**Committee Name:** ATIS/SIP Forum IP-NNI Task Force

**Meeting Date:** 6/30/2020

**TITLE:** ATIS Standard on Toll-Free Calls in the SHAKEN Framework

**SOURCE:** Mary Retka, Somos, Inc., [mretka@somos.com](mailto:mretka@somos.com), 732 672-0996

**ISSUE NUMBER:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ABSTRACT:**

This document is an ATIS Standard on Toll-Free Calls in the SHAKEN Framework

ATIS-0x0000x

ATIS Standard on

**ATIS Standard on Toll-Free Calls in the SHAKEN Framework**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This document is intended to cover Toll-Free calls and to define the principles that should be adhered to for processing those calls involving Toll-Free Numbers. Those principles align with the principles for processing calls involving TNs that are not Toll-Free Numbers. This report considers scenarios in order to attain full attestation for the Toll-Free Number. This includes in the event there is no naturally verified association available to the OSP regarding the Toll-Free customer and the use of a Toll-Free Number as the Caller ID. This document considers the scenarios for Toll-Free calls identifying the means for processing those calls within SHAKEN.

**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 ATIS IP NNI Members from the Toll-Free Number Administration are responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| May 15, 2020 | 0.1 | IPNNI-2020-00092R000 (2020 baseline) | Mary Retka, Justen Davis,  Julio Armenta |
| June 1, 2020 | 0.2 | IPNNI-2020-00092R001 | Mary Retka, Justen Davis |
| June 29, 2020 | 0.3 | IPNNI-2020-00092R002 | Mary Retka, Justen Davis |
| June 30, 2020 | 0.4 | IPNNI-2020-00092R004 | Mary Retka, Justen Davis |
| August 12, 2020 | 0.5 | IPNNI-2020-00092R005 | Mary Retka, Justen Davis |

**Table of Contents**

1 Scope, Purpose, & Application 5

1.1 Scope 5

1.2 Purpose 5

2 References 5

3 Definitions, Acronyms, & Abbreviations 6

3.1 Definitions 6

3.2 Acronyms & Abbreviations 8

4 Principles 9

5 Overview 10

5.1 Problem Statement 10

5.2 Objective 10

5.3 Toll-Free Overview 11

5.3.1 Toll-Free Number Assignment 11

5.3.2 Toll-Free Call Origination 12

6 Scenarios 12

6.1 Toll-Free in SHAKEN 12

6.2 Delegate Certificate Management for Toll-Free Number 13

6.2.1 Issuing Delegate Certificate for Toll-Free Number 13

6.2.2 Utilizing Delegate Certificate to sign Originating Toll-Free Number 13

6.3 Toll-Free Call Flows 15

6.3.1 Toll-Free Translation Prior to Authentication Server Request 15

6.3.2 Toll-Free Translation After Authentication Request 16

6.4 Toll-Free Use Case – Toll-Free Originations (On Premise PBX, Hosted/Cloud Platform) in SHAKEN 17

7 The Right to Use the Toll-Free Number 17

8 Summary 18

# Scope, Purpose, & Application

## Scope

This document is limited to scenarios that use the currently defined STIR/SHAKEN framework to process Toll-Free Calls.

## Purpose

The current SHAKEN framework provides a set of tools that enable calls to process from origination to termination. The SHAKEN protocol specification [ATIS-1000074-E] describes an authentication mechanism that can be invoked by the originating service provider (OSP) to "attest" to the legitimacy of the calling telephone number associated with a call.

In this framework, the OSP’s STI-AS creates a PASSporT and inserts this PASSporT in the SIP Identity header per RFC 8224. The SIP INVITE is then routed over the network-to-network interface (NNI) through the standard inter-domain routing configuration.

This document identifies Toll-Free call scenarios and provides the process for Toll-Free call authentication. The process described here also aligns with the process for non Toll-Free numbers.

# References

The following standards contain provisions which, through reference in this text, constitute provisions of this document. 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-0300251, *Codes for Identification of Service Providers for Information Exchange.*

ATIS-0417001-003, *Industry Guidelines For Toll-Free Number Administration.*

ATIS-1000074-E, *Errata on ATIS Standard on Signature-based Handling of Asserted Information using Tokens (SHAKEN).*

ATIS-1000080.v002, *SHAKEN: Governance Model and Certificate Management.*

ATIS-1000084-E, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators.*

IETF RFC 3261, *SIP: Session Initiation Protocol.*1

IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

IETF RFC 3966, *The tel URI for Telephone Numbers.*1

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace.*1

IETF RFC 4949, *Internet Security Glossary, Version 2.*1

IETF RFC 7044, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*.1

IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*1

IETF RFC 8225, *Personal Assertion Token.*[[1]](#footnote-2)

IETF RFC 8226, *Secure Telephone Identity Credentials: Certificates.*1

3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).*[[2]](#footnote-3)

# 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

**Authoritative Directory:** A data store of TNs and their verified association to the TN customer and which is populated by authorized parties.

**Call Diversion:** Any call feature that updates the destination telephone number of a call to a new or alternate telephone number. Example call features include the various forms of call forwarding, find-me/follow-me (simultaneous or sequential ringing), and automatic call distribution.

**Caller ID:** The originating or calling party’s telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields in the Session Initiation Protocol (SIP) [RFC 3261] messages.

**(Digital) Certificate:** Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object [RFC 4949]. See also STI Certificate.

**Certification Authority (CA):** An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [RFC 4949].

**Certificate Chain:** See Certification Path.

**Certification Path:** A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain [RFC 4949].

**Certificate Revocation List (CRL):** A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [RFC 4949].

**Certificate Signing Request (CSR):** A CSR is sent to a CA to request a certificate. A CSR contains a Public Key of the end-entity that is requesting the certificate.

**Chain of Trust:** Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain [RFC 4949].

**Certificate Validation:** An act or process by which a certificate user established that the assertions made by a certificate can be trusted [RFC 4949].

**Company Code:** A unique four-character alphanumeric code (NXXX) assigned to all Service Providers [ATIS-0300251].

**Customer:** Typically, a service provider’s subscriber, which may or not be the ultimate end-user of the telecommunications service. In the context of the SHAKEN attestation model, the Customer is the entity with a direct business relationship and a direct user-to-network interface with the OSP. Enterprises, hosted/cloud service providers, OTT providers and other service resellers may be considered customers of an OSP depending on the use case.

**End-Entity:** An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of this document, an end-entity is a Service Provider, TN Service Provider, or VoIP Entity.

**Fingerprint:** A hash result ("key fingerprint") used to authenticate a public key or other data [RFC 4949].

**Identity:** Either a canonical Address-of-Record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as ’sip:alice@atlanta.example.com’), or a telephone number, which commonly appears in either a TEL URI [RFC 3966] or as the user portion of a SIP URI. See also Caller ID [RFC 8224].

**National/Regional Regulatory Authority (NRRA):** A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

**Online Certificate Status Protocol (OCSP):** An Internet protocol used by a client to obtain the revocation status of a certificate from a server.

**Originating Service Provider (OSP):** The service provider that handles the outgoing calls from a customer at the point at which they are entering the public network. The OSP performs the SHAKEN Authentication function. OSP may also serve in the role as TNSP, RespOrg, TN reseller and other roles.

**Private Key:** In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption [RFC 4949].

**Proof of Possession of a TN:** Proof to STI verification services that it has authority to attest that the customer can legitimately originate calls from the delegated TNs.

**Public Key:** The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography [RFC 4949].

**Public Key Infrastructure (PKI):** The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [RFC 4949].

**Redirect:** As defined in [RFC 3261], "redirect" refers to the process where a SIP entity redirects a SIP request to a new destination by responding to the request with a 3xx Redirection class response. This specification addresses redirection only for INVITE requests, and only for the case where the 3xx response is handled by a recursing SIP proxy that retargets the INVITE request to the new destination.

**Responsible Organization (RespOrg):** Entity designated as the agent for the Toll-Free subscriber to obtain, manage and administer Toll-Free Numbers and provide routing reference information in the SMS/800 Toll-Free Number Registry.

**RespOrg Identification (RespOrg ID):** A 5-character code that designates or points to the Responsible Organization (RespOrg) associated with a specific Toll-Free number [ATIS-0417001-003].

**Retarget:** As defined in [RFC 7044], "retarget" refers to the process where a SIP entity updates the Request-URI of a SIP request. This specification narrows the scope of the [RFC 7044] definition to include only INVITE requests, and only for cases where the update changes the canonical value of the telephone number identified by the INVITE Request-URI.

**Root CA:** A CA that is directly trusted by an end-entity. See also Trust Anchor CA and Trusted CA [RFC 4949].

**Secure Telephone Identity (STI) Certificate:** A public key certificate used by a service provider to sign and verify the PASSporT.

**Service Provider Code:** In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider. In the US and Canada this would be a Company Code as defined in [ATIS-0300251], or a RespOrg ID assigned to a RespOrg as defined in [ATIS-0417001-003].

**Signature:** Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [RFC 4949].

**Telephone Identity:** An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

**Telephone Number Assignee (TN Assignee):** Entity (e.g., enterprise, service provider, VoIP Provider, Over the Top Provider, hosted/cloud communications provider, etc.) that has been given the authority to use TNs by virtue of having been directly assigned these TNs by an authorized Telephone Number Service Provider. In the context of tollfree numbering resources, a TN Assignee is an entity that has been assigned the use of the TN by a RespOrg. This definition also applies to Toll-Free Number Assignees (TFN Assignee),. RespOrgs (see Responsible Organization above) are the only parties who assign, manage and administer Toll-Free numbers in the SMS/800 Toll-Free Number Registry.

**Telephone Number Service Provider (TNSP):** SP that has been formally assigned TNs by the national numbering authority (e.g., NANPA). A TNSP may assign a subset of its TNs to a business entity (aka TN Assignee), to be used as Caller ID for calls originated by the business entity. TNSPs can also serve in the role as OSP or TSP. This definition also applies to Toll-Free Number Service Providers (TFNSP). RespOrgs (see Responsible Organization above) are the TFNSPs, the only parties who assign, manage and administer Toll-Free numbers in the SMS/800 Toll-Free Number Registry.

**Terminating Service Provider (TSP):** the SP whose network terminates the call (i.e., serving the called party). The TSP performs the SHAKEN Verification function.

**Trust Anchor:** An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The trust anchor is a combination of a trusted public key and the name of the entity to which the corresponding private key belongs [RFC 4949].

**Trust Anchor CA:** A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key. See also Root CA and Trusted CA [RFC 4949].

**Trusted CA:** A CA upon which a certificate user relies for issuing valid certificates; especially a CA that is used as a trust anchor CA [RFC 4949].

**Trust Model:** Describes how trust is distributed from Trust Anchors.

**VoIP Entity:** A non-STI-authorized customer entity that purchases (or otherwise obtains) delegated telephone numbers from a TNSP

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| ATIS | Alliance for Telecommunications Industry Solutions |
| B2BUA | Back-to-Back User Agent |
| CRL | Certificate Revocation List |
| CSCF | Call Session Control Function |
| CVT | Call Validation Treatment |
| HTTPS | Hypertext Transfer Protocol Secure |
| IBCF | Interconnection Border Control Function |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IP | Internet Protocol |
| JSON | JavaScript Object Notation |
| JWS | JSON Web Signature |
| NNI | Network-to-Network Interface |
| OCSP | Online Certificate Status Protocol |
| OSP | Originating Service Provider |
| PASSporT | Persona Assertion Token |
| PBX | Private Branch Exchange |
| PKI | Public Key Infrastructure |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| SKS | Secure Key Store |
| SMS/800 | 800 Service Management System |
| SP | Service Provider |
| SPID | Service Provider Identifier |
| STI | Secure Telephone Identity |
| STI-AS | Secure Telephone Identity Authentication Service |
| STI-CA | Secure Telephone Identity Certification Authority |
| STI-CR | Secure Telephone Identity Certificate Repository |
| STI-VS | Secure Telephone Identity Verification Service |
| STIR | Secure Telephone Identity Revisited |
| TFAS | Toll-Free Application Server |
| TFN | Toll-Free Number |
| TFR-DB | Toll-Free Routing Database |
| TLS | Transport Layer Security |
| TN | Telephone Number |
| TNSP | TN Service Provider |
| TSP | Terminating Service Provider |
| UA | User Agent |
| URI | Uniform Resource Identifier |
| UUID | Universally Unique Identifier |
| VoIP | Voice over Internet Protocol |

# Principles

Where the originating entity utilizes the network connectivity of the OSP who also is the RespOrg, and where the OSP has assigned the Toll-Free Number used as the Caller ID, the OSP is able to authenticate their customer's use of the Toll-Free Number following the ATIS - 1000074 SHAKEN Principles.

The following core principles should be adhered to in order to attain full attestation in the event there is no naturally verified association available to the OSP regarding the customer and the use of a TN as the Caller ID:

1. OSPs adhere to SHAKEN criteria for attestations “A”, “B” and “C”.
2. Any enhancements required to SHAKEN PASSporT fields and certificates align with ATIS/SIP Forum IP NNI Task Force standards and/or best practices.
3. ATIS-1000074 states that ultimately it is up to service provider local policy to decide which mechanisms are sufficient for an OSP to attest fully to a “legitimate right to assert a telephone number” for a given call.
4. OSPs send a SHAKEN PASSporT, signed with their own credentials, attesting to the validity of the TN independent of other information such as an enterprise signed Identity header added to the call.
5. Regardless of which enterprise mechanism is utilized, the OSPs should be able to audit the mechanism(s) used to establish authorization for a customer to use specific TNs or TFNs as the customer Caller ID for industry traceback purposes.
6. TNSPs and RespOrgs are authorized issuers of TNs and TFNs to business entities and can vouch for a customer’s right to use a given TN and TFN as their Caller ID.
7. The association between a Customer and a TN or TFN may be determined by means other than direct assignment from the OSP, e.g. “proof of possession of a TN” (see ATIS-IPNNI-2018-00018 and ATIS-IPNNI-2020-00060).
8. TSPs verify the OSP is using a SHAKEN approved CA.
9. For calls signed by an OSP, a TSP verification service should not require the calling TN or TFN to be assigned to the OSP’s in order to generate a successful validation result.

The OSPs reputation and continued membership in the SHAKEN ecosystem may be directly dependent on how rigorously they have applied the above principles within their local policies regarding Caller ID attestation.

# Overview

## Problem Statement

STIR/SHAKEN describes a framework for originating service providers to create a SHAKEN PASSporT that can be carried by the SIP signaling protocol to cryptographically attest the identity of callers.

There is a timing mismatch between the requirement for call authentication versus the readiness of the network to accommodate call authentication for Toll-Free originated calls. This mismatch will create a situation where some consumers get the benefits of call authentication while others cannot. Given the businesses who rely on Toll-Free calls to get their customers connected to them, it’s important to address the need for Toll-Free calls to process appropriately in the SHAKEN framework.

This document addresses the potential mismatch where Toll-Free calls are not currently being authenticated and provides the means for the Toll-Free calls to gain authentication. It also remains important for the governance process to include Toll-Free and a separate effort is underway to achieve that inclusion.

## Objective

The objective of this document is to address the Toll-Free inclusion in the SHAKEN environment.

This document will do the following:

* Describe Toll-Free and the RespOrg role
* Show Toll-Free in the SHAKEN environment
* Provide the architectural description and call flow ladder

## Toll-Free Overview

The SMS/800 Toll-Free Number (TFN) Registry, the database for the management and administration of Toll-Free Numbers in the North American Numbering Plan (NANP), and the authoritative directory for Toll-Free Numbers. The Toll-Free Number database is accessed by Toll-Free Service Providers (also known as Responsible Organizations (RespOrgs)) for reserving and managing Toll-Free Numbers. (see ATIS-0417001-003 Industry Guidelines for Toll-Free Number Administration). The RespOrg has been designated by the FCC as the agent for the subscriber to obtain, manage and administer Toll-Free Numbers and provide routing reference information in the SMS/800 Toll-Free Number (TFN) Registry. Reservation, assignment, or activation of Toll-Free Numbers may only be made by a RespOrg based upon negotiations with a specific prospective Customer.Toll-Free Numbers are assigned by RespOrgs to their Customers from a common pool of available numbers.

To become a RespOrg the Toll-Free Service Provider must complete the following process:

* Online application (including deposit): Any person, company, or organization that can demonstrate the required skills and financial responsibility for managing Toll-Free Numbers can apply to become a Toll-Free Service Provider (RespOrg) in the SMS/800 Toll-Free Number Registry.
* Training: Attend a SMS/800 Toll-Free Number Registry class or self-train with materials about Toll-Free.
* Successful completion of an exam on Toll-Free Industry practices: The exam includes knowledge of customer records, number administration, and service provisioning. After the exam is passed, the applicant will be certified as a Toll-Free Service Provider (RespOrg). A RespOrg ID will be assigned.

Each RespOrg is identified by a 5-character code (RespOrg ID) provided by the SMS/800 Toll-Free Number (TFN) Registry administrator. Every Toll-Free Number that resides in the SMS/800 Toll-Free Number (TFN) Registry must have an associated RespOrg ID. The SMS/800 Toll-Free Number (TFN) Registry Help Desk maintains and publishes the contact information associated with each operational RespOrg ID.

### Toll-Free Number Assignment

A screenshot of a cell phone

Description automatically generated

**Figure 1. Toll-Free Number Assignment Process**

1. Customer selects a RespOrg and requests a Toll-Free Number (TFN)
2. RespOrg reserves a TFN from the pool of available numbers within the SMS/800 TFN Registry. The TFN is marked as assigned to the RespOrg. The RespOrg also provisions the routing information
3. Routing data is delivered to Routing Database Providers and used by SPs to route calls
4. RespOrg works with the Transit Networks and SPs to establish the infrastructure to support the Toll-Free service
5. Enterprise is able to receive Toll-Free calls and make calls using the TFN as a call back number

### Toll-Free Call Origination

A close up of a logo

Description automatically generated

**Figure 2. Toll-Free Number Enterprise Originated Call**

1. Originating SP and RespOrg are different entities
2. RespOrg reserves 800-555-1212 from the pool of available numbers within the SMS/800 TFN Registry
3. RespOrg assigns 800-555-1212 to Enterprise Customer
4. Enterprise calls 555-321-4321 using 800-555-1212 as Caller ID

# Scenarios

## Toll-Free in SHAKEN

Responsible Organizations (RespOrgs) are the TN Providers (TNSP) in the SHAKEN framework for Toll-Free Numbers.

A TNSP could be a telephone Service Provider, as defined in [ATIS-1000080-E] or a RespOrg that has the authority to obtain and assign Toll-Free numbers to customers. A RespOrg is identified with a RespOrg ID assigned by the SMS/800 Toll-Free Number Registry administrator.

There are various ways in which the attestation level of a Toll-Free calling number can be determined. Two methods are summarized in this document. Other implementations are possible.

1. The RespOrg or the end-user uses the SHAKEN Delegated Certificate process. The RespOrg ID is used along with other STI-GA designated requirements to obtain SPC tokens, and to obtain end-user certificates from an STI-CA**.** The record showing the RespOrg authority over a Toll-Free number can be substantiated by the Toll-Free Number Administrator.
2. The OSP determines an appropriate attestation level, based on information it has on the caller’s right to use the signaled, Toll-Free calling number. The OSP may have direct knowledge of the relationship of the caller to the Toll-Free calling number (e.g. the OSP is the TNSP/RespOrg) or the OSP may obtain this relationship via a trusted 3rd party, such as a TN Registry provider. Refer to clause 7.

## Delegate Certificate Management for Toll-Free Number

### Issuing Delegate Certificate for Toll-Free Number

Figure 3 shows a high-level overview of the process for issuing delegate end-entity certificates to a VoIP Entity for a Toll-Free number. This does not assume that all SPs will use Delegated Certificates. Per the Digital Certificate Standard, a SHAKEN authorized SP that is not a RespOrg may issue Delegate Certificates that include TFNs to its customer, provided that the issuing SP complies with the delegate certificate specification or the TN Registry process. Information for Delegate Certificate Management can be referenced in the ATIS IPNNI-2020-00065 document.

A screenshot of a cell phone

Description automatically generated

**Figure 3. RespOrg issues Delegate Certificate for Toll-Free Number**

The procedure in Figure 3 is performed when TNSP-a as RespOrg (with RespOrg ID JTN01) assigns Toll-Free number 1-800-555-1212 to Enterprise PBX-1, as follows:

1. Subordinate CA (hosted by the RespOrg) obtains SPC Token (SPC-JTN01) from STI-PA
2. Subordinate CA uses the SPC Token to obtain CA certificate from STI-CA
3. Subordinate CA issues delegate end-entity certificate to PBX-1 (TN = 1-800-555-1212)

### Utilizing Delegate Certificate to sign Originating Toll-Free Number

Figure 4 shows a high-level overview of signing an originated Toll-Free Number with a Delegate Certificate.

A picture containing meter

Description automatically generated

**Figure 4. STI Authentication/Verification during call setup**

Figure 4 assumes that the TNSP has assigned a delegate certificate to the VoIP Entity as described in section 6.2.1. The call establishment procedure in Figure 4 is initiated when the VoIP Entity user initiates a call to called TN-x, and the VoIP Entity is configured to deliver a Toll-Free calling number (TFN-a in this example).

1. The VoIP Entity Call Control function invokes the RCD-AS to perform rcd authentication for calling TFN-a, as specified in [atis rcd specification]. The RCD-AS constructs a "rcd" PASSporT containing an "orig" claim of TFN-a and a "dest" claim of TN-x, plus "rcd" claim information for the VoIP Entity, and signs the PASSporT using the private key associated with the delegate certificate.
2. The VoIP Entity Call Control includes an Identity header containing the newly created "rcd" PASSporT in the originating INVITE request sent to the originating SP.
3. The originating SP verifies that the "rcd" PASSporT contained in the received INVITE request is valid. It then performs shaken authentication, asserting an attestation level of "A" (based on the presence of a valid "rcd" PASSporT received from the VoIP Entity). The originating SP includes two Identity headers in the INVITE request to the TSP; one containing the newly created "shaken" PASSporT, and one containing the received "rcd" PASSporT, as specified in [ATIS IPNNI-2020-00025].
4. On receiving the terminating INVITE request, the Terminating SP invokes the STI-VS to verify the received SHAKEN Identity header as specified in [ATIS-1000074] and invokes the RCD-VS to verify the received RCD Identity header as specified in [atis rcd specification].
5. RCD-VS fetches the referenced delegate certificate from the TNSP STI-CR and uses the certificate credentials to verify the "rcd" PASSporT.
6. STI-VS fetches the referenced STI certificate from the OSP STI-CR and uses the certificate credentials to verify the "shaken" PASSporT.
7. The TSP sets the INVITE Verstat parameter based on the verification results (in this case verification passed), and sends the INVITE containing the "rcd" PASSporT to the phone registered for TN-x.

## Toll-Free Call Flows

### Toll-Free Translation Prior to Authentication Server Request

A picture containing parked, meter, parking, sitting

Description automatically generated

**Figure 5. SHAKEN Architecture with Toll-Free DIP (pre-Authentication Server)**

The ladder diagram below shows the call flow for the originating portion of the call setup action. It shows the TFAS being dipped (and subsequently returning the Toll-Free Response) prior to requesting a PASSporT token from the Authentication Server (AS).

A picture containing sign, computer, street, city

Description automatically generated

**Figure 6. Toll-Free Translation Prior to Authentication Server Request**

### Toll-Free Translation After Authentication Request

A picture containing meter, parking, parked, side

Description automatically generated

**Figure 7. SHAKEN Architecture with Toll-Free DIP (post-Authentication Server)**

The second scenario is that in which the PASSPorT token is fetched from the AS before dipping the TFAS. The ladder diagram below shows the call flow for the originating portion of the call setup action.

**A screen shot of a computer

Description automatically generated**

**Figure 8. Toll-Free Translation After Authentication Server Request**

## Toll-Free Use Case – Toll-Free Originations (On Premise PBX, Hosted/Cloud Platform) in SHAKEN

A close up of a keyboard

Description automatically generated

**Figure 9. Toll-Free Origination Use Case – Leveraging 3rd Party RespOrg and Different OSPs**

1. TN Assignee with TN 555-123-1234 initiates call to 555-321-4321
2. Enterprise originates call from TFN 800-123-2234, assigned by RespOrg, using OSP E.
3. OSP E cannot authenticate the Caller ID Toll-Free Number. OSP E adds a SIP Identity header field with a SHAKEN PASSporT setting Attestation to B. The PASSporT is signed using an STI-Certificate with a TNAuthlist containing a single SPC with a value assigned to OSP E.
4. The TSP verifies that the received SHAKEN PASSporT is valid. Since the attestation level is “B” (and not “A”) the TSP populates a verstat value “No-TN-Validation” in the INVITE request sent to the called endpoint.

Also see ATIS 1000085 SHAKEN Support of “div” PASSporT for reference

The following two (2) Toll-Free Use Cases also depict examples where the OSP cannot determine the Toll-Free Calling TN is authorized to the customer and would set the Attestation as B;

* A shared use Toll-Free Number is originated from multiple enterprises. This is the case where enterprises in different geographical locations originate calls using the same Toll-Free Number but utilizing different OSPs. In this scenario, the Toll-Free Number is issued by a single RespOrg.
* The same Toll-Free Number is originated from multiple locations. This is the case where an enterprise uses the same Toll-Free Number but originates calls in different locations utilizing different OSPs.

# The Right to Use the Toll-Free Number

To enable an OSP to determine the appropriate authentication level when a Toll-Free number is used in the Caller ID, there is a process that can provide the clarity for determining the party’s right to use a Toll-Free Number. The Toll-Free Number Administrator manages the authoritative source for Toll-Free number information, the Toll-Free Number Registry.

For a party who will use their Toll-Free number in making an outbound call they can work in advance of their calls to enable them to get the information to use with an OSP in advance of the calls to provide them the proof of the right to use the Toll-Free Numbers so they can get the appropriate authentication level from the OSP when a Toll-Free number is used in the Caller ID. This is done by working with the Toll-Free Number Administrator.

To show that the Toll-Free Number is one that is in use, the Toll-Free Number Administrator will review and confirm via the authoritative source for Toll-Free number information, the Toll-Free Number Registry. The Toll-Free Number Administrator then will work with the RespOrg to ensure that the party with the Toll-Free number has the right to use that Toll-Free number. Then the Toll-Free Number Administrator will provide that information upon a specific request. This needs to be done in advance of the use of the Toll-Free number in making a call or calls. With that information the party planning to make the Toll-Free call may then provide it to a pre-authentication provider, or to the OSP whose network will be used in making the call.

# Summary

SHAKEN has been defined as a framework that utilizes protocols defined in the IETF Secure Telephone Identity Revisited (STIR) Working Group that work together in an end-to-end architecture to provide traceability of calls to the originating service provider (OSP), via a digital signature tied to a certificate identifying the OSP, and to allow the OSP to indicate whether or not a calling telephone number (calling TN) is valid.

It is recognized that there are conditions where the OSP lacks a direct mechanism to fully attest that there is a known authenticated customer and/or that the customer associated with the calling TN or TFN is valid. This document provided use cases where there is a “knowledge gap” between the information the OSP can determine locally and the information it needs, or through additional methods to provide “full attestation” marking (attestation level “A”). The information here provides the means to address these situations in the use cases and close the gap.

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-2)
2. Available from 3rd Generation Partnership Project (3GPP) at: < [https://www.3gpp.org](http://www.3gpp.org) > [↑](#footnote-ref-3)