ATIS-1000091

Mechanism for International 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.

The SIP Forum is a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. The SIP Forum is also the producer of the annual SIPNOC conferences (for SIP Network Operators Conference), focused on the technical requirements of the service provider community. One of the Forum's technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated "SIPconnect Certified" logo program that provides an official "seal of certification" for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

< http://www.sipforum.org/ >

ATIS-1000091, Mechanism for International Signature-based Handling of Asserted information using toKENs (SHAKEN)

Is an ATIS & SIP Forum Technical Report developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

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

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

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 International 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. ATIS-1000087, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)*, provides an initial mechanism for cross-border SHAKEN calls, but it recognizes that it is only the first step, and that a more general approach is required to accommodate the general cases of international SHAKEN calls. In particular, it is not scalable for all countries to execute bilateral agreements. That is a "193[2] problem" (the formula is $\frac{(n)(n-1)}{2}$). The purpose of this document is to detail how to extend SHAKEN while maintaining the SHAKEN trust framework. 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 full international deployment. This document will detail how calls authenticated in one country can be successfully verified in a second country, even when the countries may not share similar levels of trust.

1.3 Application

The mechanism described in this Technical Report will allow all countries to join an International SHAKEN registry and populate their domestic "Trusted-CA" list with minimal vetting. While this makes it easy to join the International SHAKEN ecosystem, other countries do not have to use the "Trusted-CA" information in the International SHAKEN registry. Each country retains full control over which countries they will include in their internal trusted environment. This Technical Report does not specify the format or location of the "International SHAKEN registry", but instead shows how such a registry could be used in a way that maintains the integrity of the SHAKEN trust environment.

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.

[Ref 1] ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN)* [1]

[Ref 2] ATIS-1000080, *SHAKEN: Governance Model and Certificate Management*[1]

[Ref 3] ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*[1]

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

[Ref 4] ATIS-1000087, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)*[2]

[Ref 5] draft-burger-stir-iana-cert-00, *Registry for Country-Specific Secure Telephone Identity (STIR) Root Certificates*[3]

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
CVT	Call Validation Treatment
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

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

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

STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-GA	Secure Telephone Identity Governance Authority
STI-PA	Secure Telephone Identity Policy Administrator
STIR	Secure Telephone Identity Revisited
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 authority in one country from deciding to recognize the STI-CAs from another country and instructing the STI-PA to include the STI-CAs in their "Trusted STI-CA" list. The merged trusted STI-CA list could then be distributed to all service providers using existing interfaces and procedures. Calls authenticated in one country would then successfully verify in the second country. ATIS-1000087, *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)* [Ref 4], provides a mechanism for sharing "Trusted STI-CA" lists between countries with similar legal and regulatory environments but does not cover the more general case of full International SHAKEN. This document specifies the architecture and interfaces that could be used to exchange trusted STI-CA lists between all countries, while still maintaining the SHAKEN trust environment.

4.1 International SHAKEN Architecture

At a high level, the SHAKEN trust model is illustrated below, with a focus on the terminating service provider:

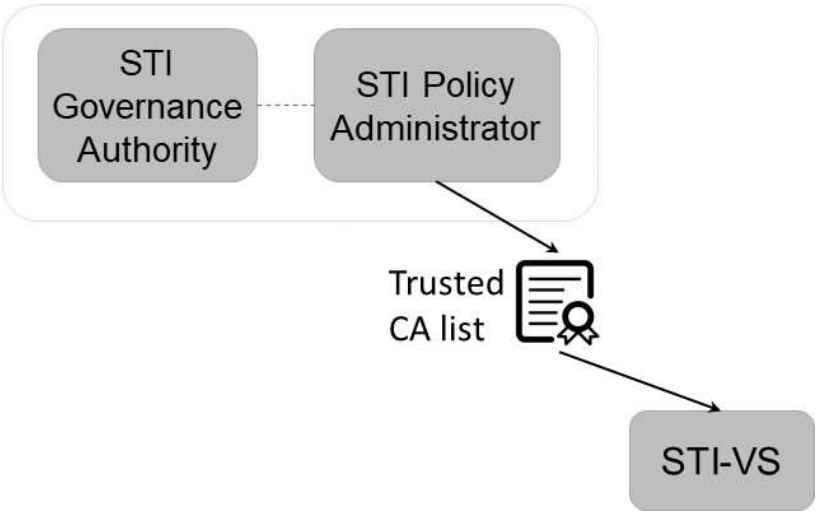

Figure 4-1: SHAKEN Trust Model

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* [Ref 3], as:

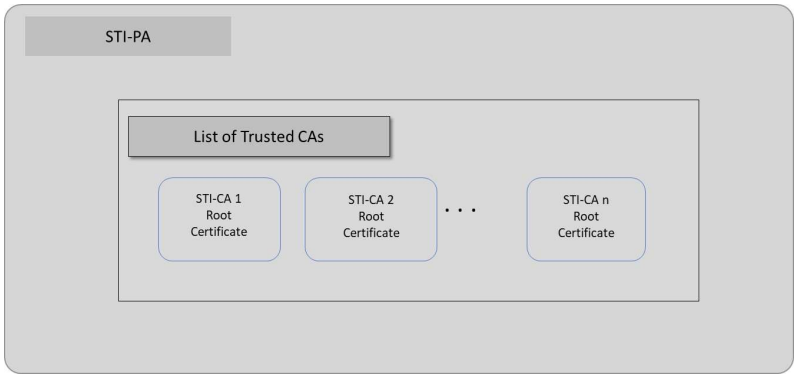

Figure 4-2: List of Trusted STI-CAs

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 have separate "Trusted STI-CA" lists and calls authenticated in one country would not be successfully verified in another country.

If country-specific "Trusted STI-CA" lists are combined, then SHAKEN calls between countries can be successfully verified. To support this functionality, the following entities are identified:

- International SHAKEN registry
- Interface to access the registry
- Reputation-based feedback

Each of these will be discussed in the following sections.

4.2 SHAKEN Governance Model

The SHAKEN governance model in ATIS-1000080 [Ref 2] includes blocks for STI Governance Authority and STI Policy Administrator but doesn't specify how these functions should be implemented. This is shown below.

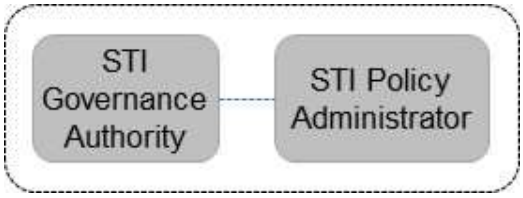

Figure 4-3: SHAKEN Governance

One approach would be to implement the Governance Authority and Policy Administrator as the independent entities illustrated in ATIS-1000080 [Ref 2], but other implementations are consistent with the model. The following diagram illustrates some of the possible alternate approaches to instantiate SHAKEN governance within an individual country.

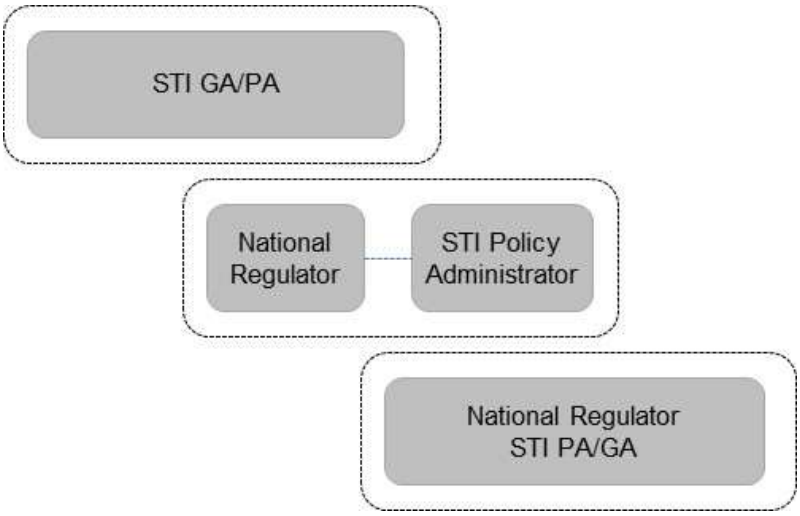

Figure 4-4: SHAKEN Governance Alternatives

Each country has the latitude to implement SHAKEN governance in accordance with their individual situation and requirements. This Technical Report doesn't assume all implementations will be the same – only that each country will have some form of SHAKEN governance recognized by the National Telecommunications Regulator.

4.3 International SHAKEN Registry

This Technical Report does not specify the details of the International SHAKEN registry, but instead is based on the proposal outlined in draft-burger-stir-iana-cert-01 [Ref 5] as the starting point for the registry. In ATIS-1000087 [Ref 4] it is assumed that individual STI-GAs apply a rigorous vetting process before deciding to trust another STI-GA and to merge "Trusted STI-CA" lists, but it was recognized that applying this same process to all countries would be combinatorically prohibitive. Therefore, for the International SHAKEN registry it is assumed that the process for registration will be lightweight and involve very little vetting to ease the process for countries to join the ecosystem. Rather than attempt to apply rigorous vetting when entering the system, this Technical Report assumes that individual countries will apply vetting before they decide to use the information in the registry. This avoids the need for a single, global vetting process and allows individual countries to have maximum flexibility in terms of local policies. The assumed registration process is illustrated below:

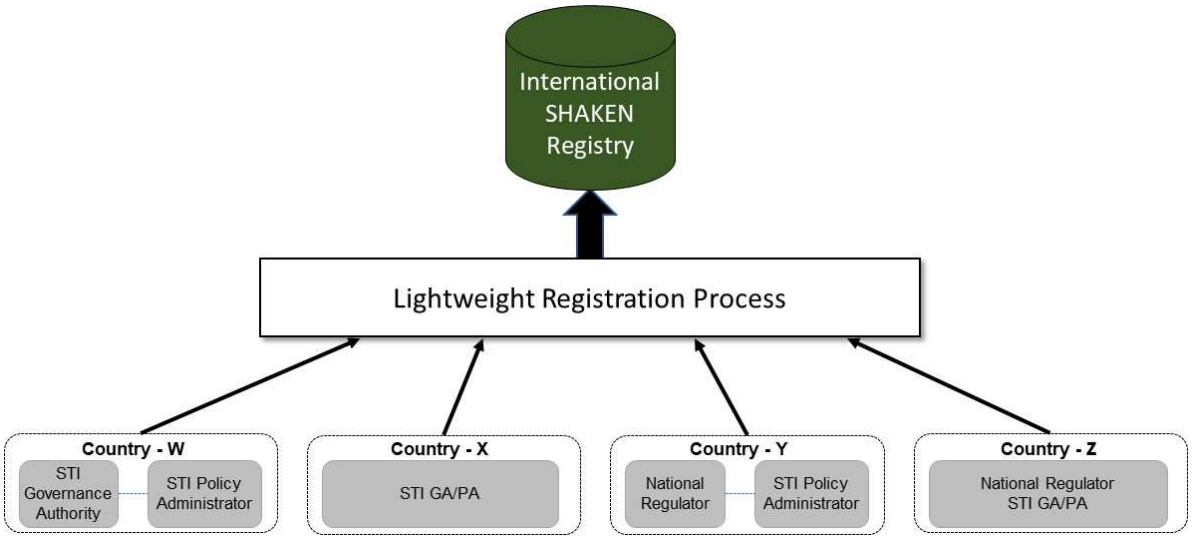

Figure 4-5: International SHAKEN Registry

The proposed specification of the International SHAKEN registry in draft-burger-stir-iana-cert-00 [Ref 5] is still a work in progress, so the details are not fully described here. However, this is not a problem, because this Technical Report does not count on the registration process to maintain the integrity of the SHAKEN ecosystem.

4.4 Interface to Access International SHAKEN Registry

Once information has been populated in the International SHAKEN registry, individual STI-GA/PAs can decide when to use this information, or if they will use it at all. In addition, the STI-GA/PA can decide to trust some countries and include their "Trusted STI-CA" list, while opting not to trust other countries. This is entirely a matter of local policy and out of scope for this document.

In practice, the STI-GA will approve accessing the International SHAKEN registry, but it will be the STI-PA that accesses the information and uses it for the local Trusted STI-CA list. These interfaces are shown below:

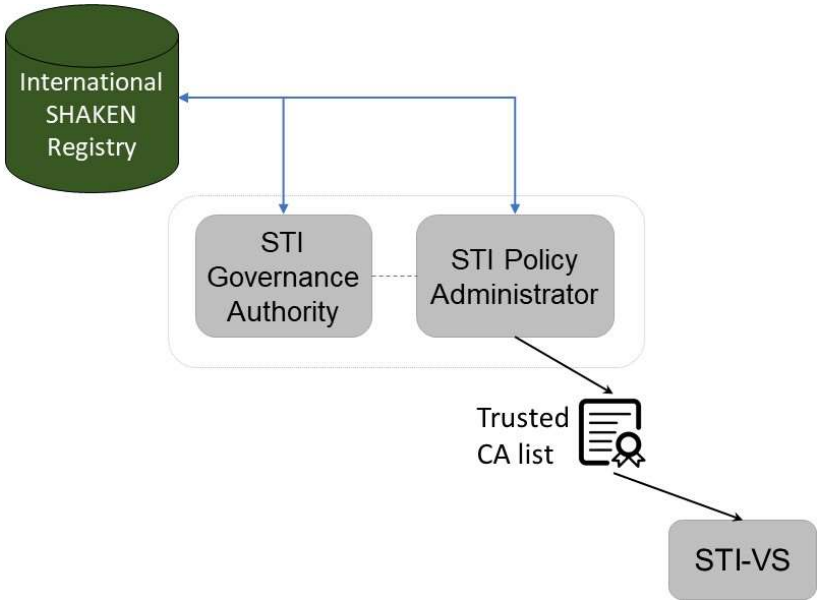

Figure 4-6: Interface to International SHAKEN Registry

The interfaces to the International SHAKEN registry can be as specified in ATIS-1000087, Clause 4.3.1 [Ref 4].

4.5 Reputation-based Feedback

The previous sections recognize that individual STI-GA/PAs can decide if they will trust other countries, but it does not say what data might be used in making this decision. This report assumes that one factor that can inform the decision is the "reputation" of the country but does not specify how that reputation will be established and updated. The SHAKEN architecture includes an analytics function that has the potential to establish reputation. The following diagram shows the SHAKEN architecture with a focus on the terminating service provider and includes the Call Validation Treatment (CVT) elements and highlights the fact that the CVT element can effectively establish a reputation for calling numbers based on usage history.

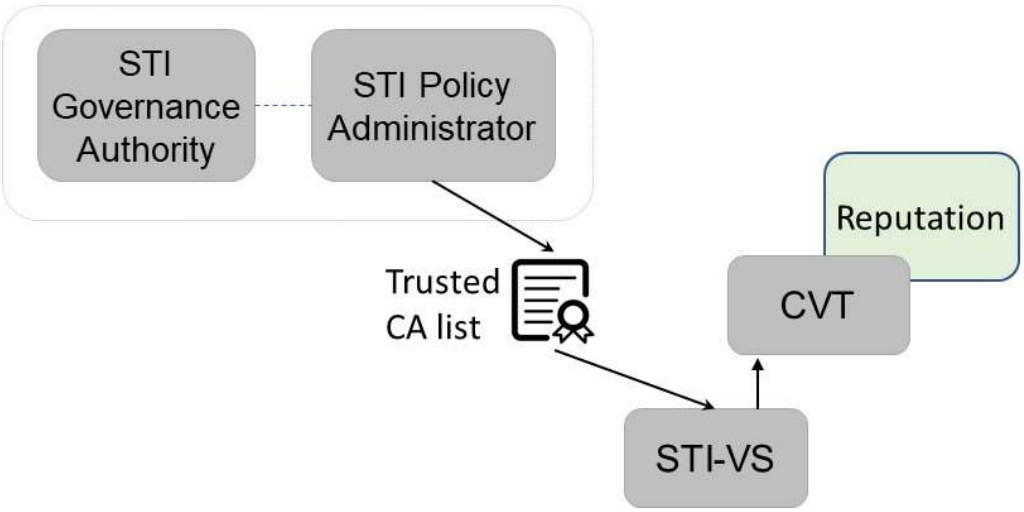

Figure 4-7: CVT and Reputation

The CVT reputation is normally associated with individual telephone numbers for the calling party, but it may be possible to extend this to also monitor the reputation for a group of numbers, potentially including all the numbers in a country. This could then be used to help the STI-GA to decide if they will continue to include a given country in their "Trusted STI-CA" list. This feedback path is shown below:

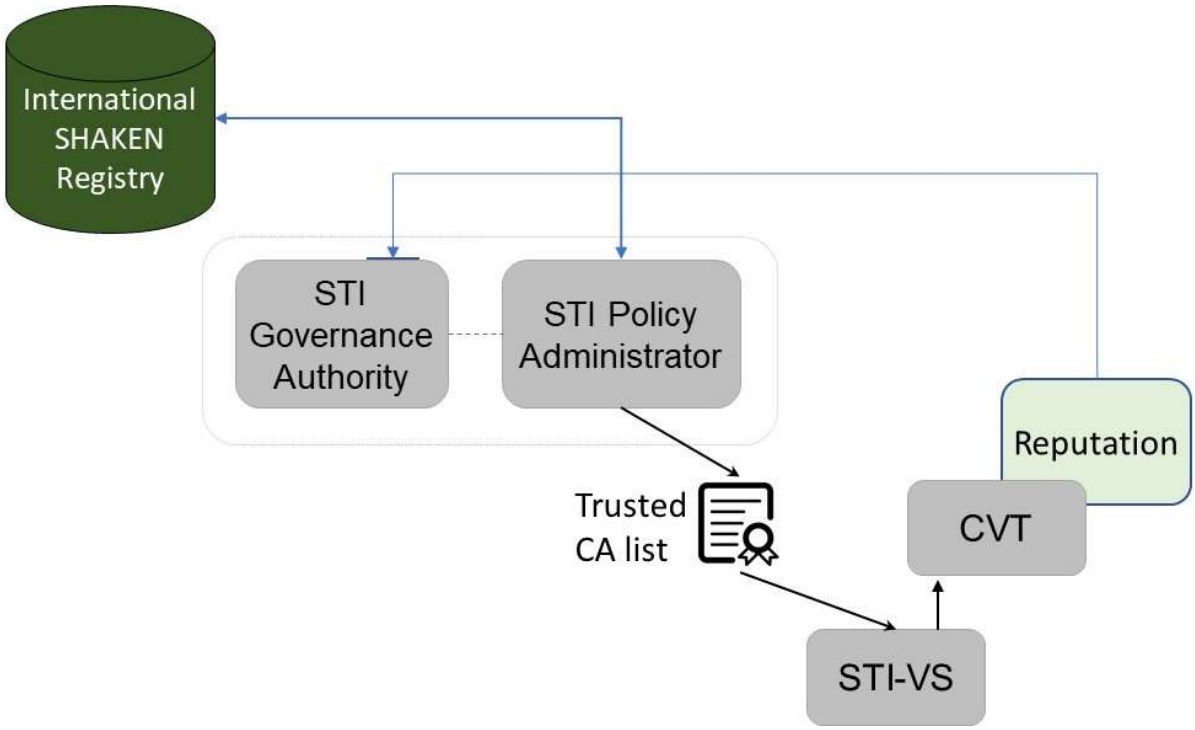

Figure 4-8: Reputation Feedback

This Technical Report identifies the mechanism that could be used for feedback to the STI-GA, but it does not provide any details on how that information would be used. This is a matter for local policy and out of scope for this Technical Report.

As an example, if a terminating STI-GA learns of calls illegally spoofed from an originating country, and that country participates in traceback and does meaningful enforcement, a terminating STI-GA is less likely to treat calls from that country as if they had no SHAKEN attestation.

The full architecture, including multiple STI-GA/PAs is shown below. This diagram also illustrates that one individual country could be excluded from the "Trusted STI-CA" list, at the discretion of the STI-GA/PA.

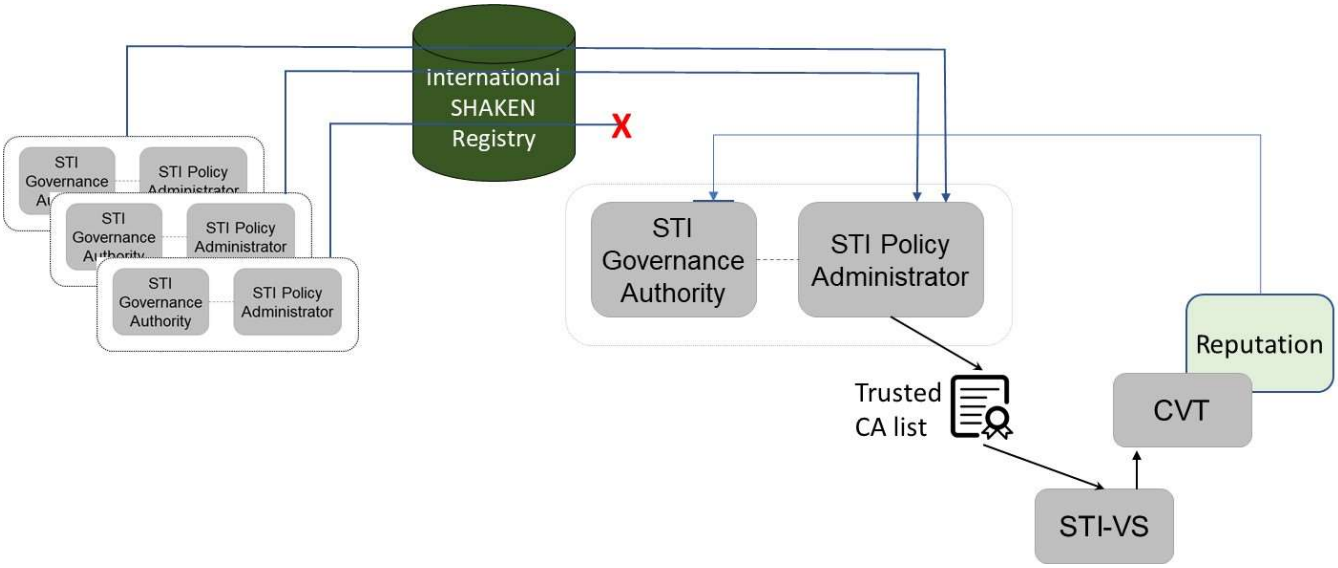

Figure 4-9: International SHAKEN Architecture

4.6 Relationship to ATIS-1000087

ATIS-1000087 [Ref 4] describes an initial mechanism to enable cross-border SHAKEN with a focus on countries with similar legal and regulatory environments. It describes how countries that fully trust each other can fully merge their "Trusted STI-CA" lists. The mechanism described in this report is intended to address the more general case with varying levels of trust. Although the mechanism in this report can be used in all cases, it does not necessarily have to be used in all cases. This approach can co-exist with ATIS-1000087 [Ref 4] and the STI-GA/PA can decide, on a country-by-country basis, which mechanism it will use.

4.7 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.