Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

M. Barnes
iconectiv

March 5, 2018

ACME Token Identifier and Challenges
draft-barnes-acme-token-challenge-02

Abstract

This document specifies an identifier and challenge type required to enable the Automated Certificate Management Environment (ACME) to issue certificates using a token for the challenge response. This token is issued by a administrative authority with whom the Certification Authority (CA) has a trust relationship. The entity requesting a certificate also has a relationship with the administrative authority, such that the administrative authority assigns a unique code to the entity. This entity code is included as part of the token that the administrative authority issues.

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 https://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 September 6, 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.

This document specifies an identifier and challenge type to enable the Automated Certificate Management Environment (ACME) to issue certificates using a token for the challenge response. This token is issued by a administrative authority with whom the Certification Authority (CA) has a trust relationship. The entity requesting a certificate also has a relationship with the administrative authority, such that the administrative authority assigns a unique code to the entity. This entity code is included as part of the token that the administrative authority issues.

The following diagram summarizes these trust relationships and protocols:

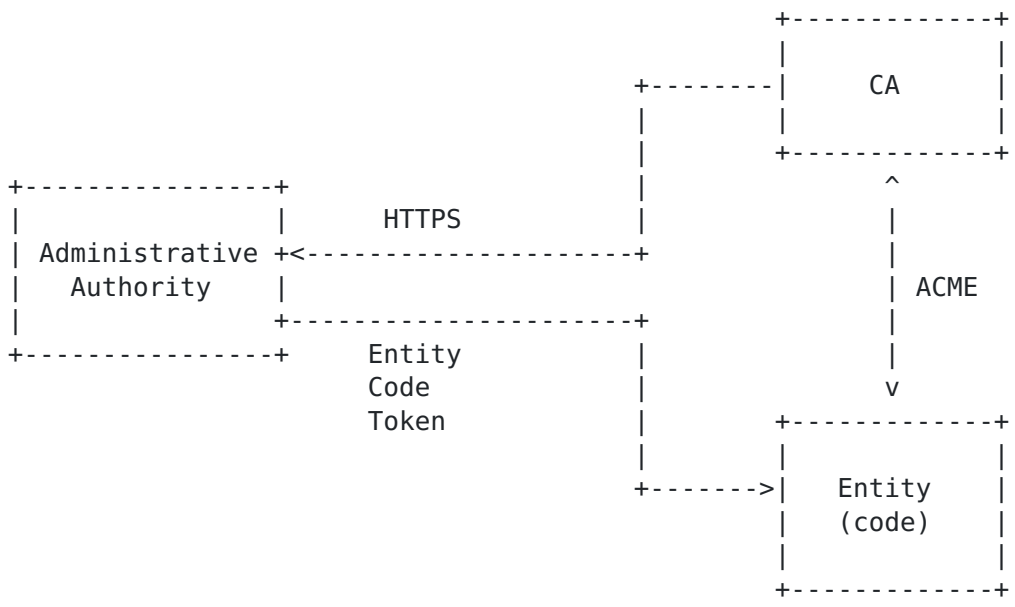

Figure 1: Relationships and Interfaces

There are several use cases that can leverage a mechanism using a generic token for the challenge response, in particular for Secure Telephony Identity Revisited (STIR). 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 use of ACME extensions to enable certification authorities to issue certificates based on telephone numbers. [I-D.ietf-acme-service-provider] specifies the use of ACME extensions to enable certification authorities to issue certificates based on service provider codes.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Overview

The intent of the challenges in this document is to provide evidence that an established administrative authority has authorized the entity requesting the issuance of certificates. The model is based on the entity that is requesting certificates being assigned a unique entity code by the administrative authority. The expectation is that the Entity code would be stable and not change frequently, if at all. The entity also requests the token that is to be used in the challenge response from the administrative authority, prior to requesting issuance of a certificate. Entities that are using this mechanism SHOULD define the lifecycle management for the entity code token - e.g., the frequency at which it should be renewed. This is expected to vary depending upon the use case.

4. Identifier for Entity Codes

In order to issue certificates based on entity 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"). This document defines a new ACME identifier type for entity codes ("EntityCode").

5. Challenges for Entity Codes

The new "EntityCode" identifier introduces a slightly different authorization process. A mechanism is required to allow the entity requesting certificates to prove it has the authority to request certificates. This document defines a new ACME challenge type of "ec-token-01" to support entity 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 "EntityCode" identifer:

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

{
  "status": "pending",

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

   "challenges": [
   {
     "type": "ec-token-01",
     "url": "https://example-ca.com/authz/asdf/0"
     "token": "DGyRejmCefe7v4NfDGDKfA" }
   ],
}
```

A client responds to this challenge by providing an entity code token. The entity code token is a standard JWT token [RFC7519] using a JWS defined signature string [RFC7515].

The entity code token JWT Protected Header MUST include the following:

alg: Defines the algorithm used in the signature of the token.

typ: Set to standard "JWT" value.

x5u: Defines the URL of the certificate of the administrative authority validating the Service Code.

The authorization code token JWT Payload MUST include the following:

sub: Entity Code value being validated in the form of an ASCII string.

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 requestor 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 an entity code token challenge, the ACME client constructs an entity code authorization ("ec-authz") using the "token" value provided in the challenge and the entity code token ("ecAuthzToken") that has been previously obtained from the administrative authority. These two values are concatenated and separated by a "." character as follows:

ecAuthorization = token || '.' || ecAuthzToken

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 "ec-token-01" in a challenge response sent by the ACME client is provided below:

```
POST /acme/authz/asdf/0 HTTP/1.1
Host: example-ca.com
Content-Type: application/jose+json

{
 "protected": base64url({
 "alg": "ES256",
 "kid": "https://example-ca.com/acme/reg/asdf",
 "nonce": "Q_s3MWoqT05TrdkM2MTDcw",
 "url": "https://example-ca.com/acme/authz/asdf/0"
}),
 "payload": base64url({
 "ecAuthorization": "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 "ecAuthzToken" is valid, the server MUST use the URL in the JWT header in the "ecAuthzToken" to obtain the certificate associated with the JWT payload. The server MUST validate the signature and verify the claims. The "sub" field MUST be the value that was included in the "EntityCode" 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.]

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 Entity Code Identifier

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

Identifier Type	Reference
EntityCode	RFC XXXX

6.2. ACME Entity Code Challenge

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

Label	Identifier Type	Reference
ec-token-01	EntityCode	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 "EntityCode" identifier and "ec-token-01" validation challenges introduce a slightly different authorization process. However, 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 code token used for authorization.

The entity code token is initially obtained through a secure exchange between the entity requesting certificates and the administrative authority that is responsible for determining what entities can request certificates.

8. References

8.1. Normative References

[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., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-09 (work in progress), December 2017.

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

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

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7638>.

8.2. Informative References

[I-D.ietf-acme-service-provider]
Barnes, M. and C. Wendt, "ACME Identifiers and Challenges for VoIP Service Providers", draft-ietf-acme-service-provider-02 (work in progress), October 2017.

[I-D.ietf-acme-telephone]
Peterson, J. and R. Barnes, "ACME Identifiers and Challenges for Telephone Numbers", draft-ietf-acme-telephone-01 (work in progress), October 2017.

[I-D.ietf-stir-certificates]
Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-18 (work in progress), December 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.

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

Author's Address

Mary Barnes
iconectiv

Email: mary.ietf.barnes@gmail.com