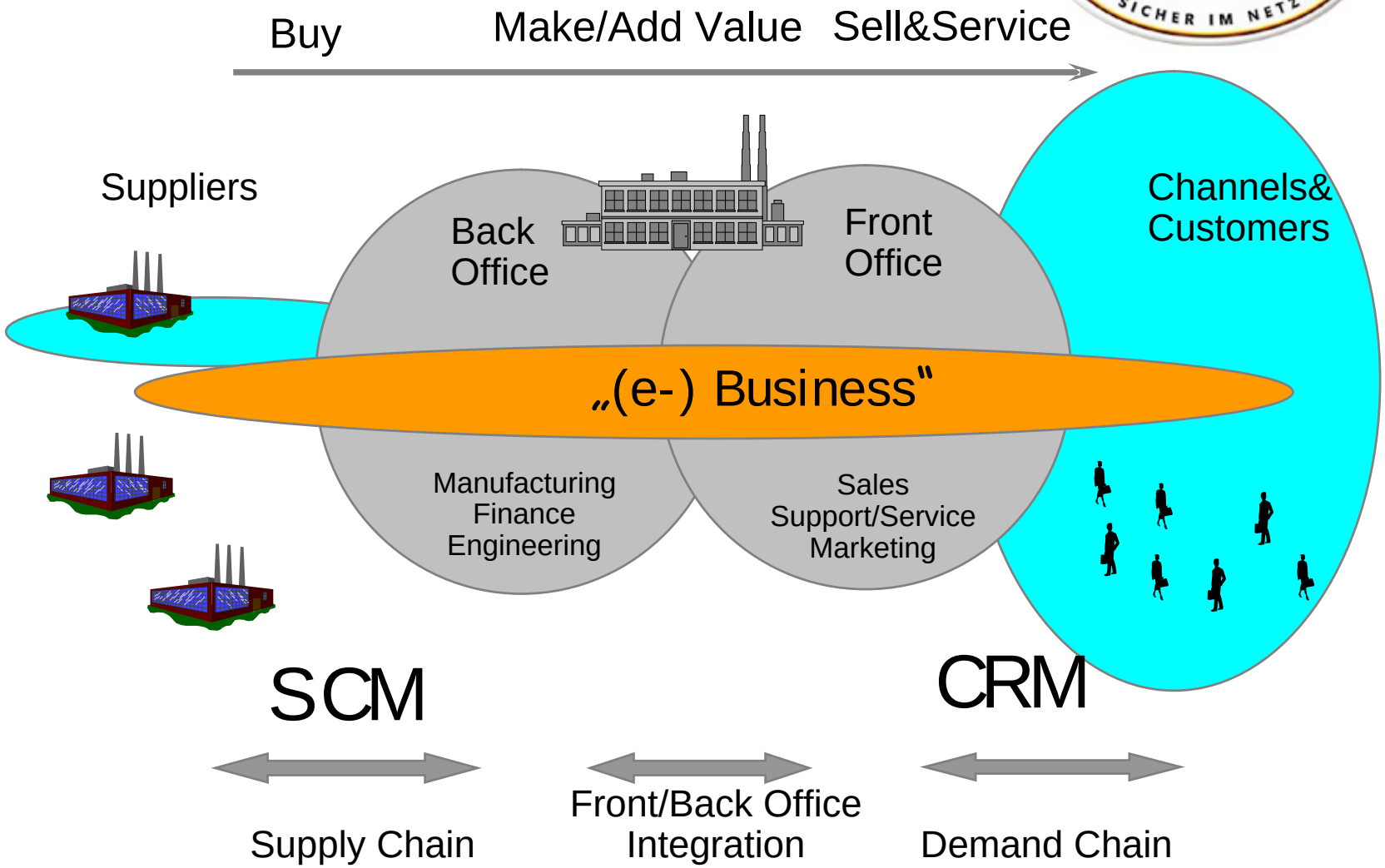
„Stärkeres Nutzervertrauen durch verläßliche Organsationsidentitäten“

Arno Fiedler (TeleTrusT e. V)

Übersicht

- Motivation EV
- Wie funktioniert EV bei verschiedenen Browsern
- Beantragung von EV Zertifikaten
- Informationen zum CA Browser Forum
- Persönliche Einschätzungen zum Markt in D


Buy
Make/Add Value
Sell&Service
Suppliers
Back Office
Front Office
Channels& Customers
„(e-) Business"
Manufacturing
Finance
Engineering
Sales
Support/Service
Marketing
SCM
CRM
Supply Chain
Front/Back Office Integration
Demand Chain

Online Business - Problem

- Phishing Angriffe stetig wachsend
  - Über 30K* Phishing Sites gemeldet (July 07)
  - Knapp $2Mrd** Verlust im US Online-Geschäft
- Ergebnis: steigendes Misstrauen der Konsumenten
  - 84% glauben, dass nicht genügend Schutznmassnahmen getroffen werden
  - 24% kaufen nicht online ***
- User benötigen Unterstützung korrekte Seiten von gefälschten Seiten zuunterscheiden
  - 90% getäuscht im April 2006 nach Harvard/UC Berkeley studie****
  - Bisheriges Wissen reicht nicht mehr:
    Goldenes Schloss zeigt nur Verschlüsselung an aber keine “Vertrauen”.

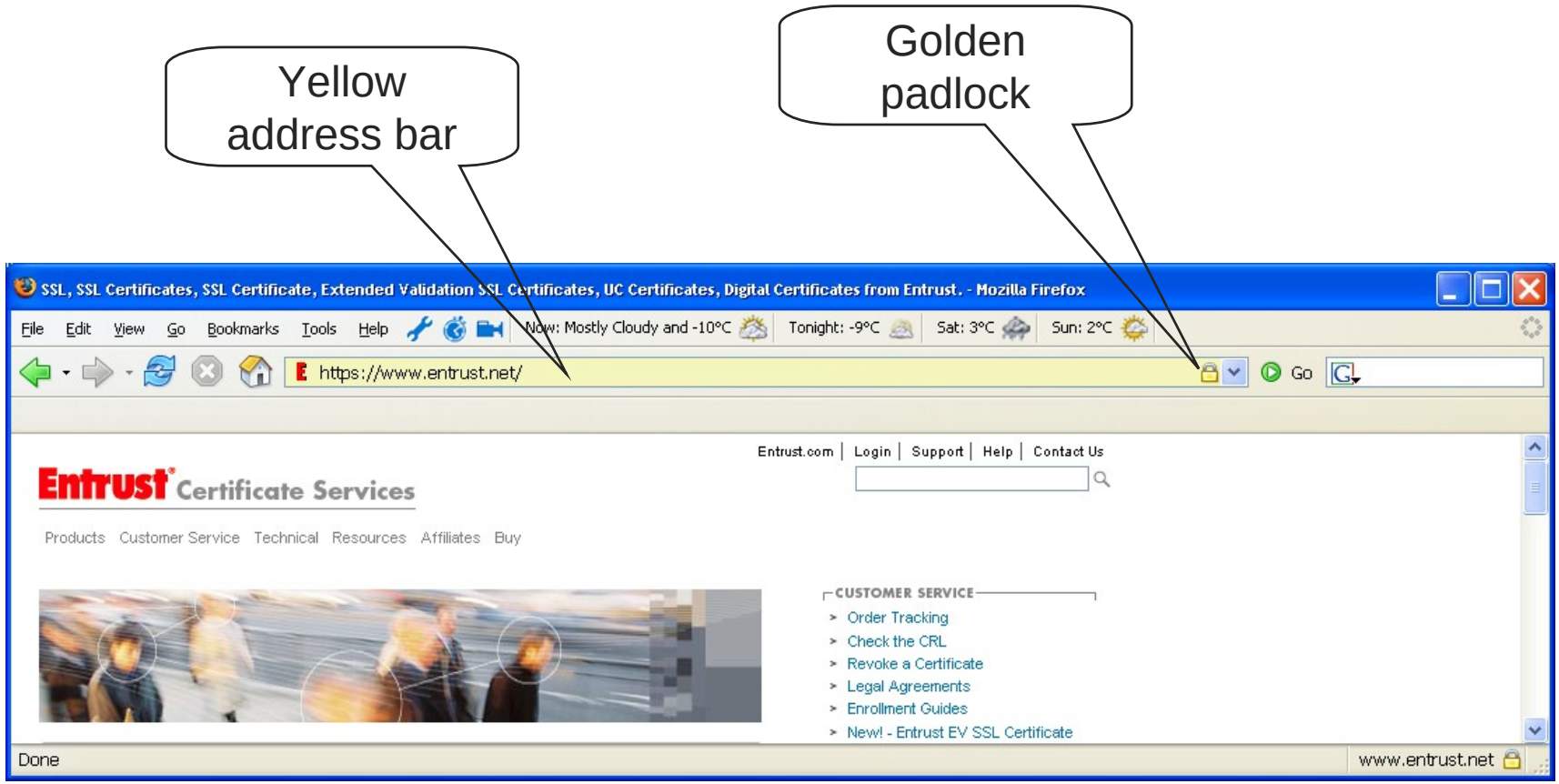
***Anti-Phishing Working Group**

****According to a Gartner Inc survey**

*****Forrester Research, December 2005. http://www.internetretailer.com/article.asp?id=17763**

******“Why Phishing Works,” April 2006. http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf**

Trust indicators



Phishing attacks

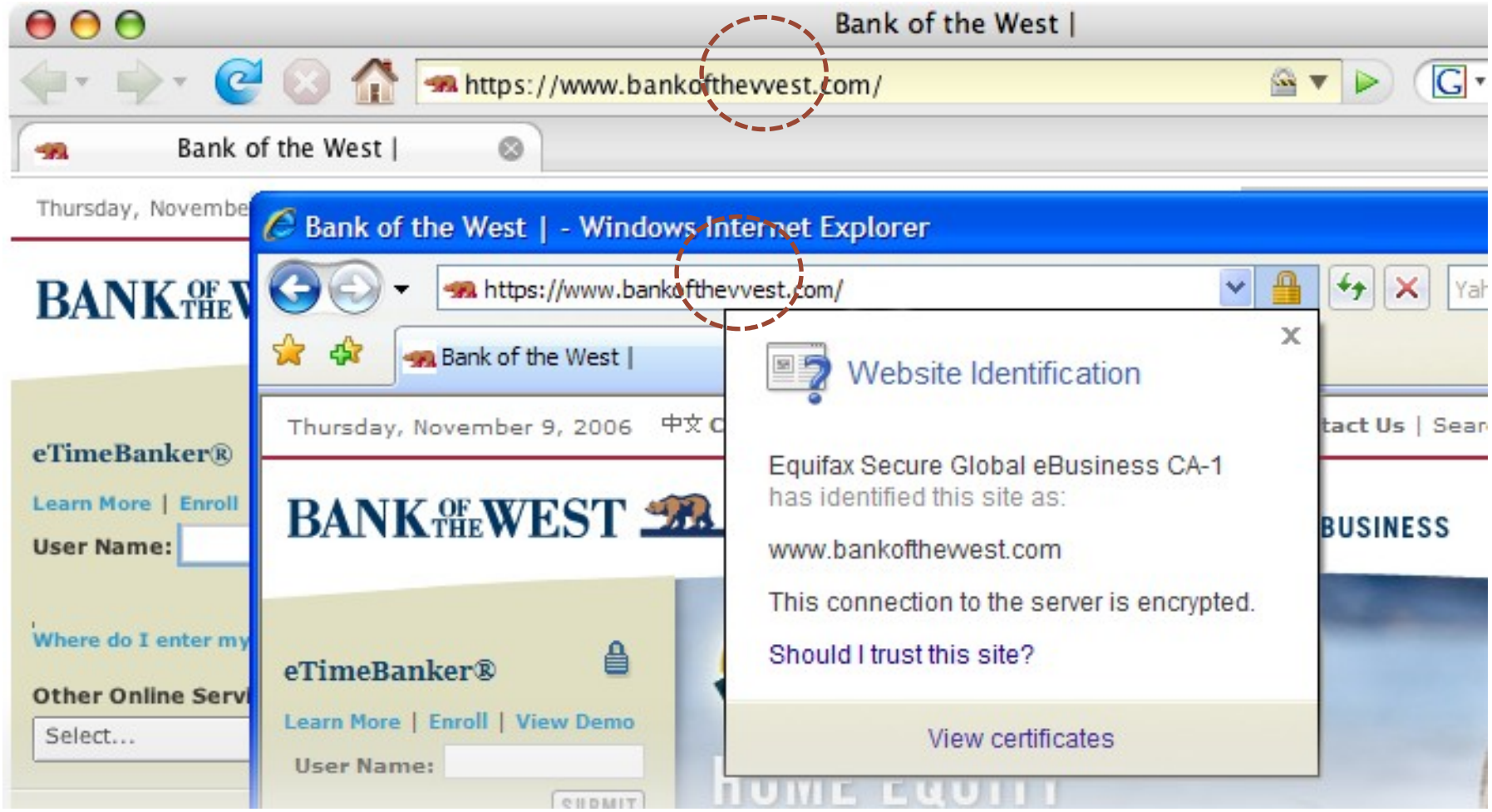


Fig 3.1, IE7 address bar for a site with a high-assurance SSL certificate
(showing the identity of the site from the SSL certificate)

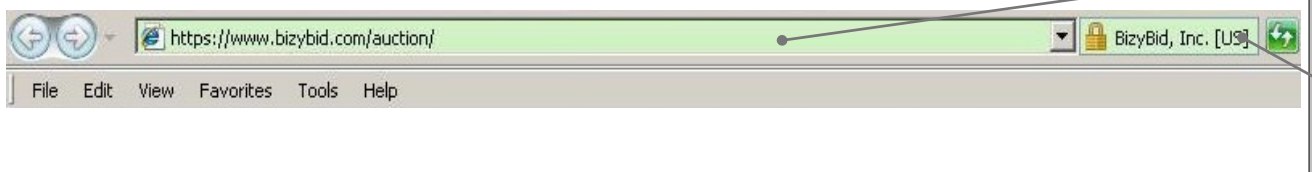
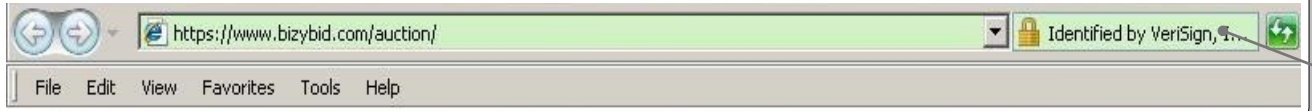


Fig 3.2, IE7 address bar for a site with a high-assurance SSL certificate
(alternating in the name of the Certification Authority who identified the site)



Green URL shows up for high assurance certs

Name of Organization that cert is issued to

CA that performed the “high assurance” authentication

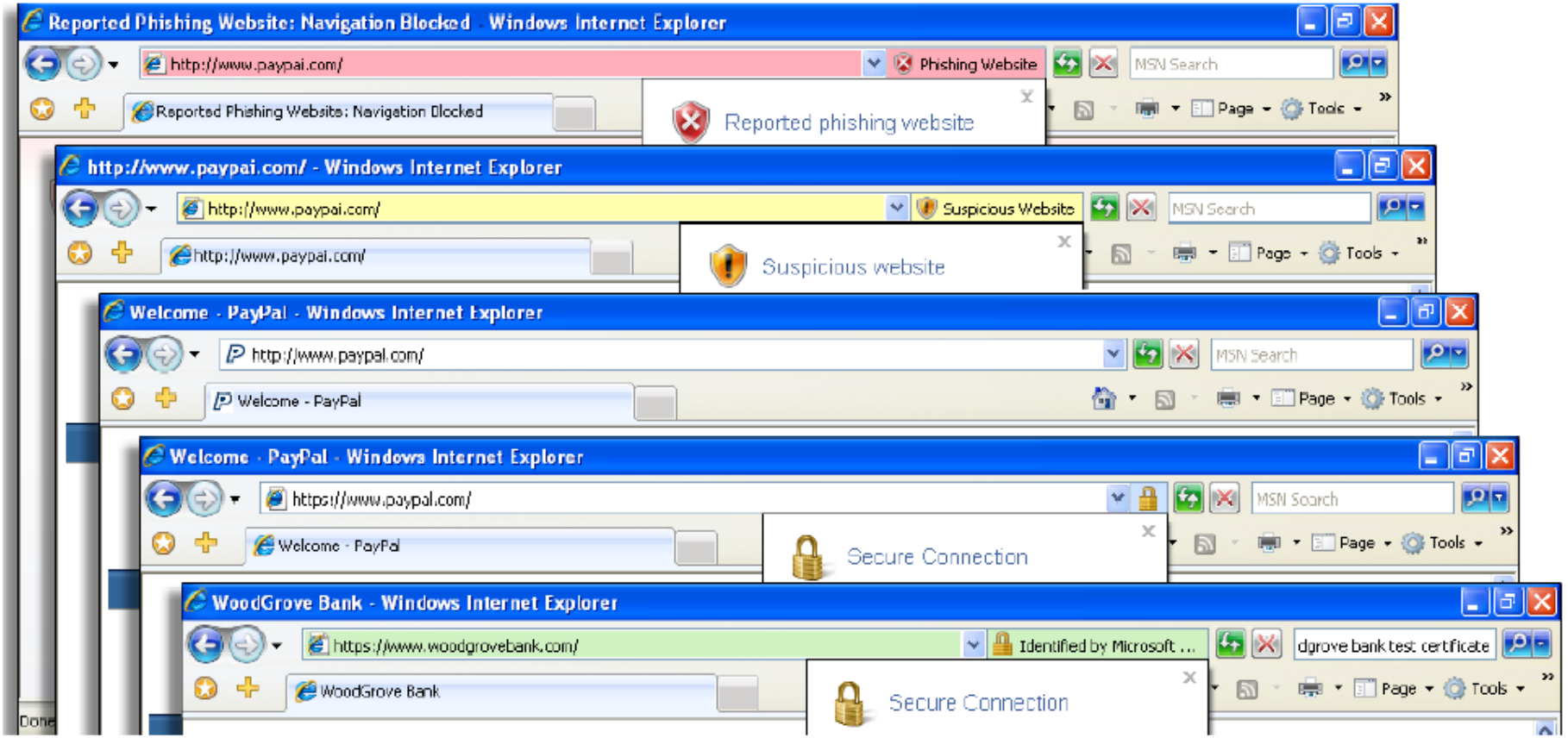
SSL – warum Extended Validation

- Zeigt dem Benutzer an, mit wem sie kommunizieren
- Bewährte Technologie:
  - Nutzt SSL Technologie
  - Abwärtskompatibel
    - Ältere Browser zeigen Zertifikate an wie gehabt
  - Standard SSL Zertifikate funktionieren wie gehabt
- Zusätzlicher Schutz gegen Phishing Attacken:
  - Verbesserte Prüfung der Zertifikatsinhaber
  - Verbesserte optische Kennzeichnung
    - Grüner Addressleiste mit Anzeige der Organisation und der CA

SSL mit EV - Anwendungsfälle

- Vorteile von EV
  - Gesteigertes Vertrauen in Ihre Webseite
  - Wettbewerbsvorteile
  - Förderung des Onlinehandels
- Zielkunden
  - Betreiber von E-Commerce Webseiten
  - Finanzinstitute wie Banken, Versicherungen etc.
  - Unternehmen, die ihren Namen/Brand schützen wollen

IE7 Phishing filter and EV SSL



Phishing, Suspected phishing, HTTP, HTTPS, EV

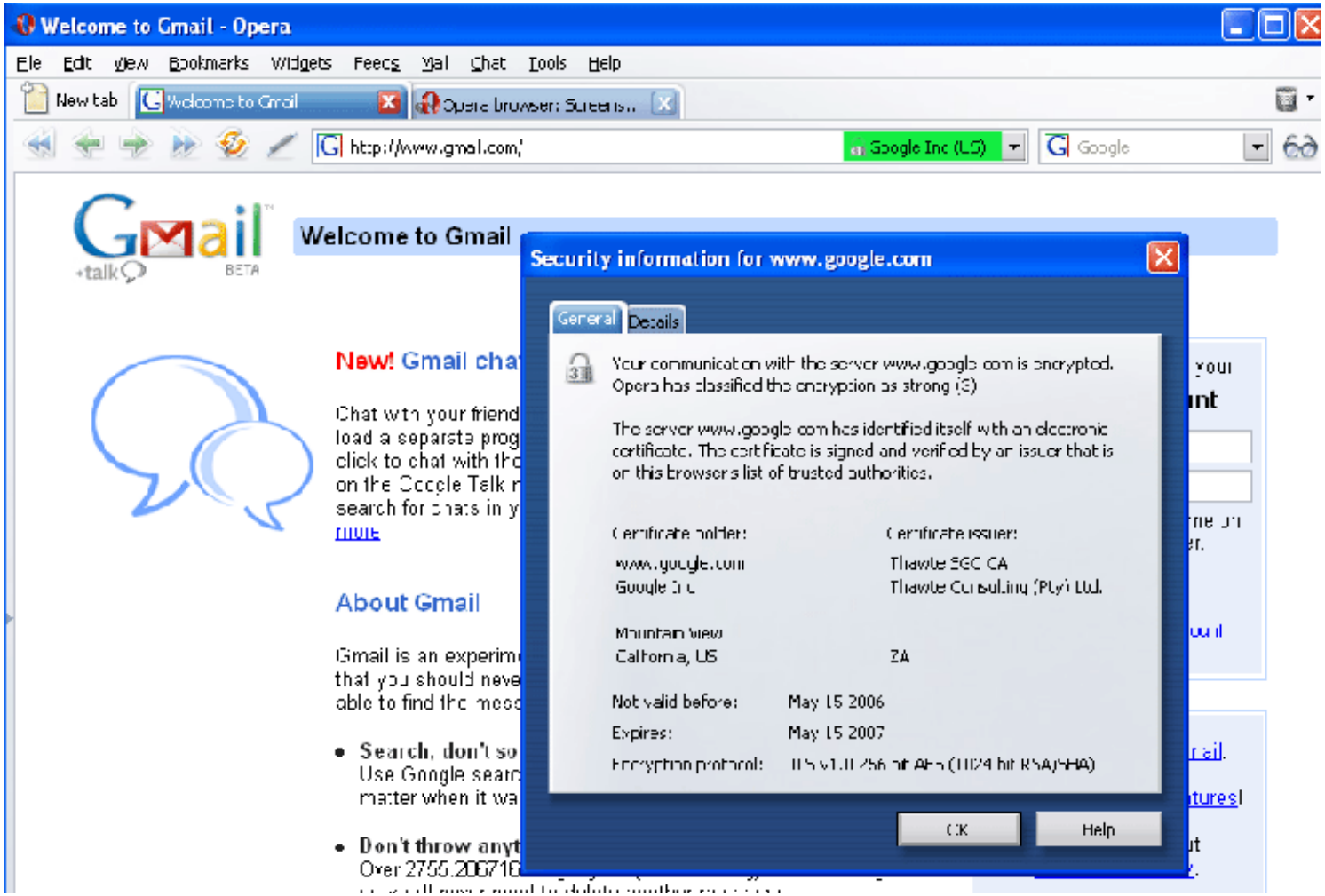
Änderungen bei CAs und Browsern

- CAs unterliegen strengeren Audit-Anforderungen
  - Jährliche (WebTrust) Audits
- Browsers verwenden CAs EV OID um Extended Validation Status anzuzeigen
  - IE7 unterstützt als erster Browser EV
  - Andere Browserhersteller planen EV Unterstützung
- Die grüne Adressleiste funktioniert nur mit EV Zertifikaten von autorisierten CAs
- Nur entsprechend geschultes Personal darf die Antragsinformationen prüfen
- Der Browser prüft Gültigkeit der Root and OID

Windows XP Kompatibilität

- IE7 on Windows Vista – unterstützt EV
- IE7 on Windows XP – unterstütz EV nicht native
- EV Upgrader ermöglicht Windows XP clients im IE7 die grüne Adressleiste zu unterstützen
  - XP erfordert manuelle Installation der Root oder “Web beacon” Technologie
  - Web beacon muss auf der besuchten Webseite enthalten sein
    - Automatisches Update der Rootzertifikate
    - Nutzt existierende Windows Root Update Funktionalität

Opera 9


Welcome to Gmail - Opera
File Edit View Bookmarks Widgets Feeds Mail Chat Tools Help
New tab
Welcome to Gmail
http://www.gmail.com/
Google Inc (US)
Google
Gmail
BETA
Welcome to Gmail
New! Gmail chat
About Gmail
Security information for www.google.com
General
Details
Your communication with the server www.google.com is encrypted.
Opera has classified the encryption as strong (3)
The server www.google.com has identified itself with an electronic certificate. The certificate is signed and verified by an issuer that is on this browser's list of trusted authorities.
Certificate holder:
Certificate issuer:
www.google.com
Google Inc
Thawte SGC CA
Thawte Consulting (Pty) Ltd.
Mountain View
California, US
ZA
Not valid before: May 15 2006
Expires: May 15 2007
OK
Help

Antragsprozess - Übersicht

- Antragssteller unterliegen höheren Registrierungs-anforderungen
- Wer kann EV Zertifikate beantragen?
  - Behörden
  - Kapitalgesellschaften
  - Personengesellschaften
  - Einzelunternehmen
- Prüfung des Antrages umfasst
  1. Existenz der Organisation (Offizielle Registrierung)
  2. Zertifikatsverwendungszweck
  3. Domaininhaberschaft
  4. Organisationsname

Vorbereitung seitens Antragssteller

- Sicherstellen, dass die Organisation bei den zuständigen offiziellen Zulassungsbehörden registriert ist
  - Der Antragssteller benötigt die Informationen betr. der Unternehmensregistrierung
- Aktualisierung der “Whois”-Information damit diese mit dem offiziellen Organisationsnamen übereinstimmt
- Zusätzliche Dokumente
  - Falls die ausstellende CA nicht unabhängig die Befugnis des Antragsstellers prüfen kann, so verlangt die CA zusätzliche Informationen und/oder Dokumente wie z.B. ein Rechtsgutachten welches verschiedene Antragsdaten bestätigt.

EV Antragsinformationen

- Registrierungsprozess dauert länger als für Standard SSL Zertifikate
  - Mehrere Wochen
- Zertifikat wird per E-Mail ausgeliefert
- Zertifikatshierarchie komplexer
  z. B. bei TC Trustcenter:
  - GeoTrust Extended Validation SSL CA (
  - GeoTrust Primary Certificate Authority (cross certified with Equifax Secure CA root)
- Siegel Installation empfohlen
  - Inkl. EV Upgrader Funktionalität

EV Antragsinformationen

- EV Zertifikate verfügbar mit 1 und 2 Jahren Laufzeit
  - Max. Laufzeit entsprechend Richtlinien
- CSRs (Anträge) können wie bei SSL-Certs bisher erstellt werden
- Information zum beantragenden Unternehmen/Organisation
  - Die Antragsdaten werden geprüft und werden im Zertifikat aufgenommen
- Domaininhaberschaft wird überprüft

EVC Angebote (unverbindlich, Stand 24.01.08)

Unternehmen:	Preis für 2 Jahre
Entrust (not managed)	1129 Eur
VeriSign	2295 Eur
TC Trustcenter via Geotrust	1129 Eur
DigiCert (derzeit nicht in D)	544 Eur
Globalsign	958 Eur

The EV SSL Certificate and its Contents

Organization name - This field must contain the Subject's (i.e., certificate holding entity's) full legal organization name as listed in the official records of the Incorporating Agency in the Subject's Jurisdiction of Incorporation. In addition, an assumed name or d/b/a (doing business as) name used by the Subject may be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of the full legal organization name and the assumed or d/b/a name exceeds 64 bytes as defined by RFC 3280, the CA should use only the full legal organization name in the certificate.

Domain name - This field must contain one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV SSL Certificates.

Jurisdiction of Incorporation - These fields must contain information only to the level of the Incorporating Agency - e.g., the Jurisdiction of Incorporation for an Incorporating Agency at the country level would include country information but would not include state or province or city or town information; the Jurisdiction of Incorporation for an Incorporating Agency at the state or province level would include both country and state or province information, but would not include city or town information; and so forth. Country information must be specified using the applicable ISO country code. State or province information, and city or town information (where applicable) for the Subject's Jurisdiction of Incorporation must be specified using the full name of the applicable jurisdiction.

Registration Number - This field must contain the unique Registration Number assigned to the Subject by the Incorporating Agency in its Jurisdiction of Incorporation (for Private Organization Subjects only).

Address of Place of Business - This field must contain the address of the physical location of the Subject's Place of Business. City, state and country information is required. Street number and ZIP/postal are optional.

Certificate Class	Assurance Level			Usage			
	High Assurance with Extended Validation	High assurance	Medium assurance	Code/ Content Signing	Secure SSL/TLS Sessions	Authenti-cation	Signing and encryption
Class 3 Certificates		+		+	+	+	+
Class 3 EV Certificates	+	+			+	+	+

CA / Browser Forum (2005)

- Major CAs and browser suppliers got together
- Formed the CA / Browser Forum
- Objective – Improve trustworthiness of the Web
- Project to develop certificate issuance guidelines for new browser trust indicators
- Microsoft has adopted an interim draft of the CABForum guidelines as the criteria for inclusion in their root embedding program

CA/Browser Forum Membership Requirements

CA/Browser Forum members shall meet at least one of the following criteria.

Issuing CA:- The member organization operates a certification authority that has a current and successful WebTrust for CAs audit, or ETSI 102042 or ETSI 101456 audit report prepared by a properly-qualified auditor, and that actively issues certificates to Web servers that are openly accessible from the Internet using any one of the mainstream browsers.

Root CA:- The member organization operates a certification authority that has a current and successful WebTrust for CAs, or ETSI 102042 or ETSI 101456 audit report prepared by a properly-qualified auditor, and that actively issues certificates to subordinate CAs that, in turn, actively issue certificates to Web servers that are openly accessible from the Internet using any one of the mainstream browsers.

Browser:- The member organization produces a software product intended for use by the general public for browsing the Web securely.

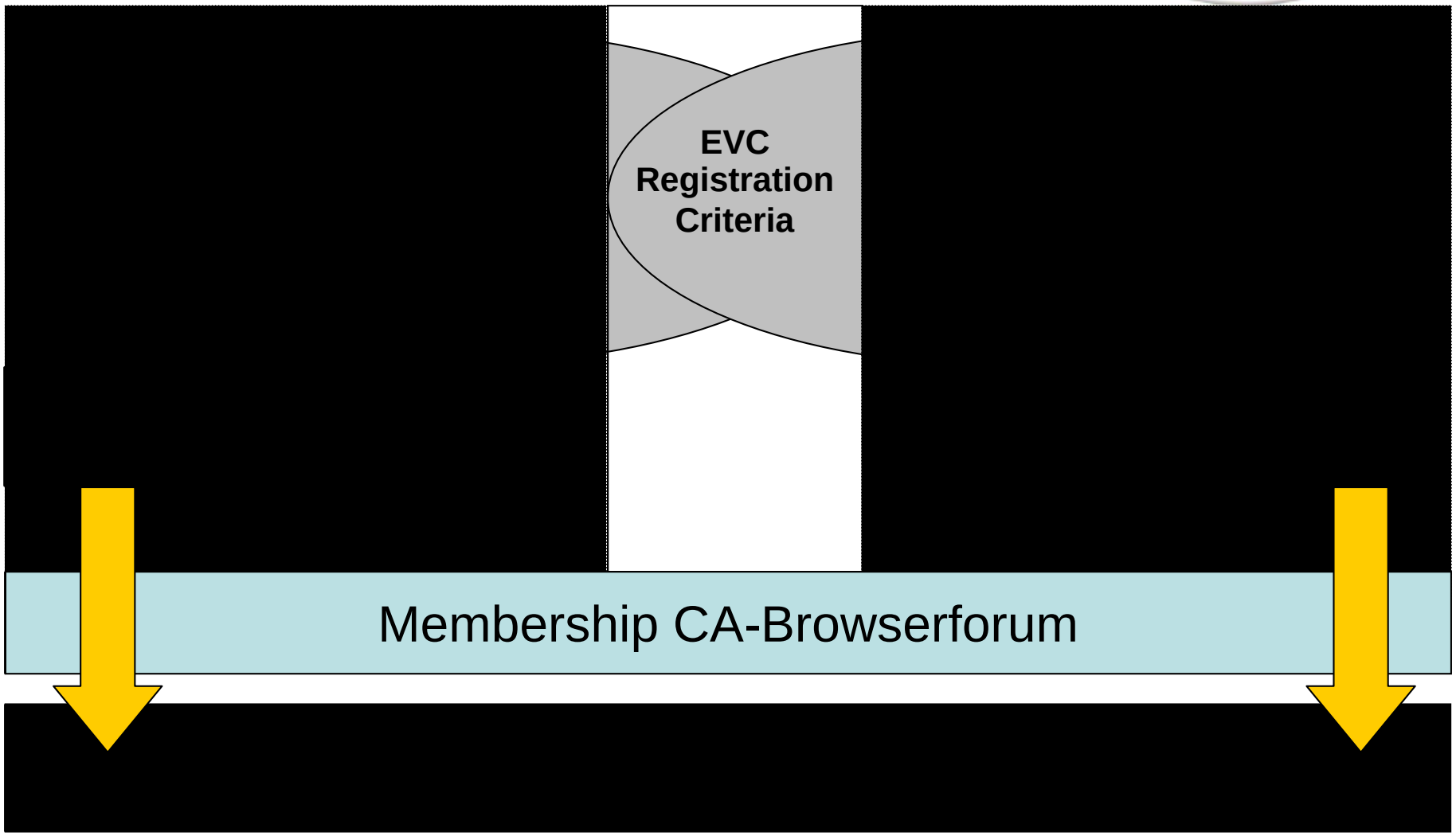
the CA/Browser Forum members:

Certification Authorities

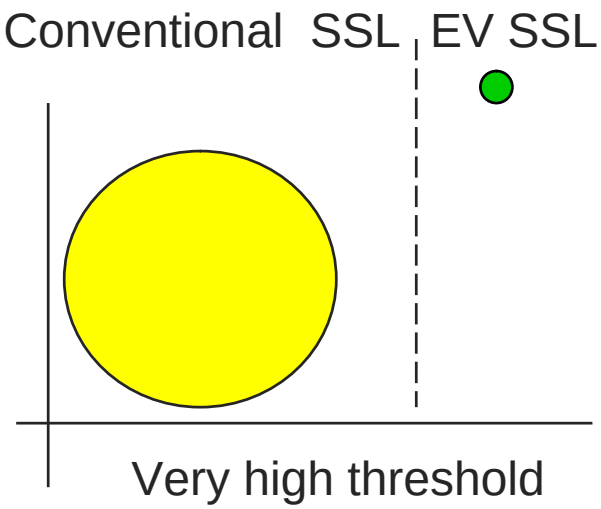
- A-Trust GmbH
- Trustwave
- Certum
- Comodo CA Ltd
- Cybertrust
- DigiCert, Inc.
- DigiNotar
- Echoworx Corporation
- Entrust, Inc.
- GeoTrust, Inc.
- Getronics PinkRoccade
- GlobalSign
- GoDaddy.com, Inc.
- IdenTrust, Inc.
- ipsCA, IPS Certification Authority s.l.
- Izenpe S.A.
- Network Solutions, LLC
- QuoVadis Ltd.
- RSA Security, Inc.
- SECOM Trust Systems CO., Ltd.
- SSC
- SwissSign AG
- TC TrustCenter GmbH
- TDC Certification Authority
- Thawte, Inc.
- Trustis Limited
- VeriSign, Inc.
- Wells Fargo Bank, N.A.

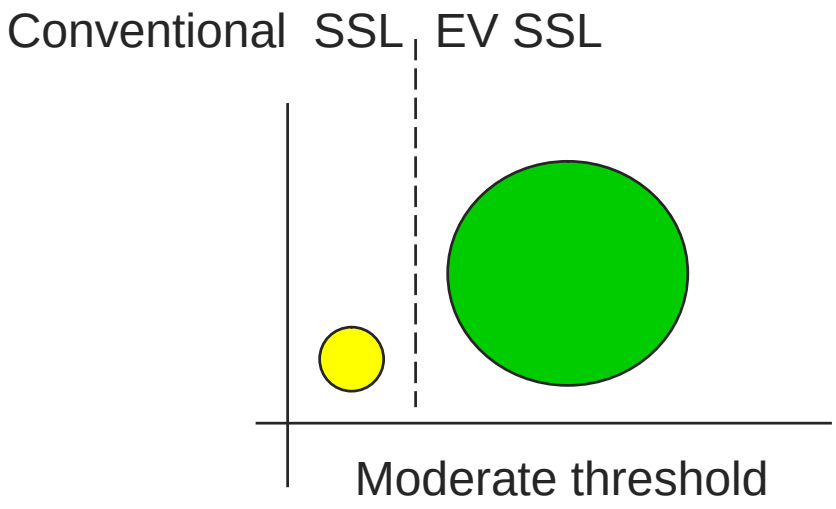
Internet Browser Software Vendors

- KDE
- Microsoft Corporation
- Opera Software ASA
- The Mozilla Foundation

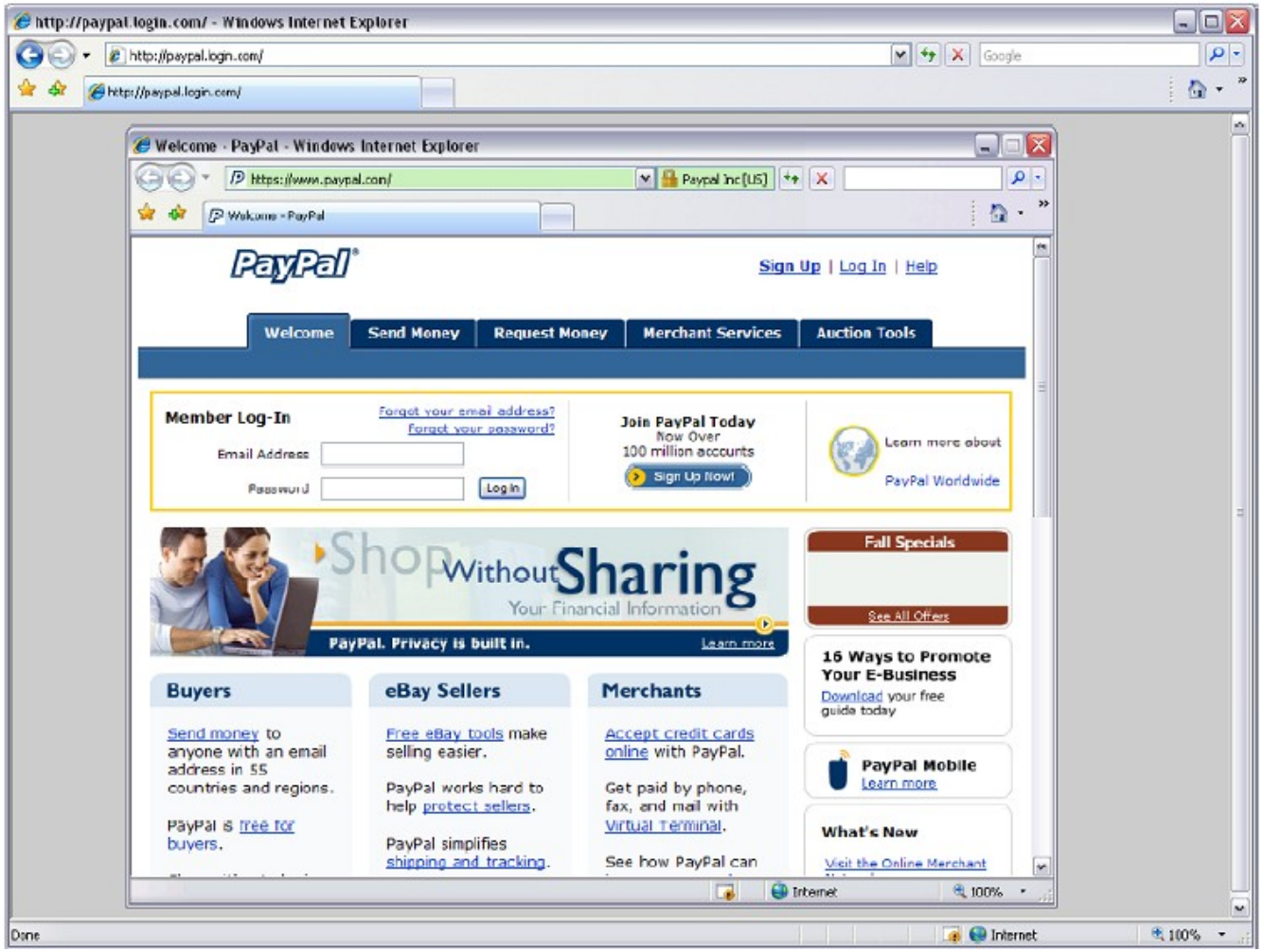

EVC
Registration
Criteria
Membership CA-Browserforum

The SSL Marketplace - after EV (two points of view)





It’s not foolproof – picture-in-picture



Das Spannungsfeld der Anforderungen

Bedarf an staatlicher Regulierung?
„felix austria“ mit „Amtssignatur und Organsationssiegeln“?

Murphy‘s Laws on Justice (Bureaucracy?):

If the government hasn‘t taxed, licensed or regulated it, isn‘t probably worth anything.

Zusammenfassung:

- Browser Sicherheit UND Nutzervertrauen kann durch EV SSL drastisch verbessert werden
- Erste Marktreaktionen sind vielversprechend
- EVC wird “Stand der Technik” im Online-Handel
- “Awareness” bleibt kritischer Erfolgsfaktor: Grünes Licht bei einer Ampel garantiert auch NICHT die Sicherheit!

Mehr Informationen:
www.teletrust.de
www.sicher-im-netz.de
www.cabforum.org