

Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 22, 2017

M. Barnes
MLB@Realtime Communications
C. Wendt
Comcast
June 20, 2017

ACME Identifiers and Challenges for VoIP Service Providers
draft-ietf-acme-service-provider-00

Abstract

This document specifies identifiers and challenges required to enable the Automated Certificate Management Environment (ACME) to issue certificates for VoIP service providers to support Secure Telephony Identity (STI).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 22, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Overview	2
3.	Identifier for Service Provider Codes	3
4.	Challenges for Service Providers	3
5.	TNAuthList Identifier Code and Challenges Example	4
6.	IANA Considerations	5
6.1.	ACME TNAuthList Identifier	5
6.2.	ACME Service Provider Challenge	6
7.	Security Considerations	6
8.	Informative References	6
	Authors' Addresses	7

[1.](#) Introduction

[I-D.ietf-acme-acme] is a mechanism for automating certificate management on the Internet. It enables administrative entities to prove effective control over resources like domain names, and automates the process of generating and issuing certificates.

The STIR problem statement [[RFC7340](#)] identifies the need for Internet credentials that can attest authority for the originator of VoIP calls in order to detect impersonation, which is currently an enabler for common attacks associated with illegal robocalling, voicemail hacking, and swatting. These credentials are used to sign PASSports [[I-D.ietf-stir-passport](#)], which can be carried in using protocols such as SIP [[I-D.ietf-stir-rfc4474bis](#)]. Currently, the only defined credentials for this purpose are the certificates specified in [[I-D.ietf-stir-certificates](#)].

[I-D.ietf-stir-certificates] describes certificate extensions suitable for associating telephone numbers and service provider codes with certificates. [[I-D.peterson-acme-telephone](#)] specifies the ACME extensions to enable certification authorities to issue certificates based on telephone numbers. This specification defines extensions to ACME to enable certification authorities to issue certificates based on service provider codes.

[2.](#) Overview

The document [[SHAKEN Certificate Mgmt](#)] provides a framework and model for using certificates based on service provider codes. In this

model, each service provider requires only a few certificates, which are used in conjunction with a PASSporT that contains additional information attesting to a service provider's knowledge of the originator of the call. Further details on the PASSporT extensions for this model are provided in the SHAKEN Framework [[ATIS-1000074](#)].

In the SHAKEN Certificate Management framework, there is an administrative entity that is responsible for allocating service provider codes. This is referred to as the STI Policy Administrator (STI-PA). This allows a certification authority to validate that the entity requesting issuance of a certificate is authorized to request certificates on behalf of the entity that has been assigned a specific service provider code. A single VoIP service provider can be allocated multiple service provider codes. A service provider can choose to use the same certificate for multiple service providers as reflected by the structure of the TN Authorization List certificate extension defined in [[I-D.ietf-stir-certificates](#)].

The intent of the challenges in this document is not to establish that an entity is a valid service provider but rather to provide evidence that an established governance entity has authorized the entity to provide VoIP services in the network and thus to request credentials on behalf of the VoIP users in the network.

[3.](#) Identifier for Service Provider Codes

In order to issue certificates for service providers based on service provider code values, a new ACME identifier type is required for use in ACME authorization objects. The baseline ACME specification defines one type of identifier, for a fully-qualified domain name ("dns"). The document [[I-D.peterson-acme-telephone](#)] defines an ACME identifier type for telephone numbers ("tn"). This document defines a new ACME identifier type for service provider codes ("TNAuthList"). The "TNAuthList" identifier is the same type that is specified in the TN Authorization List certificate extension [[I-D.ietf-stir-certificates](#)] for service provider codes. An example is provided in [Section 5](#).

[4.](#) Challenges for Service Providers

The new "TNAuthList" identifier introduces a slightly different authorization process. A mechanism is required to allow the service

provider to prove it has the authority to request certificates on behalf of the entities for whom it is providing VoIP services.

The STI-PA in the SHAKEN Certificate Management framework has a secure exchange with the Service Provider in order to provide a service provider code token that the Service Provider can use for authorization by the CA when requesting a certificate. The service provider code token ("spc-token") is a standard JWT token [RFC7519] using a JWS defined signature string [RFC7515]. Note that further details on the CA interface to the STI-PA for the authorization are provided in [SHAKEN Certificate Mgmt].

This document defines a new ACME challenges type of "spc-token" to support the SHAKEN Certificate Management framework. An example of the use of the "spc-token" for ACME is provided in [Section 5](#).

[5](#). TNAuthList Identifier Code and Challenges Example

The section provides examples of the use of the TNAuthList identifier as a challenge mechanism.

The following is the response that the ACME client receives when it sends a GET for the challenges:

```
HTTP/1.1 200 OK
Content-Type: application/json
Link: <https://example.com/acme/some-directory>;rel="directory"
```

```
{
  "status": "pending",

  "identifier": {
    "type": "TNAuthList",
    "value": ["1234-0111"]
  },

  "challenges": [
    {
      "type": "spc-token",
      "url": "https://sti-ca.com/authz/asdf/0"
      "token": "DGyRejmCefe7v4NfDGDKfA" }
  ]
}
```

```
  ],  
}
```

The following is the response to the challenge sent by the ACME client:

```
POST /acme/authz/asdf/0 HTTP/1.1  
Host: sti-ca.com  
Content-Type: application/jose+json  
  
{  
  "protected": base64url({  
    "alg": "ES256",  
    "kid": "https://sti-ca.com/acme/reg/asdf",  
    "nonce": "Q_s3MwoqT05TrdkM2MTDcw",  
    "url": "https://sti-ca.com/acme/authz/asdf/0"  
  }),  
  "payload": base64url({  
    "type": "spc-token",  
    "keyAuthorization": "I1irfxKKXA...vb29HhjjLPSgwiE"  
  }),  
  "signature": "9cbg5J01Gf5YLjjz...SpkUfcdPai9uVYYQ"  
}
```

6. IANA Considerations

This document defines a new ACME Identifier type and ACME Challenge type to be registered.

[[RFC EDITOR: Please replace XXXX above with the RFC number assigned to this document]]

6.1. ACME TNAuthList Identifier

This document defines the "TNAuthList" ACME Challenge type in the ACME Identifier Type registry as follows:

Identifier Type	Reference
TNAuthList	RFC XXXX

6.2. ACME Service Provider Challenge

This document defines the "spc-token" ACME Challenge type in the ACME Challenge Types registry as follows:

Label	Identifier Type	Reference
spc-token	TNAuthList	RFC XXXX

7. Security Considerations

This document relies on the security considerations established for the ACME protocol per [[I-D.ietf-acme-acme](#)]. The new "TNAuthList" identifier and "spc-token" validation challenges introduce a slightly different authorization process. Although, the challenges still have a binding between the account private key and the validation query made by the server, via the key authorization.

The "spc-token" is initially obtained through a secure exchange between the service provider and the entity in the network that is responsible for determining what entities can operate as VoIP service providers (the STI Policy Administrator). Further details on this are provided in [[SHAKEN Certificate Mgmt](#)].

8. Informative References

[ATIS-1000074]

ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENS (SHAKEN)", January 2017.

[I-D.ietf-acme-acme]

Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", [draft-ietf-acme-acme-06](#) (work in progress), March 2017.

[I-D.ietf-stir-certificates]

Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", [draft-ietf-stir-certificates-14](#) (work in progress), May 2017.

[I-D.ietf-stir-passport]

Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", [draft-ietf-stir-passport-11](#) (work in progress), February 2017.

[I-D.ietf-stir-rfc4474bis]

Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session

Initiation Protocol (SIP)", [draft-ietf-stir-rfc4474bis-16](#) (work in progress), February 2017.

[I-D.peterson-acme-telephone]

Peterson, J. and R. Barnes, "ACME Identifiers and Challenges for Telephone Numbers", [draft-peterson-acme-telephone-00](#) (work in progress), October 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", [RFC 7340](#), DOI 10.17487/RFC7340, September 2014, <<http://www.rfc-editor.org/info/rfc7340>>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", [RFC 7515](#), DOI 10.17487/RFC7515, May 2015, <<http://www.rfc-editor.org/info/rfc7515>>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), DOI 10.17487/RFC7519, May 2015, <<http://www.rfc-editor.org/info/rfc7519>>.

[SHAKEN_Certificate_Mgmt]

ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENS (SHAKEN): Governance Model and Certificate Management", May 2017.

Authors' Addresses

Mary Barnes
MLB@Realtime Communications

Email: mary.ietf.barnes@gmail.com

Comcast
One Comcast Center
Philadelphia, PA 19103
US

Email: chris-ietf@chriswendt.net