**ATIS-0x0000x**

ATIS Best Practice on

**Best Practices for Attestation for Enterprises and Business Entities**

**with Multi-Homing and Other Arrangements**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This Best Practices document defines the principles and provides use cases that enable business entities with multi-homed arrangement to be authenticated and authorized by the Originating SP with the highest level of attestation. These use cases are needed to support business entities when the authorized owner of a TN does not provide originating call services for that TN.

This Best Practices document is being developed based on several contributions that have been previously submitted providing Use Cases on Multi-Homed arrangements. It is an attempt to provide a comprehensive view of the options available to Service Providers, Enterprises and Business Entities due to the complexities of the Use Cases and that one single approach to all of these Use Case is not practical.

**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 XX, 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 Best Practices document will provide use cases where there may be a “knowledge gap” in attaining Attestation A and provide the principles in order guide SHAKEN signers’ decisions on local policy to close the knowledge gap and elevate the attestation where needed.

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. 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 to evaluate such mechanisms.

# 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. The purpose of this best practice document is to establish clear principles that would enable entities originating on networks without the requisite verified TN association, such as with multi-homed, multi-tenant, or other arrangements, to have the Caller ID authenticated by the Originating SP with full attestation.

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 Best Practices document 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. It is envisioned that this best practice document could encompass further contributions that assess a given mechanism against the principles. Including but not limited to delegated certificates, additional authoritative data, out of band mechanisms, or by other means.

# 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 customer and which is populated by authorized parties.

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 the TNs that the business entity (aka TN Customer) is using their Caller ID. TN Providers may also serve in the role as OSP.

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 SolutionsSIP Forum  |

# Principles

The following core principles represent best practices for 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 IP NNI Forum.
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. When upstream business entities sign their own calls using certificates, the OSP receiving that passport should verify and then replace that passport with a native SHAKEN passport. Upstream entity passports are not conveyed end to end without an accompanying SHAKEN passport signed by an OSP.
5. 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.
6. 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.
7. A Letter of Authorization (LOA) from the customer can be a means to vouch for a Hosted/Cloud provider and other entities’ authority to use specific TNs as the customer Caller ID for BYON and other use cases.
8. A Letter of Authorization (LOA) from the TNSP or RespOrg can be a means to authorize TN Resellers to vouch for a customer’s right to use a given TN as their Caller ID
9. A record of the mechanism(s) used to establish authorization for a customer to use specific TNs as the customer Caller ID must be maintained for industry traceback purposes.
10. TSPs MUST verify the OSP is using a SHAKEN approved CA
11. TNSPs should not require the TNs allocated to an OSP TNs to match the certificate scope or this will preclude other mechanisms from enabling an OSP to make a full attestation.

The service provider’s 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.

# Use Cases Scenarios

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

* Single homed business entity
* Multi-homed Enterprise PBX
* OTT-PSTN interconnect
* Toll-Free originations
* Regulated Enterprise/Government
* Multi-tenant hosted/cloud PBX
* Unified Communications
* Contact Centers
* MVNOs
* 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.

# Solution Approaches

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 of the best practice document is envisioned to identify each mechanism with a focus on what information is required, what makes it authoritative or sufficiently trustworthy, and how it is securely conveyed. It is recognized that some enterprises may want to sign their own originations while others will not. A solution may require multiple mechanisms – with and without enterprise certificates. In many cases, the Service Providers may need to provide most of the effort for the enterprises.

# Use Case Flows

## Use Case 1 – Single TNSP, Single OSP

This Use Case assumes the same TNSP and OSP.



1. TN Customer with TN 555-456-1234 assigned by TNSP dials 555-321-4321
2. OSP A is the TNSP and verifies the TN. (Note: this is all pre-configured)
3. Once verified, OSP A adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to A
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 – TNSP A, OSP B

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, but due to relationship OSP B has with Business Entity/Enterprise it applies local policy and Attestation A is obtained.



1. TN Customer with TN 555-456-1234 assigned by TNSP A dials 555-321-4321
2. OSP B verifies that the TN based on local policy, e.g., a via a certificate, additional authoritative data or otherwise
3. Once verified, OSP B adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to A
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 – OTT – PSTN Interconnect

NOTE: Need to add a Use Case

## Use Case 4 – Outgoing 8xx from RespOrg A - OSP E



1. TN Customer with TN 555-123-1234 assigned by RespOrg, calls 555-321-4321 from 800-123-2234 using OSP E.
2. OSP F checks that the TN is associated with the Enterprise/Business Entity via an authoritative directory. NOTE: The information in the authoritative directory is pre-provisioned before call time.
3. Once verified, OSP F adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to A. If not verified, Attestation B or C would be provided given local policy.
4. The PASSporT is signed using an STI-Certificate with a TNAuthlist containing a single SPC with a value assigned to OSP E.

## Use Case 5 - Regulated Enterprise/Government



TSP verifies PASSporT added by OSP.

## Use Case 6 – Multi-tenant hosted/cloud PBX

## Use Case 7 – Unified Communications

(normative/informative)

# A Annex Title

Xxx