ATIS-0x0000x

ATIS Standard on

**Technical Report on Alternatives for Caller Authentication for Non-IP Traffic**

**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 Technical Report considers scenarios where SIP connectivity is not available end-to-end (i.e., “non-IP” scenarios) and identifies potential mechanisms for to determine that the calling user is authorized to use the calling telephone number.

**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 References 1

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 3

4 Overview 5

4.1 Problem Statement 5

4.2 Objective 5

4.3 Evaluation of Non-IP Call Authentication Mechanisms 5

5 Non-IP Scenarios 5

5.1 TDM => SIP 5

5.2 SIP => TDM 6

5.3 SIP => TDM => SIP 6

5.3.1 SIP => TDM Transport 6

5.3.2 TDM Transport => SIP 6

# Scope, Purpose, & Application

## Scope

This Technical Report is limited to scenarios that cannot use the currently defined STIR/SHAKEN framework to confirm that the calling party has the right to use the calling number.

## 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 the Identity header may fail to arrive at the terminating service provider’s (TSP’s) network for verification by their STI-VS because the call does not have SIP end-to-end.

This Technical Report identifies non-IP scenarios and provides a framework for evaluation of potential mechanisms that could provide caller authentication even when the call is not SIP end-to-end.

*Note: This Technical Report may include Appendices that describe some possible mechanisms.*

# References

The following standards contain provisions which, through reference in this text, constitute provisions of this Technical Report. 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 a 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

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 end-to-end. Some calls use SIP for only part of their signaling path, and some calls that originate and terminate as SIP may have non-IP signaling for part of the path.

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.

STIR/SHAKEN is based on a well-defined scenario - SIP end-to-end. Evaluating non-IP is not as simple, since there are many different things that could disrupt the end-to-end SIP path. The Originating Service Provider (OSP) could have a TDM network, the Terminating Service Provider (TSP) could have a TDM network, or one or more TDM transport links could be used to interconnect a SIP-based OSP and TSP. Each of these scenarios could have a different architecture and requirements. Therefore, it is important to consider each separately to determine if/how call authentication can be provided in a way that complements STIR/SHAKEN.

## Objective

The objective of this Technical Report is to do the following:

* Provide architectural descriptions of non-IP scenarios that do not support SIP end-to-end.
* Identify mechanisms that could potentially provide call authentication for these non-IP scenarios.
* Propose factors that could be considered when evaluating mechanisms for providing call authentication for non-IP connections.

## Evaluation of Non-IP Call Authentication Mechanisms

The following principles should be considered when evaluating mechanisms for providing call authentication where end-to-end SIP is not available:

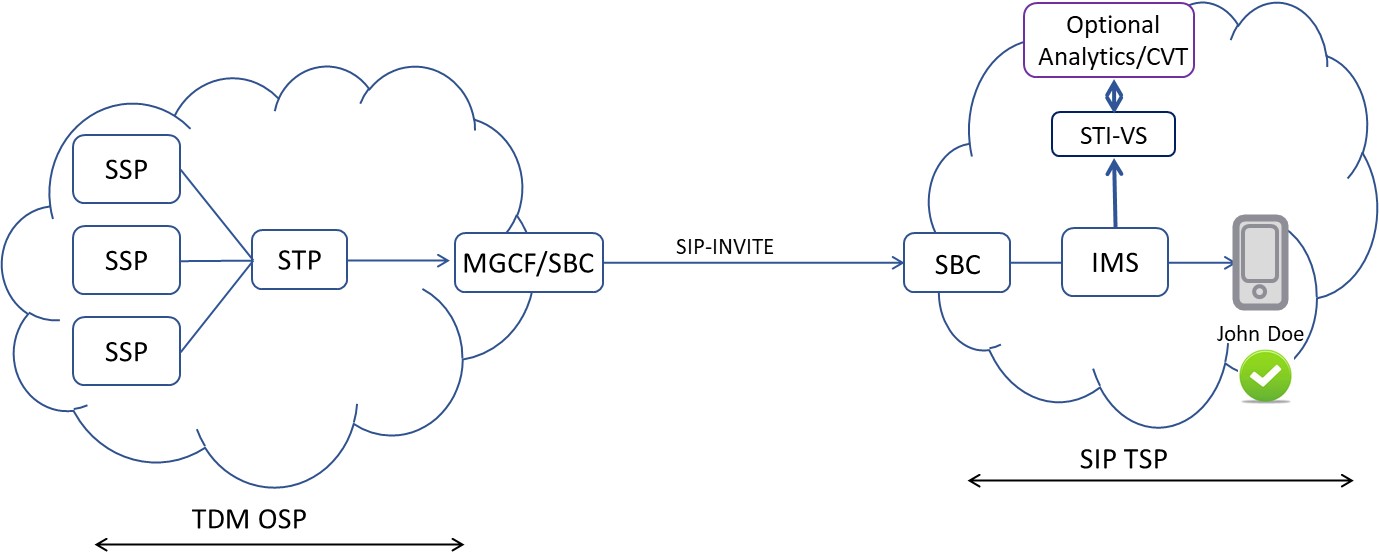
* Should support “call authentication” for TDM service providers
* Should support hybrid-technology calls:
  + SIP => TDM
  + TDM => SIP
  + SIP => TDM => SIP
* Should not impede transition to all-IP (e.g., no lingering functionality or disincentives for completing the transition)
* Complement SHAKEN, rather than duplicate or compete. This would include things like:
  + Use standard SHAKEN PASSporT
  + Interwork with SHAKEN
  + Ideally any approach would be transparent to SIP networks that have implemented SHAKEN, and would not require additional functionality to accommodate non-IP mechanisms.
* Whenever possible, the “cost causer” should be the “cost payer”
  + This is a well-established IP-NNI principle that should be considered when evaluating mechanisms.
* Should support extension to full international deployment. ATIS-1000074 did not consider international deployment for valid reasons, but today it is clear that full international interoperability will be critical for success of any mechanism for non-IP traffic.

# Non-IP Scenarios

This Technical Report identifies scenarios that do not have end-to-end SIP connectivity.

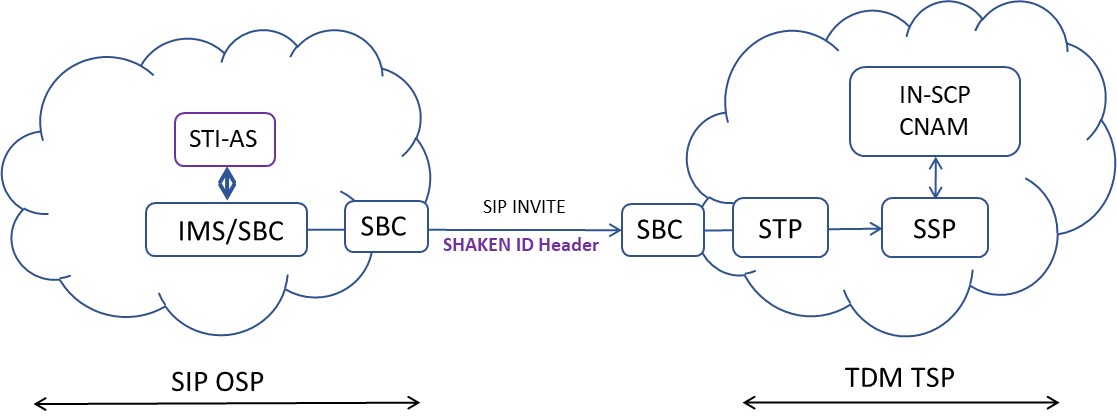
## TDM => SIP

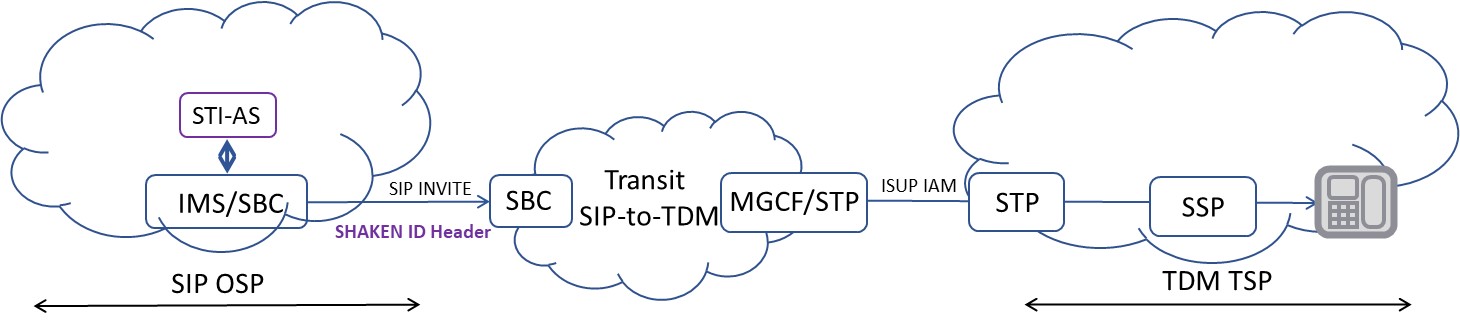
This section describes scenarios where the OSP is TDM-based and the TSP is SIP-based.



## SIP => TDM

This section describes scenarios where the OSP is SIP-based and the TSP is TDM-based.



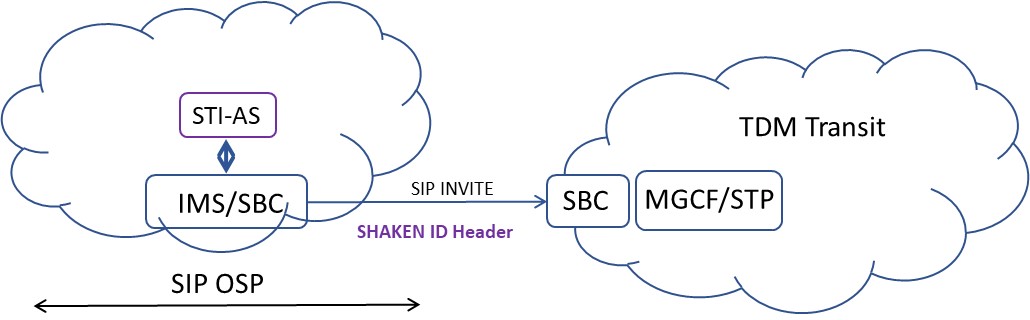


## SIP => TDM => SIP

This section describes scenarios where the OSP and TSP are both SIP-based but one or more transport links are TDM-based. For analysis, this is divided into two sub-sections.

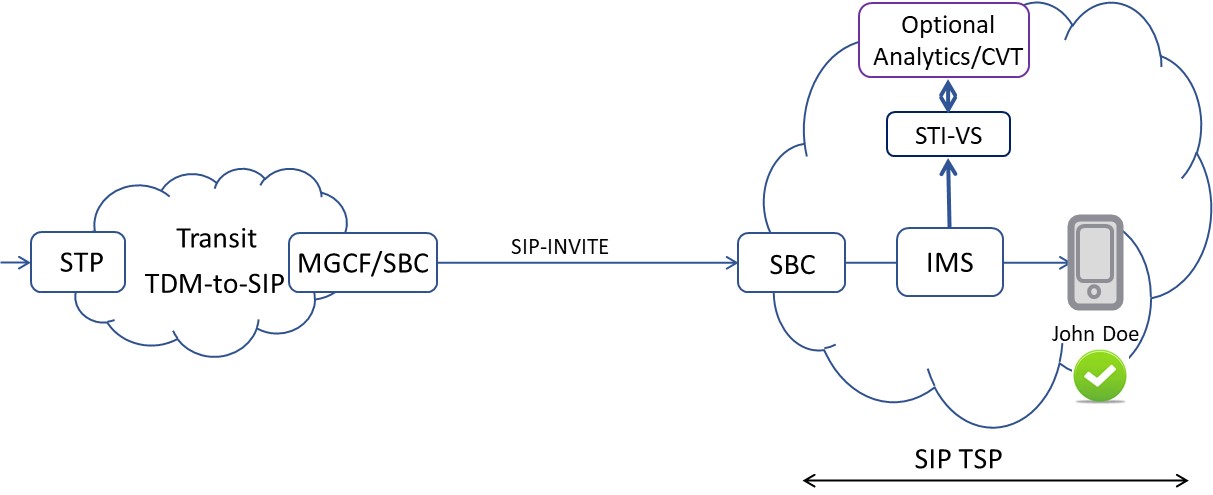
### SIP => TDM Transport

This section describes scenarios where the OSP is SIP-based and the transport network is TDM-based.



### TDM Transport => SIP

This section describes scenarios where the transport network is TDM-based, and the TSP is SIP-based.



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)