**ATIS-0x0000x**

ATIS Technical Report on

**Study of Full Attestation Alternatives**

**for Enterprises and Business Entities**

**with Multi-Homing and Other Arrangements**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This Technical Report is being developed to define the principles that should be adhered to in order to attain full attestation in the event there is no naturally verified association available to the OSP regarding the customer and the use of a TN as the Caller ID .

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The ATIS SIP Forum **IPNNI**  Joint Task Force Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| June 19, 2018 | Initial | Baseline | Gary Richenaker |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope

SHAKEN is defined as a framework that utilizes protocols defined in the IETF Secure Telephone Identity Revisited (STIR) Working Group that work together in an end-to-end architecture for the authentication and assertion of a telephone identity by an originating service provider and the verification of the telephone identity by a terminating service provider.

There are conditions where the originating Service Provider cannot fully attest to the authenticity of the Telephone Number. This Technical Report will provide use cases where there may be a “knowledge gap” in attaining the highest level of Attestation; A.

This document is focused on Caller ID attestation and does not address calling party name, intent nor reputation.

This document is not intended to provide an exhaustive set of Use Cases covering every potential calling pattern that could require supplementary techniques beyond core SHAKEN Identity passports but nonetheless captures a broad representative sample of the scenarios where additional capability is needed to get Enterprises and other Business Entities a full attestation of the Caller ID. These Use Cases and flows are illustrative and it is not intended to provide a standard mechanism to raise the Attestation level. The capability of a business entity to support one mechanism versus another to close the attestation knowledge gap will vary thus a suite of mechanisms are likely warranted. This document will capture the principles that should be adhered to in order to attain full attestation in the event there is no naturally verified association available to the OSP regarding the customer and the use of a TN as the Caller ID. Various mechanism are provided in an Annex with associated impacts to signaling, TNSP, OSP, and TNSP.

# Purpose

Operating and business policies for the various users (SPs, Enterprises/Business Entities, and Resellers) of the Telecom Ecosystem are variable and situation driven. Oftentimes, the Originating SP does not have a verified association between the customer and the Caller ID presented for all the customer’s calls.

In the SHAKEN framework, ATIS 1000074, Full Attestation is defined as follows:

**A. Full Attestation:** The signing provider shall satisfy all of the following conditions:

* 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.

This Report will define the principles for any techniques that might supplement SHAKEN attestation as well as identify the use cases where such techniques may be required to mitigate this attestation knowledge gap and identity the impacts with each of the different mechanisms. .

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

# Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

## Definitions

Authoritative Directory: A data store of TNs and their verified association to the TN customer and which is populated by authorized parties.

Telephone Number Customer (TN Customer): Entity (e.g., enterprise, VoIP Provider, Over the Top Provider, hosted/cloud communications provider, etc.) that has been given the authority to use TNs by virtue of having been assigned these TNs by an authorized party.

Hosted/Cloud Service Provider: Entity providing telephony services for multiple business entities, either using Caller ID numbers supplied by them to the business entity or provided by the business entity in a Bring Your Own Number (BYON) model. These include hosted PBX, Unified Communications providers, Communications Platform as a Service (CPaaS) providers, Contact Centers, etc.

Originating Service Provider (OSP): The service provider that handles the outgoing calls at the point at which they are entering the public network. The OSP performs the SHAKEN Authentication function. OSP may also serve in the role as TNSP, RespOrg and other roles.

OTT Provider: Entity providing telephony services for end users via Over the Top (OTT) mechanisms and which require PSTN interworking in order to support calls to traditional called parties on the public network. Similar to cloud service providers, these entities may provide TNs to their customers or support BYON capabilities.

RespOrg: A Responsible Organization is an entity authorized by the FCC to assign toll free numbers to Customers. A RespOrg may also be a service provider, a TN Reseller as well as act in other roles.

Telephone Number Service Provider (TNSP): SP that has been formally assigned TNs by the national numbering authority (e.g., NANPA). A TNSP may assign a subset of its TNs to a business entity (aka TN Customer), to be used as Caller ID for calls originated by the business entity. TNSPs can also serve in the role as OSP or TSP.

Terminating Service Provider (TSP): the SP whose network terminates the call (i.e., serving the called party). The TSP performs the SHAKEN Verification function.

TN Reseller Service Provider: Entity that is assigned TNs by a TNSP and in turn provides those TNs to various entities (e.g., contact centers, cloud providers, OTT providers) that behave as TN Customers or may also resell TNs to other TN Resellers who serve those customer entities. Reseller SP may also serve in the role of other SP types.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions  SIP Forum |

# Principles

The following core principles should be adhered to in order to attain full attestation in the event there is no naturally verified association available to the OSP regarding the customer and the use of a TN as the Caller ID:

1. Service Providers must adhere to SHAKEN criteria for attestations A, B and C.
2. Any enhancements required to SHAKEN passport fields and certificates must be standardized by the ATIS/SIP Forum IP NNI Task Force.
3. Service provider local policy dictates the mechanisms that are sufficient for an OSP to attest fully to a “legitimate right to assert a telephone number” for a given call.
4. OSPs will always send a SHAKEN passport attesting to the validity of the TN independent of if upstream business entities sign their own calls using certificates.
5. OSPs will be able to audit the mechanism(s) used to establish authorization for a customer to use specific TNs as the customer Caller ID for industry traceback purposes.
6. TNSPs and RespOrgs are authorized issuers of TNs to business entities and can vouch for a customer’s right to use a given TN as their Caller ID.
7. Verification of possession of a TN can be a means to vouch for a Hosted/Cloud and other providers’ authority to use specific TNs as the customer Caller ID for BYON and other use cases.
8. TSPs MUST verify the OSP is using a SHAKEN approved CA.
9. TNSPs should not require the TNs allocated to an OSP TNs match the certificate scope or this will preclude other mechanisms from enabling an OSP to make a full attestation.

The OSPs reputation and continued membership in the SHAKEN ecosystem may be directly dependent on how rigorously they have applied the above principles within their local policies regarding Caller ID attestation.

Editor’s Note: Participants should address the normative language and make it consistent throughout.

# Use Cases Scenarios

The Use Cases, detailed in Section 8, will include:

* Multi-homed Enterprise PBX
* OTT-PSTN interconnect
* Toll-Free originations
* Government
* Multi-tenant hosted/cloud PBX
* Unified Communications
* Contact Centers
* MVNOs (TBD)
* VoIP
* Other(s)?

Each of the Use Cases presented will have some similar and distinct issues. Therefore, various mechanisms may be applied in order to meet the objective of attaining the highest level of Attestation.

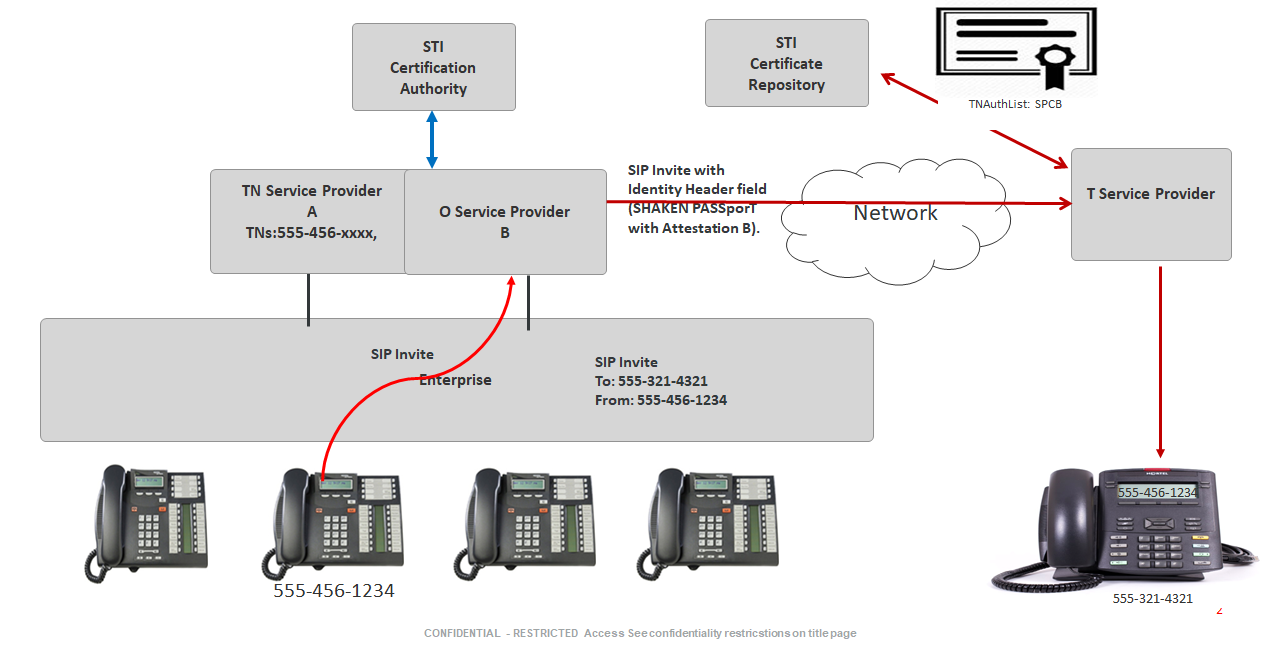
# Use Case Flows

The following Use Cases define the problem where in the SHAKEN ecosystem the Originating SP does not have a verified association between the customer and the Caller ID presented for all the customer’s calls and would therefore Attest to the call as B.

In this Section no mechanism are proposed, the Use Cases are to highlight the problem. The Annex in this report provides various mechanism and associated impacts with each Use Cases.

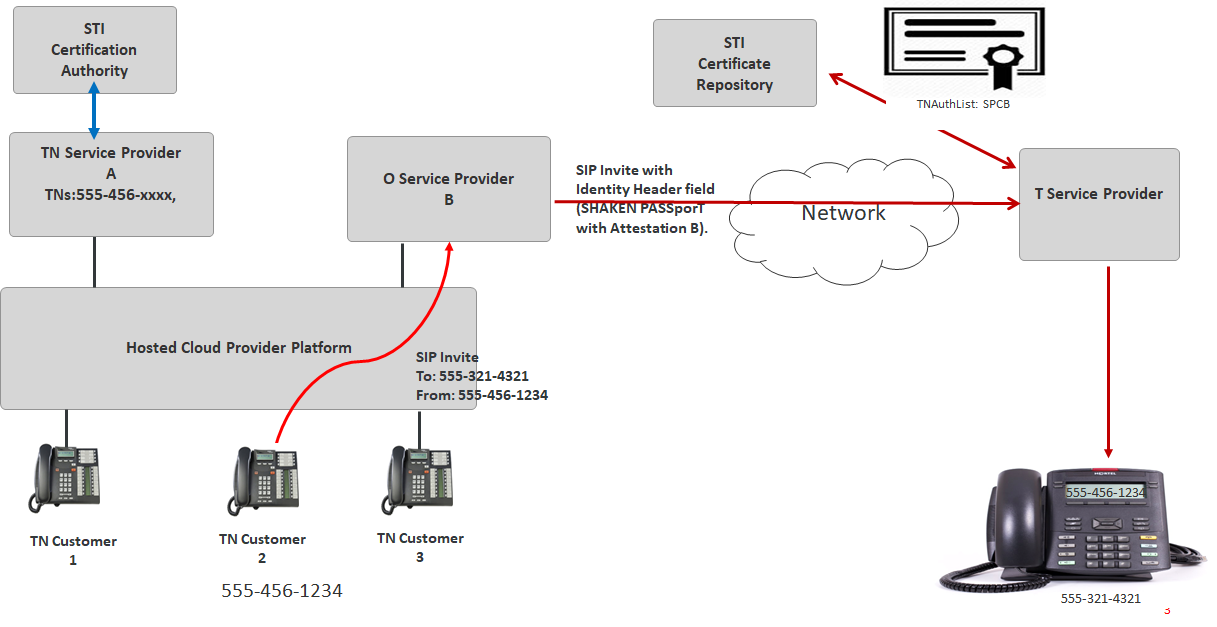
## Use Case 1 – Multi-Homed Enterprise/Government with On Premise PBX,

The TNSP and OSP are different Service Providers. Normally under SHAKEN definitions this call would receive an Attestation B since OSP B is not the TNSP.



1. TN Customer with TN 555-456-1234 assigned by TNSP A dials 555-321-4321
2. OSP B can not authenticate the TN
3. OSP B adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to B
4. The PASSporT is signed using an STI-Certificate with a TNAuthlist containing a single SPC with a value assigned to OSP B

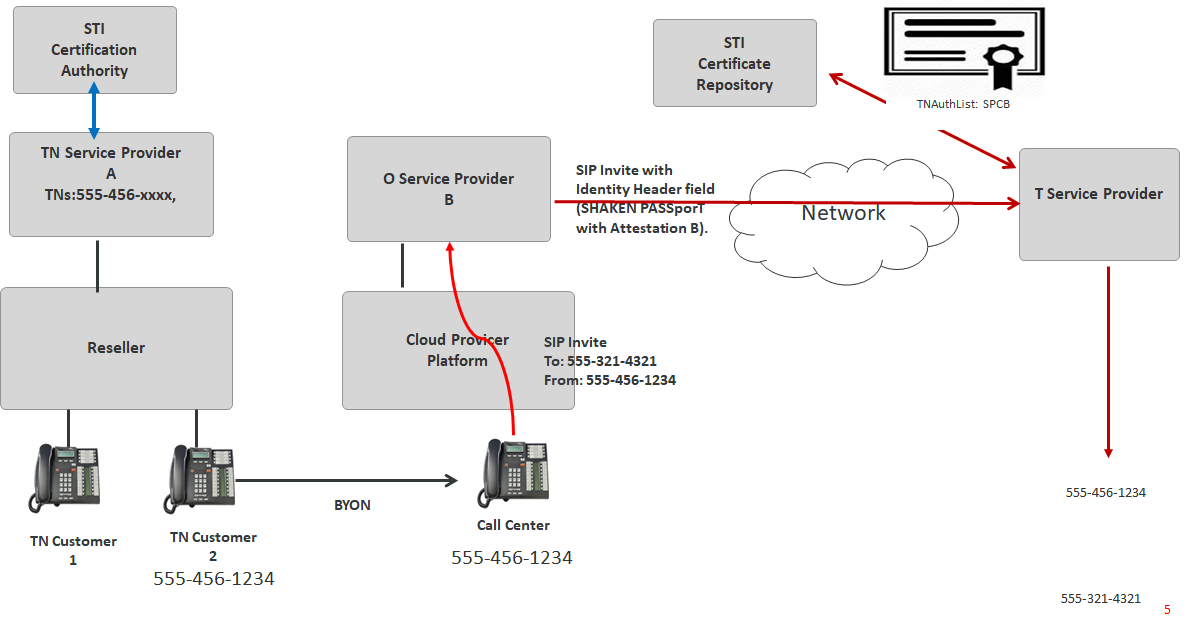
## Use Case 2 – Multi-Tenant Hosted/Cloud PBX, OTT to PSTN, Unified Communications, and or Other Cloud Communication Platform



1. TN Customer 2 with TN 555-456-1234 assigned by Cloud Provider (Not BYON) who obtained the TNs from TNSP A dials 555-321-4321. TN Customer 2 originates call to OSP B through the Hosted Cloud Provider
2. OSP B can not authenticate the Caller ID.
3. OSP B adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to B
4. The PASSporT is signed using an STI-Certificate with a TNAuthlist containing a single SPC with a value assigned to OSP B

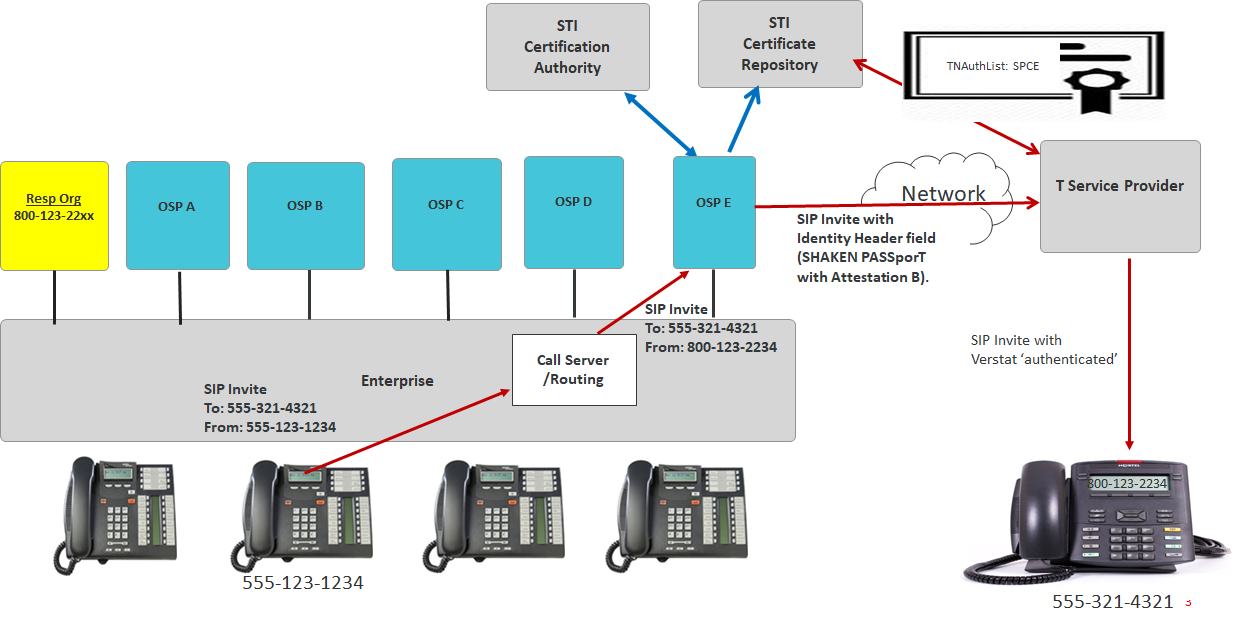
## Use Case 3 – Contact Centers, BYON

BYON applies to Use Cases UCaaS/CPaaS/OTT scenarios as an option



1. Call Center is provided TN 555-456-1234 (BYON) by TN Customer 2. This TN was obtained through a Reseller who obtained the TNs from TNSP A. Call Center dials 555-321-4321 and originates call to OSP B directly using TN Customer 2’s Caller ID and does not originate call through Reseller’s network
2. OSP B can not authenticate the Caller ID
3. OSP B adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to B
4. The PASSporT is signed using an STI-Certificate with a TNAuthlist containing a single SPC with a value assigned to OSP B

## Use Case 4 – Toll Free Originations (On Premise PBX, Hosted/Cloud Platform)



1. TN Customer with TN 555-123-1234 assigned by RespOrg, calls 555-321-4321 from 800-123-2234 using OSP E.
2. OSP E can not authenticate the Caller ID 800 Number.
3. OSP E adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to B. .
4. The PASSporT is signed using an STI-Certificate with a TNAuthlist containing a single SPC with a value assigned to OSP E.

(normative/informative)

# A Mechanisms to Address Use Cases

A major principle of any approach is to ensure integrity in a mechanism for full Attestation for business entities originating calls, even when the Originating Service Provider does not have a direct trust relationship with an Enterprise use of the TN.

This section is envisioned to identify approaches with a focus on what information is required, what makes it authoritative or sufficiently trustworthy, and how it is securely conveyed in order to enable the OSP to provide Attestation A. It is recognized that some enterprises may want to sign their own originations while others will not. A solution may require multiple mechanisms. In many cases, the Service Providers may need to provide most of the effort for the enterprises.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Mechanism  Options | Changes in SIP Signaling  Standards Impact | Impacts on OSP | Additional TN Customer Effort (i.e. Enterprise / Business Entity) | Impacts on TNSP | Impacts on TSP | Number Portability Impacts | Use Cases Addressed (when originator is capable) |
| Delegated Certificates  (certs provided by TNSPs) | Requires support for a new ID header per draft-ietf-stir-cert-delegation | OSP could ignore and leave TSP to handle this ID header  OSP can add a SIP ID header field (stacked ID headers)  OSP can terminate the delegated ID header and reconstruct in their own classic SHAKEN ID header | Obtains delegated certificate from TNSP and attaches SIP ID Header to calls.  Must sign each call using the delegate certificate from the TNSP who currently owns the TN | Maintains a CA delegated by one of the Trusted STI-CAs  Must keep TNAuth list within scope of owned TNs for all delegated certs. | May need to handle multiple SIP Identity header fields  Need to trust that originators are protecting their private keys. | Signer should use a delegated cert in each call provided by the correct TNSP owner for the TN.  Stakeholders may see certs used without proper ownership alignment until delegate cert expiry. | Multi-homed PBX & UCaaS,  Contact Ctr and CCaaS,  CPaaS,  OTT-PSTN calls,  Interconnected VoiP calls,  Wholesale traffic |
| LEMON Twist (certs provided by an STI-CA using TNSP authority token) | Optionally, introduce a new value for A’ attestation field | Same as delegated certs mechanism above | Obtains certificate per SHAKEN procedures from an approved CA, using an authority token provided by TNSP | Maintains TN assignment to EIDs for the upstream entity and provides them SPC tokens to authorize certificate requests from an STI-CA | Same as delegated certs mechanism above | Same as delegated certs mechanism above | Same as delegated certs mechanism above |
| Administrative Plane |  |  |  |  |  |  |  |
| TBD 1 |  |  |  |  |  |  |  |
| TBD 2 |  |  |  |  |  |  |  |