SWITCH

The Swiss Education & Research Network

EV certificates: is it really *time to Go Green?*

Kaspar Brand <brand@switch.ch>

2nd SWITCHpki RAO Meeting

Berne, 18 April 2007

As seen on TV^H^Hthe Web, recently

SWITCH
The Swiss Education & Research Network

Available from several CAs, since December 2006

Officially introduced with the launch of Windows Vista (30 January 2007)

EV stands for **Extended Validation**

How EV came into existence

SWITCH
The Swiss Education & Research Network

In 2005, several CAs (Verisign, Geotrust, Cybertrust, Comodo et al.) created an informal club dubbed the **CA Forum,** with first public reports of its existence in December 2005

Later on, the club was joined by a couple of (browser) software vendors – and therefore renamed to **CA/Browser Forum**

24 member CAs as of April 2007:

Certum	**Entrust, Inc.**	**Network Solutions, LLC**	TDC Certification Authority
Comodo CA Ltd	**GeoTrust, Inc.**	**QuoVadis Ltd.**	**Thawte, Inc.**
Cybertrust	**GlobalSign**	RSA Security, Inc.	Trustis Limited
DigiCert, Inc.	**GoDaddy.com, Inc.**	**SecureTrust Corporation**	**VeriSign, Inc.**
DigiNotar	IdenTrust, Inc.	Starfield Technologies, Inc.	**Wells Fargo Bank, N.A.**
Echoworx Corporation	ipsCA, IPS Certification Authority s.l.	Swisscom Digital Certificate Service	**XRamp Security Services, Inc.**

[printed in **bold** = currently configured for EV certs in Microsoft Windows]

Plus 4 browser vendors: Microsoft, Mozilla, Opera, KDE

The EV SSL Guidelines – basic facts

SWITCH
The Swiss Education & Research Network

First version became public in October 2006:
"Version 1.0 - Draft 11"

No updates since then, but several CAs have updated their existing (or issued new) CP/CPSes in the meantime and are selling EV SSL certificates now

A 65-page document, currently

Of those 65 pages, 18 are about **"information verification requirements"** – this is the core of the guidelines

Limited to "server-authentication SSL/TLS on the Internet" for the time being (not applicable to user authentication, S/MIME, code signing etc. – *may be covered in future versions*)

The EV SSL Guidelines – things to note

SWITCH
The Swiss Education & Research Network

Will not be issued to *(1) General partnerships, (2) Unincorporated associations, (3) Sole proprietorships, (4) Individuals (natural persons)* – will also make it hard for universities, probably

May actually convey a false sense of trust to users, cf. section 2 (c):

Excluded Purposes. *EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is* ***not*** *intended to provide any assurances, or otherwise represent or warrant:*

(1) That the Subject named in the EV Certificate is actively engaged in doing business;

(2) That the Subject named in the EV Certificate complies with applicable laws;

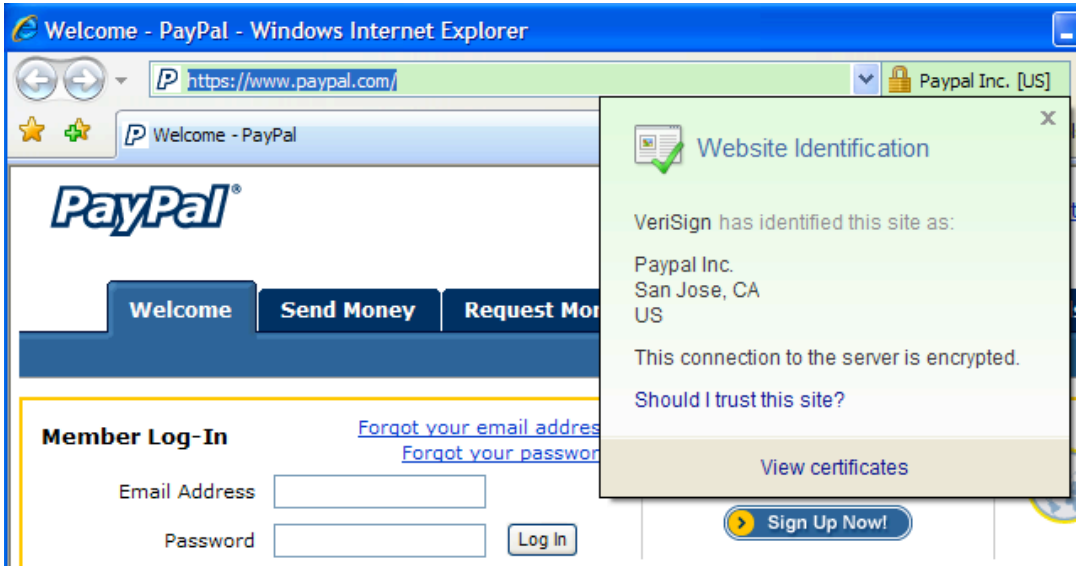
(3) That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or

(4) That it is "safe" to do business with the Subject named in the EV Certificate.

On the other hand, these guidelines include good ideas like setting detailed requirements for subject verification and technical properties (key lengths, extensions revocation management etc.)

Browser support

Limited to IE7 currently:



Firefox 3 is expected to have (some sort of) support for them, with its new location bar (cf. e.g. https://bugzilla.mozilla.org/show_bug.cgi?id=366797)

Not sure about the others:

- Opera: *There is a lot more that needs to be implemented before we can release a version with support for EV, but we will do so When It's Ready.* (http://labs.opera.com/news/2006/10/09/)
- Konqueror: http://dot.kde.org/1132619164/ … did anything happen since?
- Safari: ? (Apple is not even a member of the club)

In short

SWITCH
The Swiss Education & Research Network

EV SSL certificates are difficult (if not impossible) to get for organizations without an entry in a trade register or similar

They carry a hefty price tag: currently from $450 (GoDaddy) to $1499 (Verisign), for a one-year EV cert

Are only recognized by MSIE7 for the time being

The guidelines stipulate a couple of useful (minimum) requirements, but on the other hand are prone to being "abused" for purely commercial reasons / marketing purposes
("The impact of Extended Validation certificates on your business can be summed up in one word: TRUST", "Maximizing Site Visitor Trust Using Extended Validation SSL" etc.)

Won't be part of the SWITCHpki offering anytime soon

The Swiss Education & Research Network