**ATIS-0x0000x**

ATIS Standard on

**Best Current Practices on the protection of STIR/SHAKEN data between service providers and from service providers to enterprises**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This Recommendation explores requirements for, and mechanisms of, data exchange between service providers and from service providers to enterprises in the context of the STIR/SHAKEN framework. This Recommendation describes an industry level consensus on how those data elements should be protected in transit.

**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, IP NNI , which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The ATIS SIP Forum **IPNNI**  Joint Task Force Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| March 15m 2019 | 1.0 |  | Richard Shockey |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

* The STIR/ SHAKEN framework provides an attestation level for a call, providing a baseline level of trust of the TN making the call. In other words, if a call is fully attested the recipient may be reasonably certain the calling TN is not being spoofed and was generated legally.
* The STIR/SHAKEN framework does not provide a model for how enterprise SIP based services may consume or portray intent, user identification, and/or surrounding context of a call. The verification data and well as data analytics generated by the framework could be mission critical to multiple industries including financial services, health care, consumer services, and utilities.
* This Recommendation outlines the agreement among service providers that the data generated by the STIR/SHAKEN framework must not be altered in transit in any way shape or form unless specified under specific and defined use cases. This includes all existing and future PASSport definitions as well as VERSTAT parameters.
* This Recommendation outlines the agreement among terminating service providers that all the data generated by the STIR/SHAKEN framework should be passed to the User Agent, PBX, UCaaS, or Enterprise centric provider intact and without alteration unless specified under specific and defined use cases. This includes all existing and future PASSport definitions as well as VERSTAT parameters.

## Use Case Inter Service Provider

Alteration of the STIR/SHAKEN data by intermediary providers would negate the purpose and function of the Framework.

## Use Case Enterprise

It stands to reason there is a marketplace for data analytics collected by service providers, and/or their analytics partners, to be delivered to the enterprise. Enterprise may choose to apply different forms of data analyitics specific to their own industry and apply data it has collected in the data mix necessary to score the call for validity. It also stands to reason there is value for enterprises to provide information to service providers to be passed along to a call’s originator. [TBD]

[What Framework elements do the enterprises need want?]

## Requirements

## Existing Statutory Examples

Existing regulatory constructs have traditionally provided a framework for securing call signaling between service providers for the protection of data necessary to bill for a call. The classic example has been securing the data in either TDM or SIP network necessary for Call Billing specifically the calling party's charge number (CN).

47 USC §64.1601   Delivery requirements and privacy restrictions.

    (a) Delivery. Except as provided in paragraphs (d) and (e) of this section:

    (1) Telecommunications carriers and providers of interconnected Voice over Internet Protocol (VoIP) services, in originating interstate or intrastate traffic on the public switched telephone network (PSTN) or originating interstate or intrastate traffic that is destined for the PSTN (collectively “PSTN Traffic”), are required to transmit for all PSTN Traffic the telephone number received from or assigned to or otherwise associated with the calling party to the next provider in the path from the originating provider to the terminating provider. This provision applies regardless of the voice call signaling and transmission technology used by the carrier or VoIP provider. Entities subject to this provision that use Signaling System 7 (SS7) are required to transmit the calling party number (CPN) associated with all PSTN Traffic in the SS7 ISUP (ISDN User Part) CPN field to interconnecting providers, and are required to transmit the calling party's charge number (CN) in the SS7 ISUP CN field to interconnecting providers for any PSTN Traffic where CN differs from CPN. Entities subject to this provision who use multi-frequency (MF) signaling are required to transmit CPN, or CN if it differs from CPN, associated with all PSTN Traffic in the MF signaling automatic numbering information (ANI) field.

    (2) Intermediate providers within an interstate or intrastate call path that originates and/or terminates on the PSTN must pass unaltered to subsequent providers in the call path signaling information identifying the telephone number, or billing number, if different, of the calling party that is received with a call. This requirement applies to SS7 information including but not limited to CPN and CN, and also applies to MF signaling information or other signaling information intermediate providers receive with a call. This requirement also applies to VoIP signaling messages, such as calling party and charge information identifiers contained in Session Initiation Protocol (SIP) header fields, and to equivalent identifying information as used in other VoIP signaling technologies, regardless of the voice call signaling and transmission technology used by the carrier or VoIP provider.

    (b) Privacy. Except as provided in paragraph (d) of this section, originating carriers using Signaling System 7 and offering or subscribing to any service based on Signaling System 7 functionality will recognize \*67 dialed as the first three digits of a call (or 1167 for rotary or pulse dialing phones) as a caller's request that the CPN not be passed on an interstate call. Such carriers providing line blocking services will recognize \*82 as a caller's request that the CPN be passed on an interstate call. No common carrier subscribing to or offering any service that delivers CPN may override the privacy indicator associated with an interstate call. Carriers must arrange their CPN-based services, and billing practices, in such a manner that when a caller requests that the CPN not be passed, a carrier may not reveal that caller's number or name, nor may the carrier use the number or name to allow the called party to contact the calling party. The terminating carrier must act in accordance with the privacy indicator unless the call is made to a called party that subscribes to an ANI or charge number based service and the call is paid for by the called party.

    (c) Charges. No common carrier subscribing to or offering any service that delivers calling party number may

    (1) Impose on the calling party charges associated with per call blocking of the calling party's telephone number, or

    (2) Impose charges upon connecting carriers for the delivery of the calling party number parameter or its associated privacy indicator.

    (d) Exemptions. Section 64.1601(a) and (b) shall not apply when:

    (1) A call originates from a payphone.

    (2) A local exchange carrier with Signaling System 7 capability does not have the software to provide \*67 or \*82 functionalities. Such carriers are prohibited from passing CPN.

    (3) A Private Branch Exchange or Centrex system does not pass end user CPN. Centrex systems that rely on \*6 or \*8 for a function other than CPN blocking or unblocking, respectively, are also exempt if they employ alternative means of blocking or unblocking.

    (4) CPN delivery—

    (i) Is used solely in connection with calls within the same limited system, including (but not limited to) a Centrex system, virtual private network, or Private Branch Exchange;

    (ii) Is used on a public agency's emergency telephone line or in conjunction with 911 emergency services, on a telephone line to contact non-public emergency services licensed by the state or municipality, or on any entity's emergency assistance poison control telephone line; or

    (iii) Is provided in connection with legally authorized call tracing or trapping procedures specifically requested by a law enforcement agency.

    (e) Any person or entity that engages in telemarketing, as defined in section 64.1200(f)(10) must transmit caller identification information.

    (1) For purposes of this paragraph, caller identification information must include either CPN or ANI, and, when available by the telemarketer's carrier, the name of the telemarketer. It shall not be a violation of this paragraph to substitute (for the name and phone number used in, or billed for, making the call) the name of the seller on behalf of which the telemarketing call is placed and the seller's customer service telephone number. The telephone number so provided must permit any individual to make a do-not-call request during regular business hours.

    (2) Any person or entity that engages in telemarketing is prohibited from blocking the transmission of caller identification information.

    (3) Tax-exempt nonprofit organizations are not required to comply with this paragraph.

    (f) Paragraph (b) of this section shall not apply when CPN delivery is made in connection with a threatening call. Upon report of such a threatening call by law enforcement on behalf of the threatened party, the carrier will provide any CPN of the calling party to law enforcement and, as directed by law enforcement, to security personnel for the called party for the purpose of identifying the party responsible for the threatening call.

    (g) For law enforcement or security personnel of the called party investigating the threat:

    (1) The CPN on incoming restricted calls may not be passed on to the line called;

    (2) Any system used to record CPN must be operated in a secure way, limiting access to designated telecommunications and security personnel, as directed by law enforcement;

    (3) Telecommunications and security personnel, as directed by law enforcement, may access restricted CPN data only when investigating phone calls of a threatening and serious nature, and shall document that access as part of the investigative report;

    (4) Carriers transmitting restricted CPN information must take reasonable measures to ensure security of such communications;

    (5) CPN information must be destroyed in a secure manner after a reasonable retention period; and

    (6) Any violation of these conditions must be reported promptly to the Commission.

    [60 FR 29490, June 5, 1995; 60 FR 54449, Oct. 24, 1995, as amended at 62 FR 34015, June 24, 1997; 68 FR 44179, July 25, 2003; 71 FR 75122, Dec. 14, 2006; 76 FR 73882, Nov. 29, 2011; 82 FR 56917, Dec. 1, 2017]

    Effective Date Note: At 82 FR 56917, Dec. 1, 2017, §64.1601 was amended by revising paragraphs (d)(4)(ii) and adding paragraph (f). These paragraphs contain information collection and recordkeeping requirements and will not become effective until approval has been given by the Office of Management and Budget.

xxx

# 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 SHAKEN Framework -

# 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

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations

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

# (normative/informative)

# A Annex Title

Xxx