Symantec™

The Current State of the CAA Debate

Rick Andrews

New Developments

Gerv updated us on Mozilla's attempts to add its CAA Record:

- "I just contacted Akamai CCARE and they confirmed CAA records are not supported. Our architecture is setup so Akamai AXFRs data from our BIND based hidden masters. While our side would support the record, their ZTA (zone transfer agent) and proprietary DNS server does not.

Rick reported that

- "I managed to convince ISC to add CAA support to their upcoming version of BIND: version 9.9.6 (currently in release candidate) has support for CAA. See https://kb.isc.org/article/AA-01202/81/BIND-9.9.6rc1-Release-Notes.html."

Current Proposed Text

Add to Section 4 Definitions, new item:

- **CAA Record**: The Certification Authority Authorization (CAA) DNS Resource Record of RFC 6844 (http:tools.ietf.org/html/rfc6844) that allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of a CAA Resource Record allows public Certification Authorities to implement additional controls to reduce the risk of unintended. certificate mis-issue

Current Proposed Text

In Section 8.2.2 (Certificate Policies – Disclosure, instead of editing warranties in section 7.1.2 or verification practices in section 11, as some have suggested) add the following to the end of the paragraph:

- Effective as of [insert date that is six months from Ballot 125 adoption], section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CA’s still conforming to RFC 2527) shall disclose:
  - (1) whether the CA reviews CAA Records, and if so,
  - (2) the CA’s policy or practice on processing CAA Records and comparing them with proposed Domain Names for the Common Name field or Subject Alternative Name fields of certificates applications, and
  - (3) any actions taken as result of such comparison.

Concerns - 1

- Ryan from Google suggested changing
  - (2) the CA’s policy or practice on processing CAA Records and comparing them with proposed Domain Names for the Common Name field or Subject Alternative Name fields of certificates applications, and

to

  - (2) the CA's policy or practice on processing CAA Records for each Fully-Qualified Domain Name listed in a certificate, and

To better match language elsewhere in the BRs.

Concerns - 2

- Kirk from Trend had this concern: “Every time CAA has come up as a topic of discussion at a CAB Forum meeting or on a call, one or more CAs and browsers have expressed concern that CAA could be used as a "blocking" strategy by CAs in order to add hurdles for another CA to sell certificates to the same customer. The main way this could happen is if a CA induces a customer to insert its name to a CAA record when there is no CAA record at the time for the customer (or even worse, adds its name to a blank CAA record in the customer's name -- this could happen if the fine print of the Subscriber Agreement authorizes the CA to insert its name in a CAA record for the customer and the customer has no idea this is happening). Another potential abuse would be if a CA got its name put in blank CAA records for other domains registered to the customer that are not even part of the pending certificate order so that other CAs would find it more difficult to sell certificates for those domains.There seems to be strong sentiment among CAs and browsers for some language prohibiting this potential practice as anticompetitive. ”

Concerns - 3

- Kirk proposed this amendment: “In order to make certain that CAA is not used by CAs in an anticompetitive manner, no CA shall

  1. request or suggest that a customer include the CA’s name in a CAA record for the domain in question if the customer does not already have a CAA record that includes the name of one or more other CAs but omits the CA’s name,
  2. obtain authorization from the customer to act on the customer’s behalf (directly or by request to the customer’s DNS operator) to create a CAA record for the customer that includes the CA’s name for the domain in question if the customer does not already have a CAA record that includes the name of one or more other CAs but omits the CA’s name, or
  3. request or suggest that a customer include the CA’s name in a CAA record for other domains not the subject of the customer’s certificate order or obtain authorization from the customer to act on the customer’s behalf (directly or by request to the customer’s DNS operator) to create a CAA record for the customer for other domains not the subject of the customer’s certificate order.”

Concerns - 4

- Ryan replied that “If you feel strongly about this, I feel it is worth a separate ballot. I do not support burdening this ballot with that language.”
- Geoff from Apple said: “I am not enthusiastic about adding a simple reporting requirement. Wouldn't it be better to propose something which says how to really improve security, even if only as a recommendation?

  And, if we're adding a recommendation (or even just a reporting requirement, since surely the aim of that is to encourage CAs to say they do support CAA), I think Kirk's suggestion is quite reasonable, in principle. But I don't want to discourage CAs from telling their customers to create a CAA record, or even doing it for the customer, so long as those CAA records will be accurate.”

Concerns - 5

- Gerv from Mozilla said “We support the ballot as written, and I share Ryan's concerns about the precedents that regulating a CA's communications with its customers would set. I comment because I also have an active disagreement with Kirk's amendment. I actually think it is fine for CAs to suggest that customers consider using CAA if they are not using it - something which your first point outlaws. I agree that 2), and the analogous part in 3), are bad ideas. But not all bad ideas should be illegal.”

Next Steps?

The Case for CAA

- CAs can build it on their own (no browser support needed)
- It’s relatively simple for the customer and the CA
- Customers have to opt-in, so deployment is likely to be minimal for the next few years
- It’s not for everyone, but it gives some customers a useful tool
- It demonstrates our willingness to act to prevent mis-issuance