ATIS-1000087

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

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-1000087, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)*

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

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

Table of Figures

ATIS Technical Report on –

Considerations for Cross-Border SHAKEN

1 Scope, Purpose, & Application

1.1 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.

1.2 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.

1.3 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.

2 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]

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]

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]

[1] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

[2] Available from the International Organization for Standardization (ISO) at: < https://www.iso.org/ >.

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < www.atis.org >.

ATIS-1000080, *SHAKEN: Governance Model and Certificate Management*[Error! Bookmark not defined.]

ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*[Error! Bookmark not defined.]

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 >.

3.1 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.

3.2 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

4 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.

4.1 Cross-Border Architecture

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

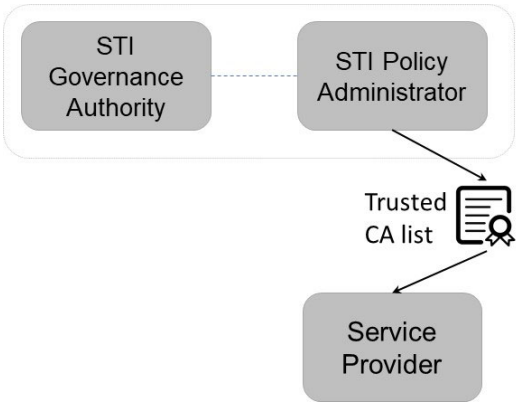

Figure 4-1: SHAKEN Trust Model

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:

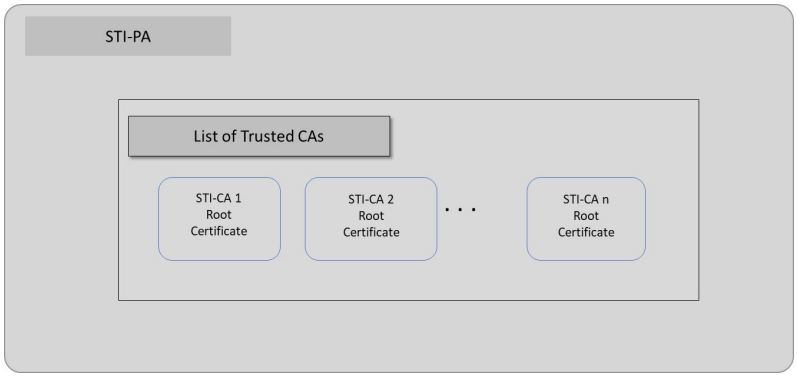

Figure 4-2: List of Trusted STI-CAs

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.

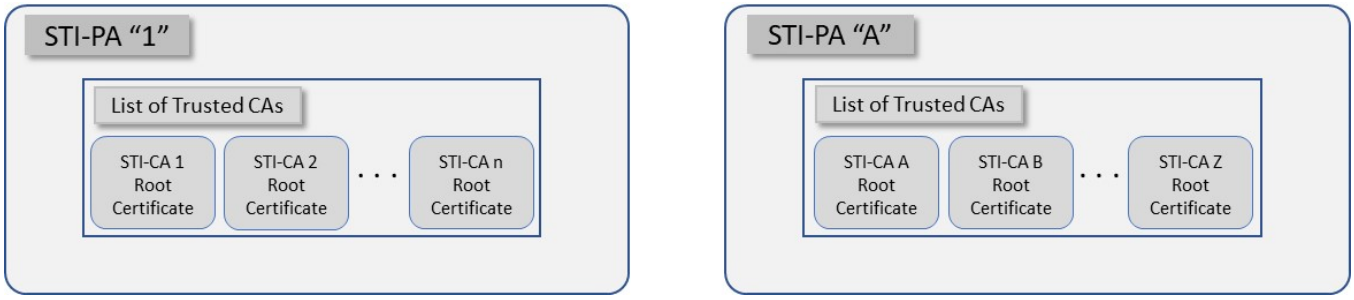

Figure 4-3: Independent lists of Trusted STI-CAs

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.

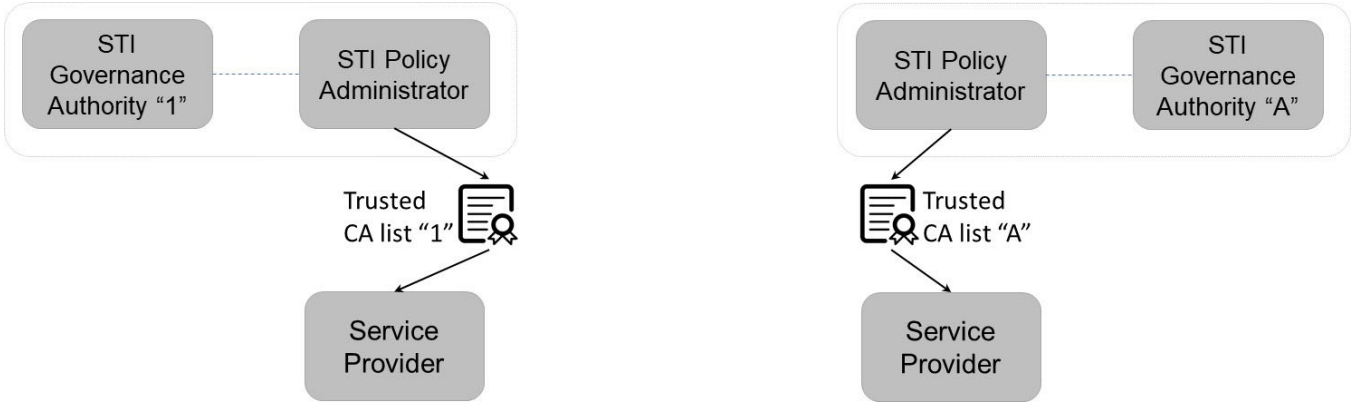

Figure 4-4: Independent Deployments of SHAKEN

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

On the other hand, if the two STI-PAs are directed to trust each other and to exchange their Trusted STI-CA lists, this would result in the following lists of trusted STI-CAs:

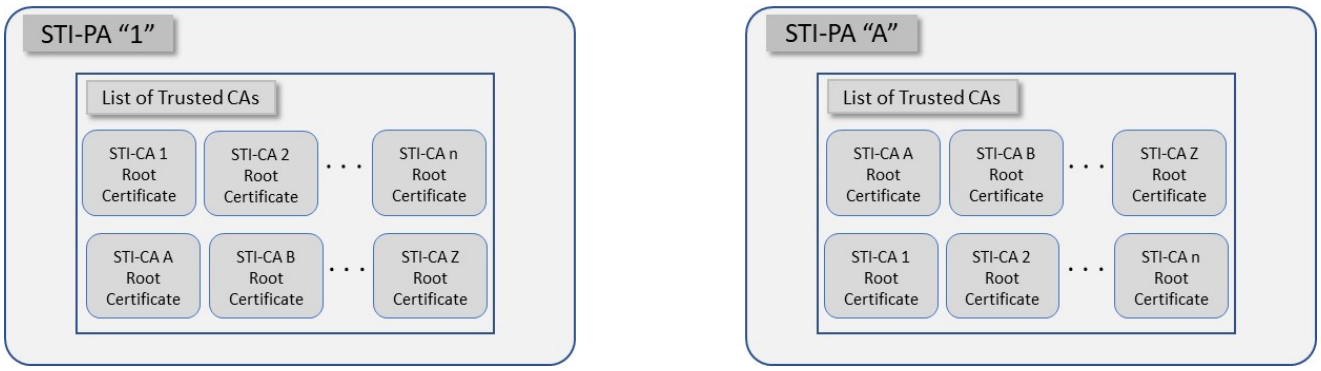

Figure 4-5: Merged Trusted STI-CA Lists at each STI-PA

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

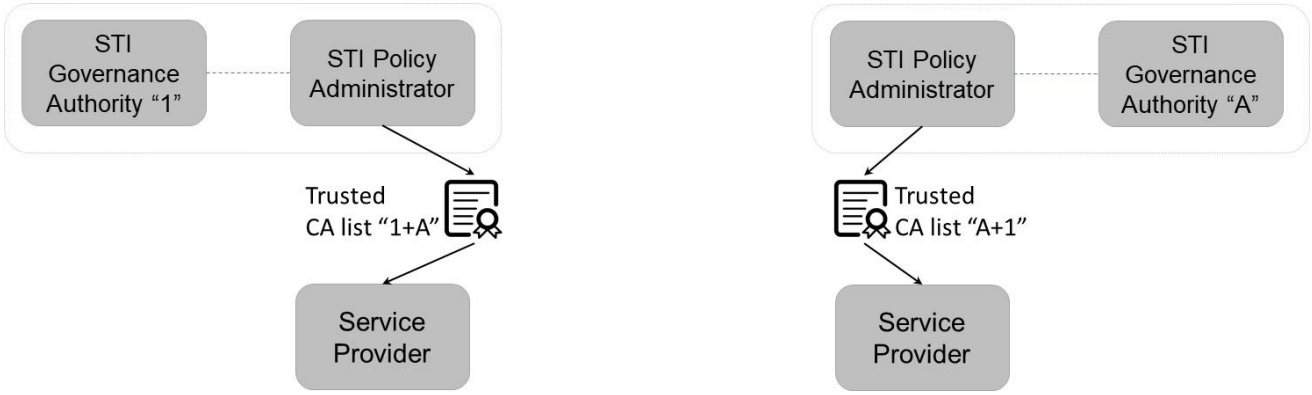

Figure 4-6: Merged Trusted STI-CA Lists at each STI-PA (Network Context)

In this case, calls authenticated in one network could successfully verify in the other network because they have the same trusted STI-CA lists. The interfaces and procedures for distributing the combined 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.

4.2 Scope of Trusted STI-CA

The original SHAKEN specification describes the use of an STI-PA within a single country, governed by a single authority. 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 may be required to uniquely identify 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 identify 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 additional naming requirement would need to be included in the Certificate Policy (CP).

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.

4.3 Combined Trusted STI-CA Lists

With the implementation of SHAKEN in another country there exist alternatives for combining the Trusted STI-CA lists:

Option 1: Both STI-PAs have explicit trust in each other. Each STI-PA will provide read-only access to the other STI-PA's Trusted STI-CA list via a limited-access account. The interfaces and mechanisms are provided in ATIS 1000084.

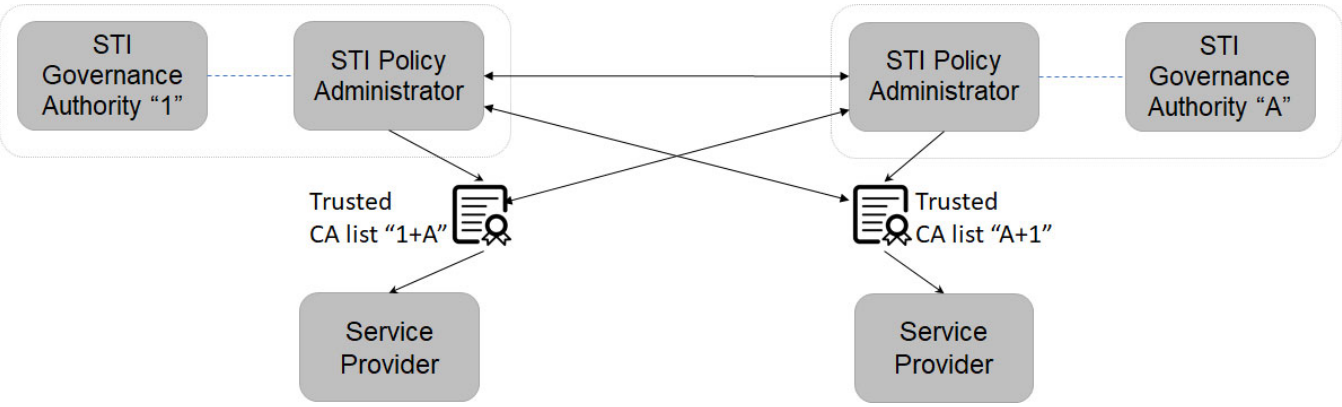

Figure 4-7: Mutual Exchange

Option 2: 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-PA is directed to exchange Trusted CA lists with another country, the STI-PA will 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. The server will also include the URL for the Certificate Revocation list. This document does not specify what the STI-PA will do with the information on Trusted CAs.

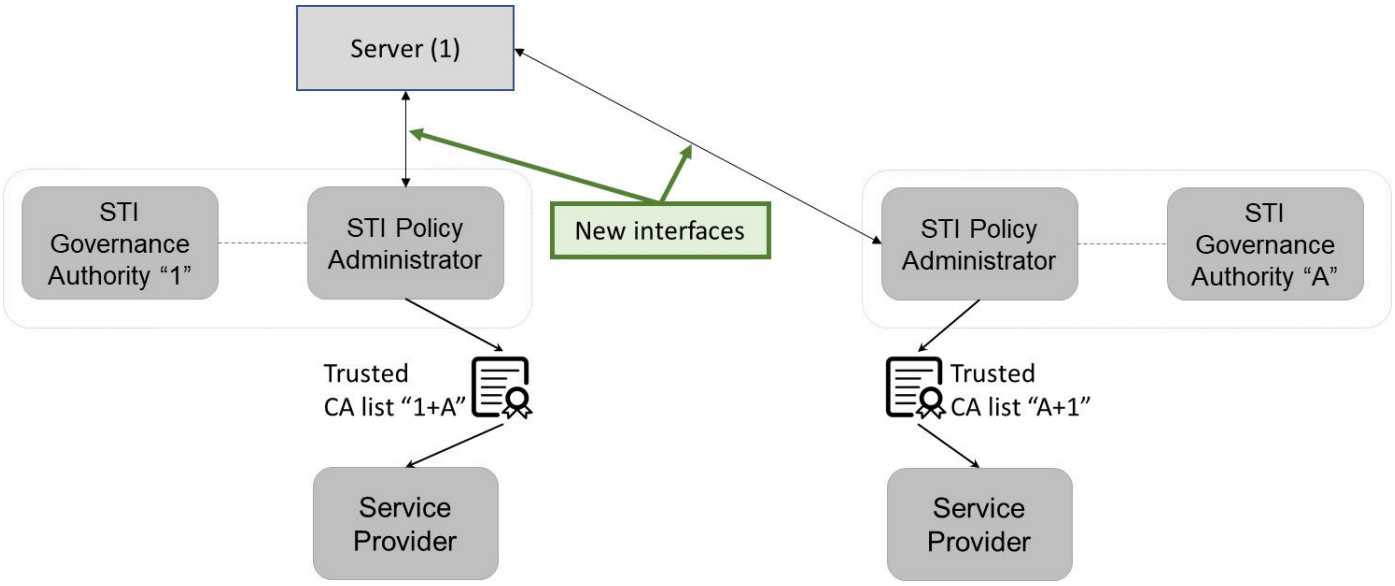

Figure 4-8: Trusted STI-CA Server

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

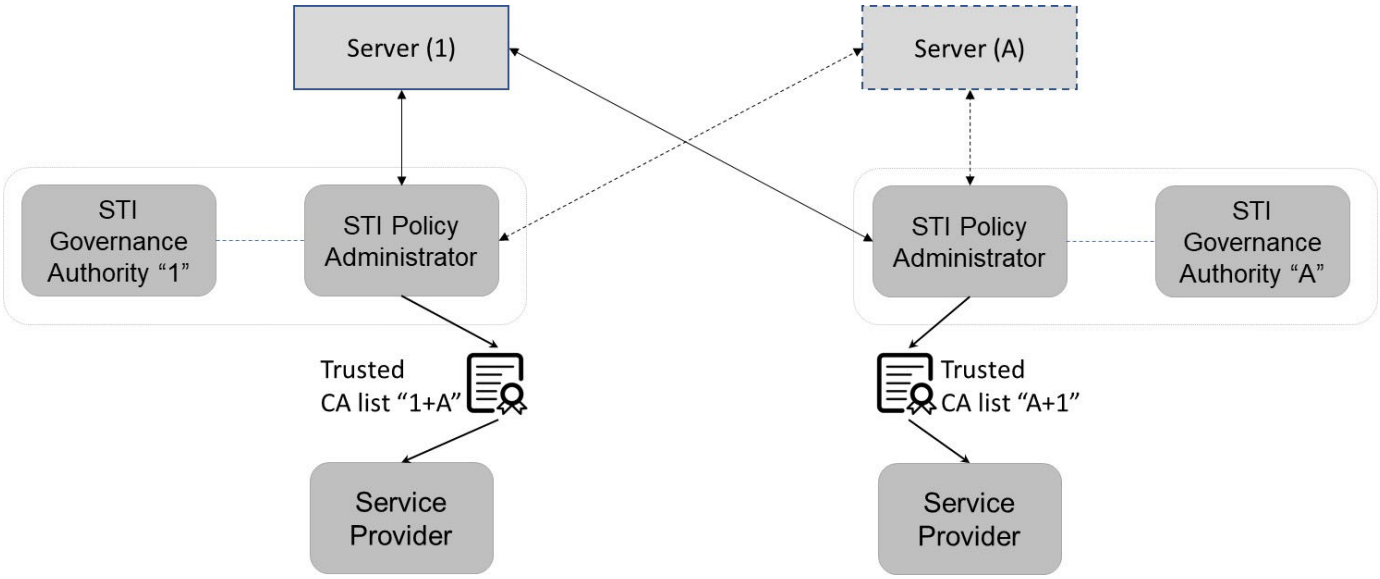

Figure 4-9: Trusted STI-CA Servers

4.3.1 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 "Country" fields in the root certification 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 provides a server with details of all STI-CAs on their Trusted CA list. The Trusted CA list contains 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).

4.3.2 Interface to Server

This document recommends the use of an API over HTTPS [RFC 7231] for the distribution of the list of trusted STI-CAs. 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].

4.3.3 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 authority 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.

4.4 Compatible Implementations

This technical report assumes the only changes required to allow for call verification between the countries are by the STI-PAs in each country. It assumes that each country has implemented compatible SHAKEN internetwork signaling and that any updates to the internetwork signaling would be coordinated between the countries involved.