



# 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?

## 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?

## Recently, on the Net...

"cert-serv.admin.ch" is a site that uses a security certificate to encrypt data during transmission, but its certificate expired on 13.3.2006 19:08 Uhr.

You should check to make sure that your computer's time (currently set to Fri Mar 17 12:05:48 2006) is correct.

Would you like to continue anyway?

Admin PKI ClassD

https://cert-serv.admin.ch/start/index.jsp

Bundesamt für Informatik und Telekommunikation BIT  
Office fédéral de l'informatique et de la télécommunication OFIT  
Ufficio federale dell'informatica e della telecomunicazione UFIT  
Uffizi federal d'informatica e telecomunicaziun UFIT

Home Kontakt Dokumentation

Français Italiano

### Registration

#### Willkommen

Willkommen auf den Registrierseiten der Admin PKI ClassD. Hier können Sie Ihr digitales Zertifikat beantragen.

Zunächst sollten Sie das CA-Zertifikat der Admin-CA-Class2 in Ihrem Browser installieren, damit diese Ihrem System als vertrauenswürdige CA bekannt ist. Klicken Sie hierzu auf den untenstehenden Link und befolgen Sie die vom Browser geführten Installationsschritte. (Erläuterungen sind unter *Hilfe* verfügbar.) Klicken Sie hierzu auf den untenstehenden Link.

[CA Zertifikat der Admin-CA-Class2 installieren](#)

cert-serv.admin.ch

General Details

**Could not verify this certificate because it has expired.**

**Issued To**

Common Name (CN)	cert-serv.admin.ch
Organization (O)	admin
Organizational Unit (OU)	Services
Serial Number	03:F4

**Issued By**

Common Name (CN)	Admin-CA-Class2
Organization (O)	admin
Organizational Unit (OU)	Services

**Validity**

Issued On	13.3.2003
Expires On	13.3.2006

**Fingerprints**

SHA1 Fingerprint	15:61:93:28:CF:CA:5C:9E:22:36:E4:39:15:4A:97:0B:32:E7:A9:8B
MD5 Fingerprint	21:05:27:D3:2A:61:61:95:85:7A:89:C1:4A:A4:25:D4

Are you sure this is really a federal authority...?

# And what about this one?

The image shows two overlapping browser windows. The left window displays an SSL certificate for **www.apache-ssl.org** issued by Equifax Secure Global eBusiness CA-1. The right window shows the details of the Unique Identifier (CUI) for the domain, including the organization A.L. Digital Ltd. and a disclaimer.

**Equifax Secure Global eBusiness CA-1**  
www.apache-ssl.org

**www.apache-ssl.org**  
Issued by: Equifax Secure Global eBusiness CA-1  
Expires: Freitag, 21. Dezember 2007 14:12 Uhr Europe/Zurich  
This certificate is valid

**Details**

Subject Name  
Country: GB  
Organization: www.apache-ssl.org  
Organizational Unit: <https://services.choicepoint.net/get.jsp?3931058105>  
Organizational Unit: See www.geotrust.com/resources/cps (c)05  
Organizational Unit: Domain Control Validated - QuickSSL(R)  
Common Name: www.apache-ssl.org

Issuer Name  
Country: US  
Organization: Equifax Secure Inc.  
Common Name: Equifax Secure Global eBusiness CA-1

Version: 3  
Serial Number: 159842

**Unique Global Business**  
<http://services.choicepoint.net/servlet/com.kx.>

**Unique Identifier**  
CUI: 3931058105  
Domain Name: www.apache-ssl.org  
Country: GB  
State: England  
Locality: London  
Organization: A.L. Digital Ltd.  
Organization Unit: Apache-SSL MIB

Disclaimer: The following information has been self-reported by the entity to which it relates for the purpose of assignment of a unique identifier (CUI). The information has not been verified nor has the entity been authenticated, credentialed, verified, or investigated in any way.

Disclaimer: The following information has been self-reported by the entity to which it relates for the purpose of assignment of a unique identifier (CUI). The information has not been verified nor has the entity been authenticated, credentialed, verified, or investigated in any way.

... 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

**WhichSSL**  
Helping you make the right choice of SSL certificate for your e-business

WHICH SSL | SSL FOR WEB HOSTS | SSL FOR RETAILERS | SSL FOR ENTERPRISES | **COMPARE VENDORS** | WHITE PAPERS | FAQ

What is SSL?  
Why do I need SSL?  
SSL benefits for Web hosts  
SSL benefits for Enterprises  
SSL for Retailers & on-line shops  
Compare SSL Vendors

**"We've done our research so you don't have to."**

What matters to me is knowing:  
which vendor has the highest browser compatibility for the lowest price

SSL Provider	Product Name	Price per Year (\$)	Browser ubiquity	Accepted Browsers
Psoft	LiteSSL	\$14.95	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape
GoDaddy	Turbo SSL	\$29.95	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape
COMODO	Intranet SSL	\$39.00	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape
COMODO	InstantSSL	\$79.95	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape
GoDaddy	High-Assurance SSL	\$89.95	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape
COMODO	InstantSSL Pro	\$109.95	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape
COMODO	EnterpriseSSL Elite	\$139.00	99%	Internet Explorer, Firefox, Safari, Opera, Chrome, Netscape

Which SSL | SSL for Web Hosts | SSL for Retailers | SSL for Enterprises | Compare Vendors | White Papers | FAQ | About Us

COMODO AUTHENTIC & SECURE

Done

# Assurance matters...

... 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?**

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 legitimate

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

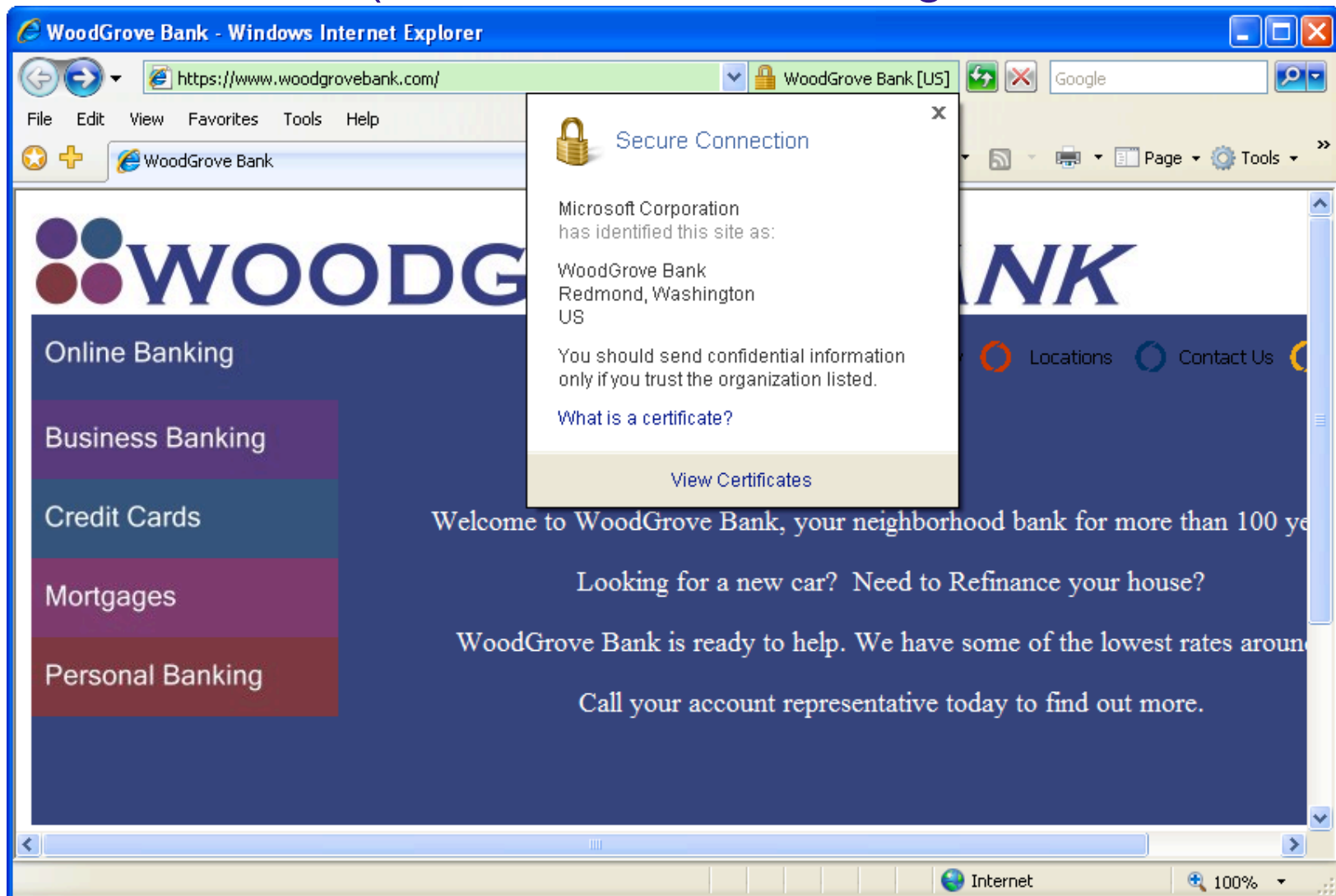
Opera is already displaying the organizationName attribute...





# A proper O= attribute is important (cont.)

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





# SWITCH

The Swiss Education & Research Network