**Ballot XXX - Make CAA Checking Mandatory**

The following motion has been proposed by Gervase Markham of Mozilla and endorsed by XXX of XXX and XXX of XXX:

**Statement of Intent**:

Certificate Authority Authorization (CAA) is a DNS Resource Record defined in RFC 6844 - <https://datatracker.ietf.org/doc/rfc6844/> , published in January 2013. It allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain and, by consequence, that no other CAs are authorized.

The intent of this motion is to make it mandatory for CAs to check CAA records at issuance time for all certificates issued (except as noted below), and to prevent issuance if a CAA record is found which does not permit issuance by that CA. This therefore allows domain owners to set an issuance policy which will be respected by all publicly-trusted CAs, and allows them to mitigate the problem that the public CA trust system is only as strong as its weakest CA.

Note that CAA is already a defined term in the BRs and so does not need definitional text to be provided by this motion.

**-- MOTION BEGINS --**

Create the following new section 3.2.2.8

3.2.2.8 CAA

As part of the issuance process, the CA must check for a CAA record for each dNSName in the subjectAltName extension of the TLS certificate to be issued according to the procedure in RFC 6844 and as clarified in this section.

When performing CAA checking, the CA MUST check every Authorization Domain Name from the specified dNSName up to and including the Base Domain Name. Checking CAA means the CA MUST perform the checks specified in Appendix A prior to issuing, reissuing, renewing or rekeying a Certificate.

The CA MUST:

* Respect the CAA Issuer Critical tag. If there is a tag that is marked critical that the CA does not support, the CAA check must fail. Failures of this type should be reported to CABF for further review and inspection to determine if CAs are abusing CAA records
* Support the CAA issue and issuewild tags
* Check CAA within these time periods prior to issuance:
	+ In the event a CAA record is found, the CA may cache the result for 12-hours or for the TTL of the CAA record, whichever is greater, but not to exceed 1-year
	+ In the event there were no CAA records found, the CA may cache the result for 24-hours
* Log CAA failures

The CA may treat record lookup failures as permission to issue if the following is true: This is not to say CAA checking as defined above should end with the first look-up failure as the CA MUST continue the complete CAA checking process even if they encounter one or more failures.

* the failure is outside the CA's infrastructure;
* the lookup has been retried at least once; and
* the domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA SHOULD support iodef types of mailto: and https:.

RFC 6844 requires that CAs "MUST NOT issue a certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies." For issuances conforming to these Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:

* The CAA check failed but was subsequently approved by an Enterprise RA or Certificate Approver with knowledge that the CAA check failed.
* CAA checking is optional for certificates for which a Certificate Transparency pre-certificate was created and logged in at least two Active CT logs as listed here <https://sites.google.com/site/certificatetransparency/known-logs>, and for which CAA was checked in accordance with this section prior to generating the Precertificate.
* CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where opting out of CAA checking is an explicit contractual provision in the contract with the Applicant.
* CAA checking is optional if the same entity or an affiliate of the entity operates the CA, owns the domain being checked, and runs the domain's DNS.

Update section 2.2 ("Publication of Information") of the Baseline Requirements, to remove the following text:

Effective as of 15 April 2015, section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state whether the CA reviews CAA Records, and if so, the CA’s policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA SHALL log all actions taken, if any, consistent with its processing practice.

and replace it with:

Effective as of XXX, section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state the CA’s policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue.

Create Appendix A – CAA checking

The following is pulled from RFC 6844 and expanded on slightly to clearly define the precise checks that MUST be performed for BR compliant CAA checking:

Let

1. CAA(X) be the record set returned in response to performing a CAA record query on the label X,
2. P(X) be the DNS label immediately above X in the DNS hierarchy, and
3. A(X) be the target of a CNAME or DNAME alias record specified at the label X.

Then:

1. If CAA(X) is not empty, R(X) = CAA (X), otherwise
2. If A(X) is not null (i.e, there is a CNAME or DNAME record for X), and R(A(X)) is not empty, then R(X) = R(A(X)), otherwise
3. If X is not a Base Domain Name, then R(X) = R(P(X)) and perform check again starting at step 1, otherwise
4. R(X) is empty.
* If any one of the returned records in R(X) contains a Domain Name from the set of the CA’s Issuer Domain Names, then the CA may issue the certificate.
* If none of the records returned in R(X) contain any Domain Name from the set of the CA’s Issuer Domain Names, then the CA MUST NOT issue the certificate
* If a CNAME or DNAME record is found, then the CAA check will start over using the returned value as the new input to the CAA check.

Update section 1.6.3 of the Baseline Requirements with this reference:

RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, January 2013.

Update section 11.7.1 of the EVGL to read as follows:

For each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant’s Parent Company, Subsidiary Company, or Affiliate, collectively referred to as “Applicant” for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4 of the Baseline Requirements and has checked CAA in accordance with Section 3.2.2.8 of the Baseline Requirements. For a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant’s control over the .onion Domain Name in accordance with Appendix F.

**-- MOTION ENDS --**