**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]

# Executive Summary

This Technical Report describes use cases where a 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 a few different mechanisms; Delegated Certificates, EV Certificates with TN Letter of Authorization (LOA), and Central Database, 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. All three 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 the general problem. The three 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. The three approaches are 1) Delegated Certificates, 2) EV Certificates with TN Letter of Authorization (LOA) and 3) Central Database. Within the Delegated Certificate approach there are various solution sub-options that differ based on who authorizes the Enterprise to obtain a certificate and who issues the certificate. It should be noted that these approaches are not mutually exclusive and more than one approach can be implemented without impacting the other(s).

As shown in the Solution Comparison Matrix in Table A.1, all three solution approaches are technically viable in terms of their ability to support the principles listed in Section 6. The three 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 a SHAKEN Identity header field.

This report recommends that the industry consider all three mechanisms as viable and a matter of Originating Service Provider local policy when determining how to address the more complex attestation use cases. The OSPs 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.

# Scope

SHAKEN (ATIS-1000074) 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 originating service provider (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.

# 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 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, 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 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.

# References

The following standards 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.

# 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.

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, 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, 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 directly assigned these TNs by an authorized Telephone Number Service Provider. In the context of tollfree 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 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 Entity: The originating entity is typically the customer of the OSP that is originating a call. This can be an enterprise, a Hosted/Cloud service provider and other entities as defined in this document.

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. 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 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. 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 tollfree numbers to Customers. A Resp Org may also be a service provider, a TN Reseller as well as act in other roles.

**Service Provider Code:** As defined in [ATIS-1000080], this term refers to any unique identifier or namespace that is allocated by a Regulatory and/or administrative entity to a service provider. In the US and Canada this would be a Company Code as defined in [ATIS-0300251] .

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 Assignee), 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: 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 of its own purposes while also delegating it to one or more outbound call center contractors for calling services executed on its behalf.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry SolutionsSIP 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. OSPs adhere to SHAKEN criteria for attestations “A”, “B” and “C”.
2. Any enhancements required to SHAKEN PASSporT fields and certificates align with ATIS/SIP Forum IP NNI Task Force standards and/or best practices.
3. ATIS-1000074 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 for industry traceback purposes.
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 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.

# Use Cases Scenarios

The Use Cases, detailed in Section 7, 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.

# Use Case Flows

The following Use Cases define the problem where in the SHAKEN ecosystem the Originating SP 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.

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

## 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.



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.

## Use Case 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.

## Use Case 3 – Call 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 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.

## Use Case 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.

# 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 originating service provider (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 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 three 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. The three approaches are 1) Delegated Certificates, 2) Extended Validation (EV) Certificates with TN Letter of Authorization (LOA) and 3) Central Database. Within the Delegated Certificate approach there are various solution sub-options that differ based on who authorizes the Enterprise to obtain a certificate and who issues the certificate. It should be noted that these approaches are not mutually exclusive and more than one approach can be implemented without impacting the other(s).

As shown in the Solution Comparison Matrix in Table A.1, all three solution approaches are technically viable in terms of their ability to support the principles listed in Section 6. The three 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 a SHAKEN Identity header field.

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 three mechanisms as viable and a matter of Originating Service Provider local policy when determining how to address the more complex attestation use cases. The OSPs 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.

(normative/informative)

# Annex 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”.

**A.1 Originating Entity Authenticated Identity: Certificate Acquisition by Originating Entity**

Three sub-options have been presented for passing vetted enterprise and other business entity’s call origination information in the SIP signaling flow to enable an originating service provider (OSP) to assign A-level attestation to enterprise originated calls.  The three solutions include; (1) Delegated Certificates; (2) Lemon-Twist; and (3) Enterprise Certificates.

The three solutions all extend the baseline SHAKEN framework to allow for an additional SIP Identity header field added by the originating entity as a mechanism for passing along required call origination information to the OSP (“originating entity signature”).  The three solutions suggest several different options by which the industry can issue STI certificates to vetted enterprise and other business entity customers.  Once an originating entity has obtained an STI certificate the three implementation models are nearly identical.

The above description presumes a certificate has been previously created and assigned to the originating entity. There will be a need to manage the assignment of these end user certificates and other lifecycle processes, including a namespace for unique certificate extended subject names for the upstream entities.

-       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 or a field, optionally with a Rich Call Data PASSporT using the enterprise SHAKEN certificate.

-       OSP evaluates the enterprise information 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 an Identity header field with a SHAKEN PASSporT giving the call A-level attestation.

-       The originating entity Identity header field and the OSP Identity header field are passed through to the terminating service provider (TSP).

- The information in the OSP Identity header field is used by the terminating service provider analytics and call validation treatment functions when presenting the inbound call to the subscriber.

-       The additional information included with the enterprise Identity header field is optionally used by the terminating service provider analytics and call validation treatment functions when presenting the inbound call to the subscriber.

-       The result is a solution that fills the “enterprise and other business entity call origination knowledge gap” using the same cryptographic standards and methods utilized in the baseline SHAKEN framework.

The details of these proposals are contained in:

* [IPNNI-2019-00086R003](https://access.atis.org/apps/org/workgroup/ipnni/download.php/48609/IPNNI-2019-00086R003.pptx) - Enterprise
* [IPNNI-2019-00082R001](https://access.atis.org/apps/org/workgroup/ipnni/download.php/48587/IPNNI-2019-00082R001.pptx) – Delegated Certs
* IPNNI-2020-00026R000 – Lemon Twist
* IPNNI- 2019- 00021R001 – Delegated Certs

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

When an originating service provider receives a call through a Customer interface (the user-to-network interface), the service provider may have an indirect relationship to the entity that is asserting the use of a calling number. For instance, the Customer may be a voice-service reseller, or it may be a value-added service provider that sells calling services as part of a larger offering that may include a hosted call processing platform, call center services, or web integration, etc. In addition, the telephone numbers used by a Customer or the indirect entity may have been assigned by a different TNSP and the entity utilizing the calling telephone number may have been delegated the use of the number by the entity the TNSP directly assigned the number to. For example, an enterprise may delegate the use of some calling numbers to one or more outbound contact center contractors.

To definitively recognize that the TN used as the calling number may be associated with a Customer in these cases where the asserting entity is not directly known, the TN may have been provided by a different TNSP, and/or the TN may have been delegated to the user by the actual TN assignee, requires the exchange of identity and authorization information between the OSP and the various parties that can provide information sufficient to determine the authorization. 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. Entities that participate in the authorization process will have commonly recognizable identity verified through a process similar to web “Extended Validation” (an EV identity) and will use PKI credentials in the administrative procedure that tie to this verified identity that can be tracked by TNSPs and OSPs that may have only an indirect relationship with the entities. Where required, this method also uses the EV identity and associated PKI credentials as part of a SHAKEN-like AS/VS transaction to allow the OSP to authenticate the indirectly known entity originating a call and to match that entity to a TN authorization record established via the TNLoA exchange. The enterprise-level identity information is consumed by the customers and service providers involved in the TNLoA exchange and the attestation determination and do not need to be forwarded through the IP-based service provider network to the terminating party.

The details of this proposal are contained in - [IPNNI-2019-00102R001](https://access.atis.org/apps/org/workgroup/ipnni/download.php/49304/IPNNI-2019-00102R001.docx)

**A.3 Central TN Database:**

In this proposed approach, a database of TNs is provided by a central authority, although access to this Central TN Database (CTND) could be provided by multiple agencies. The purpose of the CTND is to be an authoritative source of TN-to-Enterprise association, including delegated authority by Enterprises (to Call Centers, for example). It is envisaged that the CTND has a RESTful API which is accessed by carriers (as their role as TNSPs, OSPs, etc) but does not need to be accessed 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 number has been registered as “in use” by that Enterprise by a valid TNSP. Each Enterprise must have a unique ID by which it is known by the TNSPs and OSPs. The Enterprise ID is managed and allocated by the CTND.

The benefits of such an approach include: A-level attestation can be provided to all Enterprise customers including wholesalers, resellers and contact centers; no stacking of Identity headers is required and there are no precedence/interop issues. In addition, there is minimal impact on Enterprises – they 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. It also reduces complexity on the TNSPs/OSPs.

The details of this proposal are contained in - [IPNNI-2019-00084R002](https://access.atis.org/apps/org/workgroup/ipnni/download.php/48594/IPNNI-2019-00084R002.pptm) and [IPNNI-2019-00087R000.docx](http://access.atis.org/apps/org/workgroup/ipnni/download.php/48565/IPNNI-2019-00087R000.docx).

**A.4 Differences in how the vetted information is passed to the OSP**

The primary difference among the three 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:

* **Originating Entity Certificates:**

For the Delegated Certificates option, the originating entity obtains an STI certificate that chains to the trusted root certificate of an approved STI-CA and for the Enterprise and Lemon-Twist sub-option, the STI certificate is obtained from one of the trusted STI-CAs. At call origination time, the originating entity asserts its authorization to use the calling TN by including a PASSporT, 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 originating SP 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 use the origid claim of the originating SP’s SHAKEN PASSporT, and the certificate path of the signing certificate, to identity the originating entity. In the case of Lemon-Twist, an Entity ID in the SPC token in the TNAuthList provides additional information on the identity of the originating entity. .

The three sub-options differ in how the identity of the originating entity is vetted, and how the originating entity obtains STI certificates. For the Enterprise Certificate and Lemon-Twist options, the authorization model is flat; the originating entity’s identity is vetted by the STI-PA. Once vetted, the originating entity receives authorization from the STI-PA to obtain STI certificates directly from the STI-CA. The Delegated Certificate model is more hierarchical. For delegated certificates, while the STI-PA vets the identity of the TNSP, an STI-CA delegates to the TNSP the authority to issue certificates directly to its customers. In the case, the TNSP hosts an issuing STI-CA. 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 by that layer. In the case of Delegated Certificates, a CA delegated by one of the trusted STI-CAs in the ecosystem, issues certificates to the enterprise. The SP implicitly trusts the TN customer and no additional authorization mechanism is required for the TN customer to obtain a certificate. In the case of Lemon-Twist, the SP logically serves as the Trust Authority for authorizing the enterprises to obtain certificates from one of the Trusted STI-CAs. The SP (or another entity authorized by the SP) issues an SPC token to the TN customer. The SPC token contains a unique enterprise identifier. The authorization mechanism to obtain certificates is then the same as the Enterprise Certificate option – i.e., the same as base SHAKEN.

The three sub-options also differ in the scope of authority of the STI certificate issued to the originating entity, which in turn affects the ability of verifiers, such as the OSP, to validate the originating entity’s authority to use the calling TN signed by the certificate. For the Delegate Certificate and Lemon Twist sub-options, 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 entity is authorized to use. This enables the OSP to explicitly verify that the originating 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 own the calling TN or have a direct relationship with the originating entity. The Lemon-Twist solution also includes an Entity ID in the SPC token that uniquely identifies the entity 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 Delegated Certificate models 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 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 (TNLoA) 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 database:**

In this model, a TNSP adds TN authorization information to a central 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 the central database authority and known to the central authority, 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 database to check that its 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.

The table below characterizes three approaches but is not intended to provide detailed specifications for each approach. In the case of delegated certificates, 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. For a centralized 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 would be desirable.

Table A.1 – Solution Comparison Matrix

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Delegated****Certificates[[1]](#footnote-1)** | **EV Certificates****with TN LOAs** | **Central****Database** |
| OSP defines attestation via local policy | Yes | Yes | Yes |
| OSP adds SHAKEN Identity header | Yes[[2]](#footnote-2) | Yes | Yes |
| Enterprise call origination information is provided to OSP to support the STI-AS function | Yes | Yes | Yes |
| Modification required to STI-AS process to use enterprise call origination information | Yes | Yes | Yes |
| TNSP controls TN delegation | Yes | Yes | Yes |
| Number Portability supported | Yes | Yes | Yes |
| TSP verifies SHAKEN Identity header | Yes | Yes | Yes |
| Solution functions without changes to STI-VS function at TSP | Yes | Yes | Yes |
| Enterprise identity must be vetted to participate | Yes | Yes | Yes |
| Enterprise allocation of TN resources can be vetted to participate | Yes[[3]](#footnote-3) | Yes | Yes |
| Solution supports multiple vetting agencies | Yes | Yes | Yes |
| Supports “bring your own number” use cases (enterprise TN used by call center vendor) | Yes | Yes | Yes |
| Supports call-center reallocation of TNs to a new enterprise | Yes | Yes | Yes |
| Solution can technically coexist with other solutions[[4]](#footnote-4) | Yes | Yes | Yes |
| Supports directly connected enterprise use case: (Enterprise 🡪 OSP) | Yes | Yes | Yes |
| Supports trusted-vendor use case: (Enterprise 🡪 Vendor 🡪 OSP) | Yes | Yes | Yes |
| Supports complex use cases: (Enterprise 🡪 Vendor 🡪 CPaaS 🡪 OSP) | Yes | Yes | Yes[[5]](#footnote-5) |
| Functions without requiring enterprise (or designated agent) to sign each call | No | No[[6]](#footnote-6) | Yes |
| TSP option to access enterprise rich call data | Yes[[7]](#footnote-7) | No | No |
| OSP option to access enterprise rich call data | Yes | Yes[[8]](#footnote-8) | Yes[[9]](#footnote-9) |
| Uses SHAKEN STI Certificates | Yes | No[[10]](#footnote-10) | No |
| Ported numbers take effect immediately | Yes | Yes | Yes |

1. This column represents all three delegate certificate models mentioned above; (1) Delegated Certificates; (2) Lemon Twist; and (3) Enterprise Certificates. [↑](#footnote-ref-1)
2. Although OSPs may add their SHAKEN Identity header in the enterprise certificate model, it is not mandatory as authorized enterprises with certificates will be able to attest to their originated calls. [↑](#footnote-ref-2)
3. The Enterprise Certificates proposal does not require TN Authentication lists. [↑](#footnote-ref-3)
4. All three solutions can co-exist in the market. During early days of implementing enterprise SHAKEN/STIR, each enterprise and its selected OSPs can choose to support one or more options while the industry gains practical experience in dealing with varied enterprise call-origination use cases. [↑](#footnote-ref-4)
5. 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-cases. [↑](#footnote-ref-5)
6. Additional authentication only required if the entity asserting the use of the TN is not the direct Customer of the O-SP [↑](#footnote-ref-6)
7. Enterprise can add rich call data (rcd) Identity header signed with delegated-certificate. TSP can optionally use the rcd claims provided by the enterprise on a call-by-call basis to inform both analytics and call validation treatment functions. [↑](#footnote-ref-7)
8. While not required for attestation determination, an OSP can choose to forward an enterprise-signed User 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.” [↑](#footnote-ref-8)
9. Enterprise can add rich call data information to the central database via TNSP which can then be accessed by the OSP to populate calling name information if desired. [↑](#footnote-ref-9)
10. EV Certificate solution uses certificate that identifies the entity placing a call without a direct tie to assigned TN resources in a TN-Authlist as per STI certificates. TN allocation to the entity identified by the EV certificate is shared administratively via TN LOAs between TNSPs and OSPs. [↑](#footnote-ref-10)