

# SECURITY 2013



21. ročník konference o bezpečnosti v ICT

## Zabezpečení dat pomocí SSL

přehled důvěryhodných certifikačních autorit na trhu

Petr Komárek, Jindřich Zechmeister

ZONER software, a.s.

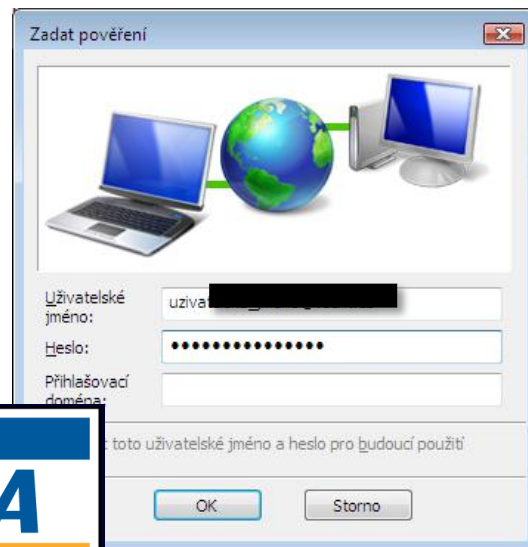




# WWW a bezpečnost

## Nutnost bezpečné komunikace na internetu:

- e-komerční řešení (platby kartami)
- výměna důvěrných informací (intra/extra-net)
- při zpracování citlivých osobních údajů, dat (administrace)
- elektronická pošta (webmail, Exchange, ..)
- legislativní povinnosti, které vyžadují zabezpečené přenosy
- atd.



# WWW a bezpečnost

## ■ Jsme správně?

Intranet ZONER Software x SERVIS 24 Internetbanking x AEC - Program konference x

file:///C:/Users/petr.komarek.ZONER/Documents/\_ZONEF

SERVIS 24 INTERNETBANKING 956 777 956 Internetové bankovníctví České spořitelny

**Přihlášení SERVIS 24**

Heslem Klientským certifikátem

Klientské číslo

Heslo

Klávesnice ? Návod k přihlášení Přihlásit

**Videoukázky**

Mobilní banka - Android

SERVIS 24 Internetbanking

- Demo
- Více informací

ČESKÁ SPOŘITELNA

Bezpečnost | Kontakty | Návoděda | Pro nevidomé 2013 © Česká spořitelna, a. s. – všechna práva vyhrazena.





# SSL (Secure Sockets Layer)

Nestcape Corporation - SSL v1/v2/**v3** (1994-1996 )

- nezávislé na systému
- vlastní specifikace

Transport Layer Security (TLS)

- nástupce SSL, standardizovaný protokol (RFC)
- dnes TLS 1.2 (SSL 3.3) ÷ TLS/SSL



HTTPS, FTPS, SMTPS, POP3S, IMAPS



## Co je potřeba

- webový server podporující SSL
- je vystaven a nainstalován na server serverový certifikát
- IP adresa nebo podpora SNI (Server Name Indication)
- webové stránky jsou ošetřeny pro použití SSL komunikace





# Fungování SSL

## Komunikace

- Asymetrické šifrování (2 klíče) 1024 b klíče (2048 b)
- Symetrické šifrování (pro ušetření systémových prostředků), klíče 128b, 256b

## "Báječný svět elektronického podpisu"

**Jiří Peterka**

zdarma ke stažení na <http://knihy.nic.cz/>  
[www.bajecnysvet.cz](http://www.bajecnysvet.cz)





# Důvěra x Nedůvěra

Certifikační autorita potvrzuje serverový certifikát.





# Nedůvěryhodný certifikát



## Toto připojení není důvěryhodné



### Bezpečnostní certifikát webu není důvěryhodný!

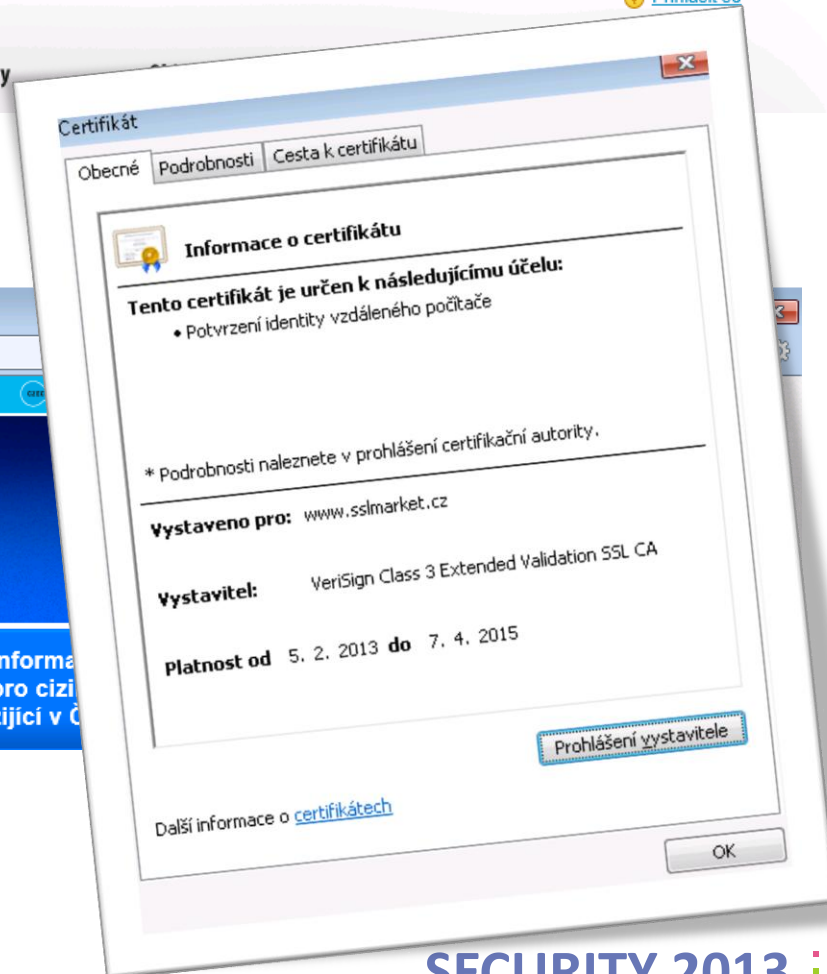
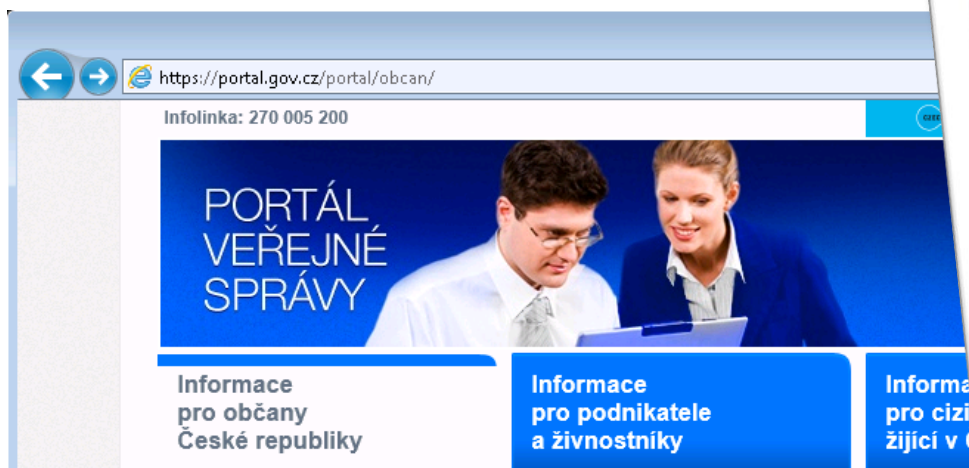
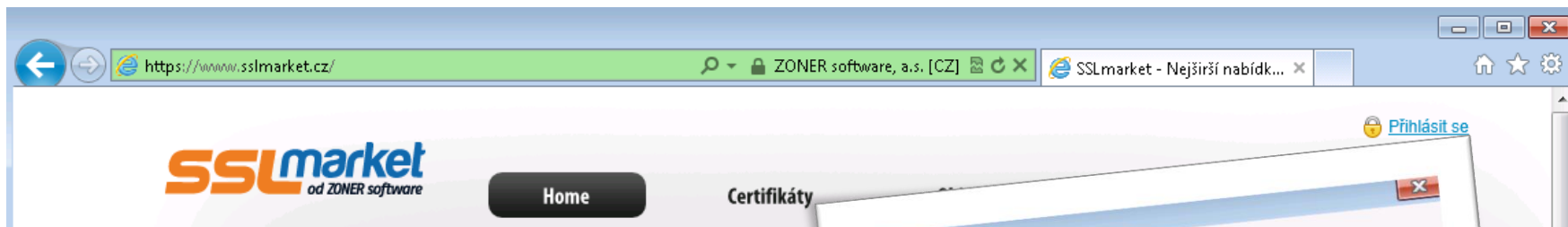
Pokusili jste se přejít na server [redacted], ale server předložil certifikát vydaný subjektem, kterému operační systém vašeho počítače nedůvěřuje. To může znamenat, že server generoval vlastní bezpečnostní záruky, u nichž Google Chrome nemůže spoléhat na informace o identitě, nebo že se vaší komunikaci může pokoušet zachytit útočník.

Neměli byste pokračovat, **zvláště** pokud jste takové varování u těchto stránek dosud neviděli.

► [Potřebuji vysvětlení](#)

▼ Další informace

# "důvěryhodný" certifikát





# Certifikační autority (CA)

Světové CA

\*

České CA

\*

Vlastní CA





# VeriSign



- Leader v internetové bezpečnosti.
- Správce domén (.com, .net, .cc, .tv, .name, .jobs, .edu)
- Založena 1995 jako oddělená společnost od RSA Data Security
- 1998 vstup na burzu
- Mnoho akvizic i prodejů.



Známa značka VeriSign Secured





# THAWTE



- Založena 1995, Mark Shuttleworth (1973)
- Specializace na digitální certifikáty a internetovou bezpečnost
- Prodej 12/1999 za 600 miliónů dolarů společnosti VeriSign

## Mark Shuttleworth

- 2. vesmírný turista (2002, 9 dnů, \$20mio.)
- v roce 2005 založil Ubuntu Foundation
- leden 2013 Ubuntu pro chytré telefony





- 1./2. největší poskytovatel SSL certifikátů
- Více jak 100 000 zákazníků ve 150 zemích
- Vlastník CA RapidSSL
- Prodej 09/2006 za 125 miliónů dolarů společnosti VeriSign





- Kompletní nákup SSL portfolia VeriSign v roce 2010
- Prodány kompletní služby PKI, SSL, ...
- Cena \$1.28 billion (miliardy USD)

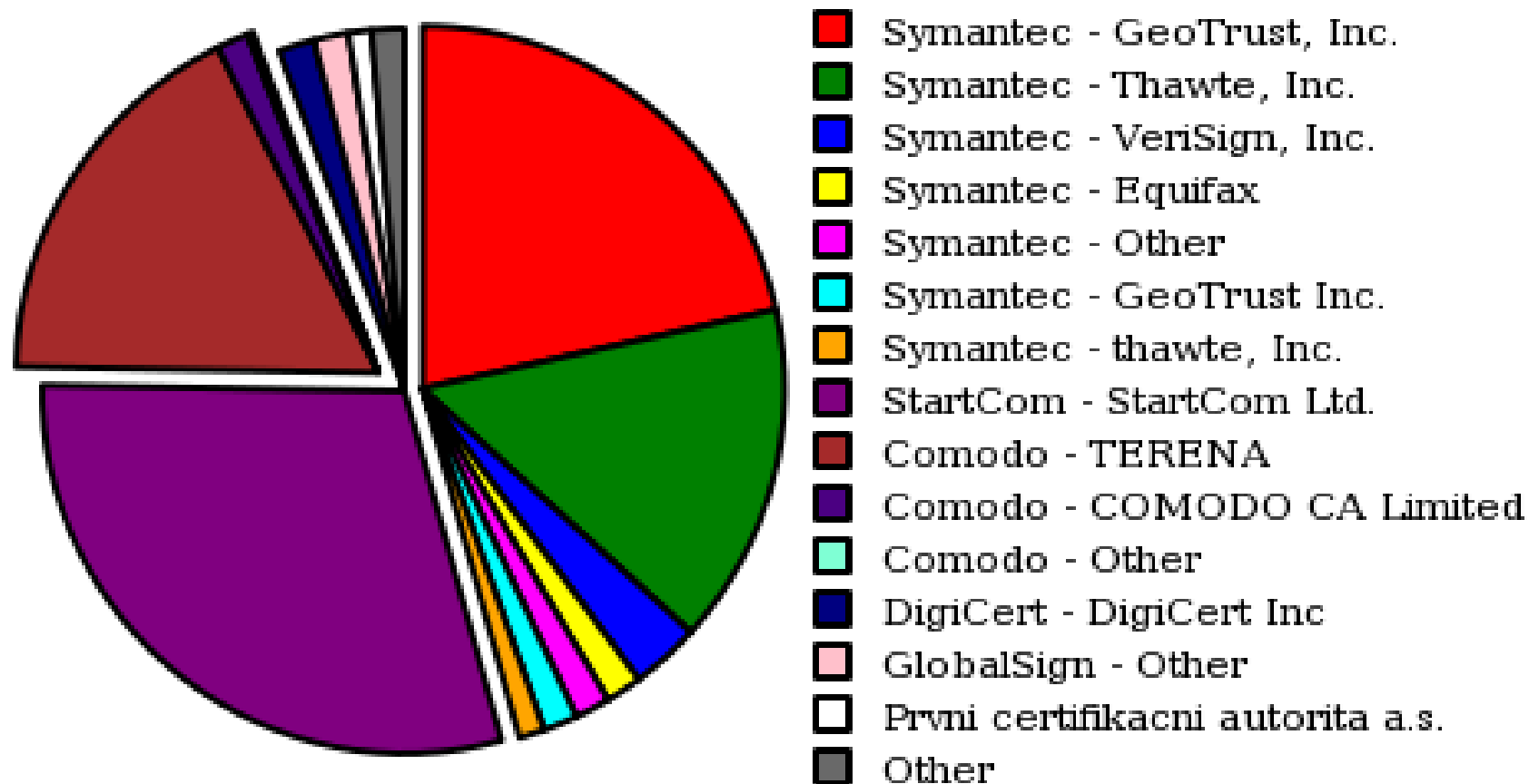
## **Netcraft studie - únor 2011**

celkem 1,660,040 validních SSL certifikátů od CA  
z toho 698,992 certifikátů poskytnuto pod značkami Symantec (42 %)





# Další světové CA



+ GoDaddy (USA)

Česká republika, říjen 2012





## **PostSignum ([www.postsignum.cz](http://www.postsignum.cz))**

Komerční serverové certifikáty, platnost certifikátu 1 rok

Cena: 661 Kč (800 Kč s DPH)

*Od 24. 5. 2010 jsou certifikáty v programu Microsoft Root*

*Firefox: Na pokusu o zařazení se pracuje. Ale nároky tohoto webového prohlížeče jsou dost těžko splnitelné.*

*Acrobat Reader: Na pokusu o zařazení se intenzivně pracuje.*

*17.01.2013 Elektronický podpis v mobilu? Žádný problém*

## **První certifikační autorita, a.s. ([www.ica.cz](http://www.ica.cz))**

Certifikát pro server, 12 měsíců (365 dní), 2048 bitový klíč

Základní cena: 966,94 Kč (1170,- Kč s DPH)

*Součástí systému Windows: I.CA - Accredited Provider of Certification Services*

*9. 1. 2013 V roce 2012 vydala společnost První certifikační autorita celkem 197.424 certifikátů.*

## **Eldentity ([www.eidentity.cz](http://www.eidentity.cz))**

Komerční serverový certifikát, 12 měsíců

(k již vydanému kvalifikovanému systémovému certifikátu)

Cena: 895,- Kč (1.074 Kč s DPH)



# Vlastní CA



```
C:\cygwin\bin\openssl.exe

Standard commands
asn1parse      ca             ciphers        crl             crl2pkcs7
dgst           dh            dhparam        dsa            dsaparam
ec             ecparam       enc            engine         errstr
gendh          gendsa       genrsa         nseq          ocsf
passwd        pkcs12       pkcs7         pkcs8         prime
rand          req          rsa            rsautl        s_client
s_server      s_time      sess_id       smime         speed
spkac         verify      version       x509

Message Digest commands (see the 'dgst' command for more details)
md2           md4           md5            rmd160         sha

Cipher commands (see the 'enc' command for more details)
aes-128-cbc   aes-128-ecb   aes-192-cbc   aes-192-ecb   aes-256-cbc
aes-256-ecb   base64        bf            bf-cbc        bf-cfb
bf-ecb        bf-ofb        cast          cast-cbc      cast5-cbc
cast5-cfb    cast5-ecb    cast5-ofb    des           des-cbc
des-cfb      des-ecb      des-ede      des-ede-cbc   des-ede-cfb
des-ede-ofb  des-ede3     des-ede3-cbc des-ede3-cfb  des-ede3-ofb
des-ofb      des3         desx         rc2           rc2-40-cbc
rc2-64-cbc   rc2-cbc      rc2-cfb      rc2-ecb      rc2-ofb
rc4          rc4-40

OpenSSL> req -new -nodes -keyout myserver.key -out server.csr -newkey rsa:2048
Generating a 2048 bit RSA private key
.....+++
.....+++
unable to write 'random state'
writing new private key to 'myserver.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:_
```



# SSL certifikáty - praxe



Ověření SSL certifikátů z rodiny Symantec



# 3 stupně ověření SSL certifikátů

- Doménové ověření (DV)

nejlevnější SSL, vystavení již od 5 minut

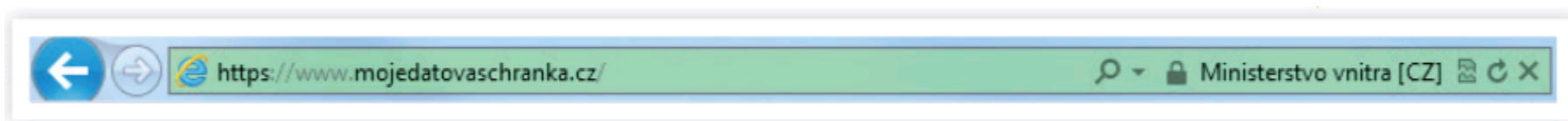
| Vloženo        | Splatnost | Upomínka | Zaplaceno      | Zažádáno       | Vydáno         |
|----------------|-----------|----------|----------------|----------------|----------------|
| 18.02.13 23:26 | 28.02.13  | -        | 18.02.13 23:27 | 18.02.13 23:27 | 18.02.13 23:30 |

- Ověření organizace (OV)

vyšší důvěryhodnost, kompletní identifikace společnosti

- Rozšířené ověření (EV)

uživatelsky nejbezpečnější forma komunikace - zelená barva

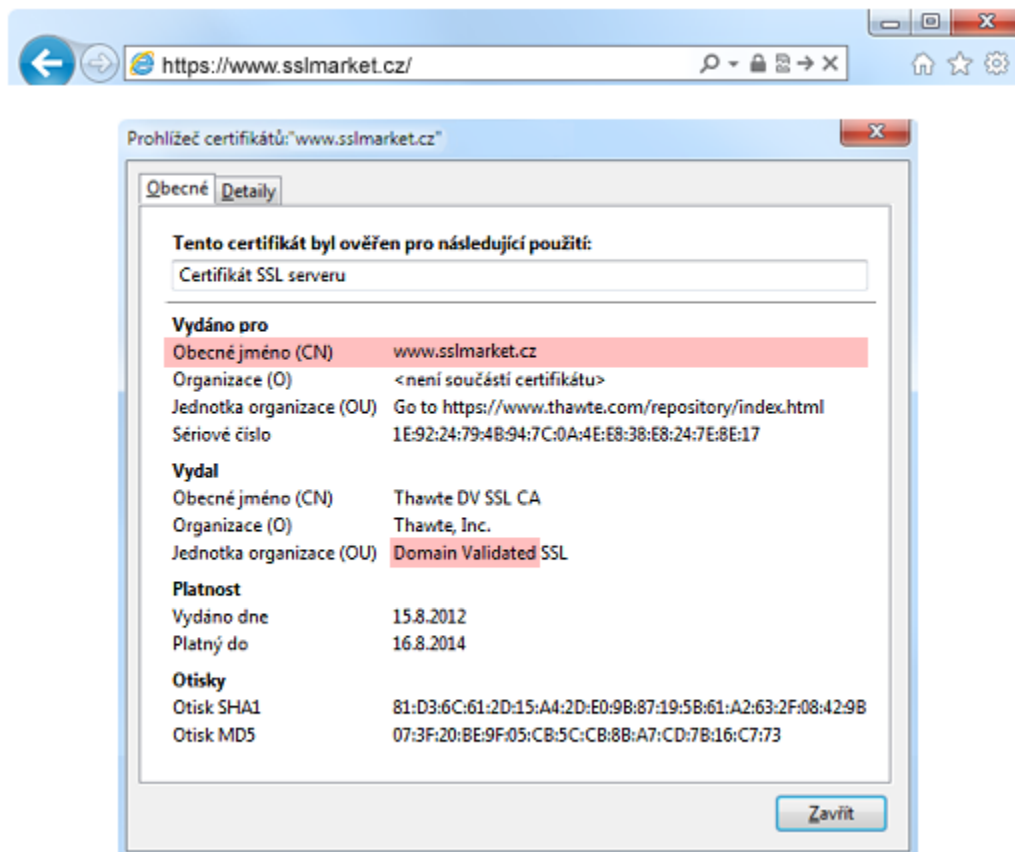




# Typy ověření



# Doménové ověření (DV)





# Doménové ověření

- Na zvolenou adresu na doméně zaslán ověřovací e-mail
  - admin@
  - administrator@
  - hostmaster@
  - postmaster@
  - webmaster@
  - E-mail vlastníka domény (veřejný)



# Doménové ověření

- Po potvrzení přes zaslaný odkaz je certifikát vydán

Dobry den,

dekujeme za Vase objednani SSL 123 THAWTE certifikatu.

Nyni je nutne provest overeni certifikatu primo na strankach THAWTE. Toto overeni certifikatu by mela provadet osoba, ktera o certifikat zazadala:

```
=====
thawte SSL Certificate:          SSL123
Issued To:                      https://webftp.czechia.com
Your Order Number:              8626227
Name:                           [REDACTED]
E-mail:                         [REDACTED]
Phone:                          +420543257244
=====
```

Odkaz pro overeni certifikatu:

<https://products.thawte.com/orders/A.do?p=AWXnNWTxNkKcQzZhHgkgV>



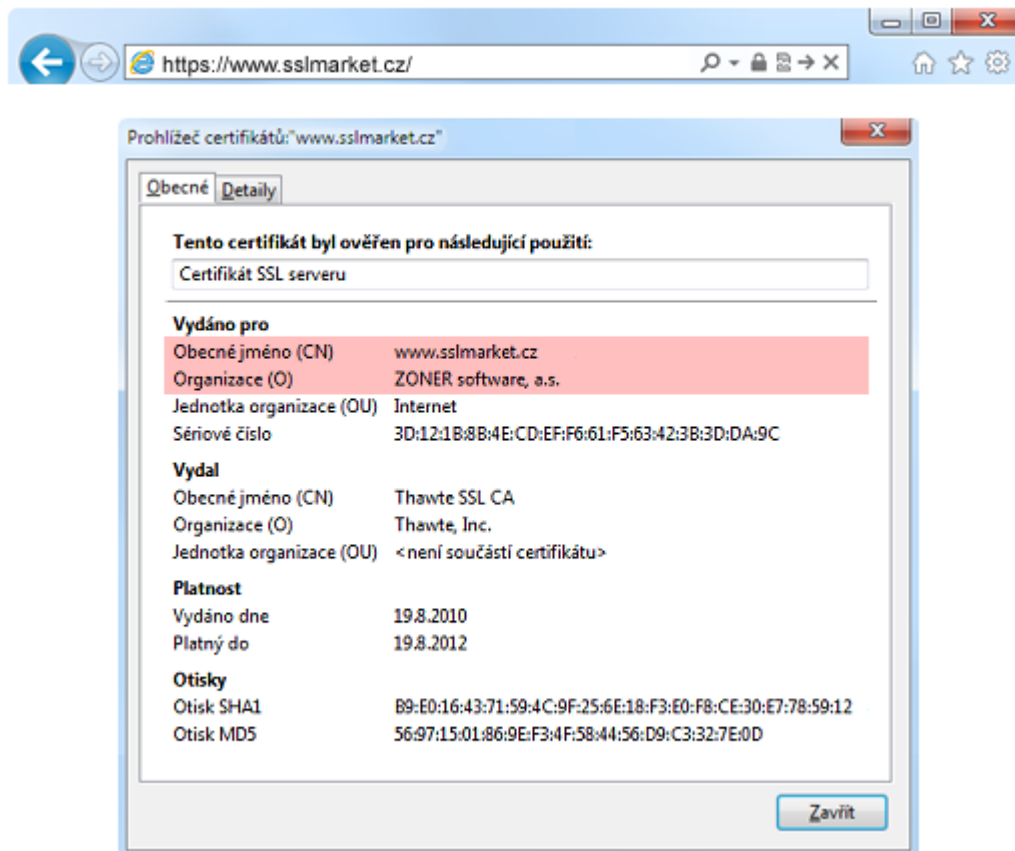


# Doménové ověření

Výjimky, které mohou nastat:

- Název domény je na blacklistu (až 10.000 slov!),  
nebo chráněn např. Facebook, bank, IBM  
-> nutné další ověření
- Namátková kontrola

# Ověření organizace (OV)



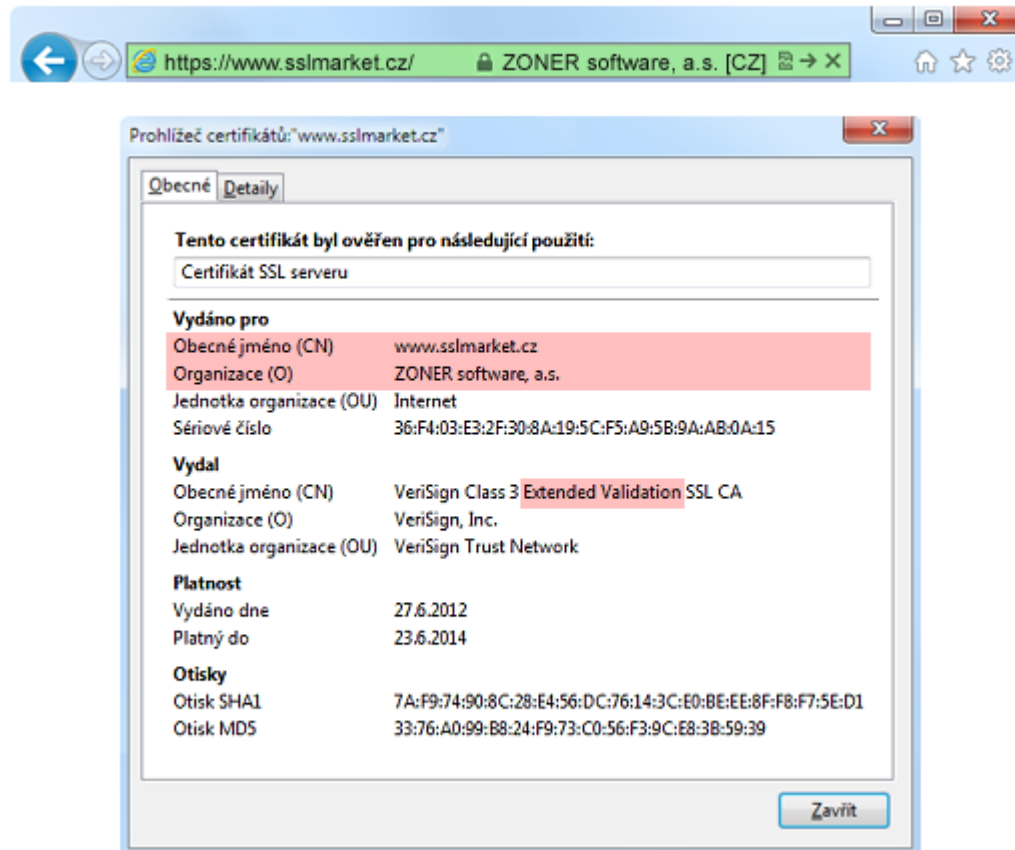


# Ověření organizace

## OV ověření má 3 části:

- Ověření registrace (Ares)
- Ověření vlastnictví domény (WHOIS)
- Ověřovací hovor (číslo z 1188.cz nebo Zlaté Str.)
  - Voláno osobě pro autorizaci

# Rozšířené ověření (EV)





# Rozšířené ověření

## Pouze u EV certifikátů – Zelený adresní řádek

Ověření má 5 částí:

- Zaslání souhlasu s podmínkami ověření
- Ověření registrace spol. (Ares + více zdrojů)
- Ověření vlastnictví domény (WHOIS)
- Tel. ověření ověřované osoby u personálního man.
- Závěrečný hovor (číslo z 1188.cz nebo Zlaté Str.)



# FAQ

1. Budou mi volat v noci? 
2. Když hovor zmeškám, objednávka propadá? 
3. Budu muset k notáři? 
4. Budu posílat kopie osobních dokladů? 
5. Budou mé osobní nebo kontaktní údaje v certifikátu? 
6. Budou volat anglicky? 
7. Budou mě z něčeho zkoušet? 



# Výhody SSLmarketu

- asistence při ověření a komunikaci s CA
- kvalifikovaná zákaznická podpora v češtině
- ceny výrazně nižší než u CA
- fakturace v Kč
- přehledná česká administrace



# SECURITY 2013

21. ročník konference o bezpečnosti v ICT

## Děkujeme za pozornost.

**ZONER software, a.s.**

**Petr Komárek, Jindřich Zechmeister**

[petr.komarek@zoner.cz](mailto:petr.komarek@zoner.cz), [jindra@zoner.cz](mailto:jindra@zoner.cz)

