ATIS-0x0000x

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Out-of-Band Token Transmission**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

The SHAKEN framework enables a SHAKEN-authorized VoIP Service Provider to deliver cryptographic proof to a called user via SIP signaling that the calling user is authorized to use the calling telephone number. This specification extends this current framework to enable an originating service provider to send the caller identity PASSporTs to the terminating service provider out-of-band, that is, across the internet, separate from the SIP signaling.

**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.

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

2 Normative References 1

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 3

4 Overview 5

4.1 Problem Statement – Why OOB-SHAKEN is needed 5

4.2 OOB-STIR Overview 5

5 OOB-SHAKEN 6

5.1 OOB-SHAKEN Architecture 7

5.2 OOB SHAKEN Call Flow Ladder 7

5.3 Example of OOB SHAKEN HTTP POST 8

6 CPS Discovery 9

6.1 Format of OCN and CPS Address List 9

# Scope, Purpose, & Application

## Scope

This specification extends the currently defined STIR/SHAKEN framework to enable an originating service provider to send caller identity PASSporTs to the terminating service provider out-of-band, that is, separate from the telephone network signaling. The mechanisms described in this specification are based on the *STIR Out-of-Band Architecture and Use Cases* defined in [draft-ietf-stir-oob] and *Out-of-Band STIR for Service Providers* in [draft-peterson-stir-servprovider-oob].

## Purpose

The current SHAKEN framework provides a set of tools that enable verification of the calling party's authorization to use a calling telephone number for a call. 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.

In today’s PSTN, and for the foreseeable future, the Identity header may fail to arrive at the terminating service provider’s (TSP’s) network for verification by their STI-VS.

Out-of-band STIR/SHAKEN remedies this by sending the PASSporT to the TSP separately, out-of-band, through implementation of a Call Placement Service (CPS) described in this document. All other STIR/SHAKEN steps for authentication, use of PKI, and verification remain the same.

# 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-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

draft-ietf-stir-oob-007, *STIR Out-of-Band Architecture and Use Cases.* 1

draft-peterson-stir-servprovider-oob-00, *Out-of-Band STIR for Service Providers*. 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

The following provides some key definitions used in this document.

**(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.

**Call Placement Service (CPS):** A device that can receive a SHAKEN PASSporT from a call source, for retrieval by the call destination’s STI-VS. (draft-ietf-stir-oob-07)

**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]. (see Operating Company Number)

**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].

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

**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].

**Root CA:** A CA that is directly trusted by an end-entity.

**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 U.S. 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].

**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.

**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  |

# Overview

## Problem Statement – Why OOB-SHAKEN is needed

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.

Not all telephone calls use SIP signaling. Some calls use SIP for only part of their signaling path. Some IP network equipment and software do not reliably deliver large SIP header fields end-to-end.

Although desirable, the underlying economic realities slow the transition of the PSTN from its current state to a future state where SHAKEN PASSporTs can be carried reliably from end-to-end.

Meanwhile, requirements for call authentication are on a much faster pace. Legislation has been signed into law to require STIR/SHAKEN in VoIP networks and reasonable measures for call authentication in non-IP networks.

There is a timing mismatch between the requirement for call authentication versus the readiness of the network to accommodate end-to-end SIP signaling. This mismatch will create a situation where some consumers get the benefits of call authentication while others cannot.

Out-of-band STIR/SHAKEN addresses this mismatch. It provides another way to transmit PASSporTs, while everything else about STIR/SHAKEN remains the same. It works with today’s telephone network and provides a way to give all service providers access to STIR/SHAKEN so they can more quickly deliver the benefits of call authentication to their customers.

Network upgrades from the legacy SS7/TDM infrastructure to a SIP infrastructure will continue at a pace that makes sense given the underlying economic and regulatory realities. Meanwhile, out-of-band STIR/SHAKEN provides a complementary approach to more broadly deliver the benefits of call authentication today.

## OOB-STIR Overview

Out-of-band STIR is described in an IETF draft, *STIR Out-of-Band Architecture and Use Cases*. It describes a method of sending SHAKEN PASSporTs to a *Call Placement Service* (CPS), which is a rendezvous place to send, temporarily store, and retrieve PASSporTs, as follows:

1. The originating service provider creates a PASSporT using normal STI-AS methods and the SHAKEN PKI.
2. Using the public key of the terminating service provider, the originating service provider encrypts the PASSporT and sends it to the CPS used by the terminating service provider.
3. When the terminating service provider receives a call, they check their CPS and fetch any PASSporTs that may be present for the call. They use their private key to decrypt the PASSporTs and continue with the usual STI-VS methods.

The following diagram presents the SHAKEN architecture, defined in ATIS 1000074-E, with the addition of a CPS. The STI-AS POSTs the PASSporT to the CPS and the STI-VS GETs the PASSporT from the CPS.



Figure 1. SHAKEN Architecture with OOB STIR

In the above referenced IETF draft, the CPS has an open, public interface for sending and receiving PASSporTs. Anyone can send PASSporTs to the CPS using an HTTP POST, and anyone can fetch PASSporTs from the CPS using an HTTP GET. This is why the originating service provider encrypts the PASSporT using the terminating service provider’s public key. The terminating service provider then uses their private key to decrypt the PASSporT. Thereby, nobody else can read this PASSporT.

A public HTTP GET interface, however, introduces a requirement that the CPS provide an encrypted PASSporT for every request, even if a PASSporT was never sent for a call. This means that, in some cases, the CPS must create an encrypted dummy PASSporT.

A considerable portion of the draft IETF deals with the complexities introduced by having an open public HTTP GET interface to read PASSporTs and the associated privacy and security issues.

Since its original conception, a simpler approach has been developed, called Out-of-Band SHAKEN. This approach retains the concept of a CPS and the public interface to send PASSporTs to it using HTTP POST.

However, with out-of-band SHAKEN, each service provider has its own CPS. Therefore, the CPS does not have an open public interface to fetch records using HTTP GET. This approach, described in the next section, addresses the privacy and security issues associated with an open public HTTP GET interface and simplifies the design considerably.

# OOB-SHAKEN

Out-of-Band (OOB) SHAKEN is a specific use case of the OOB STIR draft, which defines a Call Placement Service (CPS) being used as a public service. This is the most general, and challenging, use case for OOB STIR. The OOB STIR draft includes the following important note:

*Potential implementors should note that this document merely defines the operating environments in which this out-of-band STIR mechanism is intended to operate. It provides use cases, gives a broad description of the components and a potential solution architecture. Various environments may have their own security requirements: a public deployment of out-of-band STIR faces far greater challenges than a constrained intra-network deployment.[[3]](#footnote-4)*

This section describes a simplified out-of-band mechanism to transmit and store PASSporTs in a CPS. Implementation of OOB SHAKEN is significantly simpler and less challenging than OOB STIR for two reasons:

1. From a trust perspective, OOB SHAKEN is a “constrained intra-network deployment” since it is limited to service providers that have been approved by a recognized authority, such as the STI-PA.
2. In the OOB SHAKEN architecture, The HTTP POST interface to send PASSporTs to the CPS is open and public, while the HTTP GET interface to retrieve PASSporTs is private, secure and limited to the terminating service provider who is assigned the called number.

## OOB-SHAKEN Architecture

The following diagram shows the SHAKEN architecture defined in ATIS 1000074-E with the addition of a Call Placement Service (CPS) for OOB SHAKEN deployed by Service Provider B, the call termination service provider. The CPS is deployed at the edge of Service Provider B’s network with a public interface to receive SHAKEN PASSporTs Out-of-Band from Service Provider A via an HTTPS POST message as defined by the OOB STIR IETF draft.

Before the PASSporT is persisted, the TSP’s CPS verifies it as described in ATIS 1000074-E (except for checking that the values match the SIP INVITE) to confirm the PASSporT was generated by an approved participating service provider within the SHAKEN ecosystem using a valid SHAKEN certificate.

The interface for the STI-VS to retrieve a SHAKEN PASSporT from the CPS is private. The protocol for the STI-VS connection to the CPS is specifically not defined because it is only used internally within a service provider’s network. The HTTPS GET message as defined in the OOB STIR IETF draft may be used by the STI-VS to retrieve PASSporTs but is not required.



Figure 2. SHAKEN Architecture with OOB SHAKEN CPS

Direct integration of the CPS with the STI-VS is the key design difference between OOB STIR and OOB SHAKEN. This explicit trust relationship between the CPS and STI-VS enables TSPs to optimize the implementation of their CPS infrastructure.

## OOB SHAKEN Call Flow Ladder

The following call flow is the basic OOB SHAKEN use case. The SHAKEN PASSporT is sent both via in-band SIP signaling and out-of-band to the terminating service provider.



Figure 3. OOB SHAKEN Call Ladder

**Call Flow Details**

1. INVITE from SIP User Agent to CSCF of the originating service provider received.
2. CSCF uses either SIP or REST to obtain a signed SHAKEN PASSporT from the STI-AS.
3. STI-AS simultaneously creates and sends a signed SHAKEN PASSporT to the CPS of the terminating service provider and also returns a signed SHAKEN PASSporT to the CSCF using either SIP or REST.
4. CSCF sends SIP INVITE to the MGCF.
5. CPS returns a HTTP 201 response code to the STI-AS. The timing of this response has no impact on call processing by the STI-AS or CSCF.
6. MGCF of the originating service provider sends a call setup message to the MGCF of the terminating service provider.
7. MGCF of the terminating service provider sends a SIP INVITE to the CSCF.
8. CSCF uses either SIP or REST to obtain the verification result from the STI-VS.
9. STI-VS queries the CPS for a PASSporT received out-of-band for this call. In an event that the STI-VS receives a different PASSporT in-band and out-of-band, it uses local policy to determine which PASSporT to use.
10. STI-VS returns the verification result (e.g., verstat parameter) to the CSCF using either SIP or REST.
11. CSCF completes the call to terminating SIP User Agent.

## Example of OOB SHAKEN HTTP POST

The following message is an example of an HTTP POST to a CPS.

POST /cps/company/1234 HTTP/1.1

Content-Type: application/passport

Content-Length: 487

Host: cps.transnexus.com

eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9jZXJ0aWZpY2F0ZXMuY2xlYXJpcC5jb20vNGE4NzFjMDYtZTBiNS00Y2I5LTgzNDctNDMxMjZiZDg2Yzg1LzY0NmIxYmUzNzNmMTZlYWY4NzUzNzk5ZTM0OTkwMzJhLmNydCJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyIxOTAzMjQ2OTEwMyJdfSwiaWF0IjoxNTg0OTgzNDAyLCJvcmlnIjp7InRuIjoiMTIwMTM3NzYwNTEifSwib3JpZ2lkIjoiNGFlYzk0ZTItNTA4Yy00YzFjLTkwN2ItMzczN2JhYzBhODBlIn0.EMfXHyowsI5s73KqoBzJ9pzrrwGFNKBRmHcx-YZ3DjPgBe4Mvqq9N-bThN1\_HTWeSvbruAyet26fetRL1\_bn1g

The body contains the same PASSporT that is transmitted in-band via SIP signaling per the normal STIR/SHAKEN standards. The connection between the STI-AS and CPS must use be secured using TLS.

# CPS Discovery

OOB SHAKEN defines a model with one Call Placement Service (CPS) per terminating service provider. The STI-AS of the originating service provider must be able to discover the publicly accessible URL of the terminating service provider’s CPS. CPS discovery requires a mapping of the called party digits into a portability-corrected Operating Company Number (OCN) which is then used to identify the URL of the terminating service provider’s CPS. The mapping of OCN to CPS URL must be handled in a trusted and authoritative fashion. Multiple implementation models are possible to achieve this trusted CPS discovery service. The STI-PA, for example, is a logical party to fulfill this role with minimal incremental effort.

The following diagram, recreated from ATIS 1000084-E, summarizes the roles and responsibilities associated with the STI-PA, including the interfaces to other functional elements. This version of the diagram, however, includes the additional function of providing accurate CPS discovery. The two additions to the diagram are noted in bold text: 1) **CPS URL** provisioned by the service provider and 2) the **Mapping of OCNs to CPS URLs** published by the STI-PA.



Figure 4. Expanded STI-PA Roles and Responsibilities

The process for the STI-PA to provide accurate route discovery requires the following steps:

1. The service provider manually provisions their CPS URL for each of their OCNs to the STI-PA.
2. The STI-PA publishes the mapping of OCN to CPS URLs for all service providers.

## Format of OCN and CPS Address List

The CPS list is published via an API in the same way the STI-PA publishes the list of approved Certification Authorities (CAs). The STI-PA generates a JSON web PASSporT containing the CPS mapping data. The PASSporT is signed using the STI-PA’s private key. A sample JWT header and body are below.

Header:

{

 "alg": "ES256",

 "typ": "JWT",

 "x5u": "https://sti-pa.com/download/v1/certificate/certificateId\_1.crt"

}

Payload:

{

 "version": "1.0",

 "sequence": 1,

 "exp": 1590000000,

 "cpsMapping": {

 "1234": "https://example.com/cps/company/1234",

 "5678": "https://example.com/cps/company/5678"

 }

}

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)
3. draft-ietf-stir-oob-007, *STIR Out-of-Band Architecture and Use Cases* [↑](#footnote-ref-4)