**ATIS-0x0000x**

ATIS Standard on

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

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The base-SHAKEN framework defined a authority model that allows SHAKEN-authorized VoIP Service Provider to sign a PASSporT with an included set of claims. While “shaken” PASSporTs represent attestation the interconnected VoIP provider determines specific to the calling identity, there are additional call scenarios and new parties that represent different authority over calling or caller information being sent in the call. This specification extends the base-SHAKEN framework to represent different authoritative entities that may participate in the SHAKEN framework and eco-system and defines these authoritative models and how they can be used going forward as new frameworks and new policies embrace SHAKEN for furthering the ability to extend trust throughout the telephone number related products and services.

**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** |
| --- | --- | --- | --- |
|  | Initial | Baseline |  |

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

2 Normative References 2

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 4

4 Overview 6

5 Indirect use-cases and authority over call and caller data 6

5.1 Authority beyond 6

**Table of Figures**

Figure 1. Delegate Certificate Management Flow 7

**Table of Tables**

No table of figures entries found.

# Scope, Purpose, & Application

## Scope

This specification extends the SHAKEN.

## Purpose

The purpose of the SHAKEN

# 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-2)

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

draft-ietf-stir-cert-delegation, STIR Certificate Delegation*.* 1

TS 24.229, IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP). [[2]](#footnote-3)

# 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].

**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 Service Provider, or VoIP Entity.

**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].

**Responsible Organization (Resp Org):** Entity designated as the agent for the Toll-Free subscriber to obtain, manage and administer Toll-Free Numbers and provide routing reference information in the SMS/800 Toll-Free Number Registry.

**Resp Org Identification (Resp Org ID):** A 5-character code that designates or points to the Responsible Organization (Resp Org) associated with a specific Toll-Free number [ATIS-0417001-003].

**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], or a Resp Org ID assigned to a Resp Org as defined in [ATIS-0417001-003].

Editor’s note: Further analysis is required to determine if Resp Org should be included as part of the service provider code or somewhere else.

**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.

**VoIP Entity:** A non-STI-authorized customer entity that purchases (or otherwise obtains) delegated telephone numbers from a TNSP

## 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 |
| OSP | Originating Service Provider |
| 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 |
| SP | Service Provider |
| 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 |
| TNSP | TN Service Provider |
| TSP | Terminating Service Provider |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique Identifier |
| VoIP | Voice over Internet Protocol  |

# Overview

STIR and SHAKEN are frameworks that are fundamentally about signing information about a call, a calling identity, or the caller itself. The signer has a certificate that represents that signer’s authority in the SHAKEN eco-system and its ability to authoritatively represent the information being signed. For base SHAKEN, as defined in ATIS-1000074 and ATIS-1000080, the authority is represented by the originating service provider (OSP) and their ability to attest to the valid use of the telephone number by the End-User that initiated the call. This is generally based on their ability to both authenticate the End-User and validate the authorized use of the originating telephone number signaled in the call. Beyond the basic telephone number authority and authority over the routing of telephone calls, there is other functions and services that are part of the telephone network eco-system and related to End-Users and Customers of service providers there is other information associated with the caller that need some level of authoritative representation.

This document discusses these cases and defines a model for how and why the end-to-end authoritative model of STIR certificates is important to recognize and contextualize for who is authoritative for the information being signed in a PASSporT, whether related to the telephone number and the authorize provider associated with that telephone number, the End-User that has been given the right to use that telephone number, information about the End-User as a person or business entity, or a third-party that takes responsibility to be authoritative over the vetting or validation of any of the aforementioned information. It is furthermore important to recognize that these different set of authorized parties may need to be represented with different certificates in the context of the digital signatures protecting a PASSporT holding claim information being protected in the call. As an example, the authoritative entity that performs the vetting and TN Validation processes will likely be different and the interconnected OSP may need to derive the attestation determination using other standard mechanisms.

In addition, ATIS-1000088 and ATIS-1000089 discuss indirect routing use-cases which present further challenges to the authoritative relationship between the End-User that initiated the call and the OSP that is required to sign the SHAKEN PASSporT and attest to the telephone calling identity. ATIS-1000093 defines delegate certificates which can help to provide an additional mechanism to extend the authority model by the use of delegation of authority or the ability to protect the integrity or scope of information with a given set of delegated credentials used to sign a PASSporT.

There are a number of cases in the telephone network where the authority model is either different or complimentary but not the same or is often better managed by entities that may not be interconnected providers or OCN holders directly. This document will provide a model which is complimentary to the base SHAKEN authoritative model discussed in ATIS-1000074, ATIS-1000080, and ATIS-1000084, but extends it to support current and future extensions to the SHAKEN framework and eco-system when necessary or that can provide extended functionality to consumers of the telephone network set of services or telephone number related identity associations or services. Rich Call Data is an example of a service that can and should have a clear distinction of whom is authoritative over the telephone number used in the call and either the caller related meta-data or more importantly the determination and representation of the legal status of that information (e.g. copyright or trademark, or usage policy). As will be discussed in the document, this example shows it is key that the authoritative representative and relationships to known authorities are clear both on the originating side of the call to make the SHAKEN attestation determination, as well as at the terminating side of the call, so the terminating verification service or the end-user themselves have the potential to determine information needed to make a decision about how and by whom the signed information was validated. There is other authoritative models like toll-free or VRS services where there is separate and distinct authoritative entities and databases that serve as the basis for setting the responsible entity that is authorized to sign or delegate authority for signing PASSporTs.

# Authority models

Base SHAKEN (74, 80, 84) defines the core authority model where the eco-system has a policy that OCN holders are authoritative in the SHAKEN framework to attest their knowledge about the telephone calling identity. This document defines a more general model consisting of three authoritative relationships with the subject of the PASSporT claims being signed and the relationship of the authority to the signer of that information. The ability for an authorized party in a particular application domain can use a unique identity

## Direct Authority models

The direct authority model represents cases where the authorized entity is directly authoritative over the subject of the information being signed and can be directly represented by a unique domain specific identifier that can be used as an SPC code as defined in ATIS-1000080.



Figure 1. Direct Authority Model Diagram

## Vetting/Validation Authority models

The vetting/validation authority model represents cases where the authorized entity is indirect from the holder of the SPC, but is willing to take the responsibility to sign the subject of the claim(s) of the PASSporT on behalf of their customer directly.



Figure 2. Vetting/Validation Authority Model Diagram

## Delegated Authority models

The delegated authority model represents cases where the authorized entity is indirect from the holder of the SPC and has vetted/validated the entity and information related to the subject of the claim(s) of the PASSporT and can delegate the credentials to that party to sign the call themselves.



Figure 3. Delegate Authority Model Diagram

# Details of use of SPC and delegation to represent authority

Detailed text TBD

# Examples of authority models

Example details TBD

Vetting/Validation

The NANC CATA WG second report refers to the concepts of vetting and TN validation as key parts of both determining the entity associated with a telephone number is an established entity in good standing as well as validating their authorized use of a telephone number respectively. With rich call data, data that may have other requirements for the vetting and validation of this information, these concepts should be further adopted to determine the authoritative use of that information. For example, if a calling name is a value, it may be desirable to determine the legitimate and authorized use of copyrighted or trademarked business names or images.

VRS or Toll-free or emergency services

In the case of Video Relay Services representing the identity of their users and telephone numbers, or with RespOrgs and Toll-free use-cases, or with emergency services, the authoritative databases may be controlled by authorities outside of the traditional telephone authoritative databases or entities, and therefore require separate entities and mechanisms than for what has been allocated to date. This document details and extends the framework that is highly complementary with base SHAKEN and extends it to necessary authoritative parties as well as alternatively utilizes delegate certificates as a basis for indirect entities and the chaining of the authoritative trust. This can allow relying parties to do the verification consistently and simplistically, with the backing of the traceback and other feedback mechanisms we have in any certificate based eco-system to identify and remove those that do not conform to the policies of the SHAKEN eco-system.

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