ATIS-1000082.v002

ATIS Standard on -

Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server

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-1000082.v002

ATIS Standard on

Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server

Alliance for Telecommunications Industry Solutions

Approved April 2022

Abstract

This document provides a Technical Report on a SHAKEN APIs used to support a Centralized Signing and Signature Validation Server. These APIs provide a means for multiple and/or disparate network elements to use an HTTP-based RESTful interface to access SHAKEN Signing and Signature Validation servers. Initial SHAKEN API standards have been defined and are expected to further progress in 3rd Generation Partnership Project (3GPP).

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union Telecommunication Sector (ITU-T) and U.S. ITU Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The SIP Forum is an IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations, the SIPit, SIPconnect-IT, and RTCWeb-it interoperability testing events, special workshops, educational seminars, and general promotion of SIP in the industry. The SIP Forum is also the producer of the annual SIP Network Operators Conference (SIPNOC), focused on the technical requirements of the service provider community. One of the Forum's notable technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation for direct IP peering and interoperability between IP Private Branch Exchanges (PBXs) and SIP-based service provider networks. Other important Forum initiatives include work in Video Relay Service (VRS) interoperability, security, Network-to-Network Interoperability (NNI), and SIP and IPv6.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005, and/or to the SIP Forum, 733 Turnpike Street, Suite 192, North Andover, MA, 01845.

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.

The **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **SIP Forum Technical Working Group (TWG)** was responsible for the development of this document.

Table of Contents

Table of Figures

ATIS Standard on –

Technical Report on SHAKEN API for a Centralized Signing and Signature Validation Server

1 Introduction

This technical report defines a Representational State Transfer (REST)ful interface that can be used in the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework to sign and verify telephony identity:

- Secure Telephone Identity Authentication Service (STI-AS) exposes an Applications Programming Interface (API) to sign the provided Personal Assertion Token (PASSporT) which includes the SHAKEN extension as defined in IETF RFC 8588 [Ref 5].
- Secure Telephone Identity Verification Service (STI-VS) exposes an API to verify the signed Secure Telephone Identity (STI) according to procedures defined in IETF RFC 8224 [Ref 3].

The only algorithm currently supported by this API is ES256.

The data set defined in this document could be expanded to accommodate other data types as needed (e.g., other PASSporT extensions that may need to be supported). Standards that include and expand the data set defined in this document continue to be defined in 3rd Generation Partnership Project (3GPP).

2 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.

[Ref 1] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*.[1]

[Ref 2] IETF RFC 7519, *JSON Web Token (JWT).*[1]

[Ref 3] IETF RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol (SIP).*[1]

[Ref 4] IETF RFC 8225, *PASSporT: Personal Assertion Token.*[1]

[Ref 5] IETF RFC 8588, *PASSporT Extension for SHAKEN*.[1]

[Ref 6] ATIS-1000074, *Signature-based Handling of Asserted Information using toKENs (SHAKEN)*.[2]

[Ref 7] ATIS-1000080, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management.*[2]

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 >.

[1] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

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