中華電信
Chunghwa Telecom

Suggestions about correcting of Documents of CA/Browser Forum

Chunghwa Telecom Co., Ltd.

Li-Chun CHEN,

Engineer, CISSP, CISM, CISA, PMP

realsky@cht.com.tw

CA/Browser Forum Meeting 33

September, 16-18 , 2014

Some Problem about DN

- If a an applicant is registered as a national company and his country with no states/provinces :
  - "Bouvet Island", "British Virgin Islands", "Christmas Island", "Falkland Islands", "Faroe Islands", "French Guiana", "Gibraltar", "Guadeloupe", "Guam", "Guernsey", "Isle of Man", "Jersey", "Lebanon", "Macedonia", "Martinique", "Mayotte", "Montenegro", "Netherlands Antilles", "Niue", "Norfolk Island", "Palestinian Territory", "Pitcairn", "Reunion", "Serbia", "Singapore", "Slovenia", "South Georgia and the South Sandwich Islands", "Svalbard and Jan Mayen", "Western Sahara", "Vatican", Taiwan, etc.
  - Ref: https://www.drupal.org/node/636464

SSL B.R.(1/2)

Section	General B.R. V.1.19	Suggested modification
9.2.4 Subject Distinguished Name Fields	**C. Certificate Field:** subject:localityName (OID: 2.5.4.7) **Required** if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent. **Optional** if the subject:organizationName and subject:stateOrProvinceName fields are present. **Prohibited** if the subject:organizationName field is absent. **Contents:** If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 11.2.	**C. Certificate Field:** subject:localityName (OID: 2.5.4.7) **Optional** (1) if the subject:organizationName and subject:stateOrProvinceName fields are present. (2)if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent. **Prohibited** if the subject:organizationName field is absent. **Contents:** If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 11.2.

SSL B.R.((2/2)

Section	General B.R. V.1.19	Suggested modification
9.2.4	**D. Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8) **Required** if the subject:organizationName field is present and subject:localityName field is absent. **Optional** if subject:organizationName and subject:localityName fields are present. **Prohibited** if the subject:organizationName field is absent.	**D. Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8) **Optional** (1) if subject:organizationName and subject:localityName fields are present. (2) if the subject:organizationName field is present and subject:localityName field is absent. **Prohibited** if the subject:organizationName field is absent.

Code Signing B.R. Draft (1/2)

Contents	Code Signing B.R. Draft	Suggested modification
9.2.4	**C. Certificate Field**:subject:localityName (OID: 2.5.4.7) **Required/Optional**: Required if the subject:stateOrProvinceName field is absent. Optional if the subject:stateOrProvinceName field is present. **Contents**: If present, the subject:localityName field MUST contain the Subject's locality information as verified under BR Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with BR Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under BR Section 11.2.	**C. Certificate Field**: subject:localityName (OID: 2.5.4.7) **Optional**: (1)Optional if the subject:stateOrProvinceName field is absent. (2) Optional if the subject:stateOrProvinceName field is present. (3)Absent if a an applicant is registered as a national company or a national organization, also stateOrProvinceName field is absent. **Contents**: If present, the subject:localityName field MUST contain the Subject's locality information as verified under BR Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with BR Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under BR Section 11.2.

Code Signing B.R. Draft (2/2)

Contents	Code Signing B.R. Draft	Suggested modification
9.2.4	**d. Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8) Required/Optional: Required if the subject:localityName field is absent. Optional if thesubject:localityName field is present. **Contents:** If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under BR Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with BR Section 9.2.5, the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under BR Section 11.2.5.	**d. Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8) Optional: (1) Optional if the subject:localityName field is absent. (2) Optional if thesubject:localityName field is present. (3)Absent if a an applicant is registered as a national company or a national organization, also stateOrProvinceName field is absent. (4)Absent if an applicant is an individual who live in a country without state or province. **Contents:** If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under BR Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with BR Section 9.2.5, the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under BR Section 11.2.5.

More comments from my colleagues. Wen-Cheng Wang, Ph.D.

Our understand of the X.500 naming semantics

- According to our understand of the X.500 naming semantics , the meaning of "C=XX, ST=Place A" is to narrow down the naming space into the range of "Place A of Country XX" so that we can distinguish some entity from others within the naming space.
- Therefore, the DN "C=XX, L=Place A, O=Oragnization1" is used to distinguish Oragnization1 within the naming space of "C=XX, L=Place A" from other entities.
- The same concept applies to stateOrProvinceName(ST).

narrowing down naming space into some region of the county

- It is often that some people might interpret the meaning of "C=XX, L=Place A, O=Oragnization1" as "Organization1 is located at Place A of Country XX".
- **However, we should note that the meaning of "narrowing down naming space into some region of the county" is not always the same with the meaning of "being located at some region of the county".**

Let's take Taiwan as an example(1/3)

- In Taiwan, according our Company Law, the company name must be unique for the whole country.
- Furthermore, our Company Law requires the company to register its business location which will be some city or county.

Let's take Taiwan as an example(2/3)

- This is an example where the legally naming uniqueness scope for a entity is not the same as where the entity is legally located.
- **In Taiwan, since the company name must be unique for the whole country, the subject DN for a company, such as Chunghwa Telecom, should look like**
  - "C=TW, O=Chunghwa Telecom Co., Ltd

Let's take Taiwan as an example(3/3)

- This subject DN already uniquely identifies the company.
- There is no necessary to add RDNs such as locality(L), or stateOrProvinceName(ST) into the subject DN.
- If we specify the subject DN as "C=TW, L=Taipei City, O=Chunghwa Telecom Co., Ltd.", that will mean it is a company registered in Taipei City.
  - This will not conform to our Company Law because companies in Taiwan is registered in the country level not in the municipal level.

Small businesses according to Taiwan’s Business Registration Law

- On the other hand, in Taiwan, we have small businesses (such as stores) which is established and registered according to our Business Registration Law.
- In Taiwan, small businesses is registered in municipal level. The Business Registration Law requires that the name of the small business must be unique with the municipality (that will be a city or a county) where it is registered.

Suitable subject DN for small businesses

- For example, there might be a small business named "ABC Store" registered in Taipei City, while there might be another "ABC Store" registered in Taoyuan County.
- Therefore, the suitable subject DN for these two small businesses will be “
  - C=TW, L=Taipei City, O=ABC Store" and “
  - C=TW, L=Taoyuan County, O=ABC Store" respectively.

it is not suitable to enforce the CA to insert L or ST into the subject DN

- We believe that there are also some other small countries where stateOrProvinceName is not available and where companies is registered in the country level.
- In such situations, we do not think it is suitable to enforce the CA to insert locality(L) or stateOrProvinceName(ST) into the subject DN.

We suggest CAB Forum to relief the rule of subject DN (1/2)

- The current BR require that either locality(L) or stateOrProvinceName(ST) must appeared in the subject DN.
- However, take into account the situations for small countries, we would like to suggest CAB Forum to relief the rule of subject DN.

We suggest CAB Forum to relief the rule of subject DN (2/2)

- At least, the BR should allow the CA to not insert locality(L) or stateOrProvinceName(ST) into the subject DN if the organizationName is already unique at the country level.
  - The current BR rule of subject DN require countryName must be present if the organizationName is present.

About *Guidance on the Deprecation of Internal Server Names and Reserved IP Addresses v 1.0*

- Below URL in Guidance on the Deprecation of Internal Server Names and Reserved IP Addresses, June 2012, v 1.0 , (https://cabforum.org/wp-content/uploads/Guidance-Deprecated-Internal-Names.pdf) were disappeared:
  - http://www.iana.org/assignments/ipv4-addressspace/ipv4-address-space.xml
  - http://www.iana.org/assignments/ipv6-addressspace/ipv6-address-space.xml
- We suggest to use below URL to instead:
  - http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
  - http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

  Or
  - http://en.wikipedia.org/wiki/Reserved_IP_addresses#Reserved_IPv4_addresses


Value Creator for
Investors, Customers, Employees, and Society
Thank you!