**ATIS-0x0000x**

ATIS Standard on

**Signature-based Handling of Asserted Information Using Tokens**

**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 the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and validation of the telephone identity and other information in an IP-based service provider voice network. This specification defines the framework for telephone service providers to create signatures in SIP and defines the key Network-to-Network Interface (NNI) requirements, Network Elements, the X.509 certificate framework to validate the initiator of the signature, and the various classes of signers and how the validation of a signature can be used towards the mitigation and identification of illegitimate use of national telecommunications infrastructure and protecting its users.

**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** |
| --- | --- | --- | --- |
| March 24, 2016 | 0.1 | Initial Draft | Chris Wendt |
| August 24, 2016 | 0.2 |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope & Purpose

## Scope

This document is intended to provide telephone services providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on the VoIP Telephone Network.

## Purpose

Using the protocols defined in draft-ietf-stir-rfc4474bis, draft-ietf-stir-passport and draft-ietf-stir-certificate, this document will define the signature-based handling of asserted information using tokens (SHAKEN) framework. This framework is targeted at telephone service providers delivering telephone calls over VoIP, addressing the implementation and usage of STIR and the architecture and management of STIR-related certificates on VoIP networks. This includes definition of what STIR certificates represent, as well as how they should be managed and distributed. It also discusses the general architecture of service provider authentication and verification services and identifies NNI and peering impacts and dependencies. Finally, it provides guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general, and also in the context of different call origination and destination scenarios.

Illegitimate CallerID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document specifically focuses on a short term path for implementing STIR in a progressive, practical, and realistic manner, with the initial steps defined in detail and the evolution path described in broad terms. The objective is to provide an approach that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.

Editor’s Note: reconsider addressing short term path

Editor’s Note: change VoIP to IP based service provider voice network

# 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*.

IETF ????

# 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

**AAA**: xxxx.

**Bbbb**: xxxx.

## 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 presents the SHAKEN framework. SHAKEN is defined as a framework that utilizes protocols defined in IETF STIR 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.

Today, assertion of telephone identity in VoIP networks between peering service providers, particularly in a 3GPP IMS environment, typically uses the P-Asserted-ID as a network self-asserted identity. This usage assumes an inherent trust model between peering providers. However, in many telephone calling scenarios where there are many indirect call path relationships between the originating and terminating providers, these trust relationships are often simply not verifiable and do not allow for identification of the true origination of the call. In addition, P-Asserted-ID can be populated by an enterprise PBX and passed on without verification by the service provider. Secure Telephone Identity (STI) as defined in STIR and the usage of cryptographic digital signatures to verify the originator of a signed identity can provide a verifiable mechanism to identify the authorized originator of a call into the telephone network with non-repudiation and assignment of a level of assurance and a unique ID depending how are where the call is originated or received. This attestation and identifier represents the originating signers ability to vouch for the accuracy of the source of origin of the call. For example, if the service provider has an authenticated direct relationship with the origination of the call this attestation is categorized differently than calls that are originated from different networks or gateway that it may have received from unauthenticated network or unsigned. Verification of signatures will use these attestations as information to provide trace back mechanisms as well as information to feed into any call spam identification techniques it has enabled on behalf of their customer.

## STIR Overview

The documents draft-ietf-stir-rfc4474bis and draft-ietf-stir-passport define a set of protocol level tools that can be used in SIP for applying digital signatures to the CallerID or telephone number of the calling party.

### PASSporT Token

The document draft-ietf-stir-passport defines a token based signature that combines the use of JSON Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or PKI, to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The PASSporT token includes a number of "claims" the signer of the token is passing with non-repudiation. The associated public certificate is used to verify the digital signature and the “claims” included in the PASSporT token. The public certificate is also used to validate the entity that signed the token. The validated claims, and the validated identity of the entity signing the claims, can both be used to determine the level of trust in the calling party information. Call blocking applications could use this information over time to determine “reputation” of the entity signing the token, which could provide further input to determine the level of trust for the calling party information. Note that PASSporT signatures are agnostic to network signaling protocols.

### RFC4474bis

The document draft-ietf-stir-rfc4474bis defines a SIP based framework for an authentication service and verification service for using the PASSporT signature in a SIP INVITE. It defines a new "identity" header field that delivers the PASSporT signature and other associated parameters. The authentication service adds the identity header field and signature to the SIP INVITE generated by the originating provider. The INVITE is delivered to the destination provider which uses the verification service to validate the signature using the asserted identity in the P-Asserted-ID header field or FROM header field.

P-Asserted-ID must be used as the telephone identity if present, otherwise FROM header field should be used. This is true both on the Authentication side for the telephone identity verified as well as on the verification side when validation of the INVITE and identity header field occurs.

## SHAKEN Architecture

There are a number of required architectural components required for an end-to-end framework for STI.

The figure below shows the SHAKEN reference architecture. This is a logical view of the architecture and doesn’t mandate any particular deployment and/or implementation. For reference, this reference architecture is specifically based on the 3GPP IMS architecture with an IMS application server, and is only done as an example reference for discussion in this document.

 

Figure 1: SHAKEN reference architecture

This SHAKEN reference architecture includes the following elements:

* SIP UA - SIP User Agent that is authenticated by the service provider network is considered secure and the calling party identity is “known” since it is under direct management by the telephone service provider. It initiates the SIP INVITE as the calling party.
* IMS/CSCF - This component represents the SIP registrar and routing function. It also has a SIP application server interface.
* IBCF/TrGW - This function is at the edge of the service provider network and represents the NNI or peering interconnection point between telephone service providers. It is the ingress and egress point for SIP calls between providers.
* Authentication Service (STI-AS) - The SIP application server that performs the function of the authentication service defined in 4474bis. It has an HTTPS interface to the Secure Private Key Store (SKS) which stores the secret private key certificate used to create the PASSporT signature.
* Verification Service (STI-VS) - The SIP application server that performs the function of the verification service defined in 4474bis. It has an HTTPS interface to the Certificate Repository that is referenced in the identity header field to retrieve the provider public key certificate.
* Call Validation Treatment (CVT) - This is a logical function that could be an application server function or a third party application for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified and then provides a response to signal the display response for the end user.
* TN Certificate Repository – This represents the publically accessible store for public key certificates. This repository is accessed via an HTTPS interface.
* SKS – Secure Key Store is a logical place to store private keys for the authentication service to access.
* Certificate Provisioning Portal – The Certificate Authority (CA) or Telephone Authority (TA) equivalent in SHAKEN validates requests for telephony certificates and represents the mechanism the originating service provider uses to get it’s public key certificate signed via CSR.
* TN-CR: The service provider maintains and makes public certificates available in the TN-CR. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.

## SHAKEN call flow



Figure 2: SHAKEN reference call flow

1. The originating SIP UA, which first REGISTERs and is authenticated to the CSCF, creates a SIP INVITE with an E.164 calling number.
2. The CSCF of the originating provider adds a P-Asserted-Identity header field asserting the Caller ID of the originating SIP UA. The CSCF then initiates an originating trigger to the STIR-AS for the INVITE.
3. The STIR-AS in the originating SP (i.e., Service Provider A) retrieves its private key from the SKS.
4. The SKS provides the private key, and the STIR-AS signs the INVITE and adds an Identity header field per RFC 4474bis using the Caller-ID in the P-Asserted-Identity header field.
5. The STIR-AS passes the INVITE back to the SP A CSCF.
6. The originating CSCF, through standard resolution, routes the call to the egress IBCF.
7. The INVITE is routed over the NNI through the standard inter-domain routing configuration.
8. The terminating SP (Service Provider B) ingress IBCF receives the INVITE over the NNI.
9. The terminating CSCF initiates a terminating trigger to the STIR-VS for the INVITE.
10. The terminating SP STI-VS uses the “info” parameter in the Identity header field per RFC 4474bis to determine the TN-CR URI and the originating TN.
11. The STI-VS validates the certificate, which can include these steps: check the validity dates, check the certificate’s signature, check chain of trust, and check certificate validity via CRLs and/or OCSP. It then extracts the public key. It constructs the RFC 4474bis format and uses the public key to validate the signature in the Identity header field, which validates the Caller ID used when signing the INVITE on the originating service provider STIR-AS.
12. The CVT is invoked to perform call spam analytics or other mitigation techniques and return a response related to what is displayed to the user for legitimate or illegitimate call determination.
13. Depending on the result of the STI validation, the STIR-VS determines that the call is to be completed with the appropriate RFC 4474bis defined response code and the INVITE is passed back to the terminating CSCF which continues to set up the call to the terminating SIP UA.
14. The terminating SIP UA receives the INVITE and normal SIP processing of the call continues, returning “200 OK”, or optionally setting up media end-to-end.

Editor’s Note: revisit separation between signature validation and call spam evaluation

# STI Token Creation

STI as defined in draft-ietf-stir-passport specifies the process of the PASSporT token. This section provides guidance for token creation.

## PASSporT Token

PASSporT tokens have the following form:

* A protected header with the value BASE64URL(UTF(JWS Protected Header))
* A payload with the value BASE64URL(JWS Payload)
* A signature with the value BASE64URL(JWS Signature)

An example of each is as follows:

*Protected Header*

{

 "typ":"passport",

 "alg":"ES256",

 "x5u":"https://cert.example.org/passport.crt"

}

*Payload*

{

"iat":"1443208345",

 "orig":{“tn”:"12155551212"},

 "dest":{“uri”:"sip:alice@example.com"}

}

When the protected header and payload are Base64 and UTF encoded as ASCII(BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload)) the result is as follows:

eyJ0eXAiOiJwYXNzcG9ydCIsImFsZyI6IkVTMjU2IiwieDV1IjoiaHR0cHM6Ly9j

ZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNydCJ9.eyJpYXQiOiIxNDQzMjA4MzQ

1Iiwib3RuIjoiMTIxNTU1NTEyMTIiLCJkdXJpIjoic2lwOmFsaWNlQGV4YW1wbGU

uY29tIn0

The digital signature is computed using the Private Key corresponding to the certificate of the originating telephone number owner or the entity signing on their behalf.

If the following private key is used for the above example:

 -----BEGIN EC PRIVATE KEY-----

 MHcCAQEEIFeZ1R208QCvcu5GuYyMfG4W7sH4m99/7eHSDLpdYllFoAoGCCqGSM49

 AwEHoUQDQgAE8HNbQd/TmvCKwPKHkMF9fScavGeH78YTU8qLS8I5HLHSSmlATLcs

 lQMhNC/OhlWBYC626nIlo7XeebYS7Sb37g==

 -----END EC PRIVATE KEY-----

The resulting digital signature is produced:

 KK89q2RFY-BkKQQhiB0z6-fIaFUy6NDyUboKXOix9XnYLxTCjdw1UHjCbw4CefeK

 wH\_t7W-bnGlZz4pI-rMjfQ

Finally, the PASSporT token for this example is:

 eyJ0eXAiOiJwYXNzcG9ydCIsImFsZyI6IkVTMjU2IiwieDV1IjoiaHR0cHM6Ly9j

 ZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LmNydCJ9.eyJpYXQiOiIxNDQzMjA4MzQ

1Iiwib3RuIjoiMTIxNTU1NTEyMTIiLCJkdXJpIjoic2lwOmFsaWNlQGV4YW1wbGU

uY29tIn0.KK89q2RFY-BkKQQhiB0z6-fIaFUy6NDyUboKXOix9XnYLxTCjdw1UHj

Cbw4CefeKwH\_t7W-bnGlZz4pI-rMjfQ

# SIP procedures for STI

STI as defined in draft-ietf-stir-rfc4474bis specifies the format and usage of the identity header field for the SIP protocol. This section provides further clarification of usage of rfc4474bis in SHAKEN.

## 4474bis Verification procedures

Draft-ietf-stir-rfc4474bis defines authentication and verification services. If the authentication service functions correctly, and the certificate is valid and available to the verification service, the SIP message can be delivered successfully. However, if these conditions are not satisfied, errors can be generated. This section identifies important error conditions and specifies procedurally what should happen, if they occur. Error handling procedures should consider how best to always deliver the call per current regulatory requirements, while providing diagnostic information back to the signer.

There are four main procedural errors defined in rfc4474bis that can identify issues with allowing the validation of the identity header field to occur. They are:

**436** – ‘Bad-Identity-Info’ – the URI in the info parameter cannot be dereferenced (i.e., the request times out or receives a 4xx or 5xx error)

**437** – ‘Unsupported credential’ – this error occurs when a credential is supplied by the info parameter but the verifier doesn’t support it or it doesn’t contain the proper certificate chain in order to trust the credential

**438** – ‘Invalid Identity Header’ – this occurs if the signature validation fails

Two options are being discussed for how to handle these errors:

First option: The Verification Service should only send 436, 437, 438 back to originator once per originating number for a given time period (24 hours). After the 43x errors have been returned once, any subsequent calls from that originating number generating a 43x should be treated as if it were unsigned or worse.

Second option: A reason code passed in the 18x provisional response that indicates one of the four above scenerios. In addition, the provision response could be followed up by Authentication Service with a RE-INVITE in the same dialog with a “fixed” identity header field.

## Use of canon parameter

For initial SHAKEN deployment, canon must be included to avoid any potential SBC interaction with headers, especially the Date header field, which could lead to large numbers of 438, Invalid Identity Header errors.

## SIP Identity Header

Draft-ietf-stir-rfc4474bis defines the identity header field for SIP. It uses the PASSporT token as a basis for creation of the identity header field for INVITE, MESSAGE, and NOTIFY SIP messages.

The procedure is detailed in rfc4474bis, but an example of an INVITE with an identity header field is as follows:

INVITE sip:test1@siptest.comcast.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:test2@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:1000@siptest.comcast.net>
From: "Test2"<sip:5712223333@siptest.comcast.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity: lW84Z2BbPF8U4AWGg4eeKNlIYAq4j4KexICilTQJsfmEU23d2Nt7-ih1valSKqwzXYctvJqsGzs5NuqAFgrLqg;info=<https://cert-auth.poc.sys.comcast.net/example.crt>;alg=ES256;canon=eyJ0eXAiOiJwYXNzcG9ydCIsImFsZyI6IkVTMjU2IiwieDV1IjoiaHR0cHM6Ly9jZXJ0LWF1dGgucG9jLnN5cy5jb21jYXN0Lm5ldC9leGFtcGxlLmNlcnQifQ.eyJkZXN0Ijp7InVyaSI6WyJzaXA6MTAwMEBzaXB0ZXN0LmNvbWNhc3QubmV0Il19LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ1cmkiOiJzaXA6NTcxMjIyMzMzM0BzaXB0ZXN0LmNvbWNhc3QubmV0In19
Content-Length: 153
v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv

Editor’s Note: discuss NNI implications

# STI Certificate Creation

Draft-ietf-stir-certificates defines a framework for certificate creation and use in STI. This document, as discussed, will focus on the initial service provider framework for both certificate creation, usage, and management.

There is a few specific topics related to the certificate creation process important to the SHAKEN framework. To a large extent, the standard X.509 based certificate authoring applies. However, because there are different telephone service providers that support telephone service both directly to devices they manage, and also may provide telephone service on a wholesale basis to customers that either manage their own PBX like device or their own set of devices, like enterprises or call centers we will define the ability to provide a Level of Assurance indicator and Unique ID that can be embedded in the certificate at creation that will facilitate the ability to manage uniquely, but also semi-anonymously these different customer scenarios and make sure that treatment and reputation determination of both the service provider and the customers of the service provider is determined individually without any influence of one on any of the others to the extent possible.

Additionally, future work on incorporating the ability to revoke certificates using OCSP will be incorporated into this document, if it is determined that a higher level ability to invalidate certificates of bad actors is necessary.

## Certificate Attestation Policy Indication

As detailed in draft-ietf-stir-certificates, level of assurance (LOA) indicators can be included as Object Identifiers (OIDs) in the certificate’s certificate policy extension as defined in RFC5280 and used as a mechanism to represent the type of attenstation the signature is representing at the time of signing. This indication allows for both identifying the service provider that is vouching for the call as well as a potential metric used for determining confidence level of the legitimacy of the call details.

In the SHAKEN framework we will use this certificate policy indication for attestation in the following scenarios:

1. **Direct initiator** – The signer has a direct relationship with the customer and is fully attesting to the origination and caller-id used in this call.
2. **Indirect Initiator** – The signer has an indirect relationship with this call origination but can identify specifically the initiator based on customer relationship.
3. Gateway – The signer has no relationship to the initiator of the call, but is the entry point to VoIP telephone network for this call (e.g., international gateways).

There will be three SHAKEN assigned OIDs in an IANA registry that will be used globally in all certificate creation for these three scenarios. They will be of the form ‘0.0.0.0’ and will be included specifically in this document when created and available.

## Unique Origination IDs

In addition to a level of assurance, a unique origination ID is defined as part of SHAKEN. This unique origination ID should be a globally unique string corresponding to a UUID (RFC4122) that is set as the serial number attribute in the issuer field name.

The purpose of the unique origination ID is to assign an opaque unique identifier corresponding to the service provider initiated calls themselves, customers, classes of devices, or other unique groupings that a service provider should use for use in determining things like reputation or trace back identification of customers or gateways.

For Direct Initiator, in general, a single identifier will be used as part of the certificate representing direct service provider initiated calls to the telephone network. A service provider may choose to have a pool of identifiers to identify regions or classes of customers for example. Best practices will likely develop as the traceback and illegitimate call identification practices evolve.

For Indirect Initiator, a single identifier per customer is required in order to differentiate calls both for traceback and for reputation segmentation so one customers reputation doesn’t affect other customers or the service provider call reputation. A service provider may choose to be more granular (e.g., per node per customer) depending on size and classes of services that that customer offers as well.

For Gateway, best practices would be to be a granular as possible, per trunk or gateway to allow for trace back identification and reputation scoring.

Editor’s Note: revise all occurrences of level of assurance to attestation

## Certificate Examples

The likely scenario for a service provider is that it manages a pool of certificates that have the following. Certificates that have an UOID and certificate with “Direct Initiator” attestation that represents it’s direct customers, one UOID and certificate with “Indirect Initiator” attestation representing perhaps each it’s wholesale or large enterprise customers, and a UOID and certificate with “Gateway” attestation per trunk coming into it’s network.

An example service provider may have the following certificates:

Certificate A1 – LOA = Primary Holder – UOID = UUID1 – Managed devices in West Region

Certificate A2 – LOA = Primary Holder – UOID = UUID1 – Managed devices in East Region

Certificate B1 – LOA = Delegated – UOID = UUID2 – Enterprise trunking customer 1

Certficiate B2 – LOA = Delegated – UOID = UUID3 – Wholesale customer 1

Certificate C1 – LOA = Unknown – UOID = UUID4 – reserved for unknown transit calls or SS7

Editor’s Note: Needs to be updated

# STI Certificate Management

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

Certificates are initially expected to represent service providers and their recognized ability to assert telephone identities on a VoIP network. The following sections will detail the SHAKEN approach for telephone authorities that can sign certificates for use on the telephone network.

## Telephone Authority (TA)

In X.509, there is the concept of Certificate Authorities (CA). There are two flavors of CAs a root CA and 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.

As a parallel concept to Certificate Authorities, SHAKEN defines the concept of a Telephone Authority. 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. In order to promote simplicity in the management of STI certificates, the SHAKEN framework does not include the concept of intermediate telephone authorities.

This implies that service providers and the certificate signing requests (CSR) will be directly validated and processed by root TAs and there will only be service providers and root TAs as the trust anchor represented in the certificate chain.

## Certificate Management Architecture

The following figure represents the certificate management architecture for SHAKEN.



Figure 3: 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) 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 Authentication Service Application Server.
* 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

### Manual CSR Flow

Initially, it is anticipated that first deployments of SHAKEN will use current manual certificate management techniques similar to how the current interaction with Certificate Authorities works in the DNS/web world.

The flow for acquiring a signed public key certificate from a telephone authority would be as follows:

* Generate a PKCS#10 [RFC2314] Certificate Signing Request (CSR).
* Cut-and-paste the CSR into Telephone Authority (TA) 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 telephone authority signed public key certificate.

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 TA and requests that a certificate be issued for the intended domain.
* Once the TA is satisfied, 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 TA to get updated public key certificates, CRLs, or whatever else would be required to keep the server functional and its credentials up-to-date.

### Service Provider verification

A defined process that allows the telephone authority to validate the service provider requesting a signed certificate is required.

### Certificate updates/rotation best practices

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.

### 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.