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

ATIS Standard on

**Signature-based Handling of Asserted Information Using Tokens (SHAKEN): Governance 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. The Governance model defines 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 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-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

draft-ietf-stir-passport

draft-ietf-stir-rfc4474bis

draft-ietf-stir-certificates

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

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

RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

RFC 4949 Internet Security Glossary, Version 2

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

RFC 5958 *Assymetric Key Package*

RFC 6712 Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)

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 ID or From header.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CMP | Certificate Management Protocol (RFC 4210) |
| CRL | Certificate Revocation List |
| HSM | Hardware Security Module |
| NNI | Network-to-Network Interface |
| PKI | Public Key Infrastructure |
| PSTN | Public Switched Telephone Network |
| STI | Secure Telephone Identity |
| VoIP | Voice over Internet Protocol |
| X.509 | ITU-T Recommendation X.509 – “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks” |

# 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 validation of the telephone identity by the terminating service provider.

## SHAKEN Architecture

The following diagram reflects the architecture as defined in the SHAKEN Framework document. .



Figure : SHAKEN Architecture

This document focuses on the following aspects of this architecture:

* the interface between the STI-VS and the TN-CR
* how the TN-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

## 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 the profile for Internet X.509 PKI certificates and CRLs. RFC 5280 also defines functions that potentially need to be supported by management protocols. RFC 4210 defines a matching X.509 PKI Certificate Management Protocol. The draft document draft-ietf-acme-acme defines a framework for automating the issuance of X.509 certificates and the relevant domain validation procedure.

### 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]

[Editor’s note: Add summary of core functionality provided by RFC 5280 – i.e., management protocols required to support PKI and operational highlights].

### Certificate Management Protocol (CMP)

The Certificate Management Protocol (CMP) defined in RFC 4210 provides a protocol for X.509v3 certificate creation and management. While there CMP messages could theoretically be communicated over any transfer means, they are commonly transferred by means of HTTP (or HTTPS) as specified in RFC 6712.

The 3GPP TS 33.310[[1]](#footnote-1) specifies CMP for network elements to obtain X.509 certificates from the operator PKI to be used for the Network Domain Security (NDS) Authentication Framework (AF).

CMP supports requests for all possible management protocol functions specified in RFC 5280, section 3.5, including e.g.:

* registration
* initialization
* certification
* key pair update
* revocation request
* cross-certification

Authentication of requests for certificate management operations is crucial to the integrity of a PKI. When communicating with the PKI (i.e. the CA or an RA), End Entities need to authenticate their messages. For CMP, message authentication is foreseen to be done by two different means:

* use of a reference and secret value communicated by secure out-of-band means
* use of X.509 certificates from the PKI comprising the CA/RA, respectively from an external identity certificate from another PKI (cf. RFC 4210, Appendix E.7)

### Automated Certificate Management Environment (ACME) Protocol

The Automated Certificate Management Environment (ACME) protocol defined in draft-ietf-acme allows a client to request certificate management actions using a set of JSON messages carried over HTTPS. In some ways, ACME functions much like a traditional CA.

ACME is used by “Let’s Encrypt”[[2]](#footnote-2), a service provided by the Internet Security Research Group (ISRG) to enable website administrators to obtain a free X.509 certificate for HTTPS (SSL/TLS).

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)

# STI Certificate Management

Management of certificates for TLS and HTTPS based transactions on the Internet is common practice for website and internet applications. Generally, there are certification authorities recognized by browser and OS vendors, which "vouch" for the binding a domain to an application based on out-of-band verification techniques like e-mail and the ability to put unique codes on DNS servers.

Domain-based authentication is subject to certain shortcomings, like e.g. the potential lack of safeguards in organizations who is able to publish something on their DNS server, or the risk of intercepted and forged emails. Therefore critical applications, like banking, require assurance of the legal entity corresponding to the requestor of an X.509 certificate. The Extended Validation Guidelines[[3]](#footnote-3) defined by the CA/Browser Forum[[4]](#footnote-4) prove to be effective and are widely accepted.

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 following sections detail the SHAKEN approach to a certificate management. A governance model for managing certificates is introduced to support some of the unique requirements associated with how service providers manage numbers in the telephone network. The roles and responsibilities are highlighted and the management and operational aspects of certificates are detailed.

## 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)
* Telephone Authority (TA) Administrator
* Telephone Authority (TA)
* Service Provider (SP)

The Governance Authority and the TA 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 Telephone Authority and Service Provider are distinct roles, it would also be possible for a Service Provider to establish an internal Telephone 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 TA Administrator will use to authorize Telephone Authorities 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.

### Telephone Authority Administrator

The TA Administrator will apply the rules and policies defined by the Governance Authority to verify service providers are authorized to request certificates and to authorize telephone authorities to provide the certificates.

### Telephone Authority (TA)

In X.509, there is the concept of Certification Authorities (CA). 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. This generally can include the domain owner, multiple intermediate CAs and the root CA.

Analogous to the concept of Certification Authorities, SHAKEN defines the concept of a Telephone Authority (TA). A Telephone Authority acts as a root certificate provider to validate authorized signatures for telephone numbers on a VoIP network.

In the North American telephone network, it is anticipated that the number of entities that should act as an authority is a relatively limited number. Certificate signing requests (CSRs) will be directly validated and processed by TAs and will be linked to TA Administrator which is the trust anchor represented in the certificate chain. Note, that this makes the SHAKEN model slightly different than the X.509 model whereby the root CA is the trust anchor.

[Editor’s note: I think that the latter statement is a hint that this model isn’t quite right. In one sense the TA Administrator is the root CA and really the TAs are just intermediate CAs or perhaps RAs. ]

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

### Service Provider

The Service Provider obtains certificates from the Telephone Authority. During the process of obtaining a certificate as described in section 5.4, a service provider’s identity and authorization is validated. The criteria by which a service provider authorization is validated is outside the scope of the protocols associated with certificate management.

The process of validating the identity of the requestor is crucial for the integrity of the SHAKEN framework. The chosen methodology must rely on a secure protocol, but also enable operators to establish secure internal processes to prohibit fraudulent certificate requests. In the context of SHAKEN, the recommendation is to provide an authorized service provider with a X.509 certificate that is used in the identity validation process for obtaining the X.509 certificates used by the STI-AS to create the STIR tokens. Using X.509 certificates for authentication, operators are enabled to diligently protect the private keys by following best industry practices, e.g. storing them on a Hardware Security Module (HSM) or alternatively on one or more protected Smart Cards with PKI functionality. Enabling the usage of the private key protected by the HSM also enables dual control by operating staff.

## 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

### Telephone Authority Criteria

Ultimately this is the responsibility of the Governance Authority, however, the following criteria for becoming a Telephone Authority is proposed:

* A TA MUST have the necessary certificate management expertise
* A TA MUST have an in-market presence (e.g., be incorporated in the U.S.)

Optional criteria could include whether a TA has had a service provider express interest in using their service

#### Telephone Authority Approval Process

[Editor’s Note: this section will outline the process used by a Telephone Authority to obtain approval to operate as a Telephone Authority. The details as to how a Telephone Authority obtains a certificate signed by the TA 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 would need to 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.

[Editor’s Note: Adjust this diagram to better show how this relates to the Governance (i.e., SP-KMS, SKS, STI-AS and STI-VS are elements associated with a Service Provider)



 Figure : SHAKEN Certificate Management Architecture

The SHAKEN certificate management architecture defines the following elements:

* Telephone Authority Management Server (TAMS) - The telephone authority server that processes the Certificate Signing Request (CSR), respectively Certification Request 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, submits to Telephone Authority Management Server, and receives the TA signed public key certificate.
* Secure Key Store (SKS) - The store for private keys used by the originating service provider Authentication Service. This could e.g. be an HSM, while Software-based implementations are possible.
* Certificate Repository (TN-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 Certificate Management 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 manual CSR flow will need to be adjusted to the requirements of the TA, and the functionality provided by the CA (respectively RA) implementation.

The flow for authorized operator staff acquiring a X.509 certificate from a telephone authority would be as follows:

* The SP-KMS triggers secure generation of key pair on the SKS (the private key never leaves the SKS)
* The SP-KMS generate a PKCS#10 [RFC2314] Certificate Signing Request (CSR), signed by the private key on the SKS.
* Cut-and-paste the CSR into Telephone Authority (TA) web page.
* Prove identity and authorization by one of the following methods:
	+ Public Key Certificate, issued by or accepted by the TA, with the private key stored on a protected Smart Card, enabled to be utilized under dual-control
	+ Username and Password, issued by the TA, preferably enabling to be managed under dual-control of the operator staff (i.e. password split in two parts)
* Telephony Authority signs public key certificate as root
* Provider downloads the issued X.509 certificate and stores private key certificate in a Secure Key Store associated with Authentication Service and the public key certificate is stored and made publicly available in their Certificate Repository.

### CMP-based Certificate Management Flow

CMP (RFC 4210) provides automated means to acquire a TA-signed X.509 certificate.

Prior to being able to request certificates from a specific TA via CMP, upon validation of eligibility and identity, an operator receives suitable credentials to authenticate CMP messages. Those credentials must be stored and managed by the operator staff following secure processes. The SKS containing the credentials would usually be activated under dual control by the operator’s authorized staff at the time the SP-KMS service is started. The credentials can be one of the following:

* an X.509 certificate corresponding to a private key in possession and under control of the operator
* a reference number and secret

The CMP flow is as following:

1. The SP-KMS triggers secure generation of key pair on the SKS (the private key never leaves the SKS)
2. The SP-KMS generates an CMP Certification Request (cf. RFC 4210, section 5.3.3), authenticates it by means of its credentials, and sends it to the TAMS
3. The TAMS validates the CMP Certification Request and verifies the identity and authorization of the requesting operator by means of the message authentication. If the verification fails, the process stops.
4. The TAMS issues the requested certificate, and sends it with a CMP response to the SP-KMS. Should issuance of the certificate be delayed e.g. due to the need for human involvement for approval, the TAMS could make use of the polling mechanisms defined by CMP (c.f. RFC 4210, section 5.3.22).
5. The SP-KMS takes the newly generated certificate into use.

The SP-KMS is repeating those steps whenever a new certificate is needed. To ensure business continuity, new certificates for critical functions are commonly requested well before prior certificates’ validity expires.

Note: Should the operator need several concurrent certificates it might be meaningful to utilize CMP Initial Registration messages (cf. RFC 4210, sections 4.2 and 5.3.1) to request creation of applicable End Entities on the CA system.

Note: Should the issuance of a certificate trigger the revocation of an earlier certificate for this particular End Entity (SP-KMS), then it might be meaningful to utilize CMP Key Update Request messages (cf. RFC 4210, section 5.3.5) to request rekeyed certificates.

If implemented by the PKI, certificate revocation could be communicated by one of the following generally used means:

* CRL distribution over CMP, HTTP, or LDAP – while HTTP and LDAP are more common
* OCSP

### ACME based Certificate Management Flow

ACME (draft-ietf-acme-acme) provides a more automated framework and set of protocols for acquiring a telephone authority 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)

Prior to being able to request certificates from a specific TA, an ACME client needs to first be registered with that TAMS per the procedures in draft-ietf-acme-acme.

The ACME flow for a telephone authority is as follows:

* The ACME client on the Service Provider Key Management Server prompts the operator for the service provider domain the Authentication Service is to represent.
* The ACME client presents the operator with a list of TAs from which it could get a certificate.
* The operator selects a TA.
* In the background, the ACME client contacts the TAMS and requests that a certificate be issued for the intended domain.
* Once the TAMS is satisfied that the requestor is authorized to manage certificates for the requested domain per section 5.4.3, the certificate is issued and the ACME client automatically downloads and installs it, potentially notifying the operator via e-mail, SMS, etc.
* The ACME client periodically contacts the TAMS 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 authorization

Means is required that allows the telephone authority to validate that the service provider has the authority to get certificates to be used on their STI-AS for SHAKEN.

CMP allows for use of a reference/secure value communicated out-of-bands or a X.509 certificate to authenticate CMP messages. Those are used by the TAMS to validate the authorization of the Service provider participating in the scheme, fulfilling the criteria as per section 5.2.2.

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 TAMS 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 in the Resource Public Key Infrastructure (RPKI) 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.

1. 3GPP TS 33.310: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2293 [↑](#footnote-ref-1)
2. Let’s Encrypt: https://letsencrypt.org [↑](#footnote-ref-2)
3. Extended Validation Guidelines: <https://cabforum.org/extended-validation-2/> [↑](#footnote-ref-3)
4. CA/Browser Forum: https://cabforum.org/ [↑](#footnote-ref-4)