**ATIS-0x0000x**

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN):**

**Proof-of-Possession of Telephone Numbers (TN-PoP)**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This technical report defines mechanisms that enable a Service Provider to delegate STI authentication authority for a subset of its TNs to another entity. This delegation capability is needed to support STI for cases such as multi-homed SIP-PBXs, where the authorized owner of a TN does not provide originating call services for that TN.

**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** |
| --- | --- | --- | --- |
| June 29, 2017 | Initial | Baseline | David Hancock |

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

1.3 Application 1

2 Normative References 2

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 2

4 Overview 3

4.1.1 PoP Certificate 3

4.1.2 PoP PASSporT Token 4

4.1.3 TN PoP Requirements 4

4.1.4 TN PoP Procedures 4

5 TN Proof-of-Possession Architecture 7

5.1 TN Proof-of-Possession Cert Management Message Flow 8

A Annex Title 10

**Table of Figures**

Figure 1. Obtaining a PoP Certificate 5

Figure 2. PoP Certificate support of STI Authentication & Verification during Call Setup 6

Figure 3. SHAKEN Architecture to support Management of PoP Certificate 7

Figure 4. Procedure to obtain PoP certificate 8

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

TN Proof-of-Possession (TN PoP) is an extension to the base SHAKEN framework that enables an STI-authorized service provider to delegate authority for a subset of its telephone numbers to another non-STI entity. The non-STI entity can then use this “proof of possession” to provide cryptographically proof to STI verification services that it has authority to originate calls from the delegated TNs.

This specification addresses all aspects of extending SHAKEN to support TN Proof-of-Possession, including:

* The TN PoP certificate management procedures
* The TN PoP authenticate and verification procedures during SIP call establishment

## Purpose

*Note: this section still under construction.*

TN Proof-of-Possession provides a method that enables an originating entity to prove it is authorized to use the calling TN, even when the originating Service Provider does not have authority over the calling TN. Such cases include:

* *Multi-homed PBXs, where the enterprise uses multiple service providers (e.g., for redundancy or least cost routing) but obtains its numbers from just one SP. In this scenario, the PBX can legitimately originate a call via one SP but insert a calling TN owned by another SP.*
* *Toll-free numbers, where an enterprise originates a call via a host SP, but wants to display a toll-free call-back number that it purchased from a RespOrg. This scenario often applies in call centers.*
* *Legitimate spoofing cases, such as when a user originates a call using the user’s personal phone but delivers the user’s work TN.*
* *Automated outbound dialing services*

## Application

xxx

# 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.

ATIS-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

# 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

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# Overview

The base SHAKEN framework defined in [specs ref] enables an originating SP to provide full SHAKEN attestation when it has a verified association with the calling TN. However, there are a number of real-world scenarios where this is not the case; i.e., where an SP provides originating services for a calling TN, and the SP has no knowledge of the legitimacy of the calling TN. These include the following:

* A PBX that is configured with multiple SIP Trunks across multiple Service Providers (e.g., for redundancy or least cost routing) originates a call via one SPs from a calling TN that it obtained from another SP
* An enterprise originates a call via its host SP but wants the caller ID to display a toll-free number that it obtained from a RespOrg
* A legitimate spoofing service displays a user’s work TN for calls originated from the user’s home phone
* An automatic outbound dialing service originates a call via its host SP using a calling TN that is owned by another SP (e.g. a school subscribes to an outbound calling service that announces snow-day closings and displays the school TN)

For these types of call scenarios, the originating SP has no verified association with the calling TN, and therefore, it cannot fully attest that the originator can legitimately use that TN. This puts these calling users at a disadvantage, since the value of delivering calls with full SHAKEN attestation won’t be available to them (e.g., the value in achieving higher answer rates for calls that provide a “calling TN verified” display to the called user).

This document describes a mechanism called TN Proof-of-Possession that extends the base Secure Telephone Identity procedures defined by IETF STIR to enable a calling TN to be authenticated with full attestation when TN ownership and originating call processing are split between two different providers.

TN Proof-of-Possession defines two new entities:

1. Telephone Number Provider (TN Provider):
   * An entity that is authoritative over a set of telephone numbers, and that can delegate a subset of those telephone numbers to another entity. In the context of this document, a TN Provider is an STI Service Provider as defined in the base SHAKEN specification (i.e., a TN Provider is authorized by the STI-PA to obtain end-user certificates from an STI-CA).
   * Ultimately the entities entitled to obtain STI Certificates will be defined by the STI-GA, but the initial definition is “Service Providers with an OCN (Operating Carrier Number) and eligible to directly obtain TNs.
2. Customer Application Function (Customer AF):
   * A non-STI-authorized entity that purchases (or otherwise obtains) delegated telephone numbers from a Telephone Number Provider.
   * Examples include an Enterprise PBX, a legitimate spoofing application, or an automated outbound dialing service.

The TN PoP framework provides a way for the Customer AF to obtain a PoP certificate from the TN Provider, that the Customer AF can then use the to prove to remote verification services that the calling TNs is being used legitimately.

### PoP Certificate

The base SHAKEN Governance Model and Certificate Management specification [add ref] mandates support for STI certificates that have a scope of authority expressed in terms of the identity of the certificate holder. Specifically, the TN Authorization List of the SHAKEN STI certificate must contain a ServiceProviderCode data item that identifies the SP holding the certificate. The assumption is that a terminating network performing STI verification trusts that an originating SP will sign PASSporT tokens only when it has established a verified association with the TN used for the call. This is a reasonable assumption, given that the STI-VS can verify that the originating SP has been authorized by the STI-PA to perform SHAKEN authentication.

Since a Customer AF is not an STI-authorized entity, it would not be appropriate to have verification services blindly trust that an originating Customer AF holding a valid PoP certificate is authorized to use the calling TN. The scope of a PoP certificate must therefore be expressed in more granular terms that explicitly identify the TN or set of TNs that have been delegated by the TN Provider to the Customer AF. In this way, a verifier can check that the calling TN is on the list of TNs identified by the PoP certificate. This more granular scope for TN PoP certificates is achieved using the TelephoneNumber, and TelephoneNumberRange data types of the TN Authorization List.

### PoP PASSporT Token

TN PoP extends the base PASSporT token defined in draft-ietf-stir-passport. This PASSporT extension serves two purposes. First, it enables a specific set of claims to be defined for the PoP PASSporT token. Second, the PoP PASSporT “ppt” extension can serve as a trigger to inform the remote verification service that it must perform additional PoP verification procedures; specifically, the PoP-VS must verify that the calling TN belongs to the set of TNs identified in the TN Authorization List of the PoP certificate.

### TN PoP Requirements

This section describes the overall requirements that apply to the TN PoP solution.

1. When a TN provider delegates a subset of its TNs to a Customer AF, it may optionally provide a PoP certificate for the delegated TNs. A PoP certificate is required only if the Customer AF wants to originate calls from the delegated TNs with full attestation via an originating Service Provider that is different than the delegating TN provider.
2. A TN provider must ensure that the scope of a PoP certificate provided to a Customer AF covers only the TNs that it has delegated to the Customer AF.
3. A TN provider must not provide TN PoP certificates for TNs that it does not own.
4. When renewing a PoP certificate, the TN provider must ensure that the scope of the new PoP certificate identifies the set of TNs currently delegated to the Customer AF.
5. When originating a call from a delegated TN that is in-scope for one of its PoP certificates, the Customer AF must use the PoP certificate to perform PoP authentication service (i.e., build an Identity header containing a PoP PASSporT token for the calling TN).
6. An originating SP serving the Customer AF must convey any PoP Identity header received from the Customer AF unchanged toward the terminating network. In other words, TN PoP Identity headers are carried end-to-end from the originating Customer AF to the terminating network.

*Discussion – why don’t we mandate that the originating SP verify the received PoP PASSporT token, and if valid, replace it with a SHAKEN Identity header containing a SHAKEN PASSporT token with full attestation? Two reasons. First, the originating SP isn’t responsible for the delegation of TNs from the TN provider to the customer AF, and therefore its reputation should not be negatively impacted if something goes wrong. An SP should only be required provide full SHAKEN attestation for calling TNs that it owns (or has a verified association with) – requiring it to do anything beyond that would be outside the spirit of SHAKEN. Second, if a problem is detected post-verification, then we want to identify the TN provider so it can revoke the PoP certificate that was used. Carrying the PoP Identity header end-to-end provides post-verification trace-back procedures with the information needed to easily identify the TN provider.*

1. A PoP PASSporT token implicitly indicates “full” attestation. Therefore, the PoP PASSporT token does not require an explicit attestation claim.

*Discussion: is there any reason why a Customer AF would want to generate a PoP PASSporT token with anything other than full attestation?*

*Discussion: Should we allow a PoP PASSporT token to include an origid, for example, to allow the enterprise to differentiate between two locations or departments?*

### TN PoP Procedures

This section describes the information flow associated with the TN PoP procedures for managing PoP certificates, and using PoP certificates to authenticate and verify delegated TNs during call establishment.

#### PoP Certificate Management

Figure 1 shows the high-level overview of the procedure to provide TN Proof-of-Possession to the Customer AF.



Figure 1. Obtaining a PoP Certificate

At 0) in Figure 1, the TN Provider delegates a subset of its TNs to the Customer AF. This is typically done at service turn-up time via a web-portal or API hosted by the TN Provider. Once it knows the set of TNs that it has been allocated, the Customer AF initiates the procedure to obtain a PoP certificate that it can use as proof that it has authority for those TNs:

1. The Customer AF first generates a public/private key pair, and stores the private key in a private key store. The public key will be carried in the PoP certificate. The Customer AF will use the private key later, during origination call processing, to sign calling TNs.
2. The Customer AF asks the TN Provider for a PoP certificate that has a scope of authority covering the delegated TNs, and that contains the public key generated in (1).
3. Once the TN Provider has verified that the received request is valid (e.g., requested scope does not exceed delegated set of TNs), then the TN Provider requests a PoP certificate from the STI-CA, following the normal procedures defined by SHAKEN Certificate Management.
4. The STI-CA generates a PoP certificate that chains to one of the CA’s root certificates, and returns it to the TN Provider at (4).
5. The TN Provider stores the PoP certificate in its STI-CR in order to make it available to remote verification services.
6. The TN Provider delivers the PoP certificate to the Customer AF.

#### TN PoP Authentication and Verification

Figure 2 shows the high-level overview of TN PoP authentications and verification procedures used during call establishment.



Figure 2. PoP Certificate support of STI Authentication & Verification during Call Setup

Figure 2 assumes that the Customer AF and TN Provider have already complete the procedure to obtain a PoP certificate described in Figure 1. The call establishment procedure in Figure 2 is kicked off when the Customer AF receives an origination request to called TN-x from one of its delegated TNs (TN-a in this example).

1. The Customer AF Call Control function invokes the PoP-AS to perform authentication services for calling TN-a. The PoP-AS constructs a PoP PASSporT token containing the calling TN-a, and signs it using the private key associated with the PoP certificate. The PoP-AS then includes the PoP PASSporT token and the PoP certificate URL in a new Identity header.
2. The Customer AF Call Control includes the newly created Identity header in the originating INVITE to the originating SP.
3. The originating SP Call Control forwards the INVITE, including the PoP Identity header, to the terminating SP serving TN-x, following normal SIP routing procedures. The originating SP may choose to add a second SHAKEN Identity header (not shown) with “partial” attestation (“partial” because the SP does not own the calling TN). The value of this second Identity header is somewhat limited; basically, it enables the originating SP to record an “origid” claim that identifies the ingress point point used by the originating Customer AF.
4. The terminating SP Call Control invokes the STI-VS to perform verification services for the received INVITE.
5. The STI-VS first fetches the PoP certificate from the TN Provider using the received PoP certificate URL. It then verifies the received Identity header; e.g., checks that the PoP certificate chains to an authorized STI-CA, verifies that the PASSporT signature using the public key of the PoP certificate, and verifies that the calling TN is within the scope of authority of the PoP certificate.
6. The Terminating SP updates the Verstat parameter to indicate that the calling TN has been verified, and sends the INVITE to the called endpoint registered for called TN-x.

# TN Proof-of-Possession Architecture

Figure 2 shows how the SHAKEN certificate management architecture can be extended to support TN Proof-of-Possession certificates. TN PoP reuses many of the same concepts and mechanisms defined by the base SHAKEN architecture. The Customer Application Function plays a role similar to the Service Provider defined by SHAKEN, using the ACME protocol to obtain certificates from the STI CA. Since the Customer AF is not an STI-authorized entity however, it cannot talk to the STI-CA directly, but must work through the TN Provider that provided it with its set of TNs. The Telephone Provider therefore acts as a proxy between the Customer AF and the STI-CA.



Figure 3. SHAKEN Architecture to support Management of PoP Certificate

As shown in Figure 3, the new functional entities are added to the SHAKEN architecture to support the management of PoP certificates:

Customer Application Function entities:

* SKS – a Secure Key Store to store the private keys associated with PoP certificates.
* PoP-AS – the function that authenticates the calling TN using a PoP certificate and its private key
* CAF-KMS – plays a role similar to the SP-KMS

Telephone Number Provider entities:

* ACME Proxy – acts as an interworking function between the CAF-KMS and the STI-CA. From the perspective of the CAF-KMS, the ACME Proxy appears as a CA to the CAF-KMS, and as SHAKEN-compliant SP-KMS to the STI-PA and STI-PA.

## TN Proof-of-Possession Cert Management Message Flow

Figure 4 shows the message flow to obtain a PoP certificate.

*Note – this section contains a number of open issues – mostly related to how can we take advantage of the close relationship between TN Provider and Customer AF to simplify the ACME procedure (and therefore encourage adoption). For example, how does the ACME Proxy authenticate the Customer AF?*



Figure 4. Procedure to obtain PoP certificate

This procedure assumes that the TN Provider has already obtained a valid SPC token from the STI-PA, and has created an ACME account with the STI-CA. At service turn-up time, the Customer AF obtains a set of TNs from the TN Provider. The TN Provider also provides the Customer AF with the information it needs to obtain a PoP certificate covering those TNs, including the ACME credentials it will need to obtain a PoP certificate, and a URL to the ACME directory resource. The Customer AF queries the ACME directory resource to obtain the other ACME URLs it will need to obtain a certificate, including the new-account and new-order URLs. (Note that in the case of PoP certificates, both the new-account and new order URLs will resolve to the TN Provider’s ACME Proxy.) Once it has this information, the Customer AF initiates the following procedure to obtain a PoP certificate:

1. The CAF-KMS generates a public/private key pair for the PoP certificate, and stores the private key in the SKS.
2. The CAF-KMS generates a 2nd public/private key pair for the ACME account, and requests creation of a new ACME account using the new-account URL (i.e., to the ACME Proxy). The new account is identified by the account’s public key. The ACME Proxy creates its local version of the account, and returns an ACME “account created” response to the CAF-KMS.

*Question – can we simplify the account creation process for the CAF-KMS; e.g., have the ACME Proxy generate the account key pair and provide it to the CAF-KMS (would provide a kind of “shared-secret” authentication), or have the ACME Proxy create the account on behalf of the CAF-KMS?*

1. The CAF-KMS requests a new PoP certificate using the new-order URL identified by the directory resource. The CSR in the request contains the public key generated in step-1, and the list of delegated TNs. The ACME Proxy returns a challenge to the CAF-KMS.

*Open issue – what Identity challenge is this (in the context of the ACME draft)?*

1. The CAF-KMS responds to the challenge received in step-3. The ACME Proxy checks that the challenge response is valid, and verifies that the Customer AF is authorized to request the PoP certificate attributes specified in the CSR received in step-3 (e.g., verify that the list of TNs has in fact been delegated to the Customer AF).
2. The ACME Proxy sends a request for a new PoP certificate to the STI-CA. The request includes the CSR received by the ACME Proxy in step-3. The STI-CA returns a challenge to the ACME Proxy.
3. The ACME Proxy responds to the challenge received in setp-5 with a valid SPC token.
4. The STI-CA validates the challenge response SPC token with the STI-PA as specified by SHAKEN.
5. The ACME Proxy starts polling the STI-CA to determine when the PoP certificate has been issued, as specified by SHAKEN. When the PoP certificate is issued by the STI-CA, the ACME Proxy downloads the certificate.
6. The ACME Proxy stores the PoP certificate in the STI-CR.
7. In parallel with step-5, the CAF-KMS starts polling the ACME Proxy authorization resource. When it detects that the authorization resource status has transitioned to “valid” (meaning that it has satisfied the challenge from step-3), the CAF-KMS starts polling the ACME Proxy new-order resource. After the ACME Proxy stores the PoP certificate in the STI-CR in step-7, it sets its new-order resource status to “valid”, and updates the certificate URL to identify the STI-CR file where it has stored the PoP certificate. On detecting that the new-order resource has transitioned to “valid”, the CAF-KMS downloads the certificate using the new-order certificate URL. This URL will also be used by the PoP-AS to populate the certificate reference in the Identity header field and PoP PASSporT Token during PoP authentication.

(normative/informative)

# A Annex Title

Xxx