

# Praktické aspekty kryptografie v IT

MV707K Informační technologie v právní praxi

Zdeněk Říha

# Počítačová bezpečnost

1. Důvěrnost  
(bráníme neautorizovanému čtení dat)
2. Integrita  
(bráníme neautorizované modifikaci dat)
3. Dostupnost  
(data/systémy jsou dostupné podle plánu)

# Kryptografie

- Symetrická
  - Obě strany používají stejný (tajný) klíč
- Asymetrická
  - Existují různé klíče (soukromý/veřejný)
- Bezklíčová
  - Generování náhodných čísel
    - Náhodná vs. pseudonáhodná čísla
  - Hašovací funkce
    - Otisk dat (libovolný vstup, výstup fixní délky)
    - MD5, SHA-1, SHA-2, SHA-3

# Symetrické šifrování

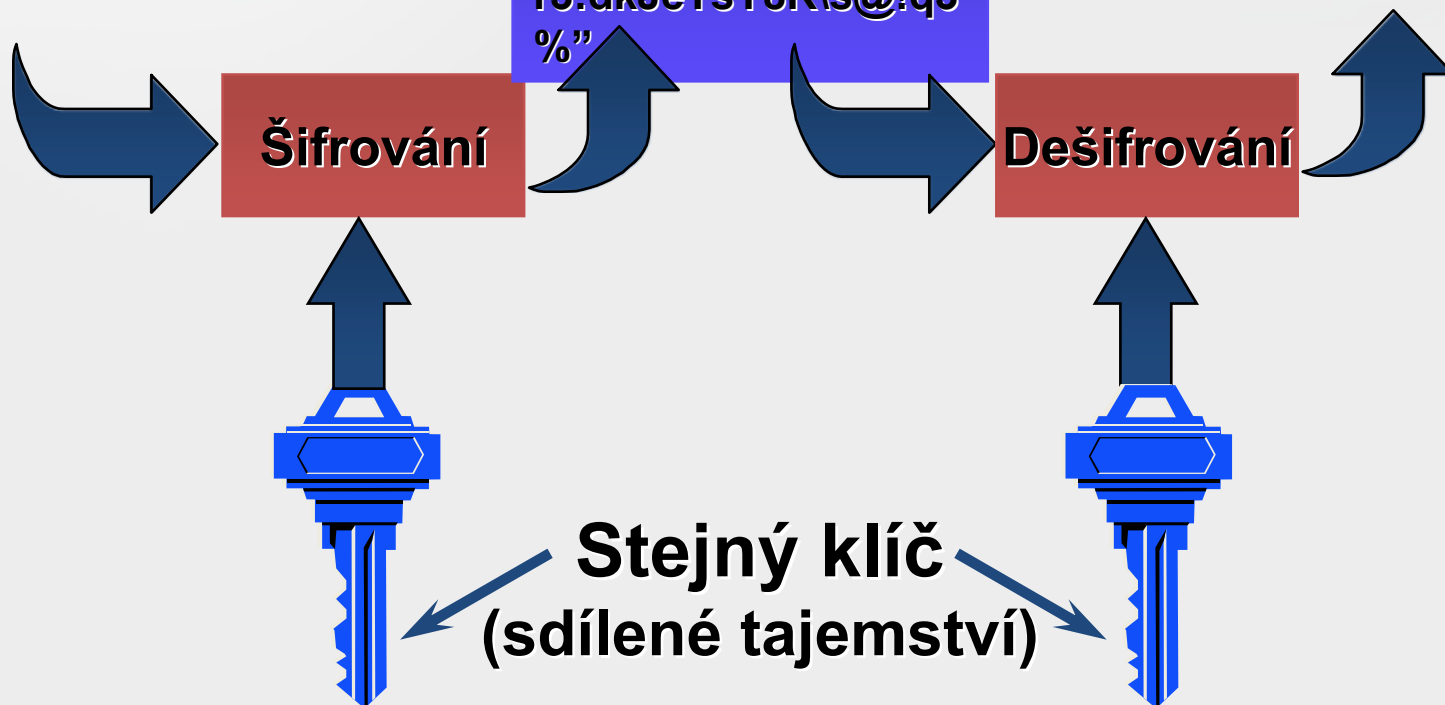
Čistý text

“Operace začne dnes v 18:00.”

Šifrový text

“AxCv;5bmEseTfid3)  
fGsmWe#4^,sdgfMwi  
r3:dkJeTsY8R\!q3  
%”

“Operace začne dnes v 18:00”



# Symetrické šifrování

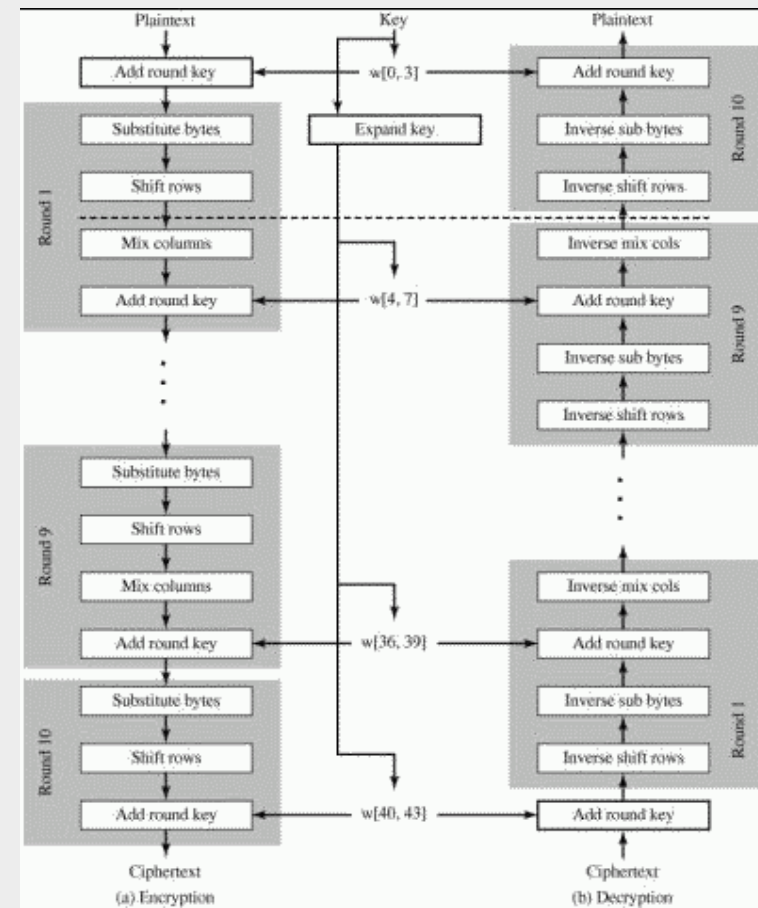
- Výhody
  - Rychlost (asi 1000 rychlejší než asymetrické šifrování)
- Nevýhody
  - Klíč je tajný a je třeba jej udržovat v tajnosti
  - Klíč je třeba domluvit předem (a tak aby se jej nedozvěděl nikdo jiný)

# Symetrické šifrovací algoritmy

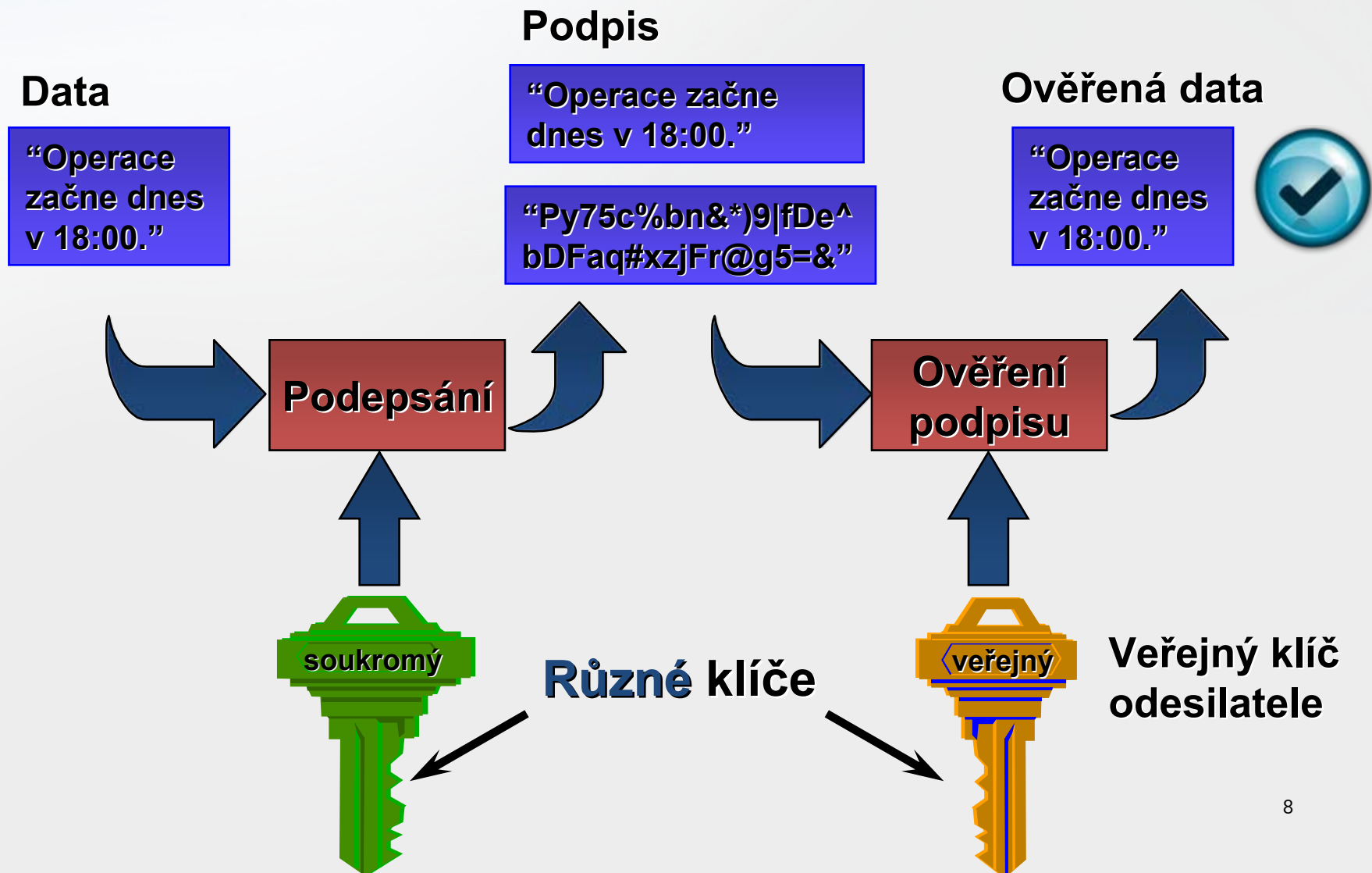
- DES
  - Klíč: 56 bitů
  - Šifruje bloky dat o velikosti 64 bitů
  - Dnes nedostatečně bezpečné
  - Lze kombinovat DES se 2 nebo 3 různými klíči, pak je bezpečné.
    - Nazývá se TrippleDES nebo 3DES
- Blowfish, Twofish
  - Rychlé a bezpečné algoritmy

# Symetrické šifrovací algoritmy

- AES (Advanced Encryption Standard)
  - Vítěz soutěže NIST z let 1997-2000
  - Původně se jmenoval Rijndael
  - Klíče o velikosti 128, 192 nebo 256 bitů
  - Rychlý a bezpečný



# Asymetrická kryptografie – digitální podpis





# Asymetrická kryptografie – šifrování

Čistý text

“Operace začne dnes v 18:00.”

Šifrový text

“Py75c%bn&\*)9|fDe^  
bDFaq#xzjFr@g5=&n  
mdFg\$5knvMd’rkveg  
Ms”

Výstupní čistý text

“Operace začne dnes v 18:00.”

Šifrování

Dešifrování

veřejný

Různé klíče

soukromý

Veřejný klíč  
příjemce

# Asymetrická kryptografie

- Výhody
  - Veřejný klíč nemusí být udržován v tajnosti
- Nevýhody
  - Pomalé algoritmy
  - Distribuce veřejného klíče
    - Ač není tajný, je důležité zajistit jeho integritu
    - Pokud někomu podstčím špatný veřejný klíč, pak bude u podvržených zpráv indikován korektní digitální podpis !!!

# Asymetrické šifrovací algoritmy

- RSA (Rivest Shamir Adleman)
  - Založen na problému faktorizace velkých čísel
- DSA (Digital Signature Algorithm)
  - Založen na problému diskrétního logaritmu
- ECDSA
  - Obdoba DSA pro eliptické křivky
  - Toto už je složitá matematika... :-)

# Matematické základy RSA

- Násobení prvočísel snadné, ale faktorizace čísel výpočetně náročná.
- Velká prvočísla  $p$  a  $q$ ,  $n = p \cdot q$ ,  $\phi(n) = (p-1)(q-1)$ .
- Zvolíme velké  $e$  takové, že  $\gcd(e, \phi(n)) = 1$ .
- Spočítáme  $d = e^{-1} \pmod{\phi(n)}$ .
- Veřejný klíč:  $n, e$ .  
Neveřejné parametry:  $p, q, d$ .
- Šifrování (ověření podpisu):  $c = w^e \pmod{n}$ .
- Dešifrování (podepisování):  $w = c^d \pmod{n}$ .

# Příklad veřejného klíče RSA

The screenshot shows a Windows 'Certifikát' (Certificate) dialog box with the 'Obecné' (General) tab selected. The 'Zobrazit:' (Show) dropdown is set to '<Vše>' (All). A table lists certificate fields and their values. The 'Veřejný klíč' (Public Key) field is highlighted, showing 'RSA (1024 Bits)'. Below the table, the hexadecimal representation of the public key is displayed in a text area.

Pole	Hodnota
Sériové číslo	70 b0 7d ce 2c 83 64 45 9d 78...
Algoritmus podpisu	sha1RSA
Vystavitel	IFX CSCA Test Cert, DE
Platnost od	9. května 2006 1:00:00
Platnost do	9. května 2007 0:59:59
Předmět	IFX CSCA Test Cert, DE
<b>Veřejný klíč</b>	<b>RSA (1024 Bits)</b>
Identifikátor klíče úřadu	ID klíče=59 d3 6a 4a 9d 00 5d ...

30 81 8a 02 81 81 00 94 3e d0 db b3 91 60 d8 28 ad e5 ac 05 fa cf 94 28  
18 58 fd c9 cc e9 54 23 8d 95 12 11 46 a3 80 eb b0 a2 a2 c9 cb 8a 1a d9  
be 76 07 d2 0b 0d cd 31 6f 37 5a a0 f9 8a ef ae 47 df d1 1c a2 77 38 c5  
3d a3 25 7c 7f cf 96 a2 ad 84 98 a8 b0 de d0 d5 25 a4 3b 43 55 bb d6 dc  
c3 df bb b0 be 84 8f 6a ae ac 5f 09 74 e4 78 fe c0 d9 f0 51 c2 77 d3 7b  
55 6f 06 35 29 6e a8 4e 0f c7 4a c7 41 e0 87 02 04 00 01 00 01

Buttons: Upravit vlastnosti..., Kopírovat do souboru..., OK

# Šifrování – velikost klíče

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA <sup>23</sup> 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$ ; $N = 160$	Min.: $k = 1024$	Min.: $f = 160$
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: $k = 2048$	Min.: $f = 224$
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: $k = 3072$	Min.: $f = 256$

Zdroj:  
NIST SP800

# Distribuce veřejného klíče

- Osobní předání
  - Flash, CD, ...
- Umístění na web
  - Webová stránka osoby, firmy, ...
- Pošleme spolu s podepsanými daty
  - Přiložíme k podpisu
- Pokud nedostaneme klíč od daného člověka osobně, jak poznáme, že klíč patří opravdu té osobě?
  - Co když někdo pošle podvrhnutý email?
  - Co když někdo hackne webovou stránku?

# Certifikační autorita

- Ověří totožnost žadatele
  - FO nebo PO
- Zkontroluje veřejný klíč žadatele
  - Žádost o vydání certifikátu digitálně podepsána
- CA nekontroluje důvěryhodnost žadatele...
- Vydá certifikát veřejného klíče
  - Digitálně podepsaná vazba osoby a veřejného klíče
  - Digitálně podepsáno certifikační autoritou
  - Existuje několik standardů
    - X.509 (podporováno zákonem o DP)
    - PGP/GnuPG



# Certifikát dle X.509

- Verze (standardu), sériové číslo (od dané CA)
- Vystavitel (CA)
- Předmět (FO, PO)
- Časová platnost (od, do)
- Veřejný klíč (RSA - nejčastější, DSA, ECDSA)
- Podepisovací algoritmus (včetně hašovací funkce)
- Případná omezení
- Digitální podpis výše uvedeného od CA

# Certifikační autorita

- Jak nám CA pomůže v distribuci veřejného klíče?
  - Nemusíme osobně předávat veřejný klíč na CD
  - K digitálnímu podpisu stačí přiložit certifikát od CA
- Pokud věříme dané CA, pak stačí ověřit digitální podpis certifikátu a známe veřejný klíč „předmětu“
  - Pro ověření podpisu certifikátu potřebujeme veřejný klíč CA.
  - Kde ten získáme?
    - Na webu CA, ministerstva vnitra apod. :-)
    - Osobně na pobočce CA
- Co s certifikátem CA, které neveríme?
  - Nic
- Musí žadatel věřit CA?
  - Ani moc ne ...

# Certifikační autority

- CA = „poskytovatel certifikačních služeb“
- CA si můžete vytvořit i doma (OpenSSL)
  - Kdo jí ale bude důvěřovat...
- Kvalifikovaný poskytovatel certifikačních služeb
  - Určité požadavky + informovat MV ČR
- Akreditovaný poskytovatel certifikačních služeb
  - Akreditace MV ČR
- Aktuálně akreditovány následující CA:
  - I. CA
  - Postsignum
  - elidentity

# Počítačová bezpečnost – další pojmy

- Autentizace
  - Ověření identity subjektu (uživatele, počítače,...)
- Autorizace
  - Přístupové právo pro nějakou akci

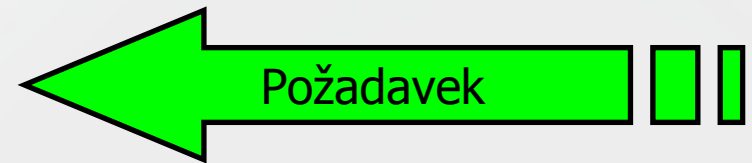
# Webová bezpečnost

http vs. https

# HTTP komunikace

- GET / HTTP/1.0
- Connection: Keep-Alive
- User-Agent: Mozilla/4.7 [en]
- (X11; U; FreeBSD 3.4-STABLE i386)
- Host: www.rtfm.com
- Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, \*/\*
- Accept-Encoding: gzip
- Accept-Language: en
- Accept-Charset: iso-8859-1, \*, utf-8
- *(blank line)*

**Hlavičky**



# HTTP komunikace

- Standardně není HTTP požadavek ani odpověď serveru nijak šifrovaná
- To se týká i:
  - Uživatelských jmen a hesel
  - Osobních údajů, které vkládáte do formulářů
    - Adresa
    - Datum narození
    - Rodné číslo
- Pokud má někdo přístup k síťové infrastruktuře, kudy data procházejí, může je odposlouchávat.
  - To se týká i hackerů, kteří se dostali k přepínačům, směrovačům po cestě...

# Příklad HTTP komunikace

- Start/spustit/cmd
- telnet www.seznam.cz 80
- GET / [enter] [enter]

```
C:\WINDOWS\system32\cmd.exe

<!DOCTYPE html>

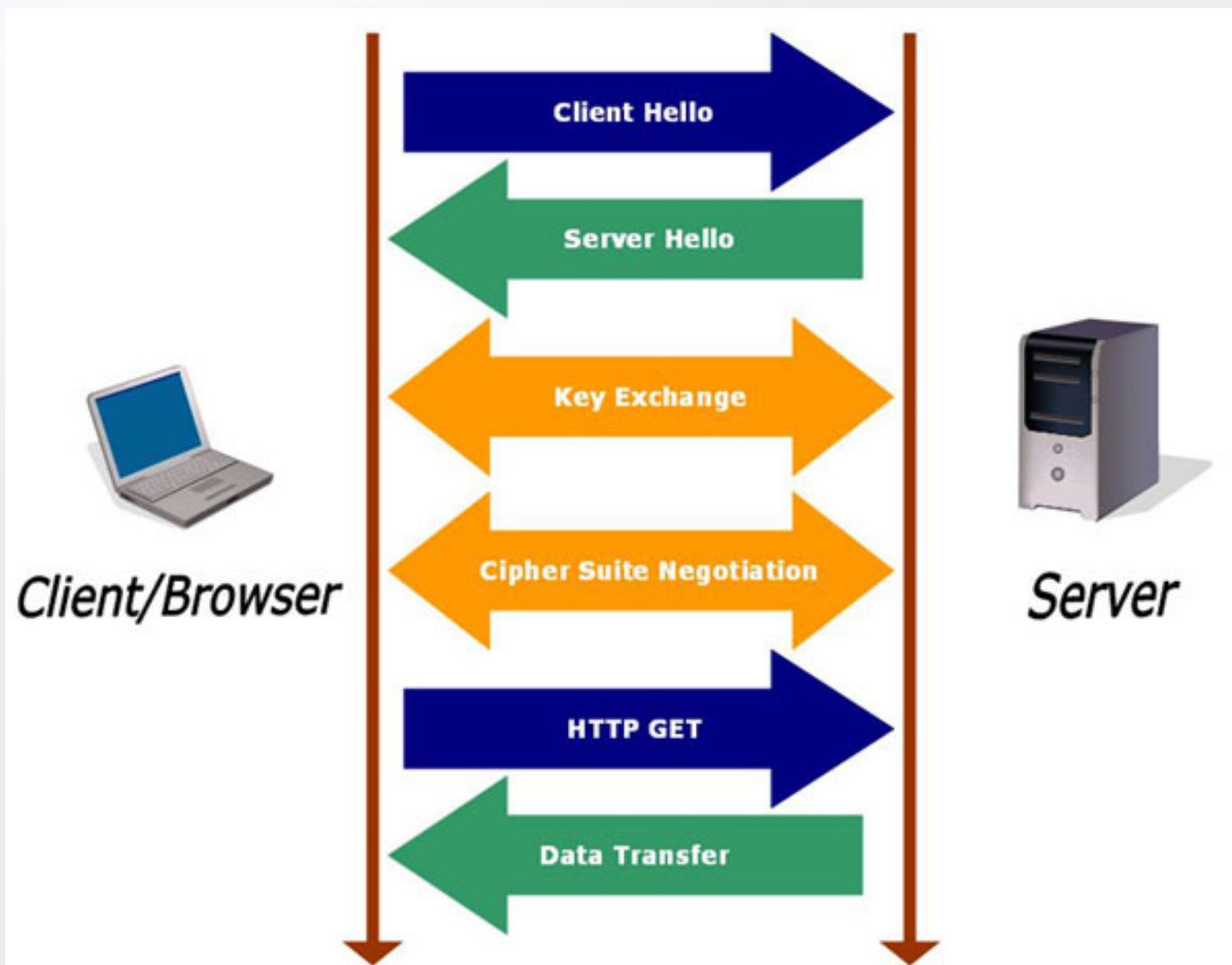
    <html xmlns:fb="http://www.facebook.com/2008/fbml">
        <head>
            <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
            <meta http-equiv="%UA-Compatible" content="IE=8" />
            <title>Seznam ôçô Najdu
            tam, co hled|ím</title>
            <link rel="alternate" type="application/rss+xml" title="
            Seznam.cz" href="http://seznam.sblog.cz/rss.xml" />
            <link rel="shortcut icon" hr
            ef="/st/img/favicon.ico" /> <link rel="openid2.provider openid.server" href="htt
            p://id.szn.cz/openidserver" /> <meta http-equiv="%X-RDS-Location" content="http:
            //id.seznam.cz/yadis" /> <link rel="stylesheet" href="/st/2.26.3/css/0-homepage.
            css?48" media="all" type="text/css" /> <script type="text/javascript" /> /* <![CDA
            TA] /* if(typeof SZN != "object") { SZN = new Object(); }; if(typeof SZN.CONF !=
            "object") { SZN.CONF = new Object(); }; SZN.CONF = { SERVICE_URL : 'http://www.
            seznam.cz', PATH_IMG : '/st/img', FRIENDS_URL : '/misc.fcgi?akce=hp_seznam_js&ha
            sh=', /*- nastaveni pro hledani*/ SEARCH_INTERNET_ID : 1, SEARCH_TAB_COUNT : 5-1
```



# HTTPS komunikace

- HTTPS = HTTP + SSL
- HTTPS komunikace je zabezpečena protokolem SSL/TLS.
- SSL/TLS zajišťuje
  - Důvěrnost přenášených dat
    - Data jsou symetricky šifrována
  - Integritu přenášených dat
    - Data jsou zabezpečena pomocí MAC (Message Authentication Code)
  - Autentizaci
    - Defaultně je povinná autentizace serveru

# Průběh SSL/TLS



# Autentizace v HTTPS

- Standardně je povinná autentizace serveru, tj. když se klient (např. webový prohlížeč) připojuje k (webovému) serveru má jistotu, že se připojil ke správnému serveru.
  - To je důležité při zadávání hesel, čísel platebních karet apod.
  - Phishing ...

# Autentizace v HTTPS

- Server posílá certifikát serveru.
- Certifikát uvádí jméno serveru a veřejný klíč serveru.
- Protokol SSL/TLS dále ověří, zda server má k dispozici soukromý klíč odpovídající certifikovanému veřejnému klíči.
  - Data se šifrují veřejným klíčem serveru, jen správný server bude umět dešifrovat.

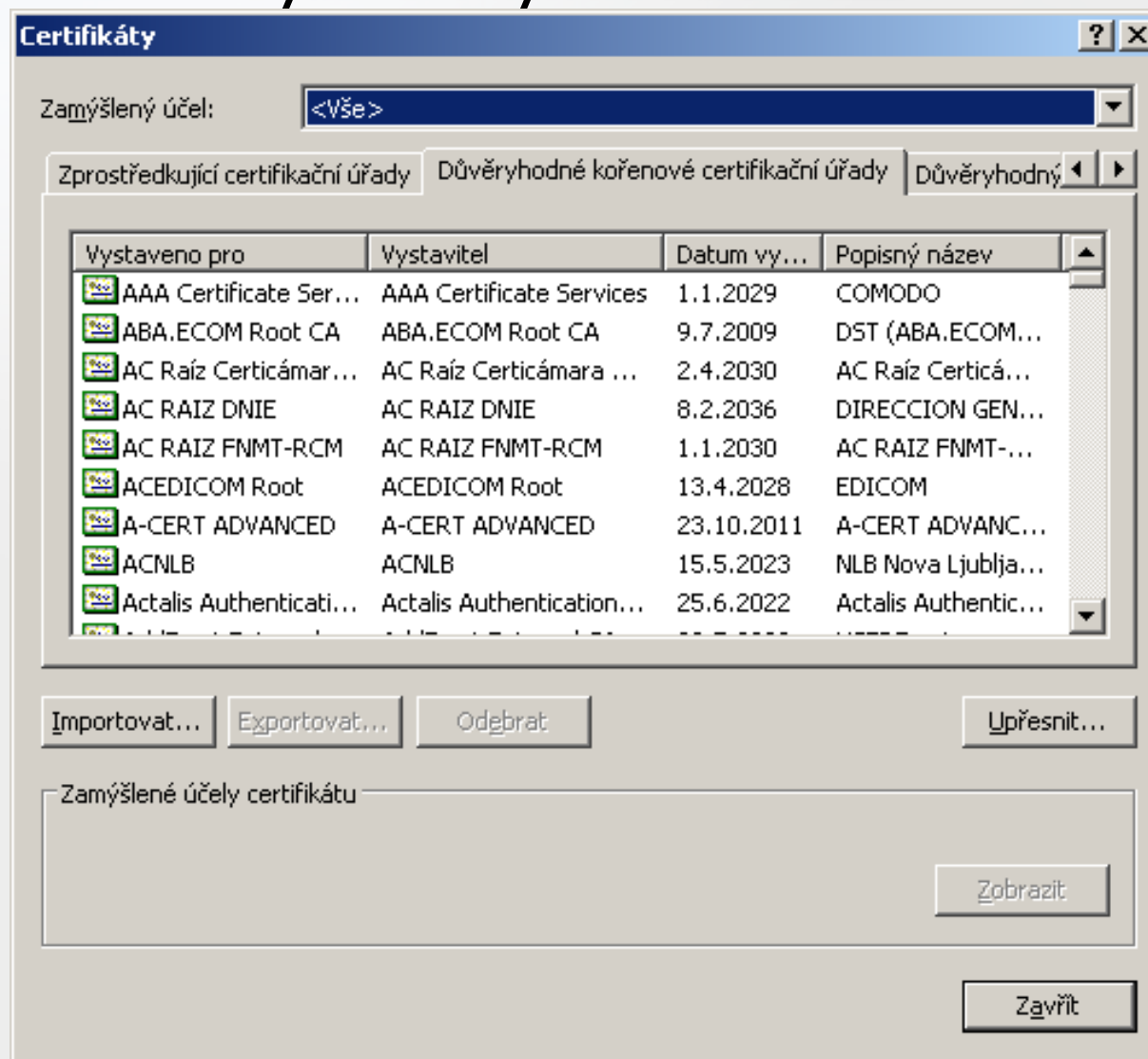
# Certifikát

- Certifikát serveru je podepsán vydávající certifikační autoritou (CA).
- Tato podepisující CA musí být považována za důvěryhodnou.
  - A její certifikát musí mít uložen v seznamu důvěryhodných CA...

# Seznam důvěryhodných CA

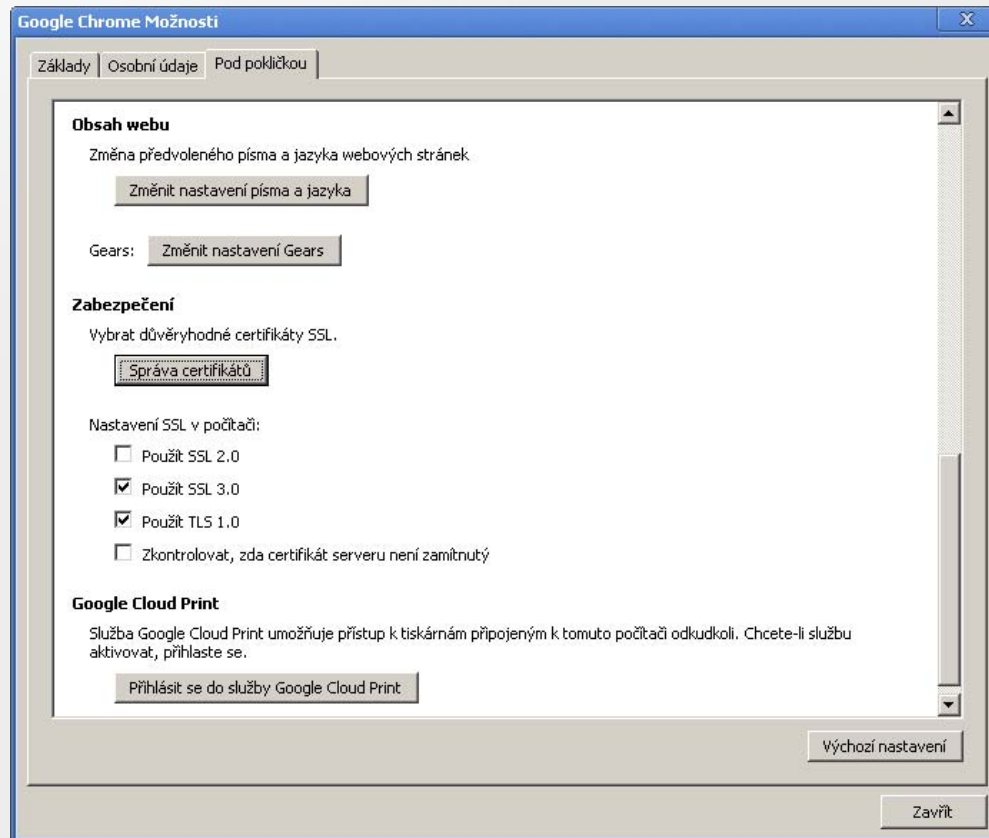
- Seznamy jsou uloženy v prohlížečích (IE bere seznam z OS)
- Tyto seznamy můžete konfigurovat.
- Iniciálně jsou tam i desítky CA o kterých jste nikdy neslyšeli...
  - Těm všem automaticky důvěřujete 😊

# Seznam důvěryhodných CA



# Seznam důvěryhodných CA

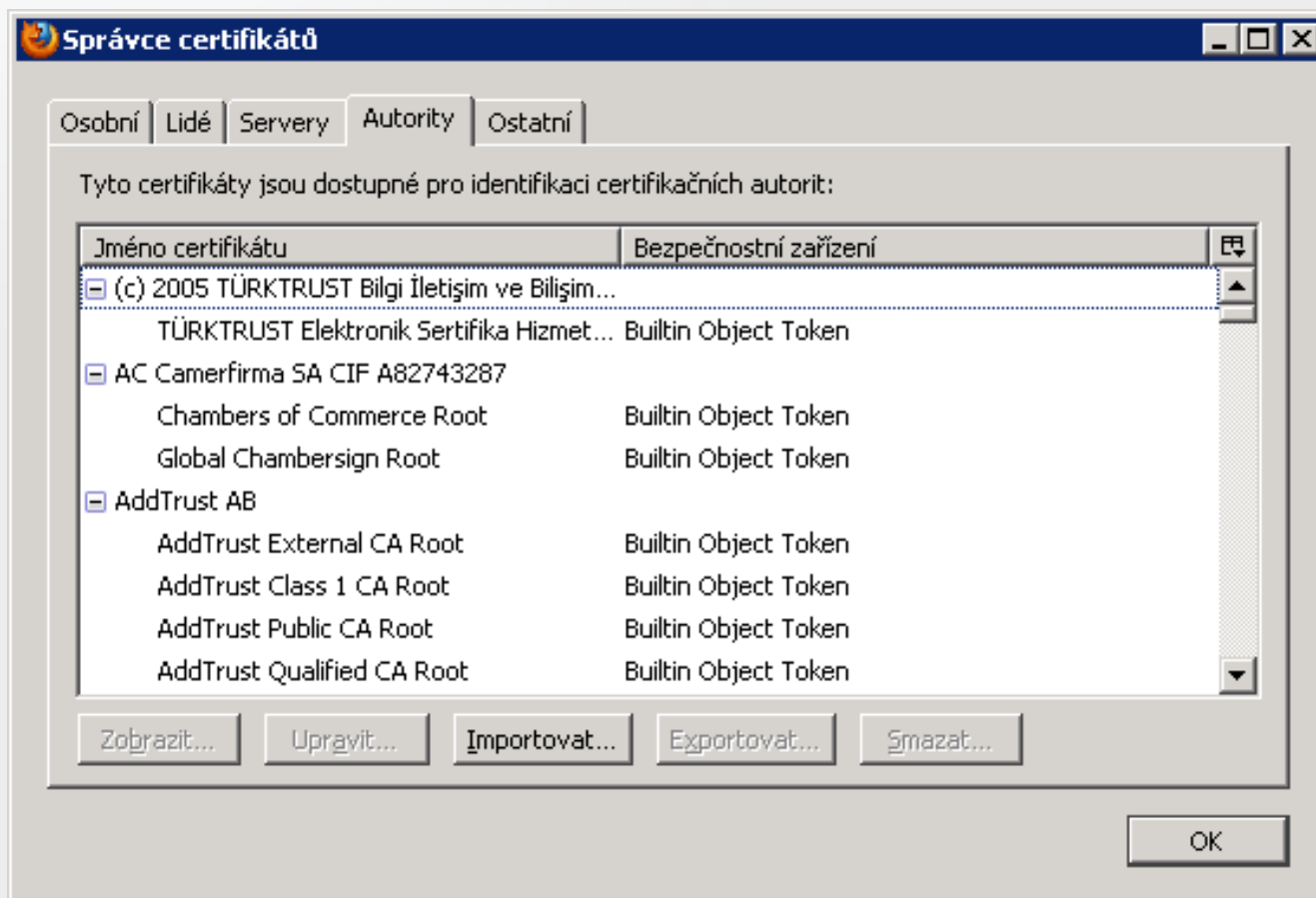
- Podobně v Google Chrome



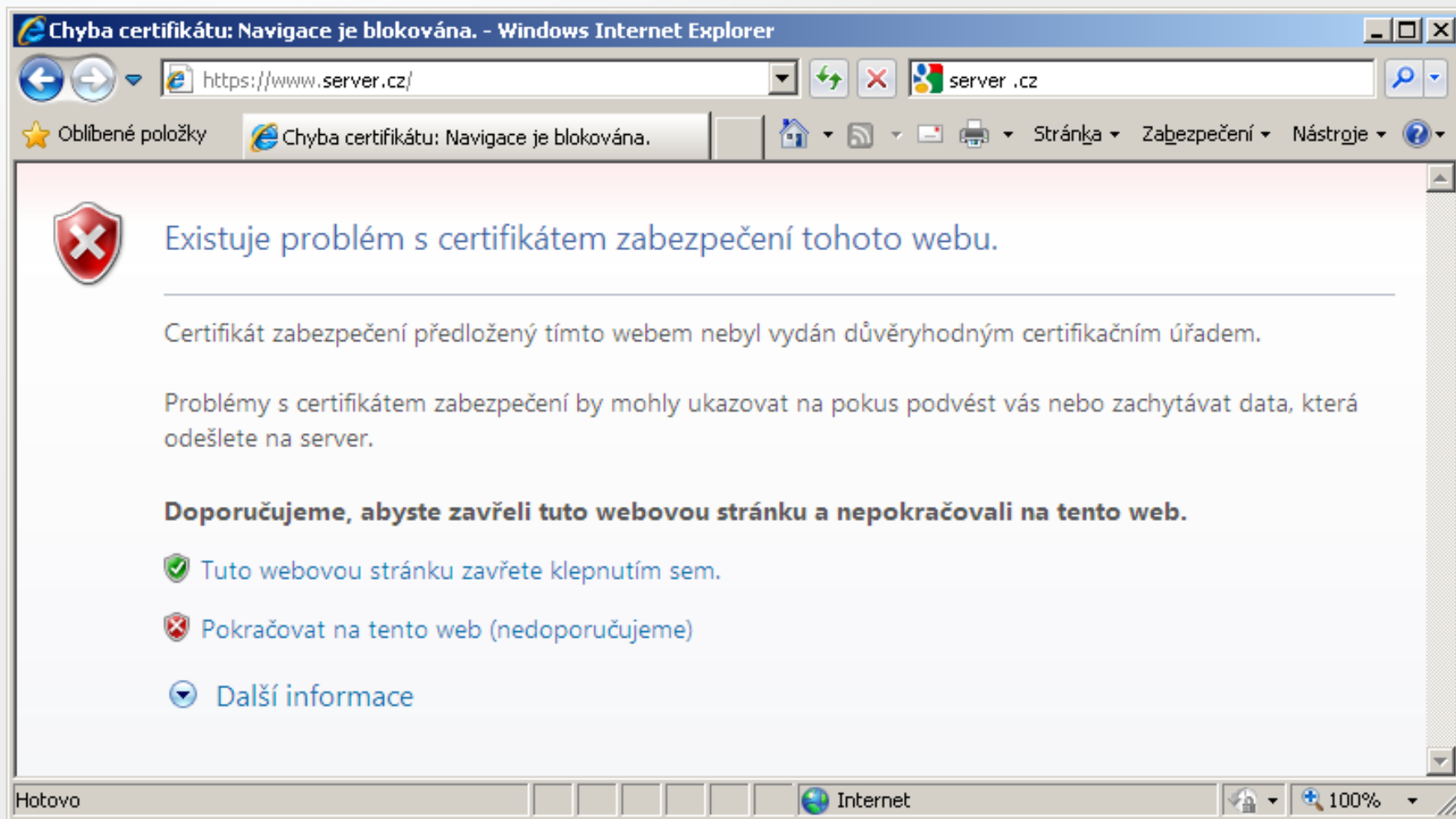


# Seznam důvěryhodných CA

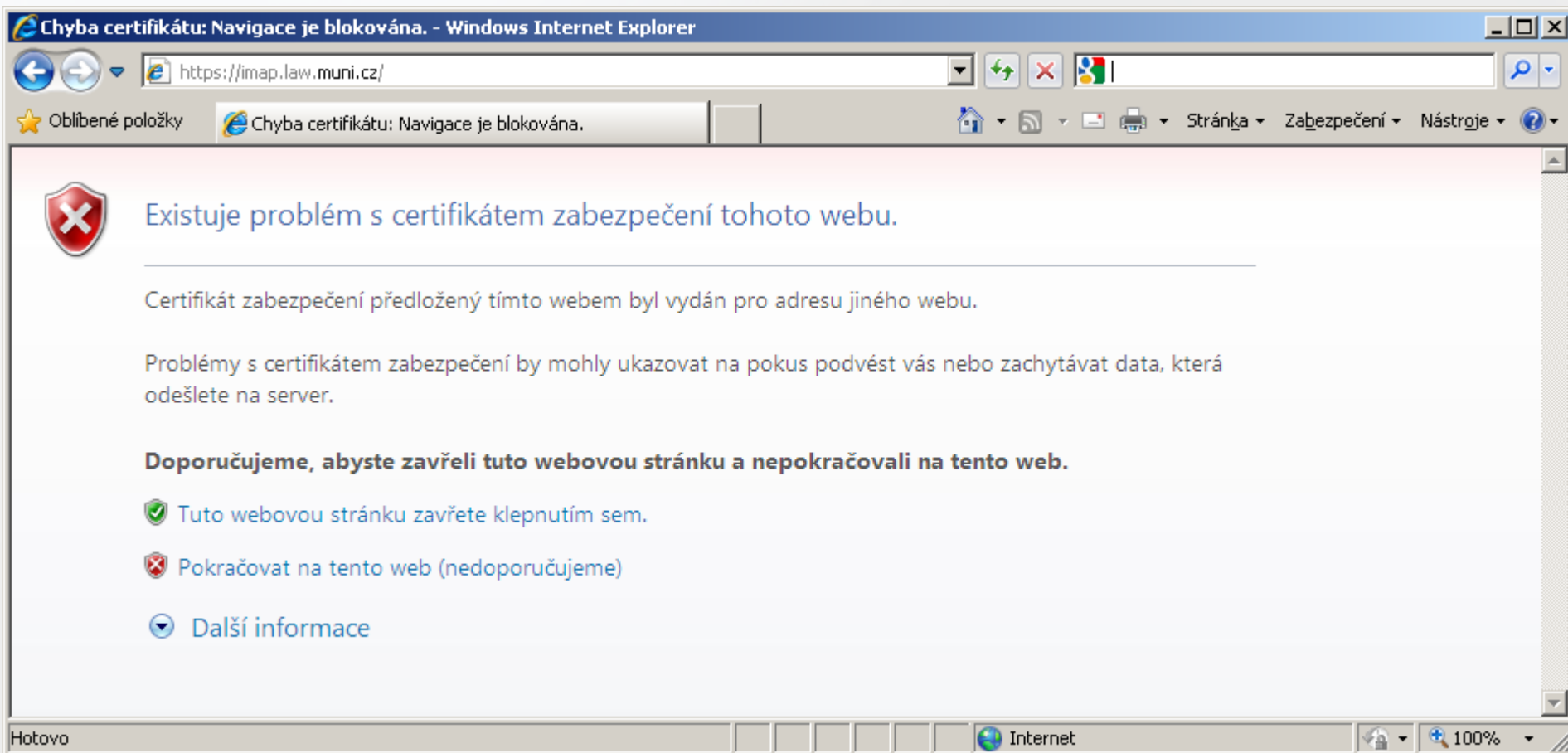
- Mozilla Firefox



# Certifikát nepodepsán důvěryhodnou CA



# Certifikát určen pro jiný web...




The screenshot shows a Windows Internet Explorer browser window with the title "Chyba certifikátu: Navigace je blokována. - Windows Internet Explorer". The address bar contains the URL "https://imap.law.muni.cz/". The main content area displays a security warning with a red shield icon containing a white 'X'. The text reads: "Existuje problém s certifikátem zabezpečení tohoto webu." followed by "Certifikát zabezpečení předložený tímto webem byl vydán pro adresu jiného webu." and "Problémy s certifikátem zabezpečení by mohly ukazovat na pokus podvést vás nebo zachytávat data, která odešlete na server." Below this, a bold recommendation states: "Doporučujeme, abyste zavřeli tuto webovou stránku a nepokračovali na tento web." Three options are listed: a green checkmark icon for "Tuto webovou stránku zavřete klepnutím sem.", a red 'X' icon for "Pokračovat na tento web (nedoporučujeme)", and a blue downward arrow icon for "Další informace". The status bar at the bottom shows "Hotovo" and "Internet".

Chyba certifikátu: Navigace je blokována. - Windows Internet Explorer

https://imap.law.muni.cz/

Oblíbené položky Chyba certifikátu: Navigace je blokována.




Stránka Zabezpečení Nástroje

 Existuje problém s certifikátem zabezpečení tohoto webu.

Certifikát zabezpečení předložený tímto webem byl vydán pro adresu jiného webu.

Problémy s certifikátem zabezpečení by mohly ukazovat na pokus podvést vás nebo zachytávat data, která odešlete na server.

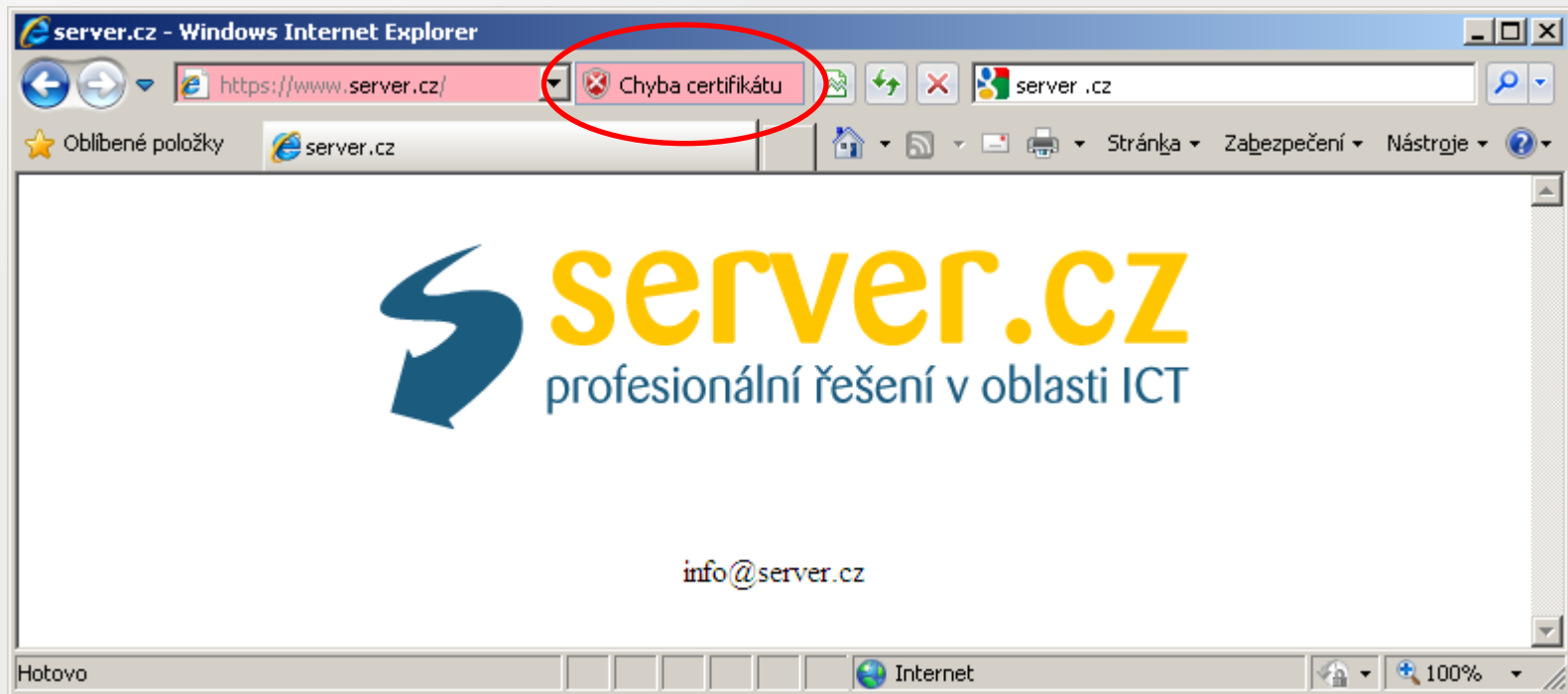
**Doporučujeme, abyste zavřeli tuto webovou stránku a nepokračovali na tento web.**

-  Tuto webovou stránku zavřete klepnutím sem.
-  Pokračovat na tento web (nedoporučujeme)
-  Další informace

Hotovo Internet 100%

# Certifikát nepodepsán důvěryhodnou CA

- Pokud přesto pokračujete:
  - V IE červené URL, ...
  - a indikováno, že certifikát je chybný



# CA lze přidat mezi důvěryhodné

## Upozornění zabezpečení



Rozhodli jste se nainstalovat certifikát z certifikačního úřadu (CÚ), který vyžaduje:

K101 CA

System Windows neověřil, zda je certifikát pochází skutečně z K101 CA. Měli byste jeho původ potvrdit dotazem na K101 CA. Následující číslo vám při procesu pomůže:

Miniatura (sha1): 87C6B4ED 60CCC638 DB0464A1 F607BE7B 8FA6CE31

Upozornění:

Jestliže nainstalujete tento kořenový certifikát, bude systém Windows automaticky důvěřovat všem certifikátům vydaným tímto certifikačním úřadem. Instalace certifikátu s nepotvrzenou miniaturou představuje bezpečnostní riziko. Klepnutím na tlačítko Ano toto riziko uznáváte.

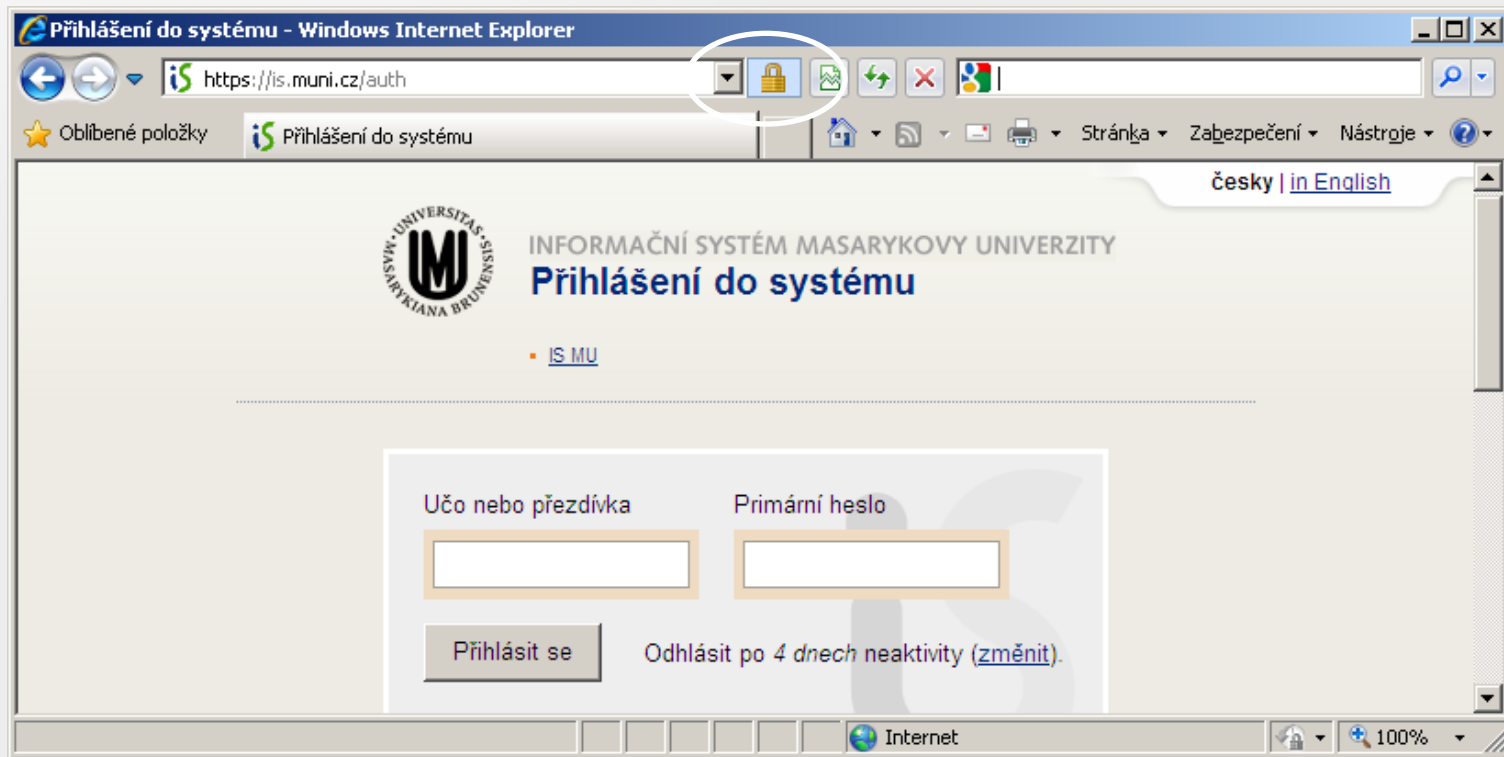
Chcete tento certifikát nainstalovat?

Ano

Ne

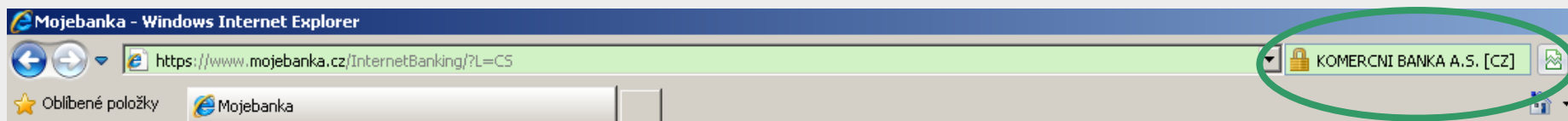
# Certifikát podepsán důvěryhodnou CA

- Certifikát je v pořádku:
  - V IE bílé URL,...
  - a znak zámku



# EV certifikát podepsán důvěryhodnou CA

- EV (extended validation) certifikát má vyšší míru důvěry ve shodu vlastníka domény s webovým serverem.
- Technicky ten stejný X.509 (s drobnou poznámkou), ale CA si více žadatele o EV certifikát „proklepne“.

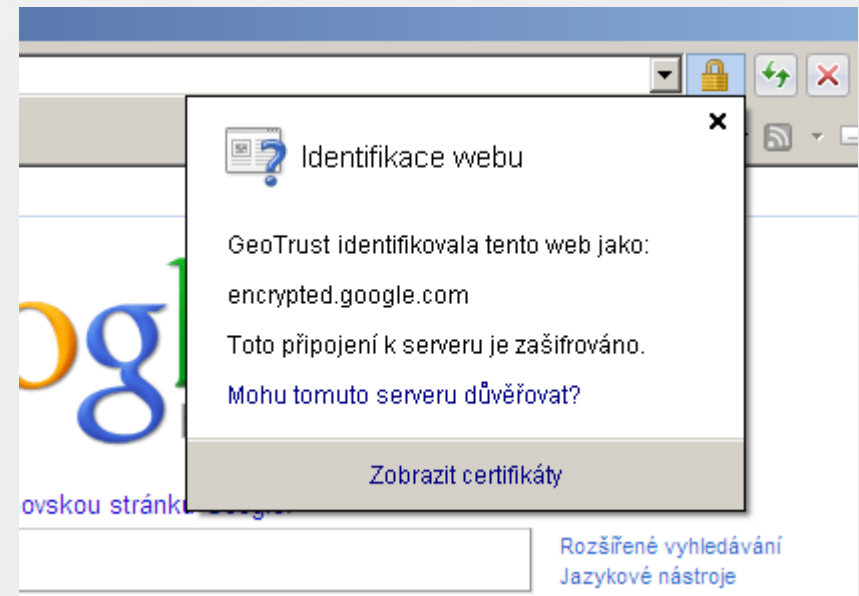
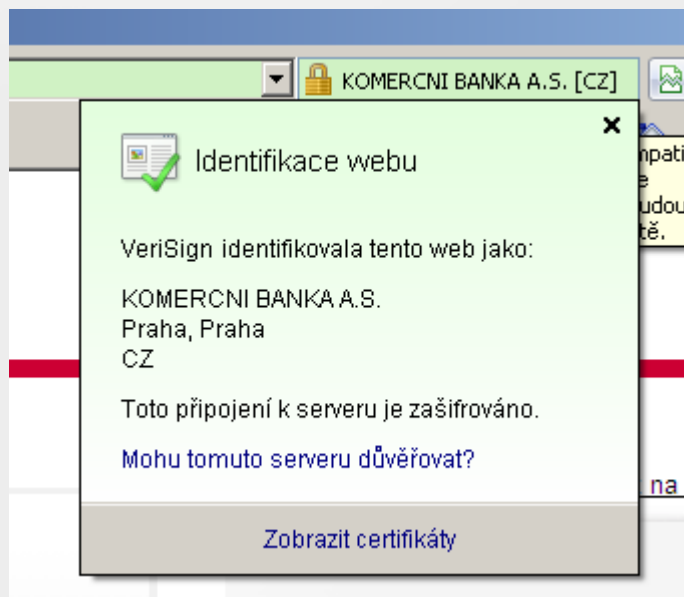


# Důvěra nebo nedůvěra

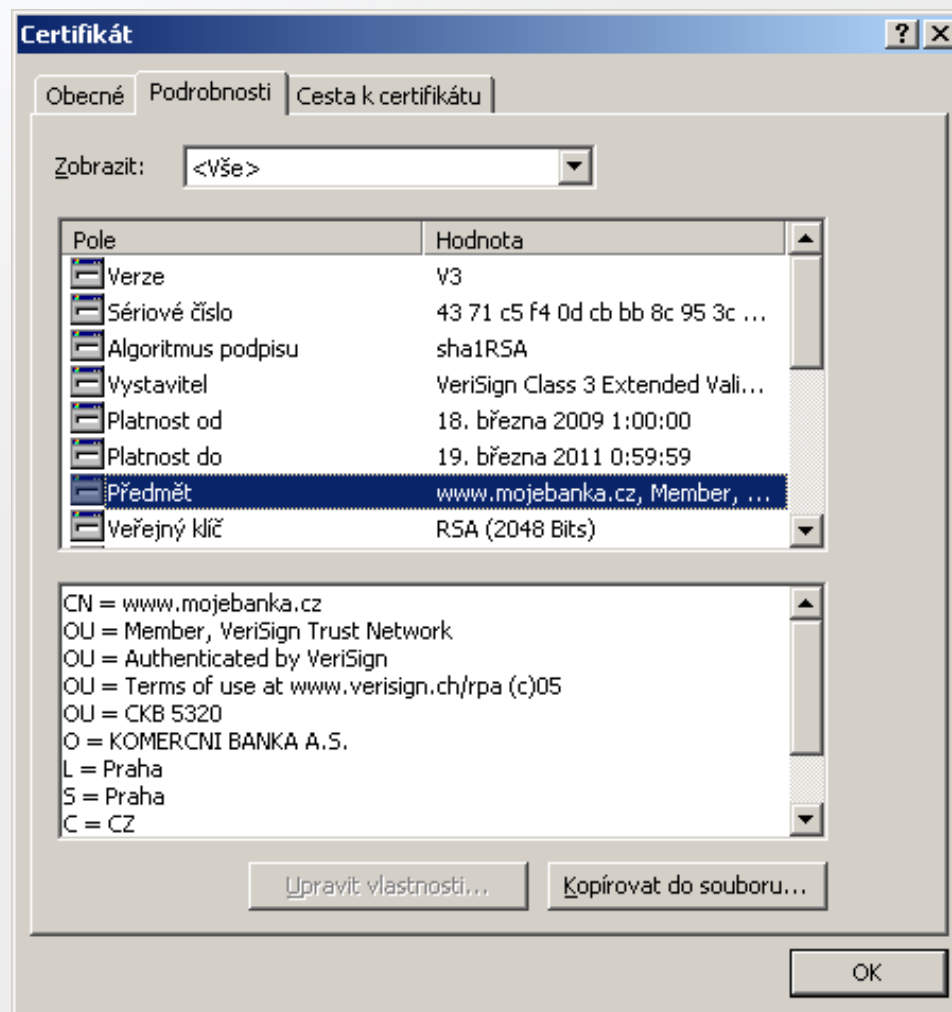
- Pokud certifikát není podepsán důvěryhodnou CA nemusí to automaticky znamenat špatnou stránku.
- Naopak certifikát podepsaný důvěryhodnou CA nemusí znamenat, že na webově stránce nemůže být nějaký malware.
- Jednoduché řešení/návody pro uživatele neexistují.



# Jak zjistit, jaká CA podepsala certifikát serveru?

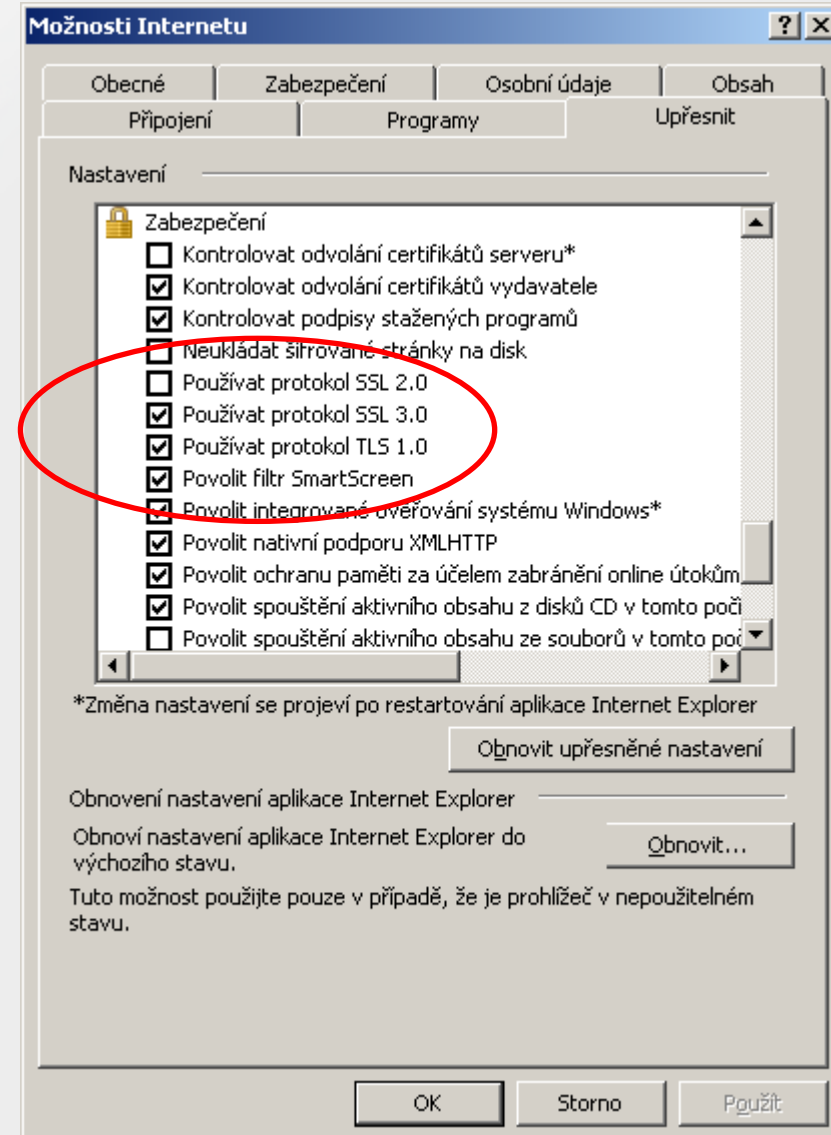


# Můžete si i prohlédnout certifikáty...

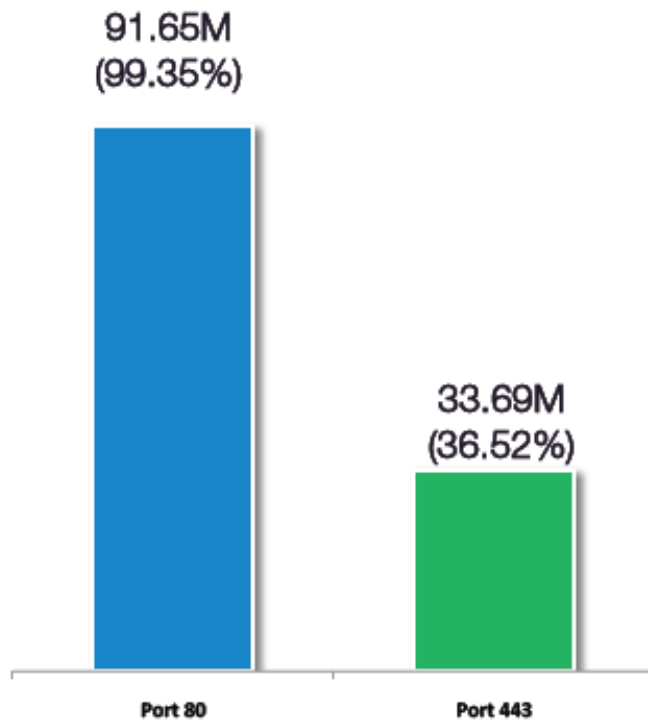


# SSL/TLS Verze

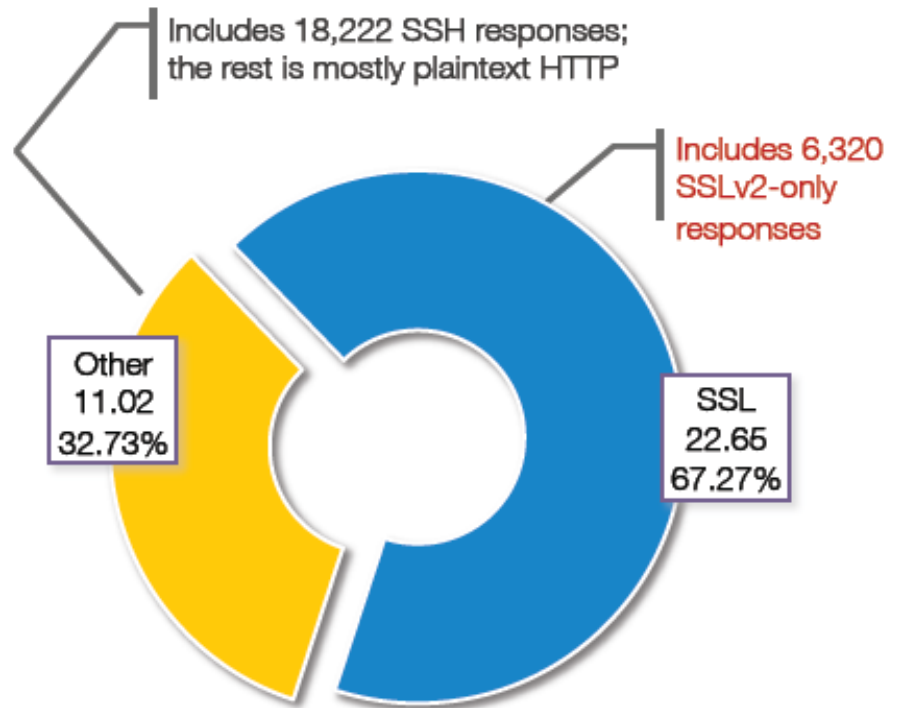
- Existuje několik verzí SSL/TLS
- SSL v2.0 není bezpečné
  - Nepoužívejte



# Pár statistik

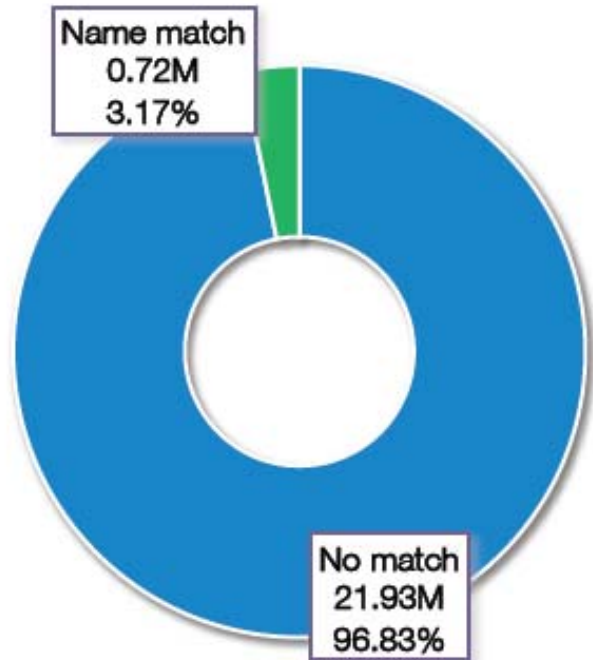


Domain responses on ports 80 and 443

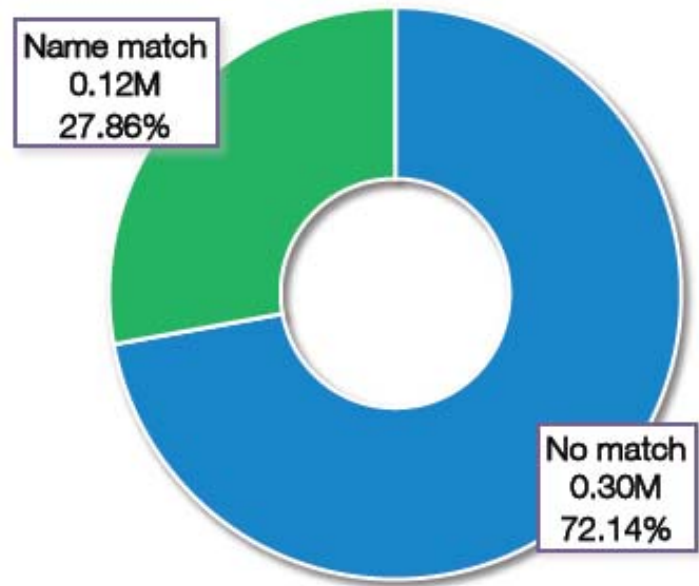


Protocols on port 443 (in millions)

# Pár statistik



Out of 22.65M domain names with SSL enabled

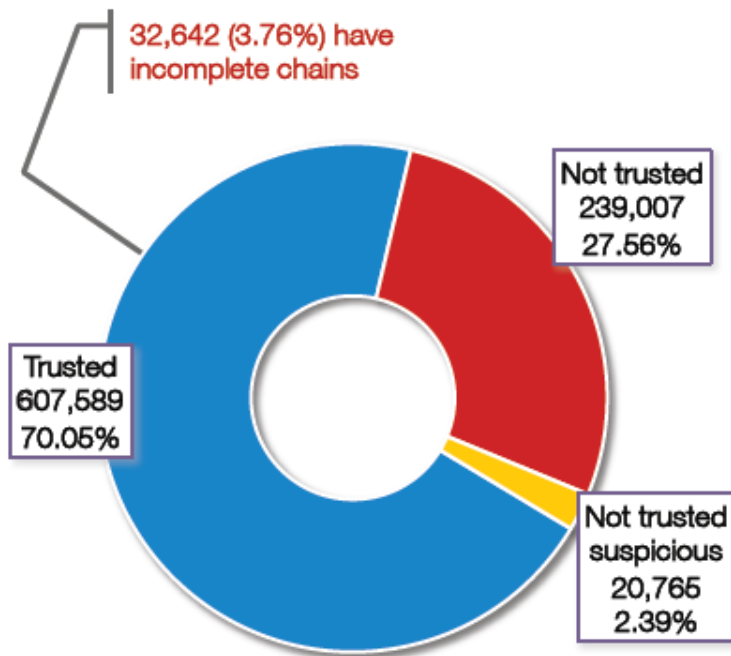


Alexa's Top 1M domain names

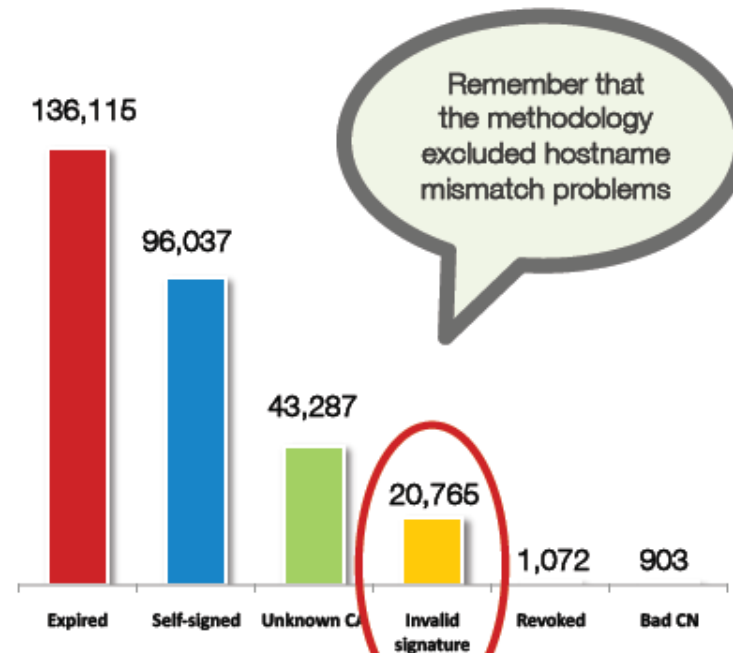
# Kontrola certifikátu

- Jméno počítače
- Časová platnost od-do
- Platný podpis
- Podpis vytvořen důvěryhodnou CA
- ...

# Pár statistik



Trusted versus untrusted certificates



Validation failures

Interoperability issues with JSSE?