Potential change to browser UI for Subject DN of an EV SSL Certificate

Chunghwa Telecom Co., Ltd.
Li-Chun CHEN,
Deputy Senior Engineer, CISSP, CISM, CISA, PMP
realsky@cht.com.tw

CA/Browser Forum Meeting 39
Redmond , Host: Microsoft
October, 20 , 2016
Two Topics in the session

- **Topic 1**: Potential change to browser UI for Subject DN of EV SSL Certificate

- **Topic 2**: Discussion of Amendment of EVGL 9.2.5 about 3 OIDs
Could the UI become:

- **CN**: github.com
- **O**: GitHub, Inc.
- **L**: San Francisco
- **S**: California
- **C**: US
- **PostalCode**: 94107
- **STREET**: 88 Colin P Kelly, Jr Street
- **SERIALNUMBER**: 5157550
- **Jurisdiction of Incorporation State or Province**: Delaware
- **Jurisdiction of Incorporation Country**: US
- **Business Category**: Private
EV SSL Certificate Detailed Information of Subject DN view in Firefox/Windows 7

Could the UI become:
CN = github.com
O = GitHub, Inc.
L = San Francisco
S = California
C = US
PostalCode = 94107
STREET = 88 Colin P Kelly, Jr Street
SERIALNUMBER = 5157550
Jurisdiction of Incorporation
State or Province = Delaware
Jurisdiction of Incorporation
Country = US
Business Category = Private
EV SSL Certificate Detailed Information of Subject DN view in IE /Windows 7

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid to</td>
<td>Wednesday, January 04, 201...</td>
</tr>
<tr>
<td>Subject</td>
<td><a href="http://www.mozilla.org">www.mozilla.org</a>, Mozilla Found...</td>
</tr>
<tr>
<td>Public key</td>
<td>RSA (2048 Bits)</td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>KeyID=3d d3 50 a5 d6 a0 a0 ...</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>83 d4 d4 of 35 a4 ba 8b be 61 ...</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>DNS Name=www.mozilla.org, ...</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Server Authentication (1.3.6...</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>11CRI Distribution Point= Dist</td>
</tr>
</tbody>
</table>

Could the UI become:
- CN = www.mozilla.org
- O = Mozilla Foundation
- L = Mountain View
- S = California
- C = US
- PostalCode = 94041
- STREET = 650 Castro St Ste 300
- SERIALNUMBER = C2543436

Jurisdiction of Incorporation
- State or Province = California
- Jurisdiction of Incorporation
- Country = US
- Business Category = Private Organization
Discussion 1

- The UI for Details of Subject information of an EV SSL certificate by Safari, Chrome in windows are the same as view in IE/Windows

- Could browsers parse the OIDS like 1.3.6.1.4.1.311.60.2.1.2 as meaningful string?

- It will greatly improve user experience to browse important sites installed by EV SSL certificates.

- Could the browser vendors' representatives help to ask the programming team if/when this request is met?
<table>
<thead>
<tr>
<th>OID</th>
<th>Proposed UI in details</th>
<th>Note</th>
</tr>
</thead>
</table>
| 1.3.6.1.4.1.311.60.2.1.1 | Option 1: Jurisdiction State or Province  
Option 2: Jurisdiction of Incorporation State or Province | EVGL 9.2.5 |
| 1.3.6.1.4.1.311.60.2.1.2 | Option 1: Jurisdiction State or Province  
Option 2: Jurisdiction of Incorporation State or Province | EVGL 9.2.5 |
| 1.3.6.1.4.1.311.60.2.1.3 | Option 1: Jurisdiction of Country  
Option 2: Jurisdiction of Incorporation Country | EVGL 9.2.5 |
| 2.5.4.15 | Business Category                                                                          | EVGL 9.2.4 |
| 2.5.4.17 | Postal Code                                                                                 | EVGL 9.2.7 |
Mozilla’s response

- Thanks for Gervase’s suggestion to file a bug for Mozilla:
  - This seems like a perfectly reasonable suggestion :-)
    As Mozilla is developed as open source, you should file a bug in our bug tracker here:
    [https://bugzilla.mozilla.org/enter_bug.cgi?product=Core&component=Security%3A%20PSM](https://bugzilla.mozilla.org/enter_bug.cgi?product=Core&component=Security%3A%20PSM) to suggest it.

- Li-Chun has filed a bug in
  [https://bugzilla.mozilla.org/show_bug.cgi?id=1308755](https://bugzilla.mozilla.org/show_bug.cgi?id=1308755)

- Gervase concluded: we are rewriting the part of Firefox which decodes certificates into JavaScript. Once that is done, the new implementation may well be able to support the changes you request.
Topic 2

Discussion of Amendment of EVGL
9.2.5 about 3 OIDs
Discussion 2-EV GL 9.2.5

- In EV GL, 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
1.3.6.1.4.1.311.60.2.1.1

OID description

<table>
<thead>
<tr>
<th>Description:</th>
<th>jurisdictionOfIncorporationLocalityName</th>
</tr>
</thead>
</table>

Short URL for this page: http://oid-info.com/get/1.3.6.1.4.1.311.60.2.1.1
 OID Repository

Home  Tree display  Search OID  FAQ

Display OID

- iso(1)  identified-organization(3)  dod(6)  internet(1)  private(4)  enterprise(1)  311  ev(60)  2  1

jurisdictionOfIncorporationStateOrProvinceName(2)

OID description

OID

1.3.6.1.4.1.311.60.2.1.2

jurisdictionOfIncorporationStateOrProvinceName(2)

Description

jurisdictionOfIncorporationStateOrProvinceName

Short URL for this page

http://oid-info.com/get/1.3.6.1.4.1.311.60.2.1.2

Disclaimer: The owner of this site does not warrant or assume any liability or responsibility for the accuracy, completeness, or usefulness of any information available on this page (for more information, please read the complete disclaimer).

All rights reserved, Orange © 2016

Webmaster  12 Jul 2012

Page top

下午 11:37
2016/10/8
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


See also the OID Repository website reference for 1.3.6.1.4.1.311.60.2.1.3

Superior references
- 1.3.6.1.4.1.311 - Microsoft
- 1.3.6.1.4.1 - IANA-registered Private Enterprises
- 1.3.6.1.4 - Internet Private
- 1.3.6.1 - OID assignments from 1.3.6.1 - Internet
- 1.3.6 - US Department of Defense
- 1.3 - ISO Identified Organization
- 1 - ISO assigned OIDs
- Top of OID tree

Search for text in all OIDs starting with 1.3.6.1.4.1.311.60.2.1.3:

Go to the top node if you need to search all entries.

Tell me about OIDs you know about
Incoming OIDs that have not been proofread yet

Entered: Sat Oct 18 23:24:03 CEST 2014 (not changed manually)
OID description

OID: 1.3.6.1.4.1.311.60.2.1.3

/ISO/Identified-Organization/6/1/4/1/311/60/2/1/3

Description: jurisdictionOfIncorporationCountryName

Short URL for this page: http://oid-info.com/get/1.3.6.1.4.1.311.60.2.1.3
X520Locality in RFC 5280

- For RFC 5280 PKIX Certificate and CRL Profile (https://www.ietf.org/rfc/rfc5280.txt), page 112,
- Naming attributes of type X520LocalityName

\[
\text{id-at-localityName \quad \text{AttributeType ::= \{ id-at 7 \}}}
\]

- Naming attributes of type X520LocalityName:
- \(X520\text{LocalityName ::= DirectoryName (SIZE (1..ub-locality-name))}\)

- Expanded to avoid parameterized type:

\[
X520\text{LocalityName ::= CHOICE \{ \\
\text{teletexString \quad TeletexString (SIZE (1..ub-locality-name)),} \\
\text{printableString \quad PrintableString (SIZE (1..ub-locality-name)),} \\
\text{universalString \quad UniversalString (SIZE (1..ub-locality-name)),} \\
\text{utf8String \quad UTF8String (SIZE (1..ub-locality-name)),} \\
\text{bmpString \quad BMPString (SIZE (1..ub-locality-name))} \}}
\]
X520StateOrProvinceName in RFC 5280

-- 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))
}
X520countryName in RFC 5280

- 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))
3 OIDs are not in RFC 5280 and X.520

- 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 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)
Ways to solve the issue

- 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 in June 2016, we are glad to modify our CPS and EV SSL certificates profiles and programs after a ballot set up an effective date.

- Erwann Abalea has offered several ways to fix the issue in https://cabforum.org/pipermail/public/2016-June/007893.html
Some response about change the OIDs and amend the EVGL(1/2)

- https://cabforum.org/pipermail/public/2016-July/007913.html, where Ryan Sleeve of Google wrote: “[I want to] indicate that we don't feel it would be appropriate or necessary to introduce new OID arcs for EV attributes, and would in fact be detrimental to the ecosystem. As such, unless new information is shared to further understand the objective, we'd vote no on any such ballot. “
Some response about change the OIDs and amend the EVGL(2/2)


Ryan,

My suggestion was based purely on the fact that any documented use of these OIDs is, to the best of my knowledge, only in CA/B Forum work product, so it seemed a good idea to me, now that we can, to transition them to actually being CA/B Forum OIDs. I don't have strong feelings on the matter, but I do think it makes things cleaner over the long haul, especially should we decide to add other related OIDs into future work product, to have them managed in house. But I do take your point as to it being a lot of technical changes, both on browser/relying party side and CA side for what, at least at this moment in time, has pretty much zero need or payback aside from the above mentioned possible future 'benefits'.

為了你 一直走在最前面 Always Ahead
Suggestion 1 by Erwann Abalea of DocuSign (1/2)

- I haven’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:

\[
\begin{align*}
\text{id-MS-jurisdictionLocalityName} & \text{ OBJECT IDENTIFIER ::= \{ 1 3 6 1 4 1 311 60 2 1 1 \}} \\
\text{id-MS-jurisdictionStateOrProvinceName} & \text{ OBJECT IDENTIFIER ::= \{ 1 3 6 1 4 1 311 60 2 1 2 \}} \\
\text{id-MS-jurisdictionCountryName} & \text{ OBJECT IDENTIFIER ::= \{ 1 3 6 1 4 1 311 60 2 1 3 \}}
\end{align*}
\]
Suggestion 1 by Erwann Abalea of DocuSign (2/2)

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.
Similar to Suggestion 1 by Peter Brown of Amazon (1/2)

- If we removed the lines with “X520” from section 9.2.5 of the EVGL and added the following,

```plaintext
id-evat OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) dod(6) internet(1)
private(4) enterprise(1) 311 60 2 1 }

id-evat-jurisdictionCountryName ATTRIBUTE ::= { id-evat 3 }
```

```plaintext
jurisdictionCountryName ATTRIBUTE ::= {
SUBTYPE OF name
WITH SYNTAX CountryName
SINGLE VALUE TRUE
LDAP-SYNTAX countryString.&id
LDAP-NAME {"jurisdictionC"}
ID id-evat-jurisdictionCountryName }
```
id-evat-jurisdictionStateOrProvinceName  

jurisdictionStateOrProvinceName ATTRIBUTE ::= { 
    SUBTYPE OF  name 
    WITH SYNTAX  DirectoryString {ub-state-name} 
    SINGLE VALUE  TRUE 
    LDAP-SYNTAX  directoryString.&id 
    LDAP-NAME  {"jurisdictionST"} 
    ID  id-evat-jurisdictionStateOrProvinceName } 

id-evat-jurisdictionLocalityName  

jurisdictionLocalityName ATTRIBUTE ::= { 
    SUBTYPE OF  name 
    WITH SYNTAX  DirectoryString {ub-locality-name} 
    SINGLE VALUE  TRUE 
    LDAP-SYNTAX  directoryString.&id 
    LDAP-NAME  {"jurisdictionL"} 
    ID  id-evat-jurisdictionLocalityName }
Suggestion 2

Use {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) extended-validation (1) jurisdictionLocalityName(1)}

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) extended-validation (1) jurisdictionStateOrProvinceName(2)}

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) extended-validation (1) jurisdictionCountryName(3)}

To replace 1.3.6.1.4.1.311.60.2.1.1, 1.3.6.1.4.1.311.60.2.1.2 and 1.3.6.1.4.1.311.60.2.1.3, respectively.

IF browsers agree to solve Topic 1, maybe browser s change the code when parsing Subject DN of an EV SSL certificate, they show 3 old proprietary Microsoft OIDs and CA/Browser Forum 3 new OIDs as meaningful string.
The CA/Browser Forum node is: - 2.23.140
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)}

<table>
<thead>
<tr>
<th>OID</th>
<th>Name</th>
<th>Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.23.140</td>
<td>ca-browser-forum</td>
<td>Node</td>
<td></td>
</tr>
<tr>
<td>2.23.140.1</td>
<td>certificate-policies</td>
<td>Node</td>
<td>CABF Policy node</td>
</tr>
<tr>
<td>2.23.140.1.1</td>
<td>extended-validation</td>
<td>Policy OID Value</td>
<td>The CABF EV Policy OID</td>
</tr>
<tr>
<td>2.23.140.1.2</td>
<td>baseline-requirements</td>
<td>Node</td>
<td>CABF Baseline Requirement Policy node</td>
</tr>
<tr>
<td>2.23.140.1.2.1</td>
<td>domain-validated</td>
<td>Policy OID Value</td>
<td>The CABF DV Policy OID</td>
</tr>
<tr>
<td>2.23.140.1.2.2</td>
<td>organization-validated</td>
<td>Policy OID Value</td>
<td>The CABF OV Policy OID</td>
</tr>
<tr>
<td>2.23.140.1.2.3</td>
<td>individual-validated</td>
<td>Policy OID Value</td>
<td>The CABF Individual Validated Policy OID</td>
</tr>
<tr>
<td>2.23.140.1.3</td>
<td>ev-code-signing</td>
<td>Policy OID Value</td>
<td>The CABF EV Code Signing Policy OID</td>
</tr>
<tr>
<td>2.23.140.1.31</td>
<td>cabf-TorServiceDescriptor</td>
<td>Policy OID Value</td>
<td>TorServiceDescriptor for onion EV Certificates</td>
</tr>
<tr>
<td>2.23.140.2</td>
<td>certificate-extensions</td>
<td>Node</td>
<td>CABF Certificate Extension node</td>
</tr>
<tr>
<td>2.23.140.2.1</td>
<td>test-certificate</td>
<td>Certificate OID Value</td>
<td>This extension will be marked critical in Test Certificates to render them invalid for browser use</td>
</tr>
</tbody>
</table>

https://www.cabforum.org/wiki/Object%20Registry
Thank you!

Welcome to 42th CA/B Forum F2F meeting host by Chunghwa Telecom Oct.3-5, 2017