ACME Working Group   H. Landau
Internet-Draft   February 04, 2017
Intended status: Standards Track
Expires: August 8, 2017

             CAA Record Extensions for Account URI and ACME Method Binding
                        draft-ietf-acme-caa-01

Abstract

   The CAA DNS record allows a domain to communicate issuance policy to
   CAs, but only allows a domain to define policy with CA-level
   granularity. However, the CAA specification also provides facilities
   for extension to admit more granular, CA-specific policy. This
   specification defines two such parameters, one allowing specific
   accounts of a CA to be identified by URI and one allowing specific
   methods of domain control validation as defined by the ACME protocol
   to be required.

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 August 8, 2017.

Table of Contents

1. Introduction

This specification defines two parameters for the "issue" and
"issuewild" properties of the Certification Authority Authorization
(CAA) DNS resource record [RFC6844]. The first, "account-uri",
allows authorization conferred by a CAA policy to be restricted to
specific accounts of a CA, which are identified by URIs. The second,
"acme-methods", allows the set of validation methods supported by an
ACME [I-D.ietf-acme-acme] based CA to validate domain control to be
limited to a subset of the full set of methods which it supports.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED",
"SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY",
and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119
[RFC2119] and indicate requirement levels for compliant ACME-CAA
implementations.

3. Extensions to the CAA Record: account-uri Parameter

A CAA parameter "account-uri" is defined for the "issue" and
"issuewild" properties defined by [RFC6844]. The value of this
parameter, if specified, MUST be a URI [RFC3986] identifying a
specific CA account.

"CA account" means an object maintained by a specific CA representing
a specific entity, or group of related entities, which may request
the issuance of certificates.

The presence of this parameter constrains the property to which it is
attached. A CA MUST only consider a property with an "account-uri"
parameter to authorize issuance where the URI specified is an URI
that the CA recognises as identifying the account making a
certificate issuance request.

If a certificate issuance request is made to a CA such that no
account URI is available, because the request is made in the absence
of any account or the account has no URI assigned to it, a CA MUST
NOT consider any property having an "account-uri" parameter as
authorizing issuance.

If a CA finds multiple CAA records pertaining to it (i.e., having
property "issue" or "issuewild" as applicable and a domain that the
CA recognises as its own) with different "account-uri" parameters,
the CA MUST NOT consider the CAA record set to authorize issuance
unless at least one of the specified account URIs identifies the
account of the CA by which issuance is requested. A property without
an "account-uri" parameter matches any account. A property with an
invalid or unrecognised "account-uri" parameter is unsatisfiable. A
property with multiple "account-uri" parameters is unsatisfiable.

The presence of an "account-uri" parameter does not replace or
supercede the need to validate the domain name specified in an
"issue" or "issuewild" record in the manner described in the CAA
specification. CAs MUST still perform such validation. For example,
a CAA property which specifies a domain name belonging to CA A and an
account URI identifying an account at CA B is unsatisfiable.

3.1. Use with ACME

An ACME [I-D.ietf-acme-acme] account object MAY be identified by
setting the "account-uri" parameter to the URI of the ACME account
object.

Implementations of this specification which also implement ACME MUST
recognise such URIs.

3.2. Use without ACME

The "account-uri" specification provides a general mechanism to
identify entities which may request certificate issuance via URIs.
The use of specific kinds of URI may be specified in future RFCs, and
CAs not implementing ACME MAY assign and recognise their own URIs
arbitrarily.

4. Extensions to the CAA Record: acme-methods Parameter

A CAA parameter "acme-methods" is also defined for the "issue" and
"issuewild" properties. The value of this parameter, if specified,
MUST be a comma-separated string of ACME challenge method names. The
use of this parameter is specific to ACME and CAs implementing it.

The presence of this parameter constrains the property to which it is
attached. A CA MUST only consider a property with the "acme-methods"
parameter to authorize issuance where the name of the challenge
method being used is one of the names listed in the comma-separated
list.

The special method value "non-acme" is defined. Where a CA supports
both ACME and the "acme-methods" parameter, but also allows the
issuance of certificates by other means, it MUST ensure that all of
its other issuance channels recognise the "acme-methods" parameter
(see section 5.3). For the purposes of validation, such non-ACME
transactions shall be considered to have a method name of "non-acme".
Thus, domains implementing CAA which wish to nominate a CA which
supports issuance via both ACME and non-ACME means can choose whether
to allow one or both.

5. Security Considerations

This specification describes an extension to the CAA record
specification increasing the granularity at which CAA policy can be
expressed. This allows the set of entities capable of successfully
requesting issuance of certificates for a given domain to be
restricted beyond that which would otherwise be possible, while still
allowing issuance for specific accounts of a CA. This improves the
security of issuance for domains which choose to employ it, when
combined with a CA which implements this specification.

5.1. Limited to CAs Processing CAA Records

All of the security considerations of the CAA specification are
inherited by this document. This specification merely enables a
domain with an existing relationship with a CA to further constrain
that CA in its issuance practices, where that CA implements this

specification. In particular, it provides no additional security
above that provided by use of the unextended CAA specification alone
as concerns matters relating to any other CA. The capacity of any
other CA to issue certificates for the given domain is completely
unchanged.

As such, a domain which via CAA records authorizes only CAs adopting
this specification, and which constrains its policy by means of this
specification, remains vulnerable to unauthorized issuance by CAs
which do not honour CAA records, or which honour them only on an
advisory basis.

5.2. Restrictions Ineffective without CA Recognition

The CAA parameters specified in this specification rely on their
being recognised by the CA named by an "issue" or "issuewild" CAA
property. As such, the parameters are not an effective means of
control over issuance unless a CA's support for the parameters is
established beforehand.

CAs which implement this specification SHOULD make available
documentation indicating as such, including explicit statements as to
which parameters are supported. Domains configuring CAA records for
a CA MUST NOT assume that the restrictions implied by the "account-
uri" and "acme-methods" parameters are effective in the absence of
explicit indication as such from that CA.

CAs SHOULD also document whether they implement DNSSEC validation for
DNS lookups done for validation purposes, as this affects the
security of the "account-uri" and "acme-methods" parameters.

5.3. Mandatory Consistency in CA Recognition

A CA MUST ensure that its support for the "account-uri" and "acme-
methods" parameters is fully consistent for a given domain name which
a CA recognises as identifying itself in a CAA "issue" or "issuewild"
property. If a CA has multiple issuance systems (for example, an
ACME-based issuance system and a non-ACME based issuance system, or
two different issuance systems resulting from a corporate merger), it
MUST ensure that all issuance systems recognise the same parameters.

A CA which is unable to do this MAY still implement the parameters by
splitting the CA into two domain names for the purposes of CAA
processing. For example, a CA "example.com" with an ACME-based
issuance system and a non-ACME-based issuance system could recognise
only "acme.example.com" for the former and "example.com" for the
latter, and then implement support for the "account-uri" and "acme-
methods" parameters for "acme.example.com" only.

A CA which is unable to ensure consistent processing of the "account-
uri" or "acme-methods" parameters for a given CA domain name as
specifiable in CAA "issue" or "issuewild" properties MUST NOT
implement support for these parameters. Failure to do so will result
in an implementation of these parameters which does not provide
effective security.

5.4. URI Ambiguity

Suppose that CA A recognises "a.example.com" as identifying itself,
CA B is a subsidiary of CA A which recognises both "a.example.com"
and "b.example.com" as identifying itself.

Suppose that both CA A and CA B issue account URIs of the form

"account-id:1234"

If the CA domain name in a CAA record is specified as "a.example.com"
then this could be construed as identifying account number 1234 at CA
A or at CA B. These may be different accounts, creating ambiguity.

Thus, CAs MUST ensure that the URIs they recognise as pertaining to a
specific account of that CA are unique within the scope of all domain
names which they recognise as identifying that CA for the purpose of
CAA record validation.

It is RECOMMENDED that CAs satisfy this requirement by using URIs
which include an authority:

"https://a.example.com/account/1234"

5.5. Authorization Freshness

The CAA specification governs the act of issuance by a CA. In some
cases, a CA may establish authorization for an account to request
certificate issuance for a specific domain separately to the act of
issuance itself. Such authorization may occur substantially prior to
a certificate issuance request. The CAA policy expressed by a domain
may have changed in the meantime, creating the risk that a CA will
issue certificates in a manner inconsistent with the presently
published CAA policy.

CAs SHOULD consider adopting practices to reduce the risk of such
circumstances. Possible countermeasures include issuing
authorizations with very limited validity periods, such as an hour,
or revalidating the CAA policy for a domain at certificate issuance
time.

5.6. DNSSEC

   Where a domain chooses to secure its nameservers using DNSSEC, the
   authenticity of its DNS data can be assured, providing that a CA
   makes all DNS resolutions via an appropriate, trusted DNSSEC-
   validating resolver. A domain can use this property to protect
   itself from the threat posed by a global adversary capable of
   performing man-in-the-middle attacks, which is not ordinarily
   mitigated by the "domain validation" model.

   In order to facilitate this, a CA validation process must either rely
   solely on information obtained via DNSSEC, or meaningfully bind the
   other parts of the validation transaction using material obtained via
   DNSSEC.

   The CAA parameters described in this specification can be used to
   ensure that only validation methods meeting these criteria are used.
   In particular, a domain secured via DNSSEC SHOULD either:

   1. Use the "account-uri" parameter to ensure that only accounts
       which it controls are authorized to obtain certificates, or

   2. Exclusively use validation methods which rely solely on
       information obtained via DNSSEC, and use the "acme-methods"
       parameter to ensure that only such methods are used.

5.7. Use without DNSSEC

   Where a domain does not secure its nameservers using DNSSEC, or one
   or more of the CAs it authorizes do not perform CAA validation
   lookups using a trusted DNSSEC-validating resolver, use of the
   "account-uri" or "acme-methods" parameters does not confer additional
   security against an attacker capable of performing a man-in-the-
   middle attack against all validation attempts made by a CA, as such
   an attacker could simply fabricate the responses to DNS lookups for
   CAA records.

   In this case, the "account-uri" and "acme-methods" parameters still
   provide an effective means of administrative control over issuance,
   except where control over DNS is subdelegated (see below).

5.8. Restrictions Supercedable by DNS Delegation

   Because CAA records are located during validation by walking up the
   DNS hierarchy until one or more records are found, the use of the
   "account-uri" and "acme-methods" parameters, or any CAA policy, is
   not an effective way to restrict or control issuance for subdomains
   of a domain, where control over those subdomains is delegated to

another party (such as via DNS delegation or by providing limited
access to manage subdomain DNS records).

6. IANA Considerations

None. As per the CAA specification, the parameter namespace for the
CAA "issue" and "issuewild" properties has CA-defined semantics.
This document merely specifies a RECOMMENDED semantic for parameters
of the names "account-uri" and "acme-methods".

7. Normative References

[I-D.ietf-acme-acme]
          Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic
          Certificate Management Environment (ACME)", draft-ietf-
          acme-acme-05 (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>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform
          Resource Identifier (URI): Generic Syntax", STD 66, RFC
          3986, DOI 10.17487/RFC3986, January 2005,
          <http://www.rfc-editor.org/info/rfc3986>.

[RFC6844] Hallam-Baker, P. and R. Stradling, "DNS Certification
          Authority Authorization (CAA) Resource Record", RFC 6844,
          DOI 10.17487/RFC6844, January 2013,
          <http://www.rfc-editor.org/info/rfc6844>.

Appendix A. Examples

The following shows an example DNS zone file fragment which nominates
two account URIs as authorized to issue certificates for the domain
"example.com". Issuance is restricted to the CA "example.net".

```
example.com. IN CAA 0 issue "example.net; \
  account-uri=https://example.net/account/1234"
example.com. IN CAA 0 issue "example.net; \
  account-uri=https://example.net/account/2345"
```

The following shows a zone file fragment which restricts the ACME
methods which can be used; only ACME methods "dns-01" and "xyz-01"
can be used.

```
example.com. IN CAA 0 issue "example.net; \
  acme-methods=dns-01,xyz-01"
```

The following shows an equivalent way of expressing the same
restriction:

```
example.com. IN CAA 0 issue "example.net; acme-methods=dns-01"
example.com. IN CAA 0 issue "example.net; acme-methods=xyz-01"
```

The following shows a zone file fragment in which one account can be
used to issue with the "dns-01" method and one account can be used to
issue with the "http-01" method.

```
example.com. IN CAA 0 issue "example.net; \
  account-uri=https://example.net/account/1234; \
  acme-methods=dns-01"
example.com. IN CAA 0 issue "example.net; \
  account-uri=https://example.net/account/2345; \
  acme-methods=http-01"
```

The following shows a zone file fragment in which only ACME method
"dns-01" can be used, but non-ACME methods of issuance are also
allowed.

```
example.com. IN CAA 0 issue "example.net; \
  acme-methods=dns-01,non-acme"
```

Author's Address

Hugo Landau

Email: hlandau@devever.net