**Contribution**

**TITLE:** Contribution on a method of determining SHAKEN attestation levels using enterprise-level credentials and Telephone Number Letter of Authorization Exchange

**SOURCE:** Doug Bellows, Inteliquent, Inc.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**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. This document offers a proposal to treat the authentication of a customer and/or TN assignee/delegee separate from the authorization decision. Furthermore, this document proposes to use 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. Authorization is established in the administrative plane and checked by the originating service provider subject to enterprise authentication. This information is offered as a possible addition to an existing or new draft Technical Report.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**NOTICE**

This is a draft document and thus, is dynamic in nature. It does not reflect a consensus of the ATIS-SIP Forum IP-NNI Task Force and it may be changed or modified. Neither ATIS nor the SIP Forum makes any representation or warranty, express or implied, with respect to the sufficiency, accuracy or utility of the information or opinion contained or reflected in the material utilized. ATIS and the SIP Forum further expressly advise that any use of or reliance upon the material in question is at your risk and neither ATIS nor the SIP Forum shall be liable for any damage or injury, of whatever nature, incurred by any person arising out of any utilization of the material. It is possible that this material will at some future date be included in a copyrighted work by ATIS or the SIP Forum.

# Introduction

The SHAKEN (ATIS-1000074-E) Identity header provides a means to authenticate the originating service provider (SP) for a call being established across one or more IP-NNIs and to protect the integrity of the call parameters populated by the originating SP. The parameters include the calling and called telephone numbers (TNs) and an attestation marking that describes the extent to which the originating SP has (a) determined the identity of a customer it received a call from and (b) determined an association between the calling TN and the customer. The terminating SP that relies on this information populated in a received (and verified) Identity header can determine the extent to which the originating 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 number. In many legitimate calling scenarios the originating service provider does not directly possess information that might allow it to determine a customer’s association with a calling TN for one or more reasons including the following:

1. The customer utilizes multiple originating service providers and marks calls with a common calling TN (e.g. a main business number)
2. The customer and end-user are different entities and the calling TN is assigned to the end user (e.g. the customer of a reseller or value-added service provider that is not the SP populating the Identity header), not the customer directly known by the originating SP
3. An enterprise or other organization contracts for calling services provided by another entity and calls are placed using the contracting organization’s calling TNs
4. TNs are assigned by a service provider to one entity that resells use of those numbers to an originating SPs customer or an unrelated end-user entity

This document proposes a method to allow an originating SP to determine that the calling TN can be associated with the customer, and therefore give the originating SP a basis for marking a call from a known and authenticated customer with full attestation. 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 Framework” (currently in draft form as IPNNI-2019-00003R005):

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 for the call when it is sent across an NNI to an intermediate or terminating SP. Note that this procedure is only applicable when the O-SP receives the call via a UNI (customer interface) and not via an NNI since the administrative procedures rely on there being 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” 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, which are indirectly placed on the Customer’s UNI interface to the originating SP. There may be additional levels of indirection (e.g. a “C3 customer”) but see notes below regarding call 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 assigns them to other entities.

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 the delegee’s 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 an outbound call center contractor for calling services executed on its behalf.

LoA or TNLoA: Telephone Number Letter of Authorization – A document exchanged between SPs to indicate a TN User is authorized to utilize a calling TN.

Other 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 Framework” (currently in draft form as IPNNI-2019-00003R005).

# General description of the proposed solution:

The proposed solution 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 TN-SPs and O-SPs (described below as the “LoA” process). TN authorization to the TN-U may either be through direct assignment by the TN-SP or by delegation from the assignee.

## Identity management process

As described in the Attestation Framework document (in draft form), 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 authorization process, the bi-lateral exchange of (enterprise) identity information and TN assignments are sufficient for the O-SP to make subsequent authorization determinations, in particular the TN authorization decision used to provide full attestation marking in the SHAKEN PASSporT.

When additional parties are involved in the authorization process, including separate TN-SPs and O-SPs and entities with only an indirect relationship to the O-SP or TN-SP (for example C2 entities and TN delegees), there is a need for a form of identity that is commonly recognized and verifiable across all parties involved in the process to drive authorization transactions and to authenticate the party claiming to be authorized in the administrative channel and at the UNI. This document proposes using PKI credentials tied to a proven real-world identity at the enterprise level, possibly similar to web Extended Validation (EV) procedures. In an EV X.509 certificate the subject typically contains a business name, location, and government registration ID. In the USA this includes the 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 the common EV procedures or a possible enhanced procedure. 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 the proposal is that for TN authorization purposes these transactions are only triggered by entities with the direct relationship to the SP). Similarly, service providers involved in the authorization exchange may identify themselves using PKI credentials similar to SHAKEN certificates that are tied to an industry-recognized service provider code (SPC), traceable to a real-world business identity verified by industry and regulatory processes.

## LoA 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-U). 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 use by a direct assignee the TN-U element will contain the identity of the TN 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. The documents would be signed with the TN-SPs credentials (e.g. certificates similar to 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 could be the SHAKEN store or a similar set of CAs authorized to provide certification of service provider identity. 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>

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

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

}

}

Payload claims:

iss – Issurer (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 (a complete scope replaces all previous authorizations)

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

A proposed method for the exchange of the documents is a “pull” mechanism initiated by the O-SP, combined with a notification (e.g. push notification) mechanism from the TN-SP to trigger updates for specific TN-U authorizations. 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, there should be a notification mechanism to allow the TN-SP to trigger the O-SPs relying on particular sets of TNLoA documents to pull the updated sets of documents. An O-SP may also audit TN authorizations against porting activity to identify those no longer valid due to porting (presumably the authorization could be moved to the new serving TN-SP).

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 access 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).

# 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 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 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 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 an “enterprise Identity header” signed with C2’s enterprise credentials.

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

O-SP BCF matches the INVITE to Customer’s authenticated UNI. O-SP authenticates C2 identity via verifying the enterprise Identity header against C2’s enterprise 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 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 an Enterprise Identity header signed with C2’s enterprise credentials.

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

O-SP BCF matches the INVITE to Customer’s authenticated UNI. O-SP authenticates C2 identity via verifying the Enterprise Identity header against C2’s enterprise 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 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.