



SIP FORUM

ATIS-1000080.v003

**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 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 a leading IP communications industry association that engages in numerous activities that promote and advance SIP-based technology, such as the development of industry recommendations; interoperability testing events and special workshops, educational activities, and general promotion of IP communications standards, services, and technology for service provider, enterprise, and governmental applications. 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 technical activities is the development of the SIPconnect Technical Recommendation – a standards-based SIP trunking recommendation that provides detailed guidelines for direct IP peering and interoperability between IP PBXs and SIP-based service provider networks, and the SIPconnect Certification Testing Program, a unique certification testing program that includes a certification test suite and test platform, and an associated “SIPconnect Certified” logo program that provides an official “seal of certification” for companies products and services that have officially achieved conformance with the SIPconnect specification. Other important Forum initiatives include work in security, SIP and IPv6, and IP-based Network-to-Network Interconnection (IP-NNI). For more information about all SIP Forum initiatives, please visit:

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

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [<http://www.atis.org/legal/patentinfo.asp>] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000080.v003, 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

Copyright © 2020 by Alliance for Telecommunications Industry Solutions and by SIP Forum LLC.
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380 or the SIP Forum at 203.829.6307. ATIS is online at < <http://www.atis.org> > and the SIP Forum is online at < <http://www.sipforum.org> >.

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

Alliance for Telecommunications Industry Solutions

Approved August 14, 2020

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

1. Scope & Purpose	1
1.1 Scope	1
1.2 Purpose	1
2. References	1
2.1 Normative References	1
2.2 Informative References	2
3. Definitions, Acronyms, & Abbreviations	2
3.1 Definitions	2
3.2 Acronyms & Abbreviations	4
4. Overview	6
5. SHAKEN Governance Model	6
5.1 Requirements for Governance of STI Certificate Management	6
5.2 Certificate Governance: Roles & Responsibilities	7
5.2.1 <i>Secure Telephone Identity Policy Administrator (STI-PA)</i>	8
5.2.2 <i>Secure Telephone Identity Certification Authority (STI-CA)</i>	8
5.2.3 <i>Service Provider (SP)</i>	8
6. SHAKEN Certificate Management	9
6.1 Requirements for SHAKEN Certificate Management	9
6.2 SHAKEN Certificate Management Architecture	10
6.3 SHAKEN Certificate Management Process	10
6.3.1 <i>SHAKEN Certificate Management Flow</i>	11
6.3.2 <i>STI-PA Account Registration & Service Provider Authorization</i>	13
6.3.3 <i>STI-CA Account Creation</i>	13
6.3.4 <i>Service Provider Code Token</i>	15
6.3.5 <i>Application for a Certificate</i>	19
6.3.6 <i>STI Certificate Acquisition</i>	24
6.3.7 <i>STI Certificate Management Sequence Diagrams</i>	26
6.3.8 <i>Lifecycle Management of STI Certificates</i>	27
6.3.9 <i>STI Certificate Revocation</i>	27
6.3.10 <i>Evolution of STI Certificates</i>	29
6.4 STI Certificate and Certificate Revocation List (CRL) Profile for SHAKEN	29
6.4.1 <i>SHAKEN Certificate Requirements</i>	29
6.4.2 <i>SHAKEN CRL Requirements</i>	30
Appendix A – Certificate Creation & Validation with OpenSSL	32
A.1 TNAuthorizationList extension	32
A.2 Setup directories	33
A.3 Create private key and CSR	33
A.3.1 <i>Create private key</i>	33
A.3.2 <i>Create CSR from private key</i>	33
A.4 Signing certificate using root CA	33
A.4.1 <i>Create file to be used as certificate database by openssl</i>	35
A.4.2 <i>Create file that contains the certificate serial number</i>	35
A.4.3 <i>Create directories to be used to store keys, certificates and signing requests</i>	35
A.4.4 <i>Create root key</i>	35
A.4.5 <i>Create root certificate</i>	35
A.4.6 <i>Verify root certificate</i>	35
A.4.7 <i>Sign CSR with root CA cert and create end-entity certificate</i>	36
A.4.8 <i>Verify end-entity certificate</i>	36
A.4.9 <i>Verify chain of trust</i>	37

A.5	Signing certificate using intermediate CA.....	38
A.5.1.	Create file to be used as certificate database by openssl.....	39
A.5.2.	Create file that contains the certificate serial number.....	39
A.5.3.	Create directories to be used to store keys, certificates and signing requests	39
A.5.4.	Create intermediate key.....	40
A.5.5.	Create CSR from intermediate key.....	40
A.5.6.	Create intermediate certificate.....	40
A.5.7.	Verify intermediate certificate	40
A.5.8.	Sign CSR with intermediate cert and create end-entity certificate	41
A.5.9.	Verify end-entity certificate.....	41
A.5.10.	Verify chain of trust	42

Table of Figures

Figure 5.1	– Governance Model for Certificate Management	7
Figure 6.1	– SHAKEN Certificate Management Architecture.....	10
Figure 6.2	– SHAKEN Certificate Management High Level Call Flow	12
Figure 6.3	– STI-PA Account Setup and STI-CA (ACME) Account Creation	26
Figure 6.4	– STI Certificate Acquisition.....	27
Figure 6.5	– Distribution of the CRL	28
Figure 6.6	– Using the CRL	29

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 [Ref 1] 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 [Ref 1]. 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 [Ref 11]. Per the SHAKEN framework, the certificates themselves are based on X.509 with specific policy extensions based on RFC 8226 [Ref 25]. 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. 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.

2.1 Normative References

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

[Ref 2] ATIS-1000084, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*.¹

[Ref 3] ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange*.¹

[Ref 4] ATIS-1000054, *ATIS Technical Report on Next Generation Network Certificate Management*.¹

[Ref 5] draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token*.²

[Ref 6] RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7*.²

[Ref 7] RFC 3261, *SIP: Session Initiation Protocol*.²

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