Amend of SSL BR section 7.1.4.2.2 d & e

Statement of intent:

In SSL BR section 7.1.4.2.2 d & e, either localityName or stateOrProvinceName is required for OV and IV SSL Certificates. As CABF Bugzilla – Bug#2 https://bugzilla.cabforum.org/show_bug.cgi?id=2 , We amend section 7.1.4.2.2 d & e to solve below situations:

(1). For small countries/jurisdictions, if they do not set up any state or province.

Some CAs misplaced absence province or state name.

(2). The organizationName is already unique at the country level.

If the subject:organizationName and subject:countryName fields are present and the country/jurisdiction specified by the subject:countryName field has a centralized registry for that kind of organizations so that the organization name specified by the subject:organizationName field is "unique" in the entire country/jurisdiction. Those centralized registry databases are QGIS(Qualified Government Information Source,) or QTIS(Qualified Government Tax Information Source) , and government law keep the organizations' names are unique. [Note 1]

(3).In EU, "We found it is not suitable to enforce the CA to insert locality(L) or stateOrProvinceName(ST) into the subject DN in small country" remains still open as it is the same in other EU countries too. Please see https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx

a. ETSI EN 319 412-1 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

b. ETSI EN 319 412-3 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

C.319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations

The minimal set of Subject info for legal person in Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

4.2.1 Subject

The subject field shall include at least the following attributes as specified in Recommendation ITU-T X.520 [1]:

- countryName;
- organizationName;
- organizationIdentifier; and
- commonName.

(4) There will be the possibilities of Distinguished Name collisions for different entities following current BR.

Table: Proposed versions:

SSL BR V1.3.4	Proposed versions
7.1.4.2.2 Subject Distinguished Name Fields **d. 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: (a) the subject:organizationName and subject:stateOrProvinceName fields are present. **e. 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.	1. Dr. Ben Wilson of DigiCert's version 7.1.4.2.2 Subject Distinguished Name Fields **d.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: (a) the subject:organizationName and subject:stateOrProvinceName fields are present, or (b) if the country name provided under subsection g. is Taiwan (TW), Singapore (SG)[Note 2], etc.. **e.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: (a) subject:organizationName and subject:localityName fields are present, or (b) if the country name provided

	under subsection g. is Taiwan (TW), Singapore (SG), etc..
	2. Dr. Wen-Cheng Wang of Chunghwa Telecom's Version
	7.1.4.2.2 Subject Distinguished Name Fields **d. 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: (a) the subject:organizationName and subject:stateOrProvinceName fields are present, or (b) if the subject:organizationName and subject:countryName fields are present and the country/jurisdiction specified by the subject:countryName field has a centralized registry for that kind of organizations so that the organization name specified by the subject:organizationName field is "unique" in the entire country/jurisdiction. Normally, situation (b) may exist in small countries/jurisdictions such as Singapore (SG), Taiwan (TW), etc. **e. 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: (a) the subject:organizationName and subject:stateOrProvinceName fields are present, or (b) if the subject:organizationName and subject:countryName fields are present and the country/jurisdiction specified by the subject:countryName field has a centralized registry for that kind of organizations so that the organization name specified by the subject:organizationName field is "unique" in the entire country/jurisdiction. Normally, situation (b) may exist in small countries/jurisdictions such as Singapore (SG), Taiwan (TW), etc.

Some problems if we don't amend SSL BR and soultions:

1. For a Symantec OV SSL Certificate that I found in https://mv.vatican.va/3_EN/pages/MV_Home.html (with error message by browser for the FQDN in URL is not matched the Subject Alternative Name, *.catholica.va and catholica.va, in this SSL certificate)or you can see it in https://crt.sh/?q=98+ef+2b+4c+43+39+ae+04+3b+bd+55+08+59+b2+b7+b4+ee+76+cb+af

```
Its Subject DN is
commonName=*.catholica.va
organizationName=Department of Telecommunications
localityName=Vatican City
stateOrProvinceName=Vatican City State
countryName =VA

The subject DN should be
commonName=*.catholica.va
organizationName=Department of Telecommunications
```

countryName =VA

It is enough to identify the domain name owner in Vatican.

Note that from
http://www.upu.int/fileadmin/documentsFiles/activities/addressingUnit/vatEn.pdf given by Peter Brown of Amazon
The Vatican uses an address format identical to that of Italy, except the province abbreviation, which is not used in the Vatican.

2. A wildcard SSL certificate signed by GlobalSign at https://ebank.cotabank.com.tw/eBank/,

   Its Subject DN is

   CN = *.cotabank.com.tw
   O = COTA Commercial Bank
   OU = ITDs
   L = Taichung
   S = Taichung
   C = TW

   But there is No Taichung Province or Taichung State in Taiwan, only Taichung city in Taiwan.

   I also mail to Doug of GlobalSign for below example,
   Kaohsiung city is also a special municipality as Taichung city. For a wildcard SSL Certificate for a bank as in https://accessible.bok.com.tw/
   Its Subject DN is

   CN = *.bok.com.tw
   O = BANK OF KAOHSIUNG CO., LTD.
   OU = MIS Dept.
   L = Kaohsiung
   S = Taiwan
   C = TW

   The rule by GlobalSign vetting team is not the same as in cotabank in Taichung city for BANK OF KAOHSIUNG CO., LTD. in Kaohsiung city.

Please also see the Taichung City Government English webpages in http://eng.taichung.gov.tw/mp.aspx?mp=1 and Kaohsiung City Government English webpages in http://www.kcg.gov.tw/EN/Index.aspx

These two city governments called them “City” not province. They are special municipalities, it is no need to put S=Taiwan.

We think below DN should be suitable:

CN = *.cotabank.com.tw
O = COTA Commercial Bank
OU = ITDs
C = TW

CN = *.bok.com.tw
O = BANK OF KAOHSIUNG CO., LTD.
OU = MIS Dept.
C = TW

They can be simple and clear identify *.bok.com.tw’ and COTA Commercial Bank’s organization DNs follow our country’s law and x.520.

3. Another case is as https://www.ecover.com.tw/ issued by Comodo,

CN = www.ecover.com.tw
OU = GlobalTrustSSLPro
OU = Provided by Global Digital Inc.
OU = MIS Dept
O = SOUTH CHINA INSURANCE CO., LTD.
STREET = 5F,No.560,Sec. 4,Chung Hsiao E Rd.,Taipei,Taiwan
L = Taipei
S = Taiwan
PostalCode = 110
C = TW

As Taipei City is a Municipality, we should not put S=Taiwan. Also for its address, you can see other example such as http://www.tcc.gov.tw/en/cp.aspx?n=BBF5C83DDCCEE939 of Taipei City Council:

No.507, Sec. 4, Ren-ai Rd., Xinyi Dist., Taipei City 110, Taiwan (R.O.C.)

TEL:(02)2729-7708

Last Updated: 2016-05-16

No need to put Taiwan Province.

The DN follows the Taiwan's company act and current BR should be

CN = www.ecover.com.tw
OU = GlobalTrustSSLPro
OU = Provided by Global Digital Inc.
OU = MIS Dept
O = SOUTH CHINA INSURANCE CO., LTD.
STREET = 5F,No.560,Sec. 4,Chung Hsiao E Rd., Taipei City ,Taiwan
L = Taipei City
PostalCode = 110
C = TW

But it may misinterpretate SOUTH CHINA INSURANCE CO., LTD as registered in Taipei City. So we suggest to modify SSL BR and use below DN

CN = www.ecover.com.tw
OU = GlobalTrustSSLPro
OU = Provided by Global Digital Inc.
OU = MIS Dept
O = SOUTH CHINA INSURANCE CO., LTD.
STREET = 5F,No.560,Sec. 4,Chung Hsiao E Rd., Taipei City ,Taiwan
PostalCode = 110
C = TW

Because from Note1, according Taiwan's Company Act, the company name must be unique for the whole country. So we can omit the L = Taipei City. Also Taipei

City appears in the Street field.

4. On the other hand, in Taiwan, we have small businesses (such as stores, or as Business Entities as in EVGL) which is established and registered according to our Business Registration Act(http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=J0080004, See Article 28). 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.

   For example, there might be a small business named "ABC Store" registered in Taipei City, while there might be another "ABC Store" registered in NantouCounty.
   Therefore, the suitable subject DN for these two small businesses will be "
   CN=ABC Store's FQDN
   O=ABC Store
   L=Taipei City
   C=TW

   and
   CN=ABC Store's FQDN
   O=ABC Store
   L=Nantou County

   C=TW

   respectively.

5. In X.520 or within a CA, A CA has to let different entities to have different Distinguished Name, different serial numbers and different key pairs. It is fundamental. For IV SSL certificate or citizen certificates, we can add unique serial number in Subject Distinguished Names to two different entities have the same names. (Peter Brown of Amazon in the discussion said EV SSL certificates solve the problem, but don't forget that EV SSL Certificates will not be issued to individuals, only be issued to Private Organization, Government Entities, Business entities and non-profit international organizations.)

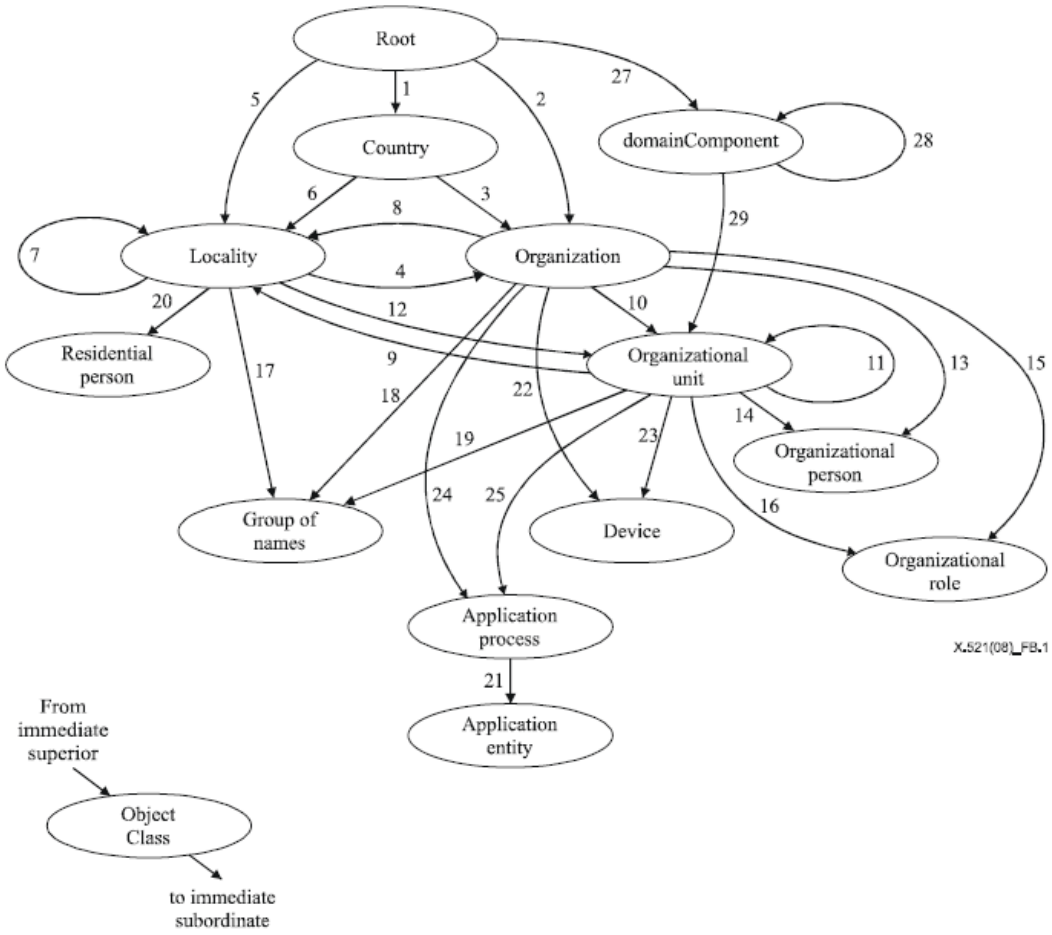
For OV SSL certificates, we have explained that there are some other small countries or jurisdictions where stateOrProvinceName is not available and where companies is registered in the country level.
In such situations, we do not think it is suitable to enforce the CA to insert locality(L) or stateOrProvinceName(ST) into the subject DN.

Peter tended to interpret the current BR that the localityName and stateOrProvinceName attributes as identifying the subject's address of existence or operation. However, to enforce this kind of interpretation and require the Subject DN must at least contain either the localityName and stateOrProvinceName attributes may cause problem in some situations as Dr. Wen-Cheng Wang's email before, especially in some small country where organizations are allowed to be registered at country-level.

For example, in Taiwan, a corporation can be registered at country-level but can also be register at city/county-level. If there is a country-level corporation named "Farmer's Association" of which physical address is located in Taipei City, with current Subject DN rule of BR, its Subject DN will be "C=TW, L=Taipei City, O=Farmer's Association". However, if there is also a city/county-level "Farmer's Association" in Taipei City, its Subject DN will also be "C=TW, L=Taipei City, O=Farmer's Association". How do you distinguish them by DN?

We do not understand why we need to enforce require the Subject DN must at least contain either the localityName and stateOrProvinceName attributes if the registered organizational name of a country-level corporation/organization is already guaranteed to be unique under the country name?

The following diagram is taken from Annex B of ITU-T X.521 (Suggested name form and Directory information tree structures). Please note path 1 -> 3, it suggests that there is no need to include a Locality attribute in the directory name of a country-level organization.



Several CAs have issued certificates with countryName = TW where other subject attributes are incorrectly set. That’s because those CA don’t not consider the real situation, so they try to fill some attributes to fill the state=Taiwan or even state=Taichung.

Other Q & A

1. In Bugzilla(CABF Bugzilla – Bug#2 https://bugzilla.cabforum.org/show_bug.cgi?id=2) , Dimitris Zacharopoulos suggested that

> There are some countries that have a centralized registry for commercial companies which means that company names are "unique" in the entire country.
>
> The BR could address this issue in Section 7.1.4.2.2d/e and provide an exception for these cases. However, the CA's qualified auditors should verify that there is a single company naming registry in the entire country which

forces uniqueness of company names. The Root programs could request a letter from the CA's auditors to verify this situation that would enable the exception.

Ans: I think the CA's qualified auditors will be glad to verify that there is a single company naming registry in the entire country which forces uniqueness of company names and offer the letter under request of Browser Root Certificate Program. Also I have showed the URL of Taiwan's company act. Taiwan's National Development Council asked Government PKI's qualified auditors to join the F2F Meeting 39 in Redmond. Li-Chun CHEN has helped David of KPMG, Taiwan to join. Below is website of Company Registration Database: http://gcis.nat.gov.tw/mainNew/classNAction.do?method=list&pkGcisClassN=4,website of Importer registration system:https://fbfh.trade.gov.tw/rich/text/indexfbOL.asp

2. In CA/B Forum meeting of July 7th, Kirk asked if a general rule can be written rather than writing up a list of specific countries. Ben said that had not been discussed.

Ans: What about discussion like the minimal set of Subject info for legal person in Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons? Or choose the edition from Ben or Wen-Cheng.

3. In certificate Policy working Group, Ben offer discussion records between Peter Brown and Li-Chun CHEN as https://www.mail-archive.com/public@cabforum.org/msg01333.html

Note that in RFC 3739 there are Qualified Certificates Profiles, In section 2.4. Uniqueness of names:

> Distinguished name is originally defined in X.501 [X.501] as a representation of a directory name, defined as a construct that identifies a particular object from among a set of all objects. The distinguished name MUST be unique for each subject entity certified by the one CA as defined by the issuer name field, for the whole life time of the CA.

For Taiwan's Government PKI, there is a certificate and CRL profile as

http://grca.nat.gov.tw/download/GPKI_Cert_and_CRL_Profiles_v2.0.pdf, we have this document around 14 years. Only that it is written in Tradition Chinese, not English. So we don't think there are some issues that Peter said, like "For end-entity certificates in the WebPKI, as implemented, there is no requirement that different entities have different Subject values."

4. Doug Beattie said in Validation Working Group : I still think it would be a good idea to enumerate the entire list of Country codes where both stateOrProvinceName and localityName can be omitted so there is no confusion and compliance can be monitored.
5.

Ans: I list all the Country Codes as in Note 2. But we have to consider it seems that some are not ISO 3166-1 code, some is ISO 3166-2 code. The original source is from **https://www.drupal.org/node/636464**, and I check by web sites such as Wikipedia, those government sites, https://en.wikipedia.org/wiki/ISO_3166and http://userpage.chemie.fu-berlin.de/diverse/doc/ISO_3166.html. We hope more volunteers provide comments and advices.

[Note 1]: In Taiwan, according our Company Act, the company name must be unique for the whole country. Furthermore, Taiwan's Company Act requires the company to register its business location which will be some city or county.

In http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=J0080001,

Company Act article 18 ,
No company may use a corporate name which is identical with that of another company. Where the corporate names of two companies contain any marks or identifying words respectively that may distinguish the different categories of business of the two companies, such corporate names shall not be considered identical with each other.

A company may conduct any business that is not prohibited or restricted by the laws and regulations, except for those requiring special approvals which shall be explicitly described in the Articles of Incorporation of the company.

Any category of business to be conducted by a company shall, when making the registration thereof, be identified with the Category Code applicable to the said business category as assigned in the Table of Categories of Businesses by the central competent authority. For a company which has already been registered, and the category of business conducted by it is registered with descriptive words, then, such descriptive words shall be replaced with the applicable Category Code as assigned in the foregoing Table, while applying for alteration of the entries of existing company registration record.

A company shall not use a name which tends to mislead the public to associate it with the name of a government agency or a public welfare organization, or has an implication of offending against public order or good customs.
Before proceeding to the company incorporation registration procedure, a company shall first apply for approval and reservation, for a specific period of time, of its corporate name and the scope of its business. Rules for examination and approval of such application shall be prescribed by the central competent authority.
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

This subject DN already uniquely identifies the company.

There is no necessary to add RDNs such as locality(L), or stateOrProvinceName(ST), Address (optional in BR) 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.

[Note 2]:

Table: Example of small countries/jurisdictions

	ISO 3166 country code
Bouvet Island	BV
British Virgin Islands	VG
Christmas Island	CX

Falkland Islands	FK
Faroe Islands	FO
French Guiana	GF
Gibraltar	GI
Guadeloupe	GP
Guam	GU
Guernsey	GG
Isle of Man	IM
Jersey	JE
Lebanon	LB
Macedonia	MK
Martinique	MQ
Mayotte	YT
Montenegro	ME
Netherlands Antilles	AN
Niue	NU
Norfolk Island	NF
Palestinian Territory	PS
Pitcairn	PN
Reunion	RE
Serbia	RS
Singapore	SG
Slovenia	SVN
South Georgia and the South Sandwich Islands	GS
Svalbard and Jan Mayen	SJ
Taiwan	TW
Vatican	VA
Western Sahara	EH