ATIS-0x0000x

ATIS Standard on

**Extending STIR/SHAKEN over TDM Interconnects**

**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 transferring verified attestation levels over TDM interconnects.

**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 2

4 STIR/SHAKEN Extension over TDM Interconnect 4

4.1 Overview 4

4.2 Procedures 5

4.3 Backward Traceability 6

4.4 Diversion Impact 6

4.5 Support For Other Claim Types 6

4.6 Security Concerns 6

4.7 Deployment Models 7

Error! Bookmark not defined.**Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| April 24, 2020 | Initial | Baseline | Tolga Asveren |
| May, 14, 2020 | v1 | Added information about authentication fidelity and support for different claim types | Tolga Asveren |

# Scope, Purpose, & Application

## Scope

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 transferring verified attestation levels over TDM interconnects.

## 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. It assumes that SIP Identity header can be carrier end-to-end between Originating and Terminating Service Providers. This, currently, is not always possible due to existence of TDM interconnects at various stages of signaling path.

The mechanisms described in this document address this problem by carrying verified attestation level over TDM interconnects.

# 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.

**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].

**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].

## Acronyms & Abbreviations

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

# STIR/SHAKEN Extension over TDM Interconnect

## Overview

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. It assumes that SIP Identity header can be carrier end-to-end between Originating and Terminating Service Providers. This, currently, is not always possible due to existence of TDM interconnects at various stages of signaling path.

The mechanisms described in this document address this problem by carrying verified attestation level over TDM interconnects.

The mechanism relies on bilateral agreements and transitive trust between operators on each end of a TDM interconnect. The nature of the agreement and whether there is an agreement at all is on a per TDM interconnect basis. Therefore, it is flexible in terms of its applicability. It covers all types of TDM interconnects as the agreement is only between operators directly connected. An operator may choose to have a different agreement or no agreement separately on each of its TDM interconnects. This allows partial upgrades and does not require any universal agreements. It also covers cases where several TDM interconnects need to be traversed.

Operator-A

Operator-B

Attestation signaled

by mechanism X

Attestation signaled

by mechanism Y

Attestation not signaled

Operator-D

Operator-C

Attestation signaled

by mechanism Z

Figure Use of different agreements among Operators

Operator-D

Operator-C

Operator-B

Operator-A

attestation=X

signaled over

TDM Interconnect

INVITE

(Identity,

attestation=X)

attestation=X

signaled over

TDM Interconnect

INVITE

(Identity, attestation=X)

Figure Carrying Attestation over multiple TDM Interconnects

STIR/SHAKEN relationship is terminated/re-generated on two ends of the TDM interconnect. The side terminating STIR/SHAKEN relationship signals the verified attestation level to the side re-generating it. The other side then re-generates it by using the received attestation level and its own private key. Each STIR/SHAKEN relationship can be considered as a separate “STIR/SHAKEN leg”.

STI-AS

STI-VS

HTTPS

Verification Response

with verified attestation

HTTPS

Verification Request

HTTPS

Signing Reply

HTTPS

Signing Request

Operator-B

Operator-A

INVITE

(Identity, attestation=X)

attestation=X signaled over

TDM Interconnect

INVITE

(Identity, attestation=X)

STIR/SHAKEN Leg-B

STIR/SHAKEN Leg-A

Figure Extending STIR/SHAKEN over TDM Interconnect Architecture with Multiple STIR/SHAKEN Legs

## Procedures

STIR/SHAKEN defines three attestation levels as A, B, C. Considering also the possibility of no Identity header, i.e. no attestation, there are in total 4 different values. These 4 values should signaled over a TDM interconnect. This can be achieved by two high level methods:

* Use 2 bits in the TDM signaling to encode the value
* Use a different TG for a particular value
* TDM Signaling Based Model

In this model the 4 different values need to be signaled as 2 bits in TDM signaling. For example, that can be achieved by making use of ISUP Screening Indicator Parameter as follows:

00 used for no Identity header received

01 used for A

10 used for C

11 used for B

It should be noted that any other parameter/bit, e.g. spare bits (H/B) of Access Delivery Information parameter, spare bits in the second octet of Called Party Parameter, spare bits of Call Reference etc…can be used for this purpose as long as the two ends of the TDM interconnect agree on their use and the meaning they represent.

* TG Based Model

In this model, a different TG would be used based on the verified attestation level. For example, TG-1 for “No Identity header received”, TG-2 for “A”, TG-3 for “B” and TG-4 for “C”.

Two operators may agree on signaling only a subset of values, e,g., “No Identity received” and “A”.

The following procedural steps are followed:

* The operator terminating STIR/SHAKEN leg verifies the Identity header in the INVITE request.
* If it validates successfully, it signals the verified attestation value over TDM Interconnect based on the model agreed with the operator at the other end of TDM Interconnect.
* The operator re-generating STIR-SHAKEN leg generates a new Identity header with attestation level it received over TDM Interconnect by using its own private key.

## Backward Traceability

The mechanism terminates-re-generates STIR/SHAKEN relationship but still allows for full backward traceability. On each STIR/SHAKEN leg, STIR/SHAKEN backward traceability procedures are applicable. The two SRIT/SHAKEN legs would be tied to each other through CDR backtracing. It should be noted that there are also attack/error scenarios applicable in an end-to-end STIR/SHAKEN model which still require CDR based backtracing, e.g. corrupted origination-id in the PassPORT claim.

## Diversion Impact

Verification of Identity header(s) at the STIR/SHAKEN applies to all claims/extensions at the STIR/SHAKEN termination. Therefore, div extension claims will be verified as well. Whether only Identity(shaken) or also Identity(div) headers based on TDM signaling diversion information needs to be generated is determined based on bilateral agreement. If verified diversion chain is used to populate TDM signaling diversion information during STIR/SHAKEN termination then Identity(div) may be generated during STIR/SHAKEN re-generation.

## Support For Other Claim Types

The hop-by-hop agreement characteristic of the mechanism makes it suitable to utilize ISUP parameters supporting additional claim types in a flexible way.

rph claims can be supported by using the ISUP Calling Party’s Category parameter.

“nam” key of rcd claim can be supported by using the Display Name Information parameter.

“crn” claim, if used to provide information about the type of the call, e.g. telemarketing, political, survey, public-service, can be supported by making use of the ISUP Originating Line Identifier field. Any categories, which do not correspond to an already defined value, may be supported by using spare values based on bilateral agreement between the operators.

In general, ISUP User-to-User Information parameter may be used for any claim type as long as the required size does not exceed limits (131 octets).

## Security Concerns

The mechanism relies on STIR/SHAKEN security principles on each STIR/SHAKEN leg and transitive trust on TDM interconnect between two operators.

Original STIR/SHAKEN authentication is verified at the STIR/SHAKEN Leg-A. The result of this verification is signaled over trusted TDM interconnect. The signaled value is used to re-construct the verified authentication level at the STIR/SHAKEN Leg-B. As such, the original authentication information is not lost and used verbatim.

## Deployment Models

Existing GW equipment at TDM interconnects may/may not have the capability/flexibility to apply the procedures associated with this mechanism. Lack of functionality support in GWs may be overcome by performing them in front-end/back-end entities. For example, a front-ending SIP entity may verify Identity(shaken) signature, remove it and populate ISUP MIME body with corresponding parameter values. Similarly, at the other end of TDM interconnect, a back-end entity may receive INVITW with ISUP MIME, which has verified attestation level encoded in a parameter, and generate an Identity(shaken) header based on it.

Similarly, a front-end entity may insert trunk-context/tgrp parameters to an INVITE to guide the FW for its selection of the TG on the TDM interconnect. Such a front-end entity would populate tgrp parameters based on the verified attestation value.

If and how to use front-end/back-end entities to support these procedures does not require any coordination among operators. It is a decision to be made/applied purely in an operator’s own domain.

INVITE

(Identity, attestation=X)

SIP Entity

attestation=X signaled over

TDM Interconnect

INVITE

(ISUP MIME with relevant

Parameter set to the value

representing attestation level X

STI-VS

HTTPS

Verification Request

HTTPS

Verification Response

with verified attestation

GW

dfgdgg

Figure SIP Front-End Entity Populating ISUP MIME Parameter for Attestation

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