**A****TIS-xxxxxxx.v000 (DRAFT)**

ATIS Technical Report on

**Technical Report on Governance and Management Considerations for Delegate Certificates**

**Alliance for Telecommunications Industry Solutions**

Approved Month day, 202x

**Abstract**

This document …

**Foreword**

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, 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[**ATIS-xxxxxxx.v000 (DRAFT)** i](#_Toc62070033)

[ATIS Technical Report on i](#_Toc62070034)

[**Alliance for Telecommunications Industry Solutions** i](#_Toc62070035)

[**Abstract** i](#_Toc62070036)

[Table of Contents iii](#_Toc62070037)

[Table of Figures iii](#_Toc62070038)

[1 Scope & Purpose 1](#_Toc62070039)

[1.1 Scope 1](#_Toc62070040)

[1.2 Purpose 1](#_Toc62070041)

[2 References 1](#_Toc62070042)

[2.1 Normative References 1](#_Toc62070043)

[2.2 Informative References 1](#_Toc62070044)

[3 Definitions, Acronyms & Abbreviations 1](#_Toc62070045)

[3.1 Definitions 1](#_Toc62070046)

[3.2 Acronyms & Abbreviations 3](#_Toc62070047)

[4 Overview of Delegate Certificates 4](#_Toc62070048)

[5 SHAKEN Governance Model and Certificate Management 5](#_Toc62070049)

[5.1 Governance Model Management of STI Certificates 5](#_Toc62070050)

[5.2 SHAKEN Governance Model and Management of Delegate Certificates 6](#_Toc62070051)

[5.2.1 Adding the STI-SCA 6](#_Toc62070052)

[5.2.2 Adding the V-SCA 7](#_Toc62070053)

[5.3 Policing the Information a non-SHAKEN VoIP Entity can Sign 7](#_Toc62070054)

[5.3.1 Encompassing TNs using TNAuthList 8](#_Toc62070055)

[5.3.2 Constraining Rich Call Data using JWTClaimConstraints 8](#_Toc62070056)

[6 Delegate Certificate Use Cases 9](#_Toc62070057)

[6.1 Identifying Delegate Certificate Entities for Traceback 9](#_Toc62070058)

# Table of Figures

[Figure 5.1 – Governance Model for Certificate Management 6](#_Toc61625897)

[Figure 5.2 – SHAKEN Governance Model for Delegate Certificate Management 7](#_Toc61625898)

# Scope & Purpose

## Scope

This technical report introduces …

## Purpose

…

# 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.

## Normative References

[Ref 1] ATIS-1000074, *Signature-based Handling of Asserted Information using Tokens (SHAKEN).*[[1]](#footnote-2)

[Ref 15] RFC 7519, *JSON Web Token (JWT).*2

[Ref 16] RFC 8226, *Secure Telephone Identity Credentials: Certificates.*2

## Informative References

[Ref 107] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules[[2]](#footnote-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> >.

## Definitions

The following provides some key definitions used in this document. Refer to IETF RFC 4949 [Ref 9] for a complete Internet Security Glossary, as well as tutorial material for many of these terms.

**(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 9]. 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 9].

**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 [Ref 9]. Synonym for Certificate Chain.

**Certificate Policy (CP):** A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [Ref 6].

**Certification Practice Statement (CPS):** A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates [Ref 6].

**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 9].

**CPS Summary (or CPS Abstract)** – A subset of the provisions of a complete CPS that is made public by a CA [Ref 6].

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

**Certificate Validation:** An act or process by which a certificate user established that the assertions made by a certificate can be trusted [Ref 9].

**Chain of Trust:** Deprecated term referring to the chain of certificates to a Trust Anchor. Synonym for Certification Path or Certificate Chain [Ref 9].

**Company Code:** A unique four-character alphanumeric code (NXXX) assigned to all Service Providers [Ref 3].

**End-Entity:** An entity that participates in the Public Key Infrastructure (PKI). Usually a Server, Service, Router, or a Person. In the context of SHAKEN, it is the Service Provider on behalf of the originating endpoint.

**Identity:** Unless otherwise qualified, an identifier that unambiguously distinguishes an entity for authentication and other security and policy application purposes. In this report, a Service Provider Code is an example of the identity of one kind of participant in the certificate management process.

**National/Regional Regulatory Authority (NRRA):** A governmental entity responsible for the oversight/regulation of the telecommunication networks within a specific country or region.

NOTE: Region is not intended to be a region within a country (e.g., a region is not a state within the US).

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

**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 aCompany Code as defined in ATIS-0300251 [Ref 3].

**Service Provider Code (SPC) Token:** An authority token that can be used by a SHAKEN Service Provider during the ACME certificate ordering process to demonstrate authority over the identity information contained in the TN Authorization List extension of the requested STI certificate. The SPC Token complies with the structure of the TNAuthList Authority Token defined by draft-ietf-acme-authority-token-tnauthlist [Ref 4], but with the restriction for SHAKEN where the TNAuthList value contained in the token’s “atc” claim identifies a single Service Provider Code.

**Signature:** Created by signing the message using the private key. It ensures the identity of the sender and the integrity of the data [Ref 9].

**Subscriber**: A user that is registered in a PKI and, therefore, can be named in the “subject” field of a certificate issued by a CA in that PKI [Ref 9].

**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 combination of a trusted public key and the name of the entity to which the corresponding private key belongs [Ref 9].

**Trust Anchor CA:** A CA that is the subject of a trust anchor certificate or otherwise establishes a trust anchor key [Ref 9]. See also Root CA and Trusted CA.

**Trust Authority:** An entity that manages a Trust List for use by one or more relying parties [Ref 10].

**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 9].

**Trust List:** A set of one or more trust anchors used by a relying party to explicitly trust one or more PKIs [Ref 10].

**Trust Model:** Describes how trust is distributed from Trust Anchors.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ACME | Automated Certificate Management Environment (Protocol) |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CA | Certification Authority |
| CRL | Certificate Revocation List |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CSR | Certificate Signing Request |
| HTTPS | Hypertext Transfer Protocol Secure |
| IETF | [Internet Engineering Task Force](http://www.ietf.org/rfc.html) |
| JSON | JavaScript Object Notation |
| JWT | JSON Web Token |
| NNI | Network-to-Network Interface |
| NRRA | National/Regional Regulatory Authority |
| NRRO | National/Regional Regulatory Oversight |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure for X.509 Certificates |
| PMA | Policy Management Authority |
| PTSC | ATIS Packet Technologies and Systems Committee |
| SHAKEN | Signature-based Handling of Asserted information using toKENs |
| SIP | Session Initiation Protocol |
| REST | Representational State Transfer |
| SKS | Secure Key Store |
| SP | Service Provider |
| SP-KMS | SP Key Management Server |
| 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-GA | Secure Telephone Identity Governance Authority |
| STI-PA | Secure Telephone Identity Policy Administrator |
| STI-VS | Secure Telephone Identity Verification Service |
| STIR | Secure Telephone Identity Revisited |
| TN | Telephone Number |
| URI | Uniform Resource Identifier |
| VoIP | Voice over Internet Protocol |

# Overview of Delegate Certificates

*Provide brief overview of delegate certificates…*

# SHAKEN Governance Model and Certificate Management

Delegate certificates add a new type of certificate authority – the Subordinate CA (SCA) – to the SHAKEN framework defined in ATIS-1000080. As defined in RFC 4949, an SCA is a CA that obtains its intermediate certificate from another CA. Per ATIS-1000092, SHAKEN supports two types of SCAs; an STI-SCA that provides the SCA function to a SHAKEN-approved Service Provider (SP), and a V-SCA that provides the SCA function to a non-SHAKEN VoIP Entity. Any certificate issued by an STI-SCA or a V-SCA chains to the trusted root certificate of an approved STI-CA.

## Governance Model Management of STI Certificates

ATIS-1000080 and ATIS-1000084 define a framework and set of procedures that enable an STI-CA or SP to achieve SHAKEN-approved status; specifically, the procedures to verify an STI-CA is authorized to issue STI certificates, and the procedures to verify that an SP is authorized to obtain STI certificates. In addition, ATIS-1000080 specifies the certificate management procedures that enable a SHAKEN-approved SP to obtain STI certificates from a SHAKEN-approved STI-CA.

The SHAKEN governance model and certificate management framework defined in ATIS-1000080 and ATIS-1000084 is shown in Figure 5.1,



Figure 5.1 – Governance Model for Certificate Management

Referencing Figure 5.1, the basic information flow for the governance and management of STI certificates is as follows:

1. The STI-GA establishes the policies and procedures that must be applied by the STI-PA to verify that an entity can play the role of an STI-CA or an SP. The policies include the Certificate Policy (CP) that must be supported by approved STI-CAs.
2. and 3) The STI-PA verifies that the Certificate Policy Statement provided by the STI-CA complies with the CP specified by the STI-GA.
3. Once the STI-CA is approved, the STI-PA adds the STI-CA’s root certificate in the Trusted STI-CA List. Relying parties verify that the STI SHAKEN PASSporT "x5u" certificate chains to a root certificate on the list.
4. The STI-PA verifies that the SP meets the criteria set by the STI-GA for obtaining SP SHAKEN-approved status; e.g., SP has been assigned a valid Service Provider Code (SPC) by a regulatory authority. Once approved, the SP can obtain SPC Tokens from the STI-PA. The scope of the token identifies an SPC assigned to the SP, and the CA boolean is set to false. Essentially, this token authorizes the SP to obtain STI end entity certificates whose scope identifies an SPC assigned to the SP holding the token.

Note: ATIS-1000080 defines the CA boolean as part of the SPC Token, but specifies its usage only for the case where the CA boolean is false. The procedures for CA=True are defined in ATIS-1000092, and described in clause 5.2 of this technical report.

1. The SP requests an STI certificate from an STI-CA, providing the SPC Token obtained from the STI-PA to demonstrate its authority to obtain the certificate.
2. The STI-CA validates the SPC Token, and if valid, issues the requested STI end entity certificate to the SP. The SP can now use the issued certificate credentials to sign SHAKEN PASSporTs.

## SHAKEN Governance Model and Management of Delegate Certificates

### Adding the STI-SCA

As shown in Figure 5.2, ATIS-1000092 introduces a new functional entity into the SHAKEN framework – the STI-SCA – which plays the role of a Subordinate CA as defined in RFC 4949. ATIS-1000092 shows a deployment model where the STI-SCA function is supported by a SHAKEN-approved SP such as a TNSP. Figure 5.2 shows a different but equally valid deployment model where the SP establishes a contractual agreement with an external entity to obtain STI-SCA services.

The STI-SCA is a function bound by the policies set forth in a CPS based on the STI-GA CP. The STI-SCA has a relationship with a Service Provider similar to an STI-CA, but with some minor differences as detailed later in this document. An STI-SCA function can also be supported by the same entity that offers STI-CA services, and use the same CPS to cover the policies of both CAs.



Figure 5.2 – SHAKEN Governance Model for Delegate Certificate Management

Referencing Figure 5.2, the basic information flow for the governance and management of delegate certificates is as follows:

1. The STI-GA procedure is the same as described for Figure 5.1, with two primary additions; a) the CP is updated to specify any CA policies unique to an STI-SCA, and b) the STI-PA can authorize an SP to obtain an SPC Token with the CA boolean set to True.
2. and 3) The STI-PA verifies that the Certificate Policy Statement provided by the STI-SCA complies with the CP specified by the STI-GA.
3. The STI-PA verifies that the SP meets the criteria set by the STI-GA for obtaining SP SHAKEN-approved status; e.g., the SP has been assigned a valid Service Provider Code (SPC) by a regulatory authority. In addition, the STI-PA verifies that the SP is authorized to issue delegate certificates to its customers. Once this verification process is complete, the SP can obtain SPC Tokens from the STI-PA containing an SPC value assigned to the SP and with the CA Boolean set to True.
4. The SP requests an STI intermediate certificate from an STI-CA, providing the SPC Token obtained from the STI-PA to demonstrate its authority to obtain the certificate. The request includes a TNAuthList containing an SPC assigned to the SP.
5. The STI-CA validates the SPC Token, and if valid, issues the requested STI intermediate certificate to the SP. The SP then passes the intermediate certificate and its credentials to the STI-SCA.

At this point, the SP can interwork with the STI-SCA via interface 10) to issue delegate certificates to VoIP Entity customers of the SP, as described in steps 7) though 9).

1. The SP vets a VoIP Entity customer who wants to obtain delegate certificates. The vetting process includes verifying the legal status of the VoIP Entity, and verifying the VoIP Entity’s authority to use TNs and potentially other rich call data information.
2. The VoIP Entity requests a delegate certificate. The request specifies a TNAuthList that identifies a set of TNs that the VoIP Entity is authorized to use, and possibly a JWTClaimConstraints extension that reflects the set of rich call data that the VoIP Entity is authorized to use (see clause 5.3.2 for details on JWTClaimConstraints).
3. If the VoIP Entity is authorized to use the requested set of TNs and rich call data information, then the SP using the STI-SCA issues a delegate certificate containing a TNAuthList that identifies the set of TNs the VoIP Entity is authorized to use, and (if required) a JWTClaimConstraints extension identifying the set of rich call data items that the VoIP Entity is authorized to use. The delegate certificate is signed with the private key of the STI intermediate certificate obtained from the STI-CA.

Even though the SP and STI-SCA are separate entities, they appear as a single entity to the outside world (i.e., appear as the SP). Exactly how this is accomplished (as represented by interface 10 in the diagram) is not specified. Ultimately, the STI-SCA needs the STI intermediate certificate and its credentials so it can sign delegate end entity certificates issued to the VoIP Entity. One way to do this is to have the SP provide the intermediate certificate and its credentials to the STI-SCA as described in step-6 above. Alternatively, the SP could give the STI-SCA its SPC Token, and let the STI-SCA request the intermediate certificate directly from the STI-CA. Or, the SP could give the STI-SCA its credentials to the STI-PA account, and let the STI-SCA do everything – interwork with the STI-PA to request an SPC Token, and then use that token to obtain an intermediate certificate directly from the STI-CA. Likewise, the specific procedures to convey delegate end entity certificates from the STI-SCA to the VoIP Entity are not specified. The SP could act as a proxy, relaying delegate certificate requests/responses between the VoIP Entity and the STI-SCA (as implied in Figure 5.2). Or , the SP could pass the VoIP Entity’s account credentials and vetted identity information to the STI-SCA, and let the VoIP Entity and STI-SCA interwork directly with each other.

### Adding the V-SCA

The V-SCA provides SCA services to a VoIP Entity when there are multiple levels of delegation (e.g., when the SP assigns a block of TNs to a reseller, and the reseller assigns subsets of that block to TNs to each of its customers). The governance and certificate management procedures associated with a VoIP Entity that utilizes the services of a V-SCA to issue delegate certificates to its customers is similar to the SP/STI-SCA procedures described in clause 5.2.1:

* The VoIP Entity must use the services of a V-SCA that has been approved by the STI-PA (i.e., the V-SCA CPS must comply with STI-GA CP).
* Instead of being vetted by the STI-PA, the VoIP Entity is vetted by its superior SP or VoIP Entity up the delegation chain.
* Instead of obtaining an STI intermediate certificate from the STI-CA, the VoIP Entity obtains a delegate intermediate certificate from its superior SP or VoIP Entity in the delegation chain, and provides that certificate to its V-SCA.

## Policing the Information a non-SHAKEN VoIP Entity can Sign

SHAKEN does not place any constraints on the calling TN or rich call data information that a SHAKEN-approved SP can sign with the credentials of an STI end entity certificate. The assumption is that in the rare case where a SHAKEN-approved SP abuses this trust, it will be identified via traceback activity (the SP is clearly identified in the STI certificate referenced by the PASSporT "x5u" field), which could result in the loss of the SP’s SHAKEN-approval status.

Non-SHAKEN-approved VoIP Entities holding delegate certificates are not granted this level of trust. Instead, the delegate certificate contains information that constrains and limits the information the VoIP Entity can sign. This enables verification services to detect when the VoIP Entity signs a PASSporT containing information it is not authorized to use.

### Encompassing TNs using TNAuthList

When issuing delegate certificates to a VoIP Entity, the SP must ensure that the certificate contains a TNAuthList identifying only the TNs that the VoIP Entity is authorized to use. Essentially, the SP must populate the TNAuthList only with TNs that meet the SHAKEN criteria for attestation level "A". Since the delegate certificate TNAuthList encompasses the "orig" TN of a PASSporT signed with the credentials of the delegate certificate, verifiers can detect cases where a VoIP Entity attempts to use its delegate certificate credentials to sign a calling TN that it is not authorized to use.

### Constraining Rich Call Data using JWTClaimConstraints

RFC 8226 defines the JWTClaimConstraints certificate extension that can be used to constrain the claims and claim values that can be signed by the VoIP Entity with the credentials of the delegate certificate. Therefore, when issuing a delegate certificate to a VoIP Entity that is to be used to sign the rich call data information carried in the "rcd" claim of an "rcd" PASSporT, the SP can include a JWTClaimConstraints extension that constrains or limits the rcd information that can be conveyed in the rcd PASSPorT. As shown in Figure 5.3, the SP does this by including a JWTClaimConstraints object that mandates that the VoIP Entity RCD authentication service must include an "rcdi" claim in the rcd PASSporT with a specific digest value (or values) calculated across the rich call data items carried in the "rcd" claim that the VoIP Entity is authorized to use.



Figure 5.3 – Using JWTClaimConstraints to constrain Rich Call Data

**Procedure:**

1. The Service Provider issues a delegate end entity certificate to the VoIP Entity containing a JWTClaimConstraints object that mandates inclusion of an "rcdi" claim with a specific claim value for all PASSporTs signed by this certificate.
2. The VoIP Entity RCD Authentication Service complies with the constraints by including an "rcdi" claim with the indicated value.
3. The signed rcd PASSPorT is carried in the Identity header field of an INVITE request to the terminating SP, where an RCD Verification Service verifies the following:
   * JWTClaimConstraints have been met (i.e., the "rcdi" claim is present and contains one of the specified permitted values)
   * Calculates a digest across the "rcd" claim value (including "rcd" claim pass-by-reference info) and compares it to the "rcdi" claim value.

A failure of either of these tests results in a verification failure.

# Delegate Certificate Use Cases

## Identifying Delegate Certificate Entities for Traceback

In the example shown in Figure 6.1, SP-1 (who is assigned SPC "1234") contracts with SHAKEN-approved CA-1 to obtain STI-CA services, and contracts with CA-2 to obtain STI-SCA services. (Note that in this example, CA-1 and CA-2 could be the same organization.) CA-2 issues delegate end entity certificates to SP-1 customer Enterprise-1.

To support traceback, the various entities are identified by the certificates in the certification path as follows:

* The Subject field of the STI root and intermediate certificates held by CA-1 identifies CA-1.
* The TNAuthList of the intermediate certificate held by CA-2 identifies SP-1. The Subject field of this intermediate certificate also identifies SP-1.
* The Subject field of the delegate end entity certificate held by Enterprise-1 identifies Enterprise-1.



Figure 6.1 – Delegate Certificate Certification Path Example

1. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < <https://www.atis.org> >. [↑](#footnote-ref-2)
2. This document is available from the National Institute of Standards and Technology (NIST) at: < <https://csrc.nist.gov/> >. [↑](#footnote-ref-3)