

LAMPS Working Group
Internet-Draft
Updates: [6844](#) (if approved)
Intended status: Standards Track
Expires: September 25, 2019

T. Wicinski
Salesforce
March 24, 2019

Alternative DNS Certification Authority Authorization (CAA) Resource
Record
draft-wicinski-lamps-caa-00

Abstract

[RFC6844] defines the Certification Authority Authorization (CAA) DNS Resource Record type to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. With large domains covering multiple web properties, defining all possible certificate authorities for the domain has security implications. It would be beneficial to define a CAA for individual host names. This will allow CAA records that can be managed with fine grain control.

This document provides an alternative CAA record using a _caa prefix label that will take precedent on a per Fully Qualified Domain Name (FQDN), if it exists. It will override any CAA record at the zone apex. This will not change current CAA record behavior, but will be an additional option.

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 25, 2019.

Internet-Draft

wicinski-lamps-caa

March 2019

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Definitions	2
2.	The _caa prefix label	2
3.	IANA Considerations	3
4.	Normative References	3
	Author's Address	3

[1.](#) Introduction

In [[RFC6844](#)] the Certification Authority Authorization (CAA) DNS Resource Record is defined to allow a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain name.

[1.1.](#) 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.

[2.](#) The _caa prefix label

[_caa.www.example.com CAA 0 issue "ca.example.net"]

_caa.www.example.com CNAME _caa.cdn.example.net

_]

Wicinski

Expires September 25, 2019

[Page 2]

Internet-Draft

wicinski-lamps-caa

March 2019

[3.](#) IANA Considerations

IANA is requested to add an entry in the "Underscored and Globally Scoped DNS Node Names" Registry with the fields "RR Type" = "CAA" and "Node Name" = "_caa",

[4.](#) 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>>.
- [RFC6844] Hallam-Baker, P. and R. Stradling, "DNS Certification Authority Authorization (CAA) Resource Record", [RFC 6844](#), DOI 10.17487/RFC6844, January 2013, <<https://www.rfc-editor.org/info/rfc6844>>.
- [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>>.

Author's Address

Tim Wicinski
Salesforce
US

Email: tjw.ietf@gmail.com

Wicinski

Expires September 25, 2019

[Page 3]