**ATIS-0x0000x**

ATIS Standard on

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

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This document provides an overview of 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 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 Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

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 a 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, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope & Purpose

## Scope

This technical report introduces operational and management considerations for STI-CAs within the context of the SHAKEN framework [ATIS-1000074] and the SHAKEN: Governance Model and Certificate Management framework [ATIS-0x0000x]. This document focuses on the operational and management aspects that impact the authentication and verification services, as well as general CA practices and policies. This document does not address the policy aspects applied by the STI-PA in determining whether a CA is qualified to serve as an STI-CA.

## Purpose

The SHAKEN Governance Model and Certificate Management framework introduces a model whereby the STI-PA maintains a list of valid STI-CAs. This list is distributed to Service Providers so that they can select a valid STI-CA when requesting issuance of certificates. The list is also used by the Service Provider 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 also provides considerations for PKI Certificate Practice Statement (CPS) and Certificate Policy (CP) documents.

# 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.

ATIS-1000074 *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*

ATIS-0300251.2007 (R2012) *Codes for Identification of Service Providers for Information Exchange*

draft-ietf-stir-passport

draft-ietf-stir-rfc4474bis

draft-ietf-stir-certificates

IETF RFC 5280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

draft-ietf-acme-acme *Automatic Certificate Management Environment (ACME)*

RFC 2986 *PKCS #10: Certification Request Syntax Specification Version 1.7*

RFC 3261 *SIP: Session Initiation Protocol*

RFC 3966 *The tel URI for Telephone Numbers*

RFC 4949 *Internet Security Glossary, Version 2*

RFC 5246 *The Transport Layer Security (TLS) Protocol Version 1.2*

RFC 5958 *Assymetric Key Package*

RFC 6749 *The OAuth 2.0 Authorization Framework*

RFC 6960 *Online Certificate Status Protocol (OSCP)*

RFC 7159 *The JavaScript Object Notation (JSON)*

RFC 7231 *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”*

RFC 7375 *Secure Telephone Identity Threat Model*

RFC 7515 *JSON Web Signatures (JWS)*

RFC 7516 *JSON Web Algorithms (JWA)*

RFC 7517 *JSON Web Key (JWK)*

RFC 7519 *JSON Web Token (JWT)*

# Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

## Definitions

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

**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]

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

**Certificate Chain**:See Certification Path.

**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 Certification Path or Certificate Chain. [RFC 4949].

**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.

**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. [draft-ietf-stir-4474bis]

**National/Regional Regulatory Authority (NRAA)**: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).

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

**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]

**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 aCompany 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]

**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]

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

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ACME | Automated Certificate Management Environment (Protocol) |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CA | Certification Authority |
| CORS | Cross-Origin Resource Sharing |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DN | Distinguished Name |
| DNS | Domain Name System |
| HTTPS | Hypertext Transfer Protocol Secure |
| IETF | [Internet Engineering Task Force](http://www.ietf.org/rfc.html) |
| JSON | JavaScript Object Notation |
| JWA | JSON Web Algorithms |
| JWK | JSON Web Key |
| JWS | JSON Web Signature |
| JWT | JSON Web Token |
| NECA | National Exchange Carrier Association |
| NNI | Network-to-Network Interface |
| NRAA | National/Regional Regulatory Authority |
| OAuth | Open Authentication (Protocol) |
| OCN | Operating Company Number |
| OCSP | Online Certificate Status Protocol |
| PASSporT | Personal Assertion Token |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure for X.509 Certificates |
| PSTN | Public Switched Telephone Network |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP  REST | Session Initiation Protocol  Representational state transfer (REST) |
| SKS | Secure Key Store |
| SMI | Structure of Management Information |
| SP | Service Provider |
| RSP-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 |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| URI | Uniform Resource Identifier |
| VoIP | Voice over Internet Protocol |

# Overview

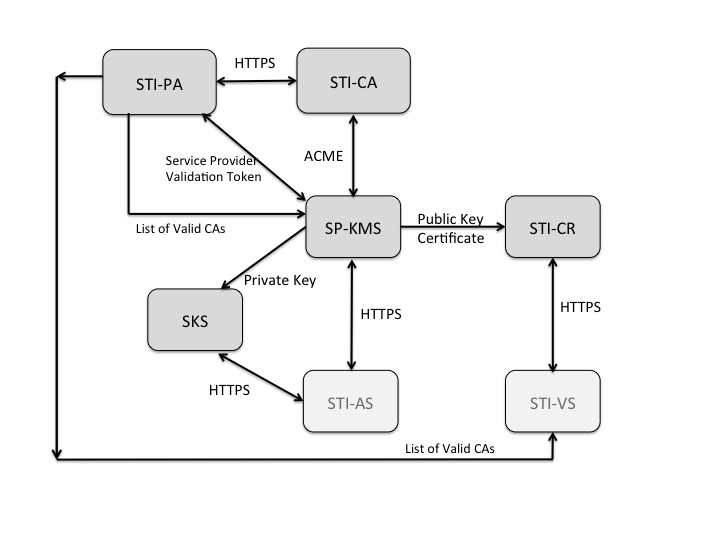
The governance model in [ATIS-0x0000x] introduces an STI-Policy Administrator that bridges the governance aspects of STI with the protocol requirements to support PKI [RFC 5280] certificates which are used by the SHAKEN framework [ATIS-1000074] to authenticate and verify telephone identities. Per the governance model and certificate management framework, the STI-PA must maintain a list of valid STI-CAs to be provided to the Authentication and Verification services.



Figure 1: Governance Model for Certificate Management

# Managing List of STI-CAs

Managing the list of STI-CAs introduces an additional interface from the STI-PA to the STI-AS & STI-VS:



[Editor’s note: the following items need to be addressed and further specified.

1. Details of what is stored in the List of Valid CAs (e.g., Domain Name, etc.)
2. Reasons a CA would be removed from the list.
3. Details as to how a CA is removed from the list.
4. Interface that is used to distribute the list – assuming API over HTTPS.
5. How frequently is the list distributed?

# Operational Considerations

[Editor’s note: this is a placeholder for items that should be considered/documented]

1. Standardize server naming and CA naming.
2. Recommendation to NOT use online Root CAs. Offline CAs should be placed in a secure vault until a new certificate or CRL needs to be issued and published.
3. Provide a way to specify extensions to be supported.
4. Recommendation to support OCSP [Editor’s note: this was removed from IETF STIR documents to get them through the process].
5. Use a Key Recovery Agent and Data Recovery agent to recover important data balancing with the importance of keeping this secure.
6. Make sure system time on CA is properly set (e.g., use NTP)