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

J. Peterson
Neustar
M. Barnes
iconectiv
D. Hancock
C. Wendt
Comcast

March 5, 2018

ACME Challenges Using an Authority Token
draft-peterson-acme-authority-token-01.txt

Abstract

A number of proposed challenges for the Automated Certificate Management Environment (ACME) effectively rely on an external authority issuing a token according to a particular policy. This document specifies a generic Authority Token challenge for ACME which supports subtype claims different identifiers or namespaces that can be defined to represent a specific application of this Authority Token challenge.

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

ACME [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.

In some cases, proving effective control over an identifier requires an attestation from a third party who has authority over the resource, for example, an external policy administrator for a namespace other than the DNS application ACME was originally designed to support. In order to automate the process of issuing certificates for those resources, this specification defines a generic Authority Token challenge that ACME servers can issue in order to acquire such a token. The challenge contains a type indication that tells the client what sort of token it needs to acquire. It is expected that the Authority Token challenge will be usable for a variety of identifier types.

For example, the system of [I-D.ietf-acme-service-provider] provides a mechanism that allows service providers to acquire certificates corresponding to a Service Provider Code (SPC) as defined in [I-D.ietf-stir-certificates] by consulting an external authority responsible for those codes. Furthermore, Communications Service Providers (CSPs) can delegate authority over numbers to their customers, and those CSPs who support ACME can then help customers to acquire certificates for those numbering resources with ACME. This can permit number acquisition flows compatible with those shown in

[I-D.ietf-modern-problem-framework]. Another, similar example would a mechanism that permits CSPs to delegate authority for particular telephone numbers to customers, as described in [I-D.ietf-acme-telephone].

2. Terminology

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

3. Challenges for an Authority Token

Proving that a device on the Internet has effective control over a non-Internet resource is not as straightforward as proving control over an Internet resources like a DNS zone or a web page. There has been considerable interest in using ACME to issue certificates associated with telephone numbers and service provider identifiers used in the telephone network, for example. Provided that the issuer of identifiers in a namespace, or someone acting on the issuer's behalf, can implement a service that grants Authority Tokens to the people to whom it has issued identifiers, a generic token could be used as a response to an ACME challenge. This specification, therefore, defines an Authority Token issued by authority over a namespace to an ACME client for delivery to a CA in response to a challenge. Authority over a hierarchical namespace can also be delegated, so that delegates of a root authority can themselves act as Token Authorities for certain types of names.

This architecture assumes a trust relationship between CAs and Token Authorities: that CAs are willing to accept the attestation of Token Authorities for particular types of identifiers as sufficient proof to issue a credential. It furthermore assumes that ACME clients have a relationship with Token Authorities which permits them to authenticate and authorize the issuance of Authority Tokens to the proper entities. This ACME challenge has no applicability to identifiers or authorities where those pre-associations cannot be assumed.

ACME challenges that support Authority Tokens therefore need to specify the type of tkauth token they require; CAs can even provide a hint in their challenges to ACME clients that tells them how to find a Token Authority who can issue tokens for a given namespace. This challenge type thus requires a new "tkauth-type" element, and may optionally supply a "token-authority" designating a location where tokens can be acquired. The set of "tkauth-type" values and the semantic requirements for those tokens are tracked by an IANA

registry. Here we as an example we use a token type of "ATC", for the Authority Token Challenge, which is further documented below. Taking the identifier example of TNAuthList from [I-D.ietf-acme-service-provider], a challenge might look as follows:

```
    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"]
      },
      "challenges": [
      {
        "type": "tkauth-01",
        "tkauth-type": "ATC",
        "token-authority": "https://authority.example.org/authz",
        "url": "https://boulder.example.com/authz/asdf/0"
        "token": "IlirfxKKXAsHtmzK29Pj8A" }
      ],
    }
```

Entities receiving this challenge know that they can as a proof acquire a ATC token from the designated token authority, and that this authority can provide tokens corresponding the identifier type of "TNAuthList". Once the ATC has been acquired by the ACME Client, it can be posted back to the URL given by the ACME challenge.

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

 {
  "protected": base64url({
  "alg": "ES256",
  "kid": "https://boulder.example.com/acme/reg/asdf",
  "nonce": "Q_s3MWoqT05TrdkM2MTDcw",
  "url": "https://boulder.example.com/acme/authz/asdf/0"
   }),
  "payload": base64url({
  "ATC": "evaGxfADs...62jcerQ"
     }),
  "signature": "5wUrDI3eAaV4wl2Rfj3aC0Pp--XB3t4YYuNgacv_D3U"
 }
```

The "ATC" field in this response contains the Authority Token.

3.1. Token Type Requirements

The IANA will control a registry of token-types under a policy of Specification Required. In order to register a new token-type, specifications must meet the following requirements.

While Authority Token types do not need to be specific to a namespace, every token must carry enough information for a CA to determine the name that it will issue a certificate for. Some types of Authority Tokens might be reusable for a number of different namespaces; other authority tokens might be specific to a particular type of name. Therefore, in defining token-types, future specifications must indicate how a token conveys to the CA the name that the Token Authority is attesting that the ACME client controls.

In most cases, an ACME client will need a protocol to request and retrieve an Authority Token. The Token Authority will require certain information from an ACME client in order to ascertain that it is the right entity to request a certificate for a particular name. The protocols used to request an Authority Token MUST convey to the Token Authority the identifier type and value from the ACME challenge, as well as the nonce, and those MUST be reflected in the Authority Token. Exactly how the Token Authority authenticates and authorizes ACME clients to receive Authority Tokens is out of the scope of this document.

Because the assignment of resources can change over time, demonstrations of authority must be regularly refreshed. Definitions

of a token-type MUST specify how they manage the freshness of authority assignments. Typically, a CA will expect a regular refreshing of the token.

3.2. Authority Token Type for ATC

This specification pre-populates the token-type registry with a token-type for "ATC".

Here the "ATC" token-type signifies a standard JWT token [RFC7519] using a JWS-defined signature string [RFC7515]. This may be used for any number of different identifier types given in ACME challenges.

For this ACME Authority Token usage of JWT, the payload of the JWT OPTIONALLY contain an "iss" indicating the Token Authority that generated the token, if the "x5u" element in the header does not already convey that information; typically, this will be the same location that appeared in the "token-authority" field of the ACME challenge. In order to satisfy the requirement for replay prevention the JWT MUST contain a "jti" element, and an "exp" claim.

The JWT payload must also contain a new JWT claim, "atc", for Authority Token Challenge, which contains three elements in an array: the identifier type, the identifier value, and the nonce. The identifier type and value are those given in the ACME challenge and conveyed to the Token Authority by the ACME client. Again, following the example of [I-D.ietf-acme-service-provider], this could be the TNAuthList, as defined in [RFC8226], that the Token Authority is attesting. Practically speaking, that may contain a list of Service Provider Code elements, telephone number range elements, and/or individual telephone numbers. The nonce is taken from the original Replay-Nonce header field of the ACME challenge.

So for example:

```
{ "typ":"JWT",
 "alg":"ES256",
 "x5u":"https://authority.example.org/cert"}
{
 "iss":"https://authority.example.org/authz",
 "exp":1300819380,
 "jti":"id6098364921",
 "atc":{"TnAuthList","1234","Q_s3MWoqT05TrdkM2MTDcw"} }
```

[More TBD. Need to add how the JWT reflects that the resource is delegatable. Need to show the request to the Token Authority as well.]

4. Acknowledgments

We would like to thank you for your contributions to this problem statement and framework.

5. IANA Considerations

Future versions of this specification will include registrations for the ACME Challenge type registries here. It will also create a registry for "token types" as used in these challenges.

6. Security Considerations

The capture of Authority Tokens by an adversary could enable an attacker to acquire a certificate from a CA. Therefore, all Authority Tokens MUST contain a field that identifies to the CA which ACME client requested the token from the authority. All Authority Tokens must specify an expiry (of the token itself as proof for a CA, as opposed to the expiry of the name), and for some application, it may make sense of that expiry to be quite short. Authority Tokens must also contain a nonce that will enable a CA to detect a replayed Authority Token. Any protocol used to retrieve Authority Tokens from an authority MUST use confidentiality to prevent eavesdroppers from acquiring an Authority Token.

More TBD.

7. Informative References

[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.

[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-star]
Sheffer, Y., Lopez, D., Dios, O., Pastor, A., and T. Fossati, "Support for Short-Term, Automatically-Renewed (STAR) Certificates in Automated Certificate Management Environment (ACME)", draft-ietf-acme-star-03 (work in progress), March 2018.

[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-modern-problem-framework]
Peterson, J. and T. McGarry, "Modern Problem Statement, Use Cases, and Framework", draft-ietf-modern-problem-framework-03 (work in progress), July 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.

[I-D.rescorla-stir-fallback]
Rescorla, E. and J. Peterson, "STIR Out of Band Architecture and Use Cases", draft-rescorla-stir-fallback-02 (work in progress), June 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>.

[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>.

[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>.

[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>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

Authors' Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@team.neustar

Mary Barnes
iconectiv

Email: mary.ietf.barnes@gmail.com

David Hancock
Comcast

Email: davidhancock.ietf@gmail.com

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net