

---

Stream: Internet Engineering Task Force (IETF)  
RFC: [8659](#)  
Obsoletes: [6844](#)  
Category: Standards Track  
Published: November 2019  
ISSN: 2070-1721  
Authors: P. Hallam-Baker R. Stradling J. Hoffman-Andrews  
*Venture Cryptography Sectigo Let's Encrypt*

# RFC 8659

## DNS Certification Authority Authorization (CAA) Resource Record

---

### Abstract

The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue. This document defines the syntax of the CAA record and rules for processing CAA records by CAs.

This document obsoletes RFC 6844.

### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc8659>.

### 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. Definitions
  - 2.1. Requirements Language
  - 2.2. Defined Terms
3. Relevant Resource Record Set
4. Mechanism
  - 4.1. Syntax
    - 4.1.1. Canonical Presentation Format
  - 4.2. CAA issue Property
  - 4.3. CAA issuewild Property
  - 4.4. CAA iodef Property
  - 4.5. Critical Flag
5. Security Considerations
  - 5.1. Use of DNS Security
  - 5.2. Non-compliance by Certification Authority
  - 5.3. Mis-Issue by Authorized Certification Authority
  - 5.4. Suppression or Spoofing of CAA Records
  - 5.5. Denial of Service
  - 5.6. Abuse of the Critical Flag
6. Deployment Considerations
  - 6.1. Blocked Queries or Responses
  - 6.2. Rejected Queries and Malformed Responses
  - 6.3. Delegation to Private Nameservers
  - 6.4. Bogus DNSSEC Responses
7. Differences from RFC 6844
8. IANA Considerations

## 9. References

### 9.1. Normative References

### 9.2. Informative References

## Acknowledgements

## Authors' Addresses

# 1. Introduction

The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain name. Publication of CAA Resource Records allows a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue.

Like the TLSA record defined in DNS-Based Authentication of Named Entities (DANE) [RFC6698], CAA records are used as a part of a mechanism for checking PKIX [RFC6698] certificate data. The distinction between CAA and TLSA is that CAA records specify an authorization control to be performed by a CA before issuing a certificate and TLSA records specify a verification control to be performed by a Relying Party after the certificate is issued.

Conformance with a published CAA record is a necessary, but not sufficient, condition for the issuance of a certificate.

Criteria for the inclusion of embedded trust anchor certificates in applications are outside the scope of this document. Typically, such criteria require the CA to publish a Certification Practices Statement (CPS) that specifies how the requirements of the Certificate Policy (CP) are achieved. It is also common for a CA to engage an independent third-party auditor to prepare an annual audit statement of its performance against its CPS.

A set of CAA records describes only current grants of authority to issue certificates for the corresponding DNS domain name. Since certificates are valid for a period of time, it is possible that a certificate that is not conformant with the CAA records currently published was conformant with the CAA records published at the time that the certificate was issued. Relying Parties **MUST NOT** use CAA records as part of certificate validation.

CAA records **MAY** be used by Certificate Evaluators as a possible indicator of a security policy violation. Such use **SHOULD** take into account the possibility that published CAA records changed between the time a certificate was issued and the time at which the certificate was observed by the Certificate Evaluator.

## 2. 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

The following terms are used in this document:

**Certificate:** An X.509 Certificate, as specified in [RFC5280].

**Certificate Evaluator:** A party other than a Relying Party that evaluates the trustworthiness of certificates issued by Certification Authorities.

**Certification Authority (CA):** An Issuer that issues certificates in accordance with a specified Certificate Policy.

**Certificate Policy (CP):** Specifies the criteria that a CA undertakes to meet in its issue of certificates. See [RFC3647].

**Certification Practices Statement (CPS):** Specifies the means by which the criteria of the CP are met. In most cases, this will be the document against which the operations of the CA are audited. See [RFC3647].

**Domain Name:** The label assigned to a node in the Domain Name System.

**Domain Name System (DNS):** The Internet naming system specified in [RFC1034] and [RFC1035].

**DNS Security (DNSSEC):** Extensions to the DNS that provide authentication services as specified in [RFC4033], [RFC4034], [RFC4035], [RFC5155], and any revisions to these specifications.

**Fully Qualified Domain Name (FQDN):** A domain name that includes the labels of all superior nodes in the DNS.

**Issuer:** An entity that issues certificates. See [RFC5280].

**Property:** The tag-value portion of a CAA Resource Record.

**Property Tag:** The tag portion of a CAA Resource Record.

**Property Value:** The value portion of a CAA Resource Record.

**Relevant Resource Record Set (Relevant RRset):** A set of CAA Resource Records resulting from applying the algorithm in Section 3 to a specific FQDN or Wildcard Domain Name.

**Relying Party:** A party that makes use of an application whose operation depends on the use of a certificate for making a security decision. See [RFC5280].

Resource Record (RR): A particular entry in the DNS, including the owner name, class, type, time to live, and data, as defined in [RFC1034] and [RFC2181].

Resource Record Set (RRset): A set of RRs of a particular owner name, class, and type. The time to live on all RRs within an RRset is always the same, but the data may be different among RRs in the RRset.

Wildcard Domain Name: A domain name consisting of a single asterisk character followed by a single "full stop" character ("\*.") followed by an FQDN.

### 3. Relevant Resource Record Set

Before issuing a certificate, a compliant CA **MUST** check for publication of a Relevant RRset. If such an RRset exists, a CA **MUST NOT** issue a certificate unless the CA determines that either (1) the certificate request is consistent with the applicable CAA RRset or (2) an exception specified in the relevant CP or CPS applies. If the Relevant RRset for an FQDN or Wildcard Domain Name contains no Property Tags that restrict issuance (for instance, if it contains only `iodef` Property Tags or only Property Tags unrecognized by the CA), CAA does not restrict issuance.

A certificate request **MAY** specify more than one FQDN and **MAY** specify Wildcard Domain Names. Issuers **MUST** verify authorization for all the FQDNs and Wildcard Domain Names specified in the request.

The search for a CAA RRset climbs the DNS name tree from the specified label up to, but not including, the DNS root "." until a CAA RRset is found.

Given a request for a specific FQDN X or a request for a Wildcard Domain Name \*.X, the Relevant RRset RelevantCAASet(X) is determined as follows (in pseudocode):

Let CAA(X) be the RRset returned by performing a CAA record query for the FQDN X, according to the lookup algorithm specified in Section 4.3.2 of [RFC1034] (in particular, chasing aliases). Let Parent(X) be the FQDN produced by removing the leftmost label of X.

```
RelevantCAASet(domain):
  while domain is not ".":
    if CAA(domain) is not Empty:
      return CAA(domain)
    domain = Parent(domain)
  return Empty
```

For example, processing CAA for the FQDN "X.Y.Z" where there are no CAA records at any level in the tree RelevantCAASet would have the following steps:

```
CAA("X.Y.Z.") = Empty; domain = Parent("X.Y.Z.") = "Y.Z."
CAA("Y.Z.")   = Empty; domain = Parent("Y.Z.")   = "Z."
CAA("Z.")     = Empty; domain = Parent("Z.")     = "."
return Empty
```

Processing CAA for the FQDN "A.B.C" where there is a CAA record "issue example.com" at "B.C" would terminate early upon finding the CAA record:

```
CAA("A.B.C.") = Empty; domain = Parent("A.B.C.") = "B.C."
CAA("B.C.")   = "issue example.com"
return "issue example.com"
```

## 4. Mechanism

### 4.1. Syntax

A CAA RR contains a single Property consisting of a tag-value pair. An FQDN **MAY** have multiple CAA RRs associated with it, and a given Property Tag **MAY** be specified more than once across those RRs.

The RDATA section for a CAA RR contains one Property. A Property consists of the following:

+0-1-2-3-4-5-6-7-	0-1-2-3-4-5-6-7-	
Flags	Tag Length = n	
+-----+-----+-----+-----+-----+-----+-----+-----+		...+-----+
Tag char 0	Tag char 1	...   Tag char n-1
+-----+-----+-----+-----+-----+-----+-----+-----+		...+-----+
Value byte 0	Value byte 1	.....   Value byte m-1
+-----+-----+-----+-----+-----+-----+-----+-----+		.....+-----+

Where  $n$  is the length specified in the Tag Length field and  $m$  is the number of remaining octets in the Value field. They are related by  $(m = d - n - 2)$  where  $d$  is the length of the RDATA section.

The fields are defined as follows:

Flags: One octet containing the following field:

Bit 0, Issuer Critical Flag: If the value is set to "1", the Property is critical. A CA **MUST NOT** issue certificates for any FQDN if the Relevant RRset for that FQDN contains a CAA critical Property for an unknown or unsupported Property Tag.

Note that according to the conventions set out in [RFC1035], bit 0 is the Most Significant Bit and bit 7 is the Least Significant Bit. Thus, according to those conventions, the Flags value 1 means that bit 7 is set, while a value of 128 means that bit 0 is set.

All other bit positions are reserved for future use.

To ensure compatibility with future extensions to CAA, DNS records compliant with this version of the CAA specification **MUST** clear (set to "0") all reserved flag bits. Applications that interpret CAA records **MUST** ignore the value of all reserved flag bits.

**Tag Length:** A single octet containing an unsigned integer specifying the tag length in octets. The tag length **MUST** be at least 1.

**Tag:** The Property identifier -- a sequence of ASCII characters.

Tags **MAY** contain ASCII characters "a" through "z", "A" through "Z", and the numbers 0 through 9. Tags **MUST NOT** contain any other characters. Matching of tags is case insensitive.

Tags submitted for registration by IANA **MUST NOT** contain any characters other than the (lowercase) ASCII characters "a" through "z" and the numbers 0 through 9.

**Value:** A sequence of octets representing the Property Value. Property Values are encoded as binary values and **MAY** employ sub-formats.

The length of the Value field is specified implicitly as the remaining length of the enclosing RDATA section.

#### 4.1.1. Canonical Presentation Format

The canonical presentation format of the CAA record is:

```
CAA <flags> <tag> <value>
```

Where:

**Flags:** An unsigned integer between 0 and 255.

**Tag:** A non-zero-length sequence of ASCII letters and numbers in lowercase.

**Value:** The Value field, expressed as either (1) a contiguous set of characters without interior spaces or (2) a quoted string. See the <character-string> format specified in [\[RFC1035\]](#), [Section 5.1](#), but note that the Value field contains no length byte and is not limited to 255 characters.

## 4.2. CAA issue Property

If the issue Property Tag is present in the Relevant RRset for an FQDN, it is a request that Issuers:

1. Perform CAA issue restriction processing for the FQDN, and
2. Grant authorization to issue certificates containing that FQDN 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 issue 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)

```

For consistency with other aspects of DNS administration, FQDN values are specified in letter-digit-hyphen Label (LDH-Label) form.

The following CAA RRset requests that no certificates be issued for the FQDN "certs.example.com" by any Issuer other than ca1.example.net or ca2.example.org.

```

certs.example.com      CAA 0 issue "ca1.example.net"
certs.example.com      CAA 0 issue "ca2.example.org"

```

Because the presence of an issue Property Tag in the Relevant RRset for an FQDN restricts issuance, FQDN owners can use an issue Property Tag with no issuer-domain-name to request no issuance.

For example, the following RRset requests that no certificates be issued for the FQDN "nocerts.example.com" by any Issuer.

```

nocerts.example.com    CAA 0 issue ";"

```

An issue 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:

```

malformed.example.com  CAA 0 issue "%%%"

```

CAA authorizations are additive; thus, the result of specifying both an empty issuer-domain-name and a non-empty issuer-domain-name is the same as specifying just the non-empty issuer-domain-name.

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 account.example.com specify their account number "230123" in each of the customer's CAA records using the (CA-defined) "account" parameter, it would look like this:

```
account.example.com    CAA 0 issue "ca1.example.net; account=230123"
```

The semantics of parameters to the issue Property Tag are determined by the Issuer alone.

### 4.3. CAA issuewild Property

The issuewild Property Tag has the same syntax and semantics as the issue Property Tag except that it only grants authorization to issue certificates that specify a Wildcard Domain Name and each issuewild Property takes precedence over each issue Property when specified. Specifically:

Each issuewild Property **MUST** be ignored when processing a request for an FQDN that is not a Wildcard Domain Name.

If at least one issuewild Property is specified in the Relevant RRset for a Wildcard Domain Name, each issue Property **MUST** be ignored when processing a request for that Wildcard Domain Name.

For example, the following RRset requests that *only* ca1.example.net issue certificates for "wild.example.com" or "sub.wild.example.com", and that *only* ca2.example.org issue certificates for "\*.wild.example.com" or "\*.sub.wild.example.com". Note that this presumes that there are no CAA RRs for sub.wild.example.com.

```
wild.example.com      CAA 0 issue "ca1.example.net"
wild.example.com      CAA 0 issuewild "ca2.example.org"
```

The following RRset requests that *only* ca1.example.net issue certificates for "wild2.example.com", "\*.wild2.example.com", or "\*.sub.wild2.example.com".

```
wild2.example.com     CAA 0 issue "ca1.example.net"
```

The following RRset requests that *only* ca2.example.org issue certificates for "\*.wild3.example.com" or "\*.sub.wild3.example.com". It does not permit any Issuer to issue for "wild3.example.com" or "sub.wild3.example.com".

```
wild3.example.com     CAA 0 issuewild "ca2.example.org"
wild3.example.com     CAA 0 issue ";"
```

The following RRset requests that *only* ca2.example.org issue certificates for "\*.wild3.example.com" or "\*.sub.wild3.example.com". It permits any Issuer to issue for "wild3.example.com" or "sub.wild3.example.com".

```
wild3.example.com     CAA 0 issuewild "ca2.example.org"
```

#### 4.4. CAA iodef Property

The iodef Property specifies a means of reporting certificate issue requests or cases of certificate issue for domains for which the Property appears in the Relevant RRset, when those requests or issuances violate the security policy of the Issuer or the FQDN holder.

The Incident Object Description Exchange Format (IODEF) [RFC7970] is used to present the incident report in machine-readable form.

The iodef Property Tag takes a URL as its Property Value. The URL scheme type determines the method used for reporting:

**mailto:** The IODEF report is reported as a MIME email attachment to an SMTP email that is submitted to the mail address specified. The mail message sent **SHOULD** contain a brief text message to alert the recipient to the nature of the attachment.

**http or https:** The IODEF report is submitted as a web service request to the HTTP address specified using the protocol specified in [RFC6546].

These are the only supported URL schemes.

The following RRset specifies that reports may be made by means of email with the IODEF data as an attachment, a web service [RFC6546], or both:

```
report.example.com      CAA 0 issue "ca1.example.net"
report.example.com      CAA 0 iodef "mailto:security@example.com"
report.example.com      CAA 0 iodef "https://iodef.example.com/"
```

#### 4.5. Critical Flag

The critical flag is intended to permit future versions of CAA to introduce new semantics that **MUST** be understood for correct processing of the record, preventing conforming CAs that do not recognize the new semantics from issuing certificates for the indicated FQDNs.

In the following example, the Property with a Property Tag of "tbs" is flagged as critical. Neither the ca1.example.net CA nor any other Issuer is authorized to issue for "new.example.com" (or any other domains for which this is the Relevant RRset) unless the Issuer has implemented the processing rules for the "tbs" Property Tag.

```
new.example.com        CAA 0 issue "ca1.example.net"
new.example.com        CAA 128 tbs "Unknown"
```

### 5. Security Considerations

CAA records assert a security policy that the holder of an FQDN wishes to be observed by Issuers. The effectiveness of CAA records as an access control mechanism is thus dependent on observance of CAA constraints by Issuers.

The objective of the CAA record properties described in this document is to reduce the risk of certificate mis-issue rather than avoid reliance on a certificate that has been mis-issued. DANE [RFC6698] describes a mechanism for avoiding reliance on mis-issued certificates.

### 5.1. Use of DNS Security

The use of DNSSEC to authenticate CAA RRs is strongly **RECOMMENDED** but not required. An Issuer **MUST NOT** issue certificates if doing so would conflict with the Relevant RRset, irrespective of whether the corresponding DNS records are signed.

DNSSEC provides a proof of non-existence for both DNS FQDNs and RRsets within FQDNs. DNSSEC verification thus enables an Issuer to determine whether the answer to a CAA record query (1) is empty because the RRset is empty or (2) is non-empty but the response has been suppressed.

The use of DNSSEC allows an Issuer to acquire and archive a proof that they were authorized to issue certificates for the FQDN. Verification of such archives may be an audit requirement to verify CAA record-processing compliance. Publication of such archives may be a transparency requirement to verify CAA record-processing compliance.

### 5.2. Non-compliance by Certification Authority

CAA records offer CAs a cost-effective means of mitigating the risk of certificate mis-issue: the cost of implementing CAA checks is very small, and the potential costs of a mis-issue event include the removal of an embedded trust anchor.

### 5.3. Mis-Issue by Authorized Certification Authority

The use of CAA records does not prevent mis-issue by an authorized CA, i.e., a CA that is authorized to issue certificates for the FQDN in question by CAA records.

FQDN holders **SHOULD** verify that the CAs they authorize to issue certificates for their FQDNs employ appropriate controls to ensure that certificates are issued only to authorized parties within their organization.

Such controls are most appropriately determined by the FQDN holder and the authorized CA(s) directly and are thus outside the scope of this document.

### 5.4. Suppression or Spoofing of CAA Records

Suppression of a CAA record or insertion of a bogus CAA record could enable an attacker to obtain a certificate from an Issuer that was not authorized to issue for an affected FQDN.

Where possible, Issuers **SHOULD** perform DNSSEC validation to detect missing or modified CAA RRsets.

In cases where DNSSEC is not deployed for a corresponding FQDN, an Issuer **SHOULD** attempt to mitigate this risk by employing appropriate DNS security controls. For example, all portions of the DNS lookup process **SHOULD** be performed against the authoritative nameserver. Data cached by third parties **MUST NOT** be relied on as the sole source of DNS CAA information but **MAY** be used to support additional anti-spoofing or anti-suppression controls.

## 5.5. Denial of Service

Introduction of a malformed or malicious CAA RR could, in theory, enable a Denial-of-Service (DoS) attack. This could happen by modification of authoritative DNS records or by spoofing inflight DNS responses.

This specific threat is not considered to add significantly to the risk of running an insecure DNS service.

An attacker could, in principle, perform a DoS attack against an Issuer by requesting a certificate with a maliciously long DNS name. In practice, the DNS protocol imposes a maximum name length, and CAA processing does not exacerbate the existing need to mitigate DoS attacks to any meaningful degree.

## 5.6. Abuse of the Critical Flag

A CA could make use of the critical flag to trick customers into publishing records that prevent competing CAs from issuing certificates even though the customer intends to authorize multiple providers. This could happen if the customers were setting CAA records based on data provided by the CA rather than generating those records themselves.

In practice, such an attack would be of minimal effect, since any competent competitor that found itself unable to issue certificates due to lack of support for a Property marked critical should investigate the cause and report the reason to the customer. The customer will thus discover that they had been deceived.

# 6. Deployment Considerations

A CA implementing CAA may find that they receive errors looking up CAA records. The following are some common causes of such errors, so that CAs may provide guidance to their subscribers on fixing the underlying problems.

## 6.1. Blocked Queries or Responses

Some middleboxes -- in particular, anti-DDoS appliances -- may be configured to drop DNS packets of unknown types, or they may start dropping such packets when they consider themselves under attack. This generally manifests as a timed-out DNS query or as a SERVFAIL at a local recursive resolver.

## 6.2. Rejected Queries and Malformed Responses

Some authoritative nameservers respond with REJECTED or NOTIMP when queried for an RR type they do not recognize. At least one authoritative resolver produces a malformed response (with the QR (Query/Response) bit set to "0") when queried for unknown RR types. Per [RFC1034], the correct response RCODE for unknown RR types is 0 ("No error condition").

## 6.3. Delegation to Private Nameservers

Some FQDN administrators make the contents of a subdomain unresolvable on the public Internet by delegating that subdomain to a nameserver whose IP address is private. A CA processing CAA records for such subdomains will receive SERVFAIL from its recursive resolver. The CA **MAY** interpret that as preventing issuance. FQDN administrators wishing to issue certificates for private FQDNs **SHOULD** use split-horizon DNS with a publicly available nameserver, so that CAs can receive a valid, empty CAA response for those FQDNs.

## 6.4. Bogus DNSSEC Responses

Queries for CAA RRs are different from most DNS RR types, because a signed, empty response to a query for CAA RRs is meaningfully different from a bogus response. A signed, empty response indicates that there is definitely no CAA policy set at a given label. A bogus response may mean either a misconfigured zone or an attacker tampering with records. DNSSEC implementations may have bugs with signatures on empty responses that go unnoticed, because for more common RR types like A and AAAA, the difference to an end user between empty and bogus is irrelevant; they both mean a site is unavailable.

In particular, at least two authoritative resolvers that implement live signing had bugs when returning empty RRsets for DNSSEC-signed zones, in combination with mixed-case queries. Mixed-case queries, also known as DNS 0x20, are used by some recursive resolvers to increase resilience against DNS poisoning attacks. DNSSEC-signing authoritative resolvers are expected to copy the same capitalization from the query into their ANSWER section but also to sign the response as if they had used all lowercase. In particular, PowerDNS versions prior to 4.0.4 had this bug.

## 7. Differences from RFC 6844

This document obsoletes [RFC6844]. The most important change is to the "Certification Authority Processing" section (now called "Relevant Resource Record Set" (Section 3), as noted below). [RFC6844] specified an algorithm that performed DNS tree-climbing not only on the FQDN being processed but also on all CNAMEs and DNAMEs encountered along the way. This made the processing algorithm very inefficient when used on FQDNs that utilize many CNAMEs and would have made it difficult for hosting providers to set CAA policies on their own FQDNs without setting potentially unwanted CAA policies on their customers' FQDNs. This document specifies a simplified processing algorithm that only performs tree-climbing on the FQDN being processed, and it leaves the processing of CNAMEs and DNAMEs up to the CA's recursive resolver.

This document also includes a "Deployment Considerations" section ([Section 6](#)) detailing experience gained with practical deployment of CAA enforcement among CAs in the WebPKI.

This document clarifies the ABNF grammar for the issue and issuewild tags and resolves some inconsistencies with the document text. In particular, it specifies that parameters are separated with semicolons. It also allows hyphens in Property Tags.

This document also clarifies the processing of a CAA RRset that is not empty but that does not contain any issue or issuewild tags.

This document removes the section titled "The CAA RR Type," merging it with "Mechanism" ([Section 4](#)) because the definitions were mainly duplicates. It moves the "Use of DNS Security" section into Security Considerations ([Section 5](#)). It renames "Certification Authority Processing" to "Relevant Resource Record Set" ([Section 3](#)) and emphasizes the use of that term to more clearly define which domains are affected by a given RRset.

## 8. IANA Considerations

IANA has added this document as a reference for the "Certification Authority Restriction Flags" and "Certification Authority Restriction Properties" registries and updated references to [\[RFC6844\]](#) within those registries to refer instead to this document. IANA has also updated the CAA TYPE in the "Resource Record (RR) TYPES" subregistry of the "Domain Name System (DNS) Parameters" registry with a reference to this document.

## 9. References

### 9.1. Normative References

- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <<https://www.rfc-editor.org/info/rfc1034>>.
- [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>>.
- [RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, DOI 10.17487/RFC2181, July 1997, <<https://www.rfc-editor.org/info/rfc2181>>.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <<https://www.rfc-editor.org/info/rfc4033>>.
- [RFC4034]

- Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <<https://www.rfc-editor.org/info/rfc4034>>.
- [RFC4035]** Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <<https://www.rfc-editor.org/info/rfc4035>>.
- [RFC5155]** Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <<https://www.rfc-editor.org/info/rfc5155>>.
- [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>>.
- [RFC5280]** Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC6546]** Trammell, B., "Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS", RFC 6546, DOI 10.17487/RFC6546, April 2012, <<https://www.rfc-editor.org/info/rfc6546>>.
- [RFC6698]** Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <<https://www.rfc-editor.org/info/rfc6698>>.
- [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>>.
- [RFC7970]** Danyliw, R., "The Incident Object Description Exchange Format Version 2", RFC 7970, DOI 10.17487/RFC7970, November 2016, <<https://www.rfc-editor.org/info/rfc7970>>.
- [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>>.

## 9.2. Informative References

- [RFC3647]** Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <<https://www.rfc-editor.org/info/rfc3647>>.



## Acknowledgements

The authors would like to thank the following people who contributed to the design and documentation of this work item: Corey Bonnell, Chris Evans, Stephen Farrell, Jeff Hodges, Paul Hoffman, Tim Hollebeek, Stephen Kent, Adam Langley, Ben Laurie, James Manger, Chris Palmer, Scott Schmit, Sean Turner, and Ben Wilson.

## Authors' Addresses

**Phillip Hallam-Baker**

Venture Cryptography

Email: [phill@hallambaker.com](mailto:phill@hallambaker.com)

**Rob Stradling**

Sectigo Ltd.

Email: [rob@sectigo.com](mailto:rob@sectigo.com)

**Jacob Hoffman-Andrews**

Let's Encrypt

Email: [jsha@letsencrypt.org](mailto:jsha@letsencrypt.org)