ACME Working Group
Internet-Draft
Intended status: Informational
Expires: October 23, 2016

H. Landau

April 21, 2016

ACME Account Key Binding via CAA Records
draft-landau-acme-caa-00

Abstract

The ACME protocol provides a means for hosts to automatically request and obtain X.509 certificates from certificate authorities. Certification authorities which implement ACME may also choose to implement the CAA DNS record, which allows a domain to communicate issuance policy to CAs. The CAA specification alone 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 such a parameter.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This specification defines a parameter for the 'issue' and 'issuewild' properties of the Certification Authority Authorization (CAA) DNS resource record [RFC6844], allowing authorization conferred by a CAA policy to be restricted to specific ACME [I-D.ietf-acme-acme] accounts. The accounts are identified by account key thumbprint.

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

3.1. acme-ak Parameter

A CAA parameter "acme-ak" is defined for the 'issue' and 'issuewild' properties defined by [RFC6844]. The value of this parameter, if specified, MUST be the base64url [RFC4648] encoding (without padding) of the JWK thumbprint [RFC7517] of the ACME account key [I-D.ietf-acme-acme].

If an ACME server finds multiple CAA records pertaining to it (i.e., having property 'issue' or 'issuewild' as applicable and a domain

that the ACME server recognises as its own) with different "acme-ak" parameters, the ACME server MUST NOT consider the CAA record set to authorize issuance unless at least one of the specified account key thumbprints matches the requesting ACME account key. A property without an "acme-ak" parameter matches any account key. A property with an invalid "acme-ak" parameter (i.e. not 43 characters long or not a valid base64url string), or multiple "acme-ak" parameters is unsatisfiable.

4. Security Considerations

This specification describes an extension to the CAA record specification increasing the granularity at which CAA policy can be expressed for ACME-based CAs. 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 ACME account keys. This improves the security of issuance for domains which choose to employ it, when combined with a CA which implements this specification.

4.1. DNSSEC

Where a domain chooses to secure its nameservers using DNSSEC, the authenticity of an ACME account key nomination placed in a CAA record can be assured, providing that a CA makes all DNS resolutions via an appropriate, trusted DNSSEC-validating resolver. In this case and so long as control of nominated keys is retained, a domain is protected from the threat posed by a global adversary capable of performing man-in-the-middle attacks, which could otherwise forge DNS responses and successfully obtain ACME authorizations and certificates for the domain.

4.2. Authorization Freshness

The CAA specification governs the act of issuance by a CA. The act of authorization as described by the ACME protocol occurs separately to issuance and may occur substantially prior to an 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 ACME authorizations with very limited validity periods, such as an hour, or revalidating the CAA policy for a domain at certificate issuance time.

5. 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 a parameter of the name "acme-ak" for ACME-based CAs.

6. Normative References

[I-D.ietf-acme-acme]
Barnes, R., Hoffman-Andrews, J., and J. Kasten, "Automatic Certificate Management Environment (ACME)", draft-ietf-acme-acme-02 (work in progress), March 2016.

[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>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <http://www.rfc-editor.org/info/rfc4648>.

[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>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <http://www.rfc-editor.org/info/rfc7517>.

Appendix A. Examples

The following shows an example DNS configuration which nominates two account keys 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; \
  acme-ak=UKNmi2whPhuAhDvAxGa_aOZgPzyJDhhsrt-8Bt2fWh0"
example.com. IN CAA 0 issue "example.net; \
  acme-ak=rlp4OZPOR9MKejkOdZAKQ5Tfwce6llawmrDIh-BtNJ0"
```

Author's Address

Hugo Landau

Email: hlandau@devever.net