What should go in the “O” Field discussion

Dean Coclin

Who can request a cert for dean.example.com?

- Dean Coclin, author of the content and logical operator of the dean.example.com origin
- Example.com, provider of hosting services for Dean Coclin
- CDN Corp, a CDN that provides SSL/TLS front-end services for example.com, which does not offer them directly
- Marketing Inc, the firm responsible for designing and maintaining the website on behalf of Dean Coclin
- Payments LLC, the payment processing firm responsible for handling orders and financial details on dean.example.com
- DNS Org, the company who operates the DNS services on behalf of Dean Coclin
- Mail Corp, the organization who handles the MX records that dean.example.com responds to

WHAT SHOULD GO IN THE “O” FIELD?

Any of these parties (but one) are entitled to obtain a cert for dean.example.com:

1. Can use a file-based method on dean.example.com, or if control over DNS, add subrecords to establish validation
2. Can use validation based on the registerable domain portion (WHOIS)
3. Can use a file-based method on dean.example.com or a DNS based method
4. Can use a file-based method or equivalent
5. Cannot obtain a certificate, unless they can get one of the other parties to make a suitable change on their behalf to satisfy a request
6. Can modify the DNS or respond to email (in the case of anonymized WHOIS that provides email forwarding services)
7. Can monitor/respond to emails as they come in

Peter Bowen said:

1. BR Section 7.1.4.2.2 requires that the organizationName and other Subject attributes contain information verified as per 3.2.2.1

2. BR Section 3.2.2.1 says "If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant[…]"

3. BR Section 1.6.1 has three definitions that are relevant:
   - "Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber."
   - "Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field."
   - "Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement."

4. BR Section 9.6.3 lays out obligations of the Subscriber

➢ So, based on this, I think it is accurate that the Subject Identify Information, including the organizationName attribute, MUST identify the natural person or Legal Entity that is the Applicant and is required to meet the obligations of the Subscriber Agreement or Terms of Use.

- Does this flow? Is there a situation where the person or entity named in the certificate subject is not the Applicant and/or not the Subscriber?

Kirk/Peter discussion

- Kirk: I can actually understand all the distinctions about names in the O field. But I don't understand what problem we are addressing. Is there an actual current problem (recent cases?), or are we just working on this in the abstract to tighten the rules?
- I recall you may have found some weird certs out there – but do you think any were actually misused?
- I think our discussion will be most productive if we have a clear focus on the problem we truly want to solve.
- Peter: As a CA, I would like to be clear on the requirements I have to meet and ensure my customers (subscribers) need to meet. The definition of Applicant/Subscriber is rather core to many of the BRs.
- I don't see the certs that I found as weird — they seem normal, especially given the requirements in 9.6.3. But obviously not all agree and I would like a clear CAB Forum position one way or the other.

Doug said:

- I don't think you're asking the right question: "Who can request a cert for dean.example.com". It's not who can request it, but more the relationship between the Org field and the Domain in the CN or SAN, right? In reality you never know who is requesting the certificate, only what they put into their request.
- Today it's just domain validation that's needed to verify domains for OV certs, no ownership:
  - Verify Org is a company using an authorized repository
  - Verify Applicant is authorized to represent the company
  - They can demonstrate domain control over the domain
- There is no requirement to verify that the organization "owns" the domain today, are you asking that we change the vetting rules for how domains are added to OV certificates?
- Even EV requirements let the company add domains to an EV cert by demonstrating Domain Control using the same procedures as OV and DV (except for item 7 is prohibited plus the signer approval step). Are you recommending we not allow companies to add domains to their certs with domain control and that they must "own" the domain?

Gerv said:

- Yes, Doug is exactly right. The "who can request a certificate for dean.example.com" question would relate to e.g. validation methods. The correct question here that one might ask is "how does the O field in the OV or EV certificate for dean.example.com relate to the various parties involved in running or operating that website?"

Dimitris said:

- Although my intuition (as a user) is closer to the argument that the "O" field should represent the owner of the content of the web site I am visiting, I can also understand the other arguments that it should represent the web-site owners or the domain owners, etc. In an attempt to minimize the gap between the different arguments, there could be a proposal to change the EV guidelines and make room for Subject entries that allow for the representation of:
- "Web site Administrator"
- "Web site Content Owner"
- "Domain Owner"
- ...
- The names are indicative. There might be appropriate existing OIDs that such information might fit but you could also create new ones as you did for the subject:JurisdictionLocalityName (OID:1.3.6.1.4.1.311.60.2.1.1) or even use CA/B Forum's arc to implement these fields.
- Since the majority think that all these fields are important for the user to know, the browsers at the UI level, could implement code to represent all this information in a sequenced manner (change this displayed info every 3-5 seconds) or default in some value (say the "Web site Content Owner") and provide the extra information if a user clicks on the presented information or the padlock or the Green bar.
- This type of verification should be feasible only for EV certificates.

Ryan said:

i. Recognize we don't have consensus yet for what the O field should present as

ii. Recognize that the VWG proposals provide many wonderful security benefits that we shouldn't let them get hungup on resolving i)

iii. Take a pass at the BRs, in their entirety, to find places where the language may be inconsistent with respect to the (unresolved) status quo, and update that language to reflect the present reality

iv. Longer term, if this is a topic members are passionate about, which I think we have evidence that some CAs are, work to build consensus as to those goals

- Before we can do iii), we need some degree of agreement on i) and ii), and I should hope that should be easy to find, but do let me know if you disagree.