SSL certifikáty a důvěryhodné CA

Konference Internet a Technologie 13

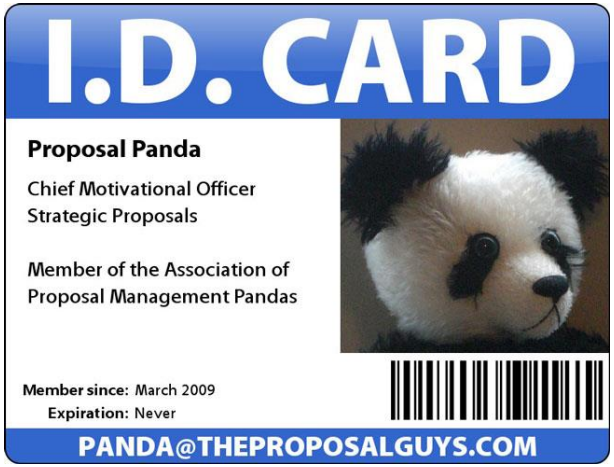
Jindřich Zechmeister
jindrich.zechmeister@zoner.cz
[jindra@zoner.cz]

ZONER software, a.s.
www.zoner.eu | www.SSLmarket.cz

SSL certifikáty – funkce a typy

Použití SSL certifikátů

- Protokol SSL/TLS
- Funkce SSL certifikátu:
  - Zabezpečení přenášených dat (odposlouchávání)
  - Autentizace a identifikace



Druhy SSL certifikátů

- Podle ověření
  - DV doménové ověření
  - OV ověření organizace
  - EV rozšířené ověření

Druhy SSL certifikátů

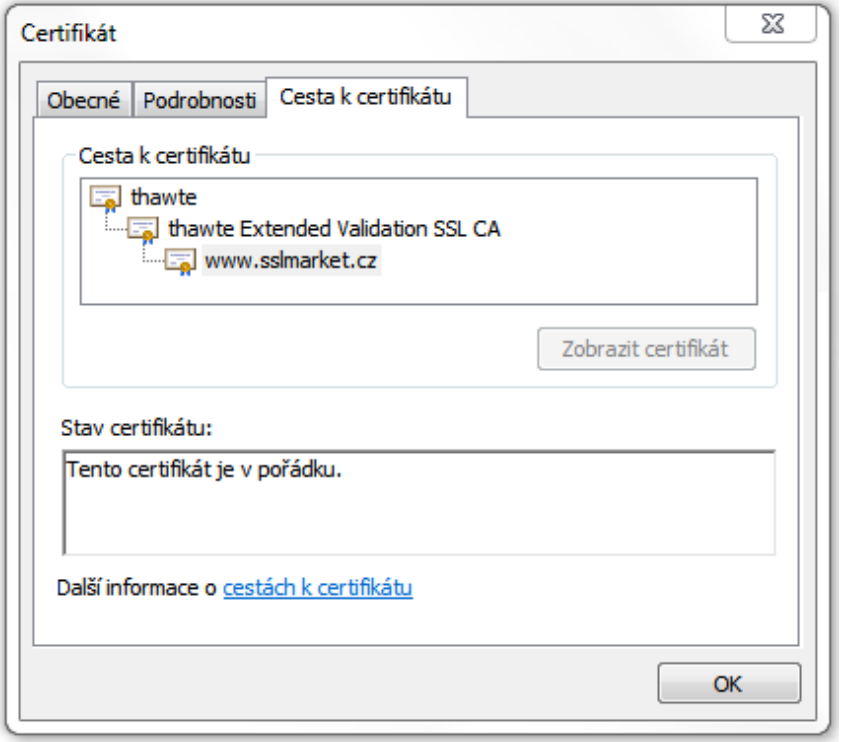
- Podle počtu zabezpečených domén
  - Wildcard (*.domena.cz)
  - SAN (DNS název)
- Jiné
  - Codesigning, SGC, osobní

Důvěryhodnost certifikátů

- Root certifikáty CA jsou v systému uživatele
  - > Systém uživatele důvěřuje CA

- Intermediate certifikáty
  - Nutné pro vazbu na Root CA

  a důvěryhodnost



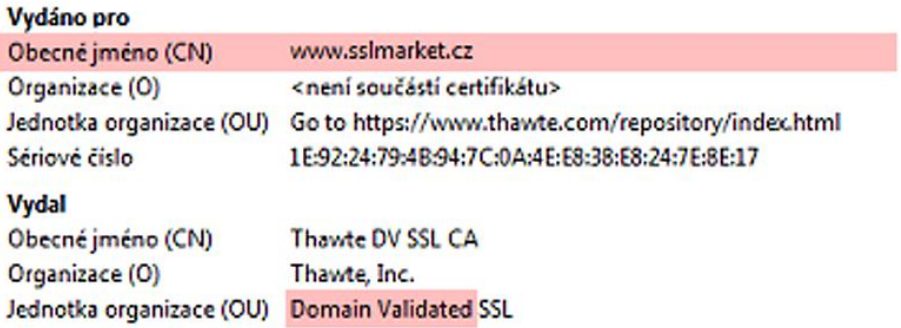
Nedůvěryhodný certifikát

- Vystavila CA, které nedůvěřuji
  - Tzv. selfsigned certifikáty či nedůvěryhodná CA
  - Není správný chain
  - Může jít o podvržený cert. útočníka

SSL certifikáty a ověření

DV certifikáty

- Rychlé vystavení
- Ověření probíhá přes e-mail
- V certifikátu je pouze doména

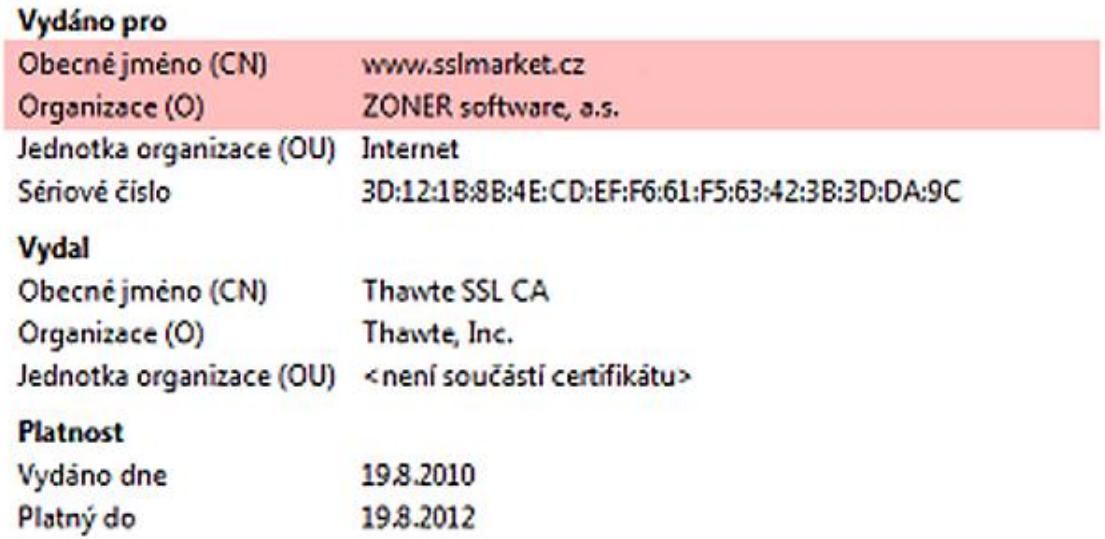


Vydáno pro	
Obecné jméno (CN)	www.sslmarket.cz
Organizace (O)	<není součástí certifikátu>
Jednotka organizace (OU)	Go to https://www.thawte.com/repository/index.html
Sériové číslo	1E:92:24:79:4B:94:7C:0A:4E:E8:38:E8:24:7E:8E:17
Vydal	
Obecné jméno (CN)	Thawte DV SSL CA
Organizace (O)	Thawte, Inc.
Jednotka organizace (OU)	Domain Validated SSL

- Blacklist názvů – kontrolované a zakázané jména (např. Facebook, bank)
  - Symantec cca 12 000 položek

OV certifikáty

- Vystavení 1-2 dny
- Ověření vlastníka domény, v OR (ARES) a tel.
- V detailu certifikátu název organizace



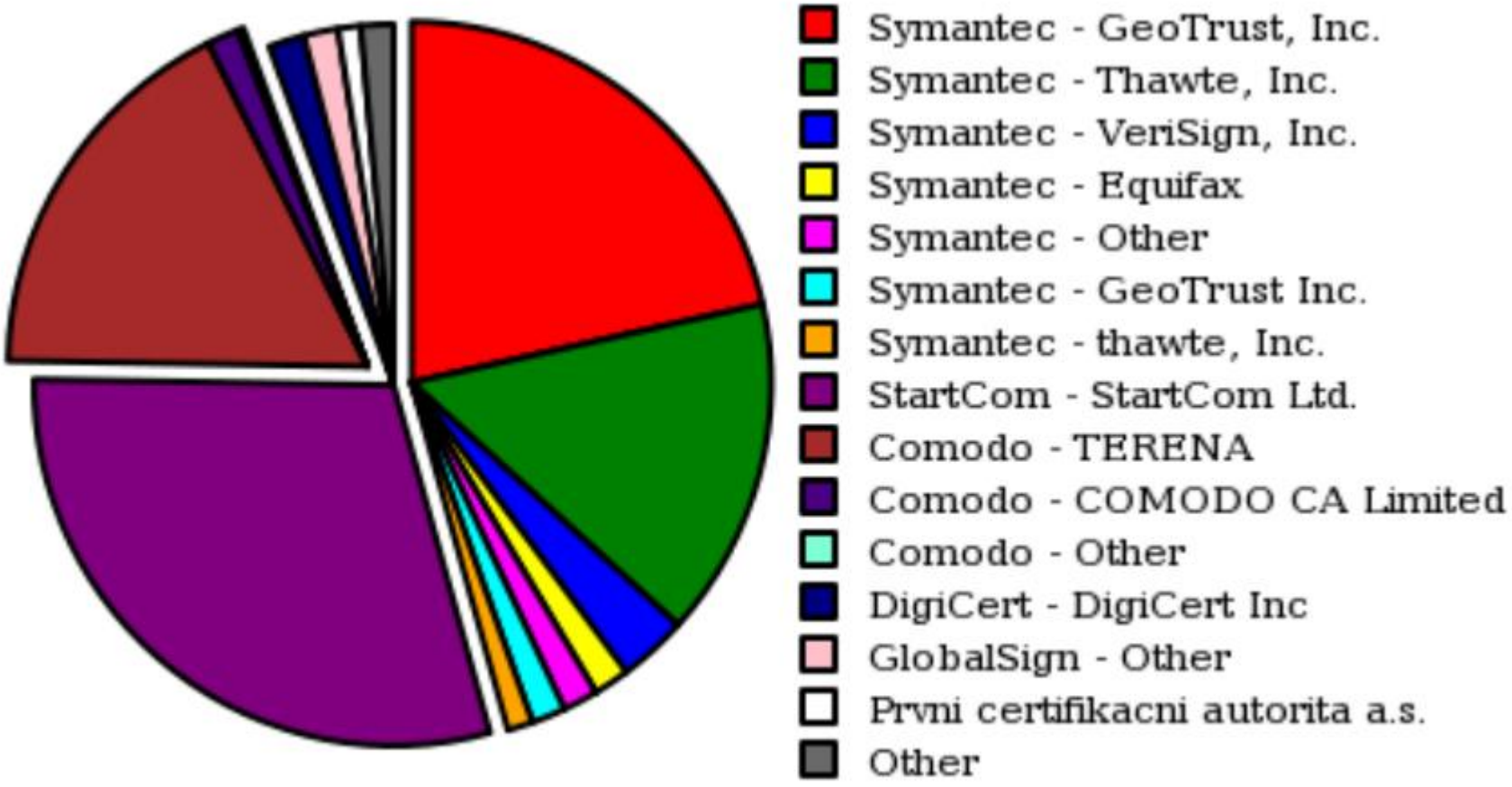
Vydáno pro	
Obecné jméno (CN)	www.sslmarket.cz
Organizace (O)	ZONER software, a.s.
Jednotka organizace (OU)	Internet
Sériové číslo	3D:12:1B:8B:4E:CD:EF:F6:61:F5:63:42:3B:3D:DA:9C
Vydal	
Obecné jméno (CN)	Thawte SSL CA
Organizace (O)	Thawte, Inc.
Jednotka organizace (OU)	<není součástí certifikátu>
Platnost	
Vydáno dne	19.8.2010
Platný do	19.8.2012

EV certifikáty

- Zelený EV pruh – nejvyšší důvěryhodnost
- Ověření – 4 fáze, více zdrojů
- Název organizace přímo z zeleném řádku
- Na první pohled zřejmý vlastník certifikátu

Certifikační autority

Certifikační autority



+ GoDaddy (USA)

Česká republika, říjen 2012

Certifikační autority II.

Přehled důvěryhodnosti CA (k 5/2013, vlastní test)

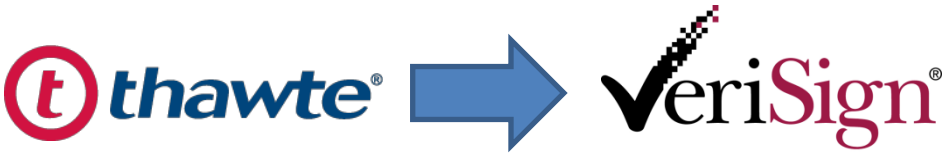
CA	MRCP (MS OS)	Mozilla Firefox	Adobe Acrobat*	Android 4.2
Symantec	✓	✓	✓ **	✓
Thawte	✓	✓	---	✓
GeoTrust	✓	✓	---	✓
RapidSSL	✓	✓	---	✓
PostSignum	✓	✗	✗	✗
1. CA	✓	✗	05/2013	✗
Eidentity	✗	✗	✗	✗
Comodo	✓	✓	✗	✓

* AATL (Adobe Approved Trust List)

** Řešení pro Adobe® Certified Document Services (CDS)

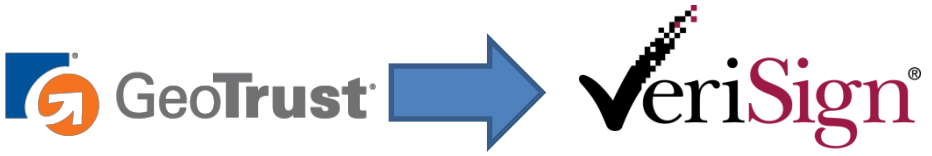
CA rodiny Symantec

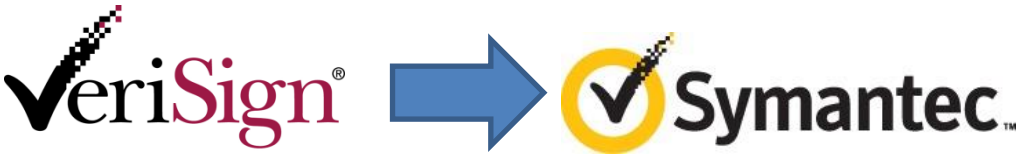
Symantec: VeriSign + Thawte + GeoTrust



1999 za 500 mil. USD

2006 za 125 mil. USD





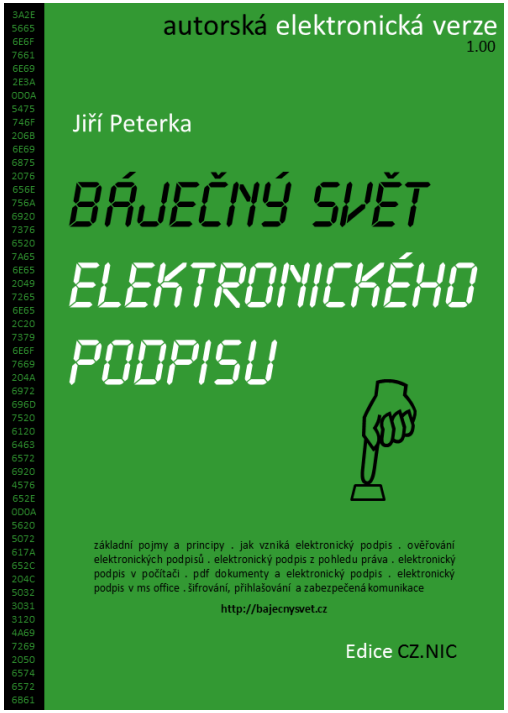
2010 >1000 mil. USD

Budoucnost CA

- Nové algoritmy pro vydávání - ECC, DSA
- CA/B fórum – společné standardy
- Automatické ověřování DV – DNS záznam
- Používání FQDN (problém interní názvy x TLD)

Informační zdroje

- Libor Dostálek, Marta Vohnoutová: Velký průvodce infrastrukturou PKI
- Jiří Peterka: Báječný svět elektronického podpisu



Děkuji za pozornost

Jindřich Zechmeister

ZONER software, a.s.

[jindra@zoner.cz]