**ATIS-0x0000x**

ATIS Standard on

**Signature-based Handling of Asserted Information Using Tokens**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

Signature-based Handling of Asserted information using Tokens (SHAKEN) is an industry framework for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing end-to-end cryptographic authentication and validation of the telephone identity and other information in a VoIP-based service provider network. This specification defines the framework for telephone service providers to create signatures in SIP and will define the Network-to-Network Interface (NNI) requirements, Network Elements, the X.509 certificate framework to validate the initiator of the signature, and the various classes of signers and how the validation of a signature can be used on the PSTN toward the mitigation of illegitimate use of the PSTN and protecting users of the PSTN.

**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, [**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** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope & Purpose

## Scope

This document is intended to provide telephone services providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls on the Public Switched Telephone Network (PSTN) and the mitigation of illegitimate spoofing of telephone identities on the PSTN.

## Purpose

Using the protocols defined in draft-ietf-stir-rfc4474bis-06 and draft-wendt-verified-token, this document will define the service provider framework around usage of the identity header and JWT tokens in SIP. This will include definition of a framework for managing service provider certificates for signing the relevant SIP header information defined in 4474bis and/or verified token. It will also define how the signed information should be carried across the telephone service provider NNI to other peering service providers. It will also specify how the positive or negative verification of the signature at the terminating service provider may be used to help mitigate illegitimate telephone identity.

# 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-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

# 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 |
| NNI | Network-to-Network Interface |
| PSTN | Public Switched Telephone Network |
| STI | Secure Telephone Identity |
| VoIP | Voice over Internet Protocol |

# Secure Telephone Identity Overview

Assertion of telephone identity on the PSTN between peering service providers particularly in a 3GPP IMS environment has typically used the P-Asserted-ID. This usage assumes trust between peering providers to believe the asserted caller-id in the P-Asserted-ID header. However, in many call scenarios where there are indirect relationships between the originating telephone service provider and the terminating provider, these trust relationships may not be able to be maintained. Secure Telephone Identity and the usage of cryptographic signatures to prove with non-repudiation the origination of a signed identity can be a tool used in the mitigation of fraudulent usage of caller-id to trick consumers.

The documents draft-ietf-stir-rfc4474bis-06 and draft-wendt-verified-token define a set of tools that can be used in the SIP protocol for applying these cryptographic signatures. This can provide many purposes depending on who the originator of the call is and what the relationship is to the authenticating provider who signed the call.

The following shows a simple call flow between two peering providers.



Figure : Title

More to follow…

# Management of Service Provider Certificates

## Telephone Number Authority Trust Anchor

Xxx

## Certificate Signing

### Traditional CSR

Xxx



Figure : Title

### ACME based Certificate Management

Proposal to use the draft-ietf-acme-acme defined protocol for automated certificate signing.

# End-to-End Call and NNI Considerations for STI

## Call Scenario Use Cases

### Verification of Calling Party Telephone Identity

### Verification of Originating Service Provider

### Verification of Transit Service Provider

### Verification of ETS Provider

### Verification of SMS Messaging Identity

### Verification of Identity for other SIP Methods

## Legitimate Spoofing Use Cases

## Verification of Transit Service Provider

# Call Validation Treatment

## Signature Verified Scenarios

[The following four scenarios copied from Pierce Gorman in a message to STIR mailing list:]

### Carrier signed, authenticated CgPN

Use case example(s): Bread-and-butter 95%+ of calls from subscriber lines (IMS-based and otherwise).

Trust Estimate: Carrier\_orig trustworthy, CgPN most trustworthy.

### Carrier signed, semi-authenticated CgPN

Use case example(s): Number block delegated from OCN, but no per-TN screen (SIP trunks).

Trust Estimate: Carrier\_orig trustworthy, CgPN less than most trustworthy but not entirely untrustworthy.

### Carrier signed, no authentication of CgPN

Use case example(s): E911 on visited network w/o roaming agreement, manual roaming.

Trust Estimate: Carrier\_orig trustworthy, CgPN entirely untrustworthy.

### Untrusted Originator

Use case example(s): Pre-IMS, legacy circuit-switched networks that don't natively support SIP or which don't choose to sign calls (e.g., international carriers).

Trust Estimate: Good luck. Carrier\_orig and CgPN entirely untrustworthy.

## Signature Not Verified Scenarios

## Multiple Signature Scenarios