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.

- An outbound dialing service automatically initiates calls on behalf of a business or other entity, and displays the business TN to the called users (e.g., school announces weather-related school closings to students, or airline sends flight information updates to its passengers).
- Wholesale TNs used by reseller SPs, Cloud Communication Providers, and others when they originate calls
- A contact center serving multiple enterprises from various locations originates calls using the unique calling TN specified by each enterprise.

The SHAKEN specification provides guidance to originating SPs on how they can satisfy the TN-legitimacy condition in order to provide full attestation for call scenarios where the OSP does not have a direct UNI relationship with the end user or other VoIP entity, or where the OSP is not the TNSP. For example, the OSP could establish the legitimacy of the calling TN as part of the service level agreement with the end user or other VoIP entity, or it could obtain the necessary TN assignment information from the TNSP using some “out-of-band” mechanism.

However, these mechanisms often have shortcomings. The service level agreement approach may be unworkable in practice due to a low level of trust between the OSP and customer. Or, the OSP may have no relationship with or knowledge of the TNSP. The TNSP itself may not know the identity of the end user or other VoIP entity that was ultimately assigned the TN (consider the case where the TNSP assigns the TN to a reseller, who then assigns the TN to one of the reseller’s customers). In customer-of-customer scenarios the OSP doesn’t even know the entity originating the call (i.e., the end user or other VoIP entity) making it difficult to “have a direct authenticated relationship with the indirect calling entity”. And finally, the ad-hoc and non-automated nature of some of these mechanisms may incur a large administrative overhead for the participating parties (e.g., the overhead required to establish relationships between otherwise unrelated providers) and could make full attestation non-viable in a number of enterprise scenarios.

The delegate mechanism defined in this specification addresses these shortcomings by providing an automated, protocol-based mechanism that provides an end user or other VoIP entity with the ability to create and sign a PASSporT on its calls using a set of credentials in the form of an asymmetric cryptography key pair associated with a delegate certificate that is specific to the telephone number resources that end user or other VoIP entity is authorized to use.

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-1000080, *SHAKEN: Governance Model and Certificate Management.*[1]

[Ref 3] Draft IPNNI-2020-00025R007 - *SHAKEN: Calling Name and Rich Call Data Handling Procedures (*draft included with this ATIS Standard)

[Ref 4] ATIS-1000085, *SHAKEN Support of "div" PASSporT*

[Ref 5] ATIS-1000088, *A Framework for SHAKEN Attestation and Origination Identifier.*[1]

[Ref 6] ATIS-0300251, *Codes for Identification of Service Providers for Information Exchange*

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

[Ref 8] RFC 4949, *Internet Security Glossary, Version 2.*[2]

[Ref 9] RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*[2]

[Ref 10] RFC 8225, *Personal Assertion Token.*[2]

[Ref 11] RFC 8226, *Secure Telephone Identity Credentials: Certificates.*[2]

[Ref 12] draft-ietf-acme-authority-token-tnauthlist, *TNAuthList profile of ACME Authority Token.* [2]

[Ref 13] draft-ietf-stir-cert-delegation, *STIR Certificate Delegation.* [2]

[Ref 14] RFC 8555, *Automatic Certificate Management Environment (ACME)*.[2]

2.2 Informative References

[Ref 101] draft-ietf-acme-authority-token, *ACME Challenges Using an Authority Token.* [2]

[Ref 102] TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).* [3]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

The following provides some key definitions used in this document.

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

[2] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

[3] Available from 3rd Generation Partnership Project (3GPP) at: < https://www.3gpp.org >

Caller ID: The originating or calling party's telephone number used to identify the caller carried either in the P-Asserted-Identity or From header fields in the Session Initiation Protocol (SIP) [Ref 7] messages.

Call Origination: In the context of this document, the OSP is responsible for the origination of the call onto the service provider voice network if the service provider receives the call via a UNI.

(Digital) Certificate: Binds a public key to a Subject (e.g., the end-entity). A certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object [Ref 8]. See also STI Certificate.

Certification Authority (CA): An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate [Ref 8].

Certificate Chain: See Certification Path.

Certification Path: A linked sequence of one or more public-key certificates, or one or more public-key certificates and one attribute certificate, that enables a certificate user to verify the signature on the last certificate in the path, and thus enables the user to obtain (from that last certificate) a certified public key, or certified attributes, of the system entity that is the subject of that last certificate. Synonym for Certificate Chain [Ref 8].

Certificate Revocation List (CRL): A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire [Ref 8].

Certificate Signing Request (CSR): A CSR is sent to a CA to request a certificate. A CSR contains a Public Key of the end-entity that is requesting the certificate.

Chain of Trust: Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain [Ref 8].

Certificate Validation: An act or process by which a certificate user established that the assertions made by a certificate can be trusted [Ref 8].

Company Code: A unique four-character alphanumeric code (NXXX) assigned to all Service Providers [Ref 6].

Customer: Typically a service provider's subscriber, which may or not be the ultimate end-user of the telecommunications service. A customer, for example, may be a person, enterprise, reseller, or value-added service provider [Ref 5].

End-Entity: An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of this document, an end-entity is a Service Provider, TNSP, or Voice over Internet Protocol (VoIP) Entity.

End user: The entity ultimately consuming the VoIP-based telecommunications service. For the purposes of this standard, an end user may directly be the customer of a service provider or may indirectly use the VoIP based telecommunications service through another entity such as a reseller or value-added service provider [Ref 5]. Note for the purposes of this standard that a delegate end-entity certificate may be associated with an entity that in operation may be an "end user" for a given set of calls or another entity that controls a UA in the call path between the end user and OSP (generally a "VoIP entity").

Fingerprint: A hash result ("key fingerprint") used to authenticate a public key or other data [Ref 8].

Identity: Either a canonical Address-of-Record (AoR) SIP Uniform Resource Identifier (URI) employed to reach a user (such as 'sip:alice@atlanta.example.com'), or a telephone number, which commonly appears in either a TEL URI [RFC 3966] or as the user portion of a SIP URI. See also Caller ID [Ref 9].

Private Key: In asymmetric cryptography, the private key is kept secret by the end-entity. The private key can be used for both encryption and decryption [Ref 8].

Public Key: The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography [Ref 8].

Public Key Infrastructure (PKI): The set of hardware, software, personnel, policy, and procedures used by a CA to issue and manage certificates [Ref 8].

Root CA: A CA that is directly trusted by an end-entity. See also Trust Anchor CA and Trusted CA [Ref 8].

Secure Telephone Identity (STI) Certificate: A public key certificate used by a service provider to sign and verify the PASSporT.

Secure Telephone Identity Subordinate CA (STI-SCA): An SCA that gets its certificate directly from an STI-CA.

Service Provider Code: In the context of this document, this term refers to any unique identifier that is allocated by a Regulatory and/or administrative entity to a service provider. In the US and Canada this would be a Company Code as defined in ATIS-0300251 [Ref 6].

Signature: Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [Ref 8].

Subordinate CA (SCA): A CA whose public-key certificate is issued by another (superior) CA [Ref 8].

Telephone Identity: An identifier associated with an originator of a telephone call. In the context of the SHAKEN framework, this is a SIP identity (e.g., a SIP URI or a TEL URI) from which a telephone number can be derived.

Trust Anchor: An established point of trust (usually based on the authority of some person, office, or organization) from which a certificate user begins the validation of a certification path. The trust anchor is a combination of a trusted public key and the name of the entity to which the corresponding private key belongs [Ref 8].

Trust Anchor CA: A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key. See also Root CA and Trusted CA [Ref 8].

Trusted CA: A CA upon which a certificate user relies for issuing valid certificates; especially a CA that is used as a trust anchor CA [Ref 8].

Verified Association: In the context of this document a signing provider can establish a verified association with a telephone number by 1) having a direct UNI relationship with the originating entity (i.e., end user) and verifying their right to use the calling telephone number, or 2) verifying a PASSporT signed with a delegate certificate that cryptographically verifies the association between the originating entity (i.e., end user) and the calling telephone number.

VoIP Entity: A non-STI-authorized end user entity or other calling entity that purchases (or otherwise obtains) delegated telephone numbers from a TNSP.

VoIP Entity Subordinate Certificate Authority (V-SCA): An SCA that gets its certificate from an STI-SCA or from another V-SCA.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
ATIS	Alliance for Telecommunications Industry Solutions
CRL	Certificate Revocation List
CPaaS	Communications Platform as a Service
CPS	Call Placement Service
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IP	Internet Protocol
JSON	JavaScript Object Notation
KMS	Key Management System
NNI	Network-to-Network Interface
OID	Object Identifier
OSP	Originating Service Provider

PASSporT	Personal Assertion Token
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
SCA	Subordinate Certification Authority
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SKS	Secure Key Store
SP	Service Provider
SPC	Service Provider Code
STI	Secure Telephone Identity
STI-AS	Secure Telephone Identity Authentication Service
STI-CA	Secure Telephone Identity Certification Authority
STI-CR	Secure Telephone Identity Certificate Repository
STI-SCA	Secure Telephone Identity Subordinate Certification Authority
STI-VS	Secure Telephone Identity Verification Service
STIR	Secure Telephone Identity Revisited
TN	Telephone Number
TNSP	TN Service Provider
TSP	Terminating Service Provider
UNI	User-to-Network Interface
URI	Uniform Resource Identifier
V-SCA	VoIP Entity Subordinate Certificate Authority
VoIP	Voice over Internet Protocol

4 Overview

SHAKEN uses the protocols and mechanisms defined by the IETF Secure Telephone Identity Revisited (STIR) Working Group. The STIR document [Ref 11] describes a credential system in the form of STI certificates that enables telephone service providers to cryptographically assert authority over telephone numbers. The scope of an STI certificate is expressed by the certificate's TNAuthList object. As defined in RFC 8226 [Ref 11], a TNAuthList can identify the set (or a subset) of TNs assigned to the certificate holder. Alternatively, the TNAuthList may contain a Service Provider Code (SPC) value assigned to the TNSP holding the certificate, with the implication that it identifies all of the telephone numbers associated with that identifier for the service provider.

To avoid unnecessary complexity, the SHAKEN specifications profile the STI certificate scoping mechanism provided by RFC 8226 [Ref 11]. ATIS-1000080 [Ref 2] restricts the contents of a SHAKEN certificate TNAuthList object to a single SPC value assigned to the SHAKEN SP holding the certificate. Furthermore, ATIS-1000074 [Ref 1] utilizes the SPC value in the TNAuthList solely as an identifier of the signing SP independent of the calling TN. This enables a SHAKEN-compliant SP to provide full attestation for a customer originating a call from a calling TN assigned by a different TN service provider. These simplifications are justified given that a SHAKEN SP must pass a very rigorous STI-PA vetting process in order to obtain a SHAKEN certificate.

The delegate certificate mechanism described in this document provides a way to extend the SHAKEN credential system to enable non-SHAKEN entities such as enterprise PBXs to create and sign a PASSporT (for example an RFC 8225 base PASSporT [Ref 10]) to demonstrate its association with the calling TN when initiating calls onto the public telephone network. The delegated certificate authorization model is hierarchical. At the top of the hierarchy, the STI-PA authenticates the identity of the TNSP, and authorizes the TNSP to issue delegate certificates to its customers. Since non-SHAKEN entities are not vetted directly by the STI-PA, this document mandates that the scope of a delegate certificate issued to an entity must identify only TNs that the entity is authorized to use. This means that the TNAuthList of a delegate certificate can obtain one or more single TNs, and/or one or more TN ranges assigned to the certificate holder. Although draft-ietf-stir-cert-delegation [Ref 13] defines a passed-by-reference option for the TNAuthList, this specification does not incorporate this option, but recognizes it as a future consideration. This more rigorous application of the RFC 8226 [Ref 11] scoping mechanism enables verifiers such as an OSP to explicitly verify that the delegate certificate holder is authorized to use any TN signed by the delegate certificate credentials.

By signing an originating call with delegate certificate credentials, a non-SHAKEN entity can demonstrate its authority to use the calling TN. This provides the SHAKEN authentication service in the OSP's network with sufficient information to satisfy the full attestation criteria, therefore enabling it to deliver a standard SHAKEN PASSporT with "A" attestation to remote verification services.

4.1 Overview of Delegate Certificate Management Procedures

The delegate certificate management framework defines two new entities:

1) Telephone Number Service Provider (TNSP):
    - An entity that is authoritative over a set of telephone numbers, and that can delegate a subset of those telephone numbers to another entity to attest for signing. In the context of this document, a TNSP is a SHAKEN entity that is authorized by the STI-PA to obtain STI certificates from an STI-CA.
    - Ultimately, the entities entitled to obtain STI certificates will be defined by the STI-GA.
2) VoIP Entity:
    - A non-STI-authorized end user entity (i.e., a non-SHAKEN entity or other VoIP entity) that purchases (or otherwise obtains) delegated telephone numbers directly or indirectly from a TNSP.
    - Examples include a SIP-PBX serving a single enterprise customer, a Cloud Communications Provider serving multiple enterprise customers, a Contact Center making and receiving calls on behalf of multiple business entities, a legitimate spoofing application (e.g., call from personal phone delivers work calling number), or an automated outbound dialing service (e.g., school closing announcement).

Figure 4.1 provides a high-level overview of the certificate management process for issuing delegate end-entity certificates to a VoIP Entity using the STIR certificate delegation procedures defined in draft-ietf-stir-cert-delegation

[Ref 13]. The VoIP Entity is any non-SHAKEN X.509 entity that requires certificate credentials for signing STI PASSporTs.

The general process is as follows:

1) The TNSP obtains an SPC Token from the STI-PA that authorizes the TNSP to issue delegate certificates. The STI-PA will issue the SPC Token only if the SPC identified in the token is assigned to the requesting TNSP.
2) The STI-SCA uses the SPC Token from step-1 to obtain a CA certificate (i.e., an STI certificate but with BasicConstraints CA boolean is true) from an STI-CA[4]. The certification path of this newly issued CA certificate terminates at an STI-CA trusted root certificate.
3) Once it has obtained a CA certificate from an STI-CA, the STI-SCA can issue delegate certificates to VoIP Entities. Since the issued delegate certificate is a child of the TNSP CA certificate, its certification path terminates at an STI-CA's trusted root certificate. The issued delegate certificate gives the VoIP Entity the authority to sign STI PASSporTs containing an "orig" claim TN that is within the scope of the delegate certificate's TNAuthList.

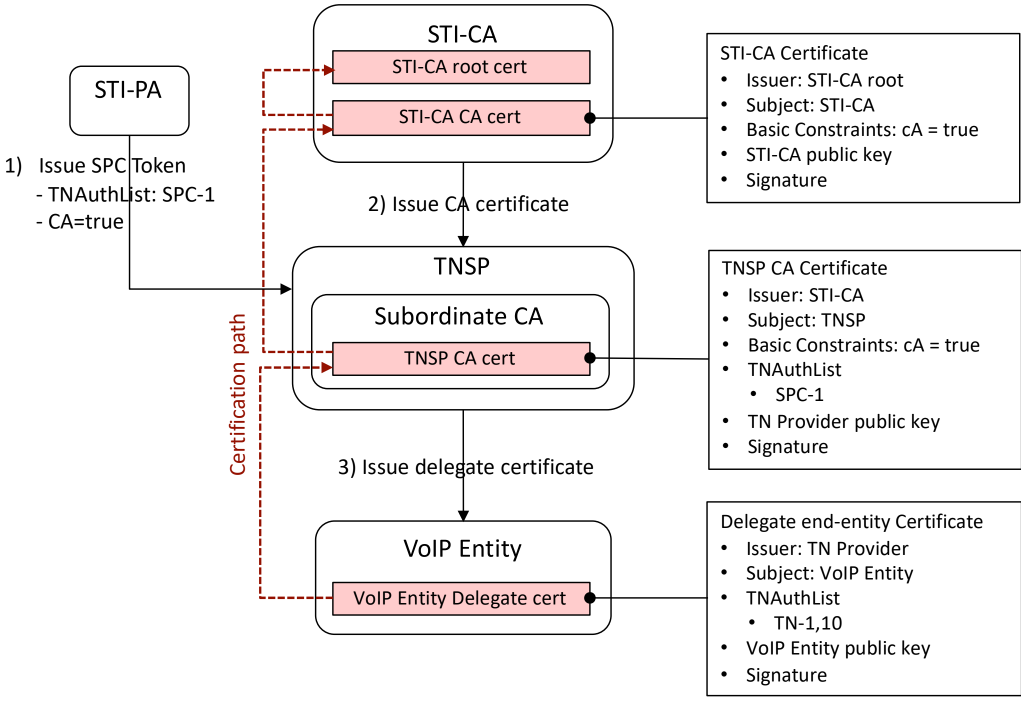


Figure 4.1 – Delegate Certificate Management Flow

Figure 4.1 shows the case where the STI-SCA issues a delegate end-entity certificate to the VoIP entity. The STI-SCA can also issue a delegate CA certificate to a V-SCA hosted by a non-SHAKEN VoIP Entity such as a reseller. The reseller can then use the delegate CA certificate as the parent to additional child delegate certificates issued to the reseller's customers. The scope of these child certificates must be encompassed by the scope of the parent delegate CA certificate.

[4] A TNSP that is also an OSP obtains two types of certificates; CA certificates for certificate delegation, and end entity certificates for SHAKEN authentication. The TNSP can obtain both types of certificates from the same STI-CA (or the same set of STI-CAs). Alternatively, the TNSP could choose to obtain the different certificate types from different STI-CAs.

4.2 Delegate Certificates and Full Attestation

ATIS-1000074 [Ref 1] defines three criteria that must be satisfied before an OSP can assert Full attestation.

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

By definition, an OSP, as the originating service provider, satisfies Full attestation criteria 1. Furthermore, an OSP that has a direct UNI relationship with the originating customer, and has assigned the calling TN to the customer, can satisfy criteria 2 and 3 with locally available information.

However, an OSP itself cannot easily satisfy criteria 2 and 3 with locally available information for cases where it does not have a direct relationship with the calling entity, and has no locally available association with the calling TN. An example of the use of delegate certificate credentials is shown in , where a non-shaken VoIP Entity (Enterprise-1) uses the services of a Communications Platform as a Service (CPaaS) to obtain access to the VoIP service provider network and acquires TNs directly from a TNSP. In the example, Enterprise-1 is assigned a range of TNs starting at +1 (250) 440-5000 from the TNSP (step A). The TNSP then issues a delegate certificate to Enterprise-1, with a scope that identifies the TNs assigned to the Enterprise (step B). At call origination time, Enterprise-1 signs a PASSporT with the delegate certificate credentials to provide its identity and to demonstrate to the OSP that it is authorized to use the calling TN (steps 1 and 2). Based on verification of a PASSporT traceable to the calling entity's identity and a set of authorized TNs, received from its CPaaS customer in INVITE "2", the OSP SHAKEN authentication service asserts Full attestation in INVITE "3" sent to the Terminating Service Provider (TSP).

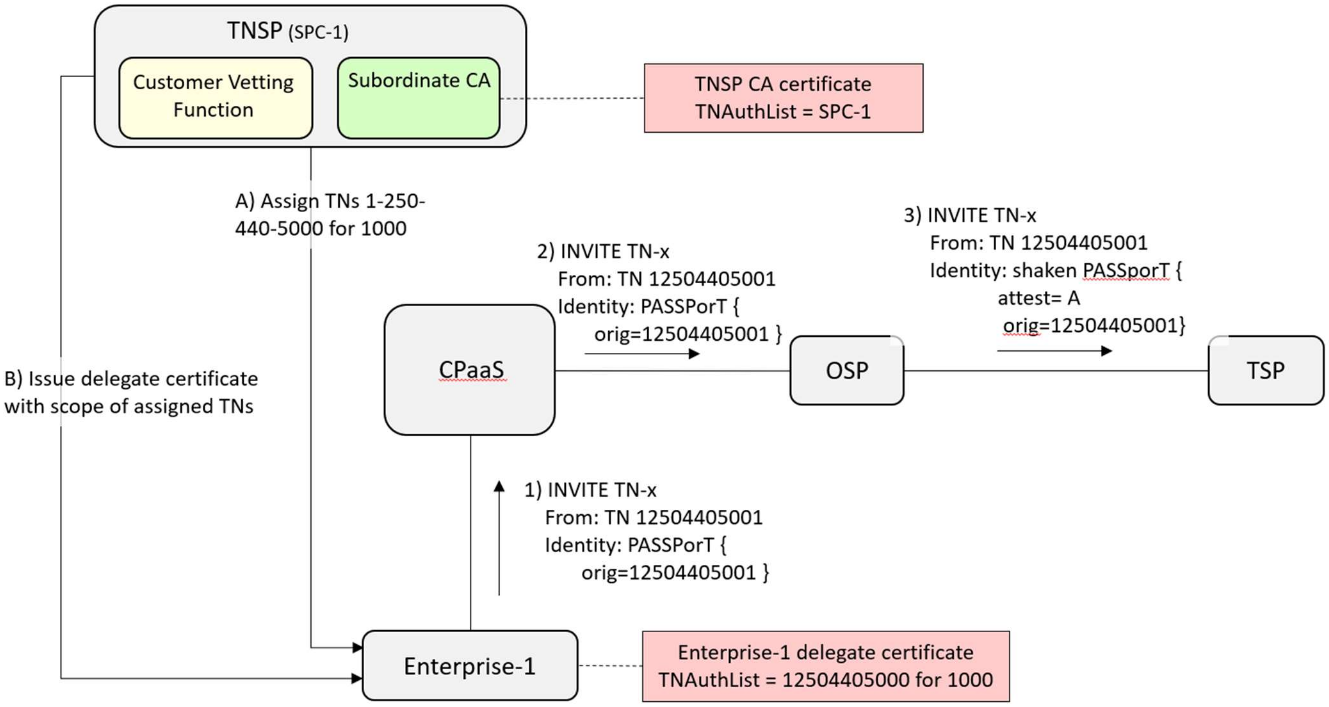


Figure 4.2 – Using delegate certificates to demonstrate that Full attestation criteria are satisfied

In this case, there are a number of preconditions that must be met for the OSP's verification of a PASSporT from an indirectly known calling entity to be considered equivalent to meeting Full Attestation criteria 2 and 3 for such a call. A governance and policy environment must be in place that makes participating TNSPs and/or other STI-SCA providers responsible to provide a certificate holder's valid identity information to any authorized OSP and other authorized bodies responsible for policy, regulatory, or law enforcement (industry traceback authorities, regulatory authorities, etc.). The TNSP and/or other entity that is fulfilling the STI-SCA function must execute an identity vetting process that establishes a verifiable identity for any entity receiving delegate certificate credentials, and the credentials must only indicate authorizations to that entity for valid directly assigned or delegated TNs.

The TNSP and/or other STI-SCA provider must also participate in enforcement mechanisms to respond to misuse of credentials for traffic originated through any OSP network.

The delegate certificate model supports multiple levels of delegation; e.g., where a STI-SCA issues a delegate CA certificate to a CPaaS, and the CPaaS V-SCA in turn issues delegate end entity certificates to its customers. In these multi-delegation-level cases the scope encompassing rules are strictly enforced for child certificates issued from delegate CA certificates (i.e., relying parties can detect if the scope encompassing rules are violated).

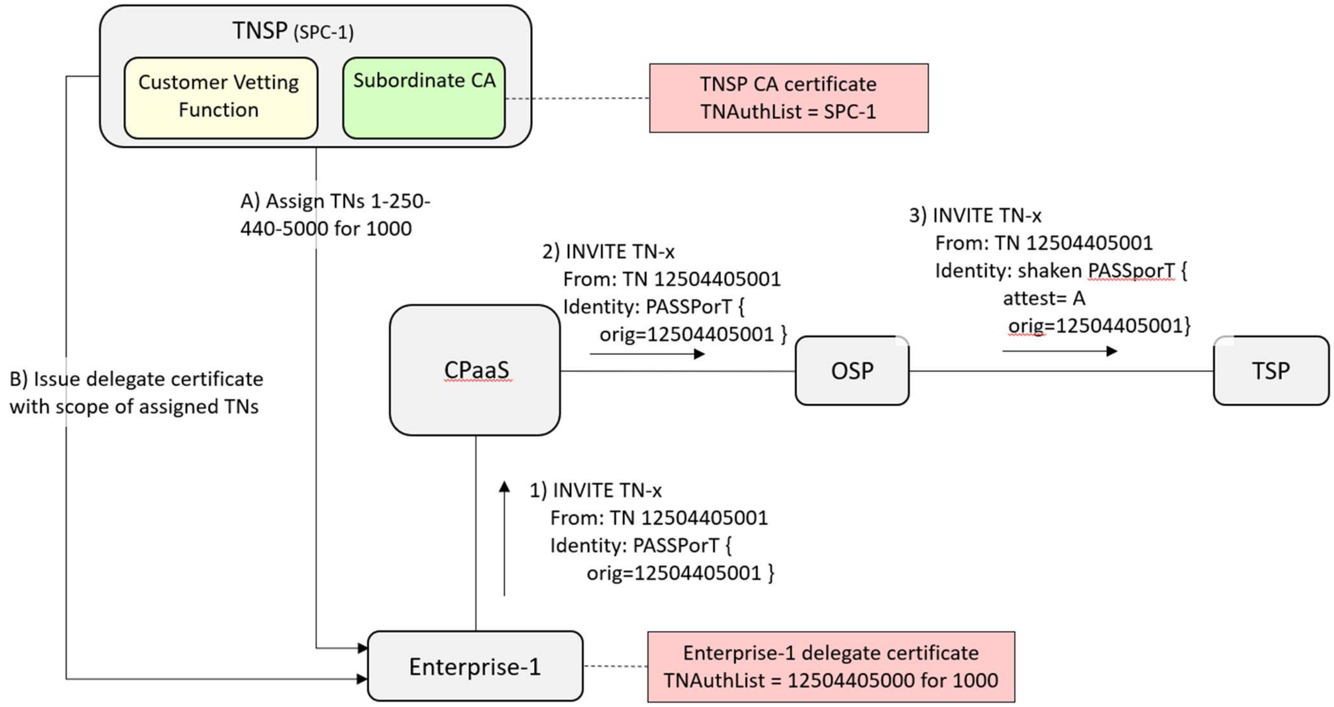


Figure 4.2 – Using delegate certificates to demonstrate that Full attestation criteria are satisfied

An OSP may use verification of a valid PASSporT signed with delegate certificate credentials as being equivalent to meeting Full attestation criteria 2 and 3, based on local policy. Example policies could include the following:

- An OSP chooses not to apply this attestation criteria procedure, and instead ignores all PASSporTs signed with delegate certificate credentials.
- An OSP chooses to apply this attestation criteria procedure for all valid PASSporTs signed with delegate certificate credentials.
- An OSP chooses to apply this attestation criteria procedure selectively based on different factors; e.g., based on the number of delegation levels, the identity of the UNI customer that sent the originating INVITE to the OSP, or the reputation of an entity identified in the certification path (e.g., the reputation of an entity hosting a STI-SCA/V-SCA or the identity indicated by the end-entity certificate).

5 Delegate Certificate Management

This clause describes the architecture, functional entities, interfaces, and procedures to issue delegate end-entity certificates to a VoIP Entity.

5.1 Certificate Management Architecture

Error! Reference source not found. shows how the SHAKEN certificate management architecture is extended to provide delegate end-entity certificates to a VoIP Entity. The TNSP hosts a STI-SCA that plays the role of a SHAKEN Service Provider defined in ATIS-1000080 [Ref 2] to obtain SPC Tokens from the STI-PA, and CA certificates from an STI-CA (i.e., from the perspective of the STI-PA and an STI-CA, the STI-SCA is the TNSP). The STI-SCA in turn plays the role of a CA in issuing delegate end-entity certificates to the VoIP Entity. The VoIP Entity is an entity that provides SIP-based VoIP services. For example, the VoIP Entity can be a VoIP provider or enterprise customer that has contractually leased telephone number resources from the TNSP. However, this same delegate certificate model could also be applied when the VoIP Entity is an originating service provider with direct responsibility for telephone numbers. This clause recommends that the STI-SCA issues delegate certificates to VoIP Entities using the ACME-based procedures described here. A STI-SCA may instead choose to issue delegate certificates using a different mechanism, as long as that mechanism has the same security properties as the procedures defined here.

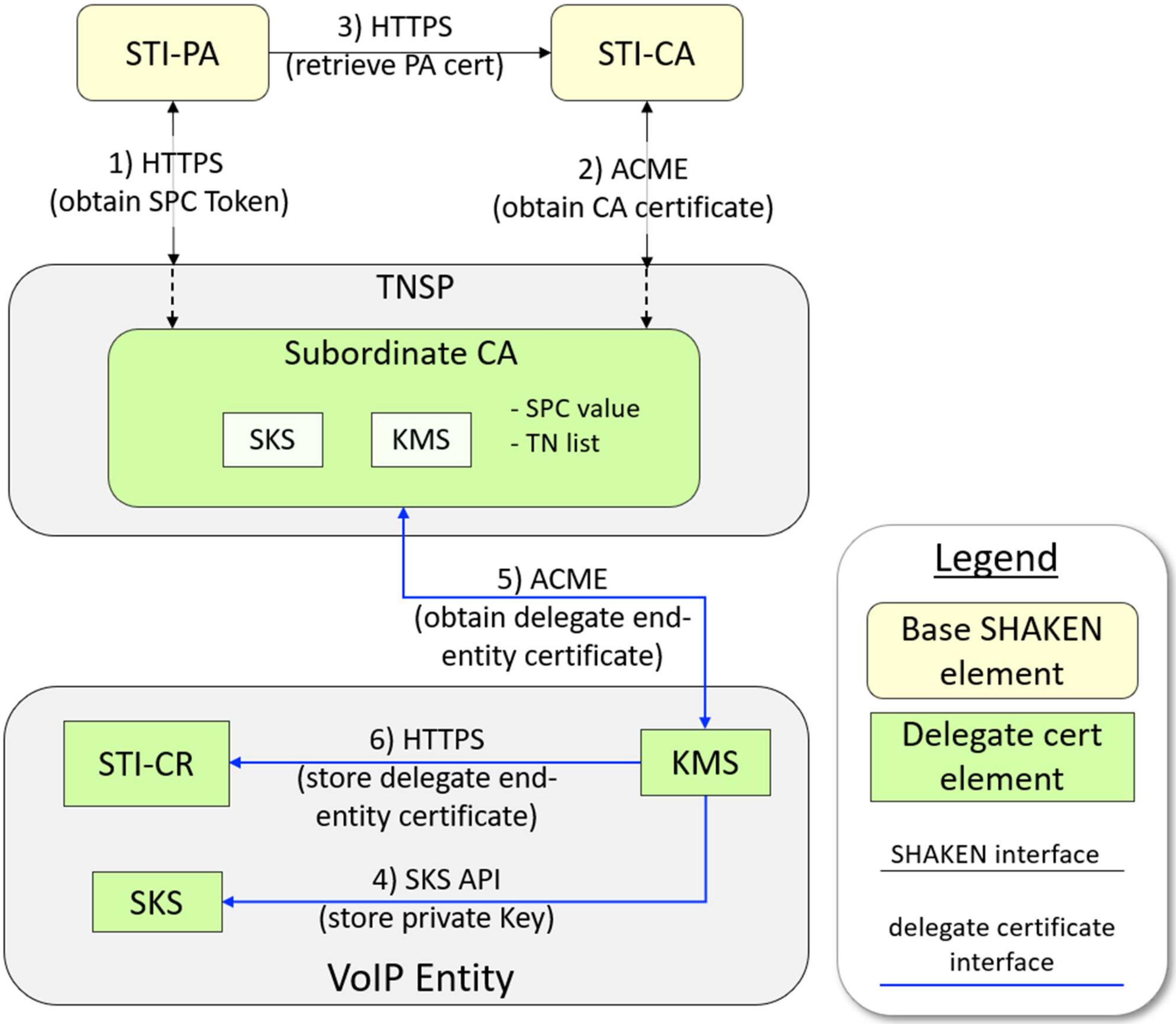


Figure 5.1 – Delegate Certificate Management Architecture

5.2 Certificate Management Interfaces

The STI-SCA obtains CA certificates from an STI-CA using interfaces 1), 2), and 3) of **Error! Reference source not found.**. Aside from the minor exceptions noted here, the procedures are identical to the certificate management procedures defined by ATIS-1000080 [Ref 2].

1) The STI-SCA obtains a fresh SPC Token from the STI-PA that authorizes the STI-SCA to obtain CA certificates from an STI-CA. The procedure is as specified in ATIS-1000080 [Ref 2], with the exception that the SPC Token “CA” boolean must be set to ‘true’.
2) Once the STI-SCA has obtained a valid SPC Token, it can order a CA certificate from an STI-CA using the procedure as specified in ATIS-1000080 [Ref 2].
3) During the authorization phase of the certificate ordering process, an STI-CA obtains the STI-PA certificate referenced by the SPC Token in order to verify the SPC Token signature, as specified in ATIS-1000080 [Ref 2].

At this point, the STI-SCA stores the newly issued CA certificate in preparation for issuing delegate end-entity certificates to the VoIP Entities that it serves. The VoIP Entity procedure to order a delegate end-entity certificate is similar to the STI end-entity certificate ordering procedure defined in ATIS-1000080 [Ref 2], except that the ACME account can be pre-authorized by leveraging the already-established security association between VoIP Entity and STI-SCA. This simplifies the ordering process, since the VoIP Entity does not have to obtain an SPC Token, and it does not have to respond to an ACME authorization challenge.

4) Following the procedures defined in ATIS-1000080 [Ref 2], the VoIP Entity Key Management System (KMS) generates two public/private key pairs; one for the ACME account, and one for the delegate end-entity certificate. It stores the private keys in its SKS.
5) The VoIP Entity orders a new delegate end-entity certificate using the certificate ordering procedure specified in ATIS-1000080 [Ref 2], minus the ACME authorization challenge/response steps (since the ACME account is pre-authorized). The STI-SCA signs the newly issued end-entity certificate with the private key of the CA certificate, and returns the URI where the newly issued certificate can be downloaded to the VoIP Entity. The VoIP Entity downloads the delegate certificate (including the certificates in the certification path).
6) The VoIP Entity stores the newly issued delegate end-entity certificate in its STI-CR.

Note: As an alternative, the STI-CR could be hosted by the TNSP instead of the VoIP Entity. In this case, the STI-SCA would store the newly issued delegate certificate in TNSP-hosted STI-CR and provide the VoIP Entity with the STI-CR URI reference to the delegate certificate in step 5. The VoIP Entity does not need to download the delegate certificate in step 6, but can simply include the STI-CR reference in the "x5u" field of the protected header of any PASSporT signed with the private key of this certificate.

5.3 Certificate Management Procedures

5.3.1 STI-SCA obtains an SPC Token from STI-PA

The STI-SCA shall obtain an SPC Token as described in ATIS-1000080 [Ref 2] with the exceptions noted in this clause.

As specified by ATIS-1000080 [Ref 2], the SPC Token request contains the “atc” JSON object defined in draft-ietf-acme-authority-token-tnauthlist [Ref 12]. The “atc” object identifies the type and scope of certificates authorized by the SPC Token. (Essentially, the STI-SCA is asking the STI-PA to issue an SPC Token that contains this same “atc” object.) In order to obtain an SPC Token that authorizes CA certificates, the token request “atc” object “CA” boolean shall be set to ‘true’. Otherwise, the token request “atc” object is populated as specified in ATIS-1000080 [Ref 2].

An example of a request for an SPC Token sent by the STI-SCA to the STI-PA is as follows:

```
POST /at/account/:id/token HTTP/1.1
Host: authority.example.com
Content-Type: application/json

{
 "atc":{"tktype":"TNAuthList",
   "tkvalue":"F83n2a...avn27DN3==",
   "ca":true,
   "fingerprint":"SHA256 56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:D3 \
   :BA:B9:19:81:F8:50:9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"}
}
```

On receiving the above token request, the STI-PA shall verify that the requesting STI-SCA is authorized to obtain CA certificates, and also that the requesting STI-SCA has authority over the SPC value identified in the received TNAuthList. If these verification checks pass, then the STI-PA shall construct an SPC Token containing the received “atc” object, as shown in the following example:

```
{ "typ":"JWT",
  "alg":"ES256",
  "x5u":https://authority.example.org/cert
}

{
 "iss":"https://authority.example.org/authz",
 "exp":1300819380,
 "jti":"id6098364921",
 "atc":{"tktype":"TnAuthList",
   "tkvalue":"F83n2a...avn27DN3==",
   "ca":true,
   "fingerprint":"SHA256
    56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:D3:BA:B9:19:81:F8:50:
    9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"}
}
```

The STI-PA shall sign the SPC Token with the private key of the STI-PA certificate referenced by the token’s “x5u” parameter, and return the token to the STI-SCA in a 200 OK response, as shown in the following example:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
"status":"success",
"token": "DGyRejmCefe7v4N...vb29HhjjLPSggwiE"},
"crl":"https://sti-pa.com/sti-pa/crl",
"message":"SPC Token granted"
}
```

5.3.2 STI-SCA obtains a CA Certificate from STI-CA

The STI-SCA shall create an ACME account and order a new CA certificate from an STI-CA using the procedures defined in ATIS-1000080 [Ref 2], with the exceptions noted in this clause.

During the finalize step of the ACME certificate ordering process, the STI-SCA shall request a CA certificate by including a BasicConstraints object in the CSR with the CA boolean set to ‘true’. When an STI-CA receives a CSR containing a BasicConstraints object with a CA boolean of ‘true’, it shall verify that the requesting STI-SCA is authorized to obtain CA certificates by checking that the SPC Token received in the challenge response contains a “ca” boolean with a value of ‘true’. If the STI-SCA is authorized to receive CA certificates, then an STI-CA shall issue a certificate containing a BasicConstraints object with a CA Boolean of ‘true’. An STI-CA shall populate the newly issued CA certificate with the TNAuthList identifier received in the ACME new-order request, as specified in draft-ietf-stir-cert-delegation [Ref 13]. (Note, as part of normal SHAKEN procedures, an STI-CA shall verify that the new-order TNAuthList and the CSR TNAuthList both match the "tkvalue" in the SPC Token challenge response.)

Once it has downloaded the newly issued CA certificate, the STI-SCA shall store the certificate locally (i.e., unlike end-entity certificates, the CA certificate is not stored in the STI-CR).

5.3.3 VoIP Entity obtains a Delegate Certificate from STI-SCA

The procedure to obtain a delegate certificate is a simplified version of the certificate ordering procedures defined in ATIS-1000080 [Ref 2] where the VoIP Entity KMS plays the role of the SP-KMS, and the STI-SCA plays the role of STI-CA.

> Note: This clause recommends that the STI-SCA issues delegate certificates to VoIP Entities using the ACME-based procedures described here. A STI-SCA may instead choose to issue delegate certificates using a different mechanism, as long as that mechanism has the same security properties as the procedures defined here.

5.3.3.1 Initial Conditions

As a pre-requisite to issuing delegate certificates, the STI-SCA must configure the VoIP Entity with the URL of the STI-SCA ACME directory resource, and the scope of delegate certificates that the VoIP Entity is authorized to obtain from the STI-SCA.

5.3.3.2 Creating an ACME Account with the STI-SCA

The VoIP Entity KMS and the STI-SCA shall support the ACME account creation process defined in ATIS-1000080 [Ref 2].

The account creation process is identical to that specified by ATIS-1000080 [Ref 2]. The VoIP Entity KMS shall generate a public/private key pair using the ES256 algorithm, to serve as credentials for the account, and shall send an HTTP POST request to the “newAccount” resource to create the ACME account, as shown in the following example:

```
POST /acme/new-account HTTP/1.1
Host: subordinate-ca.com
Content-Type: application/jose+json
{
  "protected": base64url({
     "alg": "ES256",
     "jwk": /* ACME account public key */,
     "nonce": "6S8IqOGY7eL2lsGoTZYifg",
     "url": "https:/subordinate-ca.com/acme/new-account"
  })
  "payload": base64url({
    "contact": [
       "mailto:cert-admin-kms01@voip-entity.com",
       "tel:+12155551212"
    ]
  }),
  "signature": /* signed using ACME account private key */
}
```

If the account already exists for the specified account key, then the STI-SCA shall send a “200 OK” response to the POST request. Otherwise, the STI-SCA shall create an account object and send a “201 Created” response, as shown in the following example:

```
HTTP/1.1 201 Created
Content-Type: application/json
Replay-Nonce: D8s4D2mLs8Vn-goWuPQeKA
Location: https://subordinate-ca.com/acme/acct/1
Link: <https://subordinate-ca.com/acme/some-directory>;rel="index"
{
  "status": "valid",
  "contact": [
    "mailto:cert-admin-kms01@voip-entity.com",
    "tel:+12155551212"
  ]
  "orders": "https://subordinate-ca.com/acme/acct/1/orders"
}
```

5.3.3.3 Pre-authorizing the ACME Account

The STI-SCA shall pre-authorize the new ACME account based on a security association with the VoIP Entity that was previously established via procedures outside the scope of this document. The STI-SCA shall provision an authorization object with a “status” of “valid”, with an empty set of challenges, and containing an “identifier” field of type “TNAuthList” with the ASN.1 encoding of the TN list pre-authorized for the VoIP Entity.

The STI-SCA shall advertise the URL of the authorization object in the “newAuthz” field of the directory object.

An example of the authorization object is as follows:

```
   {
     "status": "valid",
     "expires": "2018-03-01T14:09:00Z",

     "identifier": {
       "type":"TNAuthList",
       "value": "F83n2a...avn27DN3=="
     },

     "challenges": []
   }
```

5.3.3.4 Obtaining a new Delegate End-Entity Certificate from STI-SCA

The VoIP Entity KMS and STI-SCA shall support the pre-authorization certificate ordering and issuance process defined in RFC 8555 [Ref 14].

1) Ordering the Certificate

As the first step in applying for a new certificate, the VoIP Entity KMS shall provide an “identifiers” field in the new-order POST request of “type” of “TNAuthList”. The TNAuthList value shall identify the set (or a subset) of the TNs that were pre-provisioned by the STI-SCA (see 5.3.3.1). The TNAuthList must identify at least one TN.

> Note: As an alternative, the VOIP Entity KMS could simply use the TNAuthList contained in the authorization object (see Clause 5.3.3.3).

An example of the new-order POST request is as follows:

```
POST /acme/new-order HTTP/1.1
 Host: subordinate-ca.com
 Content-Type: application/jose+json
 {
   "protected": base64url({
     "alg": "ES256",
     "kid": " https://subordinate-ca.com/acme/acct/1",
     "nonce": "5XJ1L3lEkMG7tR6pA00clA",
     "url": " https://subordinate-ca.com/acme/new-order"
  })
   "payload": base64url({
     "identifiers": [{"type:"TNAuthList","value":"F83n2a...avn27DN3=="}],

     "notBefore": "2018-01-01T00:00:00Z",
     "notAfter": "2018-01-08T00:00:00Z"
   }),
  "signature": /* signed using ACME account private key */
}
```

2) Verifying the order

The STI-SCA shall verify that the “Identifiers” field in the new-order request is authorized by the “identifier” field of the pre-provisioned authorization object described in Clause 5.3.3.3 (i.e., the TNs must either match or be a subset of pre-authorized TNs).

If the request is valid, then the STI-SCA shall send a “201 Created” response containing the newly created order object, as shown in the following example:

```
   HTTP/1.1 201 Created
   Content-Type: application/json
   Replay-Nonce: MYAuvOpaoIiywTezizk5vw
   Location: https://subordinate-ca.com/acme/order/asdf
   {
     "status": "ready",
     "expires": "2016-01-01T00:00:00Z",

     "notBefore": "2016-01-01T00:00:00Z",
     "notAfter": "2016-01-08T00:00:00Z",
     "identifiers": [{"type:"TNAuthList","value":"F83n2a...avn27DN3=="}],

     "authorizations": [
       "https://subordinate-ca.com/acme/authz/1234"
     ],
     "finalize": "https://subordinate-ca.com/acme/order/asdf/finalize"
   }
```

The “authorizations” field contains the URL to the pre-provisioned authorization object described in Clause 5.3.3.3. The “finalize” field contains the URL that the VoIP Entity will use to finalize the order.

3) Finalizing the order

The VoIP Entity KMS knows that that the account is pre-authorized to issue the requested certificate based on the returned order object status of “ready”, and therefore shall proceed to finalize the order. (As an option, the VoIP Entity KMS may verify that the ACME account has been pre-authorized by performing an HTTP GET for the URL contained in the “authorizations” field in step-2, and check that the returned authorization object has a status of “valid”.)

To finalize the order, the VoIP Entity KMS shall create a CSR as specified in ATIS-1000080 [Ref 2], but containing a TNAuthList identical to the “identifiers” field of the new-order request in step-1. This means that the TNAuthList of a delegate certificate can contain one or more single TNs, and/or one or more TN ranges assigned to the certificate holder.

> Note: Although draft-ietf-stir-cert-delegation [Ref 13] defines a passed-by-reference option for the TNAuthList, this specification does not incorporate this option, but recognizes it as a future consideration.

The VoIP Entity KMS shall then finalize the order by sending an HTTP POST request to the “finalize” URL received in step-2, as shown in the following example:

```
POST /acme/order/asdf/finalize HTTP/1.1
Host: subordinate-ca.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://subordinate-ca.com/acme/acct/1",
    "nonce": "MSF2j2nawWHPxxkE3ZJtKQ",
    "url": "https://subordinaate-ca.tn-provider.com/acme/order/asdf/finalize"
  }),
  "payload": base64url({
    "csr": "5jNudRx6Ye4HzKEqT5...FS6aKdZeGsysoCo4H9P",
  }),
  "signature": /* signed using ACME account private key */
}
```

The STI-SCA shall respond to the finalize request with a “200 OK” response containing the order object, as shown in the following example:

```
HTTP/1.1 200 OK
Content-Type: application/json
Replay-Nonce: MYAuvOpaoIiywTezizk5vw
Location: https://subordinate-ca.com/acme/order/asdf
{
  "status": "processing",
  "expires": "2018-01-01T00:00:00Z",

  "notBefore": "2018-01-01T00:00:00Z",
  "notAfter": "2018-01-08T00:00:00Z",
  "identifiers": [{"type:"TNAuthList","value":"F83n2a...avn27DN3=="}],

  "authorizations": [
    "https://subordinate-ca.com/acme/authz/1234"
  ],
  "finalize": "https://subordinate-ca.com/acme/order/asdf/finalize"
}
```

At this point in the process, the STI-SCA shall execute the order by constructing a certificate containing the requested TNAuthList, and signed with the private key of the STI-SCA’s CA certificate. While the STI-SCA is filling the order, it shall maintain an order object status of “processing”.

4) Polling for the certificate

Once it has finalized the certificate order with the STI-SCA, the VoIP Entity KMS shall periodically poll the order object resource with a POST-as-GET request, as specified in ATIS-1000080 [Ref 2]. When the order has been filled, the STI-SCA shall store the newly issued certificate in the STI-CR, and shall indicate to the VoIP Entity KMS that the certificate is available by responding to the next poll as shown in the following example:

```
POST /acme/order/asdf HTTP/1.1
Host: subordinate-ca.com
Content-Type: application/jose+json

{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://subordinate-ca.com/acme/acct/1",
    "nonce": "uQpSjlRb4vQVCjVYAyyUWg",
    "url": "https://subordinate-ca.com/acme/new-order"
 }),
 "payload": "",
  "signature": "nuSDISbWG8mMgE7H...QyVUL68yzf3Zawps"
}


HTTP/1.1 200 OK
Content-Type: application/json
Replay-Nonce: MYAuvOpaoIiywTezizk5vw
Location: https://subordinate-ca.com/acme/order/asdf
{
  "status": "valid",
  "expires": "2018-01-01T00:00:00Z",

  "notBefore": "2018-01-01T00:00:00Z",
  "notAfter": "2018-01-08T00:00:00Z",
  "identifiers": [{"type:"TNAuthList","value":"F83n2a...avn27DN3=="}],

  "authorizations": [
    "https://subordinate-ca.com/acme/authz/1234"
  ],
  "finalize": https://subordinate-ca.com/acme/order/asdf/finalize
  "certificate": "https://sti-cr.tn-provider.com/cert-1"

}
```

Based on a pre-established agreement between the STI-SCA and VoIP Entity, the newly issued delegate end-entity certificate shall be stored in the STI-CR either by the STI-SCA or the VoIP Entity. If the STI-SCA stores the certificate in the STI-CR, then the VoIP Entity does not need to download the actual certificate. Instead, it can simply use the URI identified in the “certificate” field of the step-4 response to populate the “x5u” field in the PASSporT token created during STI authentication.

5.3.4 Issuing Delegate End-Entity Certificates to SHAKEN SPs

A SHAKEN Service Provider itself may want to sign PASSporTs, such as “rcd” PASSporTs, with a delegate end-entity certificate. For example, instead of obtaining short-lived SHAKEN end-entity certificates from an STI-CA, an OSP could obtain a long-lived CA certificate from an STI-CA using the procedures described above in Clause 5.3.2, and then use the CA certificate to efficiently issue new short-lived delegate end-entity certificates for its own use. Since it is both the producer and the consumer of the delegate end-entity certificates in this case, the OSP could use a proprietary mechanism to issue the delegate end-entity certificates from the CA certificate.

5.3.5 Delegate Certificate Revocation

Delegate certificates should generally be issued with short validity periods (24 to 48 hours is recommended), and therefore rely on passive revocation. The STI-PA CRL mechanism shall not be used for delegate certificate revocation.

5.3.6 Delegate Certificate Profile

This clause defines the certificate profile that must be supported for the following two types of certificates:

- Delegate certificate: a certificate that contains a TNAuthList identifying one or more TNs, and whose parent certificate contains a TNAuthList. Delegate certificates can be intermediate certificates (Basic Constraints CA boolean = true) or end entity certificates (Basic Constraints CA boolean = false).
- STI intermediate certificate held by the STI-SCA of a TNSP: an intermediate certificate that contains a TNAuthList identifying a single SPC value and whose parent is a STI certificate held by an approved STI-CA. This type of certificate is not a delegate certificate since its parent certificate does not contain a TNAuthList.

STI intermediate certificates held by the STI-SCA of a TNSP shall comply with all the SHAKEN intermediate certificate requirements in Clause 6.4.1 of ATIS-1000080 [Ref 2] with the following exceptions:

- The certificate shall contain a TNAuthList extension identifying a single SPC value,
- The Subject field Common Name attribute of a STI-SCA STI intermediate certificate shall comply with the Common Name attribute requirements for SHAKEN intermediate certificate as defined in ATIS-1000080 [Ref 2], with the exception that it shall not include the text string "SHAKEN”, shall include the text string "Subordinate CA", and shall identify the SPC value in the TNAuthList extension (e.g., "CN=Comcast Subordinate CA intermediate cert 1234").

Delegate intermediate and end entity certificates shall comply with the SHAKEN intermediate and end entity certificate requirements defined in ATIS-1000080 [Ref 2] with the following exceptions:

- A delegate certificate shall not contain a CRL Distribution Points extension,
- A delegate certificate shall contain a TNAuthList identifying one or more TNs,
- The Subject field Common Name attribute of a delegate certificate shall not contain the text string "SHAKEN", shall not contain an SPC value (since the TNAuthList does not contain an SPC value), shall contain the string "Delegate cert", and shall contain the string “Subordinate CA” if the Basic Constraints CA boolean is true (e.g., AAA Auto Repair, Delegate cert). The Common Name may contain the TN(s) identified in the TNAuthList extension of the delegate certificate.

Delegate certificates, and STI intermediate certificates held by the STI-SCA of a TNSP shall contain a Certificate Policies extension as specified in Clause 6.4.1 of ATIS-1000080 [Ref 2] with the exception that the Object Identifier (OID) shall identify a Certificate Policy Statement published by the STI-PA specifically for certificate delegation (i.e., an OID that is different than the SHAKEN Call Placement Service (CPS) OID referred to in ATIS-1000080 [Ref 2]).

6 Authentication and Verification using Delegate Certificates

The authentication and verification of PASSporTs and Identity headers that use Delegate Certificates is a function that is above and beyond the base authentication and verification procedures for "shaken" PASSporTs defined in ATIS-1000074 [Ref 1]. Therefore, delegate certificates must not be used to sign "shaken" PASSporTs. Per base SHAKEN verification procedures, a “shaken” PASSporT that is signed with delegate certificate credentials must be treated by the STI-VS as a verification failure.

Delegate certificate credentials may be used to sign PASSporT types other than "shaken" PASSporTs if and only if explicitly defined elsewhere. In these cases, the authentication and verification service procedures associated with delegate certificates is defined in the IETF and/or ATIS specification specific to the PASSporT type; e.g., the authentication procedures for signing "rcd" PASSporTs with delegate certificate credentials are defined in the draft IPNNI-2020-00025R007 - SHAKEN: Calling Name and Rich Call Data Handling Procedures [Ref 3].

Clause 6.1 of this document describes how delegate certificates can be used to sign base PASSporTs defined in RCF 8225 [Ref 10].

6.1 Delegate Certificate Authentication procedures for Base PASSporTs

An authentication service may sign a base PASSporT with delegate certificate credentials to demonstrate authority to use the telephone number identified in the PASSporT "orig" claim. In this case, the authentication service must construct the base PASSporT as follows:

- The protected header must be constructed as specified in RFC 8225 [Ref 10]. The "x5u" field must reference a delegate certificate chain, the “alg” must be “ES256”, and there shall be no "ppt" field.
- The payload "orig", "dest", and "iat" claims must be populated as specified in ATIS-1000074 [Ref 1].

An example of a base PASSPorT is as follows:

Protected Header

```
{   "alg":"ES256",

    "typ":"passport",

    "x5u":"https://del-cert.example.org/passport.cer"

}
```

Payload

```
{   "dest":{“tn”:["12155551213"]},

    "iat":1471375418,

    "orig":{“tn”:"12155551212"}

}
```

Authentication services that use delegate certificate credentials must ensure that the TNAuthList scope of a delegate end-entity certificate authoritatively covers the TN that it is asserting.

The authentication service shall add an Identity header field containing the signed PASSporT to the originating INVITE request as described in RFC 8224 [Ref 9].

An example of an INVITE request with an Identity header field that contains a signed base PASSporT is as follows:

```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---
77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+12155551213@tel.example1.net>
From: "Alice"<sip:+12155551212@tel.example2.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI
```

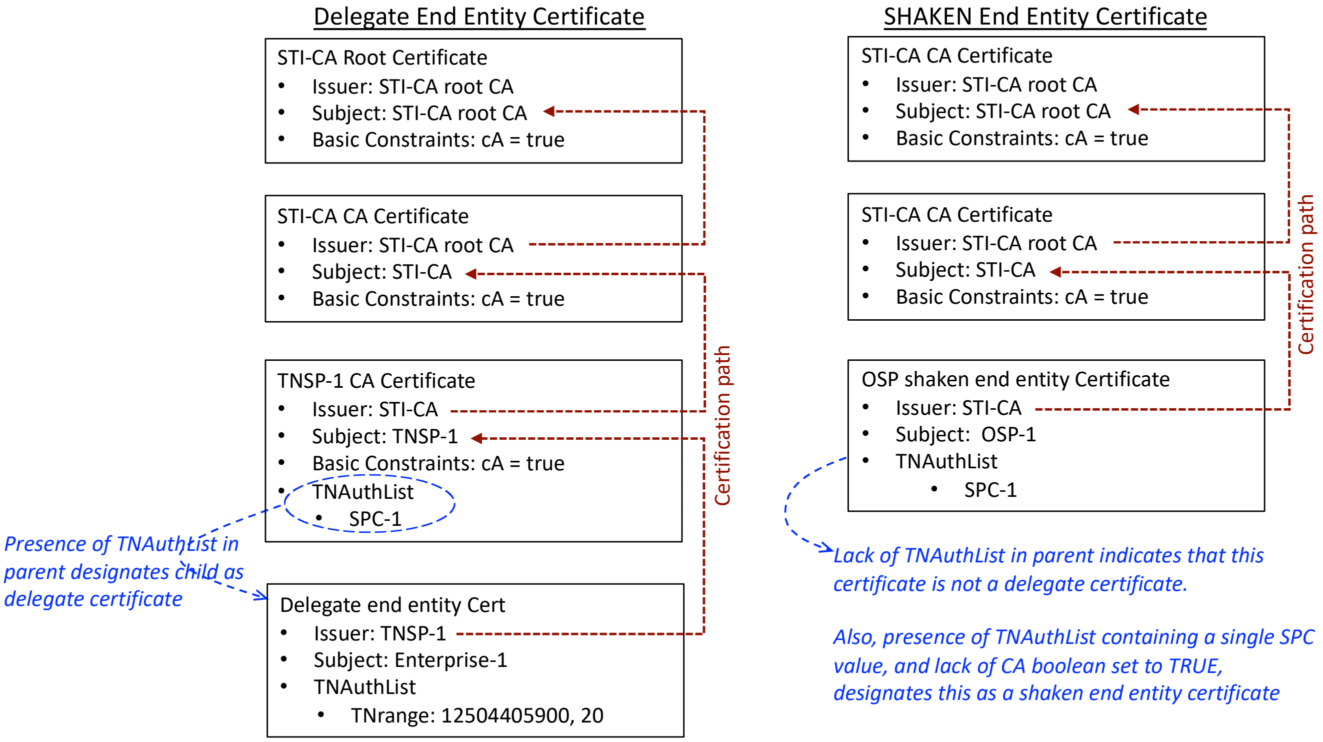
```
P-Asserted-Identity: "Alice"<sip:+12155551212@tel.example2.net>,<tel:+12155551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity:
eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9kZWwtY2VydC5leGFtcGx
lLm9yZy9wYXNzcG9ydC5jZXIifQo=.eyJkZXN0Ijp74oCcdG7igJ06WyIxMjE1NTU1MTIxMyJdfSwiaWF0I
joxNDcxMzc1NDE4LCJvcmlnIjp74oCcdG7igJ06IjEyMTU1NTUxMjEyIn19Cg==._V41ThRJ74MktxeLGaZ
QGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-EScb9otFNDxOCTjerg
;info=<https://del-cert.example.org/passport.cer>
Content-Length: 122


v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
s=-
c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv
```

6.2 Delegate Certificate Verification Procedures for Base PASSporTs

A verification service shall verify a base PASSporT defined in RFC 8225 [Ref 10] that is signed with delegate certificate credentials as specified in RFC 8224 [Ref 9]. In addition, the verification service shall verify that the value of the “orig”, “dest”, and “iat” claims of the base PASSporT are as specified in ATIS-1000074 [Ref 1] and ATIS-1000085 [Ref 4].

Verification services can detect when a PASSporT is signed by delegate certificate credentials by observing that the parent to the signing certificate contains a TNAuthList. For example, Figure 6.1 shows the certification path for two end entity certificates. The end entity certificate on the left is a delegate certificate because its parent contains a TNAuthList extension. The end entity certificate on the right is not a delegate certificate, because its parent certificate does not contain a TNAuthList extension (in this case the end entity certificate is a SHAKEN certificate, since the certificate itself contains a TNAuthList extension with a single SPC value).



Presence of TNAuthList in parent designates child as delegate certificate

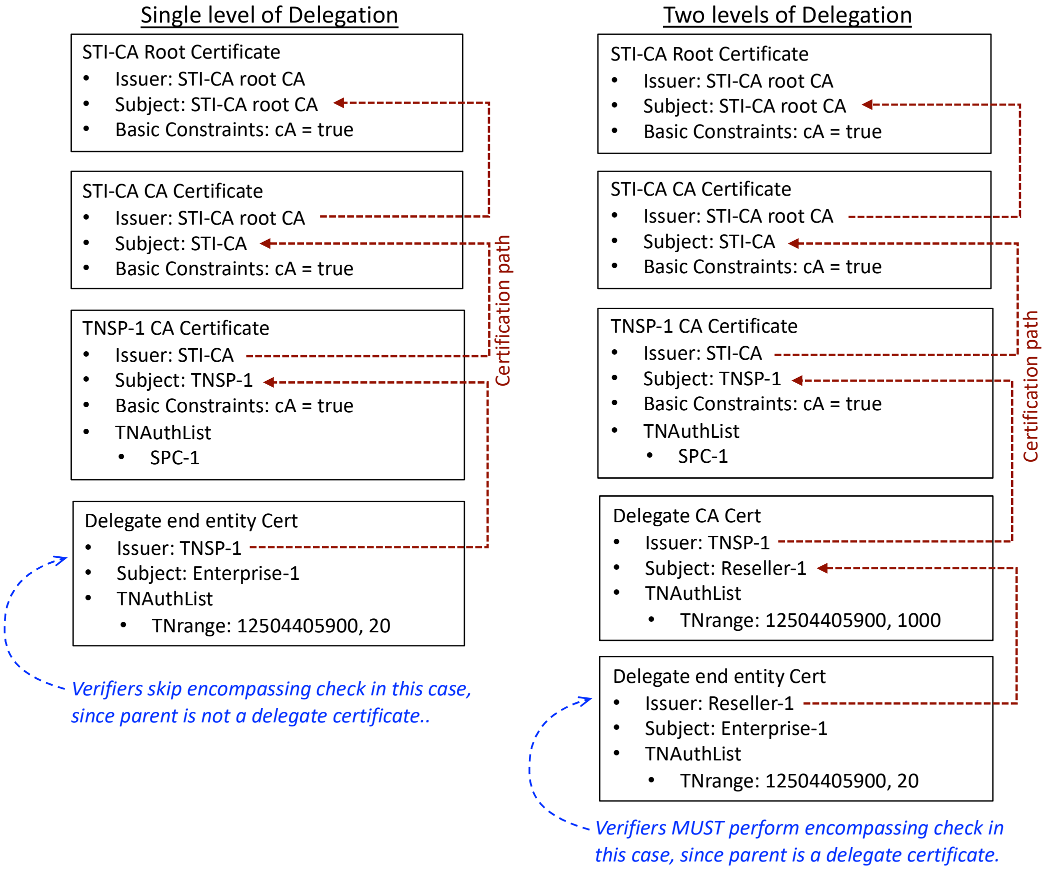
Lack of TNAuthList in parent indicates that this certificate is not a delegate certificate.

Also, presence of TNAuthList containing a single SPC value, and lack of CA boolean set to TRUE, designates this as a shaken end entity certificate

Figure 6.1 – Distinguishing between delegate and SHAKEN certificates

When verifying a base PASSporT signed with delegate certificate credentials, verifiers shall determine the validity of the certificate referenced in the “x5u” field in the base PASSporT protected header as specified in Clause 5.3.1 of ATIS-1000074 [Ref 1], with the following modifications:

- Verify that the certificates in the certification path contain a TNAuthList extension as specified in Clause 5.3 (e.g., delegate certificates must contain a TNAuthList identifying one or more TNs, the first non-delegate certificate encountered while traversing up the path from the signing certificate must contain a TNAuthList identifying a single SPC value).
- Verify that the PASSporT "orig" TN is within the scope of the signing certificate (i.e., the "orig" TN belongs to the set of TNs identified by the TNAuthList of the signing certificate).
- Verify that the scope of each delegate CA certificate in the certification path encompasses the scope of its child certificate. For example, if the parent of a delegate end entity certificate is itself a delegate certificate, then verifiers must check that the scope of the parent encompasses the scope of the child. However, if the parent of a delegate end entity certificate is not a delegate certificate, then verifiers shall skip the encompassing check (this would be the case where a Subordinate CA obtains a CA certificate from an STI-CA, and then issues child delegate end entity certificates from that CA certificate). These two cases are illustrated in Figure 6.2.



Verifiers skip encompassing check in this case, since parent is not a delegate certificate..

Verifiers MUST perform encompassing check in this case, since parent is a delegate certificate.

Figure 6.2 – Determining when to perform scope encompassing checks for delegate certificates

Any failure of the above certificate validation checks shall be treated as a verification failure (response code 437 'unsupported credential').

6.2.1 Verification of base PASSporTs signed with Delegate Certificate credentials for determining attestation level of “shaken” PASSporTs

This section describes the behavior when the delegate certificate signed PASSporT is consumed by an OSP for attestation determination. Base PASSporTs signed with delegate certificate credentials can be used as an optional mechanism to support the ability for an OSP authentication service to provide “A” level attestation to a “shaken” PASSporT defined by ATIS-1000074 [Ref 1].

A VoIP entity can demonstrate to the signing provider (i.e., the OSP) that it has a verified association with the calling telephone number, and therefore that it has the authority to use the calling TN, by populating the originating INVITE request with an "rcd" PASSporT signed with delegate certificate credentials (as described in draft IPNNI-2020-00025R007 – SHAKEN: Calling Name and Rich Call Data Handling Procedure [Ref 3]). For the case where the VoIP endpoint does not want to convey any rich call data to the called endpoint, it can demonstrate its authority to use the calling TN by providing a base PASSporT signed with delegate certificate credentials, as described in Clause 6.1.

If an OSP receives a base or rcd PASSporT in an Identity header of a INVITE request received from a UNI customer, the OSP should attempt to verify the received PASSporT to determine if the originating entity has authority to use the signaled Calling Number.

- If the base or rcd PASSporT verification passes, the OSP authentication service may, based on local policy, interpret this verification result as establishing that the entity populating the PASSporT has a known authenticated identity and an association with the calling TN. Armed with this attestation criteria information, the OSP shall perform the SHAKEN authentication procedures defined in ATIS-1000074 [Ref 1] and may assert an attestation level of Full or "A" attestation. The OSP shall sign the "shaken" PASSporT with SHAKEN certificate credentials [Ref 2] tied to its SPC.

- If the base or rcd PASSporT verification fails, the OSP authentication service should ignore this as input to determine the attestation level of a generated "shaken" PASSporT and follow the standard procedures of ATIS-1000074 [Ref 1] for determining attestation level as described in ATIS-1000074 [Ref 1] and based on local policy.

After the OSP has used the base PASSporT to determine shaken attestation level as described above, it shall discard the base PASSporT and not forward it to the TSP. Absent specification elsewhere, the OSP should apply this same rule for non-base PASSporT types signed with delegate certificate credentials.