



SIP FORUM

ATIS-1000092

**Signature-based handling of Asserted information using
toKENs (SHAKEN):
Delegate Certificates**

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-1000092, Signature-based Handling of Asserted information using toKENS (SHAKEN): Delegate Certificates

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): Delegate Certificates

Alliance for Telecommunications Industry Solutions

Approved June 30, 2020

Abstract

The base SHAKEN framework enables a SHAKEN-authorized VoIP Service Provider to deliver a cryptographically protected assertion (the "attestation" value) to a terminating service provider that under specified conditions indicates the calling user is authorized to use the calling telephone number. This specification extends the base SHAKEN framework to enable SHAKEN-authorized TN Service Providers to issue delegate certificates defined in this document to their non-SHAKEN-authorized customers that allows the customer to prove it possesses an assignment or delegation of a calling TN to a SHAKEN originating service provider that is not also the TN Service Provider. This is one possible method for an originating service provider to determine that its customer's call is entitled to full attestation for certain enterprise or legitimate call spoofing scenarios where the originating service provider does not have a direct association with the calling entity and/or the calling TN.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, 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, & APPLICATION	1
1.1	SCOPE.....	1
1.2	PURPOSE.....	1
2	REFERENCES	3
2.1	NORMATIVE REFERENCES.....	3
2.2	INFORMATIVE REFERENCES	3
3	DEFINITIONS, ACRONYMS, & ABBREVIATIONS	3
3.1	DEFINITIONS.....	3
3.2	ACRONYMS & ABBREVIATIONS	5
4	OVERVIEW	7
4.1	OVERVIEW OF DELEGATE CERTIFICATE MANAGEMENT PROCEDURES	7
4.2	DELEGATE CERTIFICATES AND FULL ATTESTATION.....	9
5	DELEGATE CERTIFICATE MANAGEMENT.....	11
5.1	CERTIFICATE MANAGEMENT ARCHITECTURE.....	11
5.2	CERTIFICATE MANAGEMENT INTERFACES	12
5.3	CERTIFICATE MANAGEMENT PROCEDURES	14
5.3.1	<i>STI-SCA obtains an SPC Token from STI-PA.....</i>	<i>14</i>
5.3.2	<i>STI-SCA obtains a CA Certificate from STI-CA.....</i>	<i>15</i>
5.3.3	<i>VoIP Entity obtains a Delegate Certificate from STI-SCA</i>	<i>15</i>
5.3.4	<i>Issuing Delegate End-Entity Certificates to SHAKEN SPs.....</i>	<i>19</i>
5.3.5	<i>Delegate Certificate Revocation</i>	<i>20</i>
5.3.6	<i>Delegate Certificate Profile</i>	<i>20</i>
6	AUTHENTICATION AND VERIFICATION USING DELEGATE CERTIFICATES	21
6.1	DELEGATE CERTIFICATE AUTHENTICATION PROCEDURES FOR BASE PASSPORTS	21
6.2	DELEGATE CERTIFICATE VERIFICATION PROCEDURES FOR BASE PASSPORTS	22
6.2.1	<i>Verification of base PASSporTs signed with Delegate Certificate credentials for determining attestation level of “shaken” PASSporTs</i>	<i>24</i>

Table of Figures

FIGURE 4.1	– DELEGATE CERTIFICATE MANAGEMENT FLOW.....	8
FIGURE 4.2	– USING DELEGATE CERTIFICATES TO DEMONSTRATE THAT FULL ATTESTATION CRITERIA ARE SATISFIED	10
FIGURE 5.1	– DELEGATE CERTIFICATE MANAGEMENT ARCHITECTURE.....	12
FIGURE 6.1	– DISTINGUISHING BETWEEN DELEGATE AND SHAKEN CERTIFICATES	23
FIGURE 6.2	– DETERMINING WHEN TO PERFORM SCOPE ENCOMPASSING CHECKS FOR DELEGATE CERTIFICATES	24

ATIS Standard on –

SHAKEN: Delegate Certificates

1 Scope, Purpose, & Application

1.1 Scope

This specification extends the SHAKEN certificate management framework to enable a telephone number (TN) service provider (TNSP) to create telephone number or range of telephone numbers specific certificates for entities that do not have access to STI certificates. The mechanisms described in this specification are based on the STI delegate certificate procedures defined in draft-ietf-stir-cert-delegation [Ref 13]. In order to manage the security and integrity of the overall SHAKEN ecosystem, this specification defines both the procedures for the entity with authority over a set of telephone number(s) to create and manage delegated certificates scoped only to the specific set of TNs assigned to the delegate certificate holder, and, in addition, the use of those credentials to create end-entity delegate certificates for authenticated end users or other VoIP entities to provide a reference to an originating service provider (OSP) or other party in the call flow, so the OSP or other party can verify a Personal Assertion Token (PASSporT) sent in the end user or other VoIP entity's SIP signaling.

1.2 Purpose

The purpose of the SHAKEN framework is to provide a set of tools that enables verification of the calling party's authorization to use a particular calling telephone number for a call. ATIS-100074, the SHAKEN protocol specification [Ref 1], describes criteria that can be invoked by the originating service provider (OSP) to "attest" to the legitimacy of the calling telephone number associated with a call. Three conditions must exist for a SHAKEN authentication service to fully attest (attestation level "A") that an originating customer can legitimately use the calling TN:

- 1) The signing provider must be responsible for the origination of the call onto the IP based service provider voice network.
- 2) The signing provider must have a direct authenticated relationship with the customer and can identify the customer.
- 3) The signing provider must have established a verified association with the calling telephone number

Condition 1 is relatively unambiguous; the originating service provider is the signing provider.

Condition 2 is satisfied for cases where the OSP has a direct User-to-Network Interface (UNI) relationship with the originating entity and has authenticated the originating entity. However, there are many deployment scenarios where an OSP serves a customer who in turn serves multiple other customers. For example, consider the case where a cloud communications provider serves multiple customers by providing access to the public telephone network via an OSP. In these customer-of-customer cases, where the OSP does not have a direct relationship with the originating entity, the delegate certificate mechanisms described in this document can provide the OSP authentication service with the information it needs to fully attest to the legitimacy of the calling TN.

Condition 3 is satisfied for the case where the OSP has authority over the calling TN, and has assigned the calling TN to the originating customer. However, there are a number of legitimate real-world call scenarios where this is not the case; i.e., where the OSP does not have direct knowledge of the set of TNs the calling user is authorized to use. Example scenarios where it is difficult to support condition 3 for attestation level "A" include the following (note, list is not exhaustive):

- A SIP-PBX obtains originating call service from multiple providers (e.g., for redundancy or least cost routing). In this case, the PBX can legitimately originate a call via one provider from a calling TN that it obtained from a different provider.
- An enterprise displays a Toll-Free callback number for Business to Consumer calls, and the Toll-Free number provider and originating provider are two separate entities.
- A "legitimate spoofing" service displays the subscriber's work TN for calls originated by the user's home phone.