The Current State of the CAA Debate

Rick Andrews

Current Proposed Text

Add to Section 4 Definitions, new item:

- **CAA**: From RFC 6844 (http:tools.ietf.org/html/rfc6844): "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. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

Current Proposed Text

Amend subparagraph 2 of 7.1.2 (Certificate Warranties) as follows:

- 2. Authorization for Certificate: That, at the time of issuance, the CA

  (i) implemented procedure**s** for verifying that the Subject authorized the issuance of the Certificate ~~and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject~~, **including procedures to**

  (a) consider the CAA record of each Domain Name to be listed in the Certificate's subject field or subjectAltName extension, and

  (b) establish that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;

  (ii) followed the procedures when issuing the Certificate; and

  (iii) accurately described the procedures in the CA's Certificate Policy and/or Certification Practices Statement, **(e.g. in Section 4.2 of an RFC2527 compliant CP/CPS or Section 4.2.2 of an RFC3647 compliant CP/CPS).**

  It is permissible for the CA to ignore CAA records completely, as long as that policy/practice is documented in the CA's Certificate Policy and/or Certification Practice Statement.

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

Concerns - 1

- Eddy said there might be concern about anti-competitive effects, where management of a company makes it more difficult to engage with a CA that is not listed in the CAA record. Stephen said he supported Eddy’s position, because a subsidiary of a large, multinational company will approach him and ask for a certificate, but that person does not deal with the person within the company who runs the DNS – it’s a bureaucratic whirlwind. So you have a situation where they are authorized to get a certificate, but the CAA record might be interpreted as prohibiting issuance altogether.
- This seemed to evolve into a discussion about how a CA determines that it has proper authorization from someone in a large company. Ryan expressed a need to set company-wide policy that could not be overridden by lower-level employees.

Concerns - 2

- Ryan asked Jeremy about the processing policy when it is apparent within an organization that there is conflict between the DNS manager and a server administrator. Jeremy said that DigiCert would seek clarification from the organization’s executive management. Ryan said that the CA would have to make assumptions about how an entity is organized and that he didn’t like that to happen on a case-by-case basis because each is different, and that would lead to inconsistency.
- Phill said that the scenario of conflicting direction from the same organization will be extremely rare. Either they won’t have a CAA record, or they will be keeping them directly.

Concerns - 3

- Stephen said that this gives a big CA the ability to embed itself anti-competitively in a business, which creates special concern when a CA operates as a registrar/DNS operator.
- Phill said that is why RFC 6844 explains that a CA describes its practices in its CP or CPS and is audited and subject to public review and self-policing. A CP or CPS could even state that a CA will not honor the record of an entity that is acting anti-competitively.
- CAA allows multiple records in the same zone file to indicate that multiple CAs are authorized

Concerns - 4

- Stephen said the real problem will be with a corporate IT department headquartered in the U.S. when the subsidiary is based in France. Ryan said that in most large corporations there is a very clear central authority and that certainly a company like Google would not tolerate a CA’s disregard of a CAA record because a CA cannot know/determine which CAs are authorized except by referring to the CAA record.
- Rick suggested that the subsidiary will probably have a DNS sub-domain (fr.example.com), and CAA requires records at a subdomain to take precedence over those at a higher-level one. It’s also likely that the subsidiary will manage a different domain name (example.fr) so there will be no conflict with example.com.

Concerns - 5

- Jeremy said that DigiCert was also concerned with CAA becoming a “do not issue” list, so DigiCert’s approach will be to treat a CAA record as a hurdle requiring it to establish that the applicant representative is authorized by the company to request a certificate and not as an absolute prohibition.
- Phill said that the same issue came up in the IETF and that is why the title of the RFC was changed.
- It’s permissible for a CA to document that they were not listed in the CAA record, but received authorization to issue from a particular customer representative. The CA does not need to be added in a CAA record in order to issue a certificate.

Concerns - 6

- Jeremy said a decision by a DNS administrator cannot always be considered as the directive of management.
  - Is this concern realistic? Do DNS administrators add records to DNS without being told to?
- Stephen said that increasingly we're likely to see friction within the management of organizations in the choices they make when they are trying to obtain a certificate. There will be business leaders within organizations who have authority to choose their vendor and there will be conflict over which CAs are named in the CAA record.
  - If the organization or its politics are too complex, it's likely that the organization will simply not deploy a CAA record.

Open Issues

Can we set an effective date without audit/browser enforcement?