Internet Engineering Task Force	P. Hallam-Baker
Internet-Draft	Comodo Group Inc.
Intended status: Standards Track	R. Stradling
Expires: October 27, 2012	Comodo CA Ltd.
	April 25, 2012

TOC

DNS Certification Authority Authorization (CAA) Resource Record draft-ietf-pkix-caa-07

Abstract

The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the certificate signing certificate(s) authorized to issue certificates for that domain. CAA resource records allow a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue.

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 October 27, 2012.

Table of Contents

1. Definitions

TOC

1.1. Requirements Language

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **RFC 2119** [RFC2119].

1.2. Defined Terms

TOC

The following terms are used in this document:

Authorization Entry
: An authorization assertion that grants or denies a specific set of permissions to a specific group of entities.

Canonical Domain Name
: A Domain Name that is not an alias.

Canonical Domain Name Value
: The value of a Canonical Domain Name. The value resulting from applying alias transformations to a Domain Name that is not canonical.

Certificate
: An X.509 Certificate, as specified in **RFC 5280** [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 Certification Authority undertakes to meet in its issue of certificates. See **RFC 3647** [RFC3647].

Certification Practices Statement (CPS)
: Specifies the means by which the criteria of the Certificate Policy are met. In most cases this will be the document against which the operations of the Certification Authority are audited. See **RFC 3647** [RFC3647]

Domain
: The set of resources associated with a DNS Domain Name.

Domain Name
: A DNS Domain name as specified in **RFC 1035** [RFC1035] and revisions.

Domain Name System (DNS)
: The Internet naming system specified in **RFC 1035** [RFC1035] and revisions.

DNS Security (DNSSEC)

Extensions to the DNS that provide authentication services as specified in **RFC 4033** [RFC4033] and revisions.

Issuer
: An entity that issues Certificates.

Extended Issuer Authorization Set
: The most specific Issuer Authorization Set that is active for a domain. This is either the Issuer Authorization Set for the domain itself, or if that is empty, the Issuer Authorization Set for the corresponding Public Delegation Point.

Issuer Authorization Set
: The set of Authorization Entries for a domain name that are flagged for use by Issuers. Analogous to an Access Control List but with no ordering specified.

Public Delegation Point
: The Domain Name suffix under which DNS names are delegated by a public DNS registry such as a Top Level Directory.

Public Key Infrastructure X.509 (PKIX)
: Standards and specifications issued by the IETF that apply the **X.509** [X.509] certificate standards specified by the ITU to Internet applications as specified in **RFC 5280** [RFC5280] and related documents.

Resource Record (RR)
: A set of attributes bound to a Domain Name.

Relying Party
: A party that makes use of an application whose operation depends on use of a Certificate for making a security decision.

Relying Application
: An application whose operation depends on use of a Certificate for making a security decision.

TOC

2. Introduction

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

Conformance with a published CAA record is a necessary but not sufficient condition for issue of a certificate. Before issuing a certificate, a PKIX CA is required to validate the request according to the policies set out in its Certificate Policy Statement. In the case of a public CA that validates certificate requests as a third party, the certificate will be typically issued under a public root certificate embedded in one or more relevant Relying Applications.

Criteria for inclusion of embedded root certificates in applications are outside the scope of this document but typically require the CA to publish a Certificate Practices Statement (CPS) that specifies how the requirements of the Certificate Policy (CP) are achieved and provide an annual audit statement of their performance against their CPS performed by an independent third party auditor.

CAA records only describe the current state of Certification Authority certificate issue authority. Since a certificate is typically valid for at least a year, 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 it was issued. Thus Relying Applications MUST NOT use failure to conform to currently published CAA records specifying issue authorization as a certificate validity criteria.

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

TOC

2.1. The CAA RR type

A CAA RR publishes a CAA property entry that corresponds to the specified domain name. Multiple property entries MAY be associated with the same domain name by publishing multiple CAA RRs at that domain name. Each property entry MAY be tagged with one or more

of the following flag values:

Critical
: If set, indicates that the corresponding property entry tag MUST be understood if the semantics of the CAA record are to be correctly understood by the specified audience.
Issuers MUST NOT issue certificates for a domain if the Extended Issuer Authorization Set contains unknown property entry tags that have both the Issuer and Critical bits set.

The following properties are defined:

issue <Domain Name> [; <tag=value>]*
: The issue property entry declares an authorization entry granting authorization to issue to the holder of the specified domain name or a party acting under the express written authority of the holder of the domain name.

iodef <URL>
: Specifies a URL to which an issuer MAY report certificate issue requests that are inconsistent with the issuer's Certification Practices or Certificate Policy or that a certificate evaluator may use to report observation of a possible policy violation. The IODEF format is used. **[RFC5070]**

The following example informs CAs that certificates MUST NOT be issued except by the holder of the domain name 'ca.example.net' or an authorized agent thereof. Since the policy is published at the Public Delegation Point, the policy applies to all subordinate domains under example.com.

```
$ORIGIN example.com
.       CAA 0 issue "ca.example.net"
```

If the domain name holder specifies one or more iodef properties, a certificate issuer MAY report invalid certificate requests to that address. In the following example the domain name holder specifies that reports MAY be made by means of email with the IODEF data as an attachment or a Web service or both:

```
$ORIGIN example.com
.       CAA 0 issue "ca.example.net"
.       CAA 0 iodef "mailto:security@example.com"
.       CAA 0 iodef "http://iodef.example.com/"
```

A certificate issuer MAY specify additional parameters that allow customers to specify additional parameters governing certificate issue. For example, the Certificate Policy under which the certificate is to be issued or the authentication process to be used.

```
$ORIGIN example.com
.       CAA 0 issue "ca.example.net; account=230123"
```

The syntax and semantics of such parameters is left to site policy and is outside the scope of this document.

Future versions of this specification MAY use the critical flag to introduce new semantics that MUST be understood for correct processing of the record, preventing Certification Authorities that do not recognize the record from issuing certificates.

In the following example, the property 'tbs' is flagged as critical. Neither the example.net CA, nor any other issuer is authorized to issue under either policy unless the processing rules for the 'tbs' property tag are understood.

```
$ORIGIN example.com
.       CAA 0 issue "ca.example.net; policy=ev"
.       CAA 128 tbs "Unknown"
```

Note that the above restrictions only apply to issue of certificates. Since the validity of an end entity certificate is typically a year or more it is quite possible that the CAA records published at a domain will change between the issue of the certificate and verification by a relying party.

---

3. Certification Authority Processing

TOC

Before issue of a certificate, a compliant CA MUST check for publication of a relevant CAA Resource Record(s) and if such record(s) are published, that the certificate requested is consistent with them. If the certificate requested is not consistent with the relevant CAA RRs, the CA MUST NOT issue the certificate.

The Issuer Authorization Set for a domain name consists of the set of all CAA Authorization Entries declared for the canonical form of the specified domain.

The Extended Issuer Authorization Set for a domain name is determined as follows:

- If the Issuer Authorization Set for the domain is empty, the Extended Issuer Authorization Set is empty.
- If the immediately superior node in the DNS hierarchy is a Public Delegation Point, the Extended Issuer Authorization Set is empty.
- Otherwise the Extended Issuer Authorization Set is that of the immediately superior node in the DNS hierarchy.

For example, if the zone example.com has a CAA record defined for caa.example.com and no other domain in the zone, the Issuer Authorization Set is empty for all domains other than caa.example.com. The Extended Issuer Authorization Set is empty for example.com (because .com is a Public Delegation Point) and for x.example.com. The Extended Issuer set for x.caa.example.com, x.x.caa.example.com, etc. is the Issuer Authorization Set for caa.example.com.

If the Extended Issuer Authorization Set for a domain name is not empty, a Certification Authority MUST NOT issue a certificate unless it conforms to at least one authorization entry in the Extended Issuer Authorization Set.

3.1. Canonical Domain Name

TOC

The DNS defines the CNAME and DNAME mechanisms for specifying domain name aliases. The canonical name of a DNS name is the name that results from performing all DNS alias operations.

An issuer MUST perform CNAME and DNAME processing as defined in the DNS specifications **1035** [RFC1035] to resolve CAA records.

3.2. Use of DNS Security

TOC

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 corresponding extended issuer authorization set whether the corresponding DNS records are signed or not.

Use of DNSSEC allows an issuer to acquire and archive a non-repudiable proof that they were authorized to issue certificates for the domain.

3.3. Archive

TOC

A compliant issuer SHOULD maintain an archive of the DNS transactions used to verify CAA eligibility.

In particular an issuer SHOULD ensure that where DNSSEC data is available that the corresponding signature and NSEC/NSEC3 records are preserved so as to enable later compliance audits.

4. Mechanism

TOC

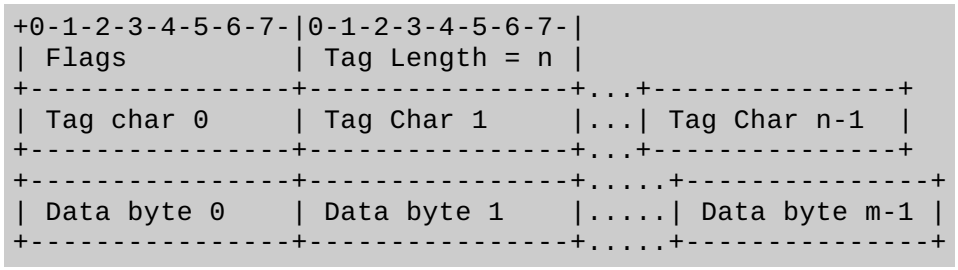
4.1. Syntax

TOC

A CAA RR contains a single property entry consisting of a tag value pair. Each tag represents a property of the CAA record. The value of a CAA property is that specified in the corresponding value field.

A domain name MAY have multiple CAA RRs associated with it and a given property MAY be specified more than once.

The CAA data field contains one property entry. A property entry consists of the following data fields:



Where n is the length specified in the tag length field and m is the remaining octets in the data field (m = d - n - 2) where d is the length of the data section.

The data fields are defined as follows:

Flags
: One octet containing the following fields:

  Bit 0: Issuer Critical Flag
  : If the value is set (1), the critical flag is asserted and the property MUST be understood if the CAA record is to be correctly processed by a certificate issuer.
    A Certification Authority MUST NOT issue certificates for any Domain that contains a CAA critical property for an unknown or unsupported property type that has the issuer bit set.

  Note that according to the conventions set out in **RFC 1035** [RFC1035] Bit 0 is the Most Significant Bit and Bit 7 is the Least Significant. Thus the flags value 1 means that bit 7 is set while a value of 128 means that bit 0 is set according to this convention.
  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 (0) all reserved flags 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 and SHOULD be no more than 15.

Tag
: The property identifier, a sequence of ASCII characters.
  Tag values MAY contain ASCII characters a through z and the numbers 0 through 9. Tag values MUST NOT contain any other characters. Matching of tag values is case insensitive.

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 Resource Record data field.

TOC

4.1.1. Canonical Presentation Format

The canonical presentation format of the CAA record is as follows:

```
CAA <flags> <tag> <data>
```

Where:

flags
: Is an unsigned integer between 0 and 255.

tag
: Is a non-zero sequence of ASCII letter and numbers in lower case.

data
: Is the ascii text Encoding of the value field

TOC

4.2. CAA issue Property

The issue property is used to request that certificate issuers perform CAA issue restriction processing for the domain and to grant authorization to specific certificate issuers.

The CAA issue property value has the following sub-syntax (specified in ABNF as per **[RFC4234]**).

```
Property = space [domain] * (space ";" parameter) space

domain = label *("." label)
label = 1* (ALPHA / DIGIT / "_" / "-" )

space = *(SP / HTAB)

parameter =  / space tag "=" value

tag = 1* (ALPHA / DIGIT)

value = *VCHAR | DQUOTE *(%x20-21 / %x23-7E) DQUOTE
```

A CAA record with an issue parameter tag that does not specify a domain name is a request that certificate issuers perform CAA issue restriction processing for the corresponding domain without granting authorization to any certificate issuer.

This form of issue restriction would be appropriate for use with a domain that the domain name owner does not intend to be used.

For example, the following CAA record set requests that no certificates be issued for the domain 'nocerts.example.com' by any certificate issuer.

```
nocerts.example.com       CAA 0 issue ";"
```

A CAA record with an issue parameter tag that specifies a domain name is a request that certificate issuers perform CAA issue restriction processing for the corresponding domain

and grants authorization to the certificate issuer specified by the domain name.

For example, the following CAA record set requests that no certificates be issued for the domain 'certs.example.com' by any certificate issuer other than the example.net certificate issuer.

```
certs.example.com       CAA 0 issue "example.net"
```

CAA authorizations are additive. thus the result of specifying both the empty issuer and a specified issuer is the same as specifying just the specified issuer alone.

An issuer MAY choose to specify issuer-parameters that further constrain the issue of certificates by that issuer. For example specifying that certificates are to be subject to specific validation polices, billed to certain accounts or issued off specific roots.

The syntax and semantics of issuer-parameters are determined by the issuer alone.

TOC

4.3. CAA iodef Property

The iodef property specifies a means of reporting certificate issue requests or cases of certificate issue for the corresponding domain that violate the security policy of the issuer or the domain name holder.

The Incident Object Description Exchange Format (IODEF) **[RFC5070]** is used to present the incident report in machine readable form.

The iodef property takes a URL as its parameter. The URL scheme type determines the method used for reporting:

mailto
: The IODEF incident 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 **[RFC6046]**.

TOC

5. Security Considerations

CAA Records assert a security policy that the holder of a domain name wishes to be observed by certificate issuers. The effectiveness of CAA records as an access control is thus dependent on observance of CAA constraints by issuers.

Observance of CAA records by issuers is subject to accountability controls and proposed industry requirements.

While a Certification Authority can choose to ignore published CAA records, doing so increases the both the probability that they will mis-issue a certificate and the consequences of doing so. Once it is known that a CA observes CAA records, malicious registration requests will disproportionately target the negligent CAs that do not, and so the mis-issue rate amongst the negligent CAs will increase. Since the CA could clearly have avoided the mis-issue by performing CAA processing, the likelihood of sanctions against the negligent CA is increased. Failure to observe CAA issue restrictions provides an objective criteria for excluding issuers from embedded roots of trust.

In contrast, a Certification Authority that processes CAA records correctly can reasonably claim that any residual mis-issue event could have been avoided had the Domain Name holder published appropriate CAA records.

5.1. Mis-Issue by Authorized Certification Authority

TOC

Use of CAA records does not provide protection against mis-issue by an authorized Certification Authority.

Domain name holders SHOULD ensure that the CAs they authorize to issue certificates for their domains employ appropriate controls to ensure that certificates are only issued to authorized parties within their organization.

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

5.2. Suppression or spoofing of CAA records

TOC

Suppression of the CAA record or insertion of a bogus CAA record could enable an attacker to obtain a certificate from a CA that was not authorized to issue for that domain name.

5.2.1. Certification Authorities

TOC

Since a certificate issued by a CA can be valid for several years, the consequences of a spoofing or suppression attack are much greater for Certification Authorities and so additional countermeasures are justified.

A CA MUST mitigate this risk by employing DNSSEC verification whenever possible and rejecting certificate requests in any case where it is not possible to verify the non-existence or contents of a relevant CAA record.

In cases where DNSSEC is not deployed in a corresponding domain, a CA 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 name server. Cached data MUST NOT be relied on but MAY be used to support additional anti-spoofing or anti-suppression controls.

5.3. Denial of Service

TOC

Introduction of a malformed or malicious CAA RR could in theory enable a Denial of Service attack.

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

5.3.1. Issuer

TOC

An attacker could in principle perform a Denial of Service 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 the protocol does not exacerbate the existing need to mitigate Denial of Service attacks to any meaningful degree.

5.4. Abuse of the Critical Flag

TOC

A Certification Authority could make use of the critical flag to trick customers into publishing records which prevent competing Certification Authorities from issuing certificates even though the customer intends to authorize multiple providers.

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 who will thus discover the deception. It is thus unlikely that the attack would succeed and the attempt might lay the perpetrator open to civil or criminal sanctions.

6. IANA Considerations

TOC

6.1. Registration of the CAA Resource Record Type

TOC

[Note to IANA, the CAA resource record has already been assigned. On issue of this draft as an RFC, the record should be updated to reflect this document as the authoritative specificaton and this paragraph (but not the following ones deleted]

IANA has assigned Resource Record Type 257 for the CAA Resource Record Type and added the line depicted below to the registry named Resource Record (RR) TYPEs and QTYPEs as defined in BCP 42 RFC 5395 [RFC5395] and located at http://www.iana.org/assignments/dns-parameters.

	Value and meaning	Reference
CAA	257 Certification Authority Restriction	[RFC-THIS]

6.2. Certification Authority Authorization Properties

TOC

[Note to IANA, this is a new registry that needs to be created and this paragraph but not the following ones deleted.]

IANA has created the Certification Authority Authorization Properties registry with the following initial values:

	Meaning	Reference
issue	Authorization Entry by Domain	[RFC-THIS]
iodef	Report incident by means of IODEF format report	[RFC-THIS]
auth	Reserved	
path	Reserved	
policy	Reserved	

Addition of tag identifiers requires a public specification and expert review as set out in **RFC5395** [RFC5395]

7. References

TOC

7.1. Normative References

TOC

[RFC1035] Mockapetris, P., "**Domain names - implementation and specification**," STD 13, RFC 1035, November 1987 (**TXT**).

[RFC2045] **Freed, N.** and **N. Borenstein**, "**Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies**," RFC 2045, November 1996 (**TXT**).

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, March 2005 (TXT).

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 4055, June 2005 (TXT).

[RFC4234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," RFC 4234, October 2005 (TXT, HTML, XML).

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format," RFC 5070, December 2007 (TXT).

[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, May 2008 (TXT).

[RFC5395] Eastlake, D., "Domain Name System (DNS) IANA Considerations," RFC 5395, November 2008 (TXT).

[RFC6046] Moriarty, K. and B. Trammell, "Transport of Real-time Inter-network Defense (RID) Messages," RFC 6046, November 2010 (TXT).

[X.509] International Telecommunication Union, "ITU-T Recommendation X.509 (11/2008): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks," ITU-T Recommendation X.509, November 2008.

7.2. Non Normative References

TOC

[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, November 2003 (TXT).

Authors' Addresses

TOC

Phillip Hallam-Baker
Comodo Group Inc.
Email: philliph@comodo.com

Rob Stradling
Comodo CA Ltd.
Email: rob.stradling@comodo.com