**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 a VoIP-based service provider network. This specification defines the framework for telephone service providers to create signatures in SIP and will define the 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 on the PSTN toward the mitigation of illegitimate use of the PSTN and protecting users of the PSTN.

**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 |
| May 18, 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 and draft-ietf-stir-passport, this document will define the signature-based handling of asserted information using tokens (SHAKEN) framework. This framework is targeted at telephone service providers and those associated with 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 will include definition of what the STIR certificate represents as well as how they should be managed and distributed. It will also discuss the general architecture of a service provider deployment of an authentication service and verification service and any NNI and peering impacts and dependencies. Finally, it will also provide guidance on how the positive or negative verification of the signature at the terminating service provider may be used to help mitigate illegitimate telephone identity, in general, and also in the context of different call origination and destination scenarios.

Because illegitimate caller-id spoofing is large concern for North American telephone service providers and their customers and the complexity of integrating new technologies into established VoIP networks with many interoperability and interworking challenges, this document tries to specifically focus on a short term path for implementing STIR in a progressive, practical, and realistic approach. An approach that can evolve over time to incorporate more comprehensive functionality and more scope in a compatible and forward looking manner.

# 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*.

# 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 to define an end-to-end architecture for the authentication and assertion of a telephone identity on origination and the validation of the telephone identity as well as strategies for mitigation of illegitimate spoofing of telephone identities.

Today, assertion of telephone identity in VoIP networks between peering service providers particularly in a 3GPP IMS environment has typically used 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 possible or verifiable or further likely do not allow for true identification of the origination of the call. Secure Telephone Identity (STI) as defined in STIR and the usage of cryptographic digital signatures to verify the originator of a signed identity can allow for a verifiable mechanism to identify and "trust" the originator of the call. This level of trust can be absolute if the signature represents the true originator of the call but can also in some scenarios when calls are gatewayed from other networks as an example, where we may need some nuance to the interpretation of what the signed call means. This document will explore some of those scenarios to provide an additional framework for confidence in the verification of the telephone identity and further aid the mitigation techniques and tools that may be available to provide telephone customers confidence in who is calling them.

## 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 caller-id 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 tied to a certificate that can be validated to be owned by the authorized party. The PASSporT token includes a number of "claims" the signer of the token is passing with non-repudiation. The digital signature and associated certificate is used to validate who signed the token, and furthermore can also be used to verify authorized signing of the token based on a trust anchor who signed the certificate.

### 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 that delivers the PASSporT signature and other associated parameters. The authentication service adds the identity header and signature to the INVITE from 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 P-Asserted-ID header or FROM field.

## SHAKEN Architecture

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

The figure below shows the SHAKEN reference architecture.

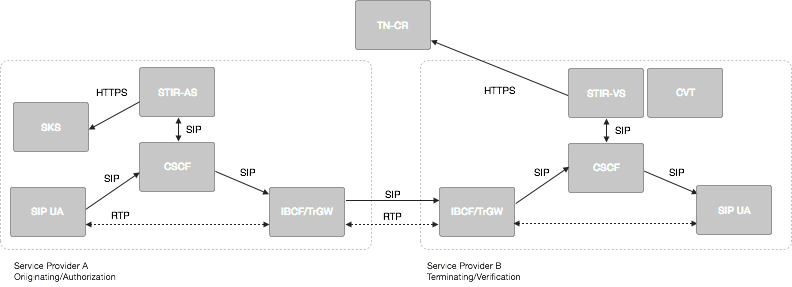


Figure 1: SHAKEN reference architecture

The SHAKEN reference architecture includes the following elements:

* SIP UA - SIP User Agent that is authenticated into the service provider network, is considered secure and 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 and is the ingress and egress point for SIP calls between providers.
* Authentication Service (STIR-AS) - The SIP application server that performs the function of the authentication service defined in 4474bis. It is associated with the Secure Private Key Store (SKS) which stores the secret private key certificate used to create the PASSporT signature.
* Verification Service (STIR-VS) - The SIP application server that performs the function of the verification service defined in 4474bis. It has an HTTP interface to the Certificate Repository that is referenced in the identity header to retrieve the provider public key certificate.
* Call ValidationTreatment (CVT) - This is a logical function that likely is an application server function for applying anti-spoofing mitigation techniques once the signature is positively or negatively verified.
* TN Certificate Repository – This represents the publically accessible store for HTTPS access to public key certificates.
* SKS – Secure Key Store a logical place to store private keys for authentication service to access. (TODO: investigate distribution of private keys through PKCS#8 objects or through CMS package defined in RFC5958)

## SHAKEN call flow

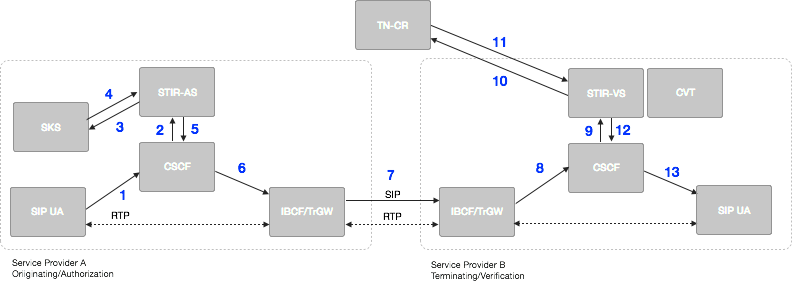


Figure : SHAKEN reference call flow

1. The originating SIP UA first REGISTERs and is authenticated to the CSCF, then creates a SIP INVITE with an E.164 calling number.
2. The originating CSCF, P-CSCF function specifically, adds a P-Asserted-Identity header asserting the Caller ID of the originating SIP UA. The CSCF then has an originating trigger to the STIR-AS for the INVITE.
3. The originating service provider (SP) A’s STIR-AS retrieves its private key from the SKS.
4. The SKS provides private key, and the STIR-AS signs the INVITE and adds an Identity header per RFC 4474bis using the Caller-ID in the P-Asserted-Identity header.
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 NNI through standard inter-domain routing configuration.
8. The SP B ingress IBCF receives INVITE from NNI.
9. The terminating CSCF has a terminating trigger to the STIR-VS for the INVITE.
10. The terminating SP STIR-VS looks at the “info” parameter in the Identity header per RFC 4474bis to determine the TN-CR URI and the originating TN.
11. The STIR-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 to validate the signature in the Identity header, which validates the Caller ID used when signing the INVITE on the originating service provider STIR-AS.
12. Depending on the result of the STI validation, the STIR-VS determines that the call is to be terminated with the appropriate RFC 4474bis defined response code and the INVITE is passed back to the terminating CSCF and continues to set up the call with the terminating SIP UA.
13. The SIP UA receives the INVITE and normal SIP processing of the call continues returning “200 OK”, or optionally setting up media end-to-end.

# STI Certificates

PASSporT defines the usage of X.509 based digital signatures using either the RSA-256 PKCS#1 v1.5 or ECDSA cryptographic algorithms with a preference for the latter.

## PASSporT token and Certificates

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",

"otn":"12155551212",

"duri":"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 originating telephone number owner or the entity signing on their behalf’s certificate.

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

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.

For STI, certificates at a minimum must represent an authorized telephone service provider and their authorization to assert telephone number on a VoIP network. The following section 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. The 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 has no need for 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.

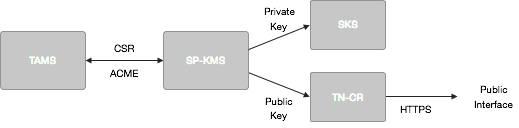


Figure : SHAKEN Certificate Management Architecture

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 keys.
* 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 certificate key pair from 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 certificate as root
* Provider downloads the issued 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 certificate key pair.

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 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.

# Appendix A – Informational - Call Authentication Procedures

Beyond the rfc4474bis mechanisms of authentication service including the addition of the identity header with signature. There are a number of call origination scenarios that must be considered for how call validation can be used successfully with the SHAKEN framework.

In order to provide the validation service the appropriate amount of information to handle call scenarios that may not fit into the ideal model where the primary call originator is also the authentication service, such as international gateways or calls gatewayed from legacy PSTN networks. An additional indicator should be provided by the authentication service to provide the information it knows about how the call was originated, if any.

A proposed PASSporT extension claim will be considered to relay one of four call origination scenarios asserted by the Authentication Service.

These origination call scenerios are defined as follows:

1. Originator Signed and Authenticated Calling Party Telephone Number

* This represents the case where the Originating provider owns the telephone number and has explicitly authenticated the origination of the telephone call from the device. This covers most subscriber line customers.
* Validation Confidence: Very High
* Indicator: “direct\_auth”

2. Originator Signed and Indirectly Authenticated Calling Party Telephone Number

* This represents the case where the Originating provider owns the telephone number and provides this telephone number to a third party customer, e.g. SIP trunks.
* Validation Confidence: High based on reputation of originator
* Indicator: “indirect\_auth”

3. Originator Signed and No Authentication of Calling Party Telephone Number

* This represents the case where the service provider is originating and signing the token but does not have any ownership of the telephone number. Examples include visited network or roaming scenarios, E911 for visited network.
* Validation Confidence: Low
* Indicator: “no\_auth”

4. Originator Signed from untrusted network

* This represents call scenarios where calls are originated from Pre-IMS, legacy circuit-switched networks, or other calls originating from gateways that opt to not sign a call.
* Validation Confidence: No confidence
* Indicator: “untrusted”

The authentication service when it constructs the PASSporT header should include the following key value pair:

“ppt”:”shaken”

This will indicate that it is using the SHAKEN extension to PASSporT

In the PASSporT payload claims the following should be included:

“confidence”:”direct\_auth”

The confidence claim represents the authentication services confidence level as described above using the indicator strings.

# Appendix B – Informational - Call Validation Treatment

When a call is received at the terminating service provider, it should provide the rfc4474bis defined validation service. The rfc4474bis document defines the procedures to validate the signature included in the identity header, but does not explicitly define what is next.

There are a few steps that can or should be taken for determination of the “validitiy” of a call.

* Validate signature per rfc4474bis and passport
* Check public key certificate chain for valid/known telephone authorities
* Check that the telephone number asserted is associated with the signature
* If the telephone number asserted is not associated, use the confidence claim as a guideline to perform other mitigation or blocking techniques based on customer preference
* If the signature isn’t valid, the appropriate error should be sent back (as defined in rfc4474bis)

The SHAKEN framework has defined the *confidence* claim as an extension to PASSporT to guide the terminating service provider on what the authenticating provider knew about the call.

There will likely be more extensions in the future that provide information to the authentication service, but we will start with the confidence claim to define the mechanism.