**Ballot XXX - Make CAA Checking Mandatory**

The following motion has been proposed by Gervase Markham of Mozilla and endorsed by Jeremy Rowley of DigiCert and Ryan Sleevi of Google:

**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 implication, that no other CAs are authorized.

The intent of this motion is to make it mandatory for CAs to check CAA records at time of issuance time for all TLS 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.

The effective date of this ballot is section is effective as of 8 September 2017.

**-- MOTION BEGINS --**

Create the following new section 3.2.2.8 as a subsection of 3.2.2 “Authentication of Organization and Domain Identity”

**3.2.2.8 CAA Records**

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 climb the DNS name tree from the specified label up to but not including the DNS root '.'. 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 or the value of the negative caching TTL.
* 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:

* 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 September 8, 2017, 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 to assure consistent interpretation of CAA requirements:

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 CAA(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 be performed on the returned value..

**Example 1 – Typical example with a CAA record**

Assume you want to find the CAA record for www.example.com and the CAA record is set on example.com, then the processing would be as follows:

1. CAA(www.example.com) – nothing
2. DNAME(www.example.com) – nothing
3. CNAME(www.example.com) – nothing
4. CAA(example.com) – **value**

**Example 2 – Typical example with no CAA record**

Assume you want to find the CAA record for www.example.com and there is no CAA record set, then the processing would be as follows:

* 1. CAA(www.example.com) – nothing
	2. DNAME(www.example.com) – nothing
	3. CNAME(www.example.com) – nothing
	4. CAA(example.com) – nothing
	5. DNAME(example.com) – nothing
	6. CNAME(example.com) – nothing
	7. CAA(com) – nothing
	8. DNAME(com) – nothing
	9. CNAME(com) - nothing

**Example 3 – Example with CNAME**

Assume you want to find the CAA record for foo.example.com and

* foo.example.com has a CNAME to bar.example.net, and
* the CAA record is set on "example.com"

Then the processing would be as follows:

1. CAA(foo.example.com) - nothing
2. DNAME(foo.example.com)
3. CNAME(foo.example.com) - **bar.example.net**
	1. CAA(bar.example.net) - nothing
	2. DNAME(bar.example.net) – nothing
	3. CNAME(bar.example.net) - nothing
	4. CAA(example.net) – nothing
	5. DNAME(example.net) - nothing
	6. CNAME(example.net) - nothing
	7. CAA(net) - nothing
	8. DNAME(net) - nothing
	9. CNAME(net) - nothing
4. CAA(example.com) - value

**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 –**

The procedure for approval of this Final Maintenance Guideline ballot is as follows:

|  |  |  |
| --- | --- | --- |
| BALLOT 187Status: Maintenance Guideline | Start time (22:00 UTC) | End time (22:00 UTC) |
| Discussion (7 to 14 calendar days) | 2017-02-22 | 2017-03-01 |
| Vote for approval (7 calendar days) | 2017-03-01 | 2017-03-08 |
| If vote approves ballot: Review Period (Chair to send Review Notice) (30 calendar days).  If Exclusion Notice(s) filed, ballot approval is rescinded and PAG to be created.If no Exclusion Notices filed, ballot becomes effective at end of Review Period. | Upon filing of Review Notice by Chair | 30 days after filing of Review Notice by Chair |
| Effective Date | 8 September 2017 |  |

From Section 2.3 of the Bylaws: If the Draft Guideline Ballot is proposing a Final Maintenance Guideline, such ballot will include a redline or comparison showing the set of changes from the Final Guideline section(s) intended to become a Final Maintenance Guideline, and need not include a copy of the full set of guidelines. Such redline or comparison shall be made against the Final Guideline section(s) as they exist at the time a ballot is proposed, and need not take into consideration other ballots that may be proposed subsequently, except as provided in Section 2.3(j) of the Bylaws.

Votes must be cast by posting an on-list reply to this thread on the Public Mail List. A vote in favor of the motion must indicate a clear “yes” in the response. A vote against must indicate a clear “no” in the response. A vote to abstain must indicate a clear “abstain” in the response. Unclear responses will not be counted. The latest vote received from any representative of a voting member before the close of the voting period will be counted. Voting members are listed here: https://cabforum.org/members/

In order for the motion to be adopted, two thirds (2/3) or more of the votes cast by members in the CA category and greater than 50% of the votes cast by members in the browser category must vote “yes”. Quorum is shown on CA/Browser Forum wiki. Under Section 2.2(g) of the Bylaws, at least the required quorum number of voting members must participate in the ballot for the ballot to be valid, either by voting in favor, voting against, or abstaining.