**ATIS-1000087.v002**

ATIS Technical Report on

**Mechanism for 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.

**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 (SP) 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](#_Toc129092182)

[1.1 Scope 1](#_Toc129092183)

[1.2 Purpose 1](#_Toc129092184)

[1.3 Application 1](#_Toc129092185)

[2 References 1](#_Toc129092186)

[3 Definitions, Acronyms, & Abbreviations 2](#_Toc129092187)

[3.1 Definitions 2](#_Toc129092188)

[3.2 Acronyms & Abbreviations 2](#_Toc129092189)

[4 Overview 3](#_Toc129092190)

[4.1 Cross-Border Architecture 4](#_Toc129092191)

[4.1.1 The Global Trust List 5](#_Toc129092192)

[4.1.2 The Global Trust List support of a Non-Jurisdictional STI-GA/PA 7](#_Toc129092193)

[4.2 Cross-Border Procedures 9](#_Toc129092194)

[4.2.1 Establishing a Cross-Border SHAKEN Agreement 9](#_Toc129092195)

[4.2.2 Coordinating Cross-Border Information Exchange with STI-PA Certificate Lifecycle 10](#_Toc129092196)

[4.2.3 Terminating a Cross-Border SHAKEN Agreement 12](#_Toc129092197)

[5 Global Trust List Data Structure 13](#_Toc129092198)

[6 Global Trust List Procedures 14](#_Toc129092199)

[6.1 STI-PA Procedures 14](#_Toc129092200)

[6.1.1 Generating the Global Trust List 14](#_Toc129092201)

[6.1.2 Downloading the Global Trust List and its Referenced Resources 15](#_Toc129092202)

[6.1.3 STI-PA Certificate Rollover 15](#_Toc129092203)

[6.1.4 STI-PA Resources that require Public Access 15](#_Toc129092204)

[6.1.5 STI-PA Certificate Profile 16](#_Toc129092205)

[6.2 STI-CA Procedures 16](#_Toc129092206)

[6.3 Authentication and Verification Service (STI-AS/VS) Procedures 16](#_Toc129092207)

**Table of Figures**

[Figure 4‑1: SHAKEN Trust Model 4](#_Toc129092208)

[Figure 4‑2: List of Trusted STI-CAs Maintained by STI-PA 5](#_Toc129092209)

[Figure 4‑3: Independent lists of Trusted STI-CAs and CRLs 5](#_Toc129092210)

[Figure 4‑4: Global Trust List 6](#_Toc129092211)

[Figure 4‑5: Cross-Border SHAKEN 7](#_Toc129092212)

[Figure 4‑6: Support for Non-Jurisdictional STI-GA/PA 8](#_Toc129092213)

[Figure 4‑7: Obtaining Cross-Border Trusted STI-CA List and CRL 9](#_Toc129092214)

[Figure 4‑8: Updating Cross-Border Information when STI-PA Root Certificate Renewed 11](#_Toc129092215)

[Figure 4‑9: Terminating a Cross-Border SHAKEN Agreement 12](#_Toc129092216)

# 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.

# 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)

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

RFC 5217, *Memorandum for Multi-Domain Public Key Infrastructure Interoperability.*1

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

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)

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.3*

ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators.3*

ATIS-1000092, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Delegate Certificates.3*

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.

**Subordinate CA**: A CA whose public-key certificate is issued by another (superior) CA [RFC 4949]. In the context of SHAKEN, a Subordinate CA is an STI-SCA or V-SCA as defined in [ATIS-1000092].**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]. In the context of SHAKEN, a Trusted CA is an STI-CA and its Subordinate CAs approved to operate in the SHAKEN PKI [ATIS-1000084].

**Trust List**: A set of one or more trust anchors used by a relying party to explicitly trust one or more PKIs [RFC 5217]. The Trust List is the Trusted STI-CA List which contains the root certificates of all approved STI-CAs within a jurisdiction [ATIS-1000084].

## 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 |
| SP | Service Provider |
| 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 share each other’s Certificate Revocation Lists (CRL). Calls authenticated in one country would then successfully verify in the other country. This document captures requirements for cross-border SHAKEN standards, and then specifies the architecture and interfaces for two countries to exchange their trusted STI-CA lists and CRLs.

## Cross-Border Requirements

The cross-border architectures and interfaces in this document are based on the following requirements:

1. A terminating service provider’s STI-VS needs access to the certificate used to sign the originating call from the other country,
2. A terminating service provider’s STI-VS needs access to the approved list of STI-CAs in the other country, as maintained by their policy administrator,
3. A terminating service provider’s STI-VS needs access to the indirect Certificate Revocation List (CRL) in the other country, as maintained by their policy administrator, and
4. A terminating service provider’s STI-VS needs access to the root certificate used by a country’s policy administrator to sign both the approved list of STI-CAs and indirect CRL (this allows the STI-VS to validate authenticity).
5. Solutions must minimize the Post Dial Delay (PDD) caused by retrieving resources (e.g., CA lists, CRLs, etc.).
6. Solutions must minimize the amount of time it takes for a TSP to become aware that a certificate has been revoked.
7. Solutions must minimize the amount of time it takes for a TSP to become aware that a new root certificate has been added to a CA list.
8. Solutions must minimize the amount of time it takes for a TSP to become aware that a root certificate has been removed from a CA list.
9. Solutions must not leverage external (e.g., TLS) PKI in the chain of trust.
10. Information exchanged between STI-PAs to enable cross-border SHAKEN must be exchanged in a secure manner to ensure the information was received from a trusted source and was integrity protected in transit.
11. Solutions must allow the STI-PA to unambiguously identify the STI-CAs it has directly approved, and distinguish them from the STI-CAs that were approved by a different STI-PA. When an STI-PA recognizes another STI-PA to create a “Global Trust List” it must be able to identify which STI-CAs were approved by each STI-PA.

## Cross-Border Architecture

At a high level, the SHAKEN trust model is illustrated in Figure 4‑1. The STI Governance Authority (STI-GA) establishes the policies within the SHAKEN PKI of a jurisdiction, and the STI Policy Administrator enforces those policies



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.

 

Figure 4‑2: Trusted STI-CA List and CRL Maintained by STI-PA

The Trusted STI-CA List 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 in Figure 4‑3. In the example in Figure 4‑3 the originating service provider (OSP) generates a PASSporT signed with the credentials of an STI certificate issued by an STI-CA in the Trusted STI-CA List for "country x”, but when the terminating service provider (TSP) verifies the PASSporT, it uses the Trusted STI-CA List for “country y” and verification fails for the cross-border call.

 

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

Figure 4-2, which is taken 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. For verification to pass, the TSP in “country y” needs access to three country x resources; the Trusted STI-CA List, the CRL, and the STI-PA root certificate that anchors the certification path of the STI-PA certificate whose credentials were used to digitally sign the Trusted STI-CA List and CRL of “country x”.

### The Global Trust List

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 where verification services local to that jurisdiction can obtain the following information associated with each trusted cross-border jurisdiction:

* The STI-PA root certificate of the STI-PA,
* The URL reference to the Trusted STI-CA List, and
* The URL reference to the CRL

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 ‑: Global Trust List

As shown in Figure 4‑5, with the Global Trust List, calls authenticated in one jurisdiction can 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 ‑: 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.

### The Global Trust List support of a Non-Jurisdictional STI-GA/PA

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 or groups of countries (i.e., “jurisdictional STI-PAs) as well as non-jurisdictional STI-PA(s), as shown in Figure 4‑6 below.

 

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

## Cross-Border Procedures

### Establishing a Cross-Border SHAKEN Agreement

Figure 4‑7 shows the procedure for establishing a cross-border SHAKEN agreement between two countries: Country-x and Country-y. For simplicity, the diagram shows the information flow only from Country-x to Country-y. Since these are bi-lateral agreements, the information flow from Country-y to Country-x would be symmetrical.



Figure ‑: Obtaining Cross-Border Trusted STI-CA List and CRL

The procedure is as follows:

1. The SPs in the jurisdiction of Country-y obtain the STI-PA-y root certificate(s) needed for path validation of the end-entity certificate(s) used to sign the in-jurisdiction Trusted STI-CA List, CRL, and Global Trust List hosted by STI-PA-y.
2. When the cross-border SHAKEN agreement is established between Country-x and Country-y, STI-PA-x provides the URL references to its Trusted STI-CA List and CRL to STI-PA-y, along with the root certificate needed for path validation of the end-entity certificate(s) used to sign these two lists.
3. STI-PA-y adds an entry for Country-x to its Global Trust List, based on the information received in step-2, and signs the list with the credentials of an end-entity certificate whose certification path chains to one of the root certificates conveyed to SP-y in step-1.
4. SP-y in Country-y downloads a new version of STI-PA-y's Global Trust List at some short interval before the current version of the list expires (this document recommends a Global Trust List lifetime of 24 hours).
5. SP-y verifies the Global Trust List, including validation that the certification path of the signing certificate chains to a trusted STI-PA root certificate obtained in step-1.
6. If the Global Trust List is valid, then SP-y uses the URL references for Country-x to download the Trusted STI-CA List and CRL from STI-PA-x.
7. SP-y verifies the two lists are valid, including validation that the certification path of the signing certificate of each list chains to the root certificate identified for Country-x in the Global Trust List. If both lists are valid, then SP-y incorporates the information contained on the lists into its PASSporT verification procedures, as follows:
	* SP-y adds the root certificates from the STI-PA-x Trusted STI-CA List to its local trusted root store,
	* SP-y PASSporT verification service uses the STI-PA-x CRL during its certificate revocation checking procedure. Specifically, if a certificate on the certification path referenced by the PASSporT’s "x5u" URL contains a CRL Distribution Point extension that references the STI-PA-x CRL, then the verification service checks the certificate’s revocation status against that CRL.

The Global Trust List, Trusted STI-CA List and CRL are digitally signed with the credentials of an STI-PA end-entity certificate that chains to a trusted STI-PA root certificate. This enables Service Providers to verify that a downloaded list came from a trusted source and was integrity protected en route. Before an SP can verify one of these signed lists, it needs to be in possession of the root certificate anchor of the local or cross-border STI-PA certificate whose credentials were used to sign the list. This exchange of STI-PA root certificates between two STI-PAs, or the distribution of an STI-PA root certificate to its in-jurisdiction Service Providers cannot be similarly protected since the STI-PA root certificate serves as the trust anchor within each jurisdiction (i.e., there is no “higher authority” to serve as a trust anchor for secure exchange of the STI-PA root certificate in these cases). Therefore, the exchange of STI-PA root certificates between cross-border STI-PAs, and the distribution of an STI-PA root certificate to its in-jurisdiction SPs must be done via a secure manual process (e.g., steps 1 and 2 in Figure 4‑7).

### Coordinating Cross-Border Information Exchange with STI-PA Certificate Lifecycle

As part of normal certificate lifecycle procedures, a new STI-PA root certificate must be issued at some interval before the current STI-PA root certificate expires. STI certificates (used to sign PASSporTs) contain a CRL Distribution Point extension that references the in-jurisdiction CRL hosted by the STI-PA. Therefore, as the expiration date of the STI-PA root certificate approaches, the STI-PA must perform the following procedure:

1. Issue a new STI-PA root certificate,
2. Create a new CRL that is signed with the credentials of an STI-PA end-entity certificate with a certification path that is anchored at the newly issued root certificate,
3. Distribute the new CRL URL to in-jurisdiction Service Providers (in the SPC Token response) so that the CRL Distribution Point extension of newly issued STI certificates references the new CRL URL.
4. Distribute the new root certificate and CRL URL to cross-border STI-PAs so cross-border verification services can validate STI certificates that reference the new CRL. (The STI-PA also creates a new Trusted STI-CA List signed with credentials that chain to the new root certificate, and provides a URL to this list to its trusted cross-border STI-PAs.)

At the completion of this process, there would still be many valid in-jurisdiction STI certificates referencing the old CRL. Therefore, the STI-PA must select the timing at which the above procedure is executed to ensure that the old root certificate does not expire before any in-jurisdiction STI certificate referencing the old CRL expires. The SHAKEN Certificate Policy administered by the STI-PA stipulates a maximum lifetime of 3 years for STI certificates issued by the STI-CA. STI-CA. This would require the STI-PA to perform the above procedure 3 years (plus a grace period) before the current STI-PA root certificate’s expiry date.

Note: As stated in clause 6.2, all end-entity and intermediate certificates in the certification path of an issued STI certificate must contain the same URL value in their CRL Distribution Point extension. This means that that once all issued STI certificates referencing the old CRL expire (maximum 3 years), verifiers will no longer encounter STI certificates referencing the old CRL.

Figure 4‑8 describes the above procedure in more detail. The initial conditions of this diagram are the final conditions of Figure 4‑7, where SP-y has local verified copies of the Global Trust List from STI-PA-y and the Trusted STI-CA List and CRL from STI-PA-x.



Figure ‑: Updating Cross-Border Information when STI-PA Root Certificate Renewed

The procedure is as follows:

1. A new root certificate is issued for STI-PA-1. STI-PA-1 creates a new Trusted STI-CA List and a new CRL that have the same contents as the old lists but are signed with an STI-PA certificate that chains to the new root certificate. The STI-PA assigns new URLs to the stores holding the new lists and their signing certificates.
2. STI-PA-1 provides two sets of cross-border information to STI-PA-y, one set for the old root certificate and one for the new root certificate. STI-PA-y updates its Global Trust Table with the new information.
3. After it has passed its new SHAKEN information to all cross-border STI-PAs, STI-PA-x continues to return the old CRL URL in the SPC Token response to local SPs for a period of 24 hours. Once 24 hours have elapsed, STI-PA-x begins distributing the new CRL URL to local STI-CAs and SPs, so that going forward all newly issued STI certificates will reference the new CRL. This 24-hour delay ensures that all local and cross-border verification services are in possession of the new STI-PA-x root certificate before it is needed to support validation of STI certificates referencing the new CRL.

4), 5), 6) and 7) SP-y downloads and verifies a new copy of the Global Trust List, and based on the new information contained on the list, downloads and verifies two sets of the Trusted STI-CA List and CRL from STI-PA-x.

8) and 9) At this point, SP-y could receive a signed INVITE from SP-x in Country-x. During PASSporT verification, SP-y must select either the old or new CRL previously downloaded from STI-PA-x, based on the contents of the CRL Distribution point extension of the STI certificates in the certification path referenced by the PASSporT’s "x5u" parameter.

1. Once all in-jurisdiction STI certificates referencing the old CRL have expired, STI-PA-x deletes the old root certificate and lists and provides STI-PA-y with a single set of cross-border information associated with the new root certificate.

The above procedure applies to the “graceful” root certificate renewal case where a new STI-PA root certificate is issued because the current root certificate is approaching end-of life. For cases where a new STI-PA root certificate is issued because the current root certificate has been compromised (e.g., private key was leaked), the STI-PA will create a new Trusted STI-CA List and CRL signed with an end-entity certificate chained to the new root certificate, as described above. However, there will be no grace period where both the old and new root certificates and CRLs co-exist. Instead, the STI-PA will immediately update its cross-border SHAKEN information to remove all data associated with the compromised root certificate. The STI-PA will also inform all in-jurisdiction STI-CAs and Service Providers to replace their existing STI certificates with new STI certificates that reference the new CRL.

### Terminating a Cross-Border SHAKEN Agreement

Figure 4‑9 shows the procedure for terminating a cross-border SHAKEN agreement.



Figure ‑: Terminating a Cross-Border SHAKEN Agreement

The procedure is as follows:

1. If Country-y decides to terminate its cross-border SHAKEN agreement with Country-x, then STI-PA-y removes all entries associated with Country-x from its Global Trust List.
2. and 3) On its next 24-hour polling interval, SP-y downloads and verifies the Global Trust List.
3. SP-y refreshes its Local STI-CA Root Certificate Store based on the CA List URLs contained in the newly downloaded Global Trust List. Since there are no entries associated with Country-x on the Global Trust List, all STI-CA root certificates associated with Country-x are removed from SP-y’s Local STI-CA Root Certificate Store.

# Global Trust List Data 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.
	+ "caListUrl": a URL reference to the Trusted STI-CA List of the STI-PA associated with this "trustList" array entry.
	+ "crlUrl": 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",

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

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

 },

 {

 "country": ["CA"]

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

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

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

 },

 {

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

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

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

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

 }

 ]

})

"signature": /\* signed using STI-PA end-entity certificate private key \*/

}

# Global Trust List Procedures

This section describes the normative requirements that must be supported by an STI-PA, STI-AS and STI-VS to enable cross-border STIR/SHAKEN.

## STI-PA Procedures

### Generating the Global Trust List

The STI-PA shall host the Global Trust List defined in clause 4.2. The "iat" claim shall be populated with a timestamp value for the current time. The "exp" claim shall be populated with a timestamp value that is 24 hours later that the timestamp value of the "iat" claim. The "nbf" claim shall be populated with a timestamp value that indicates the time before which the information in this Global Trust List should not be used.

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 additional "trustList" array entries with information received from its trusted cross-border STI-PAs. The STI-PA shall obtain this information from each trusted cross-border STI-PA using a secure manual process.

The list shall be signed with the credentials of an STI-PA end-entity certificate whose certification path is anchored at the root certificate of the STI-PA.

### Downloading the Global Trust List and its Referenced Resources

The Global Trust List shall be distributed using HTTPS. The STI-PA shall make the URL reference to the list available to in-jurisdiction 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.

An in-jurisdiction or cross-border STI-PA shall respond to HTTPS requests to the Global Trust List "trustList" claim "caListUrl" URL as specified in ATIS-1000084, where only root certificates for SHAKEN-approved STI-CAs local to that STI-PA are included in the Trusted STI-CA List returned in the response. Likewise, the STI-PA shall respond to HTTPS requests to the "trustList" claim "crlUrl" URL as specified in ATIS-1000080, where only revoked certificates issued by STI-CAs local to the responding STI-PA are included in the CRL returned in the response.

An STI-PA shall not include its root certificate in the certification path that is provided to local or cross-border verification services dereferencing the Trusted STI-CA List "x5u" URL or the CRL Authority Information Access URL. An STI-PA shall not include its root certificate in the certification path that is provided to local verification services dereferencing the Global Trust List "x5u" URL.

### STI-PA Certificate Rollover

When a new STI-PA root certificate is issued because the current root certificate is approaching its expiration date, the STI-PA shall construct a new CRL signed with the credentials of an end-entity certificate whose certification path is anchored at the new root certificate. The STI-PA shall perform a similar procedure for the Trusted STI-CA List; i.e., construct a new CA trust list signed with the credentials of an end-entity certificate that chains to the new STI-PA root certificate. The STI-PA shall store the newly created CRL and Trusted STI-CA List in publicly accessible repositories. The STI-PA shall ensure that the URL references to these two new lists and their signing certificates are different than the set of URL references to the lists and signing certificates associated with the old root certificate.

Once the new Trusted STI-CA List and CRL are uploaded to their local repositories, the STI-PA shall include two entries in the "trustList" claim of the Global Trust List sent to in-jurisdiction verification services, one containing the old STI-PA root certificate and CRL and CA trust lists, and one containing the new root certificate and lists[[5]](#footnote-6). Likewise, the STI-PA will convey two sets of STI-PA root certificates, and two sets of lists to its trusted cross-border STI-PAs. The STI-PA shall continue to provide the old root certificate and lists (along with the new root certificate and lists) to in-jurisdiction verification services and cross-border STI-PAs until all in-jurisdiction STI certificates referencing the old CRL expire, at which point the STI-PA shall stop distributing the old root certificate and lists.

As specified in ATIS-1000080, the STI-PA distributes a CRL URL to in-jurisdiction STI-CAs and SP authentication services (for example, the URL is passed to SP authentication services in the SPC Token response from the STI-PA). STI-CAs and SPs use this URL to populate the CRL Distribution Point extension of STI end-entity and intermediate certificates. When a new CRL is created during STI-PA root certificate renewal, the STI-PA shall continue to distribute the URL for the old CRL to in-jurisdiction STI-CAs and SP authentication services for a duration of 24 hours after the STI-PA has completed providing its root certificate and list information to all trusted cross-border STI-PAs. Once this 24-hour interval has ended, the STI-PA shall start distributing the new CRL URL to in-jurisdiction STI-CAs and SP authentication services. Inserting a 24-hour delay before the new CRL URL is referenced in STI certificates will ensure that local and cross-border verification services are in possession of the new STI-PA root certificate which is required for certificate path validation of the certificate referenced by the Authority Information Access extension of the new CRL.

### STI-PA Resources that require Public Access

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 included 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 Certificate Profile

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 not 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 used to sign CRLs 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 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 used to sign JWTs 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 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

The Certificate Policy extension of STI-PA intermediate and end-entity certificates shall not identify the OID of the Certificate Policy of the STI-CA.

## STI-CA Procedures

When issuing STI certificates to a Service Provider, the STI-CA shall ensure that the CRL Distribution Point extension of the issued certificate contains the current CRL URL value the STI-CA received from the STI-PA. The STI-CA shall also ensure that all STI intermediate certificates in the certification path of the issued certificate contain that same CRL URL value.

## Authentication and Verification Service (STI-AS/VS) Procedures

SP 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 secure manual out-of-band mechanism.

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 "caListUrl" 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 of the "x5u" certificate it shall use the root certificate contained in the "stiPaRoot" key of the same "trustList" array entry. The verification service shall ignore any root certificate returned when dereferencing the "x5u" claim. 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 all 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 "crlUrl" 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.

SP verification services shall not dereference URLs in the Global Trust List that meet any of the following conditions:

* URLs that use a scheme other than “https” or a port other than 443,
* URLs that contain a userinfo subcomponent, query component, or fragment identifier component as described in RFC 3986 [Ref 7],
* URLs with a host component that resolves to a special-purpose IP address described in RFC 6890, Special-Purpose IP Address Registries, or
* URLs that appear to be part of a Server-Side Request Forgery (SSRF) attack.

The verification service shall not follow HTTP redirections (i.e., the Location header of a 3xx HTTP response). The verification service may make an HTTP HEAD request to check the Content-Type or other headers before making an HTTP GET request to dereference a URL.

SP authentication services shall not use the CRL URL identified in the Global Trust List to populate the CRL Distribution Point extension of an STI certificate. Instead, as specified in ATIS-1000080, the CRL URL returned by the STI-PA in an SPC Token response shall be used for this purpose. This enables the STI-PA to control when newly issued STI certificate start referencing the new CRL during the STI-PA root certificate renewal process.

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)
5. Both CRLs will contain the same set of revoked certificates, and both Trusted STI-CA Lists will contain the same set of STI-CA root certificates. [↑](#footnote-ref-6)