**ATIS-0x0000x**

ATIS Technical Report on

**LEveraging Models for Originating eNtity Authentication -
full aTtestation With an entity Identity in a Secure Token
(LEMON TWIST)**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This Technical Report is being developed to describe a solution option that allows an originating entity, that is not a Telephone Number (TN) owner, to obtain full attestation in the event there is no naturally verified association available to an Originating Service Provider (OSP) regarding the customer and the use of a TN as the calling party identity.

**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** |
| --- | --- | --- | --- |
| January 29, 2019 | Initial | Proposed Baseline | Mary Barnes |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Executive Summary

This Technical Report describes a solution option for cases where a SHAKEN Originating Service Provider (OSP) is not able to establish a verified association between a calling party telephone number and the Service Provider’s Customer. The solution addresses the scenarios where there is a business need for the calls to be presented with an attestation of “A”, as defined by the criteria in [ATIS-1000074]. This document describes a solution that allows an originating entity to add a SIP Identity header field with a PASSporT with an attestation of “A” in the SIP Invite sent to the OSP. The proposed mechanism leverages the existing SHAKEN framework with the STI Policy Administrator (STI-PA) authorizing the originating entity to obtain certificates from an STI-CA by issuing a Service Provider Code (SPC) token. This solution expands the SPC namespace to include both an OCN and a unique identifier for the originating entity, referred to as an Entity Identifier (EID) The STI-PA remains the trust anchor for the SHAKEN PKI model as described in [ATIS-1000080] and [ATIS-1000084]. There are no impacts to the STI-CAs or the STI-CA’s interfaces to authorize the originating entity to acquire a certificate. The solution also describes an option for a Telephone Number Service Provider (TNSP) to assign EIDs to their customers within their existing OCN namespace assignment.

# Scope

The core SHAKEN specification is premised on the OSP being the owner or provider of the Telephone Number (TN) being used by the calling party. In this case, we refer to the OSP as the TN Service Provider (TNSP). This relationship is the basis for the “A” attestation value included in the PASSporT in the SIP Identity header field in the SIP Invite originated in the network by the OSP when it receives an incoming call from a user (usually a subscriber). This calling party is referred to as the originating entity in this document.

The solution described in this document addresses scenarios where the OSP is not the TNSP. In some of these scenarios, it may be possible for the OSP to establish a secure and trusted relationship with the entity originating the call with the OSP. In that case, an OSP could use an attestation of “A” without requiring that the originating entity provide any additional information when a call is originated.

The solution described in this document details the expansion of the Service Provider Code namespace beyond the OCN to include the identity of the originating entity. This allows the originating entity to use the core SHAKEN mechanisms to interface to the PA and obtain an SPC token in order to obtain STI certificates. This allows the originating entity to include a SIP Identity header field including a PASSporT with an attestation of “A”. Note, that the originating entity can also include an RCD PASSporT.

The OSP handling of a SIP Identity header field in the incoming request from the originating entity also requires consideration. This solution recommends that the OSP forward any received SIP Identity header field, as well as adding one depending upon local policy. In the case that an OSP also adds a SIP Identity header field, the TSP needs to be able to handle the receipt of multiple SIP Identity header fields. Note, this problem needs to be addressed independent of this solution proposal or others as described in [ATIS-1000089] since there are additional PASSporT types that can be included in SIP Identity header fields (e.g., Rich Call data per [draft-ietf-stir-rcd]. Thus, the details of such are not provided in this document.

This document is not intended to be a sole solution for the various use cases described in [ATIS-1000089]. The other solutions outlined in Annex A of that document may be more suitable for some deployment scenarios and business models. However, the proposed expansion of the Service Provider Code namespace beyond OCN could be leveraged by those solutions.

# Purpose

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.

With the initial deployment of core SHAKEN as described in [ATIS-1000074], the attestation value is being used as input to the process to determine what will be displayed on the user’s device. This solution proposal extends the information associated with the calling party in the SHAKEN ecosystem to ensure that legitimate calls receive an attestation such that they will not be presented to the user as potential spam or unauthenticated.

A key aspect of this solution proposal is the inclusion of an Entity Identifier in the Service Provider Code field in the “TNAuthList” in the STI certificate and in the request for an SPC token. This provides additional information about the calling party and can be used to enhance the treatment of the call by the OSP and/or TSP.

# References

The following standards contain provisions which, through reference in this text, constitute provisions of this Technical Report. 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.

[ATIS-1000074] *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*

[ATIS-0300251] *Codes for Identification of Service Providers for Information Exchange*

[ATIS-1000080] *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*

[ATIS-1000084] *Operational and Management Considerations for SHAKEN STI Certification Authorities*

[ATIS-1000089] *Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements*

[STI-GA-SPC-Policy] <https://www.atis.org/sti-ga/resources/docs/SPC%20Token%20Access%20Policy.pdf>

# 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> >.

This document also uses the definitions defined in “Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements” [ATIS-1000089].

## Definitions

**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.

**Entity Identifier:** A four character code that is appended to the OCN, with a “-“ separator, to expand the namespace to support enterprises and other business entities (e.g., Hosted/Cloud Service Provider). This allows them to participate in the SHAKEN ecosystem by providing a unique identifier that can be used to access the same procedures defined for the SPC such as allocation of an SPC token and inclusion in the TNAuthList in an STI certificate. The EID expansion can also be leveraged for other uses outside the scope of this document.

**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

**Operating Carrier Number (OCN):** A four-character code assigned by the National Exchange Carrier Association (NECA) to a service provider. Also known as Company Code.

**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 section and described in [ATIS-1000089].

**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 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.

**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.

**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

|  |  |
| --- | --- |
| CA | Certification Authority |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| EID | Entity Identifier |
| NECA | National Exchange Carrier Association |
| OCN | Operating Company Number |
| OSP | Originating Service Provider |
| PASSporT | Personal Assertion Token |
| PKI | Public Key Infrastructure |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SP | Service Provider |
| STI | Secure Telephone Identity |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-PA | Secure Telephone Identity Policy Administrator |
| STIR | Secure Telephone Identity Revisited |
| TN | Telephone Number |
| TNSP | TN Service Provider |
| TSP | Terminating Service Provider |

# Overview

TheLEveraging Models for Originating eNtity Authentication including a full aTtestation With an entity Identity in a Secure Token (LEMON TWIST) solutionadheres to the principals as outlined in [IPNNI-00075R00x]. The key characteristic of LEMON TWIST is the extension of the namespace for the identity associated with the entity that is authorized to obtain STI certificates by assigning Entity Identifiers within the SPC (i.e., OCN) namespace, while leveraging the core SHAKEN mechanism for providing the authorization.

This solution is premised on the originating entity adding a SIP Identity header field with a PASSporT with an attestation of “A”. There are no changes to the base SHAKEN mechanisms defined in [ATIS-1000074], [ATI-1000080] and [ATIS-1000084] in terms of the following:

1. The originating entity sets up an account with the STI-PA and requests an SPC token.
2. The STI-CA that will be issuing the STI certificates to the originating entity must be approved by the STI-PA
3. The STI-CA must ensure that the SPC token received from the originating entity during the certificate acquisition process as described in [ATIS-1000080] is valid

The primary impact of this solution to a SHAKEN implementation is related to the originating entity setting up an account with the STI-PA and requesting an SPC token (item 1).

This solution also supports a TNSP providing an SPC token, which includes an EID, to an originating entity using their SPC namespace without impacting the certificate acquisition itself.

This solution has no impact on the STI-CA interfaces and the model maintains the STI-PA as the Trust Authority for the Public Key Infrastructure (PKI).

While not detailed in this document, it is recommended that the OSP also perform authentication and add a SIP Identity header field with a SHAKEN PASSporT. This would result in the TSP receiving multiple SIP Identity header fields and the normative behavior of that needs to be defined.

Section 7 of this document provides a description of the expansion of the Service Provider Code namespace beyond the OCN. Section 8 describes the originating entity’s interfaces and interactions with the STI-PA to support the solution.

# Expansion of Service Provider Code

In the SHAKEN ecosystem, the Service Provider Code namespace is intended to uniquely identity a Service Provider to provide accountability and traceback for call’s originated in that Service Provider’s network. The SPC is used to populate the “spc” field in the TNAuthList extension in the STI certificate as defined in [RFC 8226]. In order to authorize a Service Provider to obtain STI-certificates, the Service Provider first obtains an authorization token (referred to as the SPC token) from the STI-PA. The TNAuthList with the “spc” field is input to the token generation algorithm as described in [draft-acme-authority-token-tnauthlist].

There are several existing unique identifiers used by the telecom industry and the decision as to which of these identifiers to use was left as a policy decision made by the STI Governance Authority (STI-GA). For the initial deployment of the SHAKEN ecosystem, the Operating Company Name (OCN) is being used to populate the SPC field in the TNAuthList.

This section of the document provides background on the management and assignment procedures for Operating Company Numbers (OCNs), along with details of the proposal to enhance the information in the SPC namespace beyond a single OCN. This proposal would require approval from the STI-GA.

## Background

Operating Company Numbers (OCNs) are also referred to as Company Codes. The ATIS document *Codes for Identification of Service Providers for Information Exchange* [ATIS-0300251] defines a Company Code as a unique four-character alphanumeric code that identifies a service provider. The Company Code/OCN namespace is managed by NECA.

While some larger service providers have over one thousand OCNs, for the initial SHAKEN deployment service providers are using a subset of those OCNs. Note that how the SPs use the OCNs within their network is entirely their decision. Many SPs use the OCNs for geographical separation of their networks. Regardless, the characteristic of the OCN that is required for SHAKEN is uniqueness and accountability. Thus, the burden is on the Service Provider to choose the OCNs to be used as SPCs in the SHAKEN ecosystem to ensure that they facilitate traceback.

The SHAKEN specifications were not specific that an OCN should be used for the SPC. The protocol structures defined for the SPC naturally allow for extensibility.

Originally, the STI-GA had established a policy that along with an OCN, an SP must have have direct access to telephone numbers from the North American Number Plan Administrator (NANPA) and National Pooling Administrator (NPA) and have a current Form 499A on file with the FCC in order to setup an account with the STI-PA and request an SPC token in order to acquire STI Certificates [STI-GA-SPC-Policy]. The policy was changed to further support additional types of VOIP providers. This proposal to expand the information used to populate the SPC namespace beyond a single OCN would also require approval from the STI-GA.

## Entity Identifier

This section describes the proposed syntax and semantics for the Entity Identifier (EID), as well as assignment procedures and management of the EID namespace.

This document proposes that, rather than expand the purview of the NECA assignment procedures, a block of OCNs is reserved for the assignment of Entity Identifiers by the STI-PA. Section 8 provides details on the impacts to the STI-PA in order to provide this service.

This proposal requires minor updates/enhancements to the existing NECA assignment procedures to document the purpose of the reserved block, but this is very consistent with enhancements made to other telecom identifier assignment procedures. This proposal evolves the existing procedures and practices for OCN assignments, rather than introduce a new identifier and assignment procedures.

This solution also supports a Service Provider using their own namespace and assigning unique Entity Identifiers to their Customers. In that case, the properties of uniqueness and accountability are maintained. And, this would allow management of TNs associated with an EID in a database local to the TNSP that could possibly be leveraged in a distributed database model.

In the case of delegate certificates, the SP could include an EID in the SPC field of the TNAuthList to enhance the information captured for their customers.

With the LEMON TWIST extension to the OCN namespace, it would also be possible for an originating entity to add an additional unique identifier/value to the SPC to more discretely identify the calling party within their network (e.g., groups of call center agents, individual devices, specific types of calls, etc.). This effectively adds another level to the SPC namespace and the following format is proposed:

OCN-EID-<Local ID>

The OCN is limited to 4 alphanumeric characters and it’s proposed that the EID has the same limit as the EID must also have a fixed length to delineate that field from the optional Local-ID.

The following provides an example of a decoded TNAuthList field in a certificate including an SPC using the extended namespace based on the field as defined in [RFC 8226]:

Extension: ( 1.3.6.1.5.5.7.1.26 )

Critical: No

Data: 9010-0001

Note that the ASN.1 encoded form of this field is used as the TNAuthList field in the SPC token as defined in [draft-ietf-acme-authority-token-tnauthlist].

# Originating Entity Account Management

The LEMON TWIST solution proposal leverages the existing mechanisms within the SHAKEN ecosystem to authorize entities to obtain STI certificates. Per [ATIS-1000080], an entity must obtain a SPC token to provide to an STI-CA to prove they are authorized to obtain certificates. The specifications were intentional in not defining the specific identifier to be used as the SPC value, as that was deemed to be a policy decision to be made by the STI-GA. For the initial deployment of the STI-PA within the SHAKEN ecosystem, the OCN was established as the identifier to be used as the SPC value.

The SPC is a field in the authority token of type “TNAuthList” as defined [draft-ietf-acme-authority-token] and [draft-ietf-acme-authority-token-tnauthlist]. The structure of the TNAuthList, included in the SPC token request, is based on the TN Authorization List certificate extension as defined in ASN.1 syntax in [RFC 8226].

Since the SPC field is a string, there are no changes required to support the addition of an EID value to the SPC field in the “TNAuthlist” in either the certificate or SPC token. In addition, no changes are required to the ACME mechanism to support the authorization to obtain STI certificates from a CA [draft-ietf-acme-authority-token-tnauthlist], as that is based on a string comparison with no semantic interpretation of the information. Thus, this document contains the necessary semantics and operational impacts of the extension of the SPC value beyond the OCN.

The following summarizes the functional impacts on the STI-PA to support an SPC value including both OCN and EID:

1. The STI-PA shall support a mechanism to allow an originating entity to request an EID, which would be provided to the originating entity along with an OCN assigned by the STI-PA from the reserved OCN namespace. This could be done via a GUI or an out-of-band mechanism such as emailing a form. [Note: this function could also be performed by NECA, in particular if the EID is deemed useful outside the context of SHAKEN.]
2. When the originating entity creates an account with the STI-PA, the STI-PA shall accept an OCN + EID as a primary account identifier.
3. Once the account is created, the originating entity shall follow the procedures to associate all the OCN + EID values with the account.
4. When the STI-PA is processing requests for an SPC token, the STI-PA shall ensure that along with the OCN value being validated that the EID is also verified to be associated with the originating entity’s account.

Note, that there may be additional impacts to the STI-PA in terms of policies and mechanisms to vet the originating entities, but those are outside the scope of this document.

In the case where the TNSP is providing EIDs within their namespace and providing the originating entity with an SPC token, the impact is reduced. In this case, there is no requirement for any vetting by the STI-PA since the TNSP has already established an account with the STI-PA.

The current STI-PA implementations, based on [ATIS-1000080], support only OCNs for the SP accounts. So an enhancement and further specification would be required to allow the EID extension in the namespace. In the case of a TNSP extending their own OCN namespace, the value of the EID can be ignored if included in a request for an SPC token.

No changes are required to the ACME specifications.

# Applicability and Usage

In the case of an implementation of the delegate certificates [ATIS-1000092], there is no impact on the Service Provider’s account with the PA. Since the delegate certificate model is based on the implicit authorization of the originating entity, with which the Service Provider has an existing relationship, there is no SPC token required. In terms of managing the EID values, that would be entirely within the purview of the Service Provider to manage the information in the manner suitable for their business needs. It would be possible to extend the model if the information were deemed to be of use outside the Service Provider’s domain. For example, one could imagine a model whereby the entity that receives a delegate certificate wants to ensure that the EID in the TN Authorization List certificate extension is really associated with the TNSP. In this case, either a distributed or centralized database model could provide a mechanism for sharing and disseminating this information.

For originating entities using an Enterprise Certificate model that choose to leverage the EID, there is an additional impact on the STI-PA in terms of account management. To support this, the STI-PA shall ignore any information in the SPC field in verifying that the OCN is associated with the originating entity’s account, in the case of OCNs that are not in the range reserved for EIDs. The entirety of the SPC shall be used in generation of the SPC token per the base LEMON TWIST model.

While not dependent upon being sent to the TSP, LEMON TWIST recommends that the SIP Identity header field added by the originating entity be passed to the TSP, unless the OSP performs verification and is willing to provide full attestation in the SIP Identity header field that it adds. The motivation is that this adds more information as input to the analytics and provides additional information that can be used for trace back.

# Summary

LEMON TWIST provides a solution option to support cases 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. LEMON TWIST adds a naming structure and hierarchy to support identification of Customers originating calls by using both the OCN and an Entity Identifier. This provides the uniqueness and accountability that is provided by the SPC field in the TNAuthList in the STI Certificate and as input to the SPC token generation mechanism.

This EID mechanism defined by LEMON TWIST provides another protocol building block that can be used by any of the solution options as described in [ATIS-1000089]. As is the case for the Delegate Certificates and Enterprise Certificate models, LEMON TWIST is based on the originating entity adding a SIP Identity header field to the outgoing SIP INVITE sent to the OSP. LEMON TWIST recommends that this SIP Identity header field be passed to the TSP, unless the OSP performs verification and is willing to provide full attestation in the SIP Identity header field that it adds. The key advantage of passing the SIP Identity header received for the originating entity is that it provides more information as input to the analytics and perhaps, more importantly, additional information that can be used for trace back.

The proposal to expand the SPC namespace beyond OCN would require approval of the STI-GA (and perhaps broader industry support) and would require updates to the specifications of the STI-PA functionality and/or separate specification.