ATIS-1000089.v002

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: May 12, 2021

Abstract

This Technical Report describes use cases where a Signature-based Handling of Asserted information using toKENs (SHAKEN) Originating Service Provider (OSP) may not have complete locally available information to establish a verified association between a calling telephone number (calling TN) and its direct Customer, as the basis for assigning a "full attestation" value to particular calls. In addition, this report summarizes six different mechanisms: Delegated Certificates, LEveraging Models for Originating eNtity authentication – Full Attestation with Entity Identity in a Secure Token (LEMON-TWIST), Enterprise Certificates, Extended Validation (EV) Certificates with TN Letter of Authorization (TNLoA), Central TN Database, and Distributed Ledger Technology (DLT), that have been proposed to provide the OSP with additional information regarding the entity placing a call and the telephone numbers that entity has a valid association with in order to support the OSP marking the call with the highest attestation level.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

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 an 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, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

ATIS Technical Report on –

Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements

1 Executive Summary

This Technical Report describes use cases where a Signature-based Handling of Asserted information using toKENs (SHAKEN) Originating Service Provider (OSP) may not have complete locally available information to establish a verified association between a calling telephone number (calling TN) and its direct Customer, as the basis for assigning a "full attestation" value to particular calls. In addition, this report summarizes several different mechanisms that have been proposed to provide the OSP with additional information regarding the entity placing a call and the telephone numbers that entity has a valid association with in order to support the OSP marking the call with the highest attestation level.

These are:

1) Delegate Certificates,
2) LEveraging Models for Originating eNtity authentication - Full Attestation with Entity Identity in a Secure Token (LEMON-TWIST),
3) Enterprise Certificates,
4) Extended Validation (EV) Certificates with TN Letter of Authorization (TNLoA),
5) Central TN Database, and
6) Enterprise Identity using Distributed Ledger.

All six approaches are considered viable; however, they do present different tradeoffs in terms of complexity, cost to service providers and enterprises, and the assumptions around the relationship between service providers, their customers, and other entities in the SHAKEN and voice network ecosystems. It is difficult to predict how these tradeoffs will influence industry acceptance of one solution over another, and it is likely that the "best" solution will vary based on the deployment use case.

The assessment in Annex A is a relative comparison of how these different solution mechanisms approach solving the added complexities in these use cases. The six approaches in Annex A provide different solution alternatives to provide the OSP with sufficient information to fully attest that the calling TN is associated with the calling entity where that might not otherwise be supported by local policy and locally available information.

It should be noted that all these approaches are not mutually exclusive, and more than one approach can be implemented without impacting the other(s). Likewise, these approaches and the description of each herein may not be exhaustive, and carriers and other stakeholders may deploy variations. As shown in the Solution Comparison Matrix in Table A-1, all six solution approaches are technically viable in terms of their ability to support the principles listed in Clause 6. The six approaches share the following fundamental constructs:

- Enterprises and their trusted vendors are vetted by the Telephone Number Service Provider (TNSP) or a selected vetting agency,
- The OSP continues to perform its role of setting attestation via a SHAKEN Identity header field.

This report recommends that the industry consider all six mechanisms as viable. It is ultimately a matter of OSP local policy to determine how to address the more complex attestation use cases. The OSP's reputation and continued membership in the SHAKEN ecosystem may be directly dependent on how rigorously they have applied the principles in this report when implementing any of these mechanisms or other policy approaches in their SHAKEN attestation decisions.

It should be pointed out that for a given call, the same mechanism needs to be supported by the OSP, TNSP and the enterprise. In addition, it should be noted that these are proposed solutions and that key aspects are not currently implemented in the industry.

2 Scope

SHAKEN (ATIS-1000074-E, *Errata to ATIS Standard, Signature-based Handling of Asserted information using toKENs*) 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 to provide traceability of calls to the OSP via a digital signature tied to a certificate identifying the OSP, and to allow the OSP to indicate whether or not a calling telephone number (calling TN) is valid. The cryptographic signature that protects this information allows the Terminating Service Provider (TSP) to verify the OSP identity and the integrity of the calling parameters, and to make decisions about how to handle the call based on the attestation information and other call parameters.

There are conditions where the OSP cannot fully attest that there is a known authenticated customer and/or that the customer associated with the calling TN is valid. This Technical Report will provide use cases where there may be a “knowledge gap” between the information the OSP can determine locally and the information it needs from outside parties or through additional methods to provide “full attestation” marking (attestation level “A”). In particular, it covers use cases where the authorizations might be determined through technical means and not necessarily ones that rely on policy decisions.

This document is focused on the SHAKEN attestation decision and does not address protection of other characteristics associated with calls or a calling party such as calling party name, intent of the call, or reputation of the caller.

This document is not intended to provide an exhaustive set of Use Cases covering every potential calling pattern that could require supplementary techniques beyond determining attestations with locally available information but nonetheless captures a broad representative sample of the scenarios where additional capability is needed for an OSP to determine TN authorization of calls involving Enterprises, Service Resellers, and other Business Entities. These Use Cases and flows are illustrative, and are not intended to provide a standard mechanism to determine the Attestation level. The capability of service providers, service and TN resellers, and other business entities to support one mechanism versus another to close the attestation knowledge gap will vary; thus, a suite of mechanisms is likely warranted. This document will capture the principles that should be adhered to in order to determine full attestation in the event there is no locally provisioned association available to the OSP regarding the customer and the use of a calling TN. Annex A in this report provides various solution mechanisms and associated impacts with each Use Case.

3 Purpose

Operating and business policies for the various users (Service Providers, Enterprises/Business Entities, and Resellers) of the Telecom Ecosystem are variable and situation driven. Oftentimes, the OSP cannot determine a verified association between the customer and the calling TN presented for customer calls based solely on internal assignments and local customer provisioning information.

In the SHAKEN framework, ATIS-1000074-E [Ref 1], 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.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:
• The number was assigned to this customer by the signing service provider.
• This number is one of a range of numbers assigned to an enterprise or wholesale customer.

• The signing service provider has ascertained that the customer is authorized to use a number (e.g., by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
• The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes "legitimate right to assert a telephone number" but the service provider's reputation may be directly dependent on how rigorous they have been in making this assertion.

This Report will define the principles for techniques that might provide additional input to allow the OSP to satisfy the third requirement (i.e., establishing a verified association with a TN) when making the SHAKEN attestation decision as well as identify the use cases where such techniques may be required to mitigate this attestation knowledge gap and identify the impacts with each of the different mechanisms.

4 Informative References

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

[Ref 1] ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted Information using toKENs (SHAKEN)*.[1]

[Ref 2] ATIS-1000080.v003, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Handling*.[1]

[Ref 3] ATIS-1000092, *Signature-based handling of Asserted information using toKENs (SHAKEN): Delegate Certificates*.[1]

[Ref 4] Draft IPNNI-2019-00086R003, *Enterprise Certificates*.[2]

[Ref 5] ATIS-1000101 [pre-publication], *LEveraging Models for Originating eNtity Authentication - full aTtestation With an entity Identity in a Secure Token (LEMON-TWIST)*.[3]

[Ref 6] ATIS-1000100 [pre-publication], *Central TN Database Approach to Full Attestation for Enterprises with Multi-Homing and/or Multi-Tenancy*.[4]

[Ref 7] ATIS-1000099 [pre-publication], *Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange (TNLoA)*.[5]

[Ref 8] ATIS-I-0000084 [pre-publication], *SHAKEN: Enterprise Identity and Telephone Number (TN) allocation utilizing Distributed Ledger Technology for Originating Service Provider (OSP) Attestation.*[6]

[Ref 9] ATIS-I-0000076, *Enterprise Identity on Distributed Ledger for Authenticated Caller Use Cases*.[1]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/ >.

[2] This document is included in draft form with this Technical Report.

[3] The draft version of this document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://access.atis.org/ > as IPNNI-2021-00004R0xx.

[4] The draft version of this document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://access.atis.org/ > as IPNNI-2021-00026R0xx.

[5] The draft version of this document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://access.atis.org/ > as IPNNI-2020-00035R0xx.

[6] The draft version of this document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://access.atis.org/ > as IPNNI-2021-00053R0xx.

[Ref 10] RFC 8225, *PASSporT: Personal Assertion Token*.[7]

[Ref 11] draft-ietf-stir-passport-rcd, *PASSporT Extension for Rich Call Data*.[7]

5 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 >.

5.1 Definitions

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

Customer: Typically, a service provider's subscriber, which may or not be the ultimate end-user of the telecommunications service. In the context of the SHAKEN attestation model, the Customer is the entity with a direct business relationship and a direct user-to-network interface with the OSP. Enterprises, hosted/cloud service providers, Over the Top (OTT) providers and other service resellers may be considered customers of an OSP depending on the use case.

Enterprise: A business, non-governmental organization, or government entity that is a user of telecommunications services. An enterprise may have direct relationships with any type of service provider, or service or TN reseller described in this document and may have indirect relationships with any of these entities. An enterprise may initiate calls directly on its own behalf or may contract with other entities (e.g., call centers or hosted service providers) to initiate calls on its behalf.

Telephone Number Assignee (TN Assignee): Entity (e.g., enterprise, service provider, Voice over Internet Protocol [VoIP] Provider, OTT Provider, hosted/cloud communications provider, etc.) that has been given the authority to use TNs by virtue of having been directly assigned these TNs by an authorized Telephone Number Service Provider. In the context of toll-free numbering resources, a TN Assignee is an entity that has been assigned the use of the TN by a Resp Org.

Hosted/Cloud Service Provider: Entity providing telephony services for multiple business entities, either using calling TNs supplied by them to the business entity or provided by the business entity in a Bring Your Own Number (BYON) model. These include hosted Private Branch Exchange (PBX), Unified Communications providers, Communications Platform as a Service (CPaaS) providers, Contact Centers, etc. In the context of the use cases described in this document, the hosted/cloud service provider is considered the "Customer" of the OSP. Note that a hosted/cloud service provider could also be an OSP and not a separate entity.

Originating Service Provider (OSP): The service provider that handles the outgoing calls from a customer 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, Resp Org, TN reseller, and other roles.

OTT Provider: Entity providing telephony services for end users via OTT mechanisms and which require Public Switched Telephone Network (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. In the use cases described in this document an OTT provider is considered a Customer of the OSP.

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

Telephone Number Service Provider (TNSP): Service Provider (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 (i.e., TN Assignee), to be used as Caller Identification (ID) for calls originated by the business entity. TNSPs can also serve in the role as OSP or TSP.

[7] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

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

TN Delegee: An entity a TN assignee delegates TNs to for calling purposes. Note that TN delegation may not be an exclusive arrangement. For instance, a TN assignee may be an enterprise entity using a TN for its own purposes while also delegating it to one or more outbound call center contractors for calling services executed on its behalf.

5.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
AS/VS	Authentication Service/Verification Service
BYON	Bring Your Own Number
Caller ID	Caller Identification
CPaaS	Communications Platform as a Service
CTND	Central TN Database
DLT	Distributed Ledger Technology
EIDLN	Enterprise Identity Distributed Ledger Network
EV	Extended Validation
LEMON-TWIST	LEveraging Models for Originating eNtity Authentication – full aTtestation With an entity Identity in a Secure Token
OSP	Originating Service Provider
OTT	Over the Top
PASSporT	Personal Assertion Token
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RCD	Rich Call Data
SHAKEN	Signature-based Handling of Asserted information using toKENs
SP	Service Provider
SPC	Service Provider Code
STI	Secure Telephone Identity
STI-CA	Secure Telephone Identity Certification Authority
STI-PA	Secure Telephone Identity Policy Administrator
STI-VS	Secure Telephone Identity Verification Service

STIR	Secure Telephone Identity Revisited
TN	Telephone Number
TNLoA	TN Letter of Authorization
TNSP	Telephone Number Service Provider
TSP	Terminating Service Provider
UCaaS	Unified Communications as a Service
UNI	User to Network Interface
VoIP	Voice over Internet Protocol

6 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. OSPs adhere to SHAKEN criteria for attestations “A”, “B” and “C”.
2. Any modifications required to SHAKEN PASSporT fields and certificates align with ATIS/SIP Forum IP NNI Task Force standards and/or best practices.
3. ATIS-1000074-E [Ref 1] states that ultimately it is up to service provider local policy to decide which mechanisms are sufficient for an OSP to attest fully to a “legitimate right to assert a telephone number” for a given call.
4. OSPs send a SHAKEN PASSporT, signed with their own credentials, attesting to the validity of the TN independent of other information such as an enterprise signed Identity header added to the call.
5. Regardless of which enterprise mechanism is utilized, the OSPs should be able to audit the mechanism(s) used to establish authorization for a customer to use specific TNs as the customer Caller ID.
6. TNSPs and Resp Orgs 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. The association between a Customer and a TN may be determined by means other than direct assignment from the OSP, e.g., “proof of possession of a TN”.
8. TSPs verify the OSP is using an STI-CA approved by the STI-PA.
9. For calls signed by an OSP, a TSP verification service should not require the calling TN to be assigned to the OSP in order to generate a successful validation result.

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.

7 Use Case Flows

The following Use Cases define the how these different mechanisms approach solving the added complexities where in the SHAKEN ecosystem the OSP does not have a direct 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”, at best.

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

- Multi-homed Enterprise PBX
- OTT-PSTN interconnect
- Toll-Free originations
- Government
- Multi-tenant hosted/cloud PBX
- Unified Communications

- Contact Centers
- VoIP

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 if dictated by Local Policy, e.g., by business agreement) to “A”.

In this Section no solution mechanisms are proposed, as the Use Cases are to highlight how these different mechanisms approach solving the added complexities. Annex A in this report provides various solution mechanisms and associated impacts with each Use Case.

7.1 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, and therefore cannot directly establish a relationship between the customer and the caller ID.

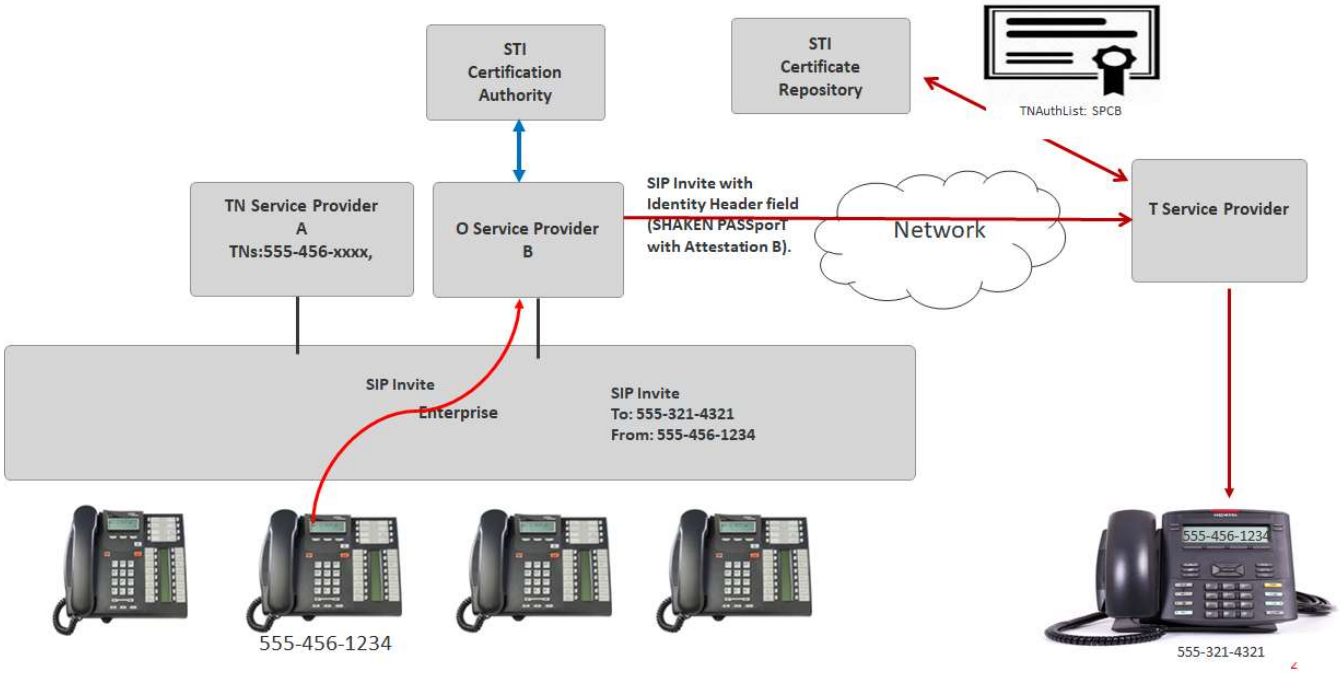

Figure 7-1: Multi-Homed Enterprise/Government with On Premise PBX

1) TN Assignee with TN 555-456-1234 assigned by TNSP A dials 555-321-4321.
2) OSP B cannot 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 Service Provider Code (SPC) with a value assigned to OSP B.

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

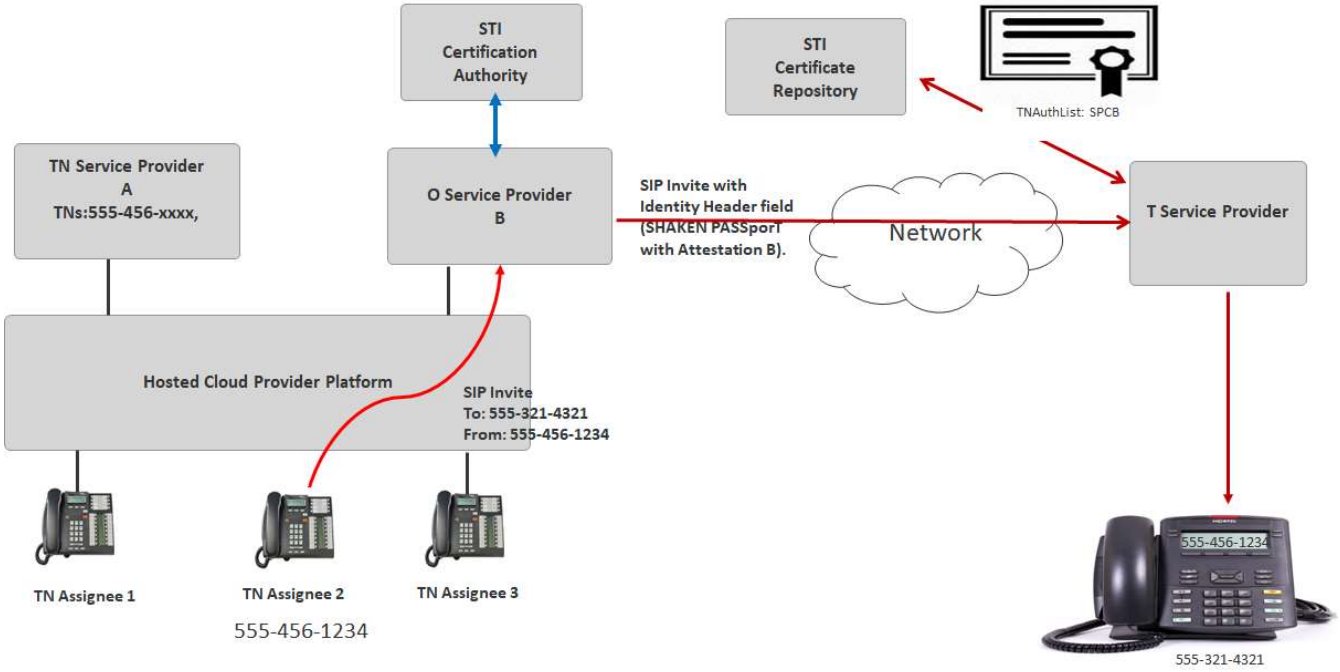

Figure 7-2: Multi-Tenant Hosted/Cloud PBX, OTT to PSTN, Unified Communications, and/or Other Cloud Communication Platform

1) TN Assignee 2 with TN 555-456-1234 assigned by Cloud Provider (not BYON) who obtained the TNs from TNSP A dials 555-321-4321. TN Assignee 2 originates call to OSP B through the Hosted Cloud Provider.
2) OSP B cannot 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.

7.3 Use Case 3 – Call Centers, BYON

BYON applies to Use Cases Unified Communications as a Service (UCaaS)/CPaaS/OTT scenarios as an option.

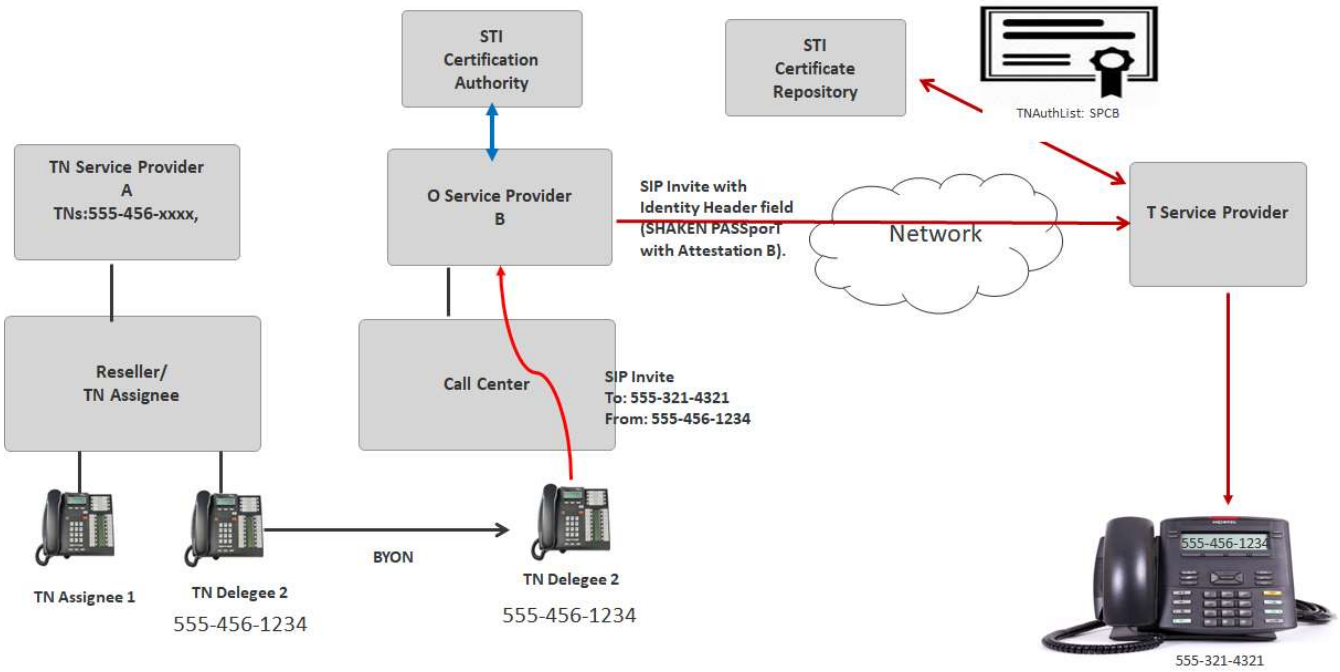

Figure 7-3: Call Centers, BYON

1) Call Center is provided TN 555-456-1234 (BYON) by TN Delegee 2. This TN was obtained through a Reseller who obtained the TNs from TNSP A and is the direct TN Assignee. Call Center dials 555-321-4321 and originates call to OSP B directly using TN Delegee 2's Caller ID and does not originate call through Reseller's network.
2) OSP B cannot 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.

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

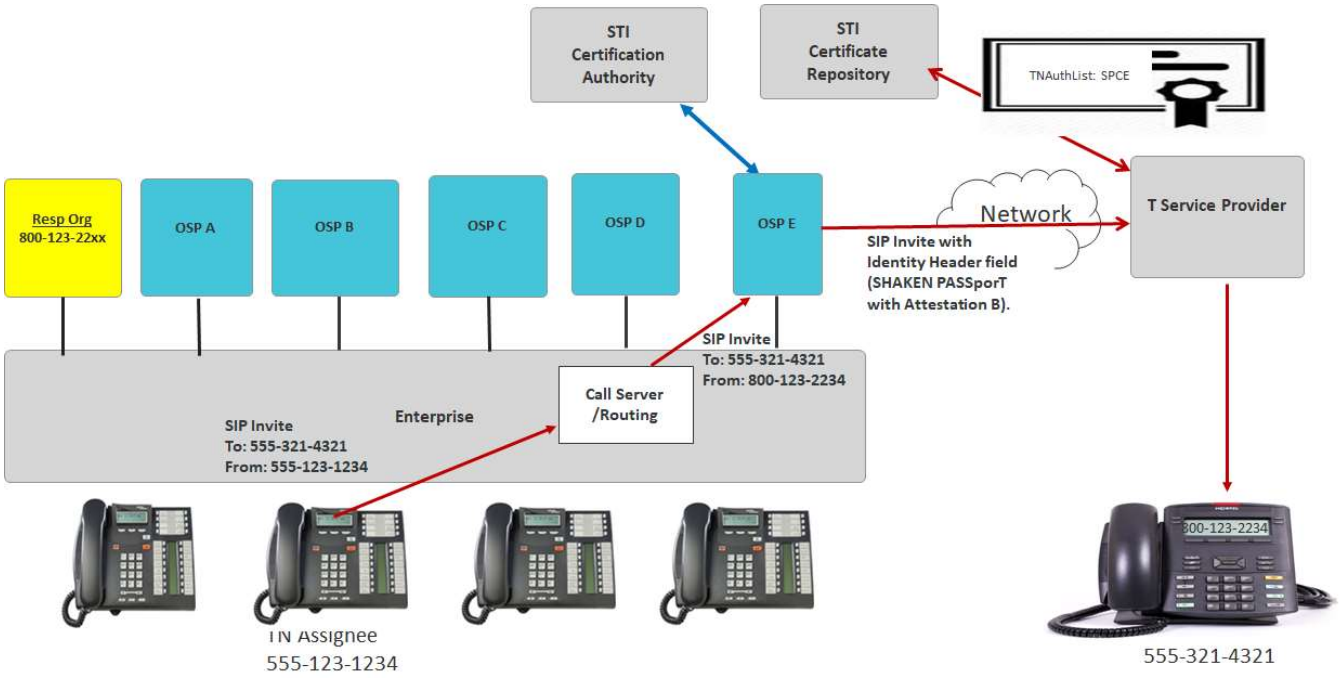

Figure 7-4: Toll Free Originations (On Premise PBX, Hosted/Cloud Platform)

1) TN Assignee with TN 555-123-1234 calls 555-321-4321 from 800-123-2234, assigned by Resp Org, using OSP E.
2) OSP E cannot authenticate the Caller ID Toll Free 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.

The following two (2) Toll Free Use Cases also depict examples where the OSP cannot determine the Toll Free Calling TN is authorized to the customer and would set the Attestation as “B”:

- A shared use Toll-Free Number is originated from multiple enterprises. This is the case where enterprises in different geographical locations originate calls using the same Toll-Free Number but utilizing different OSPs. In this scenario, the Toll-Free Number is issued by a single Resp Org.
- The same Toll-Free Number is originated from multiple locations. This is the case where an enterprise uses the same Toll-Free Number but originates calls in different locations utilizing different OSPs.

8 Summary

SHAKEN has been 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 to provide traceability of calls to the OSP, via a digital signature tied to a certificate identifying the OSP, and to allow the OSP to indicate whether or not a calling telephone number (calling TN) is valid.

It is recognized that there are conditions where the OSP lacks a direct mechanism to fully attest that there is a known authenticated customer and/or that the customer associated with the calling TN is valid. This Technical Report provided representative use cases where there is a “knowledge gap” between the information the OSP can

determine locally and the information it needs from outside parties or through additional methods to provide "full attestation" marking (attestation level "A"). In addition, Annex A identifies approaches on how each method makes it authoritative or sufficiently trustworthy, and how it is securely conveyed in order to enable the OSP to provide full Attestation.

The six total approaches in Annex A provide different solution alternatives to close the "Attestation Gap" by enabling the OSP to fully attest that the caller ID is valid. These are:

1) Delegate Certificates,
2) LEveraging Models for Originating eNtity Authentication – full aTtestation With an entity Identity in a Secure Token (LEMON-TWIST),
3) Enterprise Certificates,
4) Extended Validation (EV) Certificates with TN Letter of Authorization (TNLoA),
5) Central TN Database and,
6) Enterprise Identity using Distributed Ledger.

It should be noted that all these approaches are not mutually exclusive. More than one approach can be implemented without impacting the other(s) and building blocks from one approach can be incorporated with another.

As shown in the Solution Comparison Matrix in Table A-1, all six solution approaches are technically viable in terms of their ability to support the principles listed in Clause 6. The six approaches share the following fundamental constructs:

- Enterprises and their trusted vendors are vetted by the TNSP or a selected vetting agency.
- The OSP continues to perform its role of setting attestation via an Identity header field with a SHAKEN PASSporT.

While these different mechanisms achieve the same end-goal, they do present different tradeoffs in terms of confidence level, complexity and cost to service providers and enterprises. It is difficult to predict how these tradeoffs will influence industry acceptance of one solution over another, and it is likely that the "best" solution will vary based on the deployment use case.

This report recommends that the industry consider all six mechanisms as viable. It is ultimately a matter of OSP local policy to determine how to address the more complex attestation use cases. The OSP's reputation and continued membership in the SHAKEN ecosystem may be directly dependent on how rigorously they have applied the principles in this report when implementing any of these mechanisms or other policy approaches in their SHAKEN attestation decisions.

Note that for a given call the same mechanism needs to be supported by the OSP, TNSP, and the enterprise.

Annex A: Mechanisms to Address Use Cases (Informative)

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

This section identifies 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".

A.1 Delegate Certificates, LEMON-TWIST, and Enterprise Certificates

These three solution options are similar in that the objective is to allow the enterprise to add SIP Identity header fields with PASSporT (base, RCD, or SHAKEN) depending on the solution type and the use case to provide additional information for the OSP in determining attestation and to enhance auditing and traceback by providing additional information about the originating entity.

This section summarizes those solutions in terms of how the originating entity is authorized to obtain a certificate to sign the PASSporTs and the mechanism by which a certificate is obtained.

Once the certificate has been obtained, the basic flow is as follows:

- Vetted enterprise and/or a trusted third-party vendor originates a call using a TN resource assigned to the enterprise or trusted vendor.
- Vetted enterprise (or trusted vendor) adds a signed SIP Identity header with either a base PASSporT, RCD PASSporT, or SHAKEN PASSporT depending upon the solution option and the use case.
- OSP evaluates the SIP identity header PASSporT and uses local policy to determine if the signed information is trustworthy when attesting to the call.
- If the origin of the call is trusted, the OSP follows normal SHAKEN procedures and generates a signed Identity header with a SHAKEN PASSporT giving the call A-level attestation.
- The enterprise Identity header field with an RCD PASSporT and the OSP Identity header with a SHAKEN PASSporT are passed through to the terminating service provider (TSP). Note that the information in the RCD PASSporT and SHAKEN PASSporT may be incorporated into a single OSP Identity header field. Depending upon policy, the enterprise SHAKEN PASSporT may also be passed to the TSP.
- The information in the OSP Identity header is used by the terminating service provider analytics and call validation treatment functions when presenting the inbound call to the subscriber.

A.1.1 Delegate Certificates

The Delegate Certificate solution extends the baseline SHAKEN framework to allow for a SIP Identity header field with a base PASSporT [RFC 8225, *PASSporT: Personal Assertion Token*] or Rich Call Data (RCD) PASSporT [draft-ietf-stir-passport-rcd, *PASSporT Extension for Rich Call Data*] to be added by the enterprise as a mechanism for passing along required enterprise call origination information to the OSP ("enterprise signature"). The PASSporT is signed using a delegate certificate [Ref 3].

The PASSporT is signed using an end user delegate certificate, which is issued by a Subordinate CA. The deployment of this CA requires that the SP establish a relationship with and obtain a certificate from one of the trusted STI-CAs such that the issued certificates chain to one of the root certificates in the STI-CA trust list.

- ATIS-1000092, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Delegate Certificates* [Ref 3]

A.1.2 LEMON-TWIST

The LEMON-TWIST solution extends the base SHAKEN framework to allow for a SIP Identity header field with a SHAKEN PASSporT (and optionally an RCD PASSporT) to be added by the enterprise as a mechanism for passing along required enterprise call origination information to the OSP ("enterprise signature"). LEMON-TWIST leverages the base SHAKEN authorization model by using a Service Provider Code (SPC) token to prove to an STI Certification Authority that it is authorized to obtain an STI Certificate as detailed in ATIS-1000080.v003, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Handling* [Ref 2].

LEMON-TWIST introduces an Entity Identifier (EID) extension of the SPC namespace to include an identifier specific to the enterprise. This enterprise Entity Identifier (EID) can be assigned either by an approved authority or by a TNSP within their assigned SPC namespace. In the latter case, the enterprise EID can then be associated with the TNs assigned to the enterprise entity.

As far as allocation of the SPC token, either the enterprise creates an account with the STI-PA (as allowed by the policies established by the GA) or the TNSPs support the allocation of the SPC token.

The LEMON-TWIST solution has no impact on the existing certificate framework or Certificate Policy. Any approved STI Certification Authority can be used to acquire a certificate for SHAKEN signing. LEMON-TWIST does not require any changes or additional extensions in the STI certificate as specified in ATIS-1000080.v003 [Ref 2]. LEMON-TWIST leverages the existing fields in the TN Authorization List in the STI certificate, with the SPC field containing the enterprise specific identity.

NOTE: This proposal is still under development, thus using the following as a baseline reference for the solution is recommended:

- ATIS-1000101 [pre-publication], LEveraging Models for Originating eNtity Authentication - full aTtestation With an entity Identity in a Secure Token (LEMON-TWIST) [Ref 5]

A.1.3 Enterprise Certificates

The Enterprise Certificate solution leverages the existing SHAKEN framework to allow the enterprise to setup an account with the STI-PA. The enterprise can then obtain an SPC token from the STI-PA that allows the enterprise to acquire a certificate from one of the trusted STI-CAs with whom they have established a business relationship. This solution option does require that the enterprise obtain their own OCN using the existing industry procedures.

As does the LEMON-TWIST solution, there is no impact on the existing certificate framework or certificate content. Once the enterprise has obtained a certificate, the flow is identical to that of LEMON-TWIST:

NOTE: This proposal is still under development, thus using the following as a baseline reference for the solution is recommended:

- IPNNI-2019-00086R003, Enterprise Certificates [Ref 4]

A.2 Determining SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange

This method of attestation determination proposes the exchange of TN authorization information between TNSPs and OSPs in the administrative plane by means of electronic "TN Letter of Authorization" documents, with records tied to verified enterprise identities. Each entity that participates in the authorization process will have a commonly recognizable identity verified through a process similar to web "Extended Validation" (an "EV identity") and will use Public Key Infrastructure (PKI) credentials tied to this identity in the administrative procedure. The EV identity and its associated TN authorizations can be tracked by TNSPs and OSPs that may have only an indirect relationship with the entity. Where required, this method also uses the EV identity and associated PKI credentials as part of an Authentication Service/Verification Service (AS/VS) transaction to allow the OSP to authenticate an indirectly known entity originating a call and to match that entity to a TN authorization record established via the TNLoA exchange.

The AS/VS transaction may utilize a base PASSporT or RCD PASSporT signed by the indirectly-known calling entity with EV credentials. The enterprise-level identity information is consumed by the customers and service providers involved in the TNLoA exchange and the attestation determination. This enterprise-level information does not need to be forwarded through the IP-based service provider network to the terminating party.

NOTE: This proposal is still being developed and draft details are contained in:

- ATIS-1000099 [pre-publication], Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange (TNLoA) [Ref 7]

A.3 Central TN Database

In this proposed approach, a database of TNs is provided by a central authority or is synchronized between or federated across multiple providers. There may also be multiple service bureaus that provide access to the Central TN Database (CTND). The purpose of the CTND is to be an Authoritative Directory of TN-to-Enterprise associations, including delegated authority by Enterprises (to Call Centers, for example). It is envisaged that the CTND has a Representational state transfer (REST)ful Application Programming Interface (API) which is accessed by carriers (in their roles as TNSPs, OSPs, etc.) and by Enterprises.

The database is updated by a TNSP when an Enterprise requests a set of TNs. The TN-to-Enterprise mapping is accessed by an OSP to confirm that an Enterprise has permission to use a particular TN on an outbound call, and therefore that the TN has been registered as “in use” by that Enterprise by a valid TNSP. Each Enterprise has a unique ID by which it is known by the TNSPs and OSPs. This Enterprise ID is managed and allocated by the CTND.

This approach supports providing A-level attestation to Enterprise customers including wholesalers, resellers and contact centers. Further, no stacking of multiple Identity headers is required and no precedence/interop issues are anticipated. In addition, there is minimal impact on Enterprises – they should only have to update their TNSP if they resell/provide TNs to another Enterprise, and all certificate issuance/governance is retained at the STI-CA.

NOTE: This proposal is still being developed and draft details are contained in:

- ATIS-1000100 [pre-publication], Central TN Database Approach to Full Attestation for Enterprises with Multi-Homing and/or Multi-Tenancy [Ref 6]

A.4 Enterprise Identity and TN Authorization using Distributed Ledger Technology (DLT)

This Distributed Ledger Technology (DLT) based service extends the capabilities of SHAKEN to provide an “Enterprise Identity Distributed Ledger Network” (EIDLN). The EIDLN enables an enterprise to establish vetted “Enterprise Identity” credentials together with “TN right to use” authorization proofs, by applying Distributed Ledger Technology and its cryptographic principles that can be verified and authenticated by an OSP from the EIDLN.

A vetted “Enterprise Identity” credential on the EIDLN, allows the enterprise to be assigned or delegated telephone numbers by authorized Telephone Number Service Providers (TNSPs) or Telephone Number Resellers (TNRs) on the EIDLN as signed “TN right to use” proofs. The enterprise can further delegate a TN that they are authorized to use to a call center, for example, to place calls on their behalf. This delegation is also recorded on the EIDLN as a “TN right to use” proof. All TN assignments and delegations are cryptographically signed “TN right to use” credential claims on the EIDLN, providing proof of an “Enterprise Identity” authorization to place calls with a TN.

An enterprise will create a SIP Identity header on its outgoing calls containing a PASSporT signed with their “Enterprise Identity” private key and including a TN authorization reference (“TN right to use” credential claim), the signature and TN authorization reference. This PASSporT will enable any OSP connected to the EIDLN to authenticate the enterprise caller identity using the “Enterprise Identity” public key stored on the EIDLN. The OSP can then verify that the Originating TN being used for the outgoing call has been authorized to be used by this “Enterprise Identity”. This verification is done by checking the signed “TN proof of use” credential for the TN used to place the call.

Using distributed ledger technology to record, verify, and authorize “Enterprise identity” credentials and “proof of use” credentials can provide a single source of truth for all connected stakeholders.

The “Enterprise Identity” credential is implemented using a W3C-standard Decentralized Identifier recorded on the distributed ledger and authenticated by Public/Private Key pair cryptography.

All authorized TN assignments or delegations recorded on the distributed ledger by the issuing authority use signed verifiable credentials according to the W3C standard format.

The following published white paper details the industry use cases and the stakeholder benefits of using a DLT based solution:

- ATIS-I-0000076: Enterprise Identity on Distributed Ledger for Authenticated Caller Use Cases [Ref 9]

NOTE: The proposals are still being developed and draft details are contained in:

- ATIS-I-0000084 [pre-publication], (SHAKEN): Enterprise Identity and TN allocation utilizing Distributed Ledger Technology for OSP Attestation [Ref 8]

A.5 Differences in how the vetted information is passed to the OSP

The primary difference among these different approaches is in how the vetted enterprise information and the TNSP delegation/assignment information is passed to the OSP for attestation determination, audit and traceback purposes. These can be summarized as follows:

- **Delegate Certificates, LEMON-TWIST, and Enterprise Certificates:**

  For these three options, the originating enterprise entity obtains an STI certificate that chains to the trusted root certificate of an approved STI-CA. At call origination time, the originating enterprise entity asserts its authorization to use the calling TN by including an RCD or base PASSporT in the case of Delegate Certificates, and a SHAKEN PASSporT in the case of LEMON-TWIST and Enterprise Certificates. The PASSporT(s) are signed with the STI certificate credentials, in an Identity header field of the originating INVITE request sent to the OSP. On receiving the originating INVITE request, the OSP performs SHAKEN authentication to assert the originating entity’s authorization to use the calling TN based on local policy (which may include verifying the contents of the received Identity header field). Audit and traceback functions can use the “origid” claim of the OSPs’ SHAKEN PASSporT, and the certificate path of the signing certificate, to identity the originating entity. In the case of LEMON-TWIST, the enterprise Entity ID in the SPC token in the TNAuthList provides additional information on the identity of the enterprise originating entity that can also be used for audit and traceback functions.

  The three options differ in how the identity of the enterprise entity is vetted, and in terms of how the enterprise entity obtains STI certificates. For the Enterprise Certificate option, the authorization model is flat; the enterprise entity’s identity is vetted by the STI-PA in the same manner as is done for base SHAKEN. Once vetted, the enterprise entity receives authorization from the STI-PA to obtain STI certificates directly from the STI-CA. The Delegate Certificate model is more hierarchical. The STI-PA sits at the top of this hierarchy, where it vets the identity of the TNSP and authorizes the TNSP to obtain a CA certificate from an STI-CA. This certificate allows the TNSP to host a Subordinate CA that it can then use to issue STI delegate certificates to its enterprise customers. If there are additional layers in the chain of delegation of TNs to the enterprise entity (e.g., TNSP → reseller → enterprise entity) then identity vetting and authorization to issue STI certificates is relayed from each layer to the next lower layer. The authority to issue STI certificates at each layer is constrained by the TNs owned at that layer. The LEMON-TWIST solution supports a model whereby the enterprise entity can be vetted by the STI-PA using an identifier assigned in the existing namespace, which is then quite similar to the Enterprise Certificate option, where the enterprise entity is vetted by the TNSP and assigned a unique Entity ID within that TNSP’s namespace.

  The three sub-options also differ in the scope of authority of the STI certificate issued to the originating enterprise entity, which in turn affects the ability of verifiers, such as the OSP, to validate the originating enterprise entity’s authority to use the calling TN signed by the certificate. For the Delegate Certificate option, the scope of authority of the certificate (as indicated by the certificate’s TN Authorization List) identifies the specific set of TNs that the originating enterprise entity is authorized to use. This enables the OSP to explicitly verify that the originating enterprise entity is authorized to use the calling TN. This means that for the LEMON-TWIST and Delegate Certificate models, the signing certificate contains sufficient information to enable the OSP to confidently assert a SHAKEN “A” attestation level, even though it may not have been assigned the calling TN or have a direct relationship with the originating entity. The LEMON-

TWIST solution also includes an enterprise Entity ID in the SPC token that uniquely identifies the enterprise that is authorized to use the TNs. For the Enterprise Certificate solution, the scope of authority of the STI certificate is expressed as an SPC value which does not identify the TNs assigned to the originating entity. In this case, the signing certificate does not contain sufficient information to enable the OSP to verify that the originating entity is authorized to use the calling TN. Therefore, for the Enterprise Certificate model, the OSP must use other criteria beyond the information contained in the signing enterprise certificate to determine that "A" level attestation is appropriate. Note that while the signing certificate in these solution options contains the identity of the certificate holder, this identity information is not used by the OSP to verify whether or not the signing entity is authorized to use the calling TN.

- **EV Certificates/TNLoA:**

  In the "EV Certificates/TNLoA" model the entity asserting the use of a calling TN is either directly known via Customer UNI identity/authentication at the OSP or is identified by a user-populated Identity header whose signature is tied to Extended Validation (EV) credentials. The real-world legal identity of the calling entity is vetted by a CA that performs the EV procedure and is contained in the subject of its certificate. The CA does not necessarily need to be an STI-CA as the certificate does not by itself convey TN authorization information. The OSP determines the TN authorization by a local authorization database populated from TN Letter of Authorization electronic documents exchanged with the TNSP or through local assignments. The authorization record is tied to the EV identity and the Customer whose UNI the calling entity has been allowed to use. The calling entity's identity is exposed in its certificate or is known as the direct Customer of the OSP for audit and traceback purposes.

- **Central TN Database:**

  In this model, a TNSP adds TN authorization information to a Central TN Database when TNs are assigned to an Enterprise. The TNSP will augment this information when advised by the Enterprise that these TNs have been further delegated to another entity (e.g., TNSP → reseller → originating entity → hosted cloud provider). The identity of an Enterprise or delegated entity is vetted by a central database authority and known to this authority, the TNSP, and OSP for audit and traceback purposes.

  On receiving an originating INVITE request, the OSP will know the entity asserting the use of the calling TN directly via its Customer UNI or, for an indirect calling entity, by the calling TN received. The OSP can access the TN authorization information contained in the Central TN Database to check that this Customer is authorized to provide an INVITE containing that calling TN on behalf of the originating entity. The Customer must certify that an INVITE that it receives from an indirect calling entity and passes to the OSP UNI contains a calling TN expected from that entity. The Customer may enforce this via TN screening or other means.

- **Distributed Ledger Technology:**

  The "Enterprise Identity Distributed Ledger Network" (EIDLN) separates the "Enterprise Identity" vetting and authentication process from the "TN right to use" authorization. In doing so the enterprise has an "Enterprise Identity" that is vetted by any authorized vetting provider of the EIDLN. A vetter can be the number assigner/delegator or any 3rd party authorized vetting agency. Once the enterprise has a vetted "Enterprise Identity", they can be assigned/delegated TNs from authorizing TNSPs or TNRs. All calls placed by an enterprise uses their "Enterprise Identity" to prove their identity, which enables traceback to the real business entity placing the calls.

  By using DLT to record all authorizations of "Enterprise Identity" and "TN right to use", ensures that any change in permission is immediately available for anyone connected to the EIDLN to verify, ensuring a single source of truth. For example, when a "TN right to use" authorization is revoked, or an "Enterprise Identity" is revoked, everyone connected to the EIDLN will know immediately.

  Using DLT enables all data required to authenticate "Enterprise Identities" and "TN right to use" credentials to be co-located within the OSP network, minimizing call validation latency.

The table below characterizes the six approaches but is not intended to provide detailed specifications for each approach. In the case of Delegate Certificates, it is recognized that some enterprises may want to sign their own originations while others may not. A solution may require multiple mechanisms. For a Central TN Database

approach, the specification of the provisioning of authenticated data and access to that data is not defined because there may be multiple competitive solutions providing different interfaces, etc. However, an industry-specified API could be desirable.

Table A-1: Solution Comparison Matrix

	Delegate Certificates	LEMON-TWIST	Enterprise Certificates	EV Certificates with TNLoAs	Central TN Database	Distributed Ledger Technology
OSP defines attestation via local policy	Yes	Yes	Yes	Yes	Yes	Yes
OSP adds SHAKEN Identity header	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise call origination information is provided to OSP to support the STI-AS function	Yes	Yes	Yes	Yes	Yes	Yes
Modification required to STI-AS process to use enterprise call origination information	Yes	Yes	Yes	Yes	Yes	Yes
TNSP controls TN delegation	Yes	Yes	Yes	Yes	Yes	Yes
800 Toll Free Number Supported	Yes	Yes	Yes	Yes	Yes	Yes
Number Portability supported	Yes	Yes	Yes	Yes	Yes	Yes
Solution functions without changes to STI-VS function at TSP	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise identity must be vetted to participate	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise allocation of TN resources can be vetted to participate	Yes	Yes	Yes[8]	Yes	Yes	Yes

[8] The Enterprise Certificates proposal does not require TN Authentication List extension (TNAuthList).

	Delegate Certificates	LEMON-TWIST	Enterprise Certificates	EV Certificates with TNLoAs	Central TN Database	Distributed Ledger Technology
Solution supports multiple vetting agencies	Yes	Yes	Yes	Yes	Yes	Yes
Supports "bring your own number" use cases (enterprise TN used by call center vendor)	Yes	Yes	Yes	Yes	Yes	Yes
Supports call-center reallocation of TNs to a new enterprise	Yes	Yes	Yes	Yes	Yes	Yes
Solution can technically coexist with other solutions	Yes	Yes	Yes	Yes	Yes	Yes
Supports directly connected enterprise use case: (Enterprise → OSP)	Yes	Yes	Yes	Yes	Yes	Yes
Supports trusted-vendor use case: (Enterprise → Vendor → OSP)	Yes	Yes	Yes	Yes	Yes	Yes
Supports complex use cases: (Enterprise → Vendor → CPaaS → OSP)	Yes	Yes	Yes	Yes	Yes[9]	Yes
Functions without requiring enterprise (or designated agent) to sign each call	No	No	No	No[10]	Yes	No
TSP option to access enterprise rich call data[11]	Yes	Yes	Yes	No	Yes	Yes

[9] Information is stored about the chain of entities that have delegated a TN, and which of these entities are allowed to originate a call rather than relay the call. This will allow the OSP to identify the source of the call in a complex call origination use case.

[10] Additional authentication only required if the entity asserting the use of the TN is not the direct Customer of the OSP.

	Delegate Certificates	LEMON-TWIST	Enterprise Certificates	EV Certificates with TNLoAs	Central TN Database	Distributed Ledger Technology
OSP option to access enterprise rich call data	Yes	Yes	Yes	Yes[12]	Yes[13]	Yes
Uses SHAKEN STI Certificates	Yes	Yes	Yes	No[14]	No	No

[12] While not required for attestation determination, an OSP can choose to forward an enterprise-signed Identity header independent of its use as an input to attestation. Attestation and validation of any "orig" claim is solely based on the OSP's determination as populated in the SHAKEN Identity header.

[13] Enterprise can add rich call data information to the Central TN Database which can then be accessed by the OSP or TSP to populate calling name information if desired.

[14] EV Certificate solution uses certificates that identify the entity placing a call without a direct tie to the assigned TN resources in a "TNAuthList" as per STI certificates. TN allocation to the entity identified by the EV certificate is shared administratively via TNLoAs between TNSPs and OSPs.