**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**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

TN Proof-of-Possession 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 inform other STI SPs 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 extensions to the base SHAKEN framework and certificate management procedures to support TN Proof-of-Possession
* The impacts to the SHAKEN SIP procedures to support TN Proof-of-Possession

## Purpose

In the majority of cases, the originating service provider owns the calling TN, and is therefore able to provide full SHAKEN attestation for that calling TN during STI-VS authentication. However, there are a number of voice services scenarios where this is not the case; where the originating service provider does not own the calling TN. These include:

* *Need to describe the different real-world cases where orig SP doesn’t own calling TN, for example…*
* *Multi-homed PBXs, where the PBX can originate a call via one of its host SPs from a calling TN owned by another host SP.*
* *Toll-free numbers, where an enterprise originates a call via its host SP using a toll-free calling number that it purchased from a RespOrg.*
* *Legitimate spoofing cases, such as when a user originates a call on her personal phone and delivers the office 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

Draft-ietf-stir-certificates-14 defines an X.509 certificate extension that specifies the scope of authority of the certificate in terms of the telephone numbers that the certificate holder has authority over. This extension enables an STI verification service to verify that the calling TN identified in a PASSporT token does in fact belong to the owner of the private key that signed the PASSporT token. The set of TNs authorized by a certificate is identified by a new certificate attribute called “TN Authorization List”. This attribute conveys three different data types:

1. ServiceProviderCode: identifies a Service Provider that holds the certificate
2. TelephoneNumberRange: specifies a contiguous range of telephone numbers authorized to be used by the holder of the certificate
3. TelephoneNumber: specifies a specific telephone number authorized to be used by the holder of the certificate

ServiceProviderCode has the semantics of “this certificate is authoritative for all the telephone numbers owned by this service provider”. The TelephoneNumber and TelephoneNumberRange data types are used to explicitly list the telephone numbers that are within the certificate’s scope of authority.

The base SHAKEN Governance Model and Certificate Management document [add ref] mandates support for the TN Authorization List extension, but only for the ServiceProviderCode data type. The assumption is that a terminating network performing STI verification trusts that an originating SP will sign PASSporT tokens only for calling numbers that it has authority over. This seems like a reasonable assumption, since the STI-VS knows that the originating SP was able to obtain a valid STI certificate that chains to the root certificate of authorized STI-CA.

This document describes how SHAKEN can be extended to support TN Proof-of-Possession using the “TN Authorization List” TelephoneNumber and TelephoneNumberRange data types.

## TN Proof-of-Possession Cert Management Architecture

This document defines two new entities for the SHAKEN framework:

1. Telephone Number 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
	* Examples include telephone service provider (LEC), RespOrg
2. Customer Application Function:
	* An entity that purchases (or otherwise obtains) delegated telephone numbers from a Telephone Number Provider
	* Examples include Enterprise PBX, legitimate spoofing app, automated outbound dialing service



Figure 1. Telephone Number Provider and Customer Application Function

As shown in Figure 1, the Telephone Number Provider delegates a subset of its TNs to the Customer Application Function, and also provides the Customer Application Function with the PoP certificate whose scope covers those same TNs.

Figure 2 shows how these two entities fit within the existing SHAKEN Governance and Cert Management framework. The TN Provider plays the role of an STI SP in the base SHAKEN framework, where it supports the SP-KMX, STI-CR, and SKS functions. The TN Provider also supports a new function; the ACME Proxy. an ACME Proxy that

Service Provider that authorized to obtain STI certificates from an STI-CA.



Figure 2. SHAKEN Architecture to support Management of PoP Certificate

*Add text describing above architecture diagram…*

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



Figure 1. Procedure to obtain PoP certificate

Figure 1 shows the high-level message flow to obtain a PoP certificate. At service turn-up time, the customer obtains a set of TNs from the SP, plus any additional information it needs to obtain a PoP certificate covering those TNs (e.g., ACME Proxy FQDN). Once it has the set of TNs, the PBX initiates the procedure to obtain a PoP certificate whose scope gives it the authority to initiate calls from those TNs. *PBX probably gets credentials from SP at this point too – need to mention that.*

1. The ACME client generates a public/private key pair, and stores the private key in the SKS.
2. The ACME client creates a CSR containing the public key, and the list of TNs it received from the SP. The ACME client sends a request for a PoP cert, including the CSR, to the ACME Proxy.
3. thru 6) The ACME proxy verifies that the TNs listed in the CSR have in fact been delegated to the customer. It then requests a PoP certificate from the STI-CA as described in the SHAKEN Governance/management spec, with the addition that the CSR passed to STI-CA contains a list of TNs delegated to the customer.
4. The ACME Proxy stores the new cert in the STI-CR
5. The ACME Proxy returns the cert plus the cert URL to the ACME Client.
6.

(normative/informative)

# A Annex Title

Xxx