ATIS-0300117

ATIS Standard on -

Operational Standard for the Signature-based Handling of Asserted information using toKENs (SHAKEN) Governance Model and Certificate Management

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0300117

ATIS Standard on

Operational Standard for the Signature-based Handling of Asserted information using toKENs (SHAKEN) Governance Model and Certificate Management

Alliance for Telecommunications Industry Solutions

Approved September 18, 2019

Abstract

This document is intended to provide Next Generation Network (NGN) telephone service providers (SPs) guidance regarding operational concerns for the Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) governance model and certificate management procedures to ensure the completion of legitimate calls and the mitigation of illegitimate spoofing of telephone identities. This document will facilitate interoperability between and within NGN SPs by addressing the operational concerns for the signature-based handling of asserted information using tokens, i.e., SHAKEN governance model and certificate management procedures.

.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next generation network interconnection and interoperability topics associated with emerging technologies. Specifically, it develops operational procedures that involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues that impact the interconnection of existing and next generation networks and facilitate the transition to emerging technologies.

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, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

Karen Riepenkroger, Sprint

Randee Ryan, Comcast

Table of Contents

Table of Figures

ATIS Standard on –

Operational Standard for the Signature-based Handling of Asserted information using toKENs (SHAKEN) Governance Model and Certificate Management

1 Scope & Purpose

1.1 Scope

This document is intended to provide Next Generation Network (NGN) telephone service providers (SPs) guidance regarding operational concerns for the Signature-Based Handling of Asserted Information Using Tokens (SHAKEN) governance model and certificate management procedures to ensure the completion of legitimate calls and the mitigation of illegitimate spoofing of telephone identities.

1.2 Purpose

This document will facilitate interoperability between and within NGN SPs by addressing the operational concerns for the signature-based handling of asserted information using tokens, i.e., SHAKEN governance model and certificate management procedures.

2 Normative References

The following standards contain provisions that, 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-0300106, *Intercarrier Call Completion/Call Termination Handbook.*[1]

ATIS-0300116, *Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted Information Using Tokens (SHAKEN)*.[1]

ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange*.[1]

ATIS-1000054, *ATIS Technical Report on Next Generation Network Certificate Management.*[1]

ATIS-1000074-E, *Errata to Signature-based Handling of Asserted information using Tokens (SHAKEN).*[1]

ATIS-1000080-E, Errata to Signature-based Handling of Asserted Information using Tokens (SHAKEN): Governance Model and Certificate Management.[1]

ATIS-1000084-E, Errata to ATIS Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators.[1]

draft-ietf-acme-authority-token, *ACME Challenges Using an Authority Token.*[2]

draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token.*[2]

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/ >.

[2] Available from the Internet Engineering Task Force (IETF) at: < https://datatracker.ietf.org/doc/draft-ietf-acme-authority-token/ >.

Report and Order (R&O) and *Further Notice of Proposed Rulemaking* (*FNPRM*) in FCC 13-135 and WC Docket No.13-39, adopted October 28, 2013 and released November 8, 2013.[3]

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[2]

RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7.* [2]

RFC 3261, *SIP: Session Initiation Protocol.*[2]

RFC 3966, *The tel URI for Telephone Numbers.*[2]

RFC 4949, *Internet Security Glossary, Version 2.*[2]

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2.*[2]

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[2]

RFC 5958, *Asymmetric Key Package.*[2]

RFC 6749, *The OAuth 2.0 Authorization Framework.*[2]

RFC 6960, *Online Certificate Status Protocol (OSCP).*[2]

RFC 7159, *The JavaScript Object Notation (JSON).*[2]

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.*[2]

RFC 7375, *Secure Telephone Identity Threat Model.*[2]

RFC 7515, *JSON Web Signatures (JWS).*[2]

RFC 7516, *JSON Web Algorithms (JWA)*.[2]

RFC 7517, *JSON Web Key (JWK).*[2]

RFC 7519, *JSON Web Token (JWT).*[2]

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*.[2]

RFC 8225, *Persona Assertion Token*.[2]

RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

RFC 8555, *Automatic Certificate Management Environment (ACME).*[2]

RFC 8588, *Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN).*[2]

Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-135, *Declaratory Ruling and Order, FCC 15-72*, (released July 10, 2015).**Error! Bookmark not defined.**

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < https://glossary.atis.org >.

3.1 Definitions

(Digital) Certificate: A 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 **Secure Telephone Identity (STI) Certificate**.

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]

[3] This document is available from the Federal Communications Commission (FCC) at < https://www.fcc.gov/ >.

National/Regional Regulatory Authority (NRRA): A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region. Note that region is not intended to be a region within a country (e.g., a region is not a state within the US).

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. See also Trust Anchor CA and Trusted CA [RFC 4949].

Service Provider Code: In the context of this document, this term is refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider. In the US and Canada this would be a Company Code as defined in [ATIS-0300251.2007].

Service Provider Code (SPC) token: An authority token that can be used by a SHAKEN Service Provider during the ACME certificate ordering process to demonstrate authority over the identity information contained in the TN Authorization List extension of the requested STI certificate. The SPC Token complies with the structure of the TNAuthList Authority Token defined by [draft-ietf-acme-authority-token-tnauthlist], but with the restriction for SHAKEN where the TNAuthList value contained in the token's "atc" claim identifies a single Service Provider Code.

Secure Telephone Identity (STI) Certificate: A public key certificate used by a service provider to sign and verify the PASSporT.

Signature: A Signature is 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.

Trust Anchor: An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The combination of a trusted public key and the name of the entity to which the corresponding private key belongs. [RFC 4949].

Trusted CA: A CA upon which a certificate user relies for issuing valid certificates; especially a CA that is used as a trust anchor CA [RFC 4949].

Trust Model: Describes how trust is distributed from Trust Anchors.

Trusted Network: A trusted network is a network that follows the 3GPP Trust Model[4]

Untrusted Network: An untrusted network is a network that does not follow the 3GPP Trust Model[5]

3.2 Acronyms & Abbreviations

ACME	Automated Certificate Management Environment (Protocol)
ATIS	Alliance for Telecommunications Industry Solutions
CA	Certification Authority
IETF	Internet Engineering Task Force
NECA	National Exchange Carrier Association
OCN	Operating Company Number
PASSporT	Personal Assertion Token

[4] 3GPP TS 33.234 V023.0 (2002-11); 3GPP TS 29.165 V11.5.0 (2012-12)

[5] 3GPP TS 33.234 V023.0 (2002-11); 3GPP TS 29.165 V11.5.0 (2012-12)

PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates
PSTN	Public Switched Telephone Network
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SP	Service Provider
SP-KMS	SP Key Management Server
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-GA	Secure Telephone Identity Governance Authority
STI-PA	Secure Telephone Identity Policy Administrator
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TLS	Transport Layer Security
TN	Telephone Number
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol

4 Secure Telephone Identity Governance Authority (STI-GA)

It is expected that a recognized STI-GA is chosen via an industry or regulatory process. It is outside the scope of this operational standard to determine what entity performs the role of the STI-GA, although NGIIF recommends an industry led consortium define the specific requirements and expected functions to be performed by the STI-GA. See ATIS-1000080, *Signature-Based Handling of Asserted Information Using Tokens (Shaken): Governance Model and Certificate Management* for further detail on the STI-GA.

5 Secure Telephone Identity Policy Administrator (STI-PA)

The STI-PA shall maintain a list of CAs approved to serve as STI-CAs. The STI-PA shall notify the SP of changes to the active list of approved STI-CAs in a timely and automated manner.

The STI-PA should be required to develop the criteria and a process for STI-CA to verify and validate that a service provider requestor is authorized to obtain certificates as that service provider (i.e., Service Provider Code Token).

For further roles of the STI-PA please see ATIS-1000080, *Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Governance Model and Certificate Management* and ATIS-1000084, *Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*

The following diagram highlights the roles of the STI-PA and interfaces to other functional elements of the SHAKEN framework:

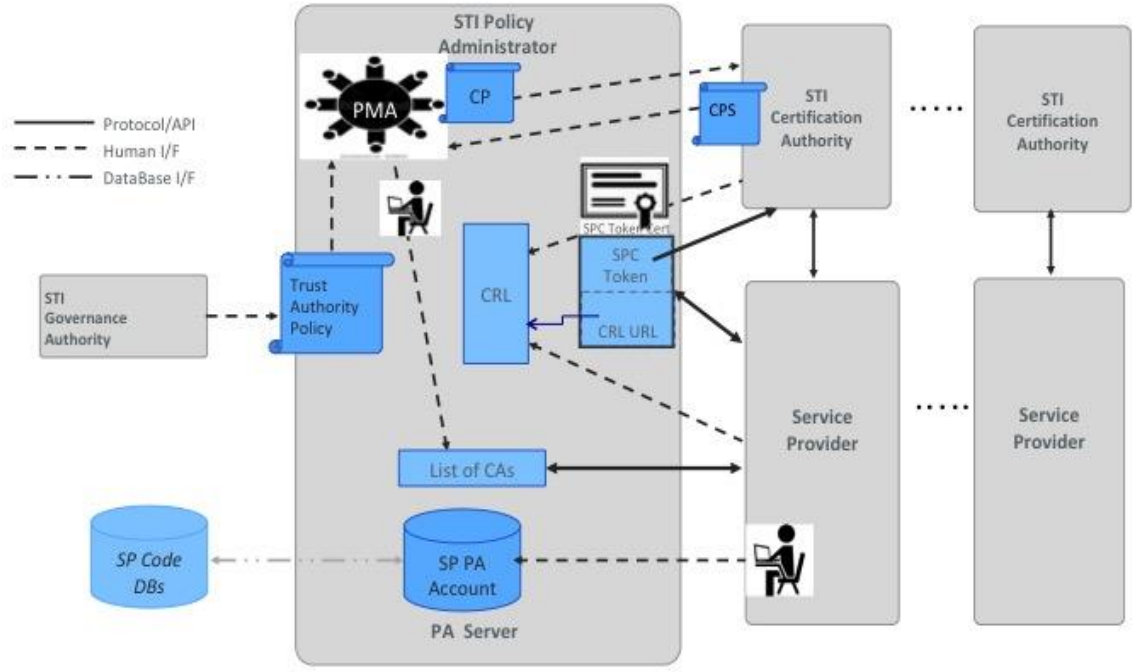

Figure 5.1: Roles of STI-PA

6 Secure Telephone Identity Certification Authority (STI-CA)

The approved STI-CA will have the responsibility of issuing X.509 certificates for the providers eligible to and holding North American Numbering Plan (NANP) resources in alignment with specified criteria determined with input from the PA and industry resources and the management processes performed in alignment with documented processes.

For the STI-CA, certificates at a minimum must represent an authorized telephone service provider and their authorization to assert telephone numbers in accordance with documented processes and guidelines. For further information on STI-CA see ATIS-1000080, *Signature-based Handling of Asserted Information using Tokens (SHAKEN): Governance Model and Certificate Management* and the appendix. An SP may choose to use multiple STI-CAs.

Should the STI-CA cease being a valid STI-CA, the STI-CA shall be removed from the list of valid STI-CAs by the STI-PA. The STI-PA shall provide the SPs with an updated list of STI-CAs. Any SP that has obtained certificates from an STI-CA that is not on the list of trusted STI-CAs shall select an approved STI-CA and obtain new certificates in order to authenticate their calls.

To the extent that the STI-CA is also operated by an SP, the STI-CA shall maintain neutrality in interactions between service providers.

7 Service Provider

The SP shall ensure that the STI-CA from which they request certificates is on the list of approved STI-CAs managed by the STI-PA.

When the certificates have become invalid the SP should consult the list of approved STI-CAs to determine a valid STI-CA and obtain new certificates to complete the service provider's calls.

When the certificates expire, the SP should ensure that the STI-CA from which certificates are being requested is still on the list of approved STI-CAs.

When a terminating call entity determines through the verification process that a certificate fails validation, it should complete that call and send a SIP response code to the originating carrier/certificate holder.

The certificate holder (originating service provider), should ensure that it has implemented functionality and investigative processes that would recognize and resolve a pattern of certificate failures.

The certificate holder (originating service provider), when notified that their certificate is failing, upon resolution of any investigation and where the certificate is determined invalid the service provider should immediately procure a valid certificate from the STI-CA, or, if the STI-CA is no longer a valid STI-CA, the SP should immediately select an approved STI-CA and obtain all new certificates from the new STI-CA and immediately implement the new certificates in order to authenticate their calls. The preferred course of action in the case of repeated certificate failure is to troubleshoot the problem.

7.1 Use of Certificates

The SHAKEN standard dictates that at least one certificate is needed for service provider. Service providers may obtain and assign certificates with varying granularity to suit their business and operational needs. These may range from the highest granularity of assigning a unique certificate to each originating network element to utilizing one blanket certificate for SHAKEN operations across the entire service provider's network. Additional granularity is at the service provider's discretion. Determination of the number of certificate(s) needs to be based on prudent business decisions. Certificates include a responsibility in terms of acquisition, renewals, and facilities for ongoing security, management, and maintenance.

SPs might opt for some in-between solution, sharing certificates among closely-related entities (such as all originating network elements within a certain geographical division such as a county, a state or a region), within certain segments of their network, or according to the internal corporate organization.

7.2 Handling SHAKEN Certificate Issues

Regardless of any issues encountered with the presence or absence of a PASSporT, or the validity or invalidity of certificates, the SP is required to complete the call.[6] To address certificate issues after completion of the call, the terminating SP should watch for a trends and refer to the STI-PA.. Subject to any call completion requirements, the SIP response should be sufficient to notify the originating provider.

7.2.1. Process for Determination of Appropriate Certificate for Acquisitions and Mergers

If mergers and/or acquisitions result in the SP being provisioned to use a different STI-CA, then the SP shall obtain new certificates from the STI-CA (per Clause 7 for procedures for selecting a STI-CA).

7.2.2. Retention of the PASSporT

It is recommended that, dependent on policy, SPs retain the PASSporT associated with call detail to allow troubleshooting for potential certificate verification failures.

8 Interconnection Configurations

8.1 Both Originating and Terminating Providers have Implemented SHAKEN Standard

Authentication processing will occur on the originating end and verification processing will occur on the terminating end and the call disposition to display to the end user will depend on the outcome of those operations.

[6] Report and Order (R&O) and Further Notice of Proposed Rulemaking (FNPRM) in FCC 13-135 and WC Docket No. 13-39, adopted October 28, 2013 and released November 8, 2013 ("Rural Call Completion")

8.2 Originating Provider has Implemented SHAKEN; Terminating Provider has not Implemented SHAKEN

Authentication processing will occur on the originating end, but verification processing will not occur on the terminating end and the call disposition to the end user will have no indication of the veracity.

8.3 Originating Provider has not Implemented SHAKEN; Terminating Provider has Implemented SHAKEN

Authentication processing will not occur on the originating end and as a result verification processing will fail on the terminating end and the call disposition to the end user will have no indication of the veracity.

8.4 Originating Provider has Implemented SHAKEN; Intermediate Provider does not Support SHAKEN

Authentication processing will occur on the originating end, however, the intermediate provider processing does not carry the authentication indication, and as a result verification processing will fail on the terminating end and the call disposition to the end user will have no indication of the veracity. See above terminating provider conditions which may vary the outcome of this example.

8.5 Originating Provider has Implemented SHAKEN; Intermediate Provider does not Support SHAKEN (Intermediate Provider Passes P-Asserted Identity header Info to Assert the Caller ID of the Originating SIP UA)

Authentication processing will occur on the originating end and verification processing will occur on the terminating end and the call disposition to display to the end user will depend on the outcome of those operations. See above terminating provider conditions which may vary the outcome of this example.

8.6 Neither the Originating Provider, nor the Terminating Provider have Implemented SHAKEN

Authentication processing will not occur on the originating end and verification processing will not occur on the terminating end and the call disposition to the end user will have no indication of the veracity.

9 SP Operational Procedures for Error Handing

9.1 Service Provider Code token Issues

The SP is required to obtain a Service Provider Code token from the STI-PA in order to prove that it is authorized to obtain certificates from an STI-CA. Prior to requesting a certificate, the SP should ensure that the service provider code token is not expired. If the Service Provider Code token has expired, the SP shall obtain a new Service Provider Code token from the STI-PA.

During the process of acquiring a certificate, if the ACME challenge/response fails, the SP should obtain a new Service Provider Code token. If the challenge/response fails with the new Service Provider Code token, the SP should notify the STI-PA for resolution assistance. In the interim, if the SP has an account with another STI-CA, the SP should consider attempting to obtain a certificate from another STI-CA. The SP should implement measures to mitigate the impact of an internal compromise of the Service Provider Code token.

9.2 Process for Management of Revoked Certificates

The procedures as defined in ATIS-1000080 should be followed in the case certificate revocation.

9.3 Process for Management of Expired Certificates

See Clause 7 for the process for management of expired certificates.