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.
- Robocalls & Spoofing is the #1 complaint to the CRTC in Canada
- Robocalls & Spoofing is the #1 complaint to OFCOM and the UK ICO
- 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.
  - US Congress had endless hearings.
- 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
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
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 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

- Certificate provisioning service
- TN Certificate Repository
- Secure Key Store
- Authentication Service Function
- Verification Service Function
- Call Validation Treatment
- SIP UA
- RTP
- 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
<table>
<thead>
<tr>
<th>Year</th>
<th>Month</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Feb</td>
<td>ATIS launches testbed to advance mitigation of unwanted robocalling and caller ID fraud</td>
</tr>
<tr>
<td></td>
<td>July</td>
<td>ATIS-1000080.v002: Signature-based Handling of Asserted information using tokens (SHAKEN): Governance Model and Certificate Management</td>
</tr>
<tr>
<td></td>
<td>May</td>
<td>ATIS-1000081: TR on Framework for Display of Verified Caller ID</td>
</tr>
<tr>
<td></td>
<td>Aug</td>
<td>Industry groups select ATIS as the STI-GA. The GA was officially launched</td>
</tr>
<tr>
<td></td>
<td>Nov</td>
<td>ATIS tested findings validate SHAKEN protocol's effectiveness in mitigating unwanted robocalling</td>
</tr>
<tr>
<td></td>
<td>Dec</td>
<td>Request for Proposal (RFP) issued for Secure Telephony Policy Administrator (STI-PA) role</td>
</tr>
<tr>
<td>2018</td>
<td>Feb</td>
<td>ATIS-1000085, SHAKEN Support of &quot;div&quot; PASSportT</td>
</tr>
<tr>
<td></td>
<td>Aug</td>
<td>ATIS-1000084, Errata to Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrative</td>
</tr>
<tr>
<td></td>
<td>Nov</td>
<td>ATIS-1000080-E, Errata to Signature-based Handling of Asserted information using tokens (SHAKEN): Governance Model and Certificate Management</td>
</tr>
<tr>
<td></td>
<td>Dec</td>
<td>ATIS-1000074-E, Errata on ATIS Standard on Signature-based Handling of Asserted information using tokens (SHAKEN)</td>
</tr>
<tr>
<td></td>
<td>Aug</td>
<td>STI-GA executes contract with iConnect as STI-PA</td>
</tr>
<tr>
<td></td>
<td>Dec</td>
<td>Target to have the STI-PA operational</td>
</tr>
</tbody>
</table>
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 (ÇN) Subsystem (IMS) and MSC Server for IMS Centralized Services (ICS)
<table>
<thead>
<tr>
<th>Title</th>
<th>Document ID</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature-based Handling of Asserted information using toKENs (SHAKEN)</td>
<td>ATIS-1000074.v003</td>
<td>IPNNI-2019-00130R003</td>
</tr>
<tr>
<td>Verification Token Use Cases</td>
<td>IPNNI-2017-00020R000</td>
<td>Living Document</td>
</tr>
<tr>
<td>Robo-Metrics</td>
<td>IPNNI-2018-00083R001</td>
<td></td>
</tr>
<tr>
<td>SHAKEN Roadmap</td>
<td>IPNNI-2019-00140R000</td>
<td></td>
</tr>
<tr>
<td>SHAKEN Delegate Certificates</td>
<td>IPNNI-2019-00129R000</td>
<td></td>
</tr>
<tr>
<td>SHAKEN Calling Name and Rich Call Data Handling Procedures</td>
<td>IPNNI-2019-00024R001</td>
<td></td>
</tr>
<tr>
<td>Best Current Practices on the protection of STIR/SHAKEN data between service providers and from service providers to enterprises</td>
<td>IPNNI-2019-00055R000</td>
<td></td>
</tr>
<tr>
<td>Considerations for Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)</td>
<td>IPNNI-2019-00056R013</td>
<td>PTSC-LB-242_d</td>
</tr>
<tr>
<td>Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements</td>
<td>IPNNI-2019-00075R005</td>
<td></td>
</tr>
<tr>
<td>Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange</td>
<td>IPNNI-2019-00102R004</td>
<td></td>
</tr>
<tr>
<td>ATIS Standard on Signature-based Handling of SIP RPH Assertion using Tokens</td>
<td>IPNNI-2019-00132R000</td>
<td>PTSC Issue S0150</td>
</tr>
</tbody>
</table>
Thank you.