ATIS-1000080.v005

ATIS Standard on -

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-1000080.v005

ATIS Standard on

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

Alliance for Telecommunications Industry Solutions

Approved December 12, 2022

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 Telecommunications Industry Solutions (ATIS) is a global standards development and technical planning organization that develops and promotes worldwide technical and operations standards for information, entertainment, and communications technologies. ATIS' diverse membership includes key stakeholders from the Information and Communications Technologies (ICT) industry – wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, VoIP providers, consumer electronics companies, public safety agencies, and internet service providers. ATIS is also a founding partner and the North American Organizational Partner of the Third Generation Partnership Project (3GPP), the global collaborative effort that has developed the Long-Term Evolution (LTE) and LTE-Advanced wireless specifications.

ATIS' Packet Technologies and Systems Committee (PTSC) develops standards related to services, architectures, signaling, network interfaces, next generation carrier interconnect, cybersecurity, lawful intercept, and government emergency telecommunications service within next generation networks. As networks transition to all-IP, PTSC will evaluate the impact of this transition and develop solutions and recommendations where necessary to facilitate and reflect this evolution.

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 **Error! Bookmark not defined.**
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 Secure Telephone Identity Policy Administrator (STI-PA) 8
5.2.2 Secure Telephone Identity Certification Authority (STI-CA) 8
5.2.3 Service Provider (SP) 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 SHAKEN Certificate Management Flow 11
6.3.2 STI-PA Account Registration & Service Provider Authorization 13
6.3.3 STI-CA Account Creation 13
6.3.4 Service Provider Code Token 15
6.3.5 Application for a Certificate 19
6.3.6 STI Certificate Acquisition 25
6.3.7 STI Certificate Management Sequence Diagrams 26
6.3.8 Lifecycle Management of STI Certificates 28
6.3.9 STI Certificate Revocation 28
6.3.10 Evolution of STI Certificates 30
6.4 STI Certificate and Certificate Revocation List (CRL) Profile for SHAKEN 30
6.4.1 STI Certificate Requirements 31
6.4.2 SHAKEN CRL Requirements 32
Appendix A – SHAKEN Certificate Management Example with OpenSSL 34
A.1 TNAuthorizationList extension 34
A.2 Setup directories 35
A.3 Create private key and CSR 35
A.3.1. Create private key 35
A.3.2. Create CSR from private key 35
A.4 Signing certificate using root CA 35
A.4.1. Create file to be used as certificate database by openssl 37
A.4.2. Create file that contains the certificate serial number 37
A.4.3. Create directories to be used to store keys, certificates and signing requests 37
A.4.4. Create root key 37
A.4.5. Create root certificate 38
A.4.6. Verify root certificate 38
A.4.7. Sign CSR with root CA cert and create End-Entity certificate 39
A.4.8. Verify End-Entity certificate 39
A.4.9. Verify chain of trust 40

A.5 Signing certificate using intermediate CA 40
A.5.1. Create file to be used as certificate database by openssl 42
A.5.2. Create file that contains the certificate serial number 42
A.5.3. Create directories to be used to store keys, certificates and signing requests 42
A.5.4. Create intermediate key 42
A.5.5. Create CSR from intermediate key 42
A.5.6. Create intermediate certificate 43
A.5.7. Verify intermediate certificate 43
A.5.8. Sign CSR with intermediate cert and create End-Entity certificate 44
A.5.9. Verify End-Entity certificate 44
A.5.10. Verify chain of trust 45

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 27
Figure 6.4 – STI Certificate Acquisition 28
Figure 6.5 – Distribution of the CRL 29
Figure 6.6 – Using the CRL 30

ATIS Standard on –

SHAKEN: Governance Model and Certificate Management

1 Scope & Purpose

1.1 Scope

This document expands the ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*, 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 Engineering Task Force (IETF) RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Per the SHAKEN framework, the certificates themselves are based on X.509 with specific policy extensions based on RFC 8226, *Secure Telephone Identity Credentials: 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 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] 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-1000054*, ATIS Technical Report on Next Generation Network Certificate Management.*[1]

[Ref 4] ATIS-1000092, *Signature-based Handling of Asserted information using toKENs (SHAKEN): Delegate Certificates*.[1]

[Ref 5] ATIS-1000093, *ATIS Standard on Toll-Free Numbers in the SHAKEN Framework.*[1]

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