**ATIS-0x0000x**

ATIS Standard on

**Considerations for Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The Signature-based Handling of Asserted information using toKENs (SHAKEN) standard specifies operation within the domain of a single national or regional regulatory authority - in most cases this means within a single country. This was a conscious decision by the joint Alliance for Telecommunications Industry Solutions (ATIS) and SIP Forum IP-NNI Task Force (IP-NNI TF) in order to more quickly develop a solution that explicitly addressed U.S. requirements. However, SHAKEN does not assume unique U.S. attributes, and therefore should be equally applicable to other countries. Calls that originate in one country and terminate in another country, are not explicitly addressed in the existing SHAKEN standard. This document provides a mechanism to extend the SHAKEN trust environment to include more than one country.

**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** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[ATIS-0x0000x i](#_Toc11424211)

[ATIS Standard on i](#_Toc11424212)

[Considerations for Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN) i](#_Toc11424213)

[Alliance for Telecommunications Industry Solutions i](#_Toc11424214)

[Abstract i](#_Toc11424215)

[1 Scope, Purpose, & Application 1](#_Toc11424216)

[1.1 Scope 1](#_Toc11424217)

[1.2 Purpose 1](#_Toc11424218)

[1.3 Application 1](#_Toc11424219)

[2 Normative References 1](#_Toc11424220)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc11424221)

[3.1 Definitions 2](#_Toc11424222)

[3.2 Acronyms & Abbreviations 2](#_Toc11424223)

[4 Overview 3](#_Toc11424224)

[4.1 Cross-Border Architecture 4](#_Toc11424225)

[4.2 Scope of Trusted STI-CA 6](#_Toc11424226)

[4.3 Merging Trusted STI-CA Lists 6](#_Toc11424227)

[4.3.1 Server 7](#_Toc11424229)

 [Interface to Server 8](#_Toc11424230)

[4.3.2 8](#_Toc11424231)

[4.3.3 Procedures to Update Server 8](#_Toc11424232)

[A Annex Title 9](#_Toc11424233)

**Table of Figures**

[Figure 1: SHAKEN Trust Model 4](#_Toc9258371)

[Figure 2: List of Trusted CAs 4](#_Toc9258372)

[Figure 3: Independent lists of Trusted CAs 4](#_Toc9258373)

[Figure 4: Independent Deployments of SHAKEN 5](#_Toc9258374)

[Figure 5: Merged Trusted CA Lists 5](#_Toc9258375)

[Figure 6: Merged Trusted CA Lists (Network Context) 5](#_Toc9258376)

[Figure 7: Merging Trusted CA Lists 6](#_Toc9258377)

# Scope, Purpose, & Application

## Scope

This document provides telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks) in scenarios where a call originates in one country and terminates in a different country. The primary focus of this document is to specify how the trust environment created by Signature-based Handling of Asserted information using toKENs (SHAKEN) in a single country can be extended to include other countries. This document does not require any changes to the existing SHAKEN specifications but does identify new interfaces and functions to exchange information between countries.

## Purpose

The purpose of this document is to extend the SHAKEN trust environment to encompass more than one country. This will specify how calls authenticated in one country can be successfully verified in a second country.

## Application

The mechanism specified in this standard will allow countries with similar interests and regulatory environments to federate their SHAKEN infrastructure and extend the trust environment to include both countries. This specification only considers the case of two countries, but it could be extended through additional “pairwise agreements” where the countries have similar interests and regulatory environments. However, this mechanism may not be appropriate for the more general case where SHAKEN is extended globally. This more general problem is for further study.

# 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.

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

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

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

IETF RFC 8588 , *PASSporT SHAKEN Extension*.1

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

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

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1

IETF RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP).*1

ATIS-1000080, *SHAKEN: Governance Model and Certificate Management**[[2]](#footnote-2)*

ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators2*

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

ATIS-0x0000x, *Technical Report*.

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

Editor’s note: at a minimum add ATIS-1000074, ATIS-1000080, and ATIS-1000084.

# 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

**Caller ID**: The originating or calling party telephone number used to identify the caller carried either in the P-Asserted Identity or From header.

## 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 |
| JWT | JSON Web Token |
| NNI | Network-to-Network Interface |
| PASSporT | Personal 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 |
| SPC | Service Provider Code |
| 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-GA | Secure Telephone Identity Governance Authority |
| STI-PA | Secure Telephone Identity Policy Administrator |
| STIR | Secure Telephone Identity Revisited |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| TrGW | Transition Gateway |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique Identifier |
| VoIP | Voice over Internet Protocol  |
|  |  |

# Overview

SHAKEN specifications state that the Secure Telephone Identity- Policy Administrator (STI-PA) approves Secure Telephone Identity-Certificate Authorities (STI-CAs) using criteria established by the Policy Management Authority and then distributes the list of “Trusted STI-CAs” to all service providers in the SHAKEN ecosystem. The SHAKEN governance model only considers a single country, but nothing in the existing technical specification precludes two Secure Telephone Identity-Governance Authorities (STI-GAs) agreeing they will recognize each other’s STI-CAs and instructing their respective STI-PAs to merge their “Trusted STI-CA” lists. The merged trusted STI-CA list could then be distributed to all service providers in both of the participating countries, using existing interfaces and procedures. Calls authenticated in one country would then be successfully verified in the other country. This document specifies the architecture and interfaces for two countries to merge trusted STI-CA lists.

Initial deployment of cross-border SHAKEN using this model is likely to be based on direct bilateral agreement between two STI-GAs. This could be extended through additional bilateral agreements, but as deployment increases, other mechanisms could also be introduced. For example, several countries could appoint an entity to act on their behalf, with a single agreement covering all the countries. Alternatively, an industry association could act as a central clearing house, allowing new participants to sign a single agreement with the association to gain access to all other members of the association. All these arrangements (i.e., bilateral agreements, regional organization, and industry association) could coexist using the mechanism defined in this standard, depending on the circumstances of the participating countries.

## Cross-Border Architecture

At a high level, the SHAKEN trust model is illustrated below:



Figure 1: SHAKEN Trust Model

The List of Trusted STI-CAs shown in this diagram is specified in ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators* as:



Figure 2: List of Trusted STI-CAs

The list of trusted STI-CAs in the above figure is assumed to be for a single country. Therefore, if two countries implement SHAKEN independently, they will end up with separate “Trusted STI-CA” lists, as shown below.



Figure 3: Independent lists of Trusted STI-CAs

In the context of separate networks, this would lead to the following scenario with distinct network deployments and distinct lists of trusted STI-CAs as shown below.



Figure 4: Independent Deployments of SHAKEN

In scenario shown above, cross-border calls would not be successfully verified because they would not have the same Trusted STI-CA lists.

On the other hand, if the two STI-GAs agreed to trust each other, and instructed their respective STI-PAs to merge their Trusted STI-CA lists, this would result in the following lists of trusted STI-CAs:



Figure 5: Merged Trusted STI-CA Lists

In the network context, this would lead to the following.



Figure 6: Merged Trusted STI-CA Lists (Network Context)

In this case, calls authenticated in one network would be successfully verified in the other network because they have the same trusted STI-CA lists. The interfaces and procedures for distributing the merged list of trusted STI-CAs are identical to the procedures for distributing the original list of trusted STI-CAs, as specified in ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*. No changes to the existing SHAKEN specifications would be required. However, an additional interface and function will be required to facilitate sharing of trusted STI-CA lists. The additional functionality is discussed in the next section.

## Scope of Trusted STI-CA

The original SHAKEN specification describes the use of an STI-PA within a single country, governed by a single STI-GA. Therefore all STI-CAs have the same scope – i.e., they can issue certificates to any Service Provider within that single country. In the case of multiple STI-PAs, a mechanism is required to uniquely identity the STI-PA that has approved the STI-CA to issue certificates for a specific country. While E.164 Country Codes (CC) are assigned for telephone numbers, they are not necessarily unique to a country (e.g., the US and Canada have the same E.164 country code). In order to uniquely identity the STI-PA that has approved a specific STI-CA in the SHAKEN ecosystem, the ISO 3166-1 alpha 2 country code can be included in the root certificate. During certificate path validation, the STI-VS checks that the root certificate in the chain is on the list of Trusted STI-CAs.

This document specifies the format for storing the above information on the server and for retrieving this information. It does not specify what the STI-PA will do with this information once it has been retrieved.

## Merging Trusted STI-CA Lists



Figure 7: Trusted STI-CA Server

Each STI-PA will be responsible for providing a server with the required information on their Trusted STI-CAs. When an STI-GA agrees to merge Trusted CA lists with another country, it will instruct the STI-PA to provide credentials to allow the STI-PA in the other country to read information in the server. This will allow the other STI-PA to obtain the required information on Trusted CAs. This document does not specify what the STI-PA will do with the information on Trusted CAs.



Figure 8: Trusted STI-CA Servers

Each STI-PA is responsible for providing a server listing their Trusted CAs, as shown in the above diagram.

### Server

The format of the list of trusted STI-CAs is the same as specified in ATIS-1000084, with the additional requirement that the Subject and Issuer Name in the root certification shall contain the ISO 3166-1 alpha 2 country code associated with the STI-PA which approved the specific STI-CA as part of the SHAKEN ecosystem.

Each STI-PA shall provide a server with details of all STI-CAs on their Trusted CA list. The Trusted CA list shall contain the key for the trust list as well as the algorithm used for the signature. The trust list is distributed in the form of a standard JWT with the following fields in the protected header:

* alg: Algorithm used in the signature of the STI-CA list.
* typ: Set to the standard “jwt” value.
* x5u: Contains the URL of the STI-PA root certificate associated with the signature of the JWT.

 The payload contains the following fields:

* version (required, int): Version number for this list format. The version number shall be changed if the format/contents of the STI-CA list is modified or extended.
* exp: The timestamp after which the service provider considers this list of STI-CAs no longer valid. This field shall be a number containing a NumericDate value. If the list has expired, the Service Provider shall request an updated list.
* sequence (required, int): The sequence number is incremented by one each time a new list is provided by the STI-PA. A 64 bit integer is recommended.
* trustList (required, array of strings): The trustList is represented as a JSON array of root certificate strings. Each string in the array is a base64-encoded (Section 4 of RFC 4648) DER X.509 root certificate for an approved STI-CA.  Each root certificate must include the country code in the Subject and Issuer Name to uniquely identify the country associated with the STI-PA that approved the addition of the root certificate to the list of Trusted STi-CAs
* extensions (optional, string).

### Interface to Server

This document recommends the use of an API over HTTPS [RFC 7231] for the distribution of the list of trusted STICAs. Clause 4.3.1 provides details on the format and contents of the STI-CA list in the form of a JSON Web Token (JWT) [RFC 7519].

### Procedures to Update Server

Each STI-PA will maintain a separate server for information on their Trusted CA list, and ensure the list is up to date at all times. When the STI-GA instructs the STI-PA to share Trusted CA information with another STI-PA, the first STI-PA will give read-only credentials to the second STI-PA, allowing them to access the Trusted CA list. The information on the server will identify the trusted STI-CAs. The second STI-PA will follow the same process to allow access to its Trusted CA list.

**Annex A**

(normative/informative)

# A Annex Title

Xxx

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-1)
2. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < [www.atis.org](http://www.atis.org) >. [↑](#footnote-ref-2)
3. Available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org > [↑](#footnote-ref-3)