**ATIS-0x0000x**

ATIS Standard on

**ATIS Technical Report on a Framework for SHAKEN Attestation and Origination Identifier**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This document provides a ATIS Technical Report on a Framework for Signaling Modifications and Display of Verified Caller ID in Support of the SHAKEN Framework. It describes problems associated with originating party spoofing in IP communication networks, identifies potential mitigation options, analyze pros and cons of mitigation options.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

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

[**LEADERSHIP LIST**]

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

**Revision History**

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

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

This technical report provides a framework for SHAKEN attestation and granularity of the Origination Identifier.

## Purpose

## Application

.

# 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.

# 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 identity:** The originating phone number included in call signalling used to identify the caller for call screening purposes.In some cases this may be the Calling Line Identification or Public User Identity. For the purposes of this study, the caller identity may be set to an identity other than the caller’s Calling Line Identification or Public User Identity.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# Architecture

## SHAKEN reference architecture

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 architecture is specifically based on the 3GPP IMS architecture with an IMS application server, and is only provided as an example to set the context for the functionality described in this document. The diagram shows the two IMS instances that comprise the IMS half-call model; an originating IMS network hosted by Service Provider A, and a terminating IMS network hosted by Service Provider B.



**Figure 4.1 – SHAKEN Reference Architecture**

This SHAKEN reference architecture includes the following elements:

* SIP UA – The SIP User Agent that is authenticated by the service provider network 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 Network-to-Network Interface (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 should either itself be highly secured and contain the Secure Key Store (SKS) of secret private key(s) or have an authenticated, Transport Layer Security (TLS)-encrypted interface to the SKS which stores the secret private key(s) used to create PASSporT signatures.
* 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 Telephone Number 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 providing a response to signal the display response for the end user.
* SKS – The Secure Key Store is a logical highly secure element that stores secret private key(s) for the authentication service (STI-AS) to access.
* Certificate Provisioning Service – A logical service used to provision certificate(s) used for STI.
* Telephone Number Certificate Repository (TN-CR): This represents the publically accessible store for public key certificates. This should be an HTTPS web service that can be validated back to the owner of the public key certificate.

Xxx



# Attestation

The SHAKEN framework defines the following three levels of attestation:

A.  **Full Attestation:** The signing provider shall satisfy all of the following conditions:

* is responsible for the origination of the call onto the IP based service provider voice network.
* has a direct authenticated relationship with the customer and can identify the customer.
* has established a verified association with the telephone number used for the call.

NOTE 1: The signing provider is asserting that their customer can “legitimately” use the number that appears as the calling party (i.e., the Caller ID). The legitimacy of the telephone number(s) the originator of the call can use is subject to signer-specific policy, but could use mechanisms such as the following:

* The number was assigned to this customer by the signing service provider.
* This number is one of a range of numbers assigned to an enterprise or wholesale customer.
* The signing service provider has ascertained that the customer is authorized to use a number (e.g. by business agreement or evidence the customer has access to use the number). This includes numbers assigned by another service provider.
* The number is not permanently assigned to an individual customer but the signing provider can track the use of the number by a customer for certain calls or during a certain timeframe.

NOTE 2: Ultimately it is up to service provider policy to decide what constitutes “legitimate right to assert a telephone number” but the service provider’s reputation may be directly dependent on how rigorous they have been.

B. **Partial Attestation:** The signing provider shall satisfy all of the following conditions:

* is responsible for the origination of the call onto its IP based voice network.
* has a direct authenticated relationship with the customer and can identify the customer.
* has NOT established a verified association with the telephone number being used for the call.

NOTE: When partial attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature. As described in section 5.2.4, the unique origination identifier allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. The identifier also provides a reliable mechanism to determine the customer for forensic analysis or legal action where appropriate.

C. **Gateway Attestation:** The signing provider shall satisfy all of the following conditions:

* is the entry point of the call into its VoIP network.
* has no relationship with the initiator of the call (e.g., international gateways).

NOTE: The token will provide a unique origination identifier of the node in the “origid” claim. (The signer is not asserting anything other than “this is the point where the call entered my network”.)

## Guidelines

### Full Attestation

### Partial Attestation

#### Enterprise Scenario

### Gateway Attestation

### New Attestation???

# Origination Identifier

Per SHAKEN Framework, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a UUID (RFC 4122).

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

For Full Attestation, in general, a single identifier will be used as part of the certificate representing direct service provider-initiated calls on its VoIP network. A service provider may, for example, also choose to have a pool of identifiers to differentiate geographic regions or classes of customers. Best practices will likely develop as trace back and illegitimate call identification practices evolve.

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

For Gateway Attestation, best practices will dictate that the “origid” should be sufficiently granular to identify the originating node or trunk to allow for trace back identification and reputation scoring.

## Guidelines

# Conclusions

**Annex A**

(normative/informative)

# A Illustrative Examples

This annex will document supportive material





# B Use case examples for UNI Identity, Authentication, and Authorization in relation to SP use of SHAKEN

There are many possible use cases of UNI security services as inputs to SHAKEN processing. These should be thought of both in the management plane and in the transport and call processing planes. The process begins with establishing the customer real-world identity at on-boarding time and negotiating terms of use, establishing UNI authentication credentials and securing network paths, and establishing and maintaining TN authorization. In the service plane, it consists of authentication of the customer and determining TN authorization for each call to the extent that is part of the calling scenario. The process continues with monitoring of customer/TN usage patterns to enforce policy.

The scenarios are different, among other dimensions, based on whether the customer is the direct end user or the end user is behind a customer proxy/b2bua, which entity is assigned a TN, and whether or not the originating SP assigned the TN. A way to represent the scenarios is a matrix of the service usage, security services applied, and expected SHAKEN attestation result. Below are some examples:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **End user** | **Customer** | **TN assigned to** | **TN assigned by** | **Identity established by** | **Authentication type** | **Authorization established by** | **Attestation result** |
| Mobile subscriber | Same as end user | Subscriber | Originating SP | Customer name/address/credit checks | Device | Direct assignment | A |
| Enterprise PBX | Same as end user | Enterprise customer | Other SP | Customer name/address/credit checks | Customer ID/pre-shared key, IP network ACL | Letter of Authorization | A |
| Individual or enterprise | VASP | VASP | Originating SP | Customer name/address/credit checks, end-user traced through customer | Customer ID/IP network ACL | Direct assignment, terms of use (customer responsible for end use) | A |
| Non-domestic entity | Gateway provider | End user | Non-domestic provider/not determined | Not determined (gateway provider not the originating SP) | Network interconnection | Not determined | C |
| Individual or enterprise | Reseller | End user | Other SP | Customer name/address/credit checks, end-user traced through customer | Network interconnection | Terms of use | A or B based on terms enforcement |
| … |  |  |  |  |  |  |  |