**A****TIS-0x0000x**

ATIS Standard on

**Signature-based Handling of Asserted Information Using Tokens (SHAKEN): Governance Model and Certificate Management**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

Signature-based Handling of Asserted information using Tokens (SHAKEN) is an industry framework for managing and deploying Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and verification of the telephone identity and other information in an IP-based service provider voice network. This specification expands the SHAKEN framework, introducing a governance model and defining the X.509 certificate management procedures. Certificate management provides mechanisms for validation of the certificate and verification of the signature, allowing for the identification of illegitimate use of national telecommunications infrastructure.

**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 an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [**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** |
| --- | --- | --- | --- |
| October 4, 2016 | 0.1 | Initial Draft | Mary Barnes |
|  | 0.2 | Baseline Draft |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope & Purpose

## Scope

This document expands the SHAKEN framework, defining a Governance model and certificate management procedures for Secure Telephone Identity (STI) technologies.

## Purpose

This document introduces a Governance model and certificate management procedures to the SHAKEN framework [ATIS-1000074]. The Governance model defines recommended roles and relationships, such that the determination of who is authorized to administer certificates for VoIP networks can be established. This model allows for the application of specific regulatory requirements independent of the mechanisms for certificate management. The certificate management is based on the definition of roles similar to those defined in “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, IETF RFC 5280. Per the SHAKEN framework, the certificates themselves are based on X.509 with specific policy extensions. The objective of this document is to provide recommendations and requirements for implementing the protocol specifications to support certificate management for the SHAKEN framework.

# 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)*

draft-ietf-stir-passport

draft-ietf-stir-rfc4474bis

draft-ietf-stir-certificates

IETF RFC 1422 - *Part II: Certificate-Based Key Management*

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

RFC 5958 *Assymetric Key Package*

RFC 6960 *Online Certificate Status Protocol (OSCP)*

# 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

**Caller ID**: the originating or calling parties telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields.

**Telephone Number Certificate Repository (TN-CR):** This term is used in ATIS-1000074 and is synonymous with the term Secure Telephone Identity Certificate Repository (STI-CR) used in this document.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |
| NNI | Network-to-Network Interface |
| PSTN | Public Switched Telephone Network |
| STI | Secure Telephone Identity |
| VoIP | Voice over Internet Protocol |

# Overview

This document defines a Governance model and Certificate Management procedures for the SHAKEN framework. SHAKEN is defined as a framework that utilizes protocols defined in the IETF STIR working group (WG) that work together in an end-to-end architecture for the authentication and assertion of a telephone identity by an originating service provider and the verification of the telephone identity by the terminating service provider.

## SHAKEN Architecture

The following diagram is reproduced from ATIS-1000074:



Figure : SHAKEN Architecture

This document focuses on the following aspects of this architecture:

* the interface between the STI-VS and the STI-CR
* how the STI-CR is populated
* the functional realization of the “Certificate Provisioning Portal”
* the interface between the SKS and the entity that generates the private keys
* the interface between the SKS and the STI-AS

[Editor’s note: need to update the TN-CR in the diagram]

## Protocol Overview

The document draft-ietf-stir-certificates describes the use of X.509 certificates in establishing authority over a telephone number. RFC 5280 defines a model for certificate management along with the X.509 certificate format. The document draft-ietf-acme-acme defines a protocol for automatic management of certificates.

### STI Certificates

The document draft-ietf-stir-certificates describes the use of certificates in establishing authority over telephone numbers based on X.509 version 3 certificates in accordance with RFC 5280. The document details two non-exclusive approaches that can be employed to determine authority over telephone numbers with certificates. The document requires that all credential systems used by STIR explain how they address the following requirements:

 1. The URI schemes permitted in the SIP Identity header "info" parameter, as well as any special procedures required to dereference the URIs.

 2. Procedures required to extract keying material from the resources designated by the URI. Implementations perform no special procedures beyond dereferencing the "info" URI.

 3. Procedures used by the verification service to determine the scope of the credential.

 4. The cryptographic algorithms required to validate the credentials. Implementations are required to support both ECDSA with the P-256 curve [RFC4754] and RSA PKCS#1 v1.5 (see RFC3447 Section 8.2) for certificate signatures.

The document also includes additional certificate-related requirements such as certificate policies extensions.

### X.509 Public Key Infrastructure Certificate (PKIX) and Certificate revocation List (CRL) profile

RFC 5280 profiles the format and semantics of certificates and certificate revocation lists (CRLs) for the Internet Public Key Infrastructure (PKI). It also introduces an architectural model referenced by X.509 v3 (PKIX) specifications. The model consists of the following components:

* End entity: user of PKI certificates and/or end user system that is the subject of a certificate;
* CA: Certification Authority;
* RA: Registration authority, i.e., an optional system to which a CA delegates certain management functions;
* CRL issuer: a system that generates and signs CRLs; and
* Repository: a system or collection of distributed systems that stores certificates and CRLs and serves as a means of distributing these certificates and CRLs to end entities.

[Editor’s note: Add diagram]

In X.509, there are two types of CAs - a root CA and an intermediate CA. The root CA represents the Trust Anchor in a X.509 certificate. When constructing a public key certificate for general Internet usage, a certificate chain is created that represents a chain from the domain owner to the trust anchor. This generally can include the domain owner, multiple intermediate CAs and the root CA. There is also the concept of a Registration Authority to which the CA can delegate some functions (e.g., validation).

[Editor’s note: Add summary of management protocols required to support PKI and operational highlights].

### Automated Certificate Management Environment (ACME) Protocol

The Automated Certificate Management Environment (ACME) Protocol defined in draft-ietf-acme-acme allows a client to request certificate management actions using a set of JSON messages carried over HTTPS.

ACME enables the following certificate management functions:

* Account Key Registration
* Application for a Certificate
* Account Key Authorization
* Certificate Issuance
* Lifecycle Management of certificates (including Revocation)

[Editor’s note: Add more overview material based on ACME overview slides in IPNNI-2016-00080R000 presented at 11/21 virtual meeting.]

# STI Certificate Management

Management of certificates for TLS and HTTPS based transactions on the Internet is a fairly well defined and common practice for website and internet applications. Generally, there are recognized certification authorities that can "vouch" for the authenticity of a domain owner based on some out-of-band validation techniques like e-mail and unique codes in DNS.

The certificate management model for SHAKEN is based on Internet best practices for PKI to the extent possible. The model is modified where appropriate to reflect unique characteristics of the service provider based telephone network. Certificates are initially expected to take advantage of service providers’ recognized ability to legitimately assert telephone identities on a VoIP network. The fundamental requirements are identified in section 5.1.

A governance model for managing certificates is introduced in section 5.2 to support some of the unique requirements associated with how service providers manage the allocation and usage of numbers in the telephone network.. The roles and responsibilities are highlighted and the management and operational aspects of certificates are detailed in section 5.3. There is an obvious coupling between the latter and the governance model which is highlighted in those sections.

## Requirements for Certificate Management

This section details the fundamental functionality required for certificate management. An automated mechanism for certificate management is preferred and includes the following fundamental functional requirements:

1. A mechanism to determine the Certification Authority to be used to request certificates and the associated registration procedures.
2. A process to request issuance of certificates
3. A mechanism to validate the requesting Service Provider
4. A process for adding certificates to a Certificate Repository
5. A mechanism to renew/update certificates
6. A mechanism to revoke certificates

The governance, creation and management of certificates to support STI also introduce some requirements beyond typical web PKI. The original PKI model *RFC 1422* defines a hierarchy including an Internet Policy Registration Authority (IPRA) at the top level, Policy Certification Authorities (PCAs) below the IPRA and then the CAs at the 3rd level.

The existing *RFC 5280* model has no hierarchy and is a more distributed model. STI requires some hierarchy in terms of governance to ensure that those requesting certificates are valid Service Providers and that those issuing certificates are valid Certification Authorities. This is detailed in section 5.2.

In terms of certificate issuance, the primary difference between Web PKI and the requirements per STI is the procedure to validate that the entity requesting a certificate for a specific identifier is authorized to acquire certificates for the entity. Existing mechanisms for Web PKI, including the Automated Certificate Management (ACME) protocol rely on DNS or email. Section 5.5.3 describes the STI specific mechanism for validation.

## Certificate Governance: Roles and Responsibilities

The SHAKEN model for Governance of Certificate Management for Service providers to support STI is illustrated in the following diagram.



Figure : Governance Model

This diagram defines the following roles in the certificate management model:

* Governance Authority (GA)
* Secure Telephone Identity Policy Administrator (STI-PA)
* Secure Telephone Identity Certification Authority (STI-CA)
* Service Provider (SP)

The Governance Authority and the STI Policy Administrator are distinct roles in this model, though in practice both roles could be performed by a single entity. This entity is the root of trust for all STI certificates within a given area. For example, all certificates in the United States would be associated with a single root of trust, although other countries could have a different root of trust. It is also worth noting that although the STI Certification Authority and Service Provider are distinct roles, it would also be possible for a Service Provider to establish an internal STI Certification Authority for their own use.

The following sections describe these roles in more detail.

### Governance Authority

The Governance Authority is responsible for defining and modifying the policies and rules that the STI Policy Administrator will use to authorize STI-CAs and to validate Service Providers. It is anticipated that the Governance Authority would be structured as a Committee or as a Board of Directors. The criteria for membership/ participation in the Governance Authority is out of scope for SHAKEN. Note, that the role of the Governance Authority is similar to the IPRA in the *RFC 1422* model with the exception that it does not issue certificates for the Policy Certificate Authority.

### Secure Telephone Identity Policy Administrator

The STI Policy Administrator will apply the rules and policies defined by the Governance Authority to confirm that service providers are authorized to request certificates and to authorize STI certification authorities to provide the certificates.

The STI-PA functions very similar to a PCA in the *RFC 1422* model as it effectively certifies the STI-CAs and validates the Service providers. In X.509, there are two types of CAs - a root CA and an intermediate CA. The root CA represents the Trust Anchor in a X.509 certificate. When constructing a public key certificate, a certificate chain is created that represents a chain from the domain owner to the trust anchor. The STI-PA serves in the role of a root CA and trust anchor.

### Secure Telephone Identity Certification Authority

Analogous to the concept of Certification Authorities in X.509, SHAKEN defines the concept of a STI Certification Authority (STI-CA) In the X.509 model, the STI-CA serves as an intermediate CA. In the North American telephone network, it is anticipated that the number of entities that should act as STI-CAs is a relatively limited number. Certificate signing requests (CSRs) will be processed by STI-CAs and will be linked to STI-PA which is the trust anchor represented in the certificate chain.

 [Editor’s note: Look at cross signature hash.]

### Service Provider

The Service Provider obtains certificates from the STI Certification Authority. Before obtaining a certificate as described in section 5.4, a service provider must have been validated. The criteria by which a service provider is validated is outside the scope of the protocols associated with certificate management. When a service provider creates a certificate signing request, the service provider must prove that it has been validated and is eligible to receive a certificate. In the context of SHAKEN, the recommendation is that once a service provider has been validated, it will be pre-configured with a token that is used in the certificate signing request process to prove that it has been validated.

 [Editor’s note: Details of the “token” should be included here and may be subject to change depending upon the requirements of the governance authority.]

## Governance Model

This section describes the process for establishing Telephone Authorities and the criteria by which a Service Provider can obtain certificates.

Editor’s Note: the text from this section may be pulled out into a separate document in the future

### Secure Telephone Identity Certification Authority Criteria

Ultimately this is the responsibility of the Governance Authority, however, the following criteria for becoming a Secure Telephone Identity Certification Authority (STI-CA) is proposed for initial implementation:

* An STI Certification Authority MUST have the necessary certificate management expertise
* An STI Certification Authority MUST have an in-market presence (e.g., be incorporated in the U.S.)

#### Security Telephone Identity Certification Authority Approval Process

[Editor’s Note: this section will outline the process used by an STI Certification Authority to obtain approval to operate as an STI Certification Authority. The details as to how an STI-CA obtains a certificate signed by the STI Policy Administrator are detailed in section 5.4.]

### Service Provider Criteria

Ultimately this is the responsibility of the Governance Authority, but the initial criteria for obtaining Service Provider certificates will be having an OCN (Operating Company Number) as administered by the National Exchange Carrier Association. The OCN is proposed as an objective mechanism to determine that an entity is a service provider and entitled to sign calling party information. Initially there will not be a mechanism to revoke service provider certificates, although the Governance Authority will have the ability to define criteria for revoking certificates (e.g., signing invalid numbers) if it is determined to be appropriate. In addition, as a condition of being validated as a service provider for SHAKEN, service providers should commit to signing calling party information for all calls where it is technically and economically feasible.

## Certificate Management Architecture

The following figure represents the certificate management architecture for SHAKEN.



 Figure : SHAKEN Certificate Management Architecture

The SHAKEN certificate management architecture defines the following elements:

* Secure Telephone Identity Certification Authority (STI-CA) - The STI-CA that processes the Certificate Signing Request (CSR) following a service provider verification process.
* Service Provider Key Management Server (SP-KMS) - The service provider server that generates private/public key pair for signing, requests a certificate from the STI-CA, and receives the STI-CA signed public key certificate.
* Secure Key Store (SKS) - The store for private keys used by the originating service provider Authentication Service.
* Secure Telephone Identity Certificate Repository (STI-CR) - The HTTPS server that hosts the public key certificates used by destination service provider Verification Service to validate signatures.

## Certificate Management Process

This section describes two approaches for the detailed process of acquiring a public key certificate – a manual flow and an automated approach using the ACME protocol. While an automated approach is recommended, a manual approach could be useful in the initial stages of testing the STI-AS and STI-VS components of the SHAKEN framework.

### Manual CSR Flow

The flow for acquiring a signed public key certificate from a STI-CA would be as follows:

* Generate a PKCS#10 [RFC2314] Certificate Signing Request (CSR).
* Cut-and-paste the CSR into STI-CA web page.
* Prove ownership of the domain by one of the following methods:
	+ Put a TA-provided challenge at a specific place on the Authentication Service server.
	+ Put a TA-provided challenge at a DNS location corresponding to the target domain.
	+ Receive TA challenge at a (hopefully) administrator-controlled e-mail address corresponding to the domain and then respond to it on the TA’s web page.
* Telephony Authority signs public key certificate as root
* Provider downloads the issued public key certificate and stores private key certificate in Secure Key Store associated with Authentication Service and the public key certificate is stored and made publicly available via HTTPS in their Certificate Repository.

### ACME based Certificate Management Flow

ACME (draft-ietf-acme-acme) provides a more automated framework and set of protocols for acquiring a STI-CA signed public key certificate. ACME allows a client to request certificate management actions using a set of JSON messages carried over HTTPS, much like a traditional CA.

ACME enables the following certificate management functions:

* Account Key Registration
* Application for a Certificate
* Account Key Authorization (Service Provider Validation)
* Certificate Issuance
* Lifecycle Management of certificates (including Revocation)

The ACME processing flow is as follows:



The ACME client on the Service Provider Key Management Server determines the service provider domain the Authentication Service is to represent and the ACME client presents the operator with a list of STI-CAs from which it could get a certificate. The operator selects a Secure Telephone Identity Certification Authority.

1. If it has not already done so, the **ACME** client on the **SP-KMS** registers with the **STI-CA** prior to requesting a certificate per the procedures in draft-ietf-acme-acme
2. Once the **ACME** client on the **SP-KMS** has registered with the **STI-CA**, the **ACME** client can send a request for a new certificate to the **ACME** server hosted on the **STI-CA**.
3. In the context of the SHAKEN framework, the service provider that is requesting a signed certificate needs to be validated and prove ownership of the domain for which a certificate is being requested. In the SHAKEN framework, the **STI-PA** validates the service provider as described in section 5.4.3
4. Once the **STI-CA** receives the indication that the service provider is authorized, the **STI-CA** canissue the certificate.
5. In parallel with step 4, the **ACME** client starts polling for the status to determine if the service provider has been authorized to get a certificate and whether a certificate is available. Once the certificate has been issued, the **ACME** client downloads the certificate for use by the **SP-KMS**.
6. The **SP-KMS** distributes the private key to the **SKS**.
7. The **STI-AS** needs access to the URL for the public key when the Identity Header field and the “ppt” header field parameter (i.e., the PASSporT) are being added to an outgoing SIP INVITE request. Thus, the **SP-KMS** needs to notify the STI-AS that the public and private key pair is available. [The notification (via SIP MESSAGE, WEBPUSH, etc.) can include the URL for public key.]
8. The **SP-KMS** puts the public key in the **TN-CR**.

After initially retrieving the certificate, the ACME client periodically contacts the STI-CA to get updated public key certificates, CRLs, or whatever else would be required to keep the server functional and its credentials up-to-date as described in section 5.4.4

### Service Provider validation

A process is required that allows the STI-CA to validate that the service provider has the authority to manage certificates for the domain for which a certificate is being requested. In the context of ACME, the ACME client fetches the challenges after the request for a new certificate and then answers the challenges.

ACME uses an extensible challenge/response framework for identifier validation. For this initial deployment of the SHAKEN framework, it is recommended to use HTTP validation per draft-ietf-acme-acme. The ACME client proves its control over the domain by proving that it can provision resources on the Authentication Service server. The STI-CA challenges the ACME client to provide the “token” that has been configured for the service provider as described in section 5.2.2

### Certificate updates/rotation best practices

[Editor’s note: Per Sept. 28, 2016 virtual meeting, Stuart Wilson (Verizon) to submit a contribution proposing changes to this section.]

Consideration of impact of switching certificates and other certificate management impacts while there is in flight calls should be considered. Standard CRL techniques should be considered the initial preferred way of signaling the expiry of a certificate. OCSP techniques could be considered in the future.

[Editors’ note: Look at RFC 6489 (BCP 174) for how a CA performs a planned rollover.]

### Evolution of STI certificates

SHAKEN proposes starting with service provider level certificates. There are important use cases that may require telephone number level certificates including School District, Police and government agencies, where calls should be validated in order to guarantee delivery through the potential use of anti-spoofing mitigation techniques.