SHAKEN and STIRed - Thoughts on the Current State of:
Anti Spoofing / Caller Validation / Robocall Mitigation / Call Validation Display Rich Call Data

March 2019

Richard Shockey

Chairman of the Board SIP Forum
Principal, Shockey Consulting LLC
Member, FCC North American Numbering Council
richard@shockey.us

skype/facebook/linkedin/twitter
rshockey101

+1 703 593 2683

SIP FORUM

- Leading Non-Profit IP Communications Industry Association
- 18+ Years Old -- Founded in 2000
- 18K+ Individual “Participant” Members
  - Corporate “Full Members” that pay annual dues to support the work of the Forum
  - Academic Institutions and Research Orgs

Full Member Companies

(Partial list)

SIP FORUM Full Member Companies

Columbia University:

The Fu Foundation
School of Engineering & Applied Science

FOKUS
Fraunhofer Institute for Open Communication Systems

TEXAS A&M UNIVERSITY

ILLINOIS INSTITUTE OF TECHNOLOGY

University of Glamorgan
because great minds don't think alike

Georgetown UNIVERSITY est. 1789

Gradiant

How We Got Here

- We wanted competitive voice markets. We got them, consequently
  “No good deed goes unpunished.”

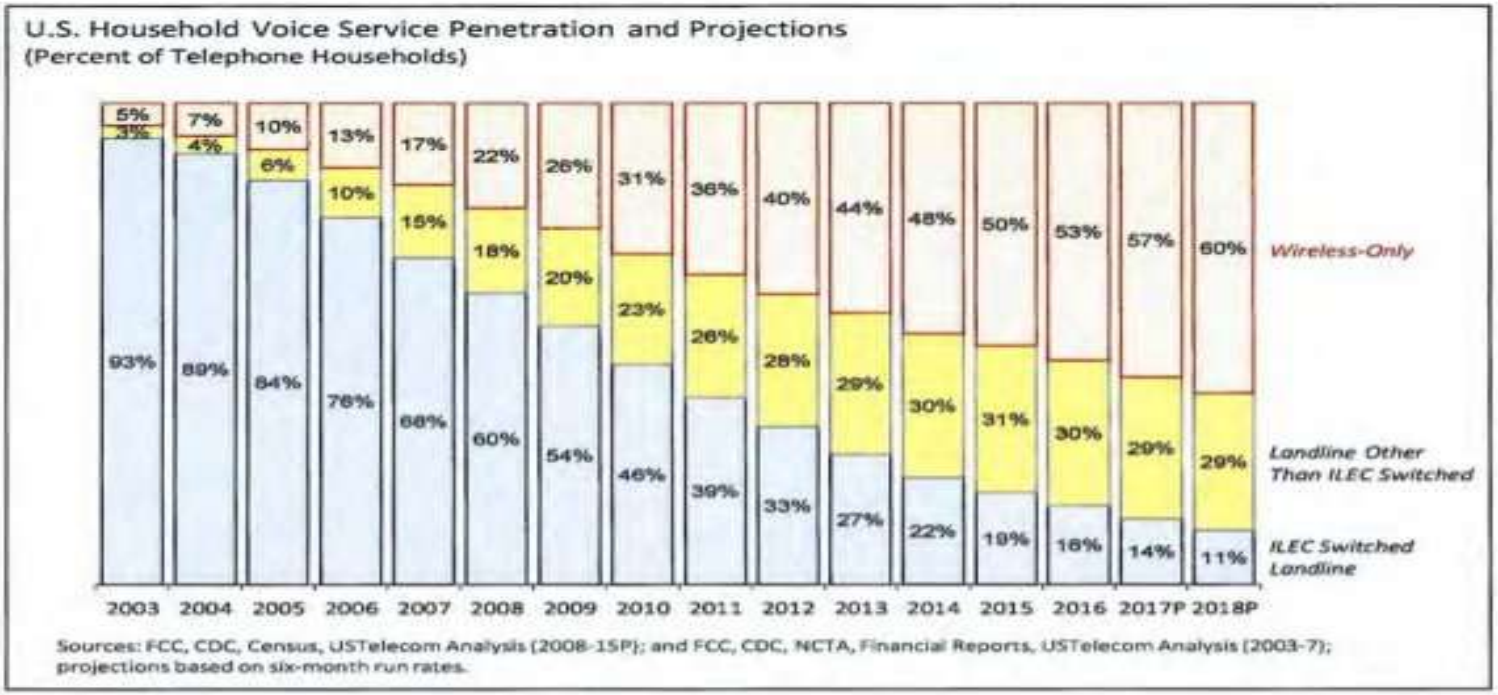
The Central issue now is restoring Trust in the Voice Networks! Call acceptance rates are dropping at an alarming rate.

- Robocalls & Spoofing is the #1 complaint to the U.S. FCC and FTC.
  https://consumercomplaints.fcc.gov/hc/en-us/articles/204009760-Consumer-Complaint-Charts-and-Data-Overview
  - U.S. Congress had held endless hearings. I was asked to testify.
  https://energycommerce.house.gov/hearings-and-votes/hearings/modernizing-telephone-consumer-protection-act

- Robocalls & Spoofing is the # 1 complaint to OFCOM and the UK ICO
  https://ico.org.uk/action-weve-taken/nuisance-calls-and-messages/
  - My presentation to UK Operators. Note the presentation from Huw Saunders of OFCOM on UK Policy direction:
  http://www.niccstandards.org.uk/meetings/forum-2016.cfm

- Robocalls & Spoofing is the # 1 complaint to the CRTC in Ottawa. Canada taking aggressive action. Their recent consultation:

The Evolving Telecom Landscape Provides Fertile Ground for Abuse



The interconnection between TDM/SS7 and SIP/IMS has been a huge attack vector as are the International Gateways.

The Status of SIP in general and the Enterprise

- My guestimate is that 65+% of all voice originates and/or terminates on SIP/IMS networks.
  - 100% of Cable
  - 80% Enterprise (T, VZ, CL Bandwidth.com, OTT)
  - Mobile
  - Advanced Residential Landline, FIOS, Uverse, etc.

- ATIS and SIP Forum NNI published IP Interconnection Routing Report (2014)
  - https://www.sipforum.org/download/joint-atissip-forum-technical-report-ip-interconnection-routing-atis-1000062-sipforum_twg-6/?wpdmdl=2780

SIP Forum/ATIS Network to Network Interface Task Force

Co-Chairs: Martin Dolly (AT&T), Chris Wendt (Comcast) who are also SIP Forum Board of Directors members.

ATIS and the SIP Forum formed the Joint Task Force to fully specify IP communications network-to-network interfaces (NNI) between North American service providers in a Open Multi-Stakeholder Consensus Driven process.

The NNI Task force has assumed overall responsibility for the direction of STIR/SHAKEN standards development

We have and will continue Identify gaps or ambiguities in existing standards and request that those gaps be addressed by the responsible Standards Development Organizations (SDOs).

For more info: https://www.sipforum.org/activities/nni-task-force-introduction/

STIR (Secure Telephone Identity Revisited)

• The IETF STIR Working Group has developed a mechanism to allow phone numbers to be “signed” at the origin, and “verified” at the termination.

  • https://datatracker.ietf.org/wg/stir/about/

• STIR set the stage for the SHAKEN work of the SIP Forum / ATIS Joint NNI Task Force to create a implementable specification including all the Certificate Management elements.

• ATIS and the SIP Forum have developed a deployment scenario to make this mechanism practical NOW! This approach has been formally endorsed by the FCC in the US (CATA) and mandated by the CRTC in Canada. More on US mandates

  • http://www.crtc.gc.ca/eng/archive/2018/2018-32.pdf

SHAKEN: The Work of the SIP Forum/ATIS NNI Task Force

1. **Signature-based Handling of Asserted information using toKENs (SHAKEN)** is an industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an IP-based service provider voice network.

2. **Joint ATIS/SIP Forum Standard – Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Governance Model and Certificate Management.** This specification expands the SHAKEN framework, introducing a governance model and defining X.509 certificate management procedures. Certificate management provides mechanisms for validation of a certificate and verification of the associated digital signature, allowing for the identification of illegitimate use of national telecommunications infrastructure. Published on July 11, 2017.

3. **Display Framework**: A framework is required to allow for the display of validated Caller ID information to end users in a consistent and secure format. Still under development

4. **Test-bed**: ATIS is facilitating a test-bed activity where they have developed a detailed test plan to validate the SHAKEN framework. This will verify the protocol and ensure interoperability between service providers.

5. TBD Enterprise Interfaces: The SIP Forum will lead efforts to take the STIR/SHAKEN framework and deliver it to the Enterprise or Contact Center.

Why did we make the technology decisions inherent in STIR/SHAKEN?

- The solution needed to be cost effective and deployable and support efforts to track and trace phone calls across the full call path.

- There was a similar problem in the Internet numbering and addressing system. Secure Inter-Domain Routing. [SIDR] The problem of spoofing the authority for a block of IP addresses as they are announced into the Border Gateway Protocol system.
  - https://datatracker.ietf.org/wg/sidr/documents/

- We rejected suggestions that each and every phone number needed a X.509 certificate associated with it. Too expensive.

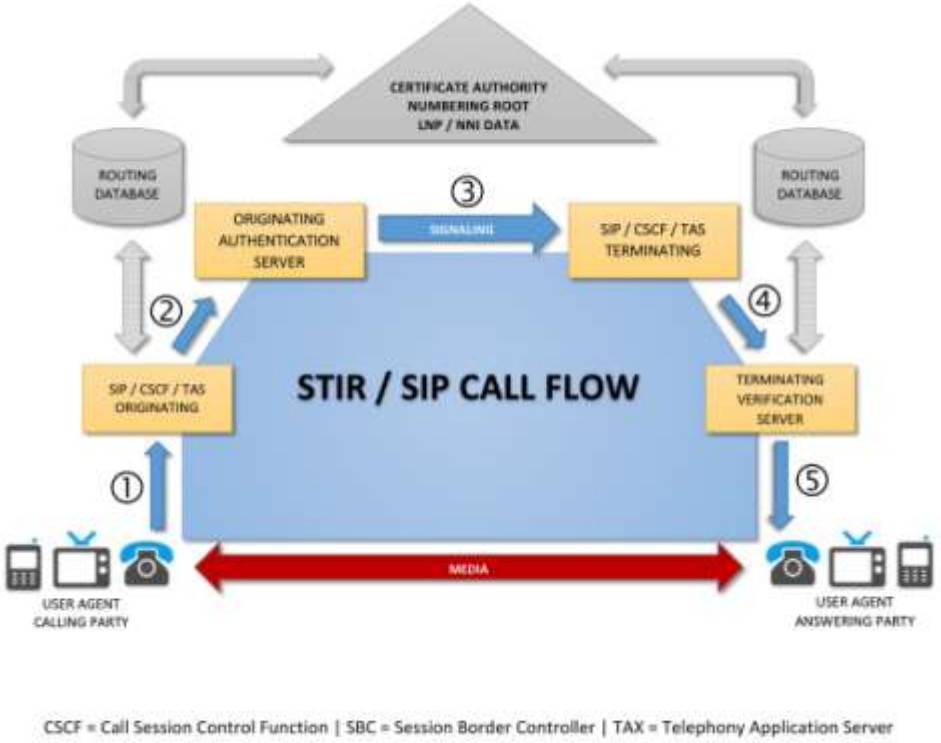
- We focused on creating a ’Circle of Trust” among service providers first and then see how things evolved.

What STIR / SHAKEN is Going to do

- We are going to capture the relevant call information and cryptographically sign every single call in the U.S. network within the SIP INVITE
  - Hopefully/Especially those coming from the International call gateways.
- STIR / SHAKEN uses well-understood, well-deployed Public Key Infrastructure principals and techniques. [PKI] X.509 Certificates & JWT Identity headers RFC 7519 (aka, PASSPorT) There may be more than one PASSPort.
- Private Cryptographic Credentials will be held by Originating Service Providers. Public Cryptographic Keys will have to be distributed to Service Providers.
- If the Originating Service Provider cannot “affirm” the data in call then it MUST not sign the INVITE.
- The Terminating Service Provider will validate the claims in the INVITE and act accordingly.
- There are some exceptions being made for US Gov’t applications, specifically GETS, and maybe Dept of Defense. They will sign their own transactions.

STIR/SHAKEN ATIS/SIP Forum Call Flows for Call Authentication / Verification

- It's the last signaling hop we have had concerns about. (5)
  - After Call Validation has been performed, what is the result and then what does the network tell the or the consumer do?
- FCC has ruled we should block calls with consumer consent. TCPA R&O



What will be Attested to...

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

In essence Carrier A says to Carrier B: "<u>This is my customer. I gave him this telephone number. This call originated on my network. You can trust it.</u>"

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

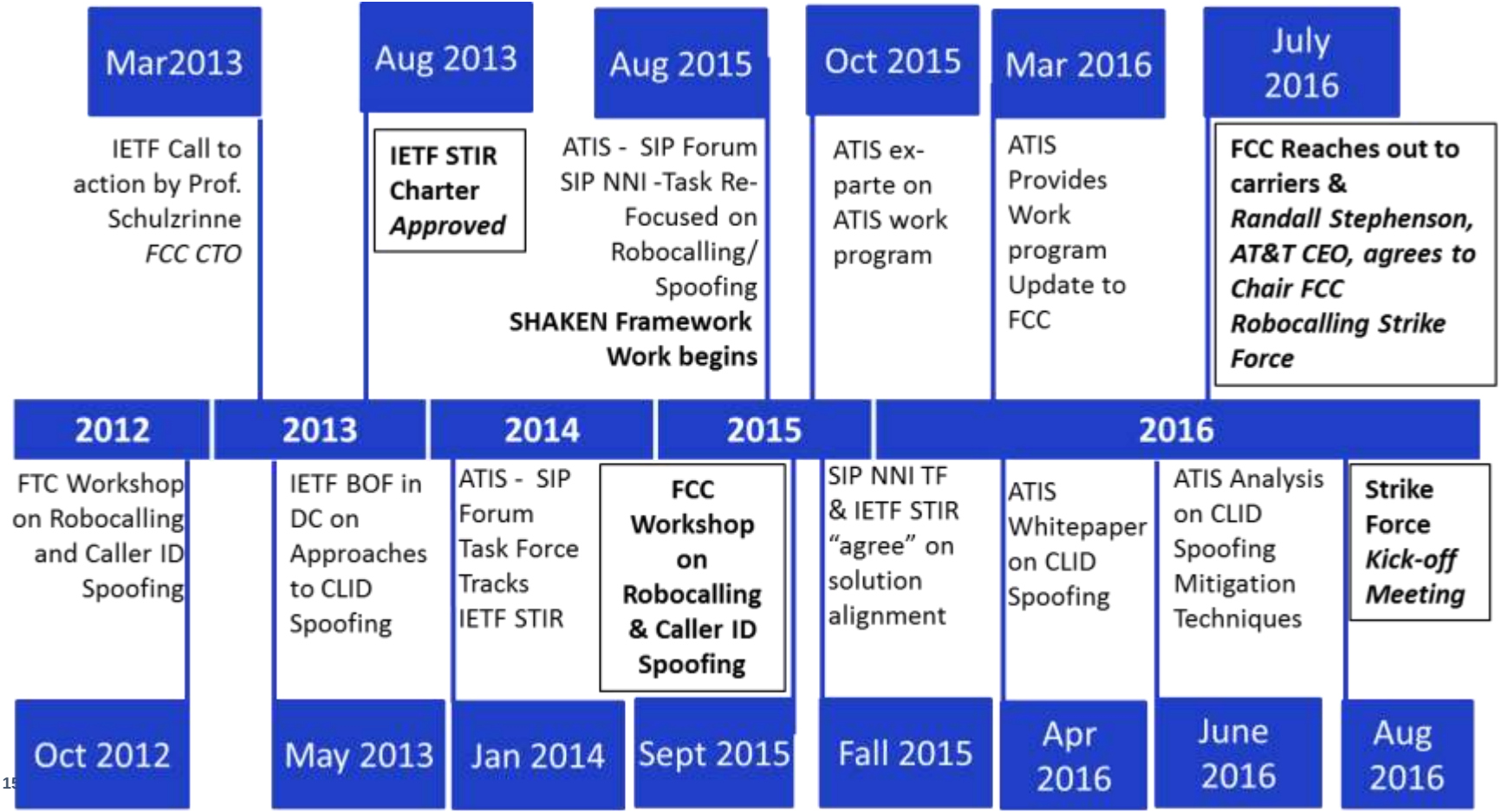
C. Gateway Attestation. The signing provider:

- 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".)

D. Super-Attestation in Development (AT&T and Verizon) – i.e., "This is my number. This is my customer. The call originated on and **<u>never</u>** left my network."

A Partial Robocalling/Spoofing Timeline in the United States



What is the FCC Doing?

- It Has Issued Multiple NOI-NPRMs and the FCC NANC has issued reports.
- WC Docket No. 17-59 Advanced Methods to Target and Eliminate Unlawful Robocalls
https://apps.fcc.gov/edocs_public/attachmatch/DOC-343731A1.pdf
- WC Docket No. 17-97 Call Authentication Trust Anchor
https://apps.fcc.gov/edocs_public/attachmatch/DOC-345474A1.pdf
- FCC North American Numbering Council Call Authentication Trust Anchor WG [CATA]
http://www.nanc-chair.org/docs/mtg_docs/Dec17_NANC_Referral_Call_Authentication.pdf
- CATA Final Report
http://www.nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf

- CATA Governance authority Board of Directors has been formed. CATA Policy Authority, which will create the root trust anchor RFP has been issued.

- Robocalls and spoofing meet FCC Chairman's Pai's three tests for active regulatory intervention:
    1. Clear Evidence of Market Failure
    2. Clear and Present Danger to Public Safety or Network Security
    3. Compelling Consumer Protection Interest.

What is Congress doing?

Two major Bills are under consideration. One from the Senate. One from the House.

House - Frank Pallone (D-NJ) is the current Chair of the House Commerce Committee

https://energycommerce.house.gov/newsroom/press-releases/pallone-reintroduces-bill-to-stop-robocalls

Senate - John Thune (R-ND) is the #3 in the Senate Hierarchy and Ed Markey the most Liberal Senator not currently running for President.

https://www.thune.senate.gov/public/index.cfm/2019/1/thune-markey-reintroduce-bill-to-crack-down-on-illegal-robocall-scams

BIG MESSAGE “Resistance is Futile”

I’ll let Dr. Burger elaborate on this…

https://www.fcc.gov/call-authentication

Chairman Pai is going to Blame and Shame each and every one of you until you submit.

Possible fines start at 10,000 PER INCIDENT under current Bills
Statute of Limitations extended to 3-5 years. And that’s only the beginning.

This is going to happen. There is going to be no way to avoid this.

Remember Local Number Portability? Oh BTW National Number Portability is coming. You are going to have to do All Call Query on Origination perhaps even termination if the call comes in through your Wholesale divisions.

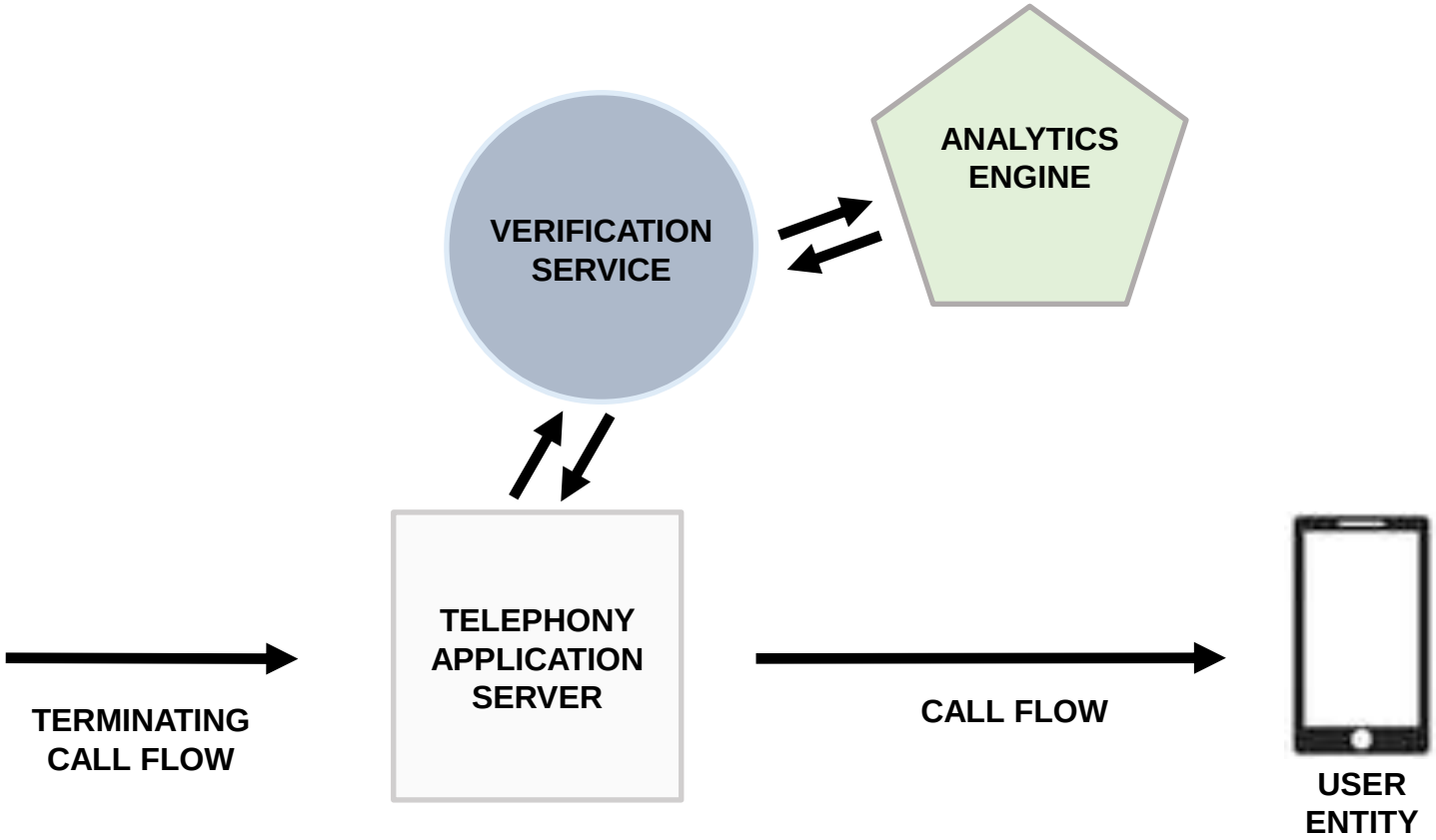
US Telecom has an active group on Track and Trace.

The Originating SIP Signaling Might Look Like This.

(This is what would go on the wire.)

- INVITE sip:test1@siptest.carrier.net SIP/2.0
  Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---77ba17085d60f141;rport
  Max-Forwards: 69
  Contact: <sip:test2@69.241.19.12:50207;rinstance=9da3088f36cc528e>
  To: <sip:1000@siptest.carrier.net>
  From: "Test2"<sip:5712223333@siptest.comcast.net>;tag=614bdb40
  Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
  CSeq: 2 INVITE
  Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
  Content-Type: application/sdp
  Date: Tue, 16 Aug 2016 19:23:38 GMT
  Identity: lW84Z2BbPF8U4AWGg4eeKNlIYAq4j4KexICilTQJsfmEU23d2Nt7-ih1valSKqwzXYctvJqsGzs5NuqAFgrLqg;info=<https://cert-auth.poc.sys.carrier.net/example.crt>;alg=ES256;canon=eyJ0eXAiOiJwYXNzcG9ydCIsImFsZyI6IkVTMjU2IiwieDV1IjoiaHR0cHM6Ly9jZXJ0LWF1dGgucG9jLnN5cy5jb21jYXN0Lm5ldC9leGFtcGxlLmNlcnQifQ.eyJkZXN0Ijp7InVyaSI6WyJzaXA6MTAwMEBzaXB0ZXN0LmNvbWNhc3QubmV0Il19LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ1cmkiOiJzaXA6NTcxMjIyMzMzM0BzaXB0ZXN0LmNvbWNhc3QubmV0In19
  Content-Length: 153
  v=0
  o=- 13103070023943130 1 IN IP4 10.36.78.177
  c=IN IP4 10.36.78.177
  t=0 0
  m=audio 54242 RTP/AVP 0
  a=sendrecv

Call Analytics Call Flow at Termination



Signaling Verification 3GPP CT 1 & 3

Verstat Parameter

TN Validation Passes
TN Validation Failed
No TN Validation

tel URI parameter in the P-Asserted-Identity
or FROM header field in a SIP requests

```
P-Asserted-Identity: tel:+14085264000;verstat=TN-Validation-Passed
```

Future: same values above for CNAM [Calling Name Delivery]

Security Considerations:

- The verstat parameter is essential for the enterprise or large call volume customer.
- Some customers will want the service provider to control the process but some may not.
- *New work will enhance this with more granularity on what type of validation is being performed.*

Display Framework – STIR/SHAKEN vs. Analytics

- The basic technical functionality
- Objective STIR/SHAKEN data and Certificate Verification are useful for:
  - Traceability
  - Accountability
  - Enforcements
- Reflects what the SP knows about the caller and how they know it
- Does not assist in determining the intent of the caller (malicious or not) but neither one actually blocks the call

- The value added functions
- Subjective
- Analytics can statistically assess the risk using:
  - Reported TNs (FTC and FCC lists)
  - Social Media
  - Reputation Data
  - STIR/SHAKEN and certificate verification results
- Call Scoring is now like Credit Scoring

The Call Origination problem….

Entities operating Outbound Call Centers will now have to consult multiple databases to insure that the dialed number is in fact correct.

Remember there are legitimate reasons to call customers.

Companies and Carriers must determine…

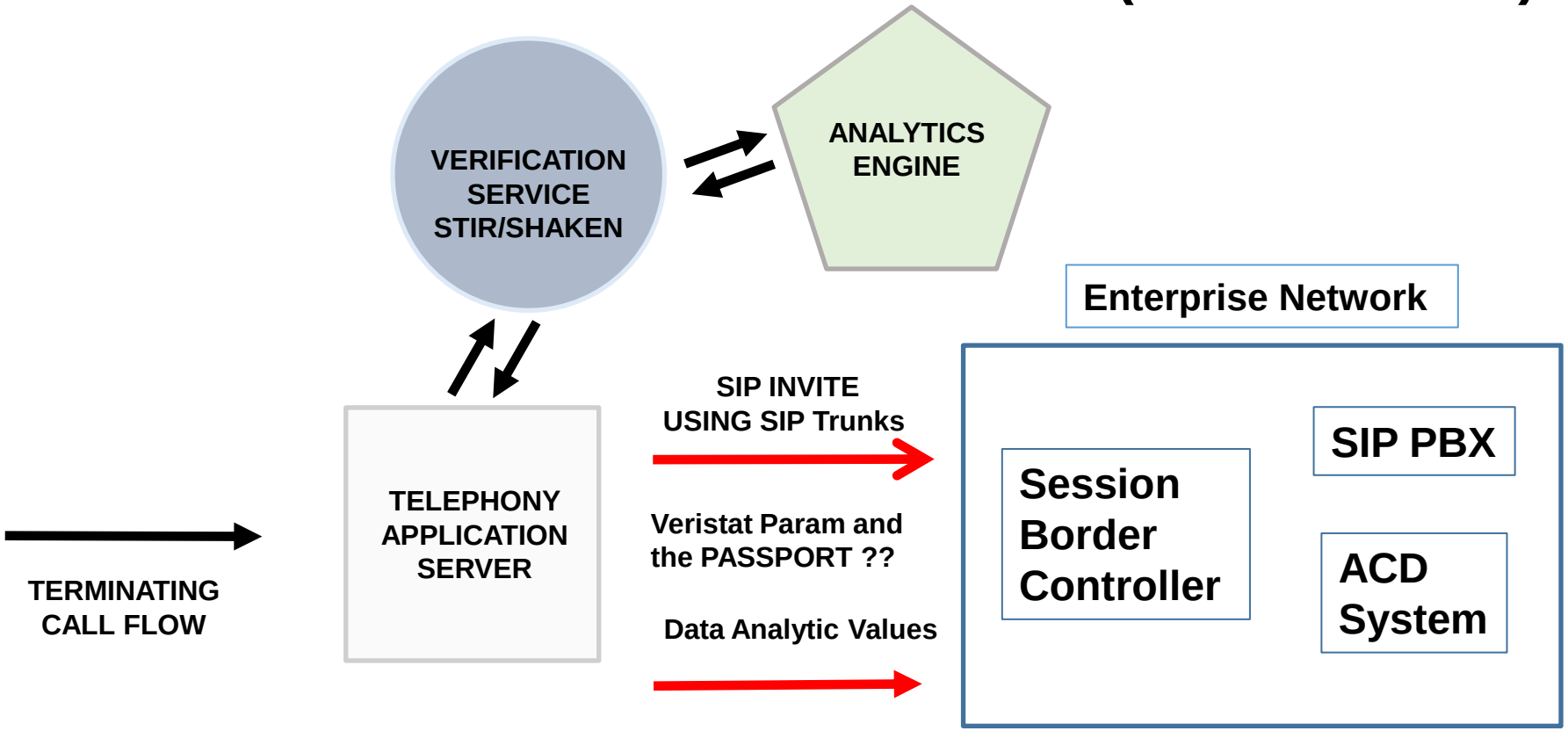
A. Is this a legitimate NANP Number ? Has it been issued? If it has NOT been issued it can be presumed to be a robocall and blocked under the new FCC rules.
B. The Do Not Call List.
C. The new Disconnected Number Database.

These are significant regulatory compliance obligations.

Anti robocall spoofing market place is splintering

- Residential – Mobile – Enterprise
  - Extremely dependent on Carrier Network Architecture
- Call signing at Origination – STIR But where?
- Call validation at Termination – SHAKEN w/ Analytics But where?
- Do Not Originate based on consumer preference
- Do Not Terminate based on consumer preference

Service Provider - Enterprise
Interaction STIR SHAKEN at Termination (In-band model)



There is no standard model for transmitting STIR/SHAKEN Data Analytics to the Enterprise or Contact Center ….Yet.

- This is the focus of much interest within Major Enterprises.

- There is ample evidence that Data Analytics is a tool that a company will pay carriers for. Call Data Analytics is now an ‘industry’.

- The ROI for this is now well understood. “Save time, save money.”
  - Reduces the need for exhaustive security checks for authentication.

- Early adopters may include:
  - Financial Services (Banks and Brokerage / Dept of Treasury SEC regs)
  - Health Care (Telephone Tag and HIPPA Hospitals now under attack)
  - Utilities (TCPA)
    - I testified before Congress on this:
      https://energycommerce.house.gov/hearings-and-votes/hearings/modernizing-telephone-consumer-protection-act

Issues and Opportunities to Monetize STIR / SHAKEN

- A standard presentation in the SIP INVITE promotes interoperability and enables the market.
- No standardization of the data on the wire yet. Where in the invite should we insert data analytics? Call-Info? In the Certificate? What represents the best solution for monetization?
- Customization of the Call Validation Display with Rich Call Data.
- Custom-Tailored Sales/Contact Center Solutions.
- Analysis/Reporting of Call Analytics Data.

Call Validation Display Framework: What are the Minimum Elements to be Imparted to the User Agent (aka the Phone)?

- Start with Green Yellow Red?

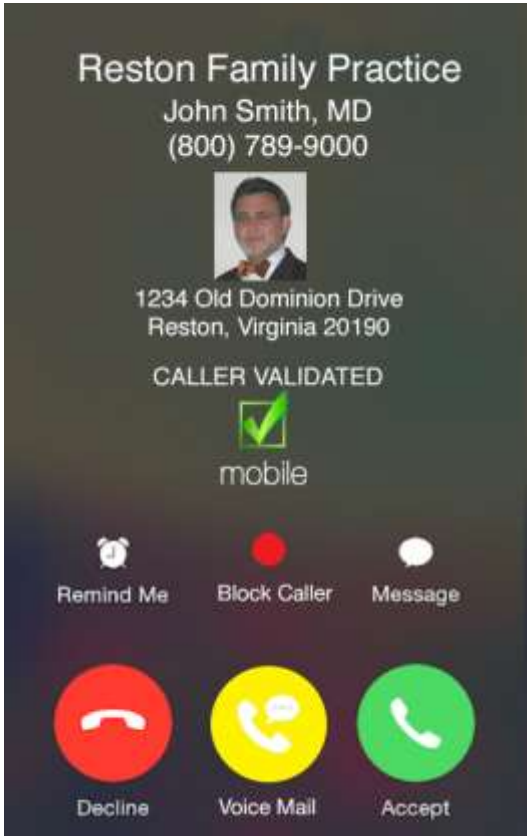
- First separate what is objective validation data vs subjective data.
- What other kinds of value added information can be given to the user by the service provider?
  - Logos?
  - Pictures?
  - Theme songs?

Enhanced Call Validation Display Options + Rich Call Data

- Existing User Display is limited to 15 Character ASCII for CNAM [Calling Name Delivery] and the Calling Party Number.

Now we can do anything!

- Calling party could display business name, address and potentially a picture as well based on Rich Call Data.
- Calling party can display alternative number to protect Doctors privacy when responding to consumer inquiries.
- Protect Emergency Personnel from revealing their true Calling Party Number.

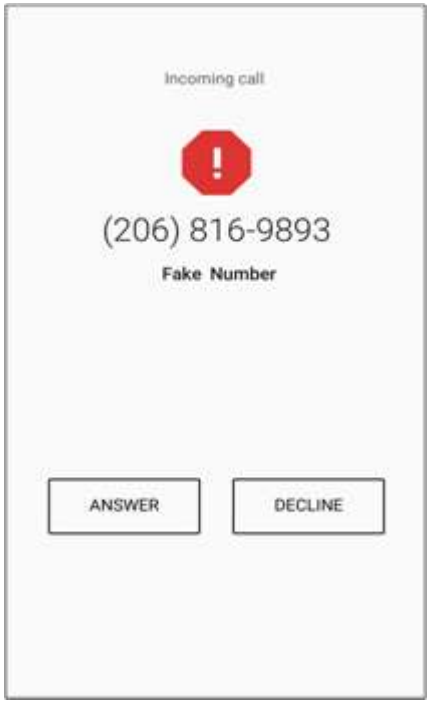


Enhanced Call Validation Display
[REALLY BAD Call]

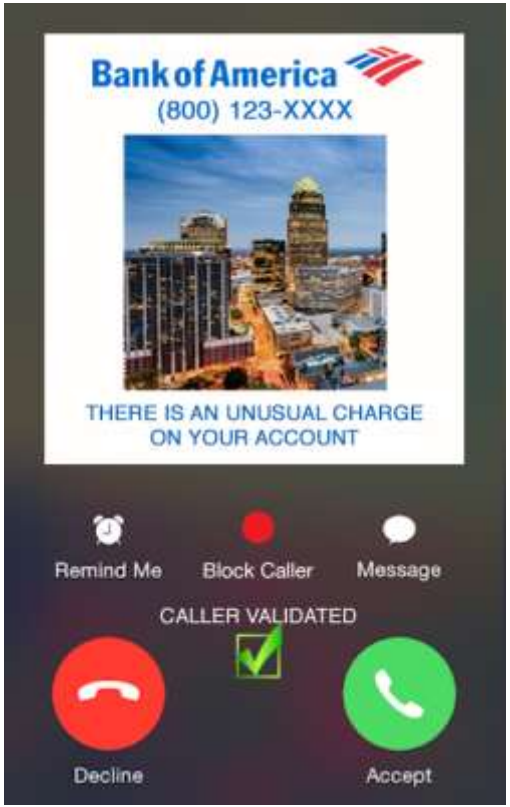
Scenario 2

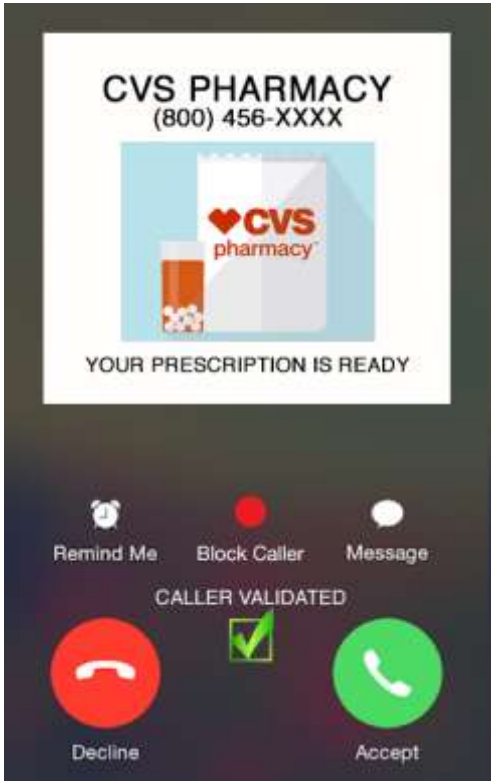
- Network has no confidence in the signaling path whatsoever; data analytics indicates possible malicious call.
- Signaling to consumer indicates very high level of distrust in the call.
- Network can alternatively block the call based on clear consumer preference.

More Examples…



And More Examples





Example Displays with STIR/SHAKEN Verified – Legacy Phones

Example Displays with STIR/SHAKEN Verified – Smart Devices

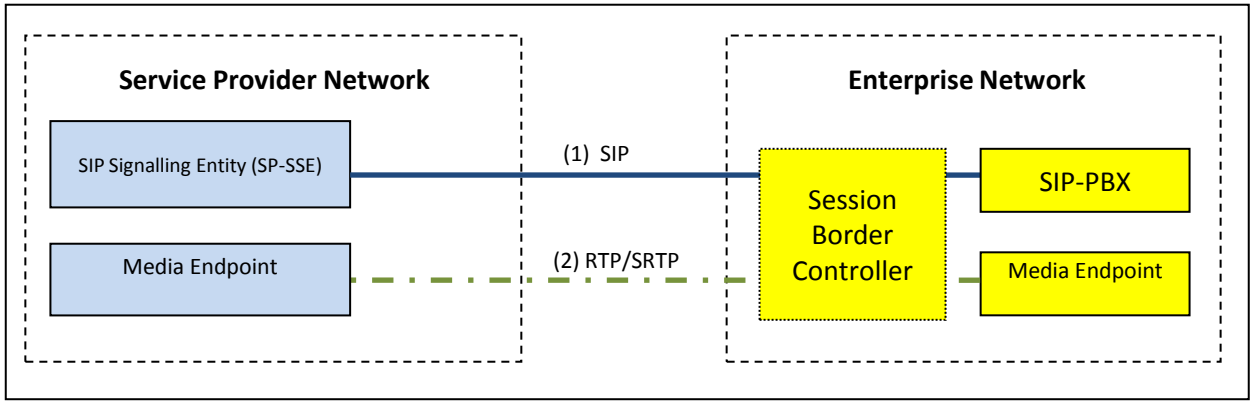
-

What are the Requirements for Enterprise Implementation of STIR / SHAKEN?

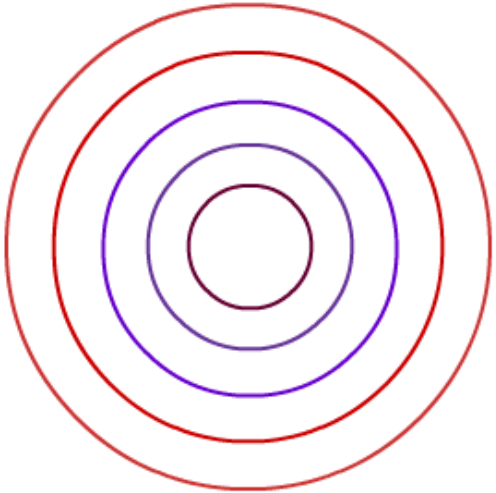
SIPconnect 2.0

The Industry-Leading Specification for Enterprise-Service Provider IP-Interconnection (a.k.a. “SIP Trunking”)

https://www.sipforum.org/technology/sipconnect/



Other Issues to Be Resolved



- STIR / SHAKEN is not a Silver Bullet.
  - There is no flash cut here
  - We need rings of defense

- The issuance of PKI credentials for the Service Providers should IMHO perfectly match the chain of authority for the North American Numbering Plan itself. The focus of the CATA Policy Authority.

- Will the FCC need to protect the integrity of the call authentication data in regulation in the same way they do call billing data? CPNI?

- 47 USC §64.1601 Delivery requirements and privacy restrictions.
- (a) Delivery. Except as provided in paragraphs (d) and (e) of this section:
-
- (1) Telecommunications carriers and providers of interconnected Voice over Internet Protocol (VoIP) services, in originating interstate or intrastate traffic on the public switched telephone network (PSTN) or originating interstate or intrastate traffic that is destined for the PSTN (collectively “PSTN Traffic”), are required to transmit for all PSTN Traffic the telephone number received from or assigned to or otherwise associated with the calling party to the next provider in the path from the originating provider to the terminating provider.

For More Information

Learn more about SIP Forum Membership!

Through the SIP Forum, ANY interested party can participate in the ongoing STIR / SHAKEN deliberations.

First sign up as a Participant member of the SIP Forum and then join the nni@sipforum.org mailing list.

SIP Forum/ATIS NNI Task Force Landing page

THANK YOU!

SIPNOC 2019

The SIP Forum held its SIPNOC [SIP Network Operators Conference] in Herndon VA December 2018.

Chairman Ian Scott of the CRTC was our keynote !

The focus was Robocalls and CLI spoofing.

Our Agenda and our presentations are here.

https://www.sipforum.org/news-events/sipnoc-2018-overview/sipnoc-2018-conference-schedule/

Yes we will have another conference early December 2019 in Herndon at the Hilton Dulles. Stay tuned.