STI Policy Administrator Technical Requirements Document (TRD)

Table of Contents

Figures

DISCLAIMER AND NOTICE

This Request for Proposal (RFP), including the associated Respondent Qualification and Technical Requirements Document (TRD), is published by the STI Governance Authority (STI-GA) to gather information that it expects to be useful in the selection of an STI Policy Administrator (STI-PA). However, the STI-GA makes no commitment to consider or purchase any offering or proposal from any party submitted in response to this RFP, or to take any action, including awarding a contract. The STI-GA reserves the right, at its sole discretion, to amend, delay, or cancel this RFP at any time for any reason.

Respondent bids must address all requirements applicable to the STI-PA in ATIS-1000074, ATIS-1000080, and ATIS-1000084 (the "ATIS SHAKEN Specifications") even if not addressed in the RFP. The STI-GA makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the information contained in this RFP, the ATIS SHAKEN Specifications, responses to questions submitted pursuant to this RFP, or any public or other materials describing the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. Any use or reliance on such information is at Respondents' risk. exchange for consideration of a Respondent's submission of questions or a proposal in response to this RFP, Respondent agrees by such submission to all of the terms of this RFP, including the limitations of liability and indemnification obligations set forth in Section 1.4.

The Respondent will bear all costs of preparing and submitting its proposal, responding to or providing any other assistance to the STI-GA in connection with this RFP.

Nothing contained herein shall be construed to confer any license or right to any intellectual property to any Respondent, whether or not the use of any information herein necessarily utilizes such intellectual property. The Respondent agrees that all documents, materials, articles, and information it submits with a question or as part of, or in support of a bid is and shall be given entirely voluntarily, and shall become, upon submission, the physical and intellectual property of the STI-GA in right that the STI-GA shall be free to use, disclose, and exploit as it sees fit, entirely without obligation or remuneration to the Respondent, and will not be returned to the Respondent at the conclusion of the RFP process.

1 General Information and Background

1.1 Introduction

The FCC North American Numbering Council (NANC) Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR,[1] completed by the NANC Call Authentication Trust Anchor Working Group, recommended establishing an industry-led governance authority with broad representation from key industry associations and stakeholders. The identified stakeholders agreed to establish the Secure Telephone Identity Governance Authority (STI-GA) under the auspices of the Alliance for Telecommunications Industry Solutions (ATIS). The NANC report also recommended that the Secure Telephone Identity Policy Administrator (STI-PA) should be selected through a Request for Proposal (RFP) process overseen by the STI-GA Board of Directors, the policy and decision-making body of the STI-GA.

The primary function of the STI-GA is to define, and modify as necessary, the rules governing the Secure Handling of Asserted information using toKENs (SHAKEN) framework. The STI-PA plays a key role in this framework, applying and enforcing the rules as defined by the STI-GA. In particular, the STI-PA verifies that a Service Provider (SP) meets the defined criteria for participation in the SHAKEN framework before issuing "Service Provider Code tokens" to the approved SP. The STI-PA must also renew the Service Provider Code token as required, after verifying that the SP continues to meet the criteria to participate in the SHAKEN framework. The Service Provider Code token is used for authentication when the SP obtains Secure Telephone Identity (STI) certificates from an approved Secure Telephone Identity Certification Authority (STI-CA). The STI-PA is also responsible for approving STI-CAs and verifying that the STI-CA meets all requirements of its Certification Practice Statement to assess compliance with Certificate Policy. Finally, the STI-PA must securely maintain a "trusted STI-CA" list and, when necessary, an SP certificate revocation list, and distribute this to all SPs participating in the SHAKEN ecosystem.

1.2 Purpose

This RFP is being issued by the STI-GA to identify a Respondent and/or any Sub-Contractor(s) (Respondent) that can design, develop, build, deliver, and operate the STI-PA function as defined in the ATIS SHAKEN Specifications ATIS-1000074, ATIS-1000080, and ATIS-1000084 (the "ATIS SHAKEN Specifications").

The chosen Respondent will be expected to deliver a secure, innovative, and efficient solution to securely manage the distribution of STI certificates to support the SHAKEN framework. The STI-PA function is envisioned to use existing, known, and proven technologies. However, no matter what solution the chosen Respondent provides, it must address all requirements.

The STI-GA will evaluate all proposals in order to select the Respondent and approach that best meets the requirements. However, the STI-GA makes no commitment to purchase any offering from a Respondent with respect to this RFP, or to take any action, including awarding a contract. The STI-GA assumes no contractual obligation, or specific contractual content by issuing this RFP, and reserves the right, at its sole discretion, to amend, delay or cancel this RFP at any time.

[1] The CATA WG's Final Report is available at: http://www.nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf

1.3 Technical Requirements Document Response Instructions

This document is the third of three components in this RFP. Respondents should begin with the RFP component and the Respondent Qualification component before completing this component.

The RFP process is comprised of three parts, which should be completed in this order and submitted together:

1. Secure Telephone Identity Policy Administrator Request for Proposal (RFP)
2. Secure Telephone Identity Policy Administrator RFP Respondent Qualification (Respondent Qualification)
3. Secure Telephone Identity Policy Administrator Technical Requirements Document (TRD)

Though the term RFP sometimes is used to refer solely to the first component, the term "RFP" encompasses all three components. The Respondent Qualification describes the criteria that must be satisfied by each prospective Respondent. This includes the Respondent's proposal, information about the Respondent's organizational structure, past performance, financial responsibility and stability, and acceptance of key business terms. The TRD (this document) describes the technical requirements for a proposal and the STI-PA's required obligations. Although great care has been taken to ensure the accuracy of the TRD and other reference documents, it is the Respondent's responsibility to ensure that any response to a specific technical requirement contained herein is based on the latest ATIS SHAKEN Specifications and other ATIS technical documents (available at http://www.atis.org/sti-ga/resources/) as well as other reference documents as currently published and made available to the industry.

Each Respondent is provided an opportunity to demonstrate how its proposal satisfies the RFP's requirements. Each Respondent is instructed to answer all questions in as concise and complete a manner as possible, and in many instances, the Respondent is provided with an opportunity to elaborate on its answers.

The STI-GA Board has authorized one of its Task Forces, the RFP Task Force (hereafter referred to as the RFP TF), to manage the STI-PA RFP process, including the solicitation and evaluation of responses. The selection process is expected to conclude in or about May 2019.

Please note:

1. Respondents must notify the STI-GA of their interest in bidding by e-mailing sti-ga@atis.org. Interested parties will be provided with credentials and instructions for bidding. E-mail, facsimile, or hard-copy responses will not be considered.

2. All questions must be emailed to sti-ga@atis.org and must be received no later than December 10, 2018. The STI-GA will endeavor to respond to questions promptly and shall make answers available to all parties.

3. Respondents must satisfy the Respondent Qualification criteria and TRD criteria.

4. All responses and submissions must be complete, truthful, and accurate. Material misrepresentations or omissions may result in disqualification or reductions in scoring.

5. All responses must be received on or before the RFP response cut-off date as described in Section 1.5.

6. Nothing contained herein shall be construed to confer any license or right to any intellectual property to any Respondent, whether or not the use of any information herein necessarily utilizes such intellectual property.

7. When a Respondent prepares its quote and submits responses, the Respondent must review all specifications and drawings associated with a particular item, as the Respondent is responsible for quoting all material, performance, quality, and technical requirements for each individual item.

1.4 Terms Applicable to RFP Submissions

Respondents agree that all responses and information provided in connection with a response is given entirely voluntarily, and shall become, upon submission, the physical and intellectual property of the STI-GA in that the STI-GA shall be free to use, disclose, and exploit as it sees fit, entirely without obligation or remuneration to Respondent, and will not be returned to the Respondent at the conclusion of the RFP process. The STI-GA Board expressly reserves the right to reject any and all responses to this RFP. The STI-GA Board may engage independent consultants to assist in the evaluation of responses and to make recommendations to the STI-GA Board. The STI-GA Board reserves the right to request additional information or clarification from Respondents.

Responses must be submitted in accordance with the instructions in Section 1.3. Any response submitted after the RFP Cut-off Date as described in Section 1.5 of this RFP may not be considered. A Respondent is solely responsible for ensuring that its response is submitted and received by the STI-GA Board in accordance with the instructions.

The STI-GA makes no representation or warranty, express or implied, with respect to the completeness, accuracy or utility of the information contained in this RFP, the ATIS SHAKEN Specifications, responses to questions submitted pursuant to this RFP, or any public or other materials describing the SHAKEN framework. Any use or reliance on such information is at the Respondent's risk. In exchange for consideration of a Respondent's submission of questions or a proposal in response to this RFP, Respondent agrees by such submission to all of the terms of this RFP, including that the STI-GA Board (and Board Committees and Task Forces), ATIS and their employees, officers, agents, contractors, consultants, members, and counsel of each (each, an "Covered Party") shall not be liable to any entity for any damage, injury, or claim of lost opportunity incurred by any person arising out of the completeness, accuracy or utility of any information contained in this RFP or other information or any decision by the STI-GA to award or not to award a contract for the STI-PA role to any entity, and to indemnify and hold harmless each Covered Party from and against any and all liabilities, demands, damages, expenses and losses arising from such submission. These indemnification obligations and limitations of liability shall survive termination of the RFP and any contract executed in connection with the RFP. The Respondent shall be solely responsible for any claims, costs (including legal fees) or damages it incurs in connection with all submissions and responses.

In the event that the STI-GA engages a Respondent in discussions of its proposal that may lead to an agreement to serve as STI-PA, the Respondent may be required to agree to the terms of a confidentiality agreement to protect confidential information prior to the execution of the agreement to be executed between the STI-PA and STI-GA that will include confidentiality terms.

1.5 RFP Respondent Selection Process Time Line

Below is the proposed time line for the Respondent selection pursuant to the RFP. The STI-GA reserves the right to modify or adjust the following dates or to otherwise change or amend this timeline:

- November 15, 2018: RFP issued and posted on STI-GA website.
- November 15, 2018: Press release published by ATIS on behalf of STI-GA.
- December 10, 2018: Last date to submit questions to STI-GA.
- February 4, 2019: RFP response cut-off date (deadline for bidders to submit proposals).
- May 2019: Selection of STI-PA by STI-GA.

1.6 Essential Functions and Structure

The SHAKEN framework (ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN)*) utilizes protocols defined in the IETF Secure Telephone Identity Revisited (STIR) Working Group to describe an end-to-end architecture for the authentication and assertion of a telephone identity by an originating SP and the verification of the telephone identity by a terminating SP. Today, Caller ID information is typically passed in the P-Asserted-Identity header field, which can be manipulated by the end user and passed on to an intermediate or terminating carrier without validation. As a result, Caller ID information may not be reliable. Use of standardized cryptographic digital signatures can provide a verifiable mechanism to identify and validate the originator of a call into the public switched telephone network. Verifiers of signatures will use these attestations to help identify call spam and to facilitate trace back mechanisms to support enforcement actions against companies making illegal robocalls. The SHAKEN framework uses X.509 certificates, as defined in IETF [RFC 5280], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, to verify the digital signatures associated with SIP identifiers.

The SHAKEN Governance Model (ATIS-1000080, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*) specifies a reference model and defines the roles and responsibilities of the STI-PA, and the relationship of the STI-PA to the STI-CA and to the SP. It defines protocols and certificate management procedures for the SHAKEN framework and provides recommendations and requirements for implementing relevant IETF specifications (RFC 8225, RFC 8224, RFC 8226, draft-ietf-acme-authority-token, draft-ietf-acme-authority-token-tnauthlist and draft-ietf-acme-acme), to support management of SP-level certificates within the SHAKEN framework.

Finally, ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*, introduces operational and management considerations for the STI-PA and STI-CAs within the SHAKEN framework and the SHAKEN Governance Model framework ATIS-1000080.

This overview of the essential functions and structure is intended to provide context and prepare the Respondent for the detailed TRD sections that follow.

Question 1:

Has the Respondent read, understood and incorporated the Essential Functions and Structure concepts into Respondent's proposal?

- Yes
- No

1.7 The SHAKEN Governance Model

The SHAKEN Governance Model identifies the following roles associated with governance and STI certificate management:

- Secure Telephone Identity Governance Authority (STI-GA): the role of the STI-GA is to govern the policies and the security around issuance and use of STI certificates by SHAKEN participants.

- Secure Telephone Identity Policy Administrator (STI-PA): The STI-PA administers the technical operations, executes the policies, and verifies participants authorized to participate in the SHAKEN ecosystem. The STI-PA will apply both the policy and direction of the STI-GA, as well as conform to the technical specification of the SHAKEN certificate framework, as they evolve to ensure security and integrity in the SHAKEN ecosystem.

- Secure Telephone Identity Certification Authorities (STI-CAs): the role of the STI-CA is to issue STI certificates to authorized service providers.

- Service Providers (SPs): in the SHAKEN framework, SPs authenticate calling party information at the call origination, and verify this information at the call termination.

Figure 1 illustrates the SHAKEN Governance Model.

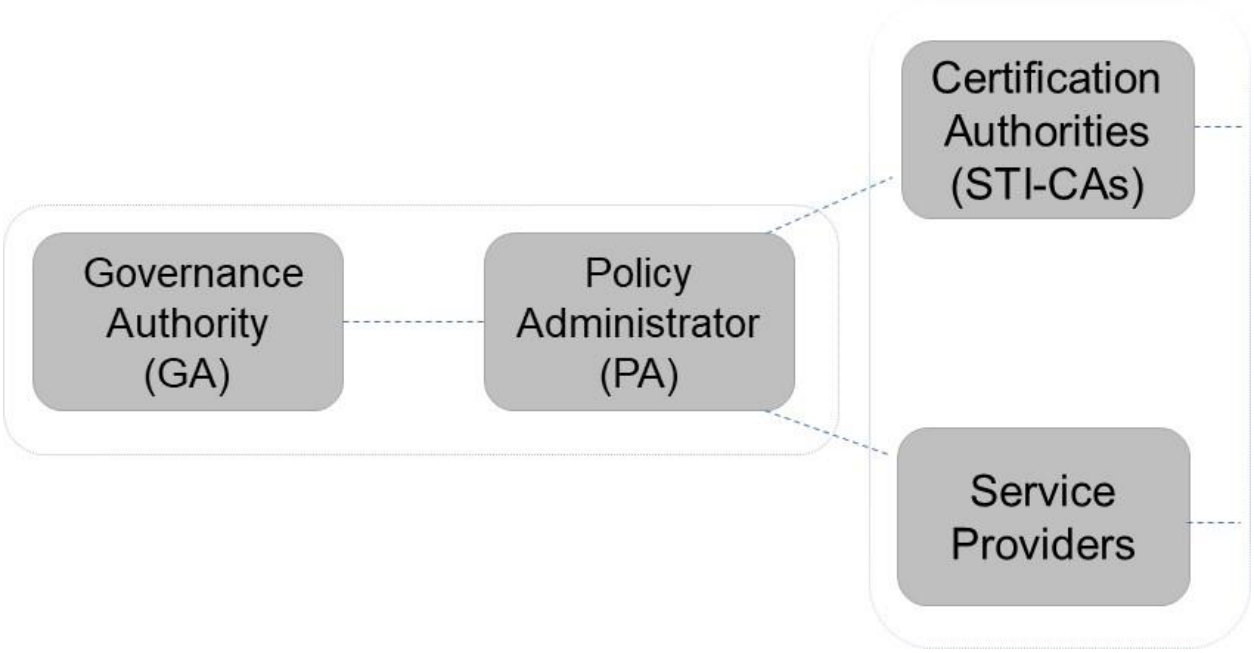

Figure 1: SHAKEN Governance Model [ATIS-1000080]

Question 2

Has the Respondent read, understood and incorporated the SHAKEN Governance Model concepts into Respondent's proposal?

- Yes
- No

1.8 The Role of the STI Policy Administrator

The STI-PA applies the rules and policies defined by the STI-GA to confirm that SPs are authorized to request STI certificates and to authorize STI-CAs to issue STI certificates.

The STI-PA manages an active, secure list of approved STI-CAs in the form of their public key certificates. When necessary, the STI-PA also manages an active, secure list of SP certificates that have been reported compromised by SPs as a revocation list. The STI-PA provides the list of both approved STI-CAs and revoked SP certificates to the SPs via a Hypertext Transfer Protocol Secure (HTTPS) interface. The SHAKEN-defined Secure Telephone Identity Verification Service (STI-VS) can then use a public key certificate to validate the root of the digital signature in the STI certificate by determining whether the STI-CA that issued the STI certificate is in the list of approved STI-CAs. The STI-VS should in addition, if it exists, use the list of revoked SP certificates as guidance to not verify digital signatures signed by these certificates.

The STI-PA also maintains a distinct X.509-based Public Key Infrastructure (PKI) for digitally signing Service Provider Code tokens, which represent the credentials and validation of SPs. An SP uses this Service Provider Code token, which is a signed JSON Web Token (JWT), for validation when requesting issuance of STI certificates from an approved STI-CA.

The SHAKEN model defines the STI-PA as the Trust Anchor for this token-based mechanism for validation of SPs within a national/regional administrative domain. For example, all STI certificates for the SP tokens in the United States will be associated with a single STI-PA Trust Anchor. Other countries could have a different Trust Anchor.

Question 3

Has the Respondent read, understood, and incorporated the role of the STI-PA into the Respondent's proposal?

- Yes
- No

1.9 Reference Architecture and Interfaces

Figure 2 illustrates the SHAKEN Certificate Management Architecture.

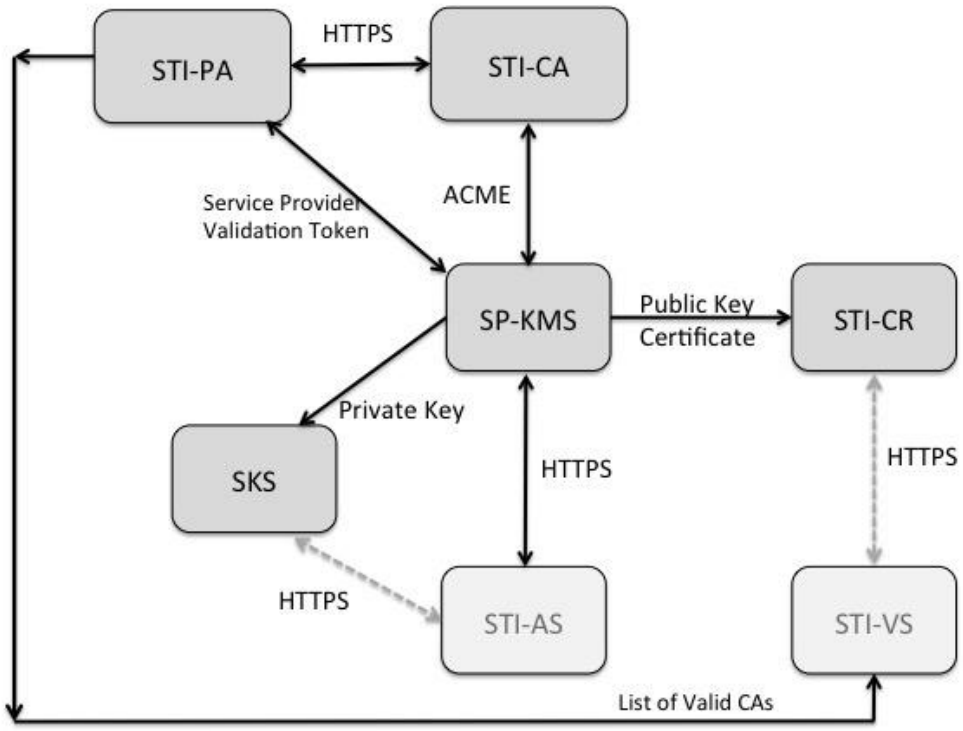

Figure 2:SHAKEN Certificate Management Architecture [ATIS-1000084]

Figure 2 shows three primary interfaces that must be supported by the STI-PA:

- HTTPS interface between the STI-PA and the STI-CA.
- Interface between the STI-PA and the SP Key Management System (SP-KMS) used to distribute Service Provider Code tokens.
- Interface between the STI-PA and the SP STI-VS used to distribute the list of approved STI-CAs and revoked SP certificates.

Question 4

Has the Respondent read, understood and incorporated the SHAKEN Reference architecture and interfaces concepts into the Respondent's proposal?

- Yes
- No

2 Technical Aspects and Standards

This section identifies key technical requirements that must be explicitly addressed in all RFP responses. In addition, all requirements applicable to the STI-PA in the ATIS SHAKEN Specifications must be satisfied even if not explicitly addressed in the sections of this RFP. If any requirements in the ATIS SHAKEN Specifications cannot be met, these must be explicitly identified in RFP responses with an explanation of the impact on the SHAKEN ecosystem.

Question 5

Has the Respondent read, understood, and incorporated all requirements in the relevant ATIS SHAKEN Specifications identified in this section into the Respondent's proposal?

- Yes
- No

2.1 Architecture Interfaces and Protocols

Figure 3 identifies the roles and responsibilities of the STI-PA, including interfaces to other functional entities in the SHAKEN framework. (All terms in this diagram are defined in Sections 2.3 – 2.11 below.)

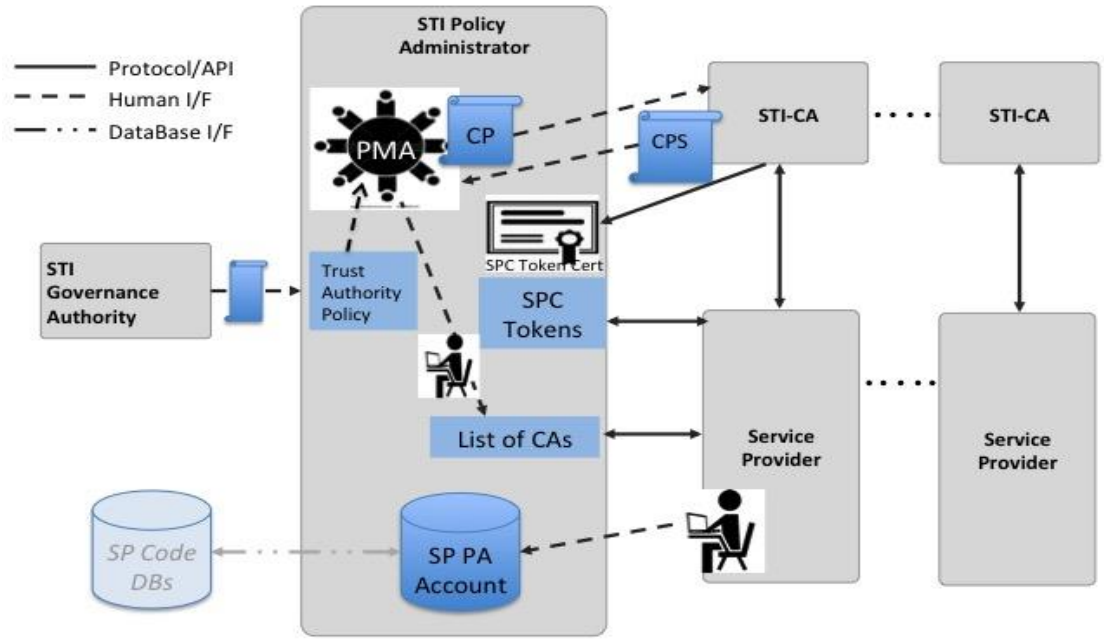

Figure 3: Architecture Interfaces and Protocols [ATIS-1000084]

The following key components of this architecture are highlighted in Figure 4, and will be addressed in the remainder of this section:

- Trust Authority Policy
- Policy Management Authority (PMA)
- List of approved STI-CAs and revoked SP certificates
- SP account registration and SP authorization
- Service Provider Code tokens

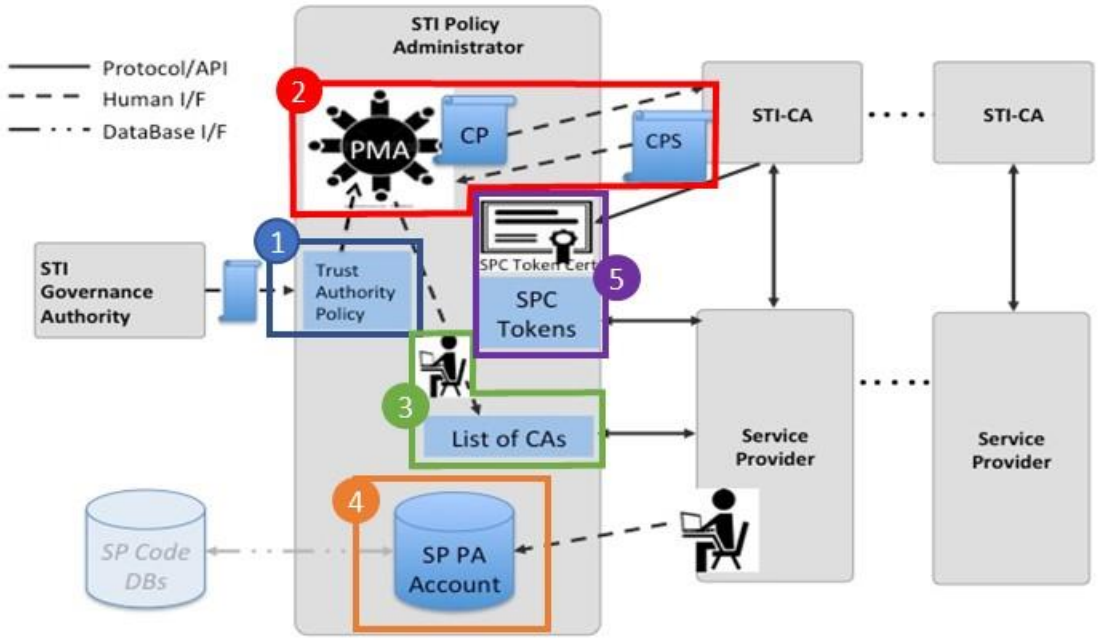

Figure 4: Architecture Interfaces and Protocols: Key Components

Question 6

Has the Respondent read, understood and incorporated the roles and responsibilities of the STI-PA, including interfaces into other functional entities into the Respondent's proposal?

- Yes
- No

2.2 Trust Authority Policy

The STI-PA is entrusted by the STI-GA to serve in a policy enforcement role and act as the Trust Authority for SHAKEN. In that role, the STI-PA applies and enforces any policies established by the STI-

GA. Based on the direction of the STI-GA, the STI-PA develops a Trust Authority Policy, including the following:

- STI-CAs shall not inherit trust from other STI-CAs in the deployment of the SHAKEN framework (i.e., the STI-PA is the only trust authority). To preclude this, policy mapping shall be inhibited.[2]

- Initially, any entity that meets the Certificate Policy (CP) established by the STI-PA can be approved as an STI-CA to manage the PKI and issue STI certificates. There are no limits currently on the number of STI-CAs. In the future, the STI-GA could introduce additional requirements for STI-CAs or impose limits on the maximum number of STI-CAs.

- The STI-PA may remove an STI-CA from the list of trusted STI-CAs based on specific criteria. Initially, the only identified criteria will be "failure to comply with the CP established by the STI-PA," although the STI-GA may specify additional criteria in the future. Compliance must be audited by the PMA on a regular basis (initially annually). The STI-GA will establish guidelines for the timeframe in which an identified problem must be resolved.

- The STI-PA shall report to SPs any revoked SP certificates for the length of the revoked certificate's lifetime. The STI-PA will validate the report of a compromised certificate from a SP before adding it to the list of revoked SP certificates. This policy would also apply for any SP that are either voluntarily or otherwise removed from the list of valid SPs and no longer have the authority to receive Service Provider Code tokens. All of the active lifetime SP certificates shall be placed on the SP certificate revocation list to prevent invalid verification of digital signatures.

- Document the policies and procedures governing which entities can acquire STI certificates. For example, the STI-GA Board may decide to make STI certificates available to all SPs with an Operating Company Number (OCN) that are eligible to directly obtain numbering resources from the North American Numbering Plan Administrator and/or the Pooling Administrator. Per ATIS-1000080, the STI-GA can define this and/or other policies and procedures governing which entities can acquire STI certificates, and may do so in the future.

- Other policies established by the STI-GA for operation of the STI-PA.

Question 7

Does the Respondent's proposal incorporate the ability of the STI-PA to serve in a policy enforcement role for the STI-GA, and the ability to act as the Trust Authority for SHAKEN Governance Model, based on the policies identified in this section and the ATIS SHAKEN Specifications, into Respondent's proposal, and has the Respondent read, understood and incorporated these concepts into the Respondent's proposal?

- Yes
- No

[2] i.e., The STI-PA should be a standalone PKI/root for the Service Provider Code tokens and must not have any inherited trust from another CA.

2.3 Policy Management Authority

The STI-PA applies and enforces any policies established by the STI-GA in the STI-PA's role as the Trust Authority. In this role, the STI-PA serves as the Trust Authority to the relying parties in the PKI. The STI-PA maintains the Trust List of authorized STI-CAs who establish their own PKI for issuing certificates, per Figure 5.

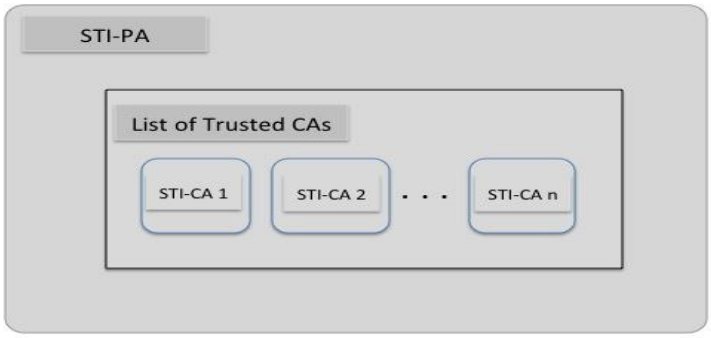

Figure 5: Trust Model [ATIS-1000084]

Each of the STI-CAs operates its own Root CA and PKI infrastructure similar to the one illustrated in Figure 6.

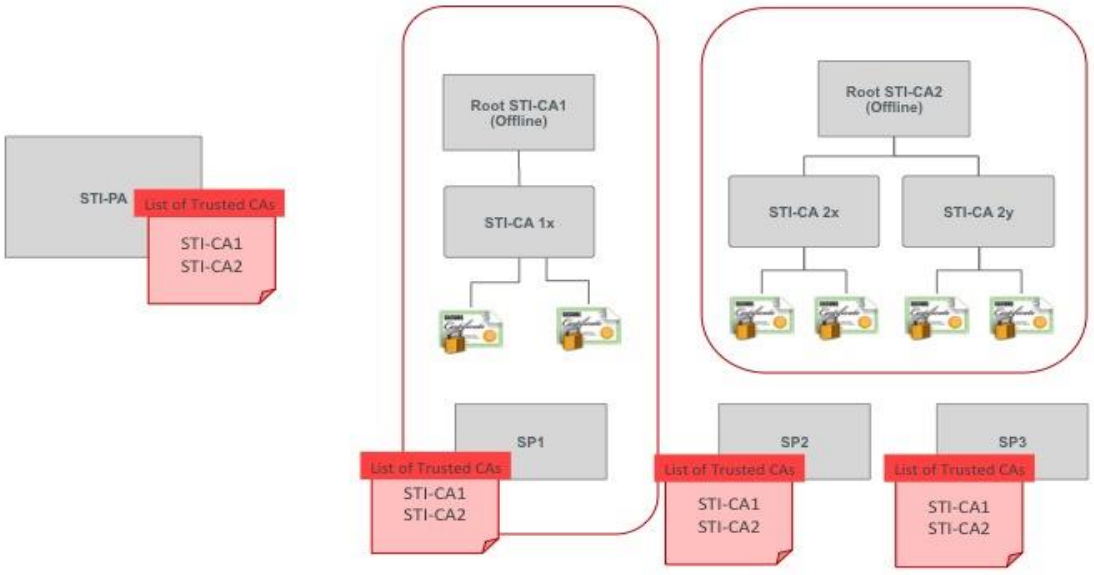

Figure 6: PKI Model [ATIS-1000084]

This multi-stakeholder PKI model includes a PMA responsible for ensuring that the established policies are followed. For SHAKEN, the STI-PA acts as the PMA.

The STI-CAs provide a Certification Practice Statement (CPS) describing their adherence to the CP during the approval process.

Question 8

Does the Respondent's proposal have the STI-PA acting as the PMA as specified in this section, and has the Respondent read, understood and incorporated these concepts into the Respondent's proposal?

- Yes
- No

2.4 Certificate Policy (CP)

The PMA defines a CP to be supported by the approved STI-CAs, as described in Clause 6.1 of ATIS-1000084. Respondents shall confirm their ability to develop a CP and to satisfy each individual sub-clause of Clause 6.1 of ATIS-1000084 in the "TRD Detailed Response" section. In addition, Respondents should provide details on relevant expertise developing Certificate Policies.

Question 9

Does the Respondent have the necessary expertise to develop a complete CP as specified in this section, and has the Respondent read, understood and incorporated these concepts into the Respondent's proposal?

- Yes
- No

2.5 Certification Practice Statement

The CPS contains the practices an STI-CA follows when issuing digital certificates. It provides detailed information about how the STI-CA implements the policy requirements documented in the CP. The CPS is written by the STI-CA.

The STI-CAs provide a CPS to the STI-PA, in the PMA role, describing their adherence to the CP during the approval process. In addition, the PMA will use the CPS during audits of STI-CAs. Respondents shall provide relevant experience using a CPS to assess compliance with CP.

Question 10

Does the Respondent's proposal include the PMA using STI-CA Certification Practice Statements to assess compliance with Certificate Policy on a regular basis?

- Yes
- No

2.6 List of Approved STI-CAs and SP Certificate Revocation List

Per the SHAKEN Governance and Certificate Management Framework, the STI-PA shall manage a list of valid CAs and revoked SP certificates. This list shall be distributed to each of the SPs for use in verifying that the STI-CA that issued the certificate has been authorized by the STI-PA and the SP certificate has not been revoked.

Managing this list of STI-CAs introduces an additional interface from the STI-PA to the STI-VS in the terminating SP's network, as Figure 7 illustrates.

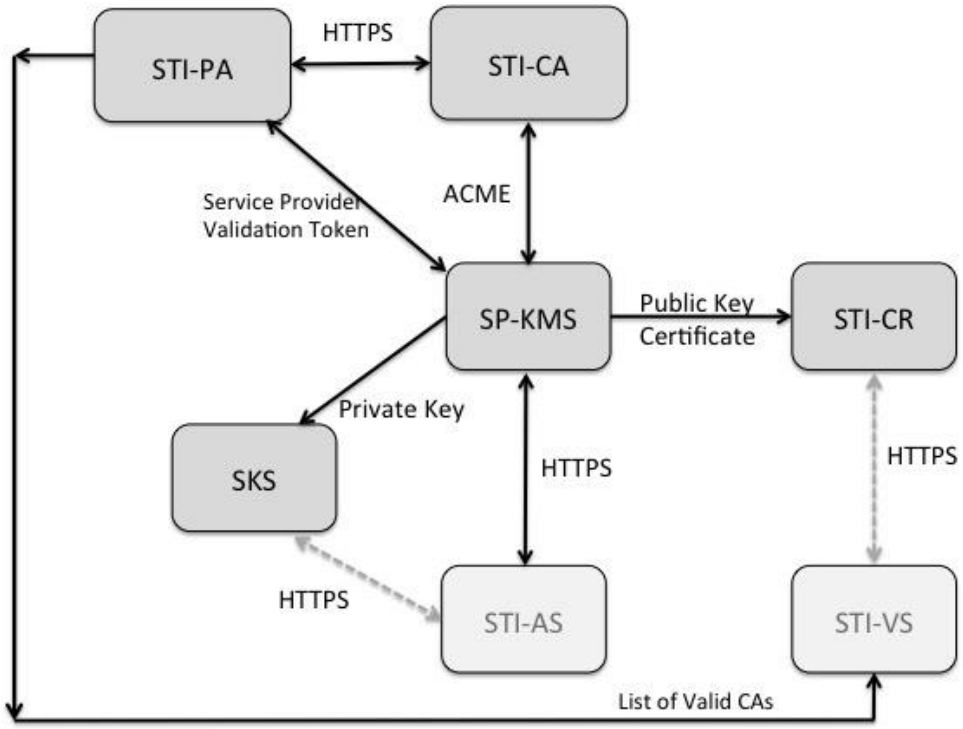

Figure 7: Interface from STI-PA to STI-VS in Terminating SP's Network [ATIS-1000084]

The STI-PA is responsible for verifying an STI-CA meets all specified requirements prior to including an STI-CA in the Trust List. The STI-PA shall only add an STI-CA to the list of Trusted STI-CAs based upon the following:

- Reviewing the CPS to determine that the PKI in which it resides is operated to an acceptable level of assurance.
- Ensuring that the Certificate Policy is supported.
- Determining that the STI-CA/PKI provides a warranty with regard to the issued certificates.

- Any other criteria that may be specified by the STI-GA.

The STI-PA is also responsible for verifying any reports of compromised SP certificates from SPs. Once the report is verified the SP certificate should be added to the SP certificate revocation list for at least the time period of the lifetime of the certificate.

Question 11

Does the Respondent's proposal include the ability to ensure that an STI-CA meets all the above criteria before adding the STI-CA to the list of Trusted STI-CAs, and the ability to receive and review any reports of compromised certificates before adding to the SP certificate revocation list, and has the Respondent read, understood and incorporated these concepts into the Respondent's proposal?

- Yes
- No

2.7 Development and Support of API

The STI-PA shall develop and support an API to distribute the list of valid STI-CAs to the STI-VS, as specified in Clause 7 of ATIS-1000084. Respondents shall provide details on the proposed API and relevant expertise.

Question 12

Does the Respondent's proposal include development and support of the API to distribute the list of valid STI-CAs to the STI-VS, and has the Respondent read, understood and incorporated the above specifications into the Respondent's proposal?

- Yes
- No

2.8 Management Interface for Populating and Updating List of Approved STI-CAs and SP Certificate Revocation List

The STI-PA must provide a management interface for populating and updating the list of approved STI-CAs and SP certificate revocation list. The Respondent must provide details about the functionality and performance of the proposed interface.

Question 13

Does the Respondent's proposal include development and support of the management interface to populate and update the list of valid STI-CAs?

- Yes
- No

2.9 SP Account Registration and SP Authorization

ATIS-1000080, Clause 6.3, provides a detailed description of the SHAKEN certificate management process. In particular, Clause 6.3.2 provides detailed requirements for the SP's registration with the STI-PA to create an account, and for the STI-PA to authorize the SP.

The STI-PA must develop, implement and support a portal for SP registration based on the above specifications. Respondents should provide details about the functionality of the SP registration portal in their TRD Detailed Response.

Question 14

Has the Respondent read, understood and incorporated these concepts for SP account registration and SP authorization into its proposal, and does the Respondent's proposal include development, support and evolution of a portal for SP registration and a function to verify that SPs meet the defined criteria before authorization?

- Yes
- No

2.10 Service Provider Code tokens

The STI-PA also maintains a distinct X.509-based PKI for digitally signing Service Provider Code tokens, which represent the credentials and validation of SPs. An SP uses this Service Provider Code token, which is a signed JWT, for validation when requesting issuance of STI certificates from an approved STI-CA. The mechanism by which the SP acquires the Service Provider Code token, the structure of the Service Provider Code token and the API are described in Clause 6.3.4 of ATIS-1000080. In addition, the STI-PA must develop, support and offer an API that allows the STI-CA to retrieve the public key of the STI-PA as specified in Clause 6.3.5.2, Step 6, of ATIS-1000080.

The account setup process is illustrated in Figure 6.3 of ATIS-1000080. The STI certificate acquisition process is illustrated in Figure 6.4 of ATIS-1000080.

Respondents must confirm their ability to implement the Service Provider Code token format and the APIs as specified in ATIS-1000080.

Question 15

Has the Respondent read, understood and incorporated these concepts into the Respondent's proposal, and does the Respondent's proposal include a function to generate Service Provider Code tokens as specified in ATIS-1000080, and does it include development, support, and operation of an API for issuing Service Provider Code tokens as specified in ATIS-1000080, and does it include development, support, and operation of an API for an STI-CA to obtain the public key of the STI-PA as specified above?

- Yes
- No

2.11 Change Management

From time to time, the STI-PA may be asked to enhance existing functions/interfaces, or to add new functions/interfaces. If SPs wish to request changes, they submit proposals to the STI-GA. Changes to the underlying technical specifications will be evaluated by the STI-GA TC and a recommendation on the need for changes proposed to the STI-GA Board for approval. The following change management process will be applied in all cases:

- The STI-GA will request a change to the STI-PA role (modification, enhancement or new functionality).

- The STI-PA will respond to the request with proposed scope of work to include approach, schedule, impact and price.

- The STI-GA will evaluate the change proposal and may either approve, reject, or modify the change proposal. If rejected or modified, the change proposal will be sent back to the STI-PA for re-assessment, if required.

- Once the STI-GA approves the final change proposal, the STI-PA proceeds with implementation.

Question 16

Has the Respondent read, understood and incorporated this change management concept into the Respondent's proposal?

- Yes
- No

2.12 Required Support and Availability

All electronic interfaces and APIs provided by the STI-PA will be offered 24/7, with at least 99.95% availability, excluding regularly scheduled maintenance windows. All manual interfaces, and support functions, will be available from 10:00 AM ET through 6:00 PM ET, Monday through Friday excluding federal holidays designated in the agreement to be executed between the STI-PA and STI-GA. Scheduled maintenance windows must be outside of these hours. The Respondent shall specify the guaranteed availability of all APIs, portals, and interfaces offered by the STI-PA.

Question 17

Does the Respondent's proposal meet the above availability, support, and maintenance window requirements?

- Yes
- No

2.13 Timeline

This TRD identifies functions and interfaces that are required to support the STI-PA role as outlined in this RFP. Respondents are asked to:

- Confirm they will provide all functions and interfaces.

- Provide a timeline detailing when each function and interface will be operational, and when the full STI-PA function will be operational. The timeline should be included in the "TRD Detailed Response" at the end of this TRD.

Question 18:

Has the Respondent read, understood and incorporated all STI-PA functions and interfaces into the Respondent's proposal?

- Yes
- No

2.14 Relevant Standards[3]

- ATIS-1000074, *Signature-based Handling of Asserted information using toKENs (SHAKEN)*
- ATIS-1000080, *Signature-based Handling of Asserted information using toKENs (SHAKEN) Governance Model and Certificate Management*
- ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*
- RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
- RFC 8225, *PASSporT: Personal Assertion Token*
- RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*
- RFC 8226, *Secure Telephone Identity Credentials: Certificates*
- draft-ietf-acme-authority-token
- draft-ietf-acme-authority-token-tnauthlist
- draft-ietf-acme-acme

[3] The following standards are available at http://www.atis.org/sti-ga/resources/

3 TRD Detailed Response

Please attach a summary document explaining how the Respondent's proposal addresses the requirements defined in this TRD. This summary should explain in detail any differences and suggested areas of improvement or enhancements that may affect the performance or security of the STI-PA, ensuring the Respondent's proposal will comply with the STI-GA’s requirements.

This summary document should also be used to include an explanation of any "No" responses.

Question 19:

- Attach the file.