**ATIS-0x0000x**

ATIS Technical Report on

**Methods to Determine SHAKEN Attestation Levels Using Enterprise-Level Credentials and Telephone Number Letter of Authorization Exchange**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

In the “enterprise” or “organization” context, the SHAKEN attestation procedure can be thought of as an identity, authentication, and telephone number authorization check at the user-to-network interface. Identification and authentication of a Customer and/or TN Assignee/delegee may be handled by the originating service provider separate from the authorization decision. This Technical Report offers a method to use non-STI PKI credentials at the granularity of an enterprise for authentication transactions across multiple participants and a “Letter of Authorization” document exchange for service providers to learn that a party is authorized to utilize a TN. TN authorization is established in the administrative plane and checked by the originating service provider subject to enterprise authentication.

**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 **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

This technical report provides a methodology for service providers to exchange telephone number authorization information and for an originating service provider (O-SP) executing SHAKEN attestation determination to use that information in conjunction with enterprise-level authentication.

## Purpose

The SHAKEN (ATIS-1000074-E, [Ref. 1]) Identity header provides a means to authenticate the O-SP for a call being established across one or more IP-NNIs and to protect the integrity of the call parameters populated by the O-SP as the call passes through two or more service provider VoIP networks. The protected parameters include the calling and called telephone numbers (TNs) and an attestation marking that describes the extent to which the O-SP has (a) determined the identity of a Customer (an entity the O-SP has a direct relationship with and a direct interface for receiving calls) it received a call from and (b) determined an association between the calling TN and the Customer. The terminating SP (T-SP) that relies on this information from a received and verified Identity header can determine the extent to which the O-SP validated the Customer identity and calling TN, and can use that information to make further decisions as to whether or not to trust the validity of the calling TN. In many legitimate calling scenarios the originating service provider may not be able to determine a Customer’s association with a calling TN solely through locally provisioned information for one or more reasons including the following:

1. The Customer utilizes multiple O-SPs and marks calls with a common calling TN (e.g. a main business number) regardless of the service provider that assigned the TN (the Telephone Number Service Provider or TN-SP)
2. The Customer and end-user are different entities, and the calling TN is assigned to the end user. For example the end-user is a Customer of a service reseller or value-added service provider (VASP) that is not the SP populating the Identity header. In this case the service reseller or VASP is the O-SP’s Customer, and the end user is the “Customer’s Customer” or “C2” entity not directly known to the O-SP.
3. An enterprise or other organization contracts for calling services provided by another entity and the contractor uses the enterprise’s calling TNs. In this case the call center contractor is the O-SP’s Customer using a delegated TN, but the enterprise is the TN Assignee.
4. TNs are assigned by a service provider to one entity that resells use of those numbers to an O-SPs Customer or an unrelated (e.g. C2) end-user entity. In this case the TN reseller is the TN Assignee, and the Customer or C2 is a TN Delegee.

This document describes a method to allow an O-SP to determine that the calling TN is associated with the Customer, and therefore give the O-SP a basis for marking a call from a known and authenticated Customer with full attestation in cases where the O-SP has not directly assigned a calling TN to the Customer and/or the entity asserting the TN is not directly the Customer of the O-SP. The method involves identification and PKI credentials exchange for service and TN resellers and other enterprise entities at the granularity of the enterprise, and the exchange of electronic “Letter of Authorization” documents (the TNLoA document) between service providers as a method to determine an enterprise is authorized to utilize calling TNs.

## Application

The methods described in this report may be used between service providers who wish to exchange TN authorization information regarding common Customers and entities that utilize the services of their Customers. Wide adoption of the TN authorization exchange methodology will require policy standards, common administrative data formats and interoperable procedures. Adoption of enterprise-level identification and PKI credentials for administrative use will also require common policy standards and procedures, and the PKI-based enterprise authentication at the user-to-network interface (as might be needed in some call flows where the call arrives indirectly at the O-SP) will require compatible SIP implementations in service-provider and enterprise user equipment. This document provides a basis for the technical and procedural implementation that can be used across participants.

Note that determining authorization to use calling TNs as part of the SHAKEN attestation determination per [Ref 1] 5.2.3 does not necessarily require technical implementation of authorization information exchange if an O-SP policy defines, for example, that contractual provisions and usage monitoring are sufficient means to determine TN authorization for a particular set of Customers. The procedures described in this document and other methods of explicit authentication and authorization information exchange may be used in cases the O-SP policy deems that non-technical methods are not sufficient for particular Customers or calling usage.

# Normative References

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

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

[Ref 2] ATIS-1000088, Technical Report on a Framework for Attestation and Origination Identity

[Ref 3] IETF RFC 8225, Personal Assertion Token

[Ref 4] CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates Version 1.7.2

[Ref 5] IETF draft-ietf-stir-passport-rcd-06, PASSporT Extension for Rich Call Data

# 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

The following terminology will be used in this document to describe the entities involved in both the call flow and the TN authorization administration process. Additional terminology used to describe network components and entities applicable to the attestation decision are described in the “ATIS Technical Report on a Framework for Attestation and Origination Identity” [ATIS-1000088, Ref 2]:

Originating service provider (originating SP or O-SP): The first SP entity that receives calls from a Customer and is capable of populating a SHAKEN Identity header (executing the STI-AS function) for the call when it is to be sent across an NNI to an intermediate or terminating SP. An O-SP may also populate Identity headers for calls received without an Identity header at an NNI, but note that the procedures described in this document are applicable for calls received at a UNI from a known and authenticated Customer as the authorization transaction relies on established customer relationships.

Customer: An entity that has a direct relationship and with the originating SP and sends calls initiated by itself or upstream parties through a “user-to-network interface” (UNI) to the originating SP.

Customer’s customer (C2 customer or C2): An entity that has a direct relationship with Customer and an indirect relationship with an Originating SP. A C2 customer sends calls through Customer’s platform, which are then indirectly placed through the Customer’s UNI interface to the originating SP. There may be additional levels of indirection (e.g. a “C3 customer”) but see notes in 5.5 below regarding call and authorization traceability chains.

End user: An entity that initiates calls, and typically known as the “caller.” Note that the end user may be the “Customer,” the “Customer’s customer,” or another entity further upstream in the call flow.

TN User (TN-U): The entity in the call path that asserts the calling TN. Note that this can be the same entity as the End User or it can be another entity between the End User and O-SP.

TN Service Provider (TN-SP): A service provider entity with direct access to numbering resources and that is the authoritative source of TN assignment information. A TN-SP is also the authoritative source of TN assignment information for TNs ported into its network by its customers.

TN Assignee: An entity that is assigned TNs for use as calling and destination TNs, although for this document is primarily concerned with calling TNs being populated in SHAKEN PASSporTs.

TN Delegee: An entity a TN Assignee delegates TNs to for use on calls placed by the delegee. 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.

TNLoA: Telephone Number Letter of Authorization – In the context of this report, an electronic document exchanged between SPs to indicate a TN User is authorized to utilize a calling TN.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |
| C2 | Customer’s customer |
| O-SP | Originating service provider |
| T-SP | Terminating service provider |
| TN | Telephone number |
| TN-A | TN Assignee |
| TN-D | TN Delegee |
| TN-U | TN User |
| TN-SP | TN Service Provider |
| UNI | User-to-network Interface |

# Enterprise ID and credentials and TNLoA

This method treats the authentication of entities in the call path and authorization of an entity to utilize calling TNs as separate procedures. In the real-time call flow, the O-SP determines the identity of the entity in the call path that is asserting the calling TN (TN-U), whether that is the Customer with the direct UNI connection to the O-SP or an indirect entity (a C2 customer) whose calls pass through the Customer UNI. The O-SP then consults a database of TNs authorized to the TN-U entity and (if necessary) a database of TN-Us authorized by the Customer to utilize its UNI (the TN-U may be either a Customer or C2). The TN authorization information is determined locally within O-SP administrative processes or exchanged in an administrative channel between the SP entity that assigned the TN or that holds the authoritative assignment information for a ported TN (the TN Service Provider or TN-SP) and the O-SP (described below as the “TNLoA” process). TN authorization to the TN-U may either be through direct assignment by the TN-SP (or in-porting to the TN-SP) or by delegation from the assignee.

## Identity management process and enterprise credentials

As described in the Attestation and Origination Identifier Framework Technical Report ([Ref. 2]), when establishing a business relationship with a Customer (in the context of this process it is assumed a Customer is an organization and likely not an individual person) an O-SP will execute an identity management procedure including “identity proofing” to determine the real-world identity of the Customer for commercial and policy enforcement purposes. The identity proofing may include gathering and verifying Customer mailing address, contact phone numbers and e-mail addresses, tax ID or other government identifiers, credit information, verifying the identity of corporate officers, etc. Once the Customer identity has been verified on a bi-lateral basis all credentials exchange and TN assignments are tied to that identity. In the simplest cases where no third-parties are involved in the identity management and TN management processes, the bi-lateral exchange of (enterprise) identity information and TN assignments are sufficient for the O-SP to determine the Customer’s authorization to use a calling TN as a basis for full attestation marking in the SHAKEN PASSporT.

When additional parties are involved in the TN management and authorization process, including separate TN-SPs and O-SPs and/or entities with only an indirect relationship to the O-SP or TN-SP (for example C2 entities and TN Delegees), the exchange of authorization information across the parties can be simplified by having a form of identity that is commonly recognized and verifiable across all parties involved in the process. This identity can then be used with associated credentials to drive authorization transactions in the administrative channel and where needed to authenticate the party claiming to be authorized at the UNI (see 4.5 below). This method uses PKI credentials tied to a proven real-world identity at the enterprise level. The means for establishing a real-world identity and certifying credentials can be a process similar to web Extended Validation (EV) procedures ([Ref.4]). In an EV X.509 certificate the subject typically contains a business name, location, and government registration ID. In the USA this includes the registered corporate name, business city, state name, and state corporate registration ID, although for these particular use cases industry participants may require other identifiers to make the subject identity more precise and verifiable. The CA providing the certificate executes an identity proofing procedure to determine (to an appropriate extent) that the requesting entity can legitimately assert the identity. This document will refer to the “EV process” and “EV credentials” to describe the enterprise identity proofing and PKI credential management process using standard EV procedures or a possible enhanced procedure.

Note that since these EV credentials only convey the identity of the principal (the end user, service or TN reseller, etc.) in the administrative transaction or supplementary UNI authentication, and they do not convey TN authorization information, the associated CAs can be any entity deemed suitable to process identification of an enterprise and do not need to be traceable to an STI-CA root. Those SPs who support the TNLoA process can determine the set of CAs that may be trusted to provide EV credentials through mutual agreement or industry-level policy, and they may also establish common identity proofing, Certificate Policy, and Certification Practice Statement requirements, and other policies each CA must meet. Once the organizational or “enterprise” identity is established and the PKI credentials are established, these may be used to sign and verify authorization transactions between various parties whether or not they have direct business relationships. Note, however, that for TN authorization purposes these transactions should ultimately be triggered by entities with the direct relationship to the SP that are taking responsibility for the correctness of the request. Similarly, service providers involved in the authorization exchange may identify themselves using SHAKEN PKI credentials tied to an industry-recognized service provider code (SPC) and that are traceable to a real-world business identity verified through industry-adopted STI management and regulatory processes.

## TN Management Process

The process of managing TN authorization must generally respond to TN management actions such as assignment, porting, and disconnects. Using industry-standard procedures, a TN-SP either assigns TNs from its own inventory to TN Assignees, or the TN Assignee requests a TN assigned by another TN-SP (the number portability donor network) be ported into the new (recipient) TN-SPs network. The main effect of TN porting is that it makes the TN routable to the recipient SP’s network. In addition, porting has the effect of moving the administrative relationship for the TN to the recipient SP (the recipient network becomes the TN-SP with the direct relationship to the TN Assignee). Either through assignment or in-porting, the TN-SP is then the authoritative source of information about the TN assignment. The TN Assignee then can utilize the TN and designate the services and endpoints to which it should route, and the TN Assignee can be identified as the TN User (TN-U) by the TN-SP when the assignee places calls with that calling TN. A TN could be ported to another TN-SP who then becomes the authoritative source of information (the former TN-SP is no longer authoritative for the TN), and a TN could be returned to the TN-SPs inventory or disconnected. Assuming the TN was from the TN-SPs own inventory it can also be reassigned to a different TN Assignee usually after an aging period.

When a TN Assignee delegates the use of a TN to another entity (a TN Delegee), the TN-SP is not typically made aware of that fact and continues to consider the TN Assignee as the responsible party for the use of the TN, and typically does not have a business relationship with the delegee. In various use cases, the TN Assignee may be an enterprise that contracts with other entities (e.g. call center operators) to place calls on its behalf, a TN reseller granting a TN delegation to a delegee for its own calling purposes, or a service reseller explicitly or implicitly delegating the use of TNs to C2 entities that then originate calls via its UNI to an O-SP.

In the context of the TNLoA process as described below, TN management activities will be prerequisites or triggers for establishing or modifying authorizations to use a TN. Establishing an authorization for a given TN may happen concurrent with or after the TNs assignment. Disconnects, out-porting, and reassignment may all be triggers for changes to an authorization. Establishing a TN delegation may also be accomplished through the TNLoA process which will establish an explicit delegation. Expiration or revocation of a delegation should also trigger an update to remove the TN authorization.from the TN Delegee. Likewise, if the underlying TN assignment is removed then the delegation must also be removed.

## TNLoA Process

TN-SPs who support this procedure may make “TN Letter of Authorization” (TNLoA) documents available to other O-SPs so an O-SP can determine the set of TNs assigned or delegated, to particular TN users (TN-Us). A TNLoA document could for instance (in keeping with formats used for the SHAKEN processes) be a JSON Web Token indicating the assigning TN-SP, the TN-U, a list of assigned TNs, a validity period for the assignment, and a document identifier. For TNLoA documents tied to a direct TN Assignee the TN-U element contains the identity of the assignee. After a delegation transaction between the TN assignee and the TN-SP, the TN-U will contain a tuple of the TN Assignee and the TN Delegee (note that there can continue to be authorizations and TNLoA documents associated with the TN Assignee as the TN-U). The documents are signed with the TN-SPs credentials (e.g. SHAKEN certificates containing the certified SPC) and contain the URL to the certificate for verification by the O-SP. The root certificate store used to verify the TNLoA documents may be the SHAKEN store. An example TNLoA document might look like the following:

Protected header:

{

“typ”: “JWT”

“alg”: “ES256”

“x5u”: <https://cert.example.org/tnloaspc.cer>

}

Payload:

{

“iss”: <SPC>

 “iat”: <timestamp>

“nbf”:<from timestamp>

“exp”:<to timestamp>

“tnloa”:{

“docid”: <document ID>

“scope”: <complete or partial>

“replaces”: <original docid>

“tnu”: {“tna”:<Subject-TN Assignee>(,”tnd”:<Subject-TN Delegee>)}

“tnlist”: [“tn”:<TN1>,”tn”:<TN2>,…,”tn”:TNn”]

}

}

Payload claims:

iss – Issuer (TN-SP)

iat – issue timestamp

nbf – not-valid-before timestamp

exp – expiration timestamp

tnloa – TN Letter of Authorization structure

docid – TNLoA document identifier in the form of a UUID

scope – document contains a complete set of TN authorizations for a TN-U or a partial set

replaces – docid of previous TNLoA document – force expiration of previous tnlist and replace it with a new tnlist

tnu – TN User (TN Assignee alone or a tuple of the TN Assignee and TN Delegee)

tna – TN Assignee (enterprise certificate subject)

tnd – TN Delegee (enterprise certificate subject)

tnlist – list of authorized calling TNs for the TN-U

An O-SP pulls TNLoA documents from a set of TN-SPs based on a request from one or more Customers. The TN-U a Customer requests will either be itself as a calling entity or a C2 entity using its services. In the TN-SP TNLoA management system the TN-U will be matched as either a TN Assignee in a document without delegation or a TN Delegee in a document with delegation. A TNLoA document may be an exhaustive list of TNs assigned to the TN-U or one of a set of documents containing different TN assignments. Individual TNs within an LoA document may become invalidated before the end of a validity period, due to porting or disconnect activity. Because of this, the TN-SP must provide a notification mechanism to trigger the O-SPs relying on particular sets of TNLoA documents to pull an updated sets of documents. An O-SP may also audit TN authorizations against porting activity to identify those no longer valid due to porting. However, assuming both TN-SPs support the TNLoA process, porting should only move the authoritative source of the TN assignment and/or delegation to a new TN-SP while the TN-U and associated TNs remain the same, With TNLoA administration integrated with a port-out/port-in and notifications from the donor and recipient TN-SP, the O-SP should be able to process TNLoA updates with minimal latency surrounding the port.

Note that such a process exposes the identity and business relationships of all the entities involved in the authorization process. This is only necessary among the entities involved in the process up to the O-SP ultimately making the TN authorization decision at call time. Therefore, it is recommended that TN-SPs implement access control to limit TNLoA delivery to specific O-SPs that are authorized by the TN Assignee. The TNLoA information does not need to be made available to all terminating SPs in the SHAKEN ecosystem for the attestation determination to be made by the O-SP (terminating/verifying parties relying on O-SP’s attestation marking do not need to be exposed to all the inputs of the determination).

## Authorization transactions

Establishing a TN authorization involves three basic steps:

1. A TN Assignee requests its TN-SP to make TNLoA documents available to a set of O-SPs for itself and/or a set of TN Delegees
2. A Customer requests its O-SP(s) to pull TNLoA documents for itself, and/or a set of C2 entities from a set of TN-SPs
3. An O-SP pulls the TNLoA documents associated with a requested TN User and populates TN authorization records in Customer’s AAA record.

Depending on the TN management and supported calling scenario, a number of prerequisites need to be met before an O-SP accepts an authorization request from a Customer:

1. The Customer itself has been identity-proofed by the O-SP and also by an EV CA recognized by the SPs.
2. The Customer has also proved that it can utilize the identity specified in its EV certificate, for instance by signing a challenge from the SP using the private key associated with the EV certificate.
3. In use cases where the prospective TN-U is a C2 entity, the C2 has been identity-proofed by Customer and an EV CA, and has proved that it can utilize the identity specified in its EV certificate to both Customer and Customer’s O-SPs (this is to limit the possibility of a Customer requesting authorization for TNs associated with entities that it does not have a relationship with).
4. Also where the TN-U is a C2 entity, the C2 has provided Customer with a list of TN-SPs that hold its TN assignments or delegations. If the TNs have been delegated, the C2 will obtain the list of TN-SPs from the TN Assignee (a Customer can also utilize delegated TNs and will need the list of TN-SPs from the assignee).

Similarly, there are prerequisites for a TN-SP to accept a request to make TNLoA documents available for TN-Us:

1. The TN Assignee has been identity-proofed by the TN-SP and an EV CA. The TN Assignee has proved to the TN-SP that it can utilize the identity specified in the EV certificate.
2. In use cases with a TN delegation, the TN Delegee has proved it can utilize the identity associated with the EV certificate to both the TN Assignee and TN-SP (similar to the C2 use case described above, this limits the possibility that a TN-SP provides a TNLoA for an entity other than a TN Delegee that has a relationship with the TN Assignee).
3. In use cases with a TN delegation, the TN Delegee has provided a list of O-SPs it intends to originate calls through to the TN Assignee, for use in TN Assignee’s authorization requests. Where the delegee is a C2 entity it must receive this information from Customer.

## PKI-based authentication of indirect calling entities

In the cases where the TN User is the direct Customer with a UNI interface to the O-SP, no additional authentication methods over and above standard UNI authentication (e.g. user-based authentication, device registration, IP whitelists, protected network paths, etc.) are needed to determine the identity of the TN User which is also the Customer. That identity is then directly available to the OSP to match against TN authorizations provisioned locally or learned through a TNLoA exchange. In cases where the TN User is not the direct Customer of the O-SP, in particular where it is a C2 entity placing calls through a Customer’s platform that are relayed to the O-SP through the Customer’s UNI, the O-SP may require an additional identity and authentication transaction to match the C2 entity to a TN User known through TNLoA authorization transactions. A PKI-based signing and verification procedure provides one way for an O-SP to identify and authenticate an indirectly known entity. The C2 UAC may populate a user-provided Identity header containing a base PASSporT [RFC 8225, Ref. 3] that the O-SP will receive through the Customer UNI. The base PASSporT will be signed using the C2’s EV credentials, and the corresponding certificate and its URL must be made available to the O-SP. The O-SP will verify the signature and read the EV (enterprise) identity from the certificate to match authorization entries in the Customer record. The C2 entity includes the calling TN it is asserting in the From URI as the “orig” claim. An example PASSporT header and payload may look like the following:

Protected header:

{ "alg":"ES256",

 "typ":"passport",

 "x5u":"https://enterprise-cr.example.org/org-ev-cert.cer"

}

Payload:

{ "dest":{"tn":["12155551001"]},

"iat":1443208345,

"orig":{"tn":"12025551000"},

 }

Once the C2 UAC populates and signs the base PASSporT and assembles the user-populated Identity header, it includes this header in its SIP INVITE to Customer’s platform. Customer’s platform, in this instance functioning as a SIP proxy or B2BUA forwards the user Identity header unchanged to the O-SP. The O-SP then verifies the identity of the C2 entity by checking the signature against the EV certificate and the root certificate store containing industry- or mutually-agreed EV identity providers’ CA certificates. A single certificate and associated public/private key pair, at the granularity of the asserting entity may be used for all calls sent by the C2 independent of its set of authorized calling TNs, and the set of certificates an O-SP will need to pull is limited to those C2s that are authorized by the O-SPs customers. Therefore, the O-SP should be able to achieve a high level of caching for the EV certificates required to authenticate C2s utilizing its Customer UNIs.

The O-SP should also validate the other applicable PASSporT claims against the unprotected SIP headers and validate the freshness of the user Identity header to protect against header replay. Once the C2 entity is authenticated the EV identity may be used to match a TN authorization in Customer’s AAA record. See 5.3 and 5.4 below for a detailed walkthrough of the indirect origination use cases with the user-populated Identity header AS/VS transaction.

.As a side note, although separate from any TNLoA information exchange and the use of organization-level authentication as part of an attestation decision, a C2 or other indirect entity may alternatively populate a PASSporT containing the Rich Call Data extension ( ‘rcd’ PASSporT type, [draft-ietf-stir-passport-rcd-06, Ref 5]) to pass claims of additional identifying information such as display name and/or jCard information. The O-SP may validate this information against information learned through an administrative channel or real-time lookup from the EV certificate issuer or another identity vetting agency. A Customer entity may also use this mechanism to pass Rich Call Data even though a PASSporT authentication/verification transaction is not necessary for the purpose of establishing its identity to its direct O-SP as part of the TN authorization check.

## SP and Extended Validation key pairs and certificates for TNLoA administration and call signing

PKI credentials may be used for different purposes as part of TNLoA management and call processing, and therefore it is likely that there will be different PKI keypairs for administrative use versus user call signing, and that these keypairs will be held in different keystore elements within the user’s network, namely in the TN administration system versus the user or SP PASSporT signing function. Since these are used at different frequencies and in elements that may have different security characteristics, the associated keypairs may also need to be cycled on different schedules. Where distinct keypairs and certificates are used by a given enterprise entity for administration and call signing the certificates should still be tied to the same EV identity, and they should be provided by the same EV CA to ensure they correspond to the same real-world identity and identity proofing procedure. A Subject Alternative Name elements may contain a domain name to distinguish the function the certificate is associated with (administrative or call signing). The Subject Common Name field should be avoided since its use would complicate matching of Subject name across certificates (its usage is deprecated in the latest EV Guidelines [Ref. 4]). For instance, in reference to a U.S. business entity the following EV Subject elements in the X.509 certificate should match across the certificates to indicate they belong to the same legal entity. Note that subject serial number refers to the corporation registration ID in the state of jurisdiction:

|  |  |
| --- | --- |
| Certificate Field | OID |
| subject:countryName  | 2.5.4.6 |
| subject:stateOrProvinceName | 2.5.4.8 |
| subject:localityName  | 2.5.4.7 |
| subject:jurisdictionCountryName  | 1.3.6.1.4.1.311.60.2.1.3 |
| subject:jurisdictionStateOrProvinceName  | 1.3.6.1.4.1.311.60.2.1.2 |
| subject:organizationName  | 2.5.4.10 |
| subject:businessCategory  | 2.5.4.15 |
| subject:serialNumber  | 2.5.4.5 |

# Use cases:

The following use cases illustrate possible ways the TNLoA mechanism may be used when the TN-U does and does not have a direct relationship with either the TN-SP and/or the O-SP. For comparison, a “base” use case is included to illustrate identity, authentication, and TN authorization where the TN-U is directly known (is Customer and TN Assignee) to one SP. The remaining cases build on this procedure and show the exchange of identity and authorization information between more parties.

## Base Use Case – Single Customer, TN-SP is the same as O-SP

### Description:

As a base reference use case, this is the authorization process between two parties, a Customer and an O-SP that also provides TN assignments, without the need to reference authorizations made by or to other parties. In this case the identity, TN management, and UNI credential management processes are all between the two parties using bi-laterally exchanged information and not requiring TNLoA exchange.

### Identity management

Customer establishes its identity to TN-SP/O-SP as part of a subscriber on-boarding procedure.

### TN management

TN-SP/O-SP assigns TNs to Customer. As O-SP, TN-SP/O-SP populates Customer record in AAA function with assigned TNs

### UNI interface credential management

Customer and O-SP exchange UNI authentication credentials (IP whitelist addresses, registration identity/password, shared secrets, VPN configurations and credentials, etc. as appropriate).

### Call flow and policy application

Customer establishes authenticated/identified UNI to O-SP using pre-exchanged credentials

Customer initiates call to O-SP network containing a (customer-asserted) calling TN

O-SP AAA function checks calling TN against authorized TNs in customer record

If calling TN matches an authorized TN in the customer record O-SP may populate an A attestation level, otherwise it may populate a B attestation level

Upon delivering the call to an egress IP-NNI, O-SP populates an Identity header containing a SHAKEN PASSporT with the customer-asserted calling TN and the determined attestation level



## Simple LoA Use Case – Single Customer, TN-SP is different than O-SP

### Description:

In this use case an O-SP’s Customer wishes to initiate calls using calling TNs provided by a separate TN-SP. The Customer, as TN Assignee, establishes a universally recognizable and verifiable identity via EV-like procedures and proves that identity to its TN-SP and O-SP. The Customer requests that the TN-SP make a TNLoA available to one or more O-SPs. The O-SP pulls the TNLoA information and populates an authorization database. When the customer places calls with TNs contained in a retrieved TNLoA the O-SP may mark the SHAKEN PASSporT with the full attestation value.

Note that this use case also covers the scenario where a call is originated by a C2 where the calling TN is assigned to the Customer. The C2 identity is not referred to as part of the TN authorization or UNI identity determination procedures and is only traceable through the Customer.

### Identity management

Customer proves its real-world identity to a 3rd-party certification authority via an EV or similar identity proofing procedure. The CA provides a PKI certificate tied to a universally recognizable subject value. Based on industry agreement, the set of authorized CAs for the enterprise certificates may be any accredited CA for providing EV certificates or a limited set specifically accredited by the industry.

Customer establishes its real-world identity separately to a TN-SP and an O-SP, and provides its EV certificate to the SPs. Customer may prove it is the entity named in the EV certificate via a request document signed with PKI credentials and/or signing of a challenge from the TN-SP and O-SP.

### TN management

TN-SP assigns TNs to Customer. Customer requests TN-SP to make a TNLoA available to O-SP. Customer requests O-SP to pull TN authorizations to its TN-U/TN Assignee identity from one or a set of TN-SPs. O-SP populates Customer record in AAA function with TNs assigned to Customer by TN-SP.

### UNI interface management

Customer and O-SP exchange UNI authentication credentials (IP whitelist addresses, registration identity/password, shared secrets, VPN configurations and credentials, etc. as appropriate). No additional UNI management procedures are required.

### Call flow and policy

Customer establishes authenticated/identified UNI to O-SP using pre-exchanged credentials

Customer initiates call to O-SP network containing a (customer-asserted) calling TN

O-SP AAA function checks calling TN against authorized TNs in customer record

If calling TN matches an authorized TN in the customer record O-SP may populate an A attestation level, otherwise it may populate a B attestation level.

Upon delivering the call to an egress IP-NNI, O-SP populates an Identity header containing a SHAKEN PASSporT with the customer-asserted calling TN and the determined attestation level.



## Indirect Call Origination Use Case

### Description:

In one indirect use case a call is originated by a C2 entity and the calling TN is assigned to the C2. For example, C2 might be an enterprise end user with its own TNs but utilizing a voice service reseller for some calls. At Customer’s request, O-SP maintains Customer/C2 entity associations in the Customer AAA record, and pulls TNLoA information from C2’s TN-SP. At call time, O-SP BCF checks the call was received on authenticated Customer UNI and that C2 originated the call. If the Customer-to-C2 relationship exists in O-SPs Customer AAA record and the C2-to-TN relationship exists in Customer’s AAA record, O-SP may populate the full attestation value in the SHAKEN PASSporT.

### Identity management

C2 proves its real-world identity to a 3rd-party certification authority via an EV or similar identity proofing procedure. The CA provides a PKI certificate tied to a universally recognizable subject value (see previous use case for details of EV-based identity proving procedure).

C2 establishes its real-world identity to TN-SP and Customer and proves its PKI subject identity. At Customer request, C2 proves its PKI subject identity to O-SP.

### TN management

TN-SP assigns TNs to C2. Customer provides O-SP list (O-SPs that Customer uses to originate traffic) to C2 and C2 provides a TN-SP list to O-SP. C2 requests TN-SP to make a TNLoA available to Customer O-SPs. Customer requests O-SP to pull TNLoAs for C2 (as TN-U/TN-assignee) from one or a set of TN-SPs. O-SP populates Customer record in AAA function with TNs assigned to C2 by TN-SP(s).

### UNI interface management

Customer and O-SP exchange UNI authentication credentials (IP whitelist addresses, registration identity/password, shared secrets, VPN configurations and credentials, etc. as appropriate). Likewise, C2 and Customer exchange user interface authentication credentials (this is the “indirect user interface” between the C2 and the Customer and is outside of UNI authentication between the Customer and O-SP).

In conjunction with identity management procedure, O-SP populates C2 as an entity authorized to utilize Customer’s UNI in Customer’s AAA record. C2 establishes PKI credentials to authenticate itself to O-SP (e.g. via an Identity header containing a base PASSporT signed with enterprise credentials – see “call flow and policy” below). The credentials need not be the same as those used to establish an identity for administrative purposes but they do need to resolve to the same EV-established subject name and should come from the same CA to assure they tie to the same identity-proofing practice. The O-SP would presumably know that they are not expecting SHAKEN Identity headers from a Customer outside the SHAKEN ecosystem, so they may choose to verify against CAs authorized to provide enterprise credentials.

### Call flow and policy

Customer establishes authenticated/identified UNI to O-SP using pre-exchanged credentials

C2 establishes authenticated/identified user interface (indirect user interface) to Customer using pre-exchanged credentials.

C2 initiates a call to Customer containing a C2-asserted calling TN. The SIP INVITE contains a user-populated Identity header containing a base PASSporT signed with C2’s EV credentials.

Customer matches INVITE to C2’s authenticated user interface and forwards the INVITE via its UNI to O-SP. The user-populated Identity header is passed transparently.

O-SP BCF matches the INVITE to Customer’s authenticated UNI. O-SP authenticates C2 identity via verifying the base PASSporT against C2’s EV certificate.

O-SP AAA function checks that C2 is authorized to utilize the Customer UNI, and that the calling TN has an authorization for C2 in Customer’s record

If calling TN matches an authorized C2 and TN in the customer record O-SP may populate an A attestation level, otherwise it may populate a B attestation level.

Upon delivering the call to an egress IP-NNI, O-SP populates an Identity header containing a SHAKEN PASSporT with the customer-asserted calling TN and the determined attestation level.



## Delegation Use Case – C2 is TN Delegee

### Description:

In this use case, the calling entity/TN-U is known indirectly to both the TN-SP and O-SP, that is it is both C2 and a TN Delegee. An example of this use case would be a call center contractor making calls on behalf of an enterprise (the TN Assignee) with the enterprise’s calling TNs, and utilizing a service reseller to originate traffic through various O-SPs. The 3rd-party TN Assignee is not part of the call flow but has authorized the use of its TNs to its contractor. In addition to the identity proofing and Customer-requested authorizations for a C2 to originate calls via the O-SP, the 3rd-party TN Assignee must request that the TN-SP make TNLoA documents available tying some of its assigned numbers to the TN Delegee.

### Identity management

C2 proves its real-world identity to a 3rd-party certification authority via an EV or similar identity proofing procedure. The CA provides a PKI certificate tied to a universally recognizable subject value (see previous use case for details of EV-based identity proving procedure).

TN Assignee proves its real-world identity to a 3rd-party certification authority via an EV or similar identity proofing procedure (TN Assignee identity is needed as part of traceability of the assignment and delegation). TN Assignee establishes C2 identity and C2 proves its identity by executing a transaction with the EV credentials. C2 proves its identity using EV credentials to TN-SP (via its relationship with TN Assignee), Customer, and O-SP via its relationship with Customer.

### TN management

TN-SP assigns TNs to 3rd-party assignee. 3rd-party assignee requests TN-SP to provide TNLoA documents for some assigned TNs delegated to C2 (as the TN Delegee). TN-SP learns Customer O-SPs via TN Assignee and C2. Customer requests O-SP to pull TNLoA documents tied to C2 as TN Delegee (TN-U identity contains both the TN Assignee subject name and the C2/TN Delegee subject name). O-SP learns TN Assignee’s TN-SPs via TN Assignee and C2/TN Delegee. O-SP pulls TNLoA documents tied to TN Assignee/TN Delegee (C2) and populates the TN authorizations in Customer’s AAA record.

### UNI interface management

Same as for the case where C2 is directly assigned the TNs (the TN delegation does not alter the identity and authentication of the C2 entity.

### Call flow and policy

Customer establishes authenticated/identified UNI to O-SP using pre-exchanged credentials

C2 establishes authenticated/identified user interface (indirect user interface) to Customer using pre-exchanged credentials.

C2 initiates a call to Customer containing a C2-asserted calling TN. The SIP INVITE contains a user-populated Identity header containing a base PASSporT signed with C2’s EV credentials.

Customer matches INVITE to C2’s authenticated user interface and forwards the INVITE via its UNI to O-SP. The user-populated Identity header is passed transparently.

O-SP BCF matches the INVITE to Customer’s authenticated UNI. O-SP authenticates C2 identity via verifying the user-populated Identity header against C2’s EV certificate.

O-SP AAA function checks that C2 is authorized to utilize the Customer UNI, and that the calling TN has an authorization for C2 in Customer’s record. The difference from the previous use case is that the C2 identity matches the TN Delegee in the TN record.

If calling TN matches an authorized C2 (as TN Delegee) and TN in the Customer record O-SP may populate an A attestation level, otherwise it may populate a B attestation level.

Upon delivering the call to an egress IP-NNI, O-SP populates an Identity header containing a SHAKEN PASSporT with the customer-asserted calling TN and the determined attestation level.



## Additional use cases

This model should enable any scenario where there is at most one level of indirection between the TN User and both the O-SP and TN-SP. Additional levels of indirection would cause service providers to rely on parties that are not their customer or not known directly to their customer which may cause problems both from a traceability and authorization perspective. Longer authorization chains, either in the upstream-direction for call processing (e.g. the TN-U is a C3 entity or greater) or further down a delegation chain (TN Delegee further delegates use of the TN) are harder to secure and audit. While a Customer, for instance, could indicate to an O-SP to accept a C3’s TNLoAs, that puts the Customer in a position of needing to validate that the TNs are correctly arriving from a C2, and that chain is now hidden from the O-SP. While a TN-U entry could theoretically carry “delegee 1” and “delegee 2” values to indicate a delegation chain, the TN-SP would need to rely on the authorization of a party it has no direct relationship with (the original TN Delegee) to populate that TNLoA. Exchange of TN-SP and O-SP identities for a TNLoA exchange is also further complicated by longer authorization chains. Within a chain of a single layer of indirection in either the call-processing or TN authorization dimension, there are a number of use cases that are supportable by this system in addition to those described above. These include the following:

1. A TN Assignee delegates a TN to Customer, Customer originates call through O-SP
2. Customer is TN Assignee, Customer makes use of the TN available to C2 (Customer is the TN-U and authorization traces to Customer)
3. C2 is TN Assignee, C2 makes use of the TN available to C3 (C2 is the TN-U and authorization traces to C2)
4. TN-SP assigns TN to another (3rd party) SP. SP delegates TN to Customer. Customer originates call through O-SP other than the TN-SP or 3rd party SP (Customer is TN Delegee).

**Annex A**

(/informative)

# A Administrative transactions to implement TNLoA request and exchange

A.1 Customer/TN Assignee interfaces and inter-SP interfaces

The TNLoA exchange interface is expected to handle a high volume of transactions and is required to be persistently available among the service providers for both TNLoA download and subscribe/notify transactions. Therefore a machine interface (e.g. REST with appropriate bi-laterally exchanged credentials between service providers) is an appropriate implementation. Administrative transactions from Customers to their OSPs and from TN Assignees to their TN-SPs are expected to be of varying volume so while there needs to be a machine interface defined there might be some use cases that could be supported by interactive interfaces. The following is a set of transactions that are required to implement identity exchange, TNLoA requests and download requests, and the inter-SP exchange and subscribe/notify to support this process.

A.2 Transaction descriptions

1. Customer or TN Assignee associates its own EV identity with TN-SP or O-SP customer account
2. Customer or TN Assignee associates C2 or TN-D EV identity with TN-SP or O-SP customer account (proxy challenge between TN-SP and TN-D or O-SP and C2)
3. (customer updates/refreshes EV identity, customer disassociates self or C2/TN-D EV identity)
4. TN-A requests TNLoA for its own TNs from TN-SP
5. (TN-A requests discontinuance/modification of TNLoA for its own TNs)
6. TN delegation transaction: TN-A requests TNLoA for delegated TNs from TN-SP, TN-A returns TN-SP and delegated TNs to TN-D
7. (TN-A requests discontinuance/modification of TNLoA for TN delegations)
8. Customer requests TNLoA download for self to O-SP
9. Customer requests TNLoA download for C2 to O-SP
10. (Customer requests modification/discontinuance of TNLoA download for self/C2)
11. O-SP requests download of TN-A’s TNLoA documents from TN-SP
12. O-SP requests download of TN-D’s TNLoA documents from TN-SP
13. O-SP subscribes to update notifications for TN-A/TN-D from TN-SP
14. O-SP cancels subscription to update notification for TN-A/TN-D from TN-SP
15. TN-SP notifies O-SP of updates available for TN-A/TN-D TNLoA documents