**ATIS-1000092**

ATIS Standard on

# 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



## Table of Figures

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-1000074, 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.