**ATIS-0x0000x**

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) 2.0:**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The base-SHAKEN framework enables a VoIP Service Provider to deliver cryptographic proof to a called user that the calling user is authorized to use the calling telephone number. This specification extends the base-SHAKEN framework to provide a number of additional capabilities, including the ability to provide cryptographic proof of human readable calling user information such as calling name, the ability for SHAKEN-authorized TN Providers to delegate SHAKEN signing authority to their non-SHAKEN customers, plus a number of additional enhancements.

**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** |
| --- | --- | --- | --- |
| Feb 8, 2018 | Initial | Baseline | David Hancock |

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

1.2.1 Rich Call Data 1

1.2.2 Service Scenarios that require Delegation of SHAKEN Certificates 1

2 Normative References 3

3 Definitions, Acronyms, & Abbreviations 3

3.1 Definitions 3

3.2 Acronyms & Abbreviations 5

4 Overview 7

4.1 Functional Requirements 7

4.2 Certificate Authority Delegation via Cross Certification 8

4.3 Authorizing Cress-Certificate constraints per TN Provider 9

A Annex Title 10

**Table of Figures**

Figure 1. STI-CA delegates authority to a TN Provider Delegate CA 8

Figure 2. The STI-PA authorizes cross-certificate constraints 9

**Table of Tables**

**No table of figures entries found.**  
In your document, select the words to include in the table of contents, and then on the Home tab, under Styles, click a heading style. Repeat for each heading that you want to include, and then insert the table of contents in your document. To manually create a table of contents, on the Document Elements tab, under Table of Contents, point to a style and then click the down arrow button. Click one of the styles under Manual Table of Contents, and then type the entries manually.

# Scope, Purpose, & Application

## Scope

This specification extends SHAKEN to provide the following:

* Provide a lightweight secure certificate delegation mechanism that enables a TN Provider to delegate signing authority to its non-SHAKEN customers.

## Purpose

### Service Scenarios that require Delegation of SHAKEN Certificates

Users of legitimate telephone services should be able to receive the benefit of SHAKEN authentication with full attestation. To that end, the base SHAKEN specification describes three conditions that must exist in order for a SHAKEN authentication service to fully attest that an originating customer can legitimately use the calling TN:

1. The signing provider must be responsible for the origination of the call onto the IP based service provider voice network.
2. The signing provider must have a direct authenticated relationship with the customer and can identify the customer.
3. The signing provider must have established a verified association with the calling telephone number

Conditions 1 and 2 are relatively unambiguous; the originating provider is the signing provider, and the originating provider typically authenticates the calling user by some industry-accepted authentication mechanism such as SIP Digest.

The 3rd condition can be more complex. Obviously, condition 3 is easily satisfied for the case where the originating provider has authority over the calling TN, has assigned the calling TN to the originating customer, and has directly authenticated the customer before the call. However, there are a number of legitimate real-world call scenarios where this is not the case; i.e., where the originating SP does not have direct knowledge of the set of TNs the calling user is authorized to use, but it may still be legitimate for the customer to receive full attestation. Example scenarios include the following (note, list is not exhaustive):

* A SIP-PBX obtains originating call service from multiple providers (e.g., for redundancy or least cost routing). In this case, the PBX can legitimately originate a call via one provider from a calling TN that it obtained from a different provider.
* An enterprise wants to display a toll-free callback number for B2C calls, and the 800-number provider (RespOrg) and the originating provider are two separate entities.
* A “legitimate spoofing” service displays the subscriber’s work TN for calls originated by the user’s home phone.
* An outbound dialing service that automatically initiates calls on behalf of a business or other entity, and displays the business TN to the called users (e.g., school announces weather-related school closings to students, or airline sends flight information updates to its passengers).
* Wholesaled TNs used by reseller SPs, Cloud Communication Providers, and others when they originate calls
* A contact center serving multiple enterprises from various locations originates calls using the unique calling TN specified by each enterprise.

The SHAKEN specification provides guidance to originating SPs on how they can satisfy the TN-legitimacy condition in order to provide full attestation for call scenarios where the originating provider is not the TN provider. For example, the originating SP could establish the legitimacy of the calling TN as part of the service level agreement with the customer, or it could obtain the necessary TN assignment information from the TN provider using some “out-of-band” mechanism. However, these mechanisms often have shortcomings. The service level agreement approach may be unworkable in practice due to a low level of trust between originating provider and customer. Or the originating provider may have no relationship with or knowledge of the TN provider. And finally, the ad-hoc and non-automated nature of these mechanisms incurs a large administrative overhead for the participating parties (e.g., the overhead required to establish relationships between otherwise unrelated providers), and could make full attestation non-viable in the majority of enterprise scenarios.

The delegate cross-certification mechanism defined in this specification addresses these shortcomings by providing an automated, protocol-based mechanism that enables an originating customer to provide cryptographic proof that the customer is authorized to use the calling TN. And finally, delegate cross-certificates allows us to extend the SHAKEN framework effective mechanism for authorities to traceback bad actors to the authorized service provider that provided their delegated certificate.

Editor’s Note: for the scenarios where there is not a pre-existing relationship between the carrier that provides the TN and the originating carrier, local policy in the originating carrier’s network may dictate partial vs. full attestation. Further discussion and contributions to follow.

# 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-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*

ATIS-1000080, *SHAKEN: Governance Model and Certificate Management,*

IETF RFC 3261, *SIP: Session Initiation Protocol.*1

IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace.*1

RFC 4949, *Internet Security Glossary, Version 2.*1

RFC 5806, *Diversion Indication in SIP*. 1

RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*. 1

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*1

RFC 8225, *Personal Assertion Token.*[[1]](#footnote-1)

RFC 8226, *Secure Telephone Identity Credentials: Certificates.*1

draft-ietf-stir-passport-shaken, *PASSporT SHAKEN Extension.* 1

draft-ietf-stir-passport-divert, *PASSporT Extension for Diverted Calls.* 1

draft-ietf-acme-authority-token, *ACME Challenges Using an Authority Token.* 1

draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token.* 1

TS 24.229, IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP). [[2]](#footnote-2)

# 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 provides some key definitions used in this document.

**Caller ID:** The originating or calling party’s telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields in the Session Initiation Protocol (SIP) [RFC 3261] messages.

**(Digital) Certificate:** Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object [RFC 4949]. See also STI Certificate.

**Certification Authority (CA):** An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [RFC 4949].

**Certificate Chain:** See Certification Path.

**Certification Path:** A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain [RFC 4949].

**Certificate Revocation List (CRL):** A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [RFC 4949].

**Certificate Signing Request (CSR):** A CSR is sent to a CA to request a certificate. A CSR contains a Public Key of the end-entity that is requesting the certificate.

**Chain of Trust:** Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain [RFC 4949].

**Certificate Validation:** An act or process by which a certificate user established that the assertions made by a certificate can be trusted [RFC 4949].

**Company Code:** A unique four-character alphanumeric code (NXXX) assigned to all Service Providers [ATIS-0300251].

**Cross-certificate:** A CA certificate where the issuer and subject are different entities; i.e., a CA certificate that has been issued from one CA to another CA, where the receiving CA uses the private key of the certificate for issuing new certificates [RFC 5280].

**Cross-certification:** The process whereby a CA delegates authority to another CA by issuing a cross-certificate to the delegate CA [RFC 5280].

**End-Entity:** An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of this document, an end-entity is a Service Provider, TN Provider, or Customer AF.

**Fingerprint:** A hash result ("key fingerprint") used to authenticate a public key or other data [RFC 4949].

**Identity:** Either a canonical Address-of-Record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as ’sip:alice@atlanta.example.com’), or a telephone number, which commonly appears in either a TEL URI [RFC 3966] or as the user portion of a SIP URI. See also Caller ID [RFC 8224].

**National/Regional Regulatory Authority (NRRA):** A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

**Online Certificate Status Protocol (OCSP):** An Internet protocol used by a client to obtain the revocation status of a certificate from a server.

**Private Key:** In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption [RFC 4949].

**Public Key:** The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography [RFC 4949].

**Public Key Infrastructure (PKI):** The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [RFC 4949].

**Root CA:** A CA that is directly trusted by an end-entity. See also Trust Anchor CA and Trusted CA [RFC 4949].

**Secure Telephone Identity (STI) Certificate:** A public key certificate used by a service provider to sign and verify the PASSporT.

**Service Provider Code:** In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider. In the US and Canada this would be a Company Code as defined in [ATIS-0300251].

**Signature:** Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [RFC 4949].

**Telephone Identity:** An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

**Trust Anchor:** An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The trust anchor is a combination of a trusted public key and the name of the entity to which the corresponding private key belongs [RFC 4949].

**Trust Anchor CA:** A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key. See also Root CA and Trusted CA [RFC 4949].

**Trusted CA:** A CA upon which a certificate user relies for issuing valid certificates; especially a CA that is used as a trust anchor CA [RFC 4949].

**Trust Model:** Describes how trust is distributed from Trust Anchors.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
| B2BUA | Back-to-Back User Agent |
| CRL | Certificate Revocation List |
| CSCF | Call Session Control Function |
| CVT | Call Validation Treatment |
| HTTPS | Hypertext Transfer Protocol Secure |
| IBCF | Interconnection Border Control Function |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| NNI | Network-to-Network Interface |
| OCSP | Online Certificate Status Protocol |
| PASSporT | Persona Assertion Token |
| PBX | Private Branch Exchange |
| PKI | Public Key Infrastructure |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SPID | Service Provider Identifier |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-VS | Secure Telephone Identity Verification Service |
| STIR | Secure Telephone Identity Revisited |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| TN-PoP | TN Proof-of-Possession |
| TrGW | Transition Gateway |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique Identifier |
| VoIP | Voice over Internet Protocol |

# Overview

This document describes a mechanism that enables the end-to-end delivery of SHAKEN authentication with full attestation when TN ownership and originating call processing are split between two different SHAKEN providers.

This document 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 to attest for signing. 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 that have an OCN (Operating Carrier Number) and are 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, Contact Center, Cloud Communication Provider, a legitimate spoofing application, or an automated outbound dialing service.

The basic mechanism specified in this document works as follows:

* The STI-CA delegates authority to the TN provider for issuing STI certificates
* Based on the authority granted to it by the STI-CA, the TN Provider issues STI certificates to its Customer AFs. The scope of each STI certificate covers the TNs that the TN Provider has delegated to the Customer AF
* When initiating a call into the public telephone network from a calling TN obtained from the TN Provider, the Customer AF uses the credentials of the STI certificate to perform SHAKEN authentication services.
* The resulting SHAKEN Identity header is delivered to the terminating network and verified per normal SHAKEN procedures.

## Functional Requirements

This section describes the overall requirements that apply to this solution.

1. When a TN provider delegates a subset of its TNs to a Customer AF, it may optionally provide an STI certificate for the delegated TNs to the Customer AF. An STI certificate is required if the customer wants to receive the benefit of SHAKEN authentication with full attestation for calls originated from the delegated TNs when the TN provider is not the originating provider.
2. A TN provider shall ensure that the scope of the STI certificate provided to a Customer AF covers only the TNs that it has delegated to the Customer AF.
3. When originating a call from a delegated TN that is in-scope for one of its STI certificates, the Customer AF shall use the certificate to perform SHAKEN authentication (i.e., build an Identity header containing a "shaken" PASSporT that claims the legitimacy of the calling TN, and that is signed with the certificate’s private key).
4. An originating SP shall convey the SHAKEN Identity header added to an originating INVITE request by the Customer AF in the outgoing INVITE request sent toward the terminating network.

## Certificate Authority Delegation via Cross Certification

Figure 1 shows the high-level overview of the certificate management process used to provide STI certificates to the Customer AF using cross-certification. The STI-CA does not issue STI certificates to the Customer AF directly, but instead, delegates authority for issuing these certificates to a Delegate CA hosted by the TN Provider. The STI-CA delegates its authority by issuing a cross-certificate to the Delegate CA. The STI-CA populates the cross-certificate with a "constraints" extension that limits the scope of the STI end-entity certificates that can be issued by the Private CA. In this case, the constraints identify the TNs (or a subset of the TNs) that the TN Provider has authority over. Once it has obtained a cross-certificate from an STI-CA, the TN Provider’s Delegate CA can issue STI end-entity certificates to its Customer AFs within the constraints specified by the cross-certificate. These end-entity certificates are chained via the cross-certificate to the trusted STI-CA’s root certificate. In addition to validating that the certificate path chains to a trusted STI-CA root, verifiers will validate that the scope of an STI end-entity certificate does not exceed the scope of any constraints specified by the cross-certificate in the certificate path.

The method of conveying the constraints in a cross-certificate is FFS. Possible options include:

* Use the X.509 name constraints extension defined in RFC 5280
* Define a new TNAuthList constrains extension
* Use the TNAuthList itself



Figure 1. STI-CA delegates authority to a TN Provider Delegate CA

## Authorizing Cross-Certificate constraints per TN Provider

As shown in Figure 2, the STI-PA is responsible for authorizing the constraints that apply to cross-certificates per TN Provider.

1. The TN Provider requests an SPC Token from the STI-PA for a TNAuthList and set of constraints. If the TN Provider is authorized, the STI-PA returns an SPC token authorizing the requested TNAuthList and constraints.
2. The TN Provider performs the ACME certificate ordering process to obtain a cross-certificate from the STI-CA. The TN Provider uses the SPC Token from step-1 to demonstrate that it has authority for the cross-certificate constraints. The Delegate CA stores the cross-certificate for later use in issuing end-entity certificates.
3. A Customer AF orders an STI end-entity certificate from the Delegate CA.
4. The Delegate CA issues a new end-entity certificate signed by the private key of the cross-certificate, and stores the new certificate in the STI-CR.
5. The Customer AF downloads the new certificate URL. The Customer AF will populate the ‘x5u’ parameter of SHAKEN PASSporT tokens with this URL during SHAKEN authentication.



Figure 2. The STI-PA authorizes cross-certificate constraints

# A Annex Title

Xxx

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-1)
2. Available from 3rd Generation Partnership Project (3GPP) at: < [https://www.3gpp.org](http://www.3gpp.org) > [↑](#footnote-ref-2)