Li-Chun CHEN’s replying to Erwann Abalea
‘s mail (https://cabforum.org/pipermail/public/2016-July/007996.html)are in red or blue color as blow.

Bonsoir,

About small countries that haven’ t set up any state or province.

X.520 definition for the stateOrProvinceName attribute is (from 201210 edition):
The State or Province Name attribute type specifies a state or province. When used as a component of a directory name, it identifies a geographical subdivision in which the named object is physically located or with which it is associated in some other important way.

«Geographical subdivision » can mean anything. Maybe some would disagree, but I think that a CA can stretch it pretty easily while respecting the BRs.
If you want to follow the intent of the « province », since this latin-based word designates an administrative subdivision, it can even be a city or a village, and doesn’t necessarily mean a State in the US way. All the countries listed in Note 2 have cities.

=====> **I think X.520 clearly specifies that 'The State or Province Name attribute type specifies a state or province.' (This is the first sentence of the stateOrProvinceName definition in X.520.) Should CAB Forum encourage the ambiguity that CAs may put the name of administrative subdivision at any level (such as a city, a county, a town, or a village) into stateOrProvinceName attribute? No, I don't think so.**

About the uniqueness of an organizationName at a country level.

OV/IV certificates are not meant to unambiguously identify the subject named in the certificate. That role is left for EV certificates.

====> **I am really surprised to see the interpretation that 'OV/IV certificates are not meant to unambiguously identify the subject named in the certificate' in the CAB Forum. Is this a common cognition of the CAB Forum? The fundamental function of a public-key certificate is to assert the binding between the subject identity and its public key, isn't it? The value of a CA in the internet community**

is to act as a Trusted Third Party (TTP) which is responsible to verify the identity of the subject and then guarantee the binding between the subject identity and its public key. I think that OV/IV certificates still need to unambiguously identify the subject named in the certificate. The difference between OV/IV certificates and EV certificates is that they provide different level of assurance regarding the identity information verified. I understand that there does not exist a global X.500 directory. However, A CA should still make its best to unambiguously identify the subject named in the OV/IV certificate. At least, the CA should guarantee that two different entities never share the same subject DN, otherwise how the relying parties can distinguish which organization/individual is actually behind the OV/IV certificate?

I have replied in previous email to Peter in https://cabforum.org/pipermail/public/2016-June/007897.html as below

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. (You 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

Note that in https://cabforum.org/pipermail/public/2016-July/007912.html, I have replied to Peter in RFC 3739 there are Qualified Certificates Profiles.
I suggest you to read

3.1.2. Subject

The serialNumber attribute type SHALL, when present, be used to differentiate between names where the subject field would otherwise be identical. This attribute has no defined semantics beyond ensuring uniqueness of subject names. It MAY contain a number or code assigned by the CA or an identifier assigned by a government or civil authority. It is the CA's responsibility to ensure that the serialNumber is sufficient to resolve any subject name collisions.

So for Taiwan’s GPKI, we can resolve any subject name collisions for government entities’ SSL certificates or citizen certificates more than 13 years.

For example, in an IV certificate, there can be more than one individuals named John Malkovich, living in the same country, same province, same city. Only one of them will obviously be able to have thejohnmalkoti.ch domain, if it exists (it doesn’t).

Talking about OV certificates, even if it’s not possible to have 2 companies with the same name in the same jurisdiction, it’s possible to have 2 certificates having the same name representing 2 different entities. For example «C=UT, ST=MyVillage, O=XXXX», if XXXX is both a company and a brand (DBA).

Combine OV and IV, and «C=UT, ST=MyVillage, O=XXXX» can represent 3 different things, if XXXX is also the full name of an individual and the CA chooses to place this full name in the O field instead of GN/SN. (for a country named Utopia)

The rule for an OV/IV is something like « if you can provide evidence of the claimed identity, it’s good».

Again, if you want to disambiguate claimed identities, you’re free to add other attributes, or provide an EV certificate.

I don’t support the proposed BR changes, they only add complexity without any real benefit.

Looking at the example certificates:

- certificate 1 is not problematic; if you want a less cluttered certificate, go for a DV; wether VA is really a country or not is left as an exercise (it’s a territory for me, but I’m not so difficult)

===>VA is really a country, they don’t set up a government entity whose legal name is called Vatican City State or Vatican City Province,

but https://crt.sh/?q=98+ef+2b+4c+43+39+ae+04+3b+bd+55+08+59+b2+b7+b4+ee+76+cb+af

The 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.

- certificate 2 is not wrong per se; Taichung City being a geographical subdivision of Taiwan, an administrative division, and a city, it’ s not wrong to have Taichung in both the ST and L attributes — second example is « ST=Taiwan, L=Kaohsiung»; Taiwan being a province of the Taiwan country, and Kaohsiung being a city, it’ s not wrong

===>Taichung City and Kaohsiung City are 6 special municipalities (Traditional Chinese: 直轄市) or called Yuan-controlled municipalities (院轄市),theYuan is referred to the Executive Yuan. Special municipalities have the rank of province. For example, following the merger of Taichung city and county on December 25, 2010, Greater Taichung became third-largest among Taiwan's six special municipalities with a population of 2,720,000 people. Its land area is three times the size of Singapore and twice that of Hong Kong.

Note that Taiwan Province is a non-public corporation, the province has been frozen to prevent Yeltsin (Борис Николаевич Ельцин)effect. (Taiwan Province , often referred to simply freeze province, downsizing or waste Province, in AD 1997 Upgrading the provisions of the Fourth Constitutional provisions of paragraph 3 of Article IX, in 1988, the province was removed the "community" status, and the Taiwan provincial government degenerate reorganized as an agency of Executive Yuan.). So the organization (Taiwan Province) has been a substantial reduction, function shrinking dramatically.

Or you can see Local Government Act of Taiwan,http://www.moi.gov.tw/english/english_law/law_detail.aspx?sn=284

Article 2.The terms used in this Act are defined as follows:

1.Local self-governing body: Bodies of standing that carries out local self-government in accordance with this Act. The Provincial Government is a branch of the Executive Yuan, while the province is not a local self-governing body.

2.Self-government matters: Matters that the local self-governing bodies may formulate legislation and carry out in accordance with the Constitution or provisions of this Act, or to matters that are to be handled by such bodies in accordance with law and where such bodies are responsible for policy formulation and implementation.

For government entity's DN and OID, our government set up a site at oid.nat.gov.tw, it is UTF 8 code in Traditional Chinese. It is no need to put S=Taiwan in DN for entities under Taichung City and Kaohsiung City.

- I think certificate 3 is also fine; Taiwan Province is a province of the country Taiwan (just like Fujian Province is also such a province), and Taipei is a locality; wether the real name is Taipei or Taipei City is another remark

----No, the address of SOUTH CHINA INSURANCE CO., LTD is in Taipei city (The first special municipality in Taiwan). 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 of previous attached file, 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.
Our government has followed our country's law to setup the government entities' DIT, Distinguished Name, OID. For unambiguously identifying the difference of Chiayi City and Chiayi county, we suggest to use L=Chiayi City and L=Chiayi county. That is why we suggest to use L=Taipei City in previous email for the example certificate.

You' re explaining your proposals by using «no need to put (some information) », or «registered in (somewhere)», but it' s not relevant here. The fact that a company is registered in a city shouldn' t prevent the CA from setting the postalCode or streetAddress attributes (it' s not wrong to set these attributes). And if you want to unambiguously identify the company « ABC Store» registered in Nantou County from the «ABC Store» registered in Taipei City, again, use an EV, that' s what they' re here for. This can raise some legitimate questions and necessary clarifications about the real content and hierarchy of jurisdiction*Name attributes, and it' s OK.

=====>I did not say if a store registered in a city, we should omit the postal code or address attribute. (But it is optional in current BR). Example 4 is just said in Taiwan, a store' s situation is different with a company. So there will be a "L" .

And forget about X.521, we' re not using it here, there' s no DIT, no object classes. We' re using X.509 certificates outside of the Big X.500 Directory, and not as an attribute of this Directory (it can be both).

===>In our cps, such as Public CA, we said

3.1.1 Types of Names

The PublicCA uses the X.500 Distinguished Name (DN) for the certificate subject name of issued certificates.

3.1.4 Rules for Interpreting Name Forms
The rules for interpreting name forms follow ITU-T X.520 name attribute definition.

As for the diagram taken from Annex B of ITU-T X.521, that is for discussion with Peter about two methods to interpret DN, then Peter's interpretation will let two different entities have the same Distinguished Name. And there is no similar diagram in X.520.

Cordialement,
Erwann Abalea

Li-Chun CHEN
Deputy Senior Engineer
CISSP, CISA, CISM, PMP,
Information & Communication Security Dept.
Data Communication Business Group
Chunghwa Telecom Co. Ltd.
realsky@cht.com.tw
+886-2-2344-4820#4025