ATIS-1000084.v003

Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators

TECHNICAL REPORT

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.

ATIS-1000084.v003, *Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*

Published by

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

ATIS-1000084.v003

ATIS Technical Report on

Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators

Alliance for Telecommunications Industry Solutions

Approved March 16, 2023

Abstract
This document provides operational and management considerations for the Certification Authorities within the context of the SHAKEN Governance Model and Certificate Management framework. It introduces considerations for the STI Policy Administrator in managing the list of valid STI-CAs and authorized Service Providers, as well as general operational and policy considerations for PKI. This document introduces those aspects which are unique to the SHAKEN use of PKI.

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

Table of Figures

ATIS Technical Report on –

Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators

1 Scope & Purpose

1.1 Scope

This technical report describes operational and management considerations for STI Certification Authorities (STI-CAs) within the context of the SHAKEN framework [ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*], Delegate Certificates [ATIS-1000092, *Signature-based Handling of Asserted Information using Tokens (SHAKEN): Delegate Certificates*] and SHAKEN governance [ATIS-1000080, *SHAKEN Governance Model and Certificate Management framework*]. This document focuses on the operational and management aspects that impact the authentication and verification services, as well as general Certification Authority (CA) practices and policies. The document addresses the STI Policy Administrator (STI-PA) operational aspects of managing the list of STI-CAs and authorization of STI Participants to obtain STI certificates and to issue delegate certificates. This document does not address any additional policy aspects defined by the STI Governance Authority (STI-GA), and applied by the STI-PA, in determining whether or not a CA is qualified to serve as an STI-CA, a service provider is a valid service provider or a service provider is authorized to issue delegate certificates. The guidelines and recommendations provided in this document are based on an STI-PA starting with a list of trusted STI-CAs and a list of authorized STI Participants or the policies set by the STI Governance Authority (STI-GA) to be applied by the STI-PA in authorizing STI Participants to participate in the ecosystem.

1.2 Purpose

The SHAKEN Governance Model and Certificate Management framework uses standard Public Key Infrastructure (PKI) for creating and distributing STI certificates and delegate certificates. As such, PKI Certification Practice Statement (CPS) and Certificate Policy (CP) documents, per RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, are an operational requirement for the STI-CAs. This document outlines the role of the STI-PA in defining and administering required certificate policies to support SHAKEN.

The SHAKEN Governance Model and Certificate Management framework introduces a model whereby the STI-PA maintains a list of trusted STI-CAs. This list is distributed to STI Participants and used during the verification process to ensure that the public key certificate associated with a specific PASSporT has been issued by a valid STI-CA. This document specifies the form of the information stored in the list and the mechanism for distributing that list to the STI Participants.

The STI Participant obtains STI certificates from an STI-CA to create signatures authenticating itself as the signing entity and protecting the integrity of the Identity header field. The STI Participant can obtain STI certificates from any approved STI-CA in the list of trusted STI-CAs received from the STI-PA with which it has an established business relationship. An STI Participant can also obtain a CA certificate from an STI-CA to establish a Subordinate CA for issuing delegate certificates to VoIP entities.

The SHAKEN certificate management framework is based on using a signed Service Provider Code (SPC) token for validation when requesting a certificate. Prior to requesting a certificate, the STI Participant requests a Service Provider Code token from the STI-PA as described in ATIS-1000080 [Ref 2] for an STI certificate or ATIS-1000092 [Ref 3] for a CA certificate to support delegate certificates. When an STI Participant initiates a Certificate Signing Request (CSR), the STI Participant proves to the STI-CA that it has been validated and is eligible to receive a certificate via the use of the SPC token. This document describes the STI-PA management of the SPC tokens.