

Assessing Barriers to implement STIR/SHAKEN

September 2020: FCC granted extensions in compliance with the STIR/SHAKEN deadline for certain categories of phone companies, including small companies with 100,000 or fewer customers
April 2021: Launch of FCC Robocall Mitigation Database
May 2021: FCC sought comment on shortening the extension granted to certain small phone companies that originate an especially large amount of calls

Best Practices

December 2020: FCC releases best practices for implementation of effective caller ID authentication framework based on expert input from FCC NANC CATA working group

Access to Numbering Resources

March 2020: FCC released notice to examine whether and how our policies regarding access to both toll free and non-toll free numbering resources can be modified to help reduce access to numbers by potential perpetrators of illegal robocalls

FCC NANC CATA Call authentication/Trust Anchor WG

May 2018 - *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR*

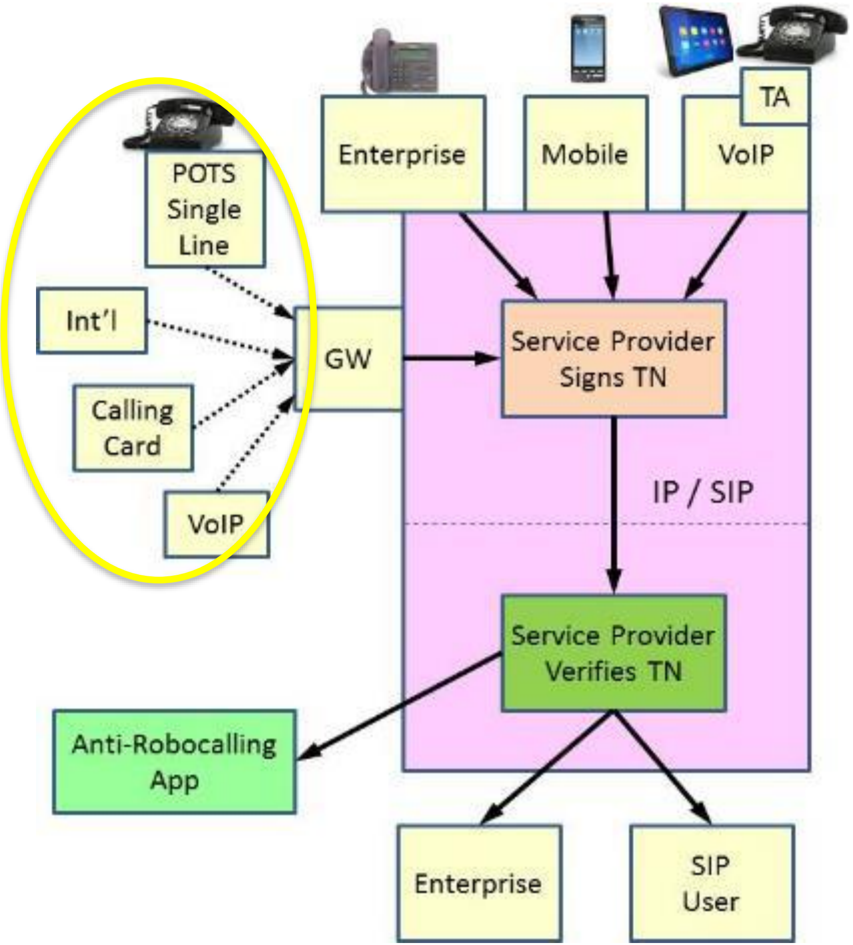
- established Governance model and initiated formation of the STI-GA/STI-GA-TC/STI-PA RFP

Sept 2020 - *Best Practices for the Implementation of Call Authentication Frameworks* - Subscriber Vetting, TN Validation, Attestation, 3rd Party Validation, International, Robocall Mitigation

Oct 2021 - *Deployment of STIR/SHAKEN by Small Voice Service Providers* - Technical Report detailing overcoming any perceived barriers to deploying STIR/SHAKEN

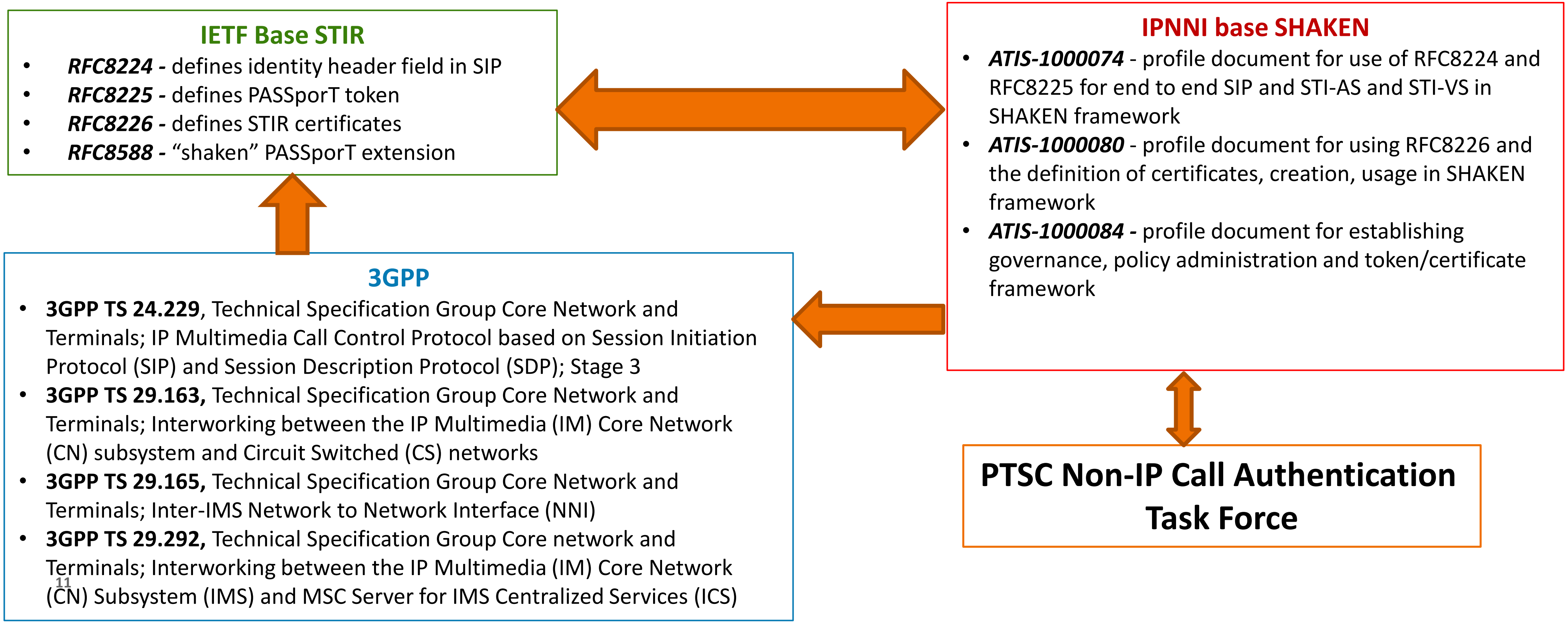
Jan 2022 - *Best Practices for Terminating Voice Service Providers using Caller ID Authentication Information* - Provides a review of many of the tools provided by STIR/SHAKEN and beyond that can be utilized to determine the legitimacy of a call

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 Work Program



IETF Base STIR

- ***RFC8224* -** defines identity header field in SIP
- ***RFC8225* -** defines PASSporT token
- ***RFC8226* -** defines STIR certificates
- ***RFC8588* -** "shaken" PASSporT extension

IPNNI base SHAKEN

- ***ATIS-1000074*** - profile document for use of RFC8224 and RFC8225 for end to end SIP and STI-AS and STI-VS in SHAKEN framework
- ***ATIS-1000080*** - profile document for using RFC8226 and the definition of certificates, creation, usage in SHAKEN framework
- ***ATIS-1000084* -** profile document for establishing governance, policy administration and token/certificate framework

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

Extensions to STIR/SHAKEN

RFC8443/ATIS-1000078 - Resource Priority - “rph” PASSporT for GETS/WPS

RFC9027/ATIS-1000098 - Resource and SIP Priority for Emergency Services - “rph”/“sph” claims

RFC8946/ATIS-1000085 - Diversion - “div” PASSporT

RFC9060/ATIS-1000092 - Delegate Certificates

ATIS-1000093 - Toll-Free Framework using Delegate Certificates

draft-ietf-stir-passport-rcd/ATIS-1000094 - Rich Call Data - “rcd” PASSporT

ATIS-1000095 - Extending STIR/SHAKEN over TDM

ATIS-1000096 - Out-of-Band PASSporT Transmission Involving TDM Networks

ATIS-1000099 - Robocall Call Blocking Notification

Enterprise extensions to STIR/SHAKEN

- ATIS-1000089 - Technical report describing potential techniques
- LEveraging Models for Originating eNtity authentication - Full Attestation with Entity Identity in a Secure Token (LEMON-TWIST)
- Extended Validation (EV) Certificates with TN Letter of Authorization (TNLoA)
- Central TN Database
- ATIS-I-0000084 - Enterprise Identity using Distributed Ledger.

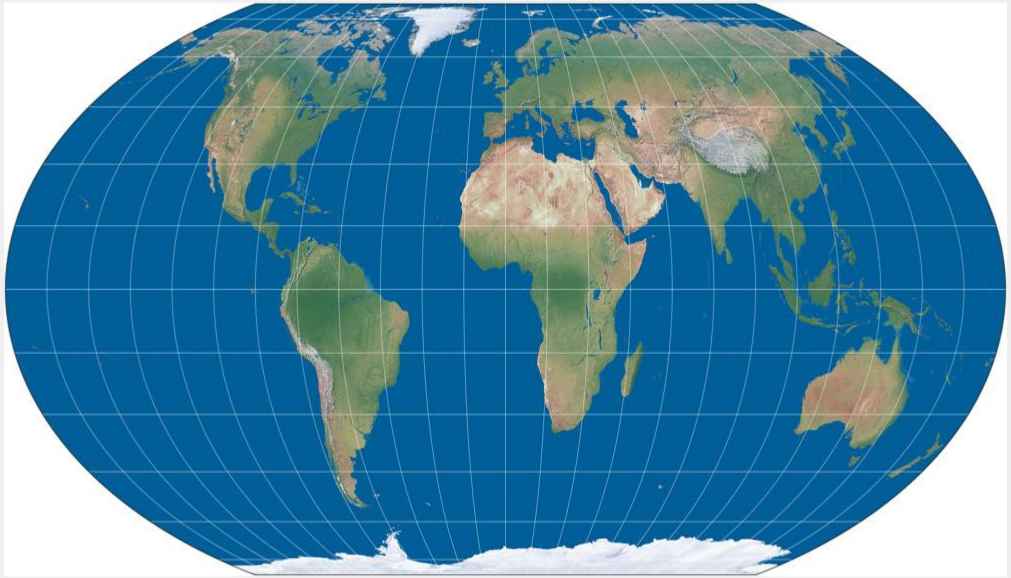
International/Cross-border STIR/SHAKEN

ATIS-1000087 - Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)

This is starting point, but there is much more to the story than the mechanics of sharing root certificates.
Evolving story.
FCC NANC CATA WG is currently working on report and guidance for where things stand today

Goals should be about a framework and set of policies that are focused on the same goals we have for domestic STIR/SHAKEN, more generally policies that support bilateral concepts of:

inclusiveness, security, and accountability



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"
}
```

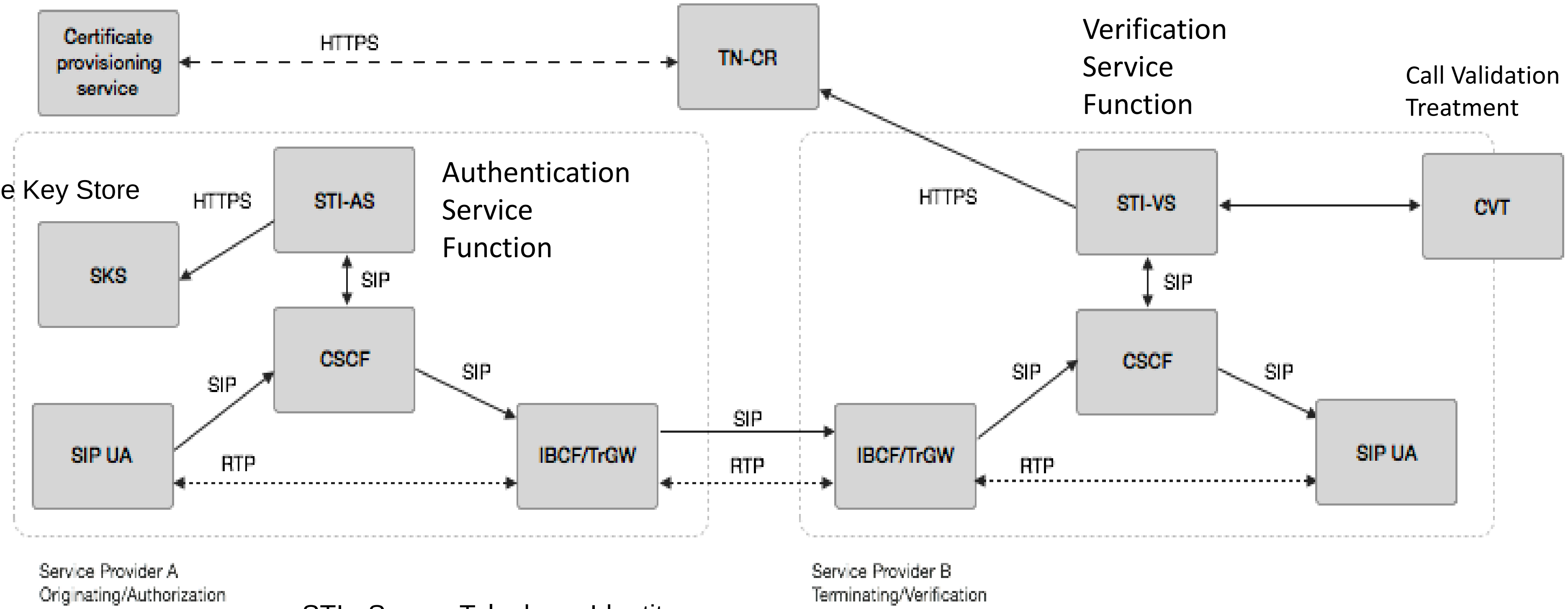
Payload

```
{
                "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)



TN Certificate Repository

Verification Service Function

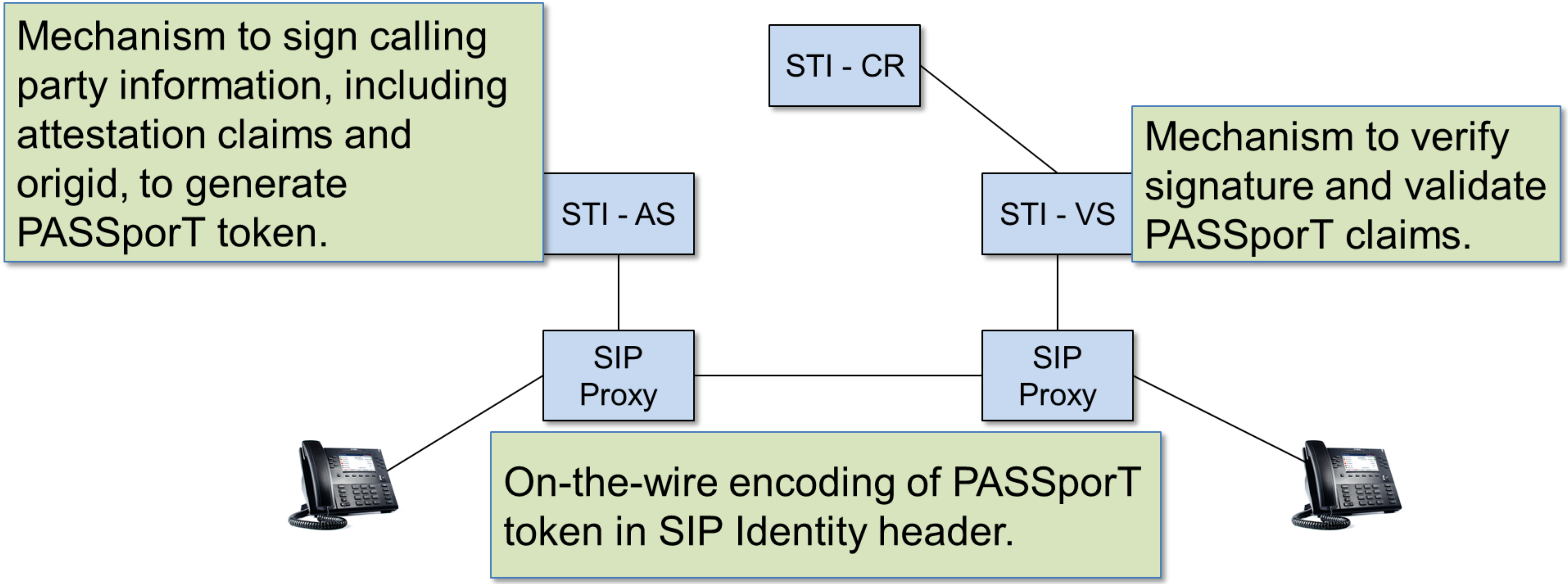
Call Validation Treatment

Secure Key Store

Authentication Service Function

STI - Secure Telephone Identity

Phase 1: ATIS-100074 SHAKEN Specification



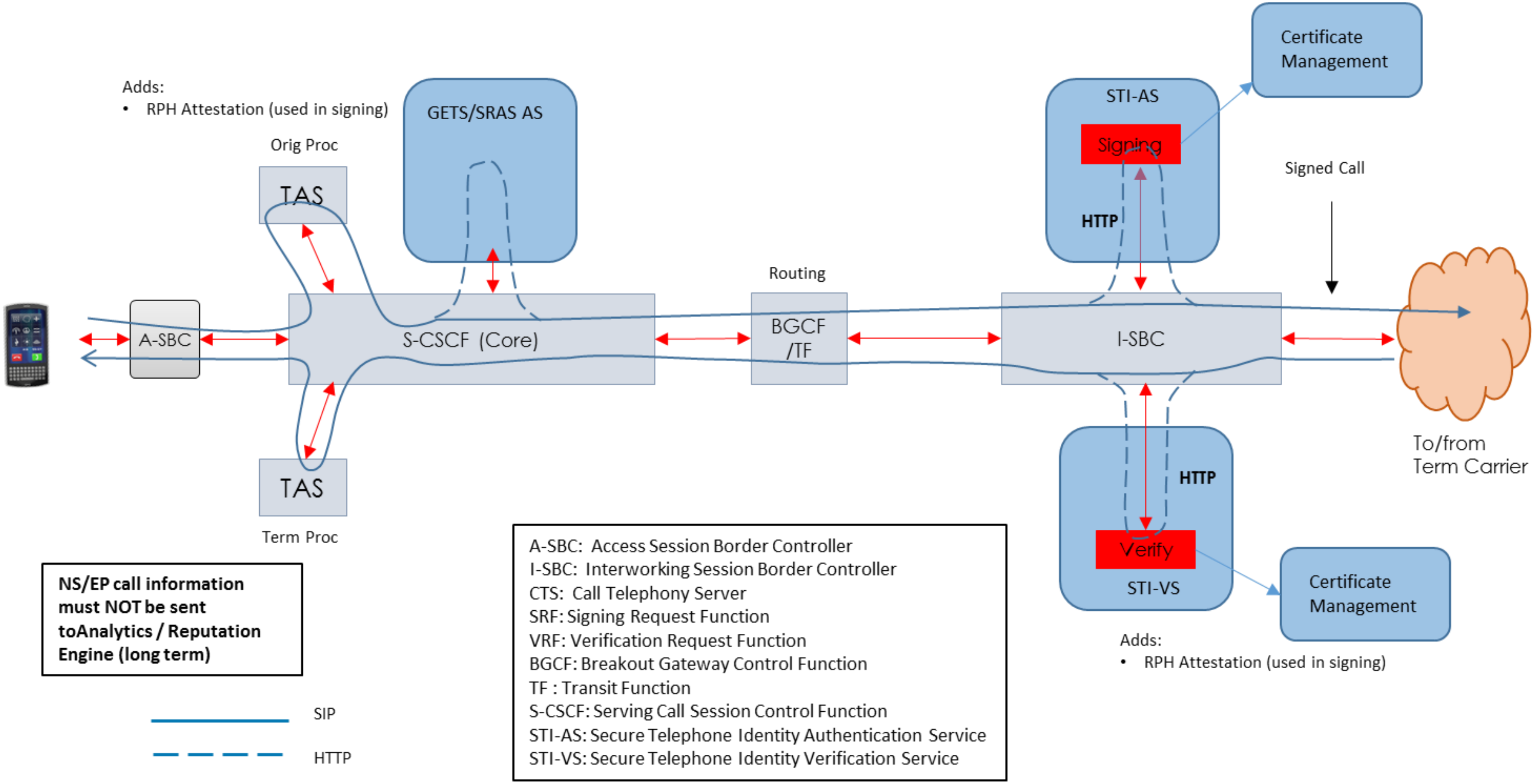
Mechanism to sign calling party information, including attestation claims and origid, to generate PASSporT token.

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)

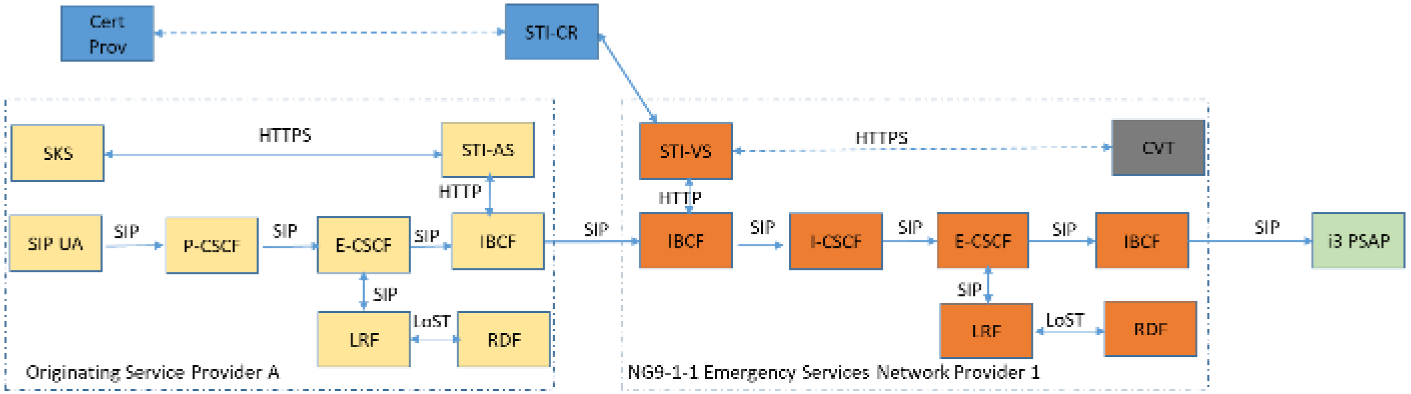
Inter-Network SHAKEN Flows (RPH)



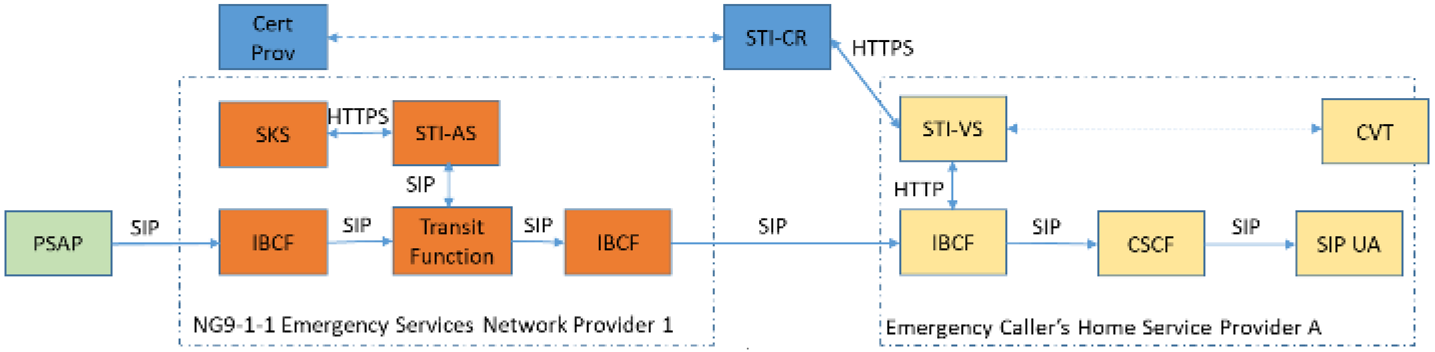
NS/EP call information must NOT be sent toAnalytics / Reputation Engine (long term)

A-SBC: Access Session Border Controller
I-SBC: Interworking Session Border Controller
CTS: Call Telephony Server
SRF: Signing Request Function
VRF: Verification Request Function
BGCF: Breakout Gateway Control Function
TF : Transit Function
S-CSCF: Serving Call Session Control Function
STI-AS: Secure Telephone Identity Authentication Service
STI-VS: Secure Telephone Identity Verification Service

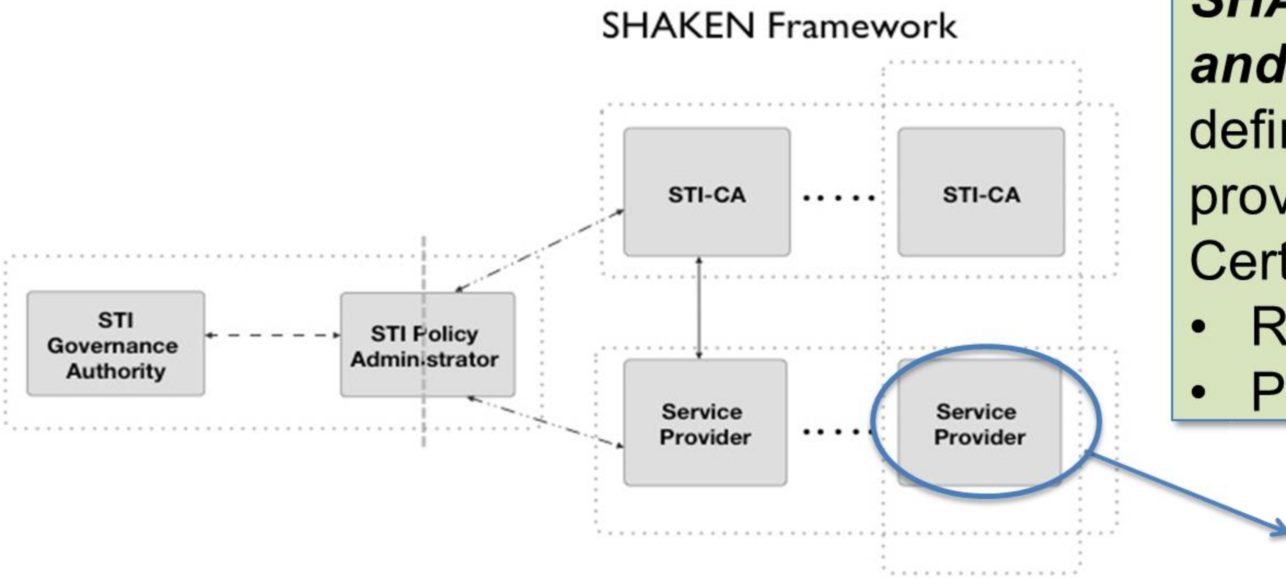
Architecture for Signing SIP RPH of Emergency Originations



Architecture for Signing SIP RPH of Callback Calls

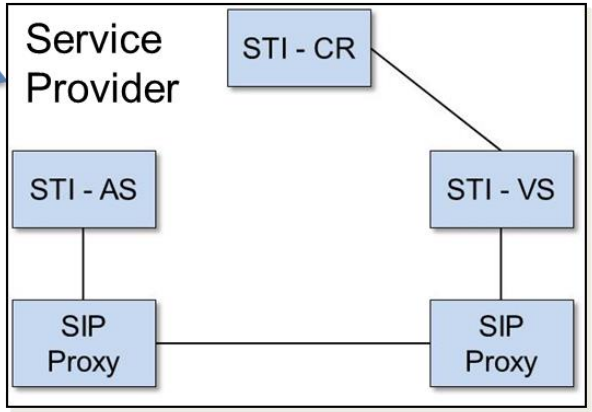


Phase 2: ATIS-1000080 SHAKEN Governance Model



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

Thank you.