ATIS-1000074

JOINT ATIS/SIP FORUM STANDARD – SIGNATURE-BASED HANDLING OF ASSERTED INFORMATION USING TOKENS (SHAKEN)

JOINT STANDARD

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 and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

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 SIPNOC conferences (for SIP Network Operators Conference), 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 PBXs and SIP-based service provider networks. Other important Forum initiatives include work in VRS interoperability, security, NNI, and SIP and IPv6.

< http://www.sipforum.org/ >

ATIS-1000074, Signature-based Handling of Asserted information using toKENs (SHAKEN)

Is an ATIS & SIP Forum Joint Standard developed by the **ATIS/SIP Forum IP-NNI Task Force** under the **ATIS Packet Technologies and Systems Committee (PTSC)** and the **Technical Working Group (TWG)** under the **SIP Forum**.

Published by

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

SIP Forum LLC
733 Turnpike Street, Suite 192
North Andover, MA 01845

ATIS-1000074

ATIS Standard on

Signature-based Handling of Asserted information using toKENs (SHAKEN)

Alliance for Telecommunications Industry Solutions

Approved January 5, 2017

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 verification of the telephone identity and other information in an Internet Protocol (IP)-based service provider voice network. This specification defines the framework for telephone service providers to create signatures in Session Initiation Protocol (SIP) and validate initiators of signatures. It defines the various classes of signers and how the verification of a signature can be used toward the mitigation and identification of illegitimate use of national telecommunications infrastructure and to protect its users.

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 –

Signature-based Handling of Asserted information using toKENs (SHAKEN)

1 Scope & Purpose

1.1 Scope

This document is intended to provide telephone service providers with a framework and guidance on how to utilize Secure Telephone Identity (STI) technologies toward the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities on IP-based service provider voice networks (also to be referred to as Voice over Internet Protocol [VoIP] networks). The primary focus of this document is on the format of STI claims, the mapping of these claims to SIP (RFC 3261), and the authentication and verification functions.

1.2 Purpose

Using the protocols defined in draft-ietf-stir-rfc4474bis and draft-ietf-stir-passport, this document defines the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. This framework is targeted at telephone service providers delivering phone calls over VoIP, and addresses the implementation and usage of the IETF STIR Working Group protocols and the architecture and use of STI-related X.509-based certificates (RFC 5280). It also discusses the general architecture of service provider authentication and verification services. Finally, it provides high level guidance on the use of positive or negative verification of the signature to mitigate illegitimate telephone identity in general.

Illegitimate Caller ID spoofing is a growing concern for North American telephone service providers and their customers. There are many Caller ID spoofing mechanisms, and illegitimate spoofing can evolve to evade mitigation techniques. Service provider solutions must therefore be flexible to respond to evolving threats in much the same way as cybersecurity solutions. In addition, the integration of new technologies into established VoIP networks imposes many interoperability and interworking challenges. As a result, this document is a baseline document on the implementation of the protocol-related requirements for STI. The objective is to provide a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS 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.

draft-ietf-stir-passport, *Persona Assertion Token.*[1]

draft-ietf-stir-rfc4474bis, *Authenticated Identity Management in the Session Initiation Protocol.*[1]

draft-ietf-stir-certificates, *Secure Telephone Identity Credentials: Certificates.*[1]

IETF RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*[1]

IETF RFC 3261, *SIP: Session Initiation Protocol.*[1]

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[1]

[1] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.