Automated Certificate Management Environment (ACME) Renewal Information (ARI) Extension

Abstract

This document specifies how an ACME server may provide hints to ACME
clients as to when they should attempt to renew their certificates.
This allows servers to mitigate load spikes, and ensures clients do
not make false assumptions about appropriate certificate renewal
periods.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Automated Certificate
Management Environment Working Group mailing list (acme@ietf.org),
which is archived at https://mailarchive.ietf.org/arch/browse/acme/.

Source for this draft and an issue tracker can be found at https://
github.com/aarongable/draft-acme-ari.

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 26 March 2022.

Table of Contents

1. Introduction

Most ACME clients today choose when to attempt to renew a certificate in one of three ways. They may be configured to renew at a specific interval (e.g. via cron); they may parse the issued certificate to determine its expiration date and renew a specific amount of time before then; or they may parse the issued certificate and renew when some percentage of its validity period has passed. The first two techniques create significant barriers against the issuing CA changing certificate lifetimes. All three techniques lead to load clustering for the issuing CA.

Being able to indicate to the client a period in which the issuing CA suggests renewal would allow both dynamic changes to the certificate validity period and proactive smearing of load. This document specifies a mechanism by which ACME servers may provide suggested renewal windows to ACME clients.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Extensions to the ACME Protocol: The "order" Resource

An ACME server which wishes to provide renewal information **MUST** include a new field, "renewalInfo", in finalized Order objects.

renewalInfo (optional, string): A URL for renewal information for the certificate that has been issued in response to this order.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "valid",
  "expires": "2021-01-20T14:09:07.99Z",

  "identifiers": [
    { "type": "dns", "value": "www.example.org" },
    { "type": "dns", "value": "example.org" }
  ],

  "notBefore": "2021-01-01T00:00:00Z",
  "notAfter": "2021-01-08T00:00:00Z",

  "authorizations": [
    "https://example.com/acme/authz/PAniVnsZcis",
    "https://example.com/acme/authz/r4HqLzrSrpI"
  ],

  "finalize": "https://example.com/acme/order/TOlocE8rfgo/finalize",
  "certificate": "https://example.com/acme/cert/mAt3xBGaobw",
  "renewalInfo": "https://example.com/acme/renewal/eXoM9UwLgbL"
}
```

Conforming clients **SHOULD** store the "renewalInfo" URL locally so that they can poll it at any time during the lifetime of the certificate.

4. Extensions to the ACME Protocol: The "renewalInfo" Resource

We define a new resource type, the "renewalInfo" resource, as part of the ACME protocol.

The structure of an ACME renewalInfo resource is as follows:

suggestedWindow (object, required): A JSON object with two keys, "start" and "end", whose values are timestamps, encoded in the format specified in [RFC3339], which bound the window of time in which the CA recommends renewing the certificate.

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "suggestedWindow": {
    "start": "2021-01-03T00:00:00Z",
    "end": "2021-01-07T00:00:00Z"
  }
}
```

Conforming servers **MUST** provide the renewalInfo resource via POST-as-GET; they **SHOULD** provide it via unauthenticated GET as well. Conforming clients **SHOULD** use unauthenticated GET to request renewalInfo resources.

The server **SHOULD** include a Retry-After header indicating the polling interval that the ACME server recommends. Conforming clients **SHOULD** query the "renewalInfo" URL again after the Retry-After period has passed, as the server may provide a different suggestedWindow.

Conforming clients **SHOULD** select a random time within the suggested window to attempt to renew the certificate. If the selected time is in the past, the client **SHOULD** attempt renewal immediately.

5. Security Considerations

The extensions to the ACME protocol described in this document build upon the Security Considerations and threat model defined in Section 10.1 of [RFC8555].

This document specifies that renewalInfo resources should be exposed via unauthenticated GET requests, a departure from RFC8555's requirement that clients must send POST-as-GET requests to fetch resources from the server. This is because the information contained in renewalInfo resources is not considered confidential, and because

allowing renewalInfo to be easily cached is advantageous to shed
load from clients which do not respect the Retry-After header.

6. IANA Considerations

Draft note: The following changes to IANA registries have not yet
been made.

6.1. New Registries

Within the "Automated Certificate Management Environment (ACME)
Protocol" registry, IANA has created the new "ACME Renewal Info
Object Fields" registry (Section 6.4).

6.2. ACME Resource Type

Within the "Automated Certificate Management Environment (ACME)
Protocol" registry, the following entry has been added to the "ACME
Resource Types" registry.

Field Name	Resource Type	Reference
renewalInfo	Renewal Info object	This draft

Table 1

6.3. ACME Order Object Fields

Within the "Automated Certificate Management Environment (ACME)
Protocol" registry, the following entry has been added to the "ACME
Order Object Fields" registry.

Field Name	Field Type	Configurable	Reference
renewalInfo	string	false	This draft

Table 2

6.4. ACME Renewal Info Object Fields

The "ACME Renewal Info Object Fields" registry lists field names
that are defined for use in ACME renewal info objects.

Template:

  *Field name: The string to be used as a field name in the JSON
   object

  *Field type: The type of value to be provided, e.g., string,
   boolean, array of string

  *Reference: Where this field is defined

Initial contents:

Field Name	Field type	Reference
suggestedWindow	object	This draft

Table 3

7. Normative References

[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>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet:
           Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002,
           <https://www.rfc-editor.org/info/rfc3339>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J.
           Kasten, "Automatic Certificate Management Environment
           (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019,
           <https://www.rfc-editor.org/info/rfc8555>.

Acknowledgments

TODO acknowledge.

Author's Address

A. Gable
Internet Security Research Group

Email: aaron@letsencrypt.org