SWITCH

The Swiss Education & Research Network

SWITCHpki SSL certificates vs. $15 low-cost certificates from LiteSSL, RapidSSL & Co.: why assurance matters

Kaspar Brand
SWITCH

What's a certificate, anyway?

SWITCH
The Swiss Education & Research Network

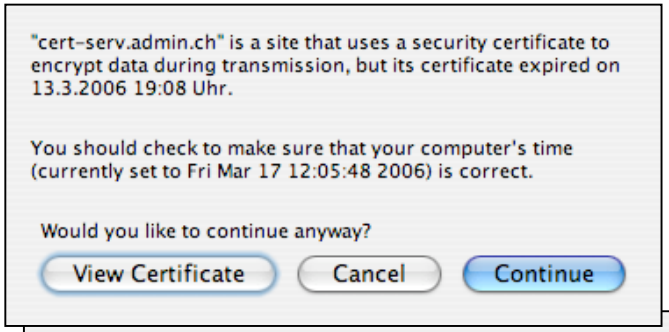
A small piece of some random and some not-so-random bits…

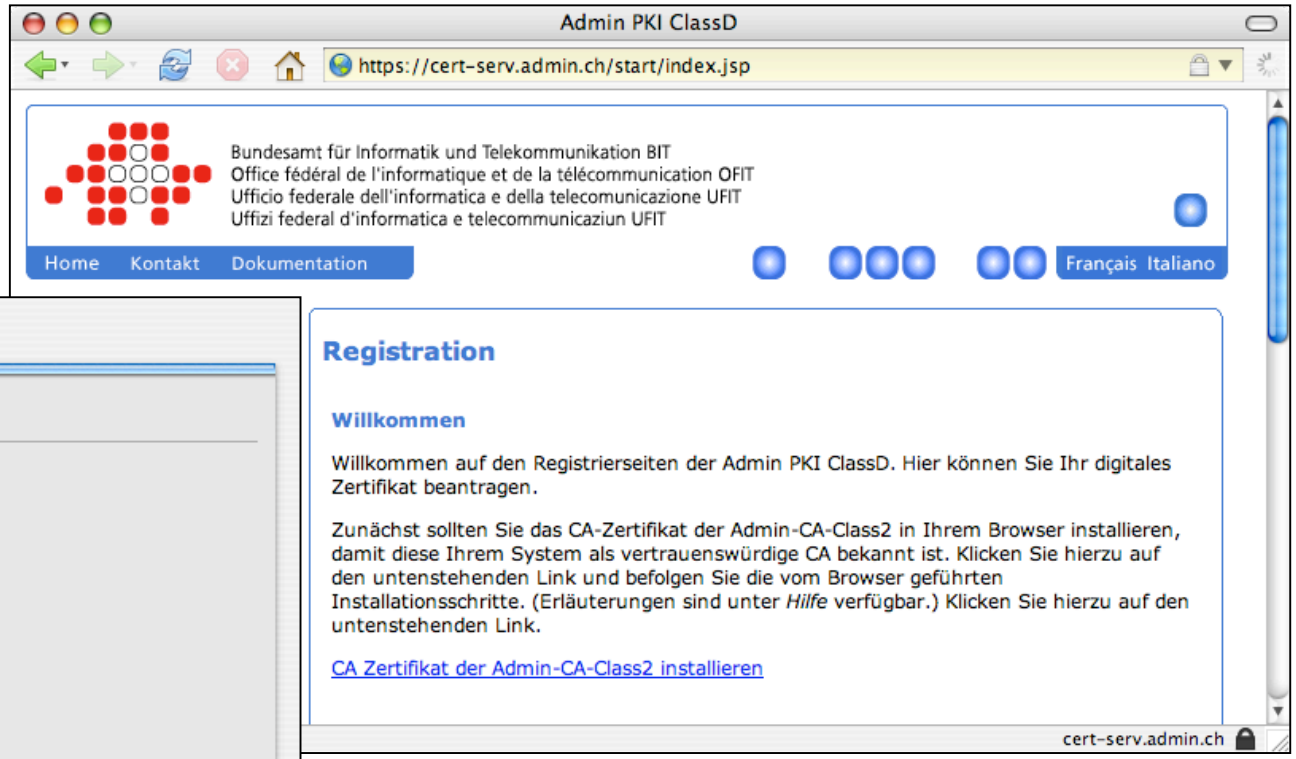
```
Data:
        Version: 3 (0x2)
        Serial Number: 2175887 (0x21338f)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town,
                O=Thawte Consulting cc, OU=Certification Services
                Division, CN=Thawte Premium Server CA/
                emailAddress=premium-server@thawte.com
        Validity
            Not Before: May 13 09:15:01 2005 GMT
            Not After : Jun 11 10:47:27 2007 GMT
        Subject: C=CH, ST=Bern, L=Bern,
                 O=Switch -  Teleinformatikdienste fuer Lehre
                 und Forschung, CN=nic.switch.ch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d0:0e:b7:16:bf:86:59:c3:97:e6:02:33:59:90:
                    65:29:b0:69:73:64:83:03:1b:df:62:a8:4d:c0:4f:
                    3c:d9:12:6b:8c:57:95:e1:57:e8:48:a6:7f:dd:15:
                    8b:9d:ad:93:dc:78:af:06:1a:ce:0f:7b:cc:c4:6f:
                    a0:06:26:40:73:04:d3:da:7b:20:c1:15:37:8c:2f:
                    58:c4:d4:c1:4b:18:84:5c:54:f1:b1:a0:44:3c:e2:
                    0e:8a:a2:63:48:6b:34:c7:10:9d:a1:23:56:77:f5:
                    4e:3d:38:9a:70:5e:03:02:30:45:ee:81:e4:94:96:
                    47:18:9e:47:37:bb:18:f6:87
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
                Authentication
            X509v3 CRL Distribution Points:
                URI:http://crl.thawte.com/ThawtePremiumServerCA.crl

            Authority Information Access:
                OCSP - URI:http://ocsp.thawte.com

            X509v3 Basic Constraints: critical
                CA:FALSE
        Signature Algorithm: md5WithRSAEncryption
            15:13:6c:20:ed:1b:85:cf:c1:07:94:5b:19:c3:57:4c:6f:86:
            7b:07:86:96:0f:21:8c:56:ee:74:b9:f0:51:e4:a1:8f:a3:89:
            d2:51:f1:fe:b4:e4:39:0c:48:8f:30:0c:bb:4d:33:46:eb:c7:
            4d:da:f7:e7:46:49:cb:5d:f7:26:0d:86:7d:7b:f4:2b:68:9d:
            8d:ab:51:f0:19:38:90:09:fb:d4:94:c4:9f:5b:b1:83:5c:98:
            18:71:30:13:e3:e3:b6:fd:a6:51:d6:e8:65:32:28:a3:80:e0:
            e8:9a:fb:5c:af:79:c1:fe:41:06:42:55:e8:a0:d8:78:26:3b:
            1d:9e
```

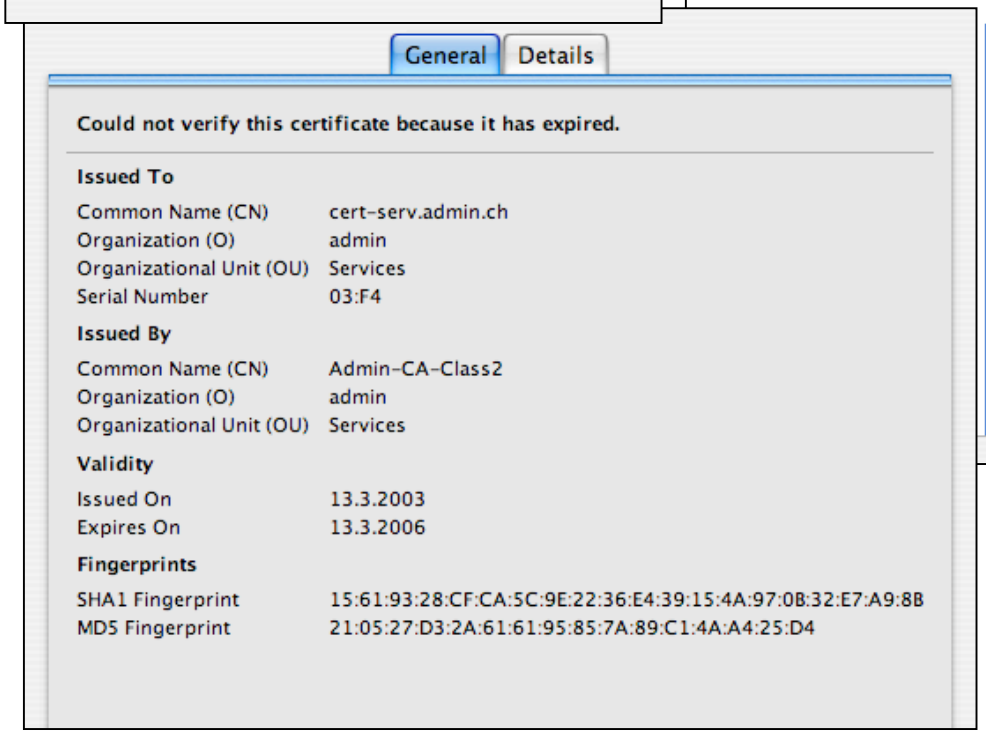
And what does a cert tell us, anyway?

SWITCH
The Swiss Education & Research Network

Recently, on the Net…



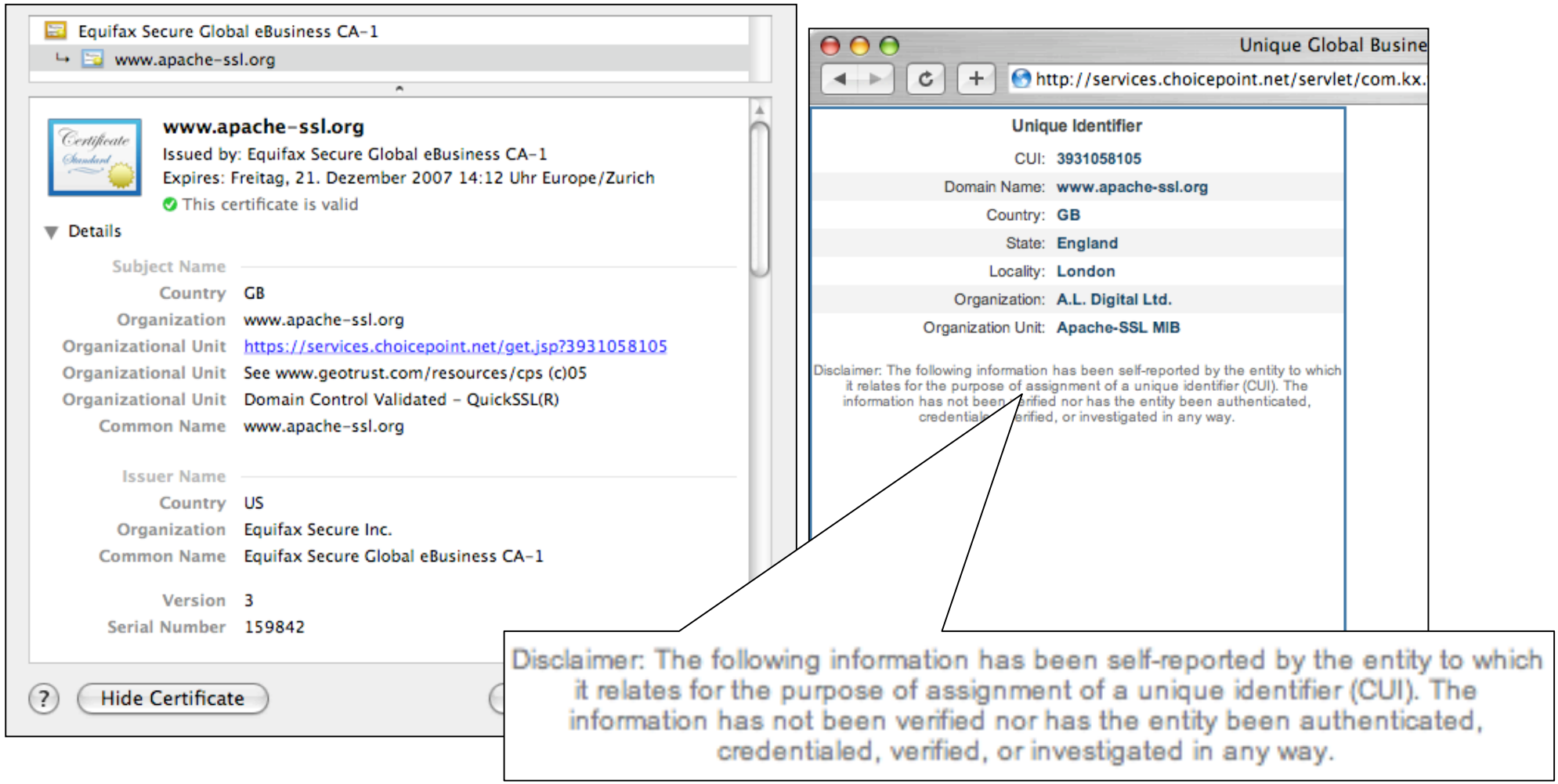




Are you sure this is really a federal authority…?

And what about this one?

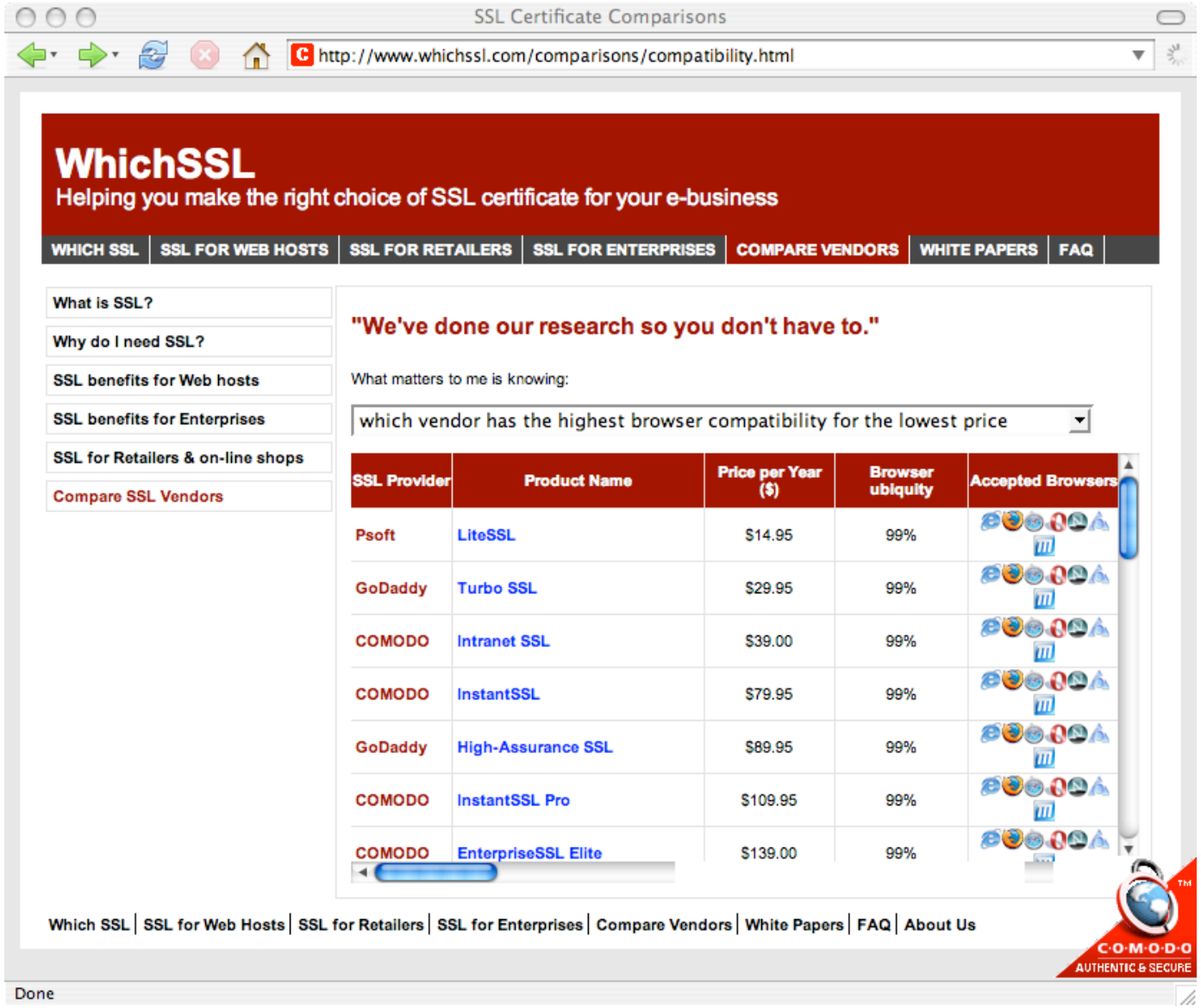
SWITCH
The Swiss Education & Research Network



… from the **No Liability Accepted for any damages whatsoever™** department (cf. the “Mountain America” case in February 2006)

Pricing shouldn't be the only concern

SWITCH
The Swiss Education & Research Network



Assurance matters…

SWITCH
The Swiss Education & Research Network

… because people connecting to your SSL server usually like to know whom they are dealing with

… because relying on DNS and Whois alone isn't enough:

```
$ whois digitalphishnet.org
[...]
Domain ID:D104521454-LROR
Domain Name:DIGITALPHISHNET.ORG
Created On:11-Jun-2004 17:42:30 UTC
Last Updated On:12-Jun-2005 01:34:11 UTC
Expiration Date:11-Jun-2006 17:42:30 UTC
Sponsoring Registrar:Schlund+Partner AG (R73-LROR)
Status:OK
Registrant ID:SPAG-33149303
Registrant Name:Domain Admin
Registrant Organization:Microsoft Corp
Registrant Street1:One Microsoft Way
Registrant Street2:
Registrant Street3:
Registrant City:Redmond
Registrant State/Province:WA
Registrant Postal Code:98052
Registrant Country:US
Registrant Phone:+212.5551212
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:digitalphishnet@mainlymail.com
[...]
```

Would you issue (and trust) a certificate for /C=US/O=Microsoft/CN=www.digitalphishnet.org based on this information?

SWITCHpki certificates

SWITCH
The Swiss Education & Research Network

Have a fully verified organizationName attribute ("**O=**") in their certificate subject:
O=Universitaet Bern
O=ETH Swiss Federal Institute of Technology Zurich
O=Switch - Teleinformatikdienste fuer Lehre und Forschung
O=Berner Fachhochschule - Haute ecole specialisee bernoise
O=Universitaet Zuerich
etc.

Are issued based on a certificate request which is approved by *you* – i.e. by those persons who are in the best position to verify whether a request is legimitate

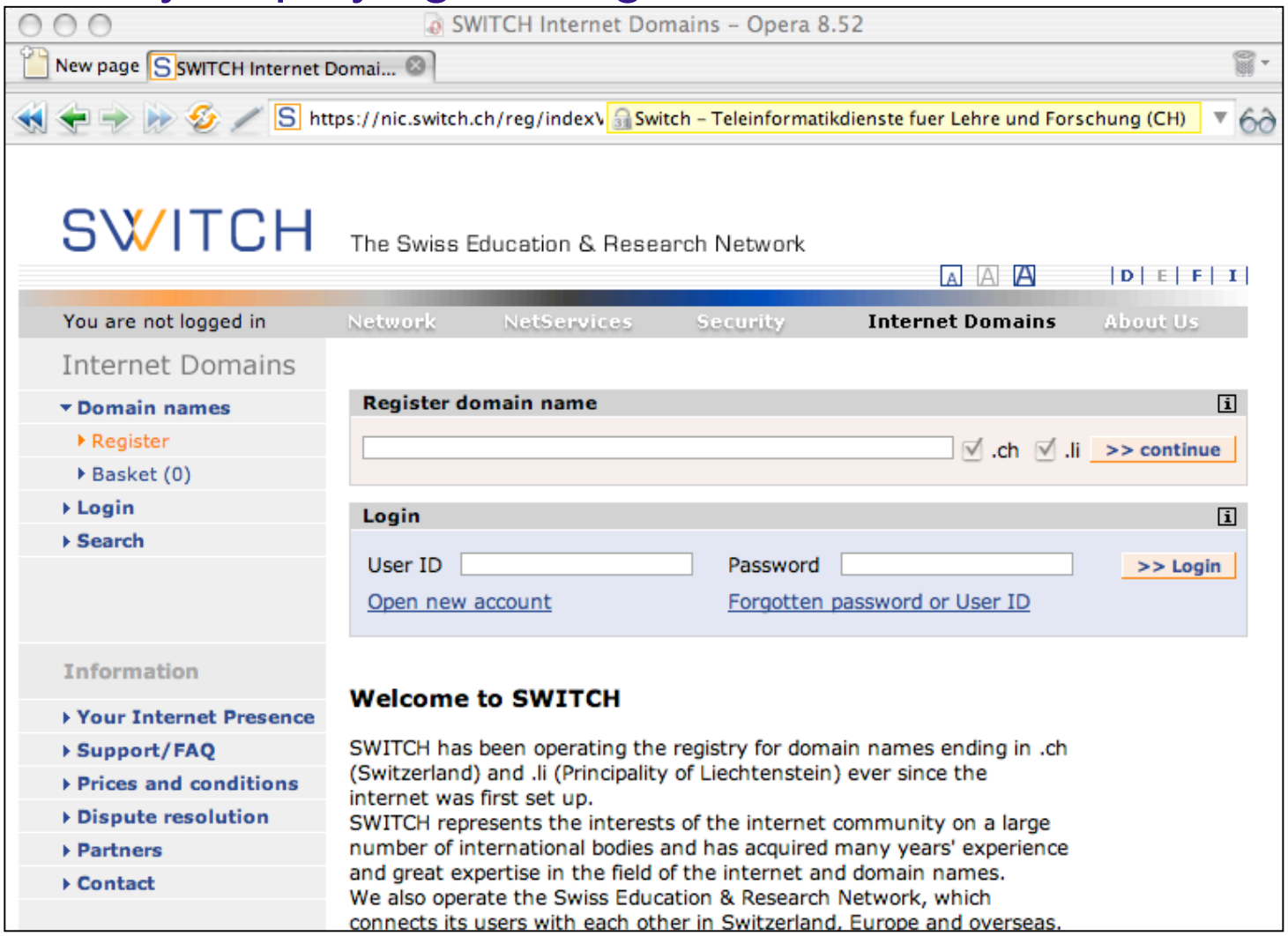
Rely on a hierarchical structure of registration authorities (RAs) located at each organization participating in SWITCHpki

Provide a distinctly higher level of assurance than domain validated certificates from low-end vendors at a very attractive price

A proper O= attribute is important

SWITCH
The Swiss Education & Research Network

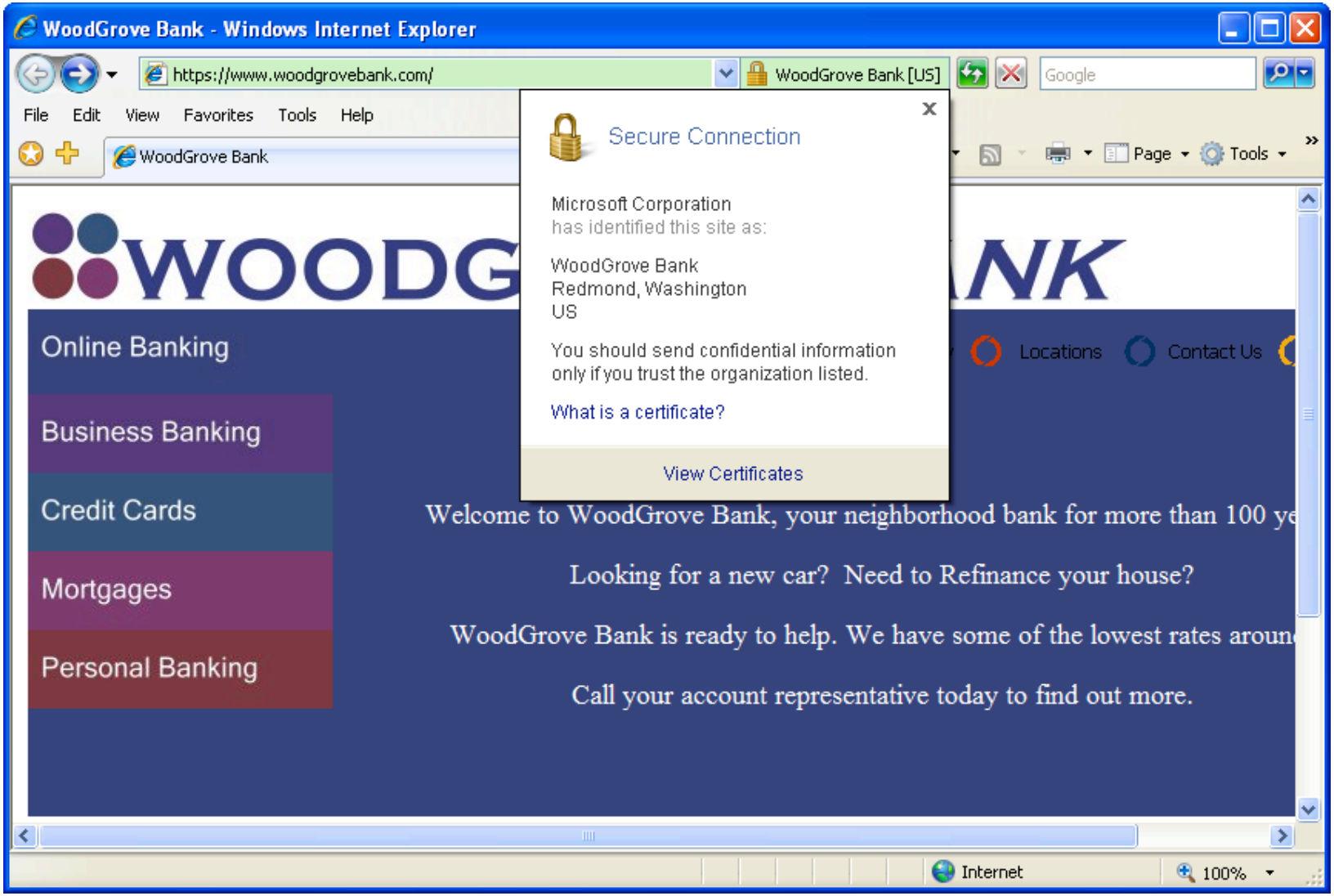
Opera is already displaying the organizationName attribute…



A proper O= attribute is important (cont.)

SWITCH
The Swiss Education & Research Network

… others will do so soon (IE 7 Beta 2 Preview, high-assurance cert)



The Swiss Education & Research Network