Mitigation Techniques for Unwanted Robocalls: *Updates on ATIS and Other Key Industry Initiatives*

Moderator

Jim McEachern, Senior Technology Consultant, ATIS

Panelists

Martin Dolly, Lead Member of Technical Staff, AT&T

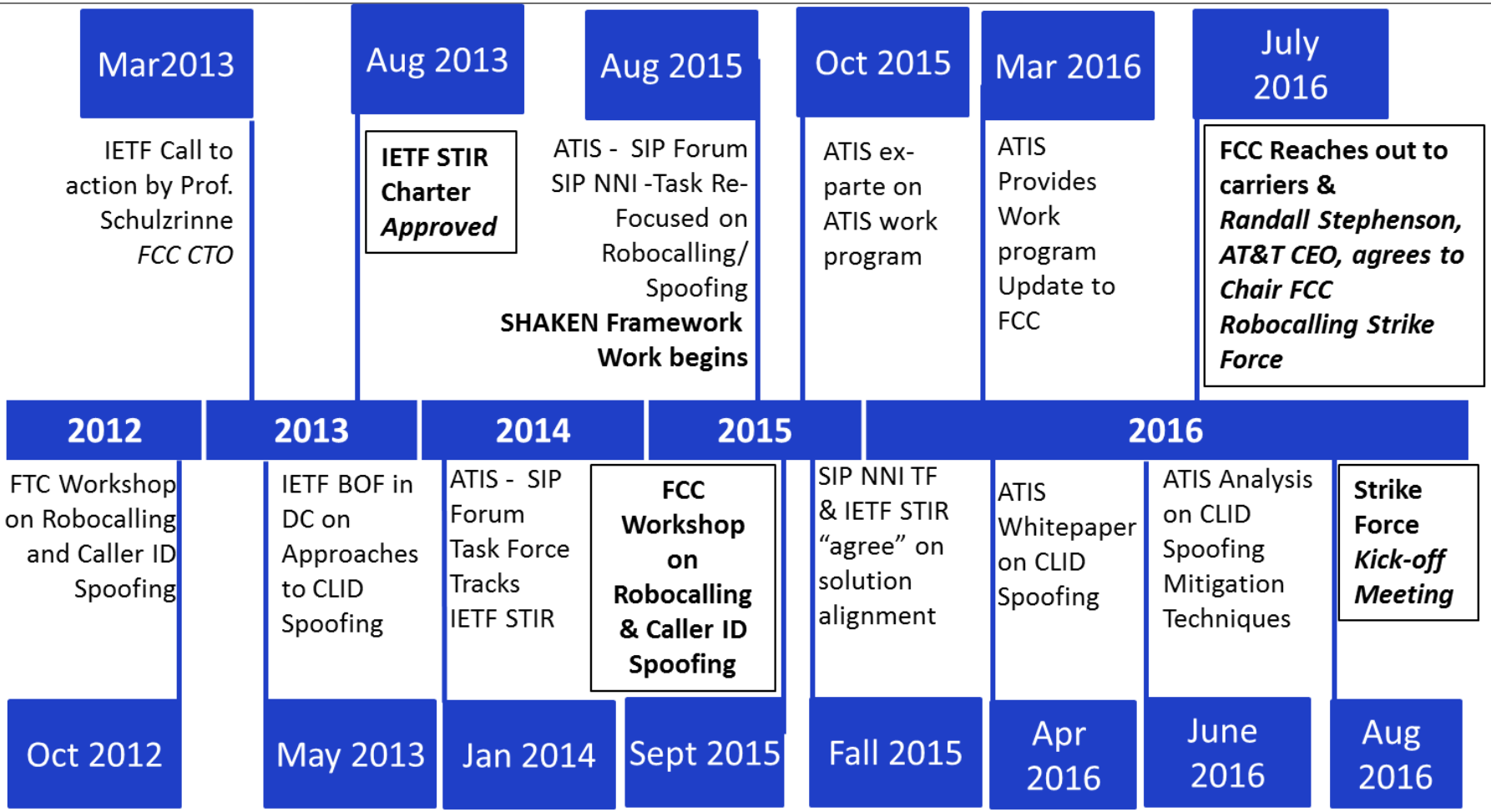
Gary Richenaker, Principal Solutions Architect, iconectiv

Chris Wendt, Director, Technical R&D IP Communications, Comcast

Background

- Caller-ID spoofing and the related issue of robocalling are under increasing scrutiny from regulators, legislators, consumer advocacy groups, and the media in general.
- ATIS programs address the full range of techniques to support effective anti-spoofing strategies providing users with meaningful mitigation techniques.
- ATIS efforts in support of reducing unwanted robocalling and caller-ID spoofing have gained additional recognition with the launch of the FCC Robocalling Strike Force in August.

Robocalling/ Spoofing Timeline



4

Standards Update: ATIS & 3GPP

Martin Dolly

Lead Member of Technical Staff

AT&T Core Network & Gov't/Regulatory Standards

Spoofed Calls Versus Robo-Calling

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.

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
- http://stakeholders.ofcom.org.uk/binaries/market-data-research/Ofcom_VoIP_RPKI_Report.pdf
- U.S. Congress had endless hearings
- https://energycommerce.house.gov/hearings-and-votes/hearings/modernizing-telephone-consumer-protection-act
- 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 U.S. CA EU

ATIS PTSC

Calling Party Spoofing Technical Assessment

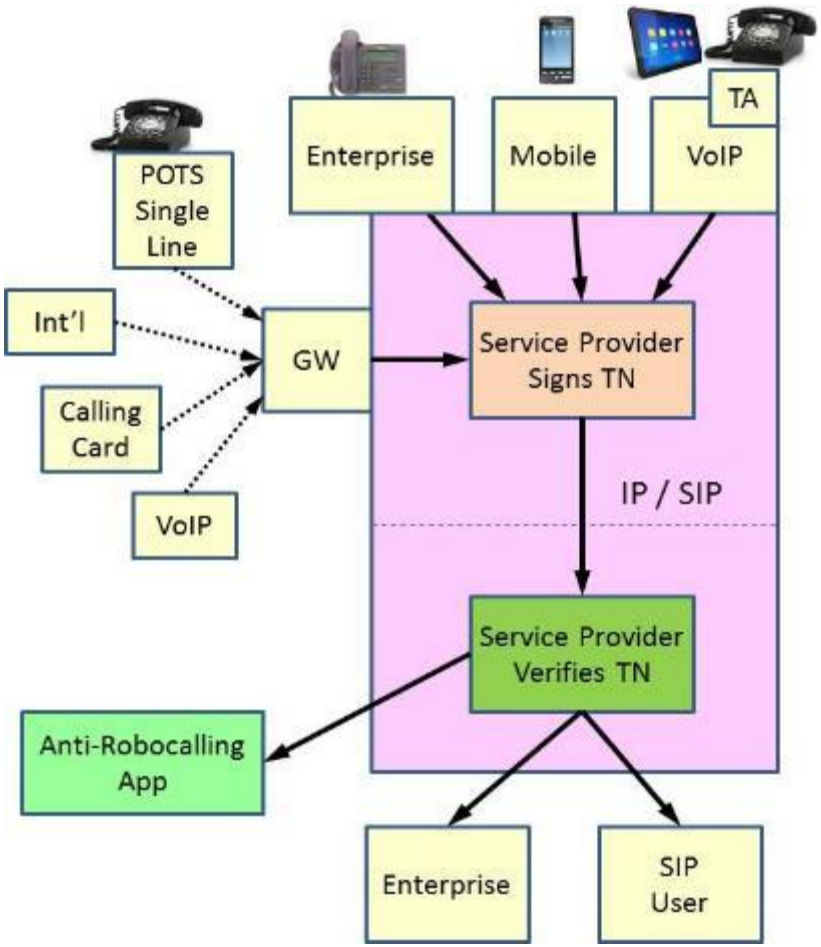
- Just like with Cybersecurity, protection against robo-calling/spoofing has no silver bullet and can only be realized by a layered approach of mitigation techniques.
- Even with the deployment of the STIR/SHAKEN Framework, traffic from CS originations and IP Gateways (International & Wholesale) will be an issue for robo-calling/spoofing, therefore deployment of other mitigation techniques in a layered approach is required.
- Everyone has a role in the fight against Calling Party spoofing:
  - Federal Trade Commission in prosecuting bad actors.
  - The carriers in deploying an appropriate layering of mitigation techniques to protect their customers. These include mitigation techniques provided by 3rd party platform/services facilitated by the serving carrier.
  - Consumers in managing their communications. Remember only the consumer can chose to block a call/session on a per call/session basis, or give permission to the carrier or 3rd party on their behalf.

ATIS PTSC - Calling Party Spoofing Technical Assessment

The layered approach of mitigation techniques needs to consider the following:

- Deployment of the STIR/SHAKEN framework.
  - The STIR/SHAKEN framework will provide a positive verification to the user that they can trust the Caller ID information received. WTS it does not address CS origination/termination.
  - In addition, the framework can be used to identify the source of the traffic is coming from an international gateway, and the customer with this knowledge and the number can chose to receive the call or not.
  - The STIR/SHAKEN framework can be initially deployed using service provider managed certificates as a more comprehensive and automated certificate management and the policy around them is enhanced.
- Some form of post call reporting is a MUST, whether via a web portal, call center, or in/post-call signaling (e.g., *xx or indication in SIP BYE) to the terminating carrier or FTC, where appropriate and aligned with CPNI rules.
- Operationalize CDR tracing which provides a mechanism for identifying the source of the Calling Party spoofing in both CS, PS and across CS-PS domains. Though parts maybe automated, it is mainly a manual process to start.
- Do Not Originate (DNO) servers should be deployed at IP gateways, where the gateway blocks numbers that “should not be there” (e.g., 911 DNC List, Government agencies).
- Blacklist/Whitelists are useful, but require data analytics to be effective.
- Service Provider verification of numbers originating from IP PBXs. Likely performed by the Service Provider’s business subscriber Application Server.

STIR/SHAKEN Limitations

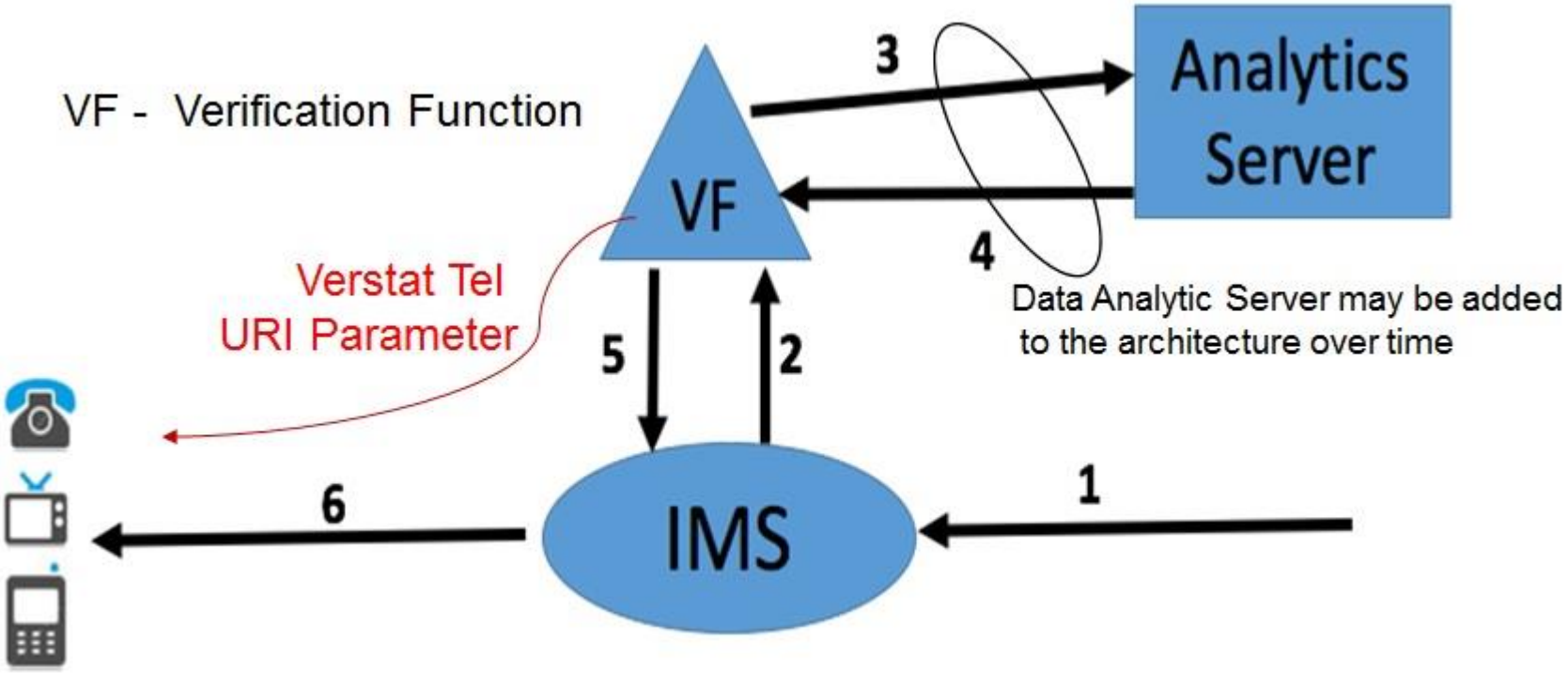


- STIR can be used to validate SIP calls in real-time or to trace calls after the fact.
- GW may sign its identity for traceability purposes, without verifying calling number.
- Calls from outside SIP network cannot be verified.
  - Domestic SIP only
  - No support for TDM

Standard References

- IETF STIR Draft RFCs, https://datatracker.ietf.org/wg/stir/documents/
  - Authenticated Identity Management in the Session Initiation Protocol (SIP)
    - draft-ietf-stir-rfc4474bis-12
  - Persona Assertion Token
    - draft-ietf-stir-passport-07
  - Secure Telephone Identity Credentials: Certificates
    - draft-ietf-stir-certificates-08
  - SIP Call-Info Parameters for Labeling Calls
    - draft-schulzrinne-dispatch-callinfo-spam-00
  - A SIP Response Code for Unwanted Calls
    - https://datatracker.ietf.org/doc/draft-schulzrinne-dispatch-status-unwanted/
- ATIS – SIP Forum Task Force
  - Signature-based Handling of Asserted Information Using Tokens (SHAKEN)
- ATIS
  - ATIS Technical Report on the use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information
- 3GPP
  - SA1 Service Requirements – CRs Approved
  - CT1 WID and CR to TS 24.229 – signaling verification status, WID & CR in progress
  - CT 1 CRs to TS 29.165 for NNI & X for Verification/Authentication Service Functions

Signaling Verification and Analytics Info



Note: Interface between VF and Data Analytics Server is outside Industry Standards and may not be available in initial deployments
& Some Analytics may be performed in the network element that performs the VF

Signaling Verification

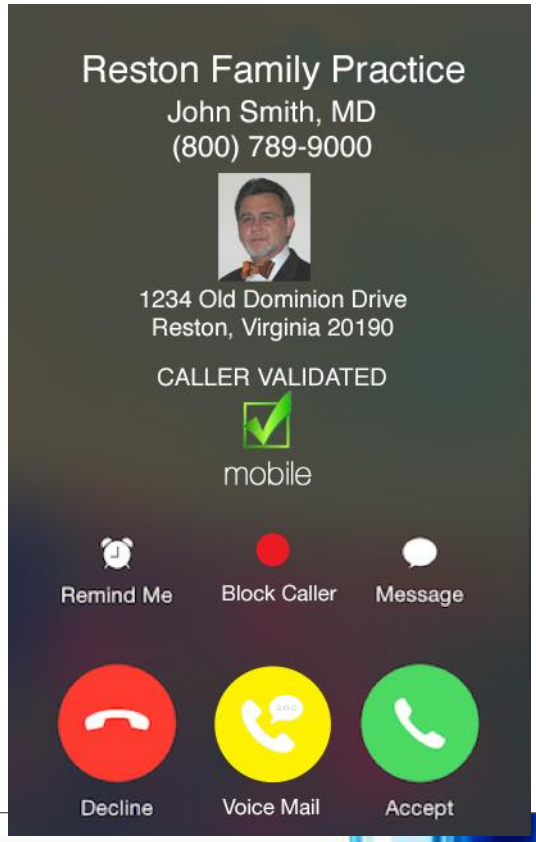
- Verstat
  - TN Validation Passed
  - TN Validation Failed
  - No TN Validation
  - Future: same values above for CNAM

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

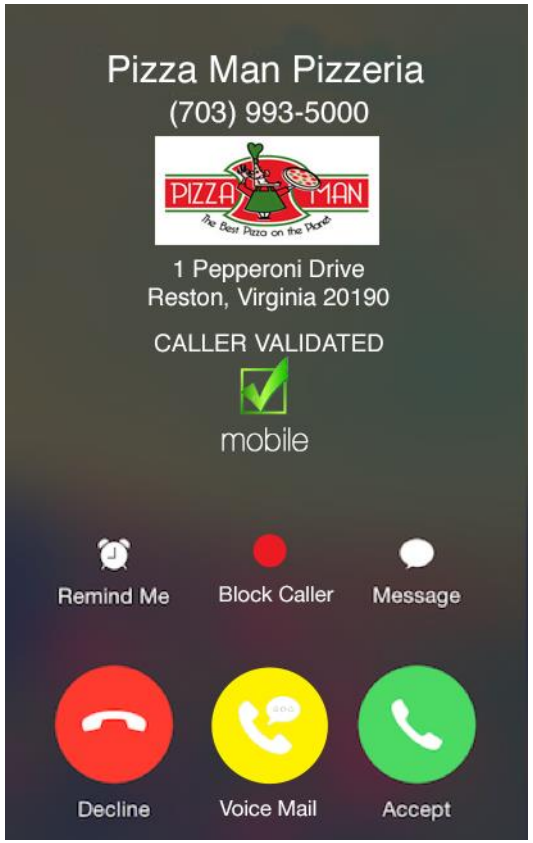
Display to the User – *for illustration only*

- **IP-NNI TF is developing a Technical Report** that provides a framework for signaling verified Caller ID information from the network to a User Equipment (UE), and displaying the information on the UE in a uniform manner, independent of technology.
- **Enhanced Validation User Display Options from the network. [Good Call]**
  - Existing User Display is limited to 15 Character ASCII for CNAM.
- **Now we can do anything**
  - Caller ID can display an extended name (up to 35 characters), a picture or the type of business based on eCNAM developed under ATIS PTSC.
  - Calling party can display alternative numbers to protect Doctors' privacy when returning patient calls
  - Protect GETS users or Emergency Personnel from revealing their true Calling Party Number.



Display to the User – *for illustration only*

Enhanced User Display



Other Considerations

- Useful indication of the caller's Authentication Assurance
- Indicator provided by the authentication service to provide the information it knows about how the call was originated

Standards Update: STIR Testbed

Gary Richenaker

Principal Solutions Architect

iconectiv

Testbed Focus

Business Problem:

- Individual testbeds duplicate many functions and are inefficient to implement and maintain.
- Industry transition initiatives call for testbeds to validate solutions or provide proof of concept in all-IP migration and to facilitate interoperability testing between providers.

Scope of Work:

- Evaluate existing testbed activities to identify common requirements and recommend a path forward in the following areas:
  - Numbering, routing, and authenticated caller-ID

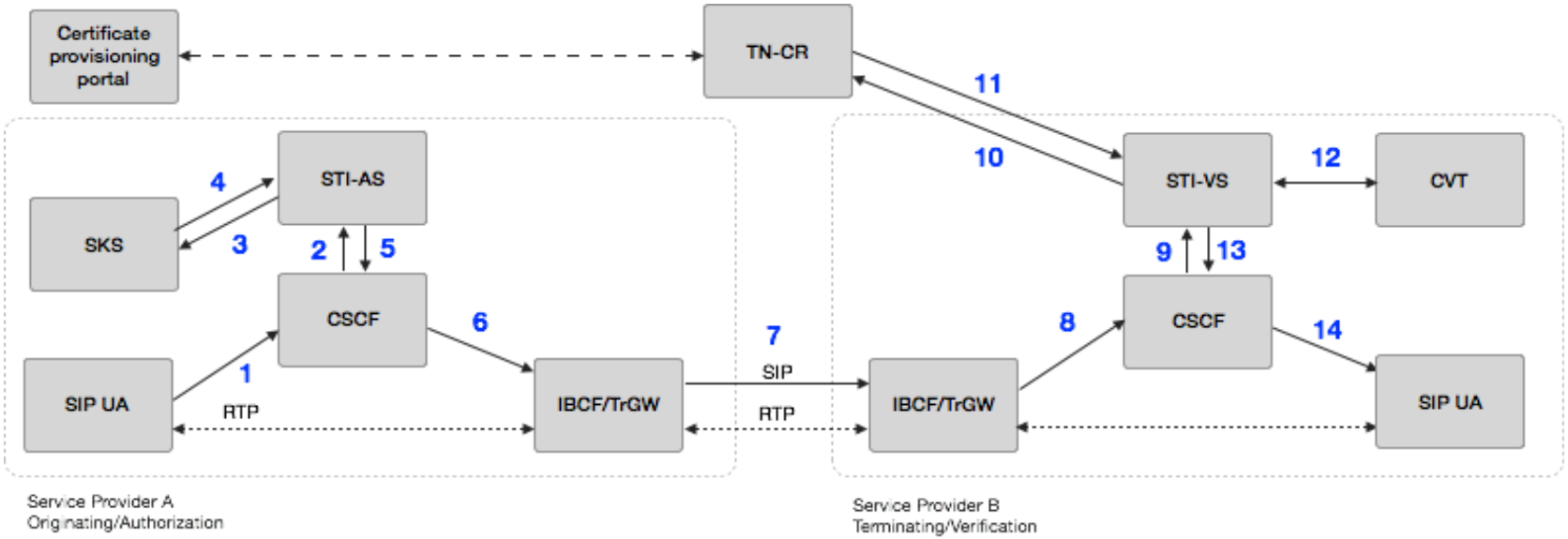
Testbeds Focus Group: Status

- Developed high-level, phased, test plans associated with each of approved use cases:
  - Phase 1 *(completed):*
    - High-level system description of each use case
    - Reference architecture and core components
    - High-level test plans
  - Phase 2:
    - NDA created and approved for testing participation
    - Detailed test plans *(in progress)*
  - Phase 3:
    - Intra-carrier and inter-carrier tests *(next step)*
  - Phase 4:
    - Reports

Test Case Scenarios – Initial Focus

- Will finalize test plans and begin testing on scenarios with multiple participants:
  - Number Assignment: Distributed Service Bureau
  - Number Assignment using existing systems
  - LERG Routing Guide IP Enhancements
  - STIR protocols for end-to-end SIP calls
- Tests will occur in phased approach each with its own timeline.
- Proposed initial focus will validate STIR / SHAKEN:
  - Align with Calling Party Anti-Spoofing Landscape Team's next steps
  - Support ATIS/SIP Forum IP-NNI Task Force protocol work
  - Provides clear business value to ATIS members

Call Flow for Testing



- Based on IMS Architecture.
- Represents new call flow and changes to SIP signaling.

Next Steps

- Phase 2 - continue work on finalizing test plans:
  - Test plans will be living documents
  - Soliciting additional industry participation
- Phase 3 - conduct tests:
  - Validate the protocol – initial testing has begun
  - Test that it works in realistic network configurations
  - Provide proof of concept
  - Late 2016 into 2017, depending on lab availability
- Phase 4 - issue reports:
  - Results will be documented and shared with the industry upon completion of Tests

Standards Update: IETF/NNI Task Force Protocols

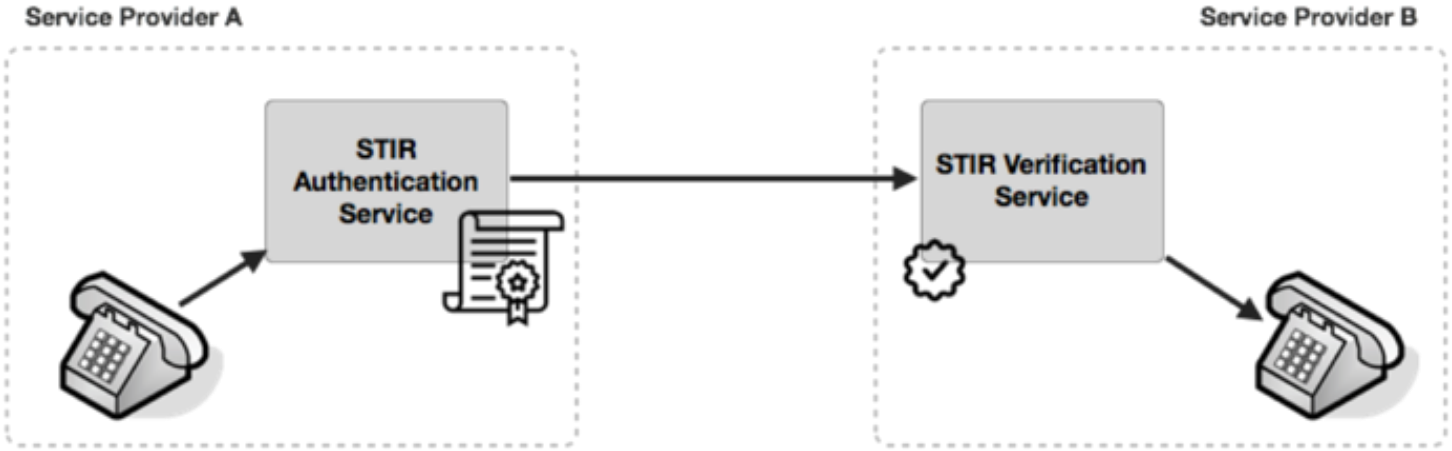
Chris Wendt

Director, Technical R&D IP Communications

Comcast

Overview

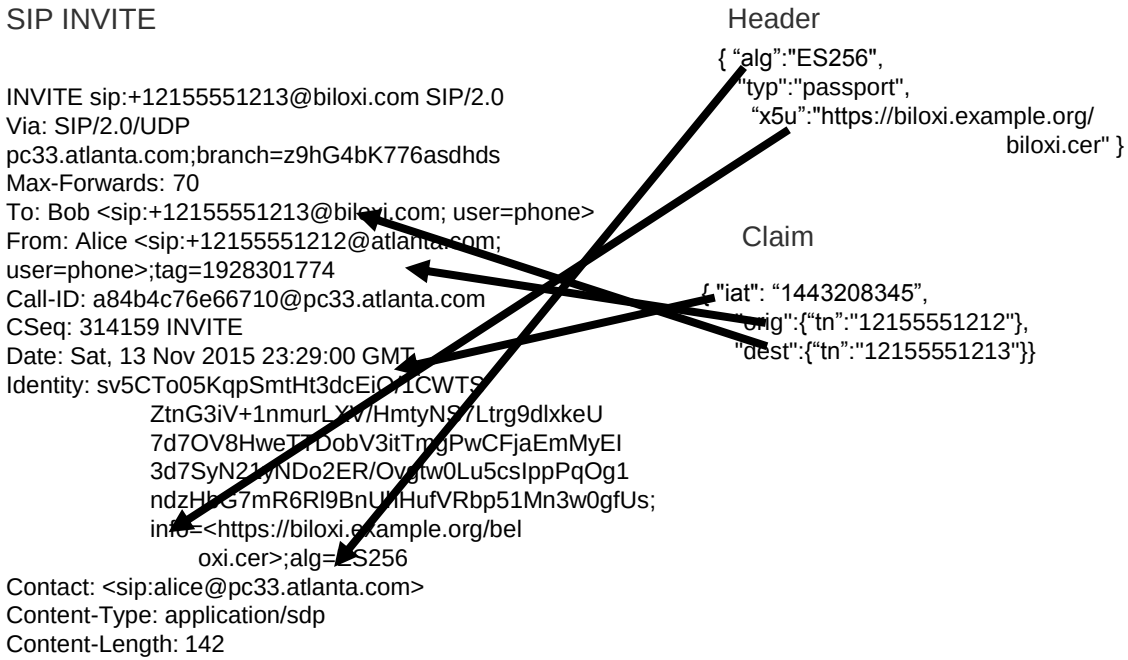
- Two key industry standards activities related to VoIP calls:
  - IETF STIR - defining core protocols and technologies for SIP and certificate usage for applying digital signatures to validate the telephone identity of the calling party
  - ATIS/SIP Forum SHAKEN - defining the industry framework for using STIR technologies and how service providers will interwork on VoIP based calls



PASSporT and 4474bis Overview

- PASSporT uses the JSON Web Token (JWT) and JSON Web Signature (JWS) formats and defines a standard set of base claims and signature.

- rfc4474bis defines how PASSporT is used in a SIP message defining the identity header.



SHAKEN PASSporT Extension – Attestation and Originating Identifier

- SHAKEN has defined a “shaken” PASSporT extension with two defined claims.
- Attestation (“attest”):
  - Provides an attestation indicator representing the level of attestation a service provider can give to its knowledge of the legitimacy of the calling identity
- Originating Identifier (“origid”):
  - Is a UUID opaque identifier that a service provider uses to indicate a particular originating trunk, node, or customer as a mechanism for automated traceback as well as call reputation correlation

SHAKEN PASSporT Extension – Attestation and Originating Identifier

- **Attestation (“attest”)** - The service provider will classify the origination of the call into one of three categories:
  - **”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.
  - **“B” Partial Attestation**: The signing provider:
    - is responsible for the origination of the call onto its IP based voice 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 its IP based voice network
    - has no relationship with the initiator of the call (e.g., international gateways).

SHAKEN PASSporT Extension – Attestation and Originating Identifier

Example PASSporT claims with SHAKEN extension:

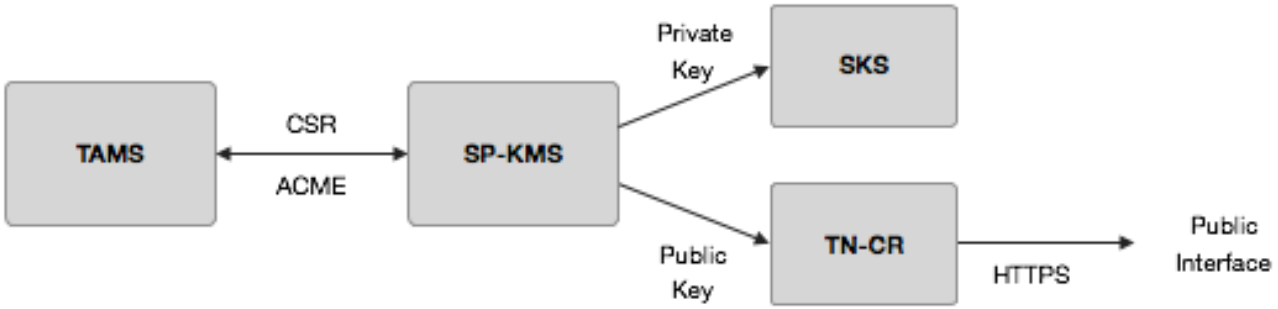
PASSporT Header

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

PASSporT Payload

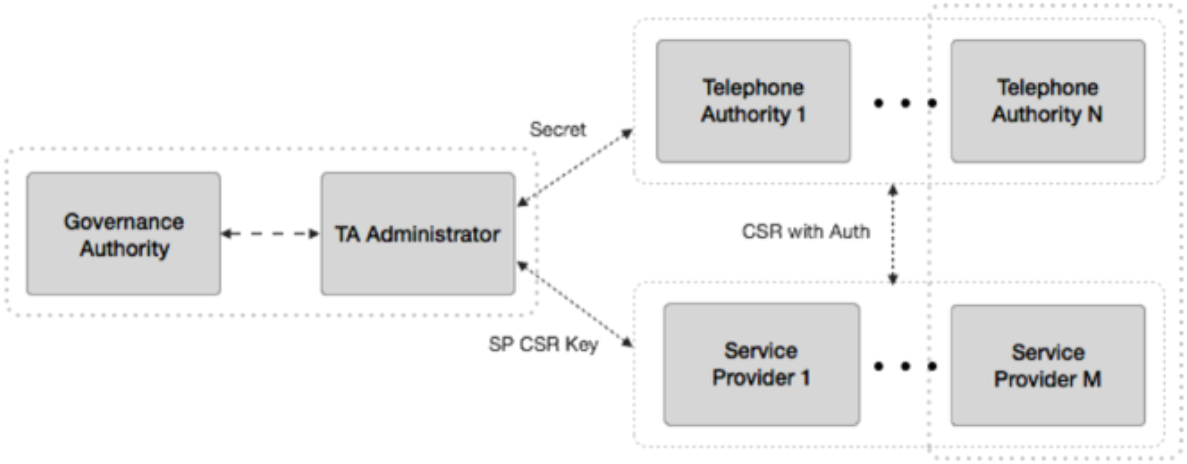
```
{
   “attest”:”A”,
   "dest":{“tn”:"12155551213"},
   “iat”:"1443208345",
   “orig":{“tn”:"12155551212"},
   “origid”:”123e4567-e89b-12d3-a456-426655440000”
}
```

SHAKEN - Telephone Authority Certificate Management



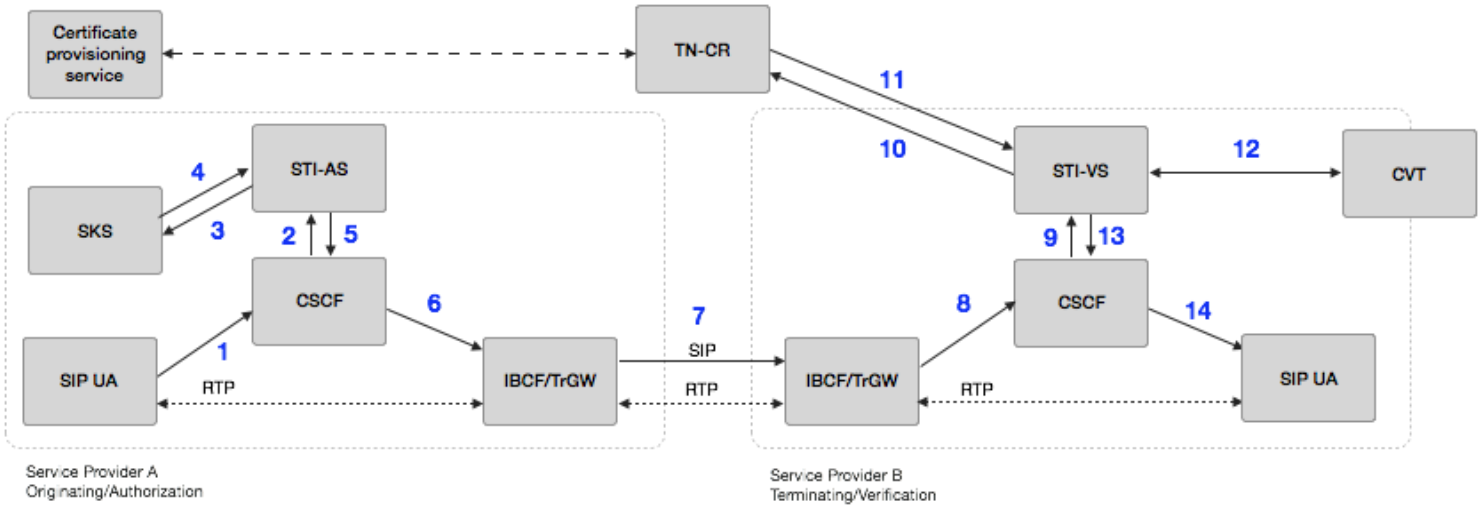
- Reference architecture
- Telephone Authority is the function that is authoritative for signing STIR certificates for VoIP telephone network based on X.509 standard certificate management
- Associated with an “authority” for assertion of the ownership of either telephone numbers or the authorization to perform telephone call routing

SHAKEN – Certificate Governance Model



- **Governance Authority** - this entity would manage, likely tied with identification and potential prosecution of bad actors, the authority for service providers to originate signed calls to the telephone network.
- **TA Administrator** - this entity would do the manual process of working with service providers to validate they are who they say they are and manage credentials of Telephone Authorities to have a secret key and the Service Providers to do CSR transactions with the Telephone Authorities. They should also have a periodic re-validation and new key issuance, as part of good practice to protect the Telephone Authority services.
  - Note: Governance and Administration are two logical functions but could be supported by a common low administrative overhead organization.
- **Telephone Authorities** - Can process automated CSR requests via ACME protocol from Service Providers creating new certificates.
- **Service provider** - Own and manage a SP certificate key, that they must have signed by TA.

STIR/SHAKEN Basic Call Flow



- Originate Call on UE, Authentication constructs 4474bis/PASSporT signature and adds identity header to SIP INVITE.
- Terminating network receives INVITE, fetches public key certificate from HTTPS URL in x5u claim and uses Validation Service to validate signature.
- In addition, there are other mitigation techniques that can be used to perform service provider specific CVT (Call Validation Treatment).

Thank you for attending
Mitigation Techniques for Unwanted Robocalls

All registered attendees will receive a follow up email containing links to a recording and the slides from this presentation.

For information on upcoming ATIS events, visit

www.atis.org/events