**ATIS-1000087**

ATIS Technical Report on

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

**Alliance for Telecommunications Industry Solutions**

Approved December 16, 2019

**Abstract**

The Signature-based Handling of Asserted information using toKENs (SHAKEN) standard “ATIS-1000074” 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 without requiring service providers to make changes to their current standard SHAKEN interfaces.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

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 an 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, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS** **Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum** **Technical Working Group (TWG)** was responsible for the development of this document.

**Table of Contents**

[1 Scope, Purpose, & Application 1](#_Toc24103655)

[1.1 Scope 1](#_Toc24103656)

[1.2 Purpose 1](#_Toc24103657)

[1.3 Application 1](#_Toc24103658)

[2 References 1](#_Toc24103659)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc24103660)

[3.1 Definitions 2](#_Toc24103661)

[3.2 Acronyms & Abbreviations 2](#_Toc24103662)

[4 Overview 3](#_Toc24103663)

[4.1 Cross-Border Architecture 3](#_Toc24103664)

[4.2 Scope of Trusted STI-CA 5](#_Toc24103665)

[4.3 Combined Trusted STI-CA Lists 6](#_Toc24103666)

[4.3.1 Server 7](#_Toc24103667)

[4.3.2 Interface to Server 8](#_Toc24103668)

[4.3.3 Procedures to Update Server 8](#_Toc24103669)

[4.4 Compatible Implementations 8](#_Toc24103670)

**Table of Figures**

[Figure 4‑1: SHAKEN Trust Model 3](#_Toc24103646)

[Figure 4‑2: List of Trusted STI-CAs 4](#_Toc24103647)

[Figure 4‑3: Independent lists of Trusted STI-CAs 4](#_Toc24103648)

[Figure 4‑4: Independent Deployments of SHAKEN 4](#_Toc24103649)

[Figure 4‑5: Merged Trusted STI-CA Lists at each STI-PA 5](#_Toc24103650)

[Figure 4‑6: Merged Trusted STI-CA Lists at each STI-PA (Network Context) 5](#_Toc24103651)

[Figure 4‑7: Mutual Exchange 6](#_Toc24103652)

[Figure 4‑8: Trusted STI-CA Server 7](#_Toc24103653)

[Figure 4‑9: Trusted STI-CA Servers 7](#_Toc24103654)

# Scope, Purpose, & Application

## Scope

This document provides telephone service providers with a framework and guidance on how to use 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 detail 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 document will detail how calls authenticated in one country can be successfully verified in a second country.

## Application

The mechanism specified in this technical report 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 a bilateral arrangement between two jurisdictions, although it may be possible to extend this to include a limited number of additional countries. The more general solution for global interworking requires further study.

# References

The following standards contain provisions which, through reference in this text, constitute provisions of this technical report. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this technical report are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

IETF RFC 4648, *The Base16, Base32, and Base64 Date Encodings*[[1]](#footnote-2)

IETF RFC 7519, *JSON Web Token (JWT)* 1

IETF RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*1

ISO 3166-1: *Codes for the Representation of Names of Countries and Their Subdivisions*[[2]](#footnote-3)

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

ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN) [[3]](#footnote-4)*

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

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

CATA-WG Report, *Adoption of Caller ID Authentication Technology and Other Techniques to Combat Robocalls by Policymakers and Providers in Countries outside the United States* [[link](https://www.fcc.gov/sites/default/files/adoption-of-caller-id-authentication-for-combatting-robocalls-outside-us.pdf)]

ISO 3166-1, *Codes for the Representation of Names of Countries and Their Subdivisions.[[4]](#footnote-5)*

# 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.

**Global Trust List**: A list of the STI-PA root certificate and the URLs to the Trusted STI-CA list and CRL hosted by the local STI-PA and each trusted cross-border STI-PA.

**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 [Ref 9].

**Trust List**: A set of one or more trust anchors used by a relying party to explicitly trust one or more PKIs [Ref 10].

## Acronyms & Abbreviations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ATIS | | Alliance for Telecommunications Industry Solutions | | |
| CC | | Country Code | | |
| CP | | Certificate Policy | | |
| CRL | | Certificate Revocation List | | |
| HTTPS | | Hypertext Transfer Protocol Secure | | |
| IETF | | Internet Engineering Task Force | | |
| IP | | Internet Protocol | | |
| JSON | | JavaScript Object Notation | | |
| JWT | | JSON Web Token | | |
| NNI | | Network-to-Network Interface | | |
| PASSporT | | Personal Assertion Token | | |
| PBX | | Private Branch Exchange | | |
| SHAKEN | | Signature-based Handling of Asserted information using toKENs | | |
| SIP | | Session Initiation Protocol | | |
| 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-PA | | Secure Telephone Identity Policy Administrator | | |
| STIR | | Secure Telephone Identity Revisited | | |
| URL | | Uniform Resource Locator | | |
| 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 stakeholders, 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 the respective authorities in two countries from 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 participating countries, using existing interfaces and procedures. Calls authenticated in one country would then successfully verify in the other country. This document specifies the architecture and interfaces for two countries to exchange their 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-PAs, at the direction of their respective authorities. 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 4‑1: SHAKEN Trust Model

The STI-PA maintains two resources that are used by verification services during the PASSporT verification procedure:

* A Trusted STI-CA List containing the root certificate of each approved STI-CA in the local jurisdiction. This list is defined in ATIS-1000084.
* An indirect Certificate Revocation List (CRL) that lists all revoked certificates issued by STI-CAs in the local jurisdiction. The CRL is defined in ATIS-1000080.

The Trusted STI-CA List and CRL hosted by the STI-PA are shown in figure 4-2 below.

Diagram

Description automatically generated

Figure 4‑2: List of Trusted STI-CAs Maintained by STI-PA

The list of trusted STI-CAs in the above figure is explicitly a list of the root certificates of STI-CAs that were approved and controlled by this STI Policy Administrator, and as such, the scope of the CAs is limited to the scope of the GA/PA (e.g., a single country). Likewise, the CRL lists only revoked certificates that were issued by STI-CAs approved by the GA/PA in the local jurisdiction. Therefore, if two countries implement SHAKEN independently, they will have separate Trusted STI-CA Lists and separate CRLs, as shown below. In the example in figure 4-3 the originating service provider will generate a PASSporT using an STI certificate issued by an STI-CA in the “Trusted STI-CA List” for "country x”, but when the terminating service provider verifies the PASSporT, it will use the “Trusted STI-CA List” for “country y” and verification will fail for the cross-border call.



Figure 4‑3: Independent lists of Trusted STI-CAs and CRLs

Figure 4-2 from ATIS-1000084 shows the service provider directly accessing the Trusted STI-CA List hosted by the STI-PA using an HTTPS URL. Figure 4-3 in this document illustrates why this approach does not automatically work for cross-border SHAKEN, since the TSP verification service does not have access to the Trusted STI-CA list and CRL in the remote originating jurisdiction.

To support cross-border SHAKEN, the STI-PA hosts a new table called the “Global Trust List”. This table provides a single location within each jurisdiction that verification services local to that jurisdiction can use to obtain the URL references for the Trusted STI-CA List and CRL of all the cross-border jurisdictions. To simplify verification service implementations, the table also contains the URL references to the local Trusted STI-CA List and CRL. The Global Trust List table is shown in figure 4-4 below.



Figure 4‑4: Global Trust List

The “Global Trust List” includes the URL references to the Trusted STI-CA list and CRL from “Country X” and “Country Y”, allowing cross-border SHAKEN to be successfully verified, as shown in figure 4-5.

In this case, calls authenticated in one jurisdiction could be successfully verified in another jurisdiction because the “Global Trust List” provides URL references that the TSP verification service can use to download the Trusted STI-CA List and CRL hosted by the cross-border STI-PA in the originating jurisdiction.



Figure 4‑5: Cross-Border SHAKEN

The format of the Trusted STI-CA List and the CLR hosted by the STI-PA remains as specified in ATIS-1000084 and ATIS-1000080 respectively. No changes to the existing SHAKEN specifications are required. However, to enable support for cross-border SHAKEN, verification services will need to be updated to download the “Global Trust List” hosted by the local STI-PA, and then download the Trusted STI-CA List and CRL of each jurisdiction listed in the Global Trust List. The additional functionality is discussed in the clause 4.2 and 4.3.

The previous diagrams all show Trusted CA Lists for STI-PAs associated with an individual country (e.g., one STI-CA list for “country x” and another for “country y”), but the CATA WG report *Adoption of Caller ID Authentication Technology and Other Techniques to Combat Robocalls by Policymakers and Providers in Countries outside the United States* [ref:xxx] also recognizes the possibility of an STI-GA/PA that is not limited to a single country (i.e., a non-jurisdictional STI-GA/PA). The mechanism described in this document can support a combination of Trusted CA Lists from several individual countries (i.e., “jurisdictional STI-PAs) as well as non-jurisdictional STI-PA(s), as shown below.



Figure 4‑6: Support for Non-Jurisdictional STI-GA/PA

## Global Trust List Structure

The Global Trust List shall be encoded as a JSON Web Token (JWT) [Ref xx], with the following Protected Header fields:

* "alg": Identifies the algorithm used to generate the JWT signature. Algorithm "ES256" shall be used.
* "typ": Identifies the object type. Value "jwt" shall be used.
* "x5u": Identifies the URL of the STI-PA certificate whose credentials were used to generate the signature of the Global Trust List JWT. The URL shall have a protocol of “https”. The URL shall either not contain a port or contain a port of “443”. The URL shall not contain a userinfo subcomponent, query component, or fragment identifier component as described in [RFC 3986]. The URL path shall end with “.pem”.

The Global Trust List JWT payload shall contain the following claims:

* "version" (string): Version number of this list format. Global Trust Lists compliant with this specification shall have a version number of “1.0”. Subsequent specifications that change or extend the Global Trust List JWT shall update the version number accordingly.

The next three claims contain a timestamp encoded in NumericDate format as defined in [RFC7519]:

* "exp": Timestamp after which this JWT is no longer valid.
* "iat": Timestamp at which this JWT was generated.
* "nbf": Timestamp before which this JWT shall not be accepted for processing.
* "sequence" (int): Sequence number is incremented by one each time a new list is provided by the STI-PA. A 64-bit integer is recommended.
* "trustList": A JSON array. The first array entry contains information associated with the local jurisdiction. Each subsequent array entry contains information associated with a trusted cross-border jurisdiction. Each array entry contains the following key/value pairs:
  + "country": an array of strings where each string is an ISO 3166-1 alpha-2 country code [ISO 3166-1, Codes for the Representation of Names of Countries and Their Subdivisions]. When the STI-PA associated with a "trustList" array entry serves multiple countries, the "country" array contain multiple entries identifying those countries.
  + "stiPaRootCert": a pem-encoded root certificate of the STI-PA associated with this "trustList" array entry.
  + "caList": a URL reference to the Trusted STI-CA List of the STI-PA associated with this "trustList" array entry.
  + "crl": a URL reference to the CRL of the STI-PA associated with this "trustList" array entry. This URL shall match the URL identified by the CRL Distribution Point extension of certificates issued by STI-CAs in the jurisdiction associated with this "trustList" array entry.

An example HTTP request/response to obtain the Global Trust List from the STI-PA in the local jurisdiction is as follows:

GET /globalTrustList HTTP/1.1

Host: https://example-us.sti-pa.com

Accept: application/jose+json

HTTP/1.1 200 OK

Content-Type: application/jose+json

{"protected": base64url({

"alg": "ES256",

"typ": "JWT",

"x5u": " https://sti-pa.com/global-trust-list/cert.pem"})

"payload": base64url({

"version": 1.0,

"sequence": 1,

"exp": 1300819380,

"iat": 1300819380,

"nbf": 1300819380,

"trustList": [

{

"country": ["us"],

"stiPaRoot": "PEM\_UNITED\_STATES\_STI-PA\_ROOT\_CERTIFICATE\_HERE",

"caList": "https://example-us-sti-pa.com/caList.txt",

"crl": "https://example-us-sti-pa.com/crl.pem"

},

{

"country": ["ca"]

"stiPaRoot": "PEM\_CANADA\_STI-PA\_ROOT\_CERTIFICATE\_HERE",

"caList": "https://example-ca-sti-pa.com/caList.txt",

"crl": "https://example-ca-sti-pa.com/crl.pem"

},

{

"country": ["IT", "VA"]

"stiPaRoot": "PEM\_ITALY\_STI-PA\_ROOT\_CERTIFICATE\_HERE",

"caList": "https://example-it-sti-pa.com/caList.txt",

"crl": "https://example-it-sti-pa.com/crl.pem"

}

]

## Global Trust List Procedures

### STI-PA Procedures

The STI-PA shall host the Global Trust List defined in clause 4.2. The list shall be distributed using HTTPS. The STI-PA shall make the URL reference to the list available to verification services by posting the URL on the STI-PA web site. Access to the list shall not require an account with the STI-PA; i.e., the list shall be publicly accessible. The list shall be signed with the credentials of an STI-PA end-entity certificate that chains to the root certificate of the STI-PA. The "exp" claim shall be populated with a timestamp value that is 24 hours later that the timestamp value of the "iat" claim. The STI-PA shall populate the first array entry of the "trustList" claim with information related to the STI-PA itself. The STI-PA shall populate an additional "trustList" array entry for each trusted cross-border STI-PA.

The STI-PA shall respond to HTTPS requests to the Global Trust List "trustList" claim "caList" URL as specified in ATIS-1000084, where only root certificates for in-jurisdiction STI-CAs are included in the 200 OK response. Likewise, the STI-PA shall respond to HTTPS requests to the "trustList" claim "crl" URL as specified in ATIS-1000080, where only revoked certificates issued by in-jurisdiction STI-CAs are included in the response.

An STI-PA shall not include its root certificate in the certification path that is provided to verification services dereferencing the "caList" or "crl" URL identified in the STI-PA’s entry in the Global Trust List. Instead, verification services shall use the root certificate contained in the "stiPaRoot" key value during certificate path validation of the STI-PA certificate whose credentials were used to sign the Trusted STI-CA List or CRL.

The STI-PA shall make the following resources publicly accessible (i.e., the STI-PA shall not require authentication or apply access controls to entities requesting information from these resources):

1. The Global Trust List URL (response is a JWT)
2. The Global Trust List certificate URL (the URL including in the x5u claim of the Global Trust List JWT)
3. The CRL URL (response is a PEM CRL)
4. The CRL certificate URL (the URL included in the Authority Information Access extension of the CRL)
5. The Trusted STI-CA List URL (response is a JWT)
6. The Trusted STI-CA List certificate URL (the URL including in the "x5u" claim of the Trusted STI-CA List JWT)

STI-PA root certificates shall support the following X.509 certificate profile:

* Shall include a Basic Constraints extension with CA attribute set to true
* Shall include a Key Usage extension set to Certificate Sign and CRL Sign only
* Shall include a Certificate Policy extension identifying the OID of the Certificate Policy supported by the STI-PA CA
* Shall not include a CRL Distribution Point extension

STI-PA intermediate certificates shall support the following X.509 certificate profile:

* Shall include a Basic Constraints extension with CA attribute set to true
* Shall include a Key Usage extension set to Certificate Sign and CRL Sign only
* Shall include a Certificate Policy extension identifying the OID of the Certificate Policy supported by the STI-PA CA
* Shall include a CRL Distribution Point extension referencing the direct CRL hosted by the STI-PA for revoked certificates issued by the STI-PA CA

STI-PA end-entity certificates shall support the following X.509 certificate profile:

* Shall include a Basic Constraints extension with CA attribute set to false
* Shall include a Key Usage extension set to Digital Signature and CRL Sign only
* Shall include a Certificate Policy extension identifying the OID of the Certificate Policy supported by the STI-PA CA
* Shall include a CRL Distribution Point extension referencing the direct CRL hosted by the STI-PA for revoked certificates issued by the STI-PA CA

### Verification Service (STI-VS) Procedures

Verification services shall download a new version of the Global Trust List from the local (in-jurisdiction) STI-PA at some short interval before the current list expires as indicated by the "exp" claim (an interval of one hour is recommended). A verification service shall not use the root certificate identified in the "stiPaRoot" key value of the local STI-PA when validating the certification path of the STI-PA certificate referenced by the Global Trust List "x5u" parameter. Instead, the verification service shall obtain the STI-PA root certificate by some trusted out-of-band mechanism (e.g., download the root certificate posted on the local STI-PA’s web site).

If a newly downloaded Global Trust List is valid, and the current time is between the times indicated by the "nbf" claim and the "exp" claim, then the verification service shall download the Trusted STI-CA List referenced by the "caList" key value of each array entry in the "trustList" claim. The verification service shall verify the newly downloaded Trusted STI-CA List of each array entry as specified in ATIS-1000084, with the exception that during certificate path validation it shall use the root certificate contained in the "stiPaRoot" key of the same "trustList" array entry. If the Trusted STI-CA List is valid, then the verification service shall add the root certificates to its local root certificate store.

When a newly downloaded Global Trust List indicates that a previously downloaded "trustList" array entry has been removed, the verification service shall ensure that the trusted root certificates associated with that previous array entry are removed from its local root certificate store.

The verification service shall also download the CRL referenced by the "crl" key value of each "trustList" array entry and validate the CRL as specified in ATIS-1000074, with the exception that during certificate path validation it shall use the root certificate contained in the "stiPaRoot" key of the same "trustList" array entry. If the CRL is valid, then the verification service shall include any revoked certificates listed on the CRL when checking for revoked certificates during PASSporT verification.

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-2)
2. Available from the International Organization for Standardization (ISO) at: < <https://www.iso.org/> >. [↑](#footnote-ref-3)
3. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < [www.atis.org](http://www.atis.org) >. [↑](#footnote-ref-4)
4. 3 This document is available from the International Organization for Standardization (ISO) at: < https://www.iso.org/ >. [↑](#footnote-ref-5)