Issue of EVGL Section 9.25 subject:jurisdictionLocalityName、subject:jurisdictionStateOrProvinceName、subject:jurisdictionCountryName and X.520 & RFC 5280.

1. In EVGL v.1.5.8

### 9.2.5 Subject Jurisdiction of Incorporation or Registration Field

**Certificate fields:**

Locality (if required):

*subject:jurisdictionLocalityName* (OID: 1.3.6.1.4.1.311.60.2.1.1)

ASN.1 - X520LocalityName as specified in RFC 5280

State or province (if required):

 *subject:jurisdictionStateOrProvinceName* (OID: 1.3.6.1.4.1.311.60.2.1.2)

ASN.1 - X520StateOrProvinceName as specified in RFC 5280

Country:

 *subject:jurisdictionCountryName* (OID: 1.3.6.1.4.1.311.60.2.1.3)

ASN.1 – *X520countryName* as specified in RFC 5280

**Required/Optional:** Required

**Contents**: These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject’s Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

2. For RFC 5280 PKIX Certificate and CRL Profile (https://www.ietf.org/rfc/rfc5280.txt)，page 112,

-- Naming attributes of type X520LocalityName

id-at-localityName AttributeType ::= { id-at 7 }

-- Naming attributes of type X520LocalityName:

-- X520LocalityName ::= DirectoryName (SIZE (1..ub-locality-name))

--

-- Expanded to avoid parameterized type:

X520LocalityName ::= CHOICE {

 teletexString TeletexString (SIZE (1..ub-locality-name)),

 printableString PrintableString (SIZE (1..ub-locality-name)),

 universalString UniversalString (SIZE (1..ub-locality-name)),

 utf8String UTF8String (SIZE (1..ub-locality-name)),

 bmpString BMPString (SIZE (1..ub-locality-name)) }

-- Naming attributes of type X520StateOrProvinceName

id-at-stateOrProvinceName AttributeType ::= { id-at 8 }

-- Naming attributes of type X520StateOrProvinceName:

-- X520StateOrProvinceName ::= DirectoryName (SIZE (1..ub-state-name))

--

-- Expanded to avoid parameterized type:

X520StateOrProvinceName ::= CHOICE {

 teletexString TeletexString (SIZE (1..ub-state-name)),

 printableString PrintableString (SIZE (1..ub-state-name)),

 universalString UniversalString (SIZE (1..ub-state-name)),

 utf8String UTF8String (SIZE (1..ub-state-name)),

 bmpString BMPString (SIZE (1..ub-state-name)) }

3. In RFC 5280 Page 114,

-- Naming attributes of type X520countryName (digraph from IS 3166)

id-at-countryName AttributeType ::= { id-at 6 }

X520countryName ::= PrintableString (SIZE (2))

4. Note that in RFC 5280 page 111,

-- Arc for standard naming attributes

id-at OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 4 }

So these OID of Locality, StateOrProvinceName, countryName in EVGL section 9.2.5. should be 2.5.4.7, 2.5.4.8 and 2.5.4.6, respectively.

In X.520 as attached file or RFC 5280(<https://tools.ietf.org/html/rfc5280>), There are no jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2), jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3). You can use search function to search attached PDF file.

These three OIDs are registered by Microsoft. Please see below three URL:

(a). <http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.60.2.1.1.html>,

# 1.3.6.1.4.1.311.60.2.1.1 - Locality

Submitted by from host (85.157.59.86) on Sat Oct 18 23:23:02 CEST 2014 using a WWW entry form.

**OID value:** 1.3.6.1.4.1.311.60.2.1.1

**OID description:**

**URL for further info:** <https://www.mozilla.org/projects/security/certs/ev/guidelines-draft-20.doc>

See also the [OID Repository website reference](http://www.oid-info.com/get/1.3.6.1.4.1.311.60.2.1.1) for 1.3.6.1.4.1.311.60.2.1.1

## Superior references

* [1.3.6.1.4.1.311](http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.html) - Microsoft
* [1.3.6.1.4.1](http://www.alvestrand.no/objectid/1.3.6.1.4.1.html) - IANA-registered Private Enterprises
* [1.3.6.1.4](http://www.alvestrand.no/objectid/1.3.6.1.4.html) - Internet Private
* [1.3.6.1](http://www.alvestrand.no/objectid/1.3.6.1.html) - OID assignments from 1.3.6.1 - Internet
* [1.3.6](http://www.alvestrand.no/objectid/1.3.6.html) - US Department of Defense
* [1.3](http://www.alvestrand.no/objectid/1.3.html) - ISO Identified Organization
* [1](http://www.alvestrand.no/objectid/1.html) - ISO assigned OIDs
* [Top of OID tree](http://www.alvestrand.no/objectid/top.html)

(b). <http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.60.2.1.2.html>

# 1.3.6.1.4.1.311.60.2.1.2 - State or province

Submitted by from host (85.157.59.86) on Sat Oct 18 23:22:46 CEST 2014 using a WWW entry form.

**OID value:** 1.3.6.1.4.1.311.60.2.1.2

**OID description:**

**URL for further info:** <https://www.mozilla.org/projects/security/certs/ev/guidelines-draft-20.doc>

See also the [OID Repository website reference](http://www.oid-info.com/get/1.3.6.1.4.1.311.60.2.1.2) for 1.3.6.1.4.1.311.60.2.1.2

## Superior references

* [1.3.6.1.4.1.311](http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.html) - Microsoft
* [1.3.6.1.4.1](http://www.alvestrand.no/objectid/1.3.6.1.4.1.html) - IANA-registered Private Enterprises
* [1.3.6.1.4](http://www.alvestrand.no/objectid/1.3.6.1.4.html) - Internet Private
* [1.3.6.1](http://www.alvestrand.no/objectid/1.3.6.1.html) - OID assignments from 1.3.6.1 - Internet
* [1.3.6](http://www.alvestrand.no/objectid/1.3.6.html) - US Department of Defense
* [1.3](http://www.alvestrand.no/objectid/1.3.html) - ISO Identified Organization
* [1](http://www.alvestrand.no/objectid/1.html) - ISO assigned OIDs
* [Top of OID tree](http://www.alvestrand.no/objectid/top.html)

(c) <http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.60.2.1.3.html>

# 1.3.6.1.4.1.311.60.2.1.3 - Country

Submitted by from host (85.157.59.86) on Sat Oct 18 23:24:03 CEST 2014 using a WWW entry form.

**OID value:** 1.3.6.1.4.1.311.60.2.1.3

**OID description:**
subject:jurisdictionOfIncorporationCountryName ASN.1 - X520countryName as specified in RFC 3280

**URL for further info:** <https://www.mozilla.org/projects/security/certs/ev/guidelines-draft-20.doc>

See also the [OID Repository website reference](http://www.oid-info.com/get/1.3.6.1.4.1.311.60.2.1.3) for 1.3.6.1.4.1.311.60.2.1.3

## Superior references

* [1.3.6.1.4.1.311](http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.html) - Microsoft
* [1.3.6.1.4.1](http://www.alvestrand.no/objectid/1.3.6.1.4.1.html) - IANA-registered Private Enterprises
* [1.3.6.1.4](http://www.alvestrand.no/objectid/1.3.6.1.4.html) - Internet Private
* [1.3.6.1](http://www.alvestrand.no/objectid/1.3.6.1.html) - OID assignments from 1.3.6.1 - Internet
* [1.3.6](http://www.alvestrand.no/objectid/1.3.6.html) - US Department of Defense
* [1.3](http://www.alvestrand.no/objectid/1.3.html) - ISO Identified Organization
* [1](http://www.alvestrand.no/objectid/1.html) - ISO assigned OIDs
* [Top of OID tree](http://www.alvestrand.no/objectid/top.html)

To solve above EV Guideline section 9.2.5 using the proprietary Microsoft OIDs that don’t appear in X.520 and RFC 5280 to represent the level of the Incorporating Agency or Registration Agency, let's collect CAs' and Browsers' opinions. For Chunghwa Telecom Co. Ltd found the issue, we are glad to modify our CPS and EV SSL certificates profiles and programs after a ballot set up an effective date may be after half a year for CA/Browser to follow. Erwann Abalea has offered several ways to fix the issue in https://cabforum.org/pipermail/public/2016-June/007893.html and another replying mail that I did not found in June or July archive of <https://cabforum.org/pipermail/public/>, but I did received it in my client e-mail software.

Take [github.com](http://github.com)'s certificate as example:

businessCategory=Private Organization, jurisdictionC=US, jurisdictionST=Delaware, serialNumber=5157550, street=88 Colin P Kelly, Jr Street, postalCode=94107,

|  |  |  |
| --- | --- | --- |
| Methods | Explanation | Comments |
| No.1  | Replacement of the jurisdiction\*Name OIDs by some allocated under CAB/F's arc (e.g. change 1.3.6.1.4.1.311.60.2.1.{1,2,3} into 2.23.140.2.{1,2,3}) | 1. If you just want to change the OIDs behind jurisdiction{C,ST,L}, it will have minimal impact on the human-readable subject name (jurisdiction\* names will have to change with the OIDs).
 |
| No.2 | Narrow down the presence and content of existing C/ST/L to match what is wanted by EV | 1. This example subject name would have to change to:

businessCategory=Private Organization, serialNumber=5157550, C=US, ST=Delaware, O=GitHub, Inc., CN=[github.com](http://github.com) |
| No.3  | Erwann Abalea hasn’t seen an authoritative definition of these 3 attributes, but always considered them the way Peter described them.Maybe Microsoft should propose a clear definition, using the syntax from RFC5912, something like this:id-MS-jurisdictionLocalityName OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 311 60 2 1 1 }id-MS-jurisdictionStateOrProvinceName OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 311 60 2 1 2 }id-MS-jurisdictionCountryName OBJECT IDENTIFIER ::= { 1 3 6 1 4 1 311 60 2 1 3 }at-jurisdictionCountryName ATTRIBUTE ::= {TYPE PrintableString (SIZE (2))IDENTIFIED BY id-MS-jurisdictionCountryName}at-jurisdictionStateOrProvinceName ATTRIBUTE ::= {TYPE DirectoryString {ub-state-name}IDENTIFIED BY id-MS-jurisdictionStateOrProvinceName}at-jurisdictionLocalityName ATTRIBUTE ::= {TYPE DirectoryString {ub-locality-name}IDENTIFIED BY id-MS-jurisdictionLocalityName}DirectoryString is also redefined in RFC5912 to have a size constraint. |  |

Other Discussion:

**From:** public-bounces@cabforum.org [mailto:public-bounces@cabforum.org] **On Behalf Of** Ryan Sleevi
**Sent:** Friday, July 15, 2016 6:44 AM
**To:** Moudrick M. Dadashov
**Cc:** CABFPub
**Subject:** Re: [cabfpub] EV Gudelines section 9.2.5 & X.520

Not really.

On Thu, Jul 14, 2016 at 3:24 PM, Moudrick M. Dadashov <md@ssc.lt> wrote:

Thanks, Ryan, in that case Section 3.2.6.1.(Predefined Statements) of RFC 3739 would be more relevant.

ETSI implementation here: ETSI EN 319 412-1, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

Thanks,

M.D.

On 7/13/2016 11:13 PM, Ryan Sleevi wrote:

Moudrick,

As the subject indicates, this is about naming OIDs, not policy OIDs - that is, the format and structure of name forms. So no, they don't represent policy OIDs, which do come from the CA/B Forum arc already.

On Wed, Jul 13, 2016 at 11:37 AM, Moudrick M. Dadashov <md@ssc.lt> wrote:

On 7/13/2016 8:33 PM, Ryan Sleevi wrote:

On Wed, Jul 13, 2016 at 10:26 AM, Rich Smith <richard.smith@comodo.com> wrote:

I don't have any concrete objection to these OIDs being maintained under Microsoft's hierarchy, however as memory serves they were put there because at the time the CA/B Forum did not have an OID hierarchy of our own under which to create them.  Personally I think it would be a good idea to duplicate these OIDs in house at this point, and over time deprecate the use of the ones under the Microsoft structure.  I don't think this is a pressing issue, and probably not even strictly necessary, but I do see it as a matter of good 'house-keeping'.  If they're under CA/B Forum control we don't need to ask someone else to define them, and we don't have to accept their definition if it's one we don't necessarily agree with.

I'm not sure I understand these last points, practically speaking.

Why is it a matter of good-housekeeping? The counter-argument is it sounds like NIH-syndrome.

Why do we need to ask someone to define them, considering they're defined already? Why do we need to worry about accepting the definition, considering it's already been accepted?

I'm explicitly opposed to the change as argued because it means needless churn and complexity in software. If this were a fresh start, I would be understanding - but even then, I'd be opposed to putting it under a CA/B Forum arc 'simply because', if an alternative presented itself. For example, if a member/vendor in possession of a small OID arc were willing to 'donate' OIDs for future purposes that were smaller, in their encoded form, then the OID arc of the CA/B Forum (presently, 2.23.140, so I mean, it's unlikely but possible), then great - let's do that instead.

I'm also not opposed to moving to a CA/B Forum set of OIDs if there were other compelling reasons to. But so far, it seems to solely be about 'branding' than any concrete technical need. Am I missing something?

Maybe not just "branding" :)

Consider OIDs  specifically representing CA/B Forum policy provisions, I mean similar to those in RFC 3739.

Thanks,

M.D.