SHAKEN and STIRed and the future of UCaaS

Anti Spoofing / Caller Validation / Robocall Mitigation / Call Validation Display

Cloud Computing Alliance
New York City
April 2017

Richard Shockey
Chairman SIP Forum
Shockey Consulting LLC
Member FCC North American Numbering Council [NANC]
richard@shockey.us
+1 703 593 2683

- Work in progress
- Disclaimer: The following opinions are those of a deranged, raving lunatic and do not necessarily reflect the opinions of the SIP Forum or its member companies..

SIP FORUM

- Leading Non-Profit IP Communications Industry Association
- 17 Years Old -- Founded in 2000
- 17K+ Individual “Participant” Membership
  - Corporate “Full Members” that pay annual dues to support the work of the Forum
  - Academic Institutions and Research Orgs

SIP FORUM Full Member Companies

(as of 03-12-2017)

The Fundamental Macro issues in Cloud Communications

- Telecom is about a 580 Billion Dollar business in the US though revenues generally flat.
- IMHO Voice alone may represent 140 Billion across all the access platforms. Residential Mobile Enterprise.
- “Protect what you have”
- Hosted Cloud Communications are the fastest growing segments of the industry.
- Cable beginning to dominate SMB markets < 24 sessions. CLEC’s and ILEC’s all have competitive offerings.
    - Vonage 8X8 etc all focused on SMB Enterprise abandoning residential
- Classic PBX markets are dying. Can you spell Avaya?
- UC B-B Meeting Technology maybe 7 Billion and highly fragmented

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 Real Time Communications in order to maintain over all industry profitability.

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.

http://www.crtc.gc.ca/eng/archive/2017/2017-4.htm

What SIP Forum STIR – SHAKEN is Proposing

- We are going to cryptographically sign the SIP/IMS Call Signaling for every single call in the U.S. network.
  - Hopefully/Especially those coming from the International call gateways.

- STIR / SHAKEN use well-understood, well-deployed Public Key Infrastructure principals and techniques. [PKI] X.509 Certificates & JWD Identity headers RFC 7519
  - PKI is everywhere. Well-understood technology especially in Financial Services

- Private Cryptographic Credentials will be held by Originating Service Providers. Public Cryptographic Keys will have to be distributed to Service Providers.

- Originating Service providers will make an attestation or “affirm” the information contained in the SIP INVITE is true. That means the Caller ID among other data.
  - If the Originating Service Provider cannot “affirm” the data in call then it MUST not sign the INVITE.

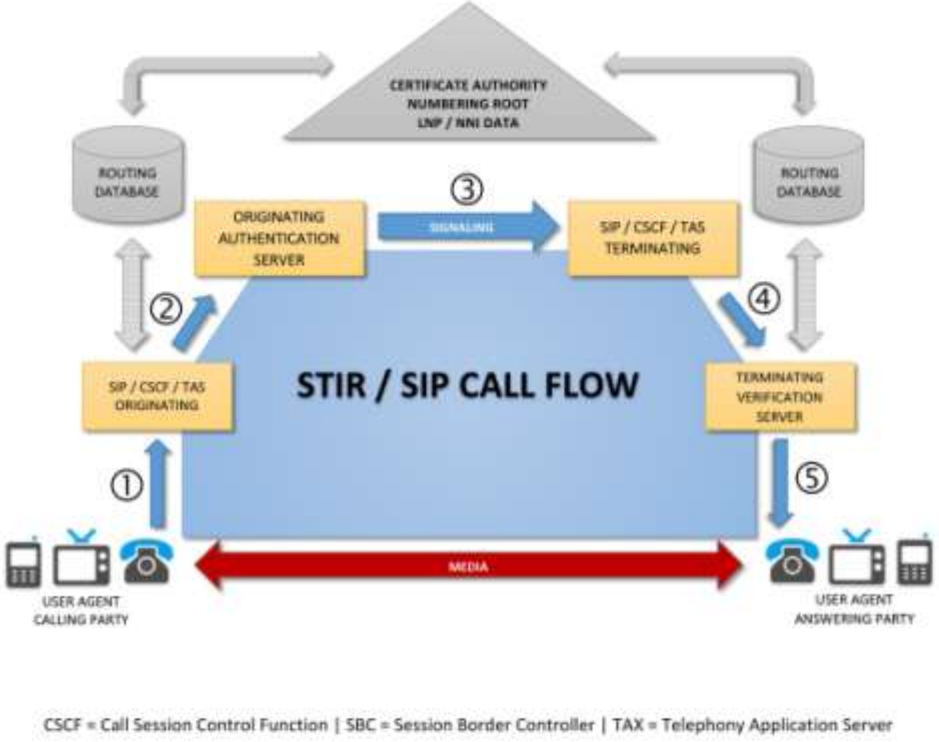
- The Terminating Service Provider will validate the claims in the INVITE and act accordingly.

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 or the consumer do?

- FCC has ruled we can block calls with consumer consent. TCPA R&O

- Can this be combined with Enhanced CNAM?



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.

    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).

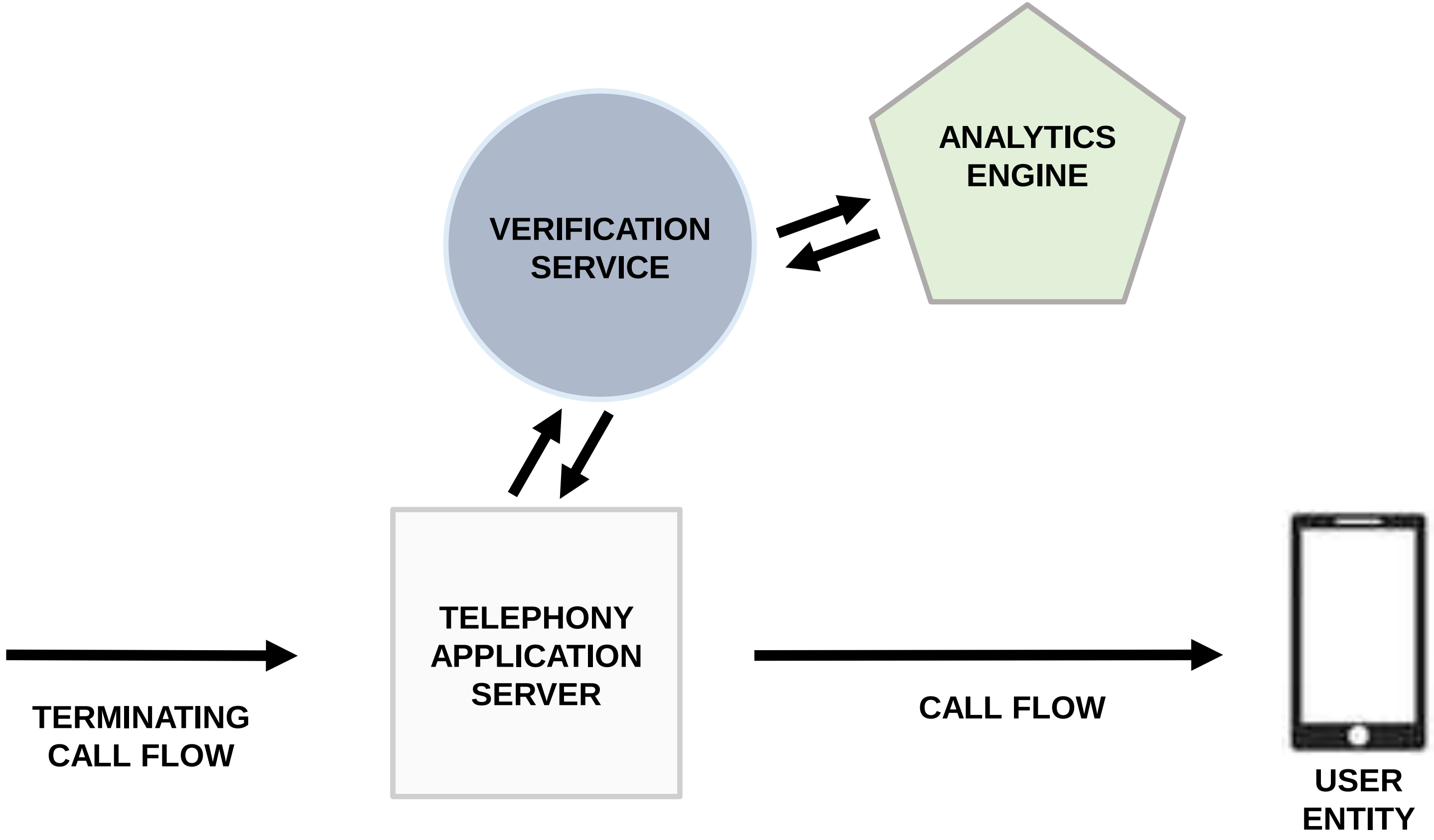
    Note: The signature will provide a unique identifier of the node. (The signer is not asserting anything other than “this is the point where the call entered my network”.)

The 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

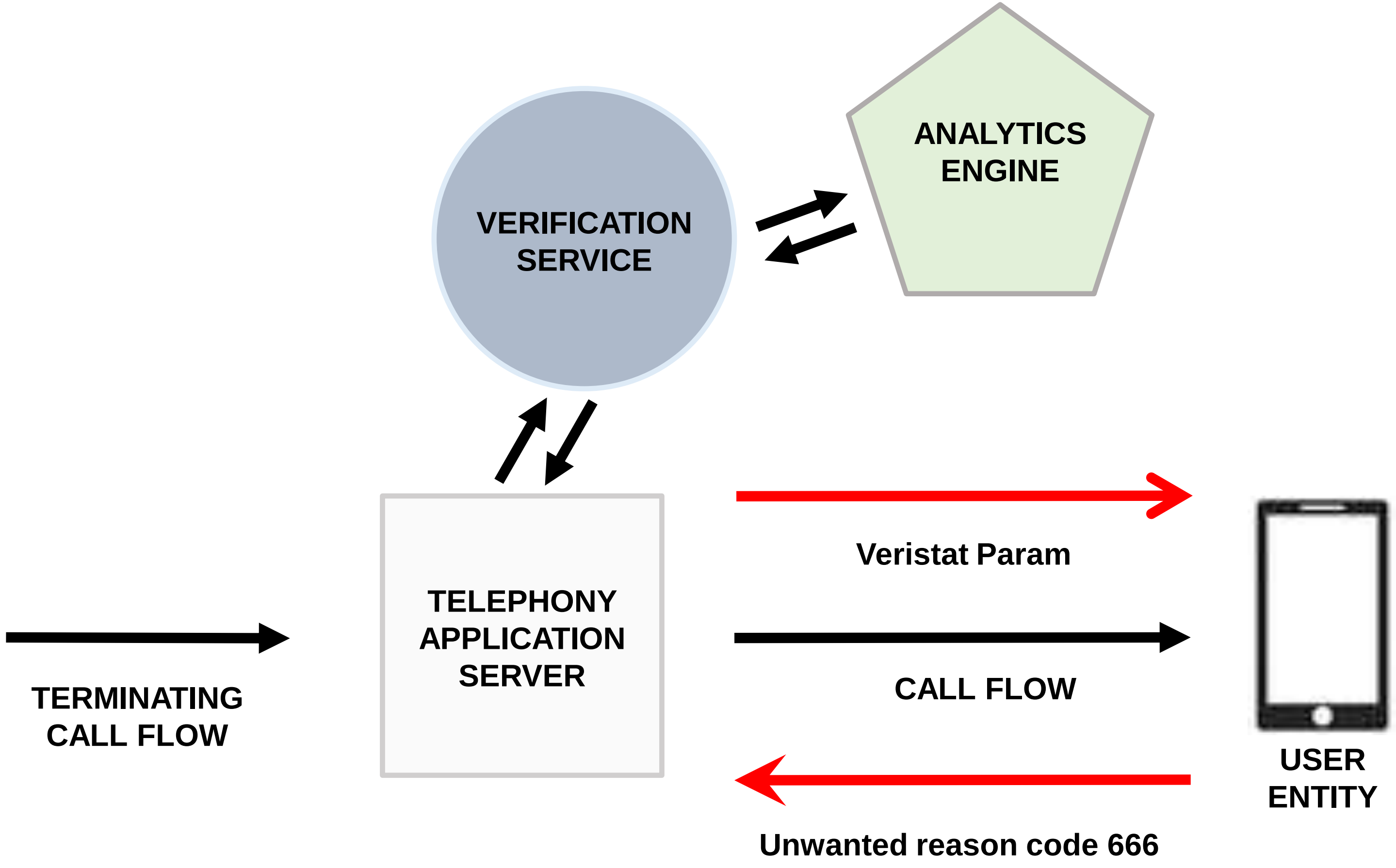


The Data Analytics Engine

- At least 7 Companies are now selling Anti-Robocall Spoofing services to carriers or for use in Client User Agents:

  – TNSI in Reston VA
  – NeuStar
  – iconectiv
  – Hiya
  – NOMOROBO
  – PrivacyStar
  – SecureLogix

User Agent Interaction at Termination



Signaling Verification Now at 3GPP CT 1 & 3

Verstat Parameter

TN Validation Passes
TN Validation Failed
No TN Validation
Future: same values above for CNAM [Calling Name Delivery]

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

Security Considerations:

- The Verification Function must drop a verstat tel URI parameter received in an INVITE
- If the terminating UE does not support the "verstat" parameter value, it must discard the parameter
- The terminating UE will act on the "verstat" parameter value, if the 200 (OK) response to the UE REGISTER includes a Feature-Caps header field, as specified in RFC 6809°[190], with a "+g.3gpp.verstat" header field parameter

The End Game Call Validation Display

Existing User Display is limited to 15 Character ASCII for CNAM [Calling Name Delivery] and the Calling Party Number. This is what needs to be enhanced.

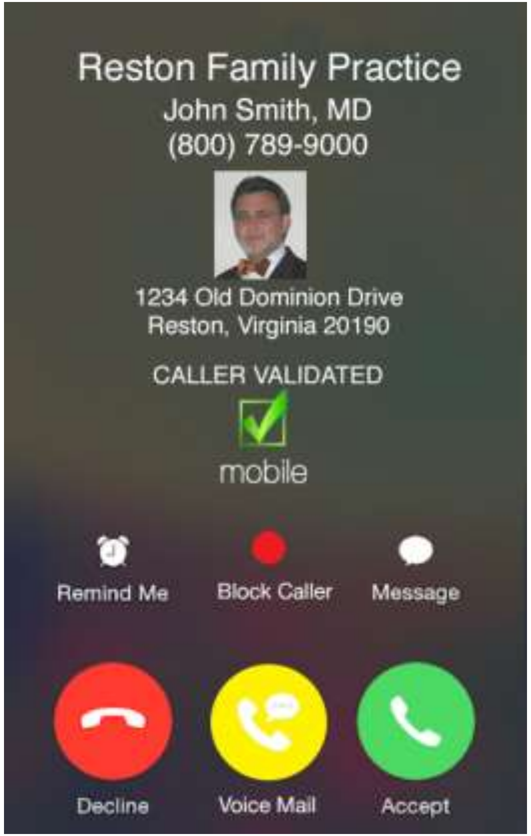
In mobile VoLTE, the handset is a SIP User Agent.

Now we can do anything!

Calling party could display business name, address and potentially a picture as well based on Enhanced CNAM, but CNAM was not popular in the UK? Right?

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.



Applicable to all SIP/IMS platforms

This is the Value Proposition for Cloud Communications. We can sell this!

Cable today can optionally display Caller ID on TV platforms. This could be added in.

A solution can work with any SIP-based Enterprise PBX system either On Premise or Hosted.

- SIP Forum could take the lead here based on our SIPconnect Technical Recommendation.

Inc

We can't fix POTS or TDM/SS7 nor do we want to.

STIR-SHAKEN / Strike Force / IETF /ATIS-SIP Forum / 3GPP

- **Phase 1** is done! You can download the STIR/SHAKEN Framework here:

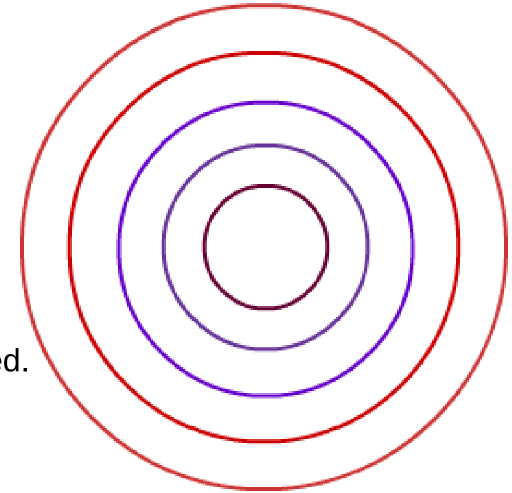
https://access.atis.org/apps/group_public/download.php/32237/ATIS-1000074.pdf

http://www.sipforum.org/component/option,com_docman/task,doc_download/gid,833/Itemid,261/

- **Phase 2** will define our recommendations for the Governance Model and Certificate Management for the Trust Anchor. That work will be completed within weeks.

- **Phase 3** will be the Call Validation Display Framework that will make recommendations to industry on how the STIR/SHAKEN process can be displayed to consumers. In addition, the Call Validation Display Framework could make voluntary recommendations on additional information displayed to the consumer such as enhanced caller identity or CNAM-like information that could display relevant information.

Issues for the U.S. [FCC] Specifically to Resolve



- How will the Certificate Trust Anchor be constituted?
  - By who? Under what governance and by what statutory authority?
  - How much will it cost? *It better be small.*
- There will have to be a Policy on who gets X 509 credentials and why.
  - The running theory in the U.S. is use of the NECA Operating Carrier Number [OCN] as well as direct access to the NANP. Alternatively SIPD / Alt-SPID. It will be controlled.

- Implementing SHAKEN/STIR for Cable Operators UCaaS is easy...not so easy for incumbents.
  - Are there privacy issues in inter-carrier data sharing and data analytics related?
- Obligations of OTT providers?

- Are there Legislative issues that need to be addressed?
  - The U.S. “Truth in Caller ID” Act is an oxymoron. Telephone Consumer Protection Act.
    - Proof of ‘intent’ to defraud is very difficult to prosecute.

We Need Your Help!

The SIP Forum and ATIS have a Joint Venture on Network to Network Interfaces.

We have 3 Classes of Membership: Full (Corporate) Members that financially support the Forum's activities [Paid], and Participant (Individual) Members [Free] and Academic Members [Free].
Please see me about Full Membership!!

Through the SIP Forum, ANY Operator and its supplier ecosystem can participate in the ongoing 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 TF Landing page

http://www.sipforum.org/content/view/439/312/