**ATIS-0x0000x**

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): International Attestation and Certificate Framework**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The base-SHAKEN framework focused on a technical framework for governance over a PKI with a single realm. International presents a situation that SHAKEN can support if jurisdictions adopt the SHAKEN standards in a common way, but can offer challenges if policies are incompatible. This document defines standards on how attestation and jurisdictional certificates consistent with existing SHAKEN specifications can be managed and interpreted in a consistent way that can align with jurisdictional interests and policies with the goal of reducing exception cases when doing cross border 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 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** |
| --- | --- | --- | --- |
|  | Initial | Baseline |  |

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

2 Normative References 2

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 4

4 Overview 6

5 Indirect use-cases and authority over call and caller data 6

5.1 Authority beyond 6

**Table of Figures**

Figure 1. Delegate Certificate Management Flow 7

**Table of Tables**

No table of figures entries found.

# Scope, Purpose, & Application

## Scope

This specification extends the SHAKEN.

## Purpose

The purpose of the SHAKEN

# 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-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*

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

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

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

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

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

RFC 5806, *Diversion Indication in SIP*. 1

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

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

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

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

draft-ietf-stir-passport-shaken, *PASSporT SHAKEN Extension.* 1

draft-ietf-stir-passport-divert, *PASSporT Extension for Diverted Calls.* 1

draft-ietf-acme-authority-token, *ACME Challenges Using an Authority Token.* 1

draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token.* 1

draft-ietf-stir-cert-delegation, STIR Certificate Delegation*.* 1

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

The following provides some key definitions used in this document.

**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].

**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.

**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].

**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].

**Responsible Organization (Resp Org):** 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.

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

**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 Resp Org ID assigned to a Resp Org as defined in [ATIS-0417001-003].

Editor’s note: Further analysis is required to determine if Resp Org should be included as part of the service provider code or somewhere else.

**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.

**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 |
| 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 |
| 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 |

# Background

## NANC CATA Working Group 2

The NANC CATA working group 2 in 2020 provided guidance to the FCC in its report relative to international gateways and identification of international subscribers. The following is an excerpt from the report:

**Identification of international subscribers**

For internationally originated calls, there is a desire for other countries to adopt corresponding STIR/SHAKEN, STI-GA and STI-PA ecosystems that provide authorized digital signatures, endorsed by local regulatory agencies and coordinated through cross-border efforts being discussed in the Joint ATIS/SIP Forum IP-NNI Task Force and other forums. This is similar to what is happening between the US and Canada, where there is coordination of providing authorized root certificates specific to a country or region.

In the United States, it is a long-standing problem that international gateway traffic is a significant source of fraudulent traffic. However, both how and where that traffic is coming from is not well defined. Traditionally, an “international gateway” is defined as a network element that specifically translates international call signaling from country specific standards to US provider compatible protocols. As VoIP services have evolved, the use of the term “international gateway” has unfortunately become less well defined. VoIP does not have as many geographic restrictions as non-IP services, which has enabled international entities to send VoIP traffic easily around the world including traffic that may terminate into a US-based provider’s network. Today, it is understood that most of the fraudulent internationally-sourced traffic is coming through domestic telephone application providers and VSPs. Often, this occurs through underground or backdoor types of operations that mainly cater to malicious entities (either international or domestic) that want to terminate traffic with illegally spoofed NANP telephone numbers or illegitimate or invalid numbers. While fraudulent traffic does happen with international calling party telephone numbers coming from the legitimate country of origin, currently the portion of this traffic to the overall fraudulent call volume is relatively small. Based on SP experience, it appears the primary source of the problem may not be “international gateways,” rather, it is VoIP applications, trunks, and wholesale providers that cater to subscribers sourcing traffic from international entities with fraudulent intent.

Fraudulent internationally sourced or originated traffic can be separated into the following broad categories:

* Internationally-based companies or individuals sending fraudulent traffic using US-based application, trunking, or wholesale services with spoofed domestic numbers;
* Internationally-based companies or individuals sending fraudulent traffic using US-based application, trunking, or wholesale services with spoofed international numbers;
* Internationally-based companies or individuals sending fraudulent traffic using internationally based application, trunking, or wholesale services with spoofed domestic numbers; or
* Internationally-based companies or individuals sending fraudulent traffic using internationally based application, trunking, or wholesale services with spoofed international numbers.
* Best practices for these use cases could utilize these broad categories to inform specific future practices.

**Alternative mechanisms to assist with interoperability in the absence of STIR/SHAKEN technologies**

Best practices for internationally-originated calls using NANP numbers are still evolving, including how to acquire sufficient information to accomplish TN Validation for elevation to “A” attestation. Industry consensus has not yet coalesced on call authentication with less than “A” (full) attestation in some call scenarios. This could include the best practices, as appropriate, endorsed by this working group and explained in this document, including the vetting of customers and the validation of telephone numbers used for the services offered.

For example, international VSPs have proposed technical and contractual solutions that may enable them to work with domestic carrier partners to apply the full range of SHAKEN attestations to calls originating overseas. This “enhanced international attestation” approach may offer international providers the means to deliver more information and value to domestic carriers and consumers than if all calls originating outside the U.S. are assigned a “C”-level attestation, or are not authenticated. International providers may enter into voluntary commercial agreements with domestic carriers or intermediate providers capable of assigning the relevant SHAKEN attestation level based on information the international provider has collected from its Customers (as well as its vetting, ordering, and TN validation procedures). Industry stakeholders should be permitted to develop the specific mechanisms or techniques by which they achieve higher levels of fidelity to SHAKEN attestation for international traffic.

In one example of this arrangement, international voice traffic could be segmented into separate streams via a multi-trunk approach that correlates to the three attestation levels of SHAKEN—“A” for calls that originated on a provider’s network from numbers assigned to the originating subscriber, “B” for calls that originated on a provider’s network from numbers that were not assigned to the originating subscriber, and “C” for calls that neither originated on a provider’s network nor from numbers assigned to the originating subscriber. Domestic carriers could then rely on information proffered by the international provider to assign the appropriate attestation level and send the traffic either to another downstream provider or to its termination point.9

It should be noted that while this approach would be voluntary for domestic carriers (permitting these providers to choose international partners that display high levels of trustworthiness), the inclusion of robust commercial and contractual remedies, if an international provider fails to appropriately identify its traffic, could obviate domestic carriers’ concerns about exposure to reputational or enforcement risk as well as regulators’ anxieties that such a mechanism could be used as a backdoor for illegal robocalls or spoofing.

Additionally, the Global System for Mobile Communications Association (GSMA) has recently undertaken an activity by establishing the Validating INtegrity of End-to-End Signaling (VINES) Working Group to develop a set of recommendations to prevent internetwork signaling fraud, which includes illegal robocalls, illegal spoofing, illegal toll bypass and consumer fraud. One of its objectives is to propose a mechanism to interwork with STIR/SHAKEN.

So, while there is definition of the problem and classification of the different scenarios involved in different types of international traffic, and general best practice suggestions and discussion, there isn’t a clear technical framework recommended and suggests the need for this standard.

This document defines a technical framework for how attestation should be applied in a SHAKEN eco-system that crosses multiple PKI associated with different governance and regulatory jurisdictions. The goal of this framework, similar to other SHAKEN specifications is to avoid global or local policy decisions and use the SHAKEN framework tools to provide a way of conveying the attestation and other SHAKEN related information using the signatures and certificate framework defined by SHAKEN and related standards.

## Technical Reports: International SHAKEN

### IP-NNI

The following ATIS Technical Reports address aspects of SHAKEN for international calls:

* ATIS-1000087: *Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN)*
* ATIS-1000091: *Mechanism for International Signature-based handling of Asserted information using toKENs (SHAKEN)*

Both documents deal with the technical mechanisms for sharing Trusted CA lists between countries but do not address the policy considerations associated with this. In addition, neither document addresses the treatment of SHAKEN PASSporTs at the international gateway. The unstated assumption is that the PASSporTs will be transparently transported across borders, and that decisions about how to deal with these PASSporTs will be made by the terminating service provider, based on local policy. Regulation will be one important input to this “local policy” but again, this is unstated.

### ATIS’ Non-IP Call Authentication Task Force

ATIS’ Non-IP Call Authentication Task Force is also developing standards that will provide “SHAKEN functionality” for non IP networks:

* Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks
* Extending STIR/SHAKEN over TDM

Both of these documents include sections discussing the handling of PASSporTs and SHAKEN attestation levels for international calls. The documents specify that PASSporTs (or the corresponding attestation level) will be sent transparently across international gateways for international calls. PASSporTs for domestic calls are never sent across international borders. In addition, for Out-of-Band PASSporT transmission, the PASSporT is handled by a network element at the international gateway that transfers the PASSporT from one jurisdiction to the other. Although this function in the proposed standards passes all PASSporTs for international calls, it could in the future apply country-specific processing if this was required by regulation.

### Applying full attestation at the international border

ATIS-1000074 only dealt with providing attestation for domestic calls.  But for calls within the U.S., service providers were allowed to provide full attestation for calls, even if the number was not associated with their OCN, as long as the call was initiated by the service provider’s “customer”, and the service provider could determine the customer had the legitimate right to use the number. This allowed full attestation for many valid use cases, such as enterprises initiating calls through two service providers for reliability or cost savings.

Extending this concept to allow a U.S. based service provider to offer full attestation for international calls, using non-U.S. numbers, and originated by non-U.S. service providers wasn’t considered as part of the original SHAKEN standard. But perhaps this question should be studied.  Some potential factors to consider include (for discussion):

* ATIS-1000074 did not define “customer”, but ATIS-1000088 (*A Framework for SHAKEN Attestation and Origination Identifier*) has since provided further analysis of ”customer” and criteria for providing full attestation. This may provide objective criteria to evaluate the feasibility of U.S. service providers offering full attestation for international calls at an international gateway (assuming they can determine the entity originating the call has a legitimate right to use the number).
* At its core, the SHAKEN trust model depends on establishing a reputation for every service provider, and the ability to “find and punish” service providers that abuse that trust.  Signing calls at the U.S. border (with sufficient verification) does not inherently undermine this model – and may in fact strengthen it because the service providers would be under U.S. jurisdiction.
* Allowing U.S. service providers to offer full attestation at international gateways (with sufficient vetting) does not preclude adopting a broader international SHAKEN framework. The two approaches can be complementary.

# Use Cases

The NANC CATA working group 2 identified two key factors that should be considered when analyzing international traffic:

* **Telephone number**: is the calling party number a domestic TN (from the NANP, and assigned to the U.S.) or an international number (anything other than a NANP number assigned to the U.S.)?
* **Origination**: is the entity offering the service (e.g., application or wholesale service) U.S. based, or non-U.S. based?

Combining these two factors gives four broad categories as the basis for additional analysis and to develop best practices. These categories are:

* Internationally-based companies or individuals sending fraudulent traffic using US-based application, trunking, or wholesale services with spoofed domestic numbers;
* Internationally-based companies or individuals sending fraudulent traffic using US-based application, trunking, or wholesale services with spoofed international numbers;
* Internationally-based companies or individuals sending fraudulent traffic using internationally based application, trunking, or wholesale services with spoofed domestic numbers; or
* Internationally-based companies or individuals sending fraudulent traffic using internationally based application, trunking, or wholesale services with spoofed international numbers.

International calls can also come from U.S. mobile customers who are roaming internationally, but this has unique characteristics and is out of scope for this analysis. This technical report will be limited to a consideration of the four categories identified by the CATA report.

# Best Practices

The CATA report identified the need for providing attestation for internationally originated calls and provided a classification scheme for the different international traffic scenarios. The role for general best practices was discussed, but it did not offer a clear technical framework. ATIS technical reports proposed a strategy for a subset of the problem space, specifically where multiple countries establish national SHAKEN infrastructure. This offers an immediate path forward but does not provide a coherent framework for the full problem space.

This document defines a technical framework for how attestation should be applied in a SHAKEN eco-system that crosses multiple PKI associated with different governance and regulatory jurisdictions. The goal of this framework, similar to other SHAKEN specifications, is to avoid uncoordinated global or local policy decisions and to provide a coherent approach to use the SHAKEN framework tools to provide a consistent way of conveying attestation and other SHAKEN related information using the signatures and certificate framework defined by SHAKEN and related standards.

## Analysis of options:

ATIS-1000074-E defines a framework for providing “attestation” about the calling party’s right to use a telephone number at the originating service provider and relaying this information in a cryptographically secure manner to the terminating service provider, within a single country. Within this context, it is relatively clear who provides attestation, and how they determine the appropriate level of attestation. Extending this framework to include international calls introduces significant complexity and uncertainty about who provides attestation, and how to confidently determine attestation levels. This section analyzes key aspects of this space to define a technical framework for international calls and to inform potential best practices.

Note: potential topics for further analysis include:

* STI certificates include an ISO code identifying the country issuing the certificate. Does this limit the certificate to signing for calls originating from that countries telephone numbers?
* Originating service providers are allowed to provide full attestation for TNs not associated with their OCN but within the same country. How does this apply for other countries TNs?
* Analysis of a range of mechanisms that could potentially be used to establish the “right to use a TN”.
* Comparison of national SHAKEN GAs vs industry associations or other international bodies as a root of trust for SHAKEN attestation.

# Recommendation

TBD

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)