ATIS-1000080

JOINT ATIS/SIP FORUM STANDARD – SIGNATURE-BASED HANDLING OF ASSERTED INFORMATION USING TOKENS (SHAKEN): GOVERNANCE MODEL AND CERTIFICATE MANAGEMENT

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-1000080, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management

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-1000080

ATIS Standard on

Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management

Alliance for Telecommunications Industry Solutions

Approved July 11, 2017

Abstract

Signature-based Handling of Asserted information using toKENs (SHAKEN) is an industry framework for managing and deploying 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 IP-based service provider voice network. This specification expands the SHAKEN framework, introducing a governance model and defining X.509 certificate management procedures. Certificate management provides mechanisms for validation of a certificate and verification of the associated digital signature, allowing for the identification of illegitimate use of national telecommunications infrastructure.

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 –

SHAKEN: Governance Model and Certificate Management

1 Scope & Purpose

1.1 Scope

This document expands the Signature-based Handling of Asserted Information using Tokens (SHAKEN) [ATIS-1000074] framework, introducing a governance model and defining certificate management procedures for Secure Telephone Identity (STI) technologies. The certificate management procedures identify the functional entities and protocols involved in the distribution and management of STI Certificates. The governance model identifies functional entities that have the responsibility to establish policies and procedures to ensure that only authorized entities are allowed to administer digital certificates within Voice over Internet Protocol (VoIP) networks. However, the details of these functional entities in terms of regulatory control and who establishes and manages those entities are outside the scope of this document.

1.2 Purpose

This document introduces a governance model, certificate management architecture, and related protocols to the SHAKEN framework [ATIS-1000074]. The governance model defines recommended roles and relationships, such that the determination of who is authorized to administer and use digital certificates in VoIP networks can be established. This model includes sufficient flexibility to allow specific regulatory requirements to be implemented and evolved over time, minimizing dependencies on the underlying mechanisms for certificate management. The certificate management architecture is based on the definition of roles similar to those defined in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Internet Engineering Task Force (IETF) [RFC 5280]. Per the SHAKEN framework, the certificates themselves are based on X.509 with specific policy extensions based on draft-ietf-stir-certificates. The objective of this document is to provide recommendations and requirements for implementing the protocols and procedures for certificate management within the SHAKEN framework.

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.

ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[1]

ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange.*[2]

ATIS-1000054*, ATIS Technical Report on Next Generation Network Certificate Management.*[3]

draft-ietf-stir-passport, *Personal Assertion Token (PASSporT)*.[4]

draft-ietf-stir-rfc4474bis, *Authenticated Identity Management in the Session Initiation Protocol*.[4]

---

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/docstore/product.aspx?id=28297 >.

[2] This document is available from ATIS at: < https://www.atis.org/docstore/product.aspx?id=26148 >.

[3] This document is available from ATIS at: < https://www.atis.org/docstore/product.aspx?id=27962 >.

[4] This document is available from the Internet Engineering Task Force (IETF) at: < https://tools.ietf.org/ >.

draft-ietf-stir-certificates, *Secure Telephone Identity Credentials: Certificates*[4]

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*[4]

draft-ietf-acme-acme, *Automatic Certificate Management Environment (ACME).*[4]

draft-barnes-acme-service-provider, *ACME Identifiers and Challenges for VoIP Service Providers.*[4]

RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7.*[4]

RFC 3261, *SIP: Session Initiation Protocol.*[4]

RFC 3966, *The tel URI for Telephone Numbers.*[4]

RFC 4949, *Internet Security Glossary, Version 2.*[4]

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2.*[4]

RFC 5958, *Asymmetric Key Package.*[4]

RFC 6749, *The OAuth 2.0 Authorization Framework.*[4]

RFC 6960, *Online Certificate Status Protocol (OSCP).*[4]

RFC 7159, *The JavaScript Object Notation (JSON).*[4]

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.*[4]

RFC 7375, *Secure Telephone Identity Threat Model.*[4]

RFC 7515, *JSON Web Signatures (JWS).*[4]

RFC 7516, *JSON Web Algorithms (JWA).*[4]

RFC 7517, *JSON Web Key (JWK).*[4]

RFC 7519, *JSON Web Token (JWT).*[4]

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 >.

3.1 Definitions

The following provides some key definitions used in this document. Refer to IETF RFC 4949 for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

Caller ID: The originating or calling party's telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields in the Session Initiation Protocol (SIP) [RFC 3261] messages.

(Digital) 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 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].

Certificate Validation: An act or process by which a certificate user established that the assertions made by a certificate can be trusted. [RFC 4949].

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. [RFC 4949]

Chain of Trust: Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain. [RFC 4949].

Certificate Chain: See Certification Path.