Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 19, 2018

M. Barnes
MLB@Realtime Communications
C. Wendt
Comcast

July 18, 2017

ACME Identifiers and Challenges for VoIP Service Providers
draft-ietf-acme-service-provider-01

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 January 19, 2018.

Table of Contents

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.ietf-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 [ATIS-1000080] 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 [ATIS-1000080], 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.ietf-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.

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. This document defines a new ACME challenge type of "spc-token-01" to support the authorization of service provider code tokens.

The following is the response that the ACME client receives when it sends a GET for the challenges in the case of a "TNAuthList" identifer:

```
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-01",
     "url": "https://sti-ca.com/authz/asdf/0"
     "token": "DGyRejmCefe7v4NfDGDKfA" }
   ],
}
```

A client responds to this challenge by providing a service provider code token. In the SHAKEN Certificate Management framework, the Service Provider has a secure exchange with the STI-PA to obtain a service provider code token that can be used for authorization by the CA when requesting a certificate. The service provider code token is a standard JWT token [RFC7519] using a JWS defined signature string [RFC7515].

The service provider code token JWT Protected Header MUST include the following:

alg: Defines the algorithm used in the signature of the token. For Service Provider Code tokens, the algorithm MUST be "ES256".

typ: Set to standard "JWT" value.

x5u: Defines the URL of the certificate of the STI-PA validating the Service Provider Code.

The service provide code token JWT Payload MUST include the following:

sub: Service Provider Code value being validated in the form of a JSON array of ASCII strings.

iat: DateTime value of the time and date the token was issued.

nbf: DateTime value of the starting time and date that the token is valid.

exp: DateTime value of the ending time and date that the token expires.

fingerprint: : Fingerprint of the ACME credentials the Service Provider used to create an account with the CA. The fingerprint is of the form: base64url(JWK_Thumbprint(accountKey)).

The "JWK_Thumbprint" step indicates the computation specified in [RFC7638], using the SHA-256 digest [FIPS180-4]. As noted in JWA [RFC7518] any prepended zero octets in the JWK object MUST be stripped before doing the computation.

To respond to a service provider code token challenge, the ACME client constructs a service provider code authorization ("spc-authz") using the "token" value provided in the challenge and the service provider code token ("spcAuthzToken") that has been previously obtained from the STI-PA. These two values are concatenated and separated by a "." character as follows:

spcAuthorization = token || '.' || spcAuthzToken

The token for a challenge is a string comprised entirely of characters in the URL- safe base64 alphabet. The "||" operator indicates concatenation of strings.

An example of the use of the "spc-token-01" in a challenge response sent by the ACME client is provided below:

```
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({
 "spcAuthorization": "DGyRejmCefe7v4N...vb29HhjjLPSggwiE"
}),
 "signature": "9cbg5JO1Gf5YLjjz...SpkUfcdPai9uVYYQ"
}
```

Upon receiving a response to the challenge, the ACME server determines the validity of the response. The ACME server MUST verify that the "token" in the response matches the "token" in the original challenge. To determine if the "spcAuthzToken" is valid, the server MUST use the URL in the JWT header in the "spcAuthzToken" to obtain the certificate associated with the JWT payload. The server MUST validate the signature and verify the claims. The "sub" field MUST be a value that is included in the values for the "TN-Auth-List" in the original challenge. The server MUST verify that the "fingerprint" field matches the ACME credentials for the ACME client that created the account with the CA. If the validation is successful, the "status" in the challenge object is set to "valid". If any step of the validation process fails, the "status" in the challenge object MUST be set to "invalid". [Editor's Note: Likely we should describe specific error responses for the above.]

5. 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]]

5.1. 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

5.2. ACME Service Provider Challenge

This document defines the "spc-token-01" ACME Challenge type in the ACME Challenge Types registry as follows:

Label	Identifier Type	Reference
spc-token-01	TNAuthList	RFC XXXX

6. 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-01" 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 since the fingerprint of the account key is contained in the service provider code token used for authorization.

The service provider code 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 [ATIS-1000080].

7. Informative References

[ATIS-1000074]
ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENs (SHAKEN)", January 2017.

[ATIS-1000080]
ATIS/SIP Forum NNI Task Group, "Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management", May 2017.

[FIPS180-4]
Department of Commerce, National, "NIST FIPS 180-4, Secure Hash Standard", March 2012.

[I-D.ietf-acme-acme]
Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-07 (work in progress), June 2017.

[I-D.ietf-acme-telephone]
Peterson, J. and R. Barnes, "ACME Identifiers and Challenges for Telephone Numbers", draft-ietf-acme-telephone-00 (work in progress), July 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.

[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>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <http://www.rfc-editor.org/info/rfc7518>.

[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>.

[RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <http://www.rfc-editor.org/info/rfc7638>.

Authors' Addresses

Mary Barnes
MLB@Realtime Communications

Email: mary.ietf.barnes@gmail.com

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
US

Email: chris-ietf@chriswendt.net