ATIS-1000084

ATIS Technical Report on

Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators

Alliance for Telecommunications Industry Solutions

Approved July 25, 2018

Abstract

This document provides operational and management considerations for the Certification Authorities with the SHAKEN Governance Model and Certificate Management framework. It introduces considerations for the STI Policy Administrator in managing the list of valid STI CAs and authorized Service Providers, as well as general operational and policy considerations for PKI. This document introduces those aspects which are unique to the SHAKEN use of PKI.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, 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.

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, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

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.

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 –

Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators

1 Scope & Purpose

1.1 Scope

This technical report introduces operational and management considerations for STI Certification Authorities (STI-CAs) within the context of the SHAKEN framework (ATIS-1000074) and the SHAKEN: Governance Model and Certificate Management framework (ATIS-1000080). This document focuses on the operational and management aspects that impact the authentication and verification services, as well as general Certification Authority (CA) practices and policies. The document addresses the STI-PA operational aspects of managing the list of STI-CAs and authorization of Service Providers to obtain STI certificates. This document does not address any additional policy aspects defined by the STI Governance Authority (STI-GA), and applied by the STI Policy Administrator (STI-PA), in determining whether a CA is qualified to serve as an STI-CA nor whether a service provider is a valid service provider. The guidelines and recommendations provided in this document are based on an STI-PA starting with a list of trusted STI-CAs and a list of valid Service Providers.

1.2 Purpose

The SHAKEN: Governance Model and Certificate Management framework uses standard Public Key Infrastructure (PKI) for creating and distributing STI certificates. As such PKI Certification Practice Statement (CPS) and Certificate Policy (CP), documents per RFC 3647, are an operational requirement for the STI-CAs. This document outlines the role of the STI-PA in defining and administering required certificate policies to support SHAKEN.

The SHAKEN Governance Model and Certificate Management framework introduces a model whereby the STI-PA maintains a list of trusted STI-CAs. This list is distributed to Service Providers and used during the verification process to ensure that the public key certificate associated with a specific SIP Identity header field has been issued by a valid STI-CA. This document specifies the form of the information stored in the list and the mechanism for distributing that list to the Service Providers.

The Service Provider obtains STI certificates from the STI-CA to create signatures authenticating the identity of originators of Session Initiation Protocol (SIP) requests. The SP can obtain STI certificates from any approved STI-CA in the list of trusted STI-CAs received from the STI-PA. During account registration with the STI-PA, as detailed in ATIS-1000080, the SP selects the preferred STI-CA(s).

The SHAKEN certificate management framework is based on using a signed Service Provider Code token for validation when requesting an STI certificate. Prior to requesting a certificate, the Service Provider requests a Service Provider Code token from the STI-PA as described in ATIS-1000080. When a Service Provider initiates a Certificate Signing Request (CSR), the Service Provider proves to the STI-CA that it has been validated and is eligible to receive an STI certificate via the use of the Service Provider Code token. This document describes the STI-PA management of the Service Provider Code tokens.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard 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, *Signature-based Handling of Asserted information using toKENs (SHAKEN):*[1] *Governance Model and Certificate Management.*

[Ref 3] ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange.*[1]

[Ref 4] IETF RFC 3261, *SIP: Session Initiation Protocol.*[2]

[Ref 5] IETF RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*[2]

[Ref 6] IETF RFC 3966, *The tel URI for Telephone Numbers.*[2]

[Ref 7] IETF RFC 4949, *Internet Security Glossary, Version 2.*[2]

[Ref 8] IETF RFC 5217, *Memorandum for Multi-Domain Public Key Infrastructure Interoperability.*[2]

[Ref 9] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[2]

[Ref 10] IETF RFC 5905, *Network Time Protocol Version 4 (NTPv4).*[2]

[Ref 11] IETF RFC 7159, *The JavaScript Object Notation (JSON).*[2]

[Ref 12] IETF RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".*[2]

[Ref 13] IETF RFC 7515, *JSON Web Signatures (JWS).*[2]

[Ref 14] IETF RFC 7516, *JSON Web Encryption (JWE).*[2]

[Ref 15] IETF RFC 7517, *JSON Web Key (JWK).*[2]

[Ref 16] IETF RFC 7518, JSON *Web Algorithms (JWA).*[2]

[Ref 17] IETF RFC 7519 *JSON Web Token (JWT).*[2]

[Ref 18] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP).*[2]

[Ref 19] IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

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

The following provides some key definitions used in this document. Refer to IETF RFC 4949 for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

(Digital) Certificate: Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object. [RFC 4949].

Certification Authority (CA): An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. [RFC 4949]

Certificate Chain: See Certification Path.

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

[2] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >.

Certification Path: A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain. [RFC 4949]

Certificate Policy (CP): A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [RFC 3647]

Certification Practice Statement (CPS): A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates. [RFC 3647]

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. [RFC 4949]

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA. [RFC 3647]

Certificate Signing Request (CSR): A CSR is sent to a CA to get enrolled. A CSR contains a Public Key of the end-entity that is requesting the certificate.

Certificate Validation: An act or process by which a certificate user established that the assertions made by a certificate can be trusted. [RFC 4949]

Chain of Trust: Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain. [RFC 4949]

Company Code: A unique four-character alphanumeric code (NXXX) assigned to all Service Providers. [ATIS-0300251.2007].

End-Entity: An entity that participates in the PKI. Usually a Server, Service, Router, or a Person. In the context of SHAKEN, it is the Service Provider on behalf of the originating endpoint.

Identity: Either a canonical address-of-record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as ’sip:alice@atlanta.example.com’), or a telephone number, which commonly appears in either a TEL URI [RFC3966] or as the user portion of a SIP URI. See also Caller ID in RFC 8224.

National/Regional Regulatory Authority (NRRA): A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

National/Regional Regulatory Oversight (NRRO): A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region. Synonym for NRRA.

Online Certificate Status Protocol (OCSP): An Internet protocol used by a client to obtain the revocation status of a certificate from a server.

Policy Management Authority (PMA): A person, role, or organization within a PKI that is responsible for (a) creating or approving the content of the certificate policies and CPSs that are used in the PKI; (b) ensuring the administration of those policies; and (c) approving any cross-certification or interoperability agreements with CAs external to the PKI and any related policy mappings. The PMA may also be the accreditor for the PKI as a whole or for some of its components or applications.

Private Key: In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption. [RFC 4949]

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography. [RFC 4949]

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates. [RFC 4949]

Relying party: A system entity that depends on the validity of information (such as another entity's public key value) provided by a certificate. [RFC 5217]

Root CA: A CA that is directly trusted by an end-entity. See also Trust Anchor CA and Trusted CA. [RFC 4949]

Service Provider Code: In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider. In the US and Canada this would be a Company Code as defined in ATIS-0300251.2007.

Signature: Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data. [RFC 4949]

Subscriber: A user that is registered in a PKI and, therefore, can be named in the "subject" field of a certificate issued by a CA in that PKI. [RFC 4949]

Telephone Identity: An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

Trust Anchor: An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The combination of a trusted public key and the name of the entity to which the corresponding private key belongs. [RFC 4949]

Trust Anchor CA: A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key. See also Root CA and Trusted CA. [RFC 4949]

Trust Authority: An entity that manages a Trust List for use by one or more relying parties. [RFC 5217]

Trusted CA: A CA upon which a certificate user relies on for issuing valid certificates; especially a CA that is used as a trust anchor CA. [RFC 4949]

Trust List: A set of one or more trust anchors used by a relying party to explicitly trust one or more PKIs. [RFC 5217]

Trust Model: Describes how trust is distributed from Trust Anchors.

3.2 Acronyms & Abbreviations

ACME	Automated Certificate Management Environment (Protocol)
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
JSON	JavaScript Object Notation
JWT	JSON Web Token
NNI	Network-to-Network Interface
NRRA	National/Regional Regulatory Authority
NRRO	National/Regional Regulatory Oversight
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates
PMA	Policy Management Authority
PTSC	ATIS Packet Technologies and Systems Committee
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol

SKS	Secure Key Store
SP	Service Provider
SP-KMS	SP Key Management Server
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-GA	Secure Telephone Identity Governance Authority
STI-PA	Secure Telephone Identity Policy Administrator
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TN	Telephone Number
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol

4 Overview

The governance model in ATIS-1000080 introduces an STI-Policy Administrator that bridges the governance aspects of STI with the protocol requirements to support digital certificates [RFC 5280] which are used by the SHAKEN framework [ATIS-1000074] to authenticate and verify telephone identities. Per the governance model and certificate management framework, the STI-PA maintains a list of trusted STI-CAs to be provided to the Authentication and Verification services. The STI-PA also provides for management of the Service Providers authorized to obtain certificates and provide STI functionality within the VoIP network. This document effectively extends the roles and functions of the STI-PA beyond those defined in ATIS-1000080 per the following diagram:

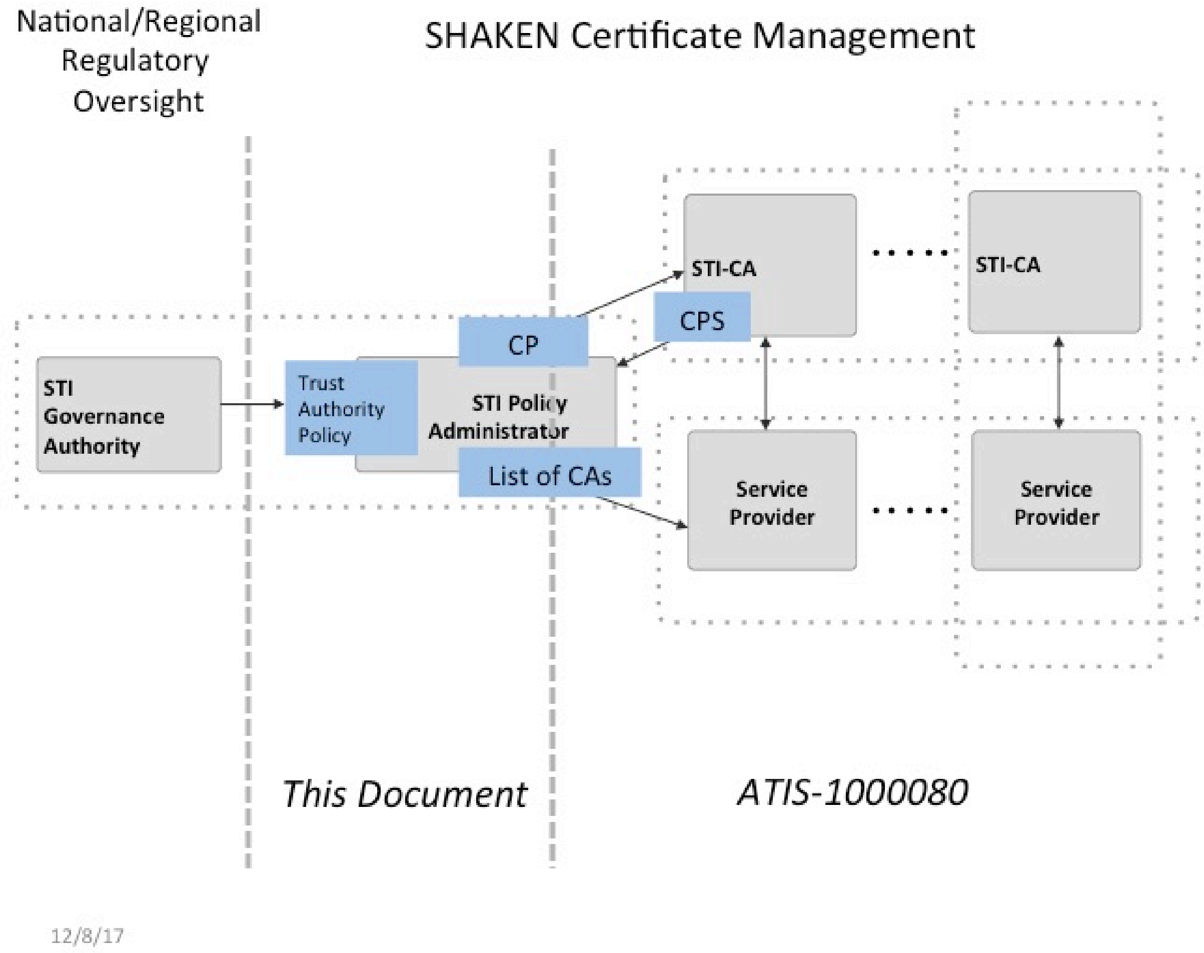

Figure 4.1 – Governance Model for Certificate Management

Clause 5 of this document describes a Trust Authority Policy that establishes the relationship between the STI Governance Authority (STI-GA) and the STI-PA's operational responsibilities.

In the context of SHAKEN, the approval of STI-CAs follows standard PKI practices, as outlined in RFC 3647, including the definition of Certificate Policies as described in clause 6. The STI-PA defines a CP and the STI-CAs provide a CPS describing their adherence to the CP during the approval process.

Details on the management of the list of STI-CAs are provided in clause 7 and the management of the authorized Service Providers in clause 8.

5 STI-PA as Trust Authority

As described in ATIS-1000080, the STI-GA is responsible for:

- Establishing policies governing which entities can manage the PKI and issue STI certificates.
- Defining the policies and procedures governing which entities can acquire STI certificates.

The STI-PA applies and enforces any policies established by the STI-GA in its 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 which each establish their own PKI for issuing certificates, per the following diagram:

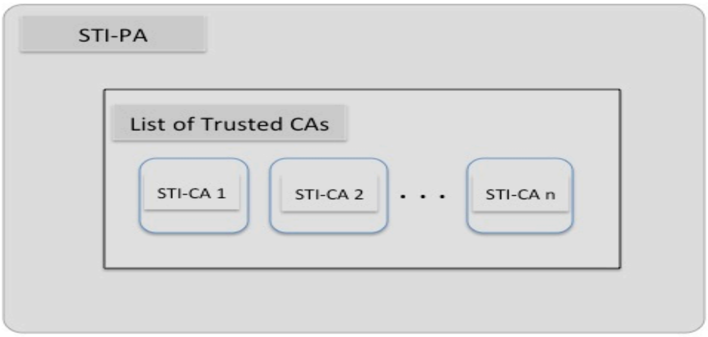

Figure 5.1 – Trust Model

Each of the STI-CAs operates its own Root CA and PKI infrastructure similar to following diagram:

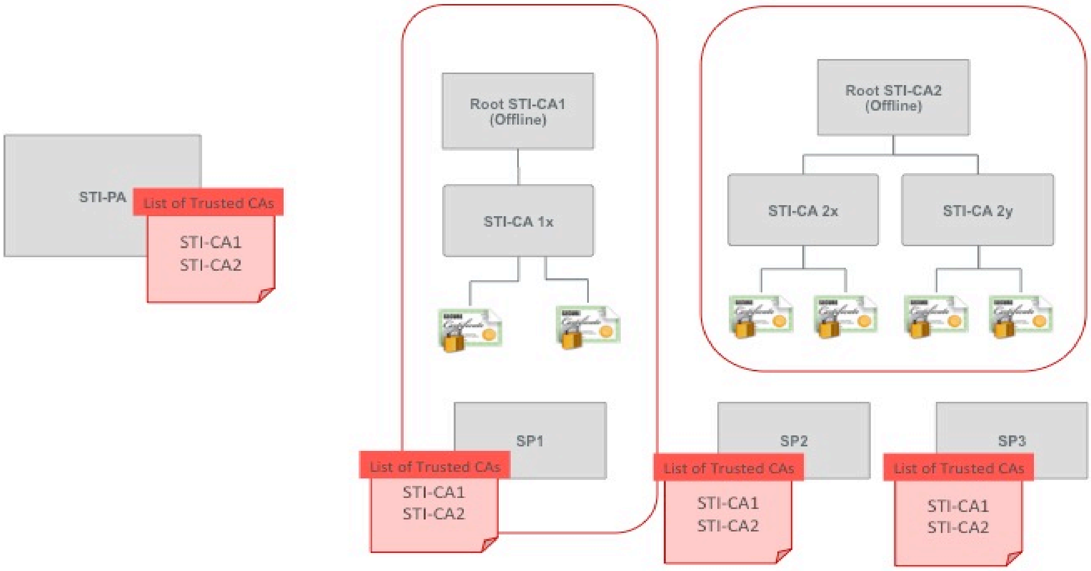

Figure 5.2 – PKI Model

In a multi-stakeholder PKI model, typically a Policy Management Authority (PMA) is established, comprising a set of people responsible for ensuring that the established policies are being adhered to. The set is typically comprised of the stakeholders (e.g., service providers in the case of SHAKEN).

The PMA defines a CP to be supported by the approved STI-CAs. The STI-CAs provide a CPS describing their adherence to the CP during the approval process. An outline of the CP to be supported by the STI-CAs is provided in clause 6.1.

The STI-PA defines 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.
- An STI-PA may remove an STI-CA from the list of trusted STI-CAs based on specific criteria such as a failure to comply with the CP established by the STI-PA or other criteria as defined by the STI-GA. Typically, compliance is audited by the PMA and thus guidelines must be established for the timeframe in which an identified problem must be resolved.
- Other policies established by the STI-GA for operation of the STI-PA.

Beyond the role of managing the list of trusted STI-CAs, the STI-PA also serves as a Trust Anchor to the relying parties in the PKI by providing service providers with the Service Provider Code Token that is used by the STI-CA in determining whether the Service Provider requesting issuance of certificates is authorized.

In the context of SHAKEN, whether an entity is authorized to acquire STI certificates is based on the Service Provider being assigned a service provider code by a Regulatory and/or administrative entity. Per ATIS-1000080, the STI-GA can define other policies and procedures governing which entities can acquire STI Certificates.

The following diagram summarizes the roles and responsibilities associated with the STI-PA, including the interfaces to other functional elements:

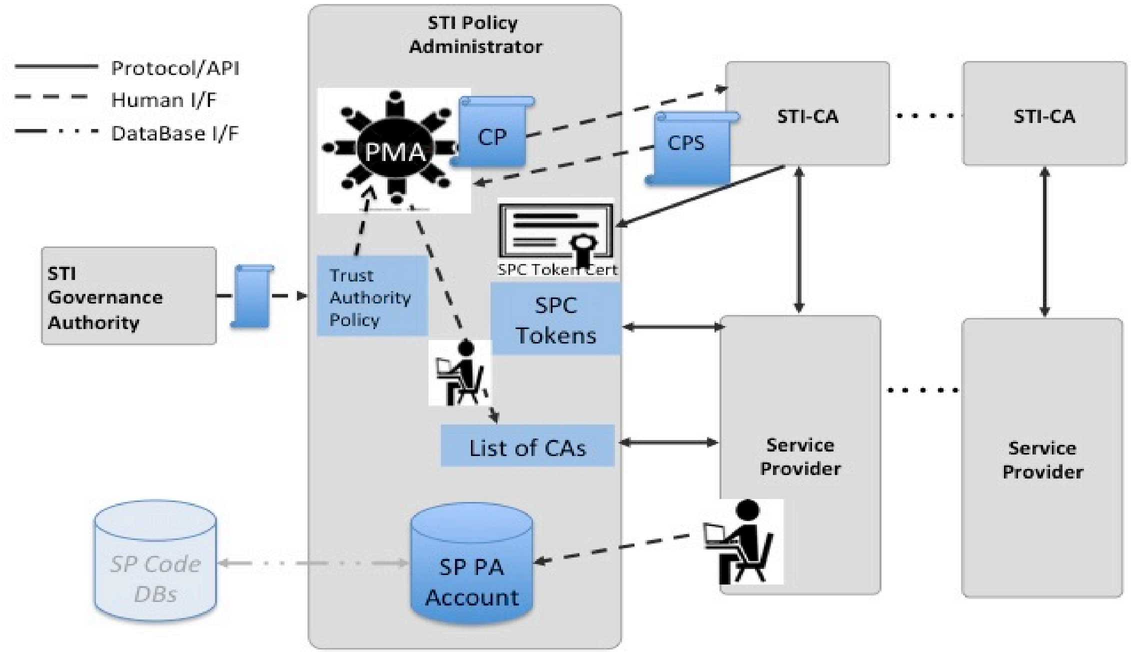

Figure 5.3 – STI-PA Roles and Functional Interfaces

6 Certificate Policy & Certification Practice Statements

The STI-PA defines a CP that prescribes the policies to be followed by an STI-CA within the SHAKEN framework. Within the SHAKEN framework, the STI-PA imposes some of these policies based on its role as the Trust Authority. The STI-CAs shall produce Certification Practice Statements defining the manner in which they abide by the Certificate Policy, aligning with their role as a CA issuing STI certificates.

6.1 Certificate Policy

A CP provides a set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [RFC 3647]. It contains the business, legal, and technical requirements for certificate approval, management, use, revocation, and renewal.

The following reference documents provide additional information about writing the CP and CPS:

- NIST SP 800-57, *Recommendation for Key Management*[3]
  - Part 1 Revision 4: *General*
  - Part 2: *Best Practices for Key Management Organization*
  - Part 3 Revision 1: *Application-Specific Key Management Guidance*, section 2 on PKI.
- FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*[3].

The CP contains policies for the STI-PA, STI-CA, STI-CR, subscribers, and relying parties. RFC 3647 contains the following outline for the contents of the Certificate Policy. The STI-PA shall address the following 9 topics:

1. Introduction
2. Publication and Repository
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile
8. Compliance audit
9. Other Business and Legal Matters.

6.1.1 Introduction

This component of the CP provides the set of provisions, and the entities and application (SHAKEN) for which the CP is targeted.

6.1.1.1 Overview

The CP shall provide an overview of the relationship between the CP and CPS, and the target audience. This section shall include the following statement: "This CP conforms to *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [Internet Engineering Task Force (IETF) RFC 3647]."

6.1.1.2 Document Name and Identification

The CP shall provide an official title. The CP shall identify certificate policies, levels of assurance, and object identifier (OID) values that will be included in certificates issued by the STI-CAs. The CP shall contain the TNAuthList OID as defined in RFC 8226.

6.1.1.3 PKI Participants

The CP provides information on the PKI participants. This shall include Certification Authorities, Registration Authorities, Subscribers, and Relying Parties. The Root CA is recommended to be an offline CA that only issues

[3] This document is available from the National Institute of Standards and Technology (NIST). < https://www.nist.gov >.

certificates to intermediate CAs. In the context of SHAKEN, service providers are the subscribers and relying parties.

6.1.1.4 Certificate Usage

The CP shall include the appropriate certificate uses and prohibited certificate uses. The CP shall specify that the certificates are used for SHAKEN.

6.1.1.5 Policy Administration

The STI-PA administers the CP. The CP shall provide contact information for STI-CAs writing their CPSs. The CP shall include additional information for reviewing the CPS compliance with the CP. The CP shall document the CP approval procedures.

6.1.1.6 Definitions and Acronyms

The CP shall include the definitions and acronyms used in the CP. This section can also reference an appendix with the information.

6.1.2 Publication and Repository Responsibilities

The CP shall include information on the certificate repositories. It shall include information on the entity that operates the STI-CR and its responsibility to publish practices, certificates, and certificate status. The CP shall include the frequency of publication and access controls.

6.1.3 Identification and Authentication

The CP shall describe the procedures used to authenticate the identity and/or other attributes of a certificate applicant prior to issuing the certificate. This shall include whether the CA supports the Automated Certificate Management Environment (ACME) protocol, as well as the ACME extension for token authorization using the Service Provider Code as described in ATIS-1000080 and [draft-ietf-acme-service-provider].

6.1.3.1 Naming

The CP shall provide information on the naming standards used in the certificates. Naming conventions used shall be standardized to avoid collisions. The Subject name in STI-CA root Certificates shall match the Issuer name as required by RFC 5280. The Issuer name in the STI certificates shall match the Subject name of the Issuing CA certificate.

6.1.3.2 Initial Identity Validation

The CP shall include the procedures required for identification and authentication for the initial registration of certificates.

6.1.3.3 Identification and Authentication for Re-key Requests

The CP shall include the procedures required for identification and authentication for re-key requests. In the context of SHAKEN, a re-key request shall require issuance of a new Certificate.

6.1.3.4 Identification and Authentication for Revocation Requests

The CP shall include the procedures required for identification and authentication for revocation requests. In the context of SHAKEN, certificate re-key requests after revocation shall follow the same process as initial Certificate issuance.

6.1.4 Certificate Life-Cycle Operational Requirements.

This component of the CP specifies requirements imposed upon issuing CAs, subject CAs, and subscribers with respect to the life-cycle of a certificate.

6.1.4.1 Certificate Application

The CP shall provide information on who can submit a certificate application and the enrollment process. The CP shall specify that the only entities to apply for certificates are valid Service Providers and certificates are not issued if an entity does not have a valid Service Provide Code token.

6.1.4.2 Certificate Application Processing

The CP shall describe the procedure for processing certificate applications.

6.1.4.3 Certificate Issuance

The CP shall include information on actions performed by the STI-CA during the issuance of the certificate and notification mechanisms.

6.1.4.4 Certificate Acceptance

The CP shall document the process for an applicant accepting a certificate, publication of the certificate by the STI-CA, and notification of certificate issuance to other entities.

6.1.4.5 Key Pair and Certificate Usage

The CP shall provide responsibilities for the use of keys and certificates. This includes subscriber's responsibilities for using the private key and the relying party responsibilities for using the public key and certificate.

6.1.4.6 Certificate Renewal

The CP shall document the process for renewing a certificate.

6.1.4.7 Certificate Re-key

The CP shall document the process for issuing a new certificate with a new public key.

6.1.4.8 Certificate Modification

The CP shall document the process for modifying certificate information, using the existing public key.

6.1.4.9 Certificate Revocation and Suspension

The CP shall document the policy for certificate revocation and suspension. The CP shall include information on reasons for certificate revocation, who can request certificate revocation, procedures for revoking the certificate, publishing certificate revocation, and mechanisms a relying party uses to check for certificate revocation. The required mechanism shall align with the Certificate Lifecycle Management procedures described in ATIS-1000080.

6.1.4.10 Certificate Status Services

The CP shall provide information on the certificate status services supported and availability of the services.

6.1.4.11 End of Subscription

The CP shall document the process for a subscriber to end the subscription services of the STI-CA.

6.1.4.12 Key Escrow and Recovery

The CP shall document the policies and practices of key escrow of the subject’s private key by the STI-CA and the recovery process used by the subscriber.

6.1.5 Facility, Management, and Operational Controls

The CP shall describe the non-technical security controls used by the STI-CA for key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving. The CP shall define the non-technical security controls on the STI-CR, STI-CAs, subscribers, and other participants.

6.1.5.1 Physical Security Controls

The CP shall describe the physical security controls on the facilities housing the STI-PA, STI-CA, and STI-CR systems.

6.1.5.2 Procedural Controls

The CP shall provide information on the trusted roles (e.g., system administrator). For each role, the CP shall provide the responsibilities, and identification and authentication requirements. The CP shall include separation of duties and the number of individuals required to perform a task.

6.1.5.3 Personnel Security Controls

The CP shall provide the policies related to personnel that perform trusted roles in the STI-PA and STI-CA. This includes qualifications, experience, background checks, clearances, training, and auditing.

6.1.5.4 Audit Logging Procedures

The CP shall provide the policies related to event logging and audit systems. The CP shall include the types of events recorded, the frequency the audit logs are processed, protection of the audit log files, and vulnerability assessments.

6.1.5.5 Records Archival

The CP shall document the requirements for records archival, including the types of records that are archived, retention period, time-stamping, backup, and protection.

6.1.5.6 Key Changeover

The CP shall document the procedure to provide a new STI-CA public key to users following a re-key by the STI-CA.

6.1.5.7 Compromise and Disaster Recovery

The CP shall provide the requirements for notification and recovery procedures in the event of compromise or disaster.

6.1.5.8 CA Termination

The CP shall document the requirements for termination of a STI-CA.

6.1.6 Technical Security Controls

The document *Security Requirements for Cryptographic Modules* [FIPS PUB 140-2] provides technical information needed for this section.

6.1.6.1 Key Pair Generation and Installation

The CP shall provide the requirements for key pair generation and installation for the STI-CA and subscribers.

6.1.6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CP shall document the requirements for private key protection and the use of cryptographic modules for STI-CAs and subscribers.

6.1.6.3 Other Aspects of Key Pair Management

The CP shall document other aspects of key pair management include public key archival and operational period of the certificates issued to the subscriber.

6.1.6.4 Activation Data

The CP shall provide the policies for protecting the activation data required to operate private keys or cryptographic modules containing private keys.

6.1.6.5 Computer Security Controls

The CP shall describe computer security controls used, including access control, audit, identification, authentication, trusted path, security testing, and penetration testing.

6.1.6.6 Life Cycle Security Controls

The CP shall describe the security controls for system development, including development environment, configuration management, software engineering practices, and software development methodology. The CP shall describe security management controls, including the tools and procedures.

6.1.6.7 Network Security Controls

The CP shall document network security controls, including firewalls.

6.1.6.8 Time-Stamping

The CP shall address the requirements for the use of timestamps. System clocks used for time-stamping shall be maintained in synchrony with an authoritative time standard – e.g., through the use of Network Time Protocol (NTP) [RFC 5905].

6.1.7 Certificate Profile and Lifecycle Management

The CP shall provide a profile of the certificates that are issued along with the lifecyle management of the issued certificates.

6.1.7.1 Certificate Profile

Certificates issued by the STI-CA shall adhere to the X.509 v3 certificate profile, documented in RFC 5280. The CP shall provide information on the certificate profile(s), including certificate extensions, algorithm object identifiers, and name constraints.

6.1.7.2 Certificate Lifecycle Management

The CP shall provide a description of the mechanism for lifecycle management. Given the SHAKEN Certificate Management architecture, the use of Certificate Revocation Lists (CRLs) or OCSP would require additional specification to support the Trust model. The lifecycle management shall be determined by the certificate lifetime.

6.1.8 Compliance Audit and Other Assessment

The CP shall provide information on compliance audits, including methodology, frequency, personnel qualifications, independence of assessor, and who is entitled to see assessment results.

6.1.9 Other Business and Legal Matters

The CP should include the details for the following business and legal aspects:

1. Financial Responsibility
2. Confidentiality of Business Information
3. Privacy of Personal Information
4. Intellectual Property Rights
5. Representations and Warranties
6. Disclaimers of Warranties
7. Limitations of Liability
8. Indemnities
9. Term and Termination
10. Individual notices and communications with participants
11. Amendments
12. Dispute Resolution Procedures
13. Governing Law
14. Compliance with Applicable Law
15. Miscellaneous Provisions
16. Other Provisions.

It is important that this section is written and/or reviewed by the legal department of the STI-PA for the CP and the STI-CA for the CPS.

6.2 Certification Practice Statement

The CPS contains the practices a CA follows when issuing digital certificates. It provides detailed information on how the policy requirements documented in the CP are implemented for the CA.

The CPS is written by the STI-CA. To ensure the Certificate Policy requirements are followed, the CPS shall use the same format as the CP. RFC 3647 contains the recommended contents of a CP and CPS, which is shown in clause 6.1. The following clauses would differ from the CP.

6.2.1 Introduction

The introduction shall provide information on the CPS, instead of the CP.

6.2.2 Policy Administration

The CPS shall include the CPS approval procedures, instead of CP approval procedures.

7 Managing List of STI-CAs

Per the SHAKEN Governance and Certificate Management Framework, the STI-PA shall manage a list of valid CAs. This list shall be distributed to each of the Service Providers for use in verifying that the STI-CA that issued the certificate has been authorized by the STI-PA.

Managing the list of STI-CAs introduces an additional interface from the STI-PA to the STI-VS in the terminating Service Provider’s network:

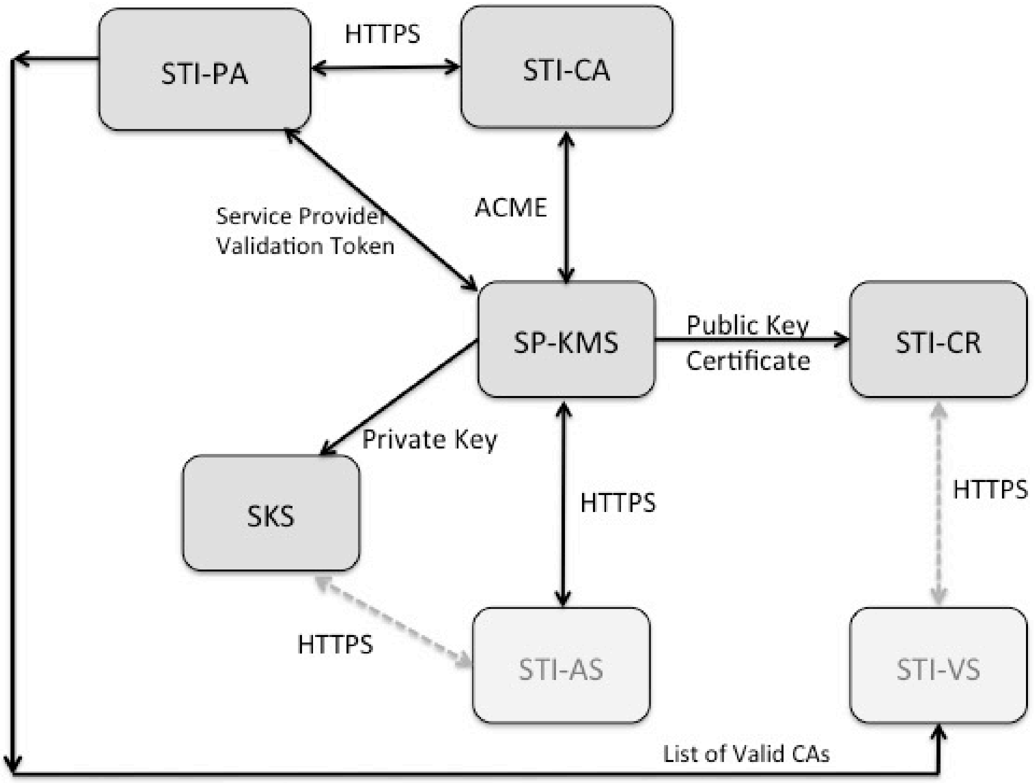

Figure 7.1 – SHAKEN Certificate Management Architecture

The STI-PA is responsible for the following 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 Certification Practice Statement of the STI-CA to determine that the PKI in which it resides is operated to an acceptable level of assurance
- Ensuring that the policies as identified in clause 6 are supported
- Determining that the STI-CA/PKI provides a warranty with regards to the issued certificates.
- Any other criteria that may be specified by the STI-GA.

7.1 Distributing Trusted STI-CA List

This document recommends the use of an API over HTTPS [RFC 7231] for the distribution of the list of trusted STI-CAs. Clause 7.2 provides details on the format and contents of the STI-CA list in the form of a JSON Web Token (JWT) [RFC 7519].

7.2 Format of STI-CA List

The STI-CA list shall contain 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.
- extensions (optional, string).

The following provides an example, noting that the trustList is not shown in the encoded form for the purposes of the example:

```
 GET /sti-pa/ca-list HTTP/1.1
 HOST: sti-pa.com

 HTTP/1.1 200 OK
 Content-Type: application/jose+json
{
 "protected": base64url({
     "alg": "ES256",
     "typ": "JWT",
     "x5u": " https://sti-pa.com/sti-pa/cert.crt"
     })
 "payload": base64url({
      "version": 1.0,
      "sequence": 1,
      "exp": 1300819380,

       "trustList": [
.      "-----BEGIN CERTIFICATE-----
        STI-CA 1 Root certificate contents
         -----END CERTIFICATE-----",
        "-----BEGIN CERTIFICATE-----
        STI-CA 2 Root certificate contents
         -----END CERTIFICATE-----",
        "-----BEGIN CERTIFICATE-----
         STI-CA 3 Root certificate contents
        -----END CERTIFICATE-----
     ],
    }) "signature": "RZPOnYoPs1PhjszF...-nh6X1qtOFPB519I"
```

Note that the contents of each of the Root Certificates would appear in a form like the following:

```
"MIIDQjCCAiqgAwIBAgIGATz/FuLiMA0GCSqGSIb3DQEBBQUAMGIxCzAJB
 gNVBAYTAlVTMQswCQYDVQQIEwJDTzEPMA0GA1UEBxMGRGVudmVyMRwwGgYD
 VQQKExNQaW5nIElkZW50aXR5IENvcnAuMRcwFQYDVQQDEw5CcmlhbiBDYW1
 wYmVsbDAeFw0xMzAyMjEyMzI5MTVaFw0xODA4MTQyMjI5MTVaMGIxCzAJBg
 NVBAYTAlVTMQswCQYDVQQIEwJDTzEPMA0GA1UEBxMGRGVudmVyMRwwGgYDV
 QQKExNQaW5nIElkZW50aXR5IENvcnAuMRcwFQYDVQQDEw5CcmlhbiBDYW1w
 YmVsbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAL64zn8/QnH
 YMeZ0LncoXaEde1fiLm1jHjmQsF/449IYALM9if6amFtPDy2yvz3YlRij66
 s5gyLCyO7ANuVRJx1NbgizcAblIgjtdf/u3WG7K+IiZhtELto/A7Fck9Ws6
 SQvzRvOE8uSirYbgmj6He4iO8NCyvaK0jIQRMMGQwsU1quGmFgHIXPLfnpn
 fajr1rVTAwtgV5LEZ4Iel+W1GC8ugMhyr4/p1MtcIM42EA8BzE6ZQqC7VPq
 PvEjZ2dbZkaBhPbiZAS3YeYBRDWm1p1OZtWamT3cEvqqPpnjL1XyW+oyVVk
 aZdklLQp2Btgt9qr21m42f4wTw+Xrp6rCKNb0CAwEAATANBgkqhkiG9w0BA
 QUFAAOCAQEAh8zGlfSlcI0o3rYDPBB07aXNswb4ECNIKG0CETTUxmXl9KUL
 +9gGlqCz5iWLOgWsnrcKcY0vXPG9J1r9AqBNTqNgHq2G03X09266X5CpOe1
 zFo+Owb1zxtp3PehFdfQJ610CDLEaS9V9Rqp17hCyybEpOGVwe8fnk+fbEL
 2Bo3UPGrpsHzUoaGpDftmWssZkhpBJKVMJyf/RuP2SmmaIzmnw9JiSlYhzo
 4tpzd5rFXhjRbg4zW9C+2qok+2+qDM1iJ684gPHMIY8aLWrdgQTxkumGmT
gawR+N5MDtdPTEQ0XfIBc2cJEUyMTY5MPvACWpkA6SdS4xSvdXK3IVfOWA=="
```

Upon receipt of the STI-CA list, the SP shall ensure that the certificate accessed via the URL in the x5u field validates as the STI-PA's root certificate. Note, that the SP shall receive the root certificate for the STI-PA via an out of band mechanism prior to account registration, in a manner similar to that used to provide the client credentials for account registration as described in ATIS-1000080.

7.3 Lifecycle of Trusted STI-CA List

This clause discusses considerations and management of the lifecycle of the STI-CA list. In order to allow a Service Provider to determine the validity of an issued certificate, it is important that the list of valid STI-CAs is updated on a regular basis (e.g., daily). Criteria by which a STI-CA would be removed from the Trust List are described in clause 5 and are subject to policy considerations. In the case that an STI-CA is to be removed from the list, in order to minimize the timeframe during which certificates issued by that STI-CA are being used for active calls, it is recommended that the STI-PA send an updated list to the Service Providers. In addition, it is recommended that the expiry of certificates be a shorter interval than the frequency at which an updated Trust List is distributed in order to reduce the number of active calls that might be using a certificate issued by an STI-CA that has been removed from the list.

8 STI-PA Administration of Service Providers

The STI-PA shall maintain a list of valid Service Providers, who hold tokens, as represented by Service Provider Codes. The assignment of Service Provider Codes is outside the scope of this document. The assumption is that the STI-GA indicates the entity that should be the source for these identifiers. The STI-PA defines a mechanism to periodically validate/renew the Service Provider Codes in this list.

The trust model for SHAKEN defines the STI-PA as the Trust Anchor for the token-based mechanism for validation of Service Providers within a national/regional administrative domain. Per the SHAKEN Governance model and certificate management framework [ATIS-1000080], the STI-PA issues Service Provider Code tokens to Service Providers. The STI-PA shall also provide guidelines for the renewal and revocation of Service Provider Code tokens.