**ATIS-0x0000x**

ATIS Standard on

**Signature-Based Handling of Asserted Information Using Tokens (SHAKEN):**

**Proof-of-Possession of Telephone Numbers (TN-PoP)**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This technical report defines mechanisms that enable a Service Provider to delegate STI authentication authority for a subset of its TNs to another entity. This delegation capability is needed to support STI for cases such as multi-homed SIP-PBXs, where the authorized owner of a TN does not provide originating call services for that TN.

**Foreword**

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The [**COMMITTEE NAME**] Committee [**INSERT MISSION**]. [**INSERT SCOPE**].

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 a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, [**COMMITTEE NAME**], 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, [**COMMITTEE NAME**], which was responsible for its development, had the following leadership:

[**LEADERSHIP LIST**]

The **[SUBCOMMITTEE NAME]** Subcommittee was responsible for the development of this document.

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| June 29, 2017 | Initial | Baseline | David Hancock |

**Table of Contents**

1 Scope, Purpose, & Application 1

1.1 Scope 1

1.2 Purpose 1

2 Normative References 2

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2

3.2 Acronyms & Abbreviations 2

4 Overview 3

4.1.1 PoP Certificate 3

4.1.2 PoP PASSporT Token 4

4.1.3 TN PoP Requirements 4

4.1.4 TN PoP Procedures 4

5 TN Proof-of-Possession Solution Description 8

5.1 TN Proof-of-Possession Architecture 8

5.1.1 TN PoP Functional Elements 8

5.1.2 TN PoP Interfaces 9

5.2 TN PoP Certificate Management Procedures 11

5.2.1 External Account Binding 11

5.2.2 Certificate Management Message Flow 12

5.2.3 ACME Certificate Management Procedures 13

5.3 TN PoP Authentication and Verification Procedures 19

A Annex Title 19

**Table of Figures**

Figure 1. Obtaining a PoP Certificate 5

Figure 2. Pre-authorizing ACME Account via External Account Binding 6

Figure 3. PoP Certificate support of STI Authentication & Verification during Call Setup 7

Figure 4. SHAKEN Architecture to support Management of PoP Certificate 8

Figure 5. Pre-authorizing ACME Account using External Account Binding 11

Figure 6. Procedure to obtain PoP certificate 12

**Table of Tables**

Table 1. TN PoP Certificate Management Interfaces 11

# Scope, Purpose, & Application

## Scope

TN Proof-of-Possession (TN PoP) is an extension to the base SHAKEN framework that enables an STI-authorized service provider to delegate authority for a subset of its telephone numbers to another non-STI entity. The non-STI entity can then use this “proof of possession” to provide cryptographic proof to STI verification services that it has authority to attest the calls from the delegated TNs.

This specification addresses all aspects of extending SHAKEN to support TN Proof-of-Possession, including:

* The TN PoP certificate management procedures
* The TN PoP authenticate and verification procedures during SIP call establishment

## Purpose

There are a number of real-world call scenarios where the originating Service Provider does not have authority over the calling TN. Examples scenarios include but not limited to:

* 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 wants to display a toll-free callback number for B2C calls, and the 800-number provider (RespOrg) and the 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 that 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).
* *Wholesaled TNs used by reseller SPs, Cloud Communication Providers, and others when they originate calls*
* *Contact centers serving multiple enterprises from various locations need to originate calls using the TN specified by the enterprise.*

The base SHAKEN framework can provide full attestation for these call scenarios only if the originating SP has a strong trust relationship with the customer. This leaves a gap for the case where the customer wants full attestation, but the SP is not willing or able to establish the necessary trust relationships. TN Proof-of-Possession closes this gap by extending SHAKEN to provide a cryptographically based mechanism to authenticate these call scenarios with full attestation.

# Normative 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.

ATIS-0x0000x, *Technical Report*.

ATIS-0x0000x.201x, *American National Standard*.

# 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

**AAA**: xxxx.

**Bbbb**: xxxx.

## Acronyms & Abbreviations

|  |  |
| --- | --- |
| ATIS | Alliance for Telecommunications Industry Solutions |

# Overview

The base SHAKEN framework defined in [specs ref] enables an originating SP to provide full SHAKEN attestation when it has a verified association with the calling TN. However, there are a number of real-world scenarios where this is not the case; i.e., where an SP provides originating services for a calling TN, and the SP has no knowledge of the legitimacy of the calling TN. These include the following:

* A PBX that is configured with multiple SIP Trunks across multiple Service Providers (e.g., for redundancy or least cost routing) originates a call via one SPs from a calling TN that it obtained from another SP
* An enterprise originates a call via its host SP but wants the caller ID to display a toll-free number that it obtained from a RespOrg
* A legitimate spoofing service displays a user’s work TN for calls originated from the user’s home phone
* An automatic outbound dialing service originates a call via its host SP using a calling TN that is owned by another SP (e.g. a school subscribes to an outbound calling service that announces snow-day closings and displays the school TN)
* *Wholesaled TNs used by reseller SPs, Cloud Communication Providers, and others when they originate calls.*

For these types of call scenarios, the originating SP or Cloud Communication Provider has no verified association with the calling TN, and therefore, it cannot fully attest that the originator can legitimately use that TN. This puts these calling users at a disadvantage, since the value of delivering calls with full SHAKEN attestation won’t be available to them (e.g., the value in achieving higher answer rates for calls that provide a “calling TN verified” display to the called user).

This document describes a mechanism called TN Proof-of-Possession that extends the base Secure Telephone Identity procedures defined by IETF STIR to enable a calling TN to be authenticated with full attestation when TN ownership and originating call processing are split between two different providers.

TN Proof-of-Possession defines two new entities:

1. Telephone Number Provider (TN Provider):
	* 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 TN Provider is an STI Service Provider as defined in the base SHAKEN specification (i.e., a TN Provider is authorized by the STI-PA to obtain end-user certificates from an STI-CA).
	* Ultimately the entities entitled to obtain STI Certificates will be defined by the STI-GA, but the initial definition is “Service Providers with an OCN (Operating Carrier Number) and eligible to directly obtain TNs.
2. Customer Application Function (Customer AF):
	* A non-STI-authorized entity that purchases (or otherwise obtains) delegated telephone numbers from a Telephone Number Provider.
	* Examples include an Enterprise PBX, Contact Center, Cloud Communication Provider, a legitimate spoofing application, or an automated outbound dialing service.

The TN PoP framework provides a way for the Customer AF to obtain a PoP certificate from the TN Provider, that the Customer AF can then use to attest to remote verification services that the calling TNs is being used legitimately.

### PoP Certificate

The base SHAKEN Governance Model and Certificate Management specification [add ref] mandates support for STI certificates that have a scope of authority expressed in terms of the identity of the certificate holder. Specifically, the TN Authorization List of the SHAKEN STI certificate must contain a ServiceProviderCode data item that identifies the SP holding the certificate. The assumption is that a terminating network performing STI verification trusts that an originating SP will sign PASSporT tokens only when it has established a verified association with the TN used for the call. This is a reasonable assumption, given that the STI-VS can verify that the originating SP has been authorized by the STI-PA to perform SHAKEN authentication.

Since a Customer AF is not an STI-authorized entity, it would not be appropriate to have verification services blindly trust that an originating Customer AF holding a valid PoP certificate is authorized to attest to the calling TN. The scope of a PoP certificate must therefore be expressed in more granular terms that explicitly identify the TN or set of TNs that have been delegated by the TN Provider to the Customer AF. In this way, a verifier can check that the calling TN is on the list of TNs identified by the PoP certificate. This more granular scope for TN PoP certificates is achieved using the TelephoneNumber, and TelephoneNumberRange data types of the TN Authorization List.

### PoP PASSporT Token

TN PoP extends the base PASSporT token defined in draft-ietf-stir-passport. This PASSporT extension serves two purposes. First, it enables a specific set of claims to be defined for the PoP PASSporT token. Second, the PoP PASSporT “ppt” extension can serve as a trigger to inform the remote verification service that it must perform additional PoP verification procedures; specifically, the PoP-VS must verify that the calling TN belongs to the set of TNs identified in the TN Authorization List of the PoP certificate.

### TN PoP Requirements

This section describes the overall requirements that apply to the TN PoP solution.

1. When a TN provider delegates a subset of its TNs to a Customer AF, it may optionally provide a PoP certificate for the delegated TNs. A PoP certificate is required any time they want to attest if the Customer AF wants to originate calls from the delegated TNs with full attestation via an originating Service Provider that is different than the delegating TN provider.
2. A TN provider must ensure that the scope of a PoP certificate provided to a Customer AF covers only the TNs that it has delegated to the Customer AF.
3. When renewing a PoP certificate, the TN provider must ensure that the scope of the new PoP certificate identifies the set of TNs currently delegated to the Customer AF.
4. When originating a call from a delegated TN that is in-scope for one of its PoP certificates, the Customer AF must use the PoP certificate to perform PoP authentication service (i.e., build an Identity header containing a PoP PASSporT token that claims the legitimacy of the calling TN and that is signed with the certificate’s private key).
5. An originating SP serving the Customer AF must convey any PoP Identity header received from the Customer AF unchanged toward the terminating network. In other words, TN PoP Identity headers are carried end-to-end from the originating Customer AF to the terminating network.

*Open issue – whether to support PoP end-to-end (as stated here), or to have the originating SP replace the PoP passport with a SHAKEN passport.*

1. A PoP PASSporT token implicitly indicates “full” attestation. Therefore, the PoP PASSporT token does not require an explicit attestation claim.

*Discussion: Who is inserting the origid? the enterprise or the originating SP? Should that be included in flow?*

### TN PoP Procedures

This section describes the information flow associated with the TN PoP procedures for managing PoP certificates, and using PoP certificates to authenticate and verify delegated TNs during call establishment.

#### PoP Certificate Management

Figure 1 shows the high-level overview of the procedure to provide TN Proof-of-Possession to the Customer AF.



Figure 1. Obtaining a PoP Certificate

At 0) in Figure 1, the TN Provider delegates a subset of its TNs to the Customer AF. This is typically done at service turn-up time via a web-portal or API hosted by the TN Provider. Once it knows the set of TNs that it has been allocated, the Customer AF initiates the procedure to obtain a PoP certificate that it can use as proof that it has authority for those TNs:

1. The Customer AF first generates a public/private key pair, and stores the private key in a private key store. The public key will be carried in the PoP certificate. The Customer AF will use the private key later, during origination call processing, to digitally sign calling TNs.

The remaining steps in the procedure are supported by the ACME protocol.

1. The Customer AF asks the TN Provider for a PoP certificate that has a scope of authority covering the delegated TNs, and that contains the public key generated in (1).
2. The TN Provider verifies that the Customer AF is authorized to obtain PoP certificates for the requested scope (see section 4.1.4.2 for details). If the requested scope does not exceed set of TNs delegated to the customer, then the TN Provider requests a PoP certificate from the STI-CA, following the normal procedures defined by SHAKEN Certificate Management.

* 1. The STI-CA verifies the “ownership” of proposed delegated TNs by the TN provider. This verification could occur with either a query to a Provider of NP correction services or the STI-CA maintaining an up-to-date NP file.

NOTE: This function could also be performed by the STI-PA. At this time it is unclear as to scope of STI\_PA but it is recommended that this function be performed by either of these entities.

1. The STI-CA generates a PoP certificate that chains to one of the CA’s root certificates, and returns it to the TN Provider at (4).
2. Discussion: We have not introduced the concept of certificate chains in STIR/SHAKENThe TN Provider stores the PoP certificate in its STI-CR in order to make it available to remote verification services.

Note: Are we saying that all SPs are now going to have an STI-CR? We should not describe a design that operators have STI-CRs. This may reside in STI-PA or STI-CA

1. The TN Provider delivers the PoP certificate to the Customer AF.

#### TN PoP Certificate Authorization

ACME supports a mechanism called External Account Binding that enables the TN Provider to pre-authorize the customer’s ACME account to issue POP certificates with the proper scope. This simplifies the certificate authorization process for the Customer AF, since it eliminates the need to support the ACME identifier authorization procedures each time a certificate is issued.

An overview of the External Account Binding procedure is shown in Figure 2.



Figure 2. Pre-authorizing ACME Account via External Account Binding

External Account Binding enables the TN Provider to bind a newly created ACME Account to customer’s already-established Customer Account, so that it can leverage the TN scope of authority of the Customer Account to pre-authorize the ACME Account.

1. At service activation time, the TN Provider and Customer AF perform some form of mutual authentication. The TN Provider creates a Customer Account, and provides the customer with its configuration data, including account ID and credentials, and the set of TNs delegated to the customer. The TN Provider also configures the Customer AF with the External Account Binding information that uniquely identifies the Customer Account.
2. The Customer AF includes the External Account Binding information in the ACME new-account request.
3. On receiving the request to create a new ACME Account, the TN Provider uses the received External Account Binding information to identify the Customer Account associated with this ACME Account.
4. The TN Provider pre-authorizes the ACME account to issue PoP certificates for the set of TNs that have been delegated to the customer.

#### TN PoP Authentication and Verification

Figure 2 shows the high-level overview of TN PoP authentications and verification procedures used during call establishment.



Figure 3. PoP Certificate support of STI Authentication & Verification during Call Setup

Figure 2 assumes that the Customer AF and TN Provider have already complete the procedure to obtain a PoP certificate described in Figure 1. The call establishment procedure in Figure 2 is kicked off when the Customer AF receives an origination request to called TN-x from one of its delegated TNs (TN-a in this example).

1. The Customer AF Call Control function invokes the PoP-AS to perform authentication services for calling TN-a. The PoP-AS constructs a PoP PASSporT token containing the calling TN-a, and signs it using the private key associated with the PoP certificate. The PoP-AS then includes the PoP PASSporT token and the PoP certificate URL in a new Identity header.
2. The Customer AF Call Control includes the newly created Identity header in the originating INVITE to the originating SP.
3. The originating SP Call Control forwards the INVITE, including the PoP Identity header, to the terminating SP serving TN-x, following normal SIP routing procedures. The originating SP may choose to add a second SHAKEN Identity header (not shown) with “partial” attestation (“partial” because the SP does not own the calling TN). The value of this second Identity header is somewhat limited; basically, it enables the originating SP to record an “origid” claim that identifies the ingress point point used by the originating Customer AF.
4. The terminating SP Call Control invokes the STI-VS to perform verification services for the received INVITE.
5. The STI-VS first fetches the PoP certificate from the TN Provider using the received PoP certificate URL. It then verifies the received Identity header; e.g., checks that the PoP certificate chains to an authorized STI-CA, verifies that the PASSporT signature using the public key of the PoP certificate, and verifies that the calling TN is within the scope of authority of the PoP certificate.
6. The Terminating SP updates the Verstat parameter to indicate that the calling TN has been verified, and sends the INVITE to the called endpoint registered for called TN-x.

An issue that may arise during call set-up is if a TN has been ported from a Service Provider and the PoP certificates has been cached by the terminating SP to reflect the “recipient” SP. This would result in an unverified call. This issue is contingent on the following factors:

* The time to live for PoP certificates, or
* The amount of time the PoP certificates are cached

Consequently, short time to live certificates might minimize this problem, but if longer time to live certificates are used by SPs or the amount of time allowed for caching could result in an indeterminate number of unverified calls.

Discussion: If AF uses the proper new cert and the verifier is cached, perhaps the verifier should check for a recent port change and refresh the cache by exception?

Discussion: Where is the origid inserted in the flow?

# TN Proof-of-Possession Solution Description

This section describes the TN Proof-of-Possession architecture, and the procedures that support PoP certificate management, and PoP authentication and verification services.

## TN Proof-of-Possession Architecture

Figure 3 shows how the SHAKEN certificate management architecture can be extended to support TN Proof-of-Possession certificates. TN PoP reuses many of the same concepts and mechanisms defined by the base SHAKEN architecture. The Customer Application Function (Customer AF) plays a role similar to the Service Provider defined by SHAKEN, using the ACME protocol to obtain certificates from the STI CA. Since the Customer AF is not an STI-authorized entity however, it cannot access the STI-CA directly, but must work through the TN Provider that provided it with its set of TNs. The Telephone Provider therefore acts as a proxy between the Customer AF and the STI-CA to ensure that the scope of the PoP certificates issued to the Customer AF do not exceed the set of TNs delegated to that customer.

 Note: Are we saying that all SPs are now going to have an STI-CR? We should not describe a design that operators have STI-CRs. This may reside in STI-PA or STI-C. Same comment in Figure 6.



Figure 4. SHAKEN Architecture to support Management of PoP Certificate

### TN PoP Functional Elements

As shown in Figure 3, the following functional elements are added to the SHAKEN architecture to support PoP certificates:

Customer Application Functional Entities:

* SKS – a Secure Key Store to store the private keys associated with PoP certificates.
* PoP-AS/VS – the function that authenticates the calling TN using a PoP certificate and its private key
* CAF-KMS – plays a role similar to the SP-KMS

Telephone Number Provider Functional Etities:

* ACME Proxy – acts as an interworking function between the CAF-KMS and the STI-CA. The ACME proxy appears as a Certificate Authority to the CAF-KMS, and as an SP-KMS to the STI-PA and STI-CA. The ACME Proxy acts as the enforcement point to ensure that issued PoP certificates do not exceed the authority of the receiving Customer AF.

### TN PoP Interfaces

The interfaces supporting the management of TN PoP certificates are described in Table-1.

Table 1. TN PoP Certificate Management Interfaces

|  |  |  |
| --- | --- | --- |
| **Interface** | **Definition** | **Description** |
| 1) Private Key | Proprietary – defined by PoP-SKS vendor | The CAF-KMS uses this interface to store the private key of a PoP certificate in the PoP-SKS. |
| 2) ACME (PoP) | ACME profile defined in [shaken] | The CAF-KMS uses this interface to order a new PoP certificate from the ACME Proxy. The ACME Proxy uses this interface to deliver the URL of the STI-CR file containing the newly issued PoP certificate to the CAF-KMS. |
| 3) PoP ACME (SHAKEN) | ACME profile defined in this specification | The ACME Proxy uses this interface to order a new PoP certificate from the STI-CA. |
| 4) PoP certificate | HTTPS POST, Content-Type: application/pem-certificate-chain  | The SP-KMS uses this interface to store a newly issued PoP certificate in the STI-CR. |
| 5) PoP certificate renewal | Proprietary – defined by Customer AF (e.g., HTTPS POST Location header field) | The CAF-KMS uses this interface to deliver the URL of the STI-CR file containing the newly issued PoP certificate to the PoP-AS/VS. |
| 6) Private Key | Proprietary – defined by PoP-SKS vendor | The PoP-AS/VS uses this interface to fetch the private key associated with a newly issued PoP certificate from the PoP-SKS. |

## TN PoP Certificate Management Procedures

This section describes the procedures that are used to issue PoP certificates to the Customer AF.

### External Account Binding

To simplify the PoP certificate authorization process for the Customer AF, the ACME interface between the Customer AF and TN Provider will utilize the External Account Binding mechanism to pre-authorize the ACME Account. A protocol-level description of the External Account Binding procedure is provided in Figure 5.



Figure 5. Pre-authorizing ACME Account using External Account Binding

1. During service activation, the TN Provider configures the Customer AF with external account binding information in the form of two data items; a key-id that identifies the Customer account, and a MAC-key that serves as a shared secret between the TN provider and Customer AF.
2. At ACME account creation time, the Customer AF builds a JWS that contains the key-id and the ACME account public key, and is signed using the MAC-key. This JWS is included in an externalAccountBinding field in the JWS of the new-account request.
3. On receiving the new-account request, the ACME Proxy verifies the externalAccountBinding field as described in [acme draft], and if valid, binds the newly created ACME account to the Customer account identified by the key-id. The ACME Proxy pre-authorizes the ACME account to issue PoP certificates for the set of TNs delegated to the customer.
4. and 5) The Customer AF orders a new PoP certificate via 4). The ACME Proxy provides the interworking functionality between 4) and 5) to fulfill the order. If the set of TNs identified in the order falls within the scope pre-authorized for this ACME account, then the ACME proxy issues the certificate via 4) without challenging the Customer AF to prove it has authority for the set of TNs. The PoP certificate itself is ordered and issued via 5), following the procedures specified in [SHAKEN spec].

### Certificate Management Message Flow



Figure 6. Procedure to obtain PoP certificate

This procedure assumes the following initial conditions have been met:

* The TN Provider has obtained a valid SPC token from the STI-PA, and has created an ACME account with the STI-CA, as defined by the SHAKEN Governance Model and Certificate Management specification [ref].
* The Customer AF has obtained the SPC value and its set of delegated TNs from the TN Provider, plus the information it needs to obtain a PoP certificate covering those TNs, including External Account Binding data, , and the URL of the ACME Proxy’s directory resource.
* The Customer AF has queried the ACME directory resource to obtain the other ACME URLs it will need to obtain a certificate, including the new-account and new-order URLs. (Note that in the case of PoP certificates, both the new-account and new order URLs will resolve to the TN Provider’s ACME Proxy.) Once it has this information, the Customer AF initiates the following procedure to obtain a PoP certificate:
1. The CAF-KMS generates a public/private key pair for the PoP certificate, and stores the private key in the SKS.
2. The CAF-KMS generates a 2nd public/private key pair for the ACME account, and requests creation of a new ACME account using the new-account URL. The new-account request contains the externalAccountBinding information that was provided by the TN Provider. The ACME Proxy creates its local instance of the account, pre-authorizes the account using the received externalAccountBinding information, and returns an ACME “201 Created” response to the CAF-KMS.
3. The CAF-KMS orders a new PoP certificate using the new-order URL identified by the directory resource. The new-order request includes the Identifier of the certificate to be issued in the form of a TNAuthList containing the SPC of the TN Provider, plus the set (or a subset) of TNs that the TN Provider previously delegated to the Customer AF. The ACME Proxy verifies that the ACME Account is pre-authorized to issue certificates for the listed TNs, and returns a "201 Created" response containing the URL to finalize the order.
4. The CAF-KMS assumes that the authorization for this order have been satisfied (i.e., it assumes that the ACME account has been pre-authorized to issue certificates for the requested identifier). Therefore, it constructs a CSR describing the certificate, and posts it to the finalize URL received in step-3. The Identifier field in the CSR is identical to the Identifier field sent with the new-order request in step-3.
5. The ACME Proxy sends a request for a new PoP certificate to the STI-CA. The request includes the identifier contained in the CSR received from the CAF-KMS in step-4.The STI-CA returns an authorization challenge, along with a finalize URL, to the ACME Proxy.
6. The ACME Proxy responds to the challenge received in setp-5 with a valid SPC token.
7. The STI-CA validates the challenge response SPC token with the STI-PA as specified by SHAKEN.
8. The ACME Proxy posts the CSR received from the CAF-KMS in step-4 to the finalize URL received from the STI-CA in step-5.
9. The ACME Proxy starts polling the STI-CA to determine when the PoP certificate has been issued, as specified by SHAKEN. When the PoP certificate is issued by the STI-CA, the ACME Proxy downloads the certificate.
10. The ACME Proxy stores the PoP certificate in the STI-CR.
11. In parallel with step-5, the CAF-KMS starts polling the ACME Proxy to determine when the certificate has been issued.. After the ACME Proxy stores the PoP certificate in the STI-CR in step-10, it responds to the poll with the certificate URL identifying the STI-CR file where it has stored the PoP certificate. This URL will be used by the PoP-AS to populate the certificate reference in the PoP PASSporT Token during PoP authentication.

### ACME Certificate Management Procedures

This section defines the profile of the of the ACME protocol that must be supported by the TN Provider and Customer AF for the management of TN Proof-of-Possession certificates. In this context, the CAF-KMS plays the role of ACME client, while the ACME Proxy plays the role of ACME Server.

*Editor’s note: “Profile” might not be the right word here, but the intended meaning is … this section defines the minimum subset of the ACME protocol that must be supported to issue PoP certificates; i.e., must use external account binding to pre-authorize the ACME account, etc.*

#### Initial Conditions

The TN Provider must configure the Customer AF with the following data items, as a pre-requisite to issuing PoP certificates using the AME protocol:

* The set of telephone numbers that it is delegating to the Customer AF,
* The SPC of the TN Provider,
* The URL of the ACME directory resource,
* A MAC key and key identity to be used to bind the ACME accounts created by his customer to the already-established customer account.

#### Creating the ACME Proxy Account

The CAF-KMS and ACME Proxy shall support the ACME account creation process defined in [draft-ietf-acme-acme]. The ACME Proxy shall set the “externalAccountRequired” subfield of the “meta” field of the directory object to “true”. The CAF-KMS shall generate a public/private key pair using the ES256 algorithm, to serve as credentials for the account. The CAF-KMS shall include an “externalAccountBinding” field in the HTTP POST request that it sends to the “newAccount” resource to create the ACME account, as shown in the following example:

POST /acme/new-account HTTP/1.1

Host: acme-proxy.tn-provider.com

Content-Type: application/jose+json

{

 "protected": base64url({

 "alg": "ES256",

 "jwk": /\* ACME account public key \*/,

 "nonce": "6S8IqOGY7eL2lsGoTZYifg",

 "url": "https:/acme-proxy.tn-provider.com/acme/new-account"

 })

 "payload": base64url({

 "contact": [

 "mailto:cert-admin-caf-kms01@caf.com",

 "tel:+12155551212"

 ]

 "externalAccountBinding": {

 "protected": base64url({

 "alg": "HS256",

 "kid": /\* key-id from TN Provider \*/,

 "url": "https://example.com/acme/new-account"

 }),

 "payload": base64url(/\* same as in "jwk" above \*/),

 "signature": /\* MAC using MAC-key from TN Provider \*/

 }

 }),

 "signature": /\* signed using ACME account private key \*/

}

If the account already exists for the specified account key, then the ACME Proxy shall send a “200 OK” response to the POST request. Otherwise, the ACME Proxy 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://acme-proxy.tn-provider.com/acme/acct/1

Link: <https://acme-proxy.tn-provider.com/acme/some-directory>;rel="index"

{

 "status": "valid",

 "contact": [

 "mailto:cert-admin-caf-kms01@caf.com",

 "tel:+12155551212"

 ]

}

#### Pre-authorizing the ACME Account

In order to pre-authorize the newly created ACME account, the ACME Proxy shall provision an authorization object with a “status” of “valid”, and containing an “identifier” field of type “TNAuthList” with the following values:

* The SPC of the TN Provider,
* The full set of TNs delegated by the TN Provider to the Customer AF.

TN Provider 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": [

 "spc":"1234",

 "tn-range":{"start":"12155551212", "count":"50"}

 ]

 },

 "challenges": []

 }

#### Obtaining a PoP Certificate

The CAF-KMS and ACME Proxy shall support the pre-authorization certificate ordering and issuance process defined in [draft-ietf-acme-acme].

**1) Ordering the Certificate**

As the first step in applying for a new certificate, the CAF-KMS shall provide an “identifiers” field in the new-order POST request of “type” of “TNAuthList. The “value” of the “identifiers” field must identify the Service Provider Code of the TN Provider, and must identify one or more of the TNs that have been delegated by the TN Provider to the Customer AF, as shown in the following example:

POST /acme/new-order HTTP/1.1

 Host: acme-proxy.tn-provider.com

 Content-Type: application/jose+json

 {

 "protected": base64url({

 "alg": "ES256",

 "kid": " https://acme-proxy.tn-provider.com/acme/acct/1",

 "nonce": "5XJ1L3lEkMG7tR6pA00clA",

 "url": " https://acme-proxy.tn-provider.com/acme/new-order"

 })

 "payload": base64url({

 "identifiers": {

 "type":"TNAuthList",

 "value": [

 "spc":"1234",

 "tn-range":{"start":"12155551212", "count":"50"}

 ]

 },

 "notBefore": "2018-01-01T00:00:00Z",

 "notAfter": "2018-01-08T00:00:00Z"

 }),

 "signature": /\* signed using ACME account private key \*/

}

**2) Verifying the order**

The ACME Proxy shall verify that the “Identifiers” field in the new-order request matches the “identifier” field of the pre-provisioned authorization object described in step-2. As an option, and based on local policy, the ACME Proxy may choose to issue certificates when the request “identifiers” field contains a subset of the TNs identified by the “identifier” field in the authorization object.

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

 HTTP/1.1 201 Created

 Replay-Nonce: MYAuvOpaoIiywTezizk5vw

 Location: https://acme-proxy.tn-provider.com/acme/order/asdf

 {

 "status": "pending",

 "expires": "2016-01-01T00:00:00Z",

 "notBefore": "2016-01-01T00:00:00Z",

 "notAfter": "2016-01-08T00:00:00Z",

 "identifiers": {

 "type":"TNAuthList",

 "value": [

 "spc":"1234",

 "tn-range":{"start":"12155551212", "count":"50"}

 ]

 },

 "authorizations": [

 "https://sti-ca.com/acme/authz/1234"

 ],

 "finalize": "https://example.com/acme/order/asdf/finalize"

 }

The “authorizations” field contains the URL to the pre-provisioned authorization object described in section 5.2.3.3. The “finalize” field contains the URL that the CAF-URL will use to finalize the order.

**3) Finalizing the order**

The CAF-KMS assumes that the account is pre-authorized to issue the requested certificate, and therefore shall proceed to finalize the order. (As an option, the CAF-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 CAF-KMS shall create a CSR as specified in [shaken spec], but containing an “identifier” field identical to the “identifiers” field of the new-order request in step-1. The CAF-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: acme-proxy.tn-provider.com

 Content-Type: application/jose+json

 {

 "protected": base64url({

 "alg": "ES256",

 "kid": "https://acme-proxy.tn-provider.com/acme/acct/1",

 "nonce": "MSF2j2nawWHPxxkE3ZJtKQ",

 "url": "https://acme-proxy.tn-provider.com/acme/order/asdf/finalize"

 }),

 "payload": base64url({

 "csr": "5jNudRx6Ye4HzKEqT5...FS6aKdZeGsysoCo4H9P",

 }),

 "signature": /\* signed using ACME account private key \*/

 }

The ACME Proxy 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

 Replay-Nonce: MYAuvOpaoIiywTezizk5vw

 Location: https://acme-proxy.tn-provider.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": [

 "spc":"1234",

 "tn-range":{"start":"12155551212", "count":"50"}

 ]

 },

 "authorizations": [

 "https://acme-proxy.tn-provider.com/acme/authz/1234"

 ],

 "finalize": "https://acme-proxy.tn-provider.com/acme/order/asdf/finalize"

 }

At this point in the process, the ACME Proxy shall apply for a PoP certificate of the requested scope with an STI-CA, as specified in [shaken spec]. While the STI-CA is filling the ACME Proxy’s order, the ACME Proxy shall maintain a value of “processing” for the CAF-KMS order.

**4) Polling for the certificate**

Once it has finalized the certificate order with the STI-CA, the ACME Proxy shall periodically poll the STI-CA order as specified in [draft-ietf-acme-acme]. When the STI-CA indicates that the order has been filled, the ACME Proxy shall download the certificate from the STI-CA and store it in the STI-CR as specified in [shaken spec]

Likewise, once it has finalized the certificate order with the ACME Proxy, the CAF-KMS shall periodically poll the ACME Proxy’s order resource as specified in [draft-ietf-acme-acme]. When the order has been filled and the certificate has been stored in the STI-CR, the ACME proxy shall indicate to the CAF-KMS that the certificate is available by responding to the next poll as shown in the following example:

 GET /acme/order/asdf HTTP/1.1

 Host: acme-proxy.tn-provider.com

 HTTP/1.1 200 OK

 Replay-Nonce: MYAuvOpaoIiywTezizk5vw

 Location: https://acme-proxy.tn-provider.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": [

 "spc":"1234",

 "tn-range":{"start":"12155551212", "count":"50"}

 ]

 },

 "authorizations": [

 "https://acme-proxy.tn-provider.com/acme/authz/1234"

 ],

 "finalize": <https://acme-proxy.tn-provider.com/acme/order/asdf/finalize>

 "certificate": "https://sti-cr.tn-provider.com/cert-1"

 }

Note that the Customer AF does not need to download the actual certificate. It will use the URL identified in the “certificate” field of the response to populate the “x5u” field in the PoP PASSportT token created during PoP authentication.

## TN PoP Authentication and Verification Procedures

…

(normative/informative)

# A Annex Title

Xxx