Workgroup:
Limited Additional Mechanisms for PKIX and
SMIME
Internet-Draft: draft-chariton-ipcaa-00
Updates: 8659, 6844 (if approved)
Published: 2 December 2022
Intended Status: Standards Track
Expires: 5 June 2023
Authors: A. A. Chariton
Google

DNS CAA Resource Record Property for IP Address Certificates

Abstract

This document specifies a new DNS CAA Resource Record Property that allows an IP Address holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that IP Address.

About This Document

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

The latest revision of this draft can be found at https://daknob.github.io/draft-chariton-ipcaa/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-chariton-ipcaa/.

Discussion of this document takes place on the WG Working Group mailing list (mailto:spasm@ietf.org), which is archived at https://datatracker.ietf.org/wg/lamps/about/. Subscribe at https://www.ietf.org/mailman/listinfo/spasm/.

Source for this draft and an issue tracker can be found at https://github.com/daknob/draft-chariton-ipcaa.

Status of This Memo

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 5 June 2023.

Copyright Notice

Table of Contents

1. Introduction

The CAA Resource Records specified in [RFC8659] allow a domain holder to limit the CAs that are authorized to issue certificates for that domain. However, there is no mechanism to provide the same functionality for IP Addresses that can be included in certificates.

This document specifies a new Property for CAA records that exist in the Reverse DNS Zones that can achieve the same effect.

A new Property is required so as not to interfere with certificate issuance for the subdomains of these two zones, and issue and issuewild continue to be valid.

2. Conventions and Definitions

2.1. Requirements Language

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.

2.2. Defined Terms

This document uses the same defined terms as Section 2.2 of [RFC8659]. The following term is redefined in this document:

Relevant Resource Record Set (Relevant RRset): A set of CAA Resource Records resulting from calculating the IP Address Reverse DNS FQDN for an IP Address.

The following terms are additionally defined:

IP Address: An IPv6 or IPv4 address.

Reverse DNS Zones: The DNS zones ip6.arpa and in-addr.arpa.

IP Address Reverse DNS FQDN: The FQDN that corresponds to an IP Address within the Reverse DNS Zones that can be calculated by using the algorithms described in Section 2.5 of [RFC3596] and Section 3.5 of [RFC1035].

3. Relevant Resource Record Set

In order to determine the Relevant RRset, a compliant CA must calculate the IP Address Reverse DNS FQDN.

Then, it must apply the algorithm specified in Section 3 of [RFC8659] for the calculated FQDN. The search stops at the Reverse DNS Zones, but does not include them.

4. CAA ip Property

If the ip Property Tag is present in the Relevant RRset for an IP Address, it is a request that Issuers:

1. Perform CAA issue restriction processing for the IP Address, and

2. Grant authorization to issue certificates containing that IP Address to the holder of the issuer-domain-name or a party

acting under the explicit authority of the holder of the issuer-domain-name.

The CAA ip Property Value has the following sub-syntax (specified in ABNF as per [RFC5234]):

```
issue-value = *WSP [issuer-domain-name *WSP]
   [";" *WSP [parameters *WSP]]

issuer-domain-name = label *("." label)
label = (ALPHA / DIGIT) *( *("-") (ALPHA / DIGIT))

parameters = (parameter *WSP ";" *WSP parameters) / parameter
parameter = tag *WSP "=" *WSP value
tag = (ALPHA / DIGIT) *( *("-") (ALPHA / DIGIT))
value = *(%x21-3A / %x3C-7E)
```

The following CAA RRset requests that no certificates be issued for the IP Address "2001:db8::1" by any Issuer other than ca1.example.net:

```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
                                                CAA 0 ip "ca1.example.net"
```

The following CAA RRset requests that no certificates be issued for the IP Address "192.0.2.2" by any Issuer other than ca2.example.org:

```
2.2.0.192.in-addr.arpa  CAA 0 ip "ca2.example.org"
```

The following CAA RRset requests that no certificates be issued for the IP Address "192.0.2.1" by any Issuer other than ca1.example.net, and that no certificates be issued for the domain "1.2.0.192.in-addr.arpa" by any Issuer other than ca2.example.org:

```
1.2.0.192.in-addr.arpa  CAA 0 ip    "ca1.example.net"
1.2.0.192.in-addr.arpa  CAA 0 issue "ca2.example.org"
```

An ip Property Tag where the issue-value does not match the ABNF grammar **MUST** be treated the same as one specifying an empty issuer-domain-name. For example, the following malformed CAA RRset forbids issuance:

```
e.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
                                                      CAA 0 ip "%%%%%"
```

The CAA ip Property Tag **MUST** be ignored if the FQDN is not a valid IP Address Reverse DNS FQDN.

An Issuer **MAY** choose to specify parameters that further constrain the issue of certificates by that Issuer -- for example, specifying

that certificates are to be subject to specific validation policies, billed to certain accounts, or issued under specific trust anchors.

For example, if ca1.example.net has requested that its customer that wants a certificate with the IP Address 192.0.2.32 specified their account number "110995" in each of the customer's CAA records using the (CA-defined) "account" parameter, it would look like this:

```
32.2.0.192.in-addr.arpa  CAA 0 issue "ca1.example.net; account=110995"
```

5. Security Considerations

The same Security Considerations described in Section 5 of [RFC8659] apply to this document. On top of these, as the IP Address Reverse DNS FQDN is not checked by CAs that do not comply to this document, the critical flag, described in Section 4.5 of [RFC8659], may have reduced efficacy.

6. Deployment Considerations

The same Deployment Considerations described in Section 6 of [RFC8659] apply to this document. On top of these, deployment of CAA ip Property Tags will increase the amount of DNS queries required when issuing certificates for IPv6 addresses, as it can include up to 32 DNS queries to the ip6.arpa zone if there are no Relevant RRsets.

7. IANA Considerations

The "Certification Authority Restriction Properties" registry needs to be updated to include the following entry:

Tag: ip

Meaning: Authorization Entry by IP Address

Reference: This document

8. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[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>.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003, <https://www.rfc-editor.org/info/rfc3596>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[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>.

[RFC8659] Hallam-Baker, P., Stradling, R., and J. Hoffman-Andrews, "DNS Certification Authority Authorization (CAA) Resource Record", RFC 8659, DOI 10.17487/RFC8659, November 2019, <https://www.rfc-editor.org/info/rfc8659>.

Acknowledgments

Author's Address

Antonios A. Chariton
Google

Email: aac@google.com