Praktické aspekty kryptografie v IT

MV707K Informační technologie v právní praxi

Zdeněk Říha

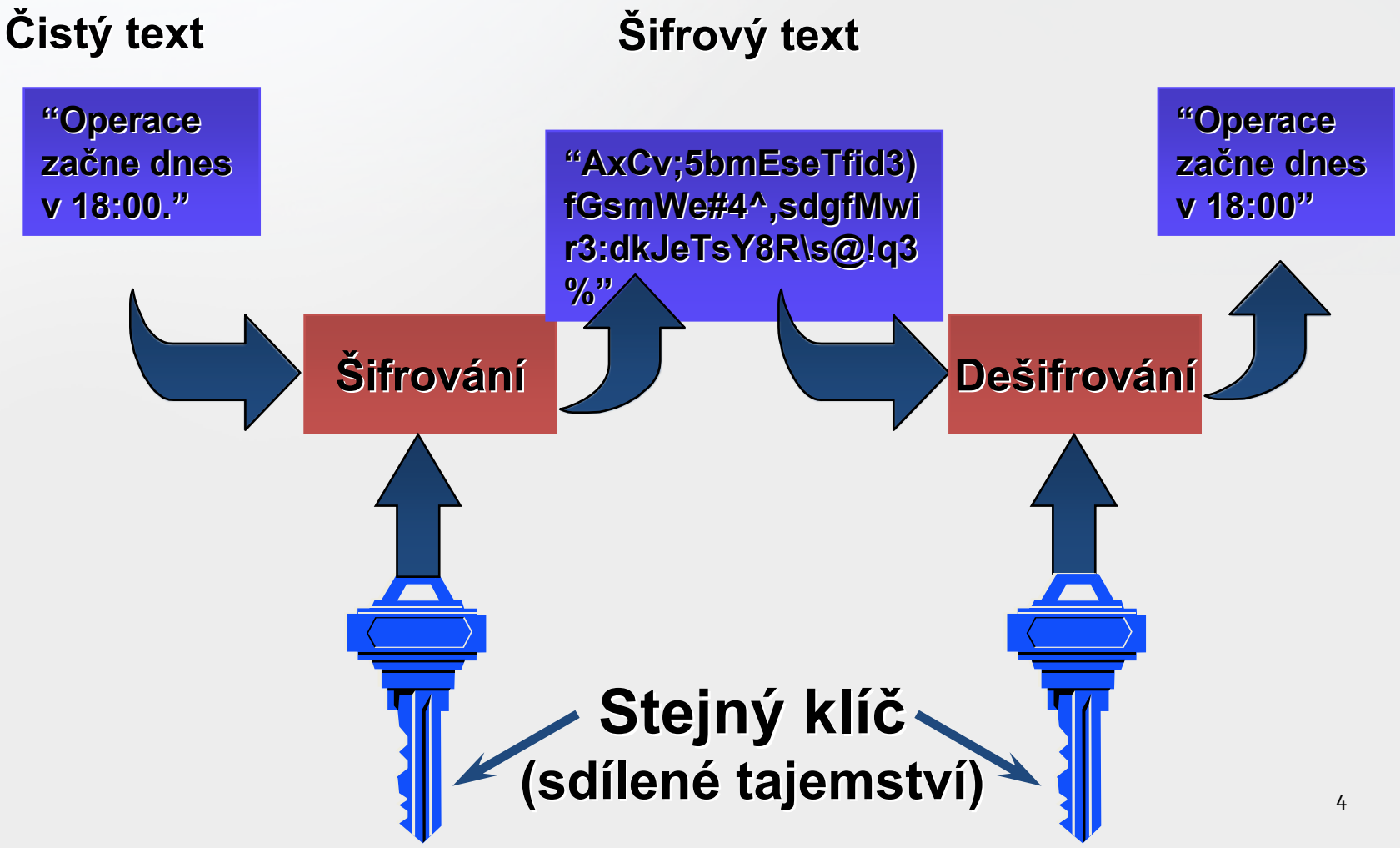
Počítačová bezpečnost

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



Symetrické šifrování

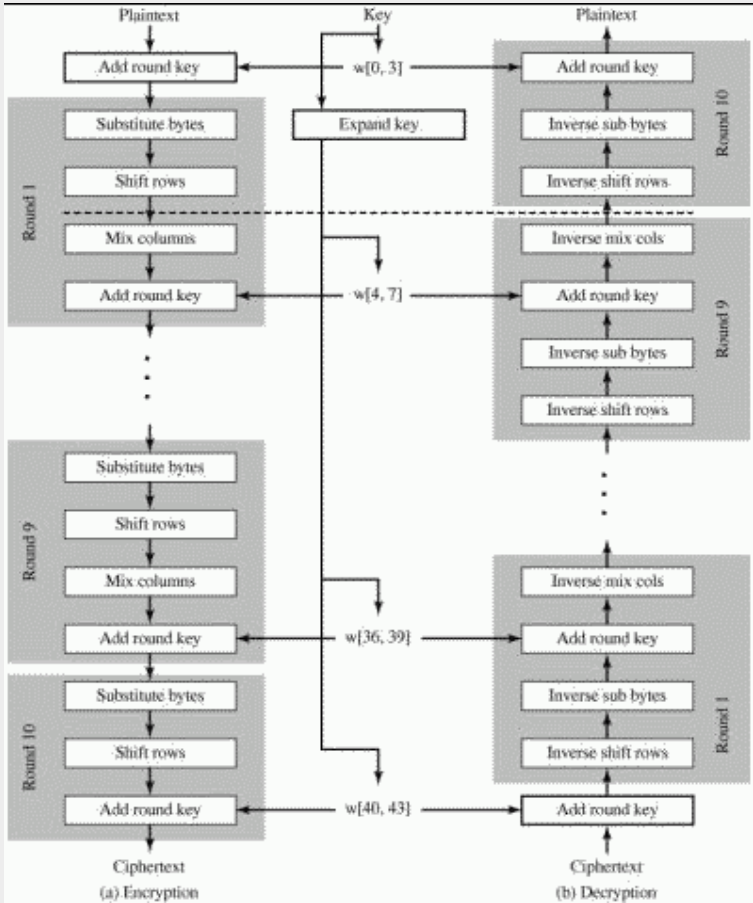
- Výhody
  - Rychlost (asi 1000 rychlejší než asymetrické šifrování)
- Nevýhody
  - Klíč je tajný a je třeba jej udržovat v tajnosti
  - Klíč je třeba domluvit předem (a tak aby se jej nedozvěděl nikdo jiný)

Symetrické šifrovací algoritmy

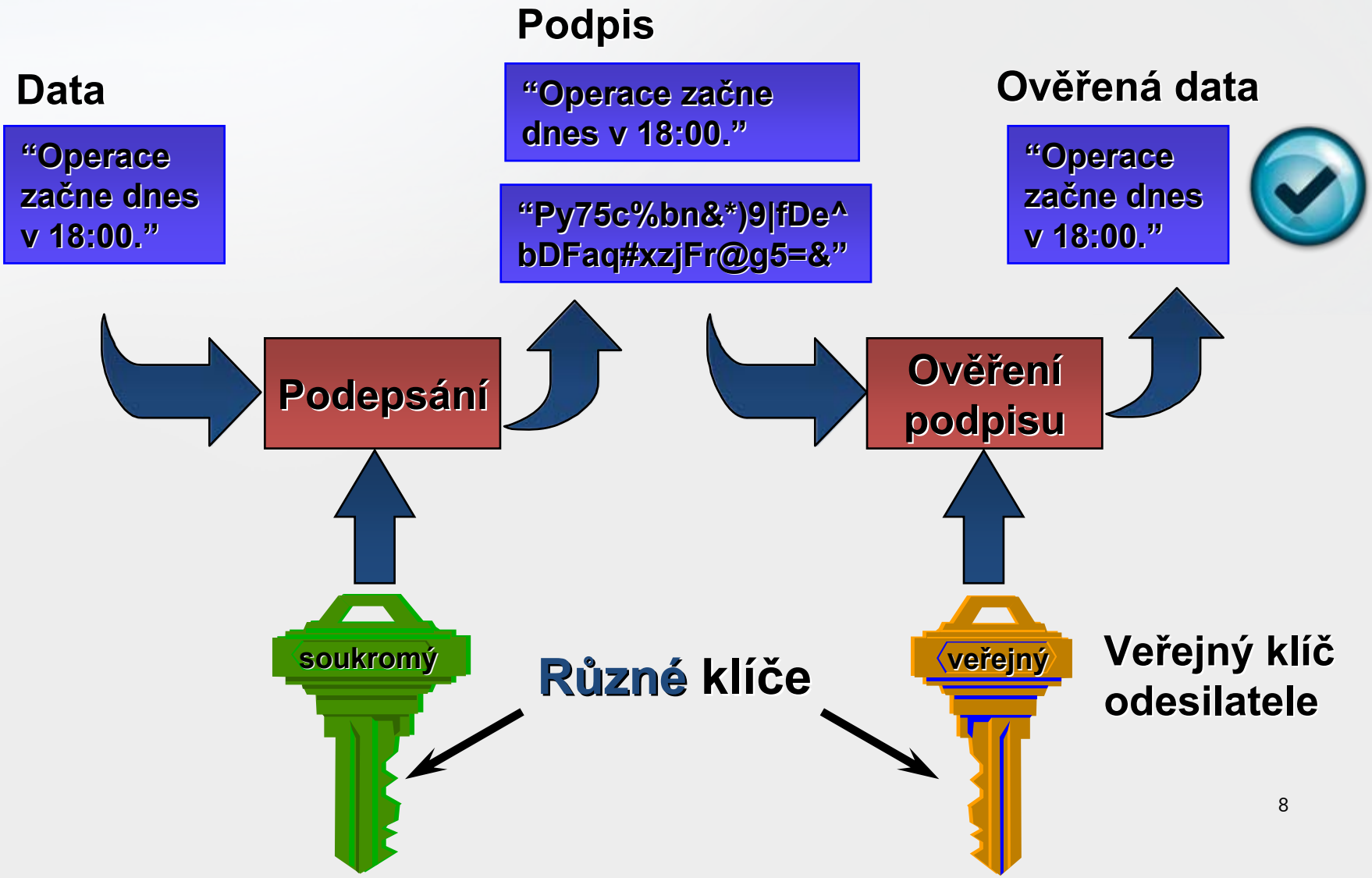
- DES
  - Klíč: 56 bitů
  - Šifruje bloky dat o velikosti 64 bitů
  - Dnes nedostatečně bezpečné
  - Lze kombinovat DES se 2 nebo 3 různými klíči, pak je bezpečné.
    - Nazývá se TrippleDES nebo 3DES
- Blowfish, Twofish
  - Rychlé a bezpečné algoritmy

Symetrické šifrovací algoritmy

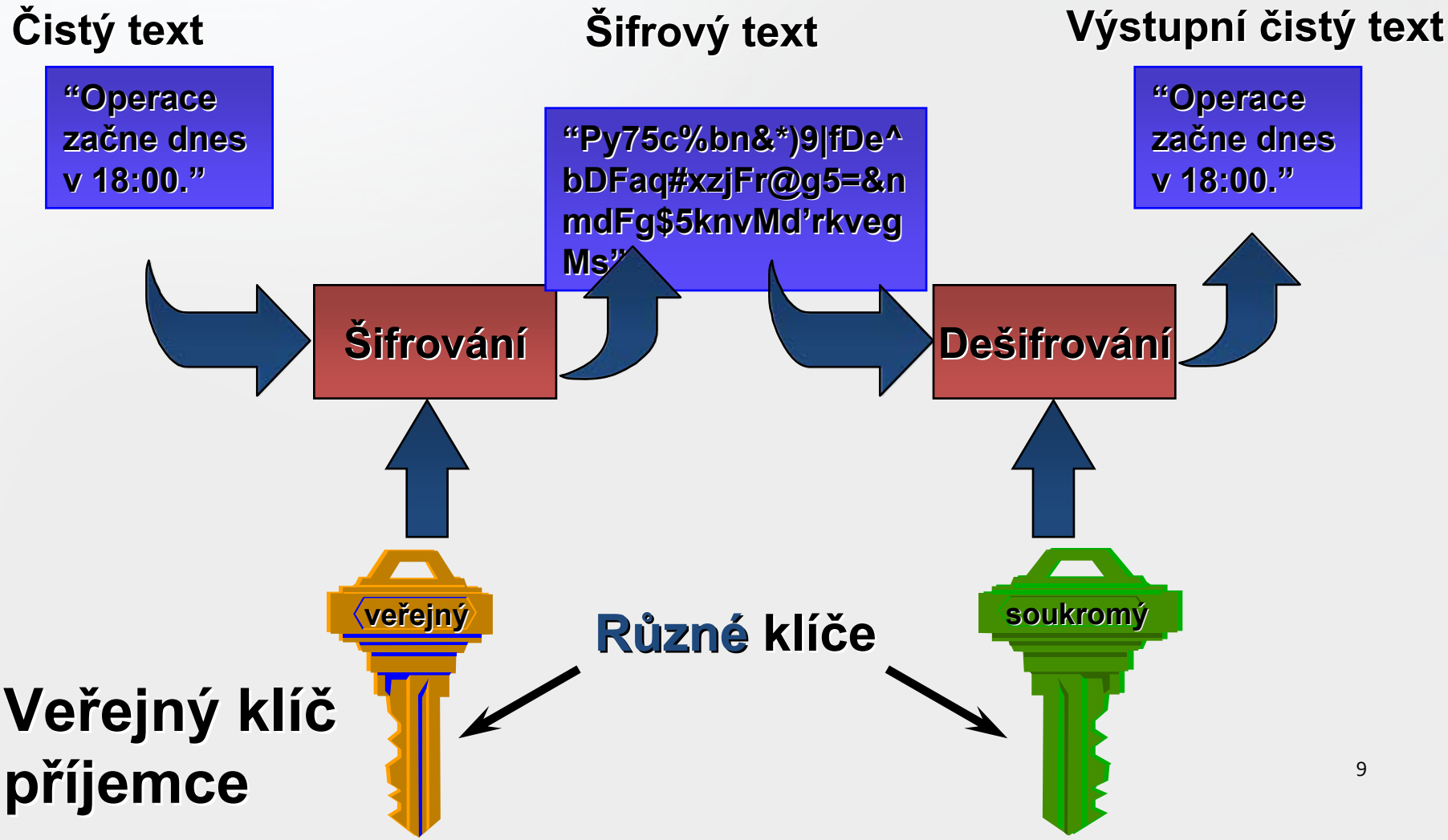
- AES (Advanced Encryption Standard)
  - Vítěz soutěže NIST z let 1997-2000
  - Původně se jmenoval Rijndael
  - Klíče o velikosti 128, 192 nebo 256 bitů
  - Rychlý a bezpečný



Asymetrická kryptografie – digitální podpis



Asymetrická kryptografie – šifrování



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 !!!

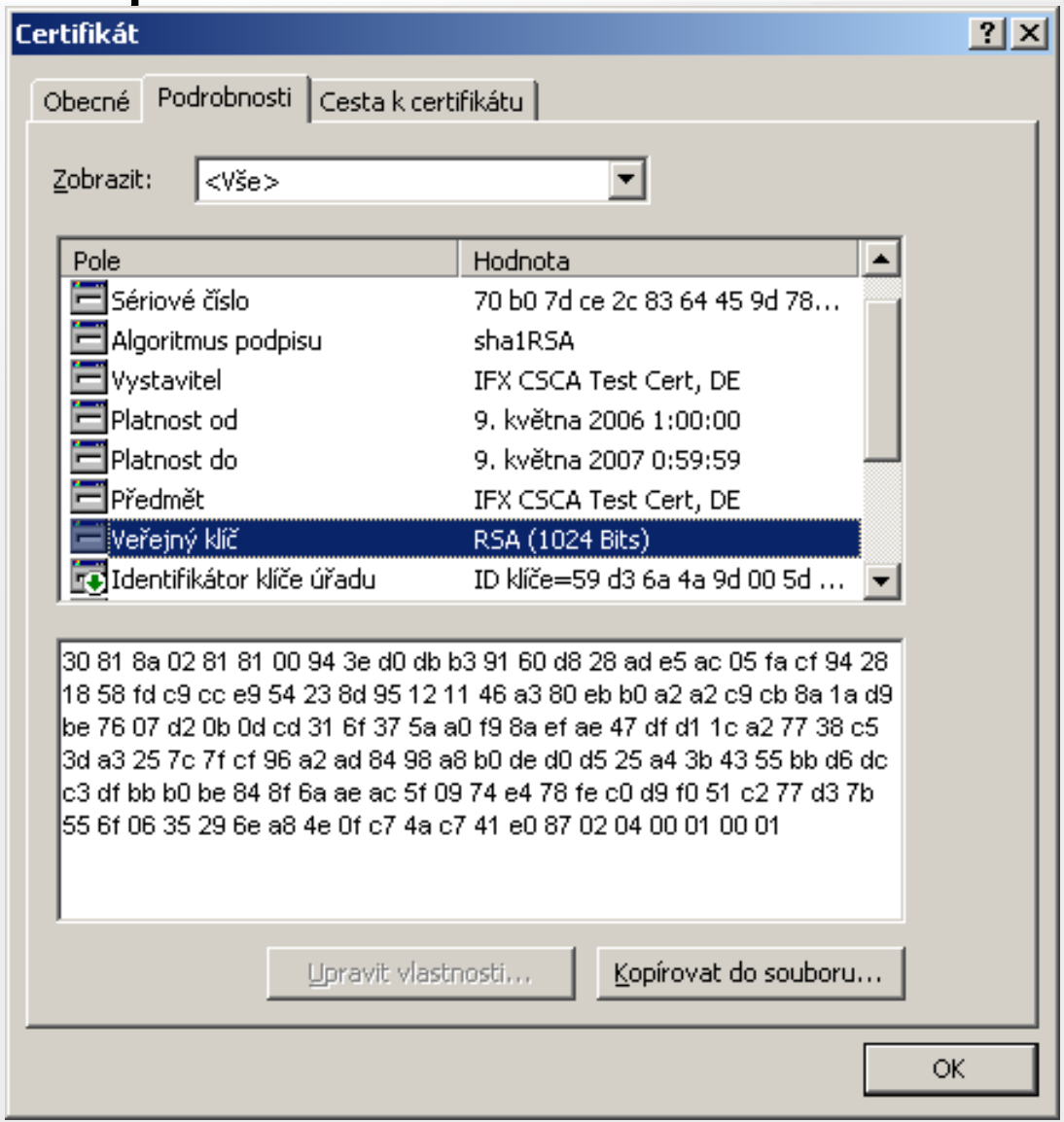
Asymetrické šifrovací algoritmy

- 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·q, ϕ(n) = (p-1)(q-1)**.
- Zvolíme velké **e** takové, že **gcd(e, ϕ(n)) = 1**.
- Spočítáme $\mathbf{d = e^{-1} \pmod{\phi(n)}}$.
- Veřejný klíč: **n, e.**
  Neveřejné parametry: **p, q, d.**
- Šifrování (ověření podpisu): $\mathbf{c = w^e \bmod n}$.
- Dešifrování (podepisování): $\mathbf{w = c^d \bmod n}$.

Příklad veřejného klíče RSA



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[23] 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 neveříme?
    - 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
  - eIdentity

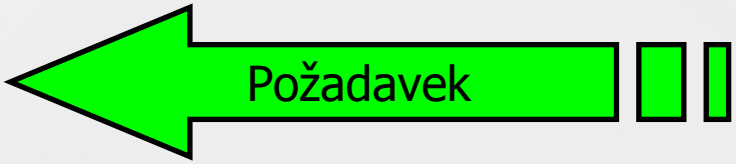
Počítačová bezpečnost – další pojmy

- 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)*

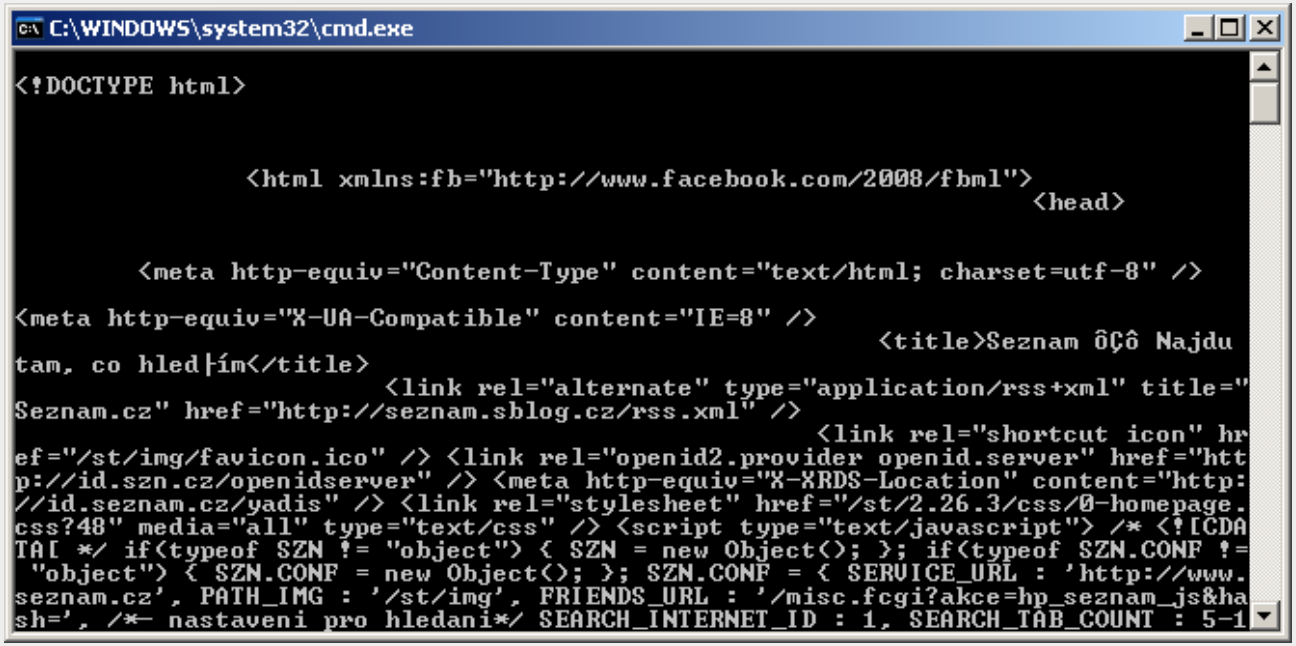
Hlavičky

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

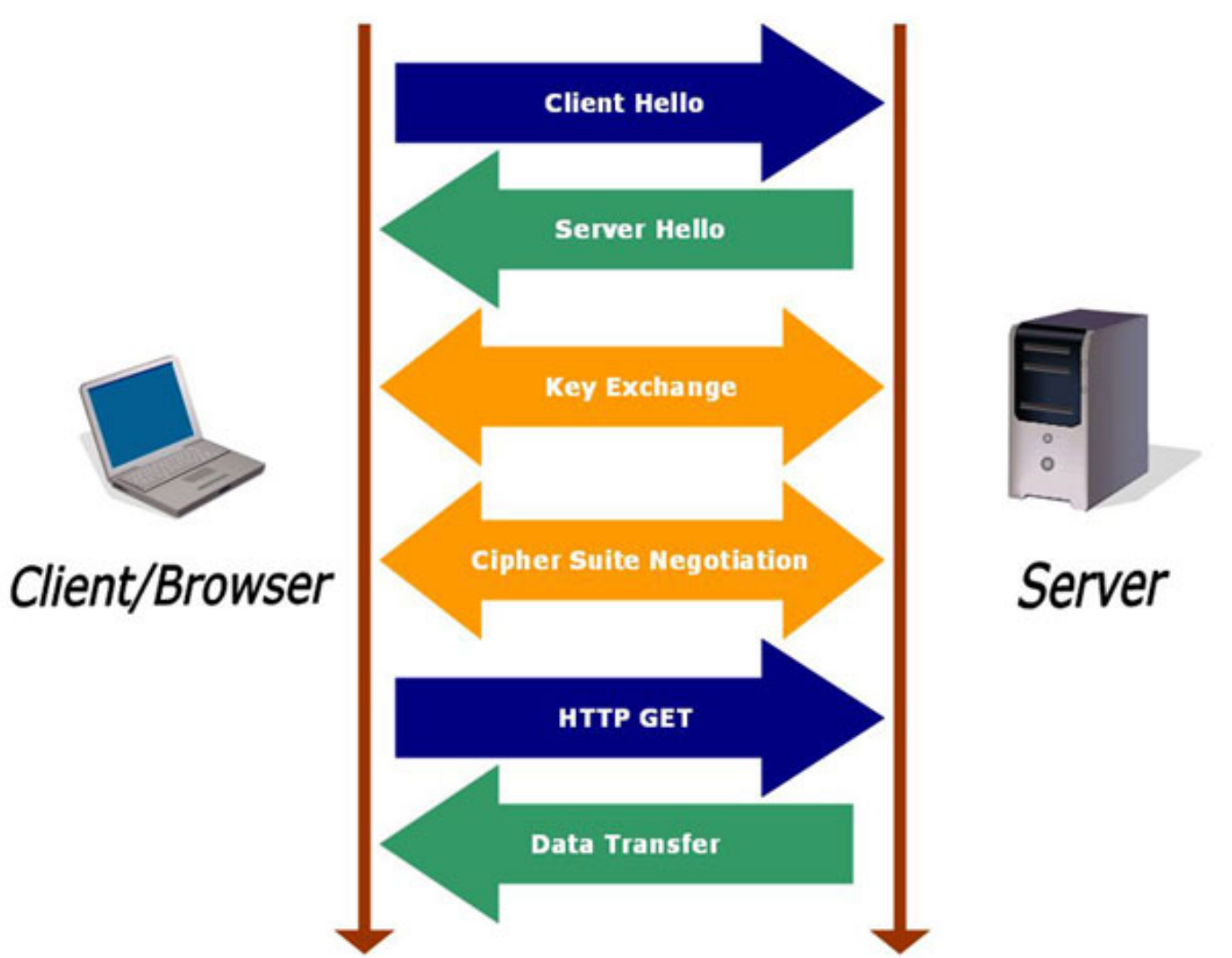
- Start/spustit/cmd
- telnet www.seznam.cz 8o
- GET / [enter] [enter]



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.

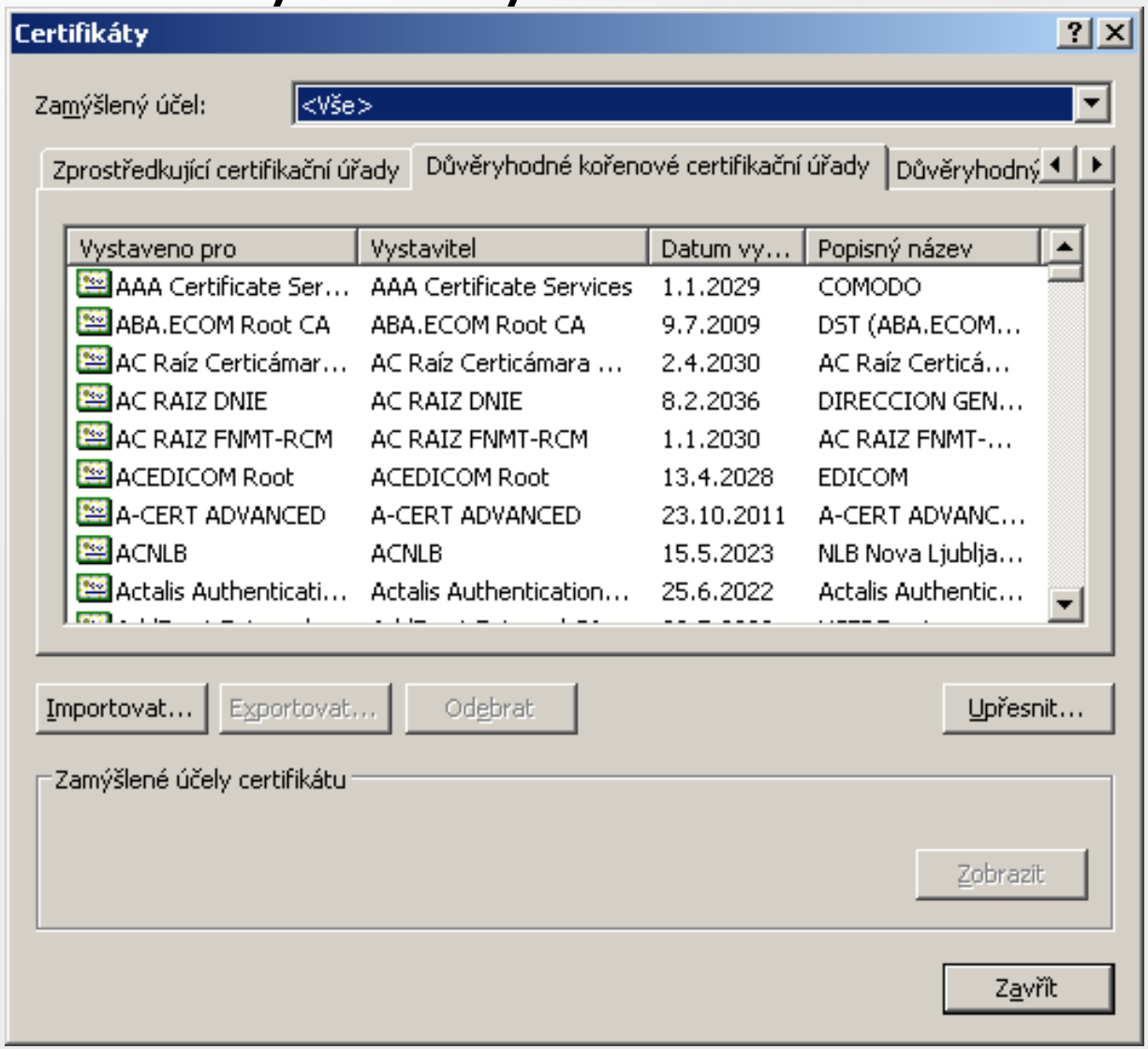
Certifikát

- 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

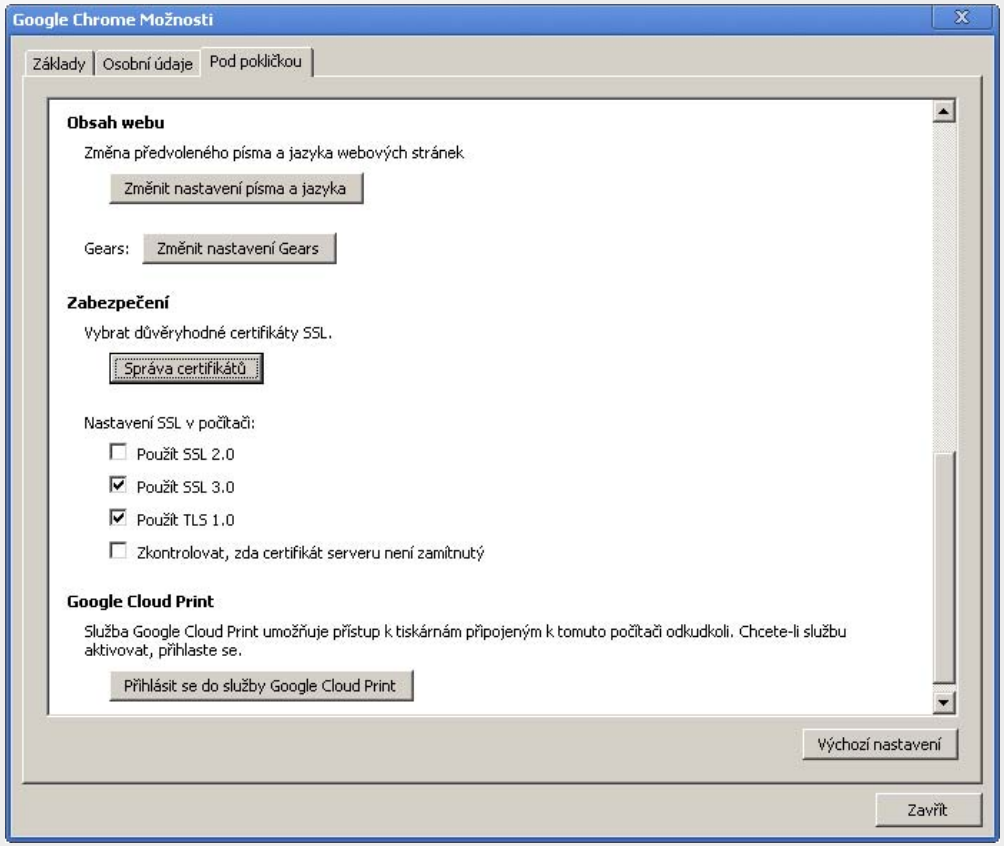
- Seznamy jsou uloženy v prohlížečích (IE bere seznam z OS)
- Tyto seznamy můžete konfigurovat.
- Iniciálně jsou tam i desítky CA o kterých jste nikdy neslyšeli…
  - Těm všem automaticky důvěřujete ☺

Seznam důvěryhodných CA



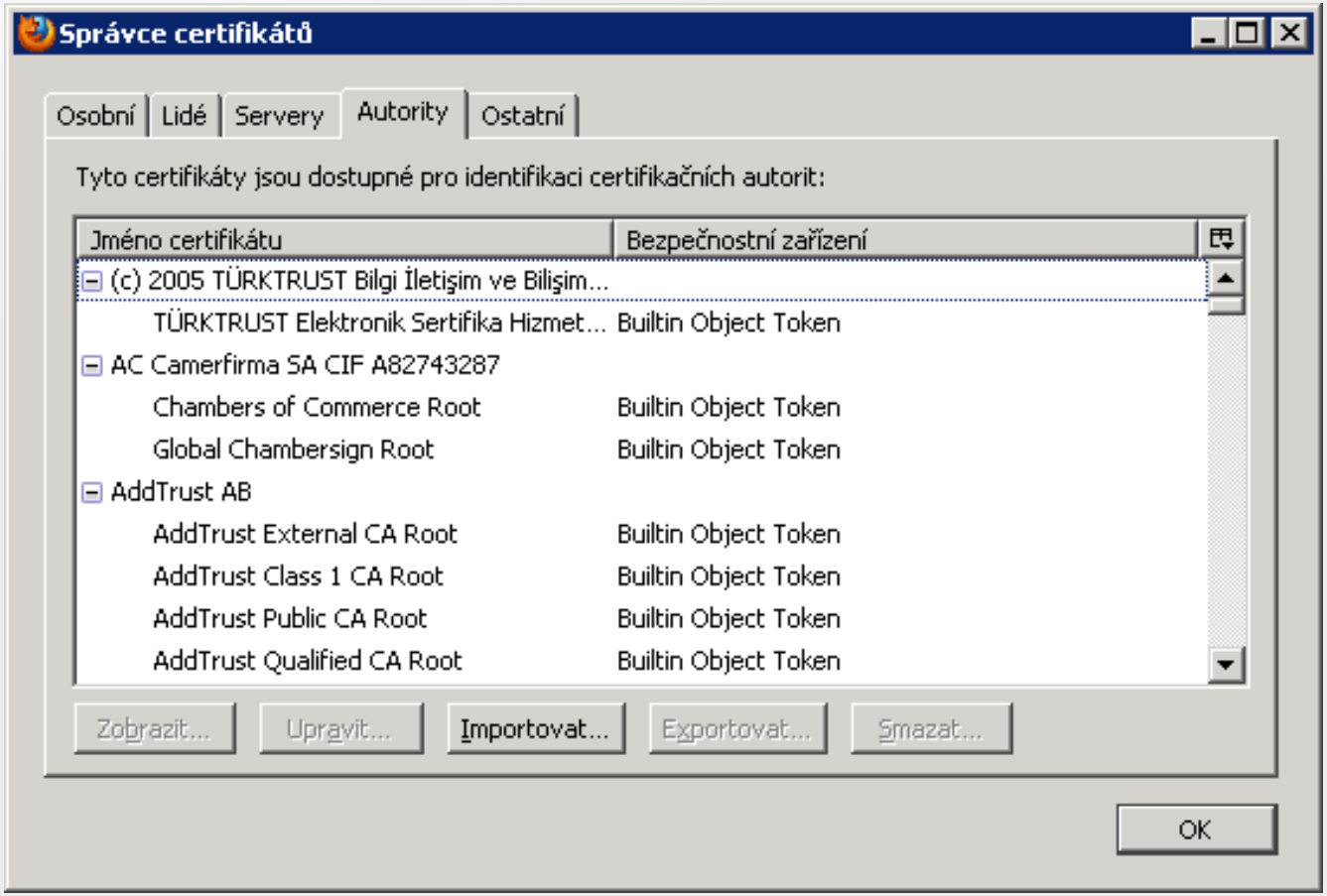
Seznam důvěryhodných CA

- Podobně v Google Chrome

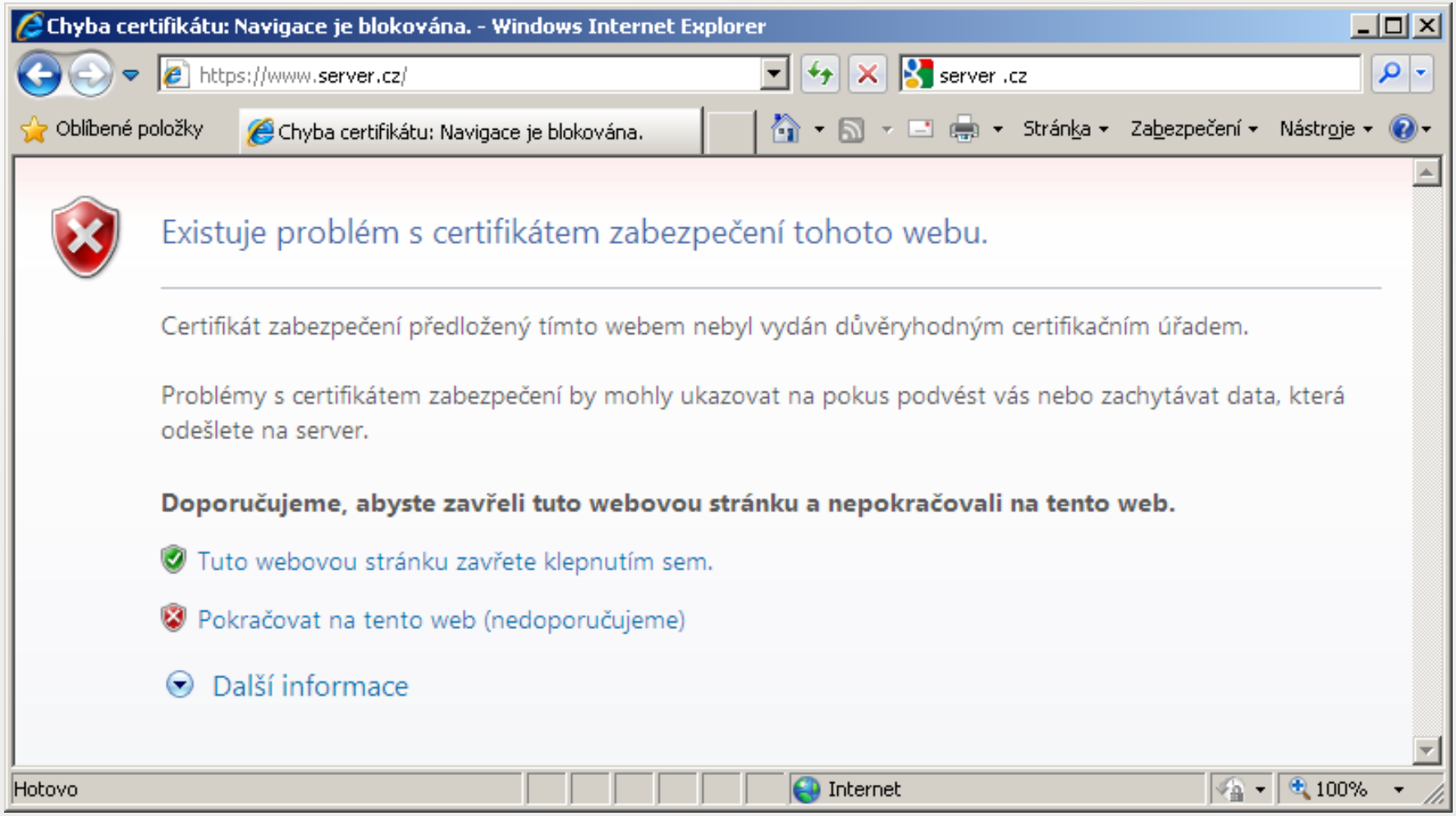


Seznam důvěryhodných CA

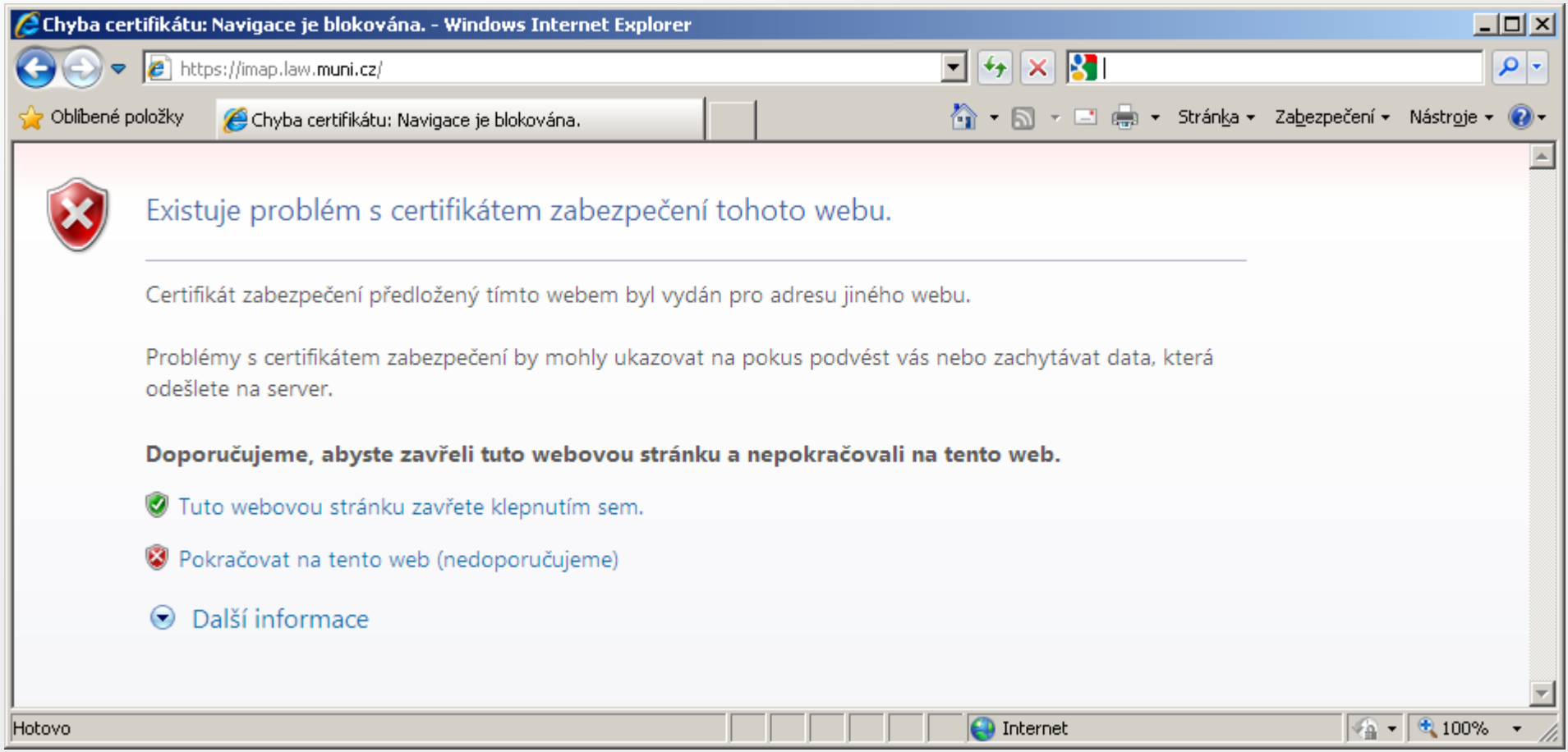
- Mozilla Firefox



Certifikát nepodepsán důvěryhodnou CA

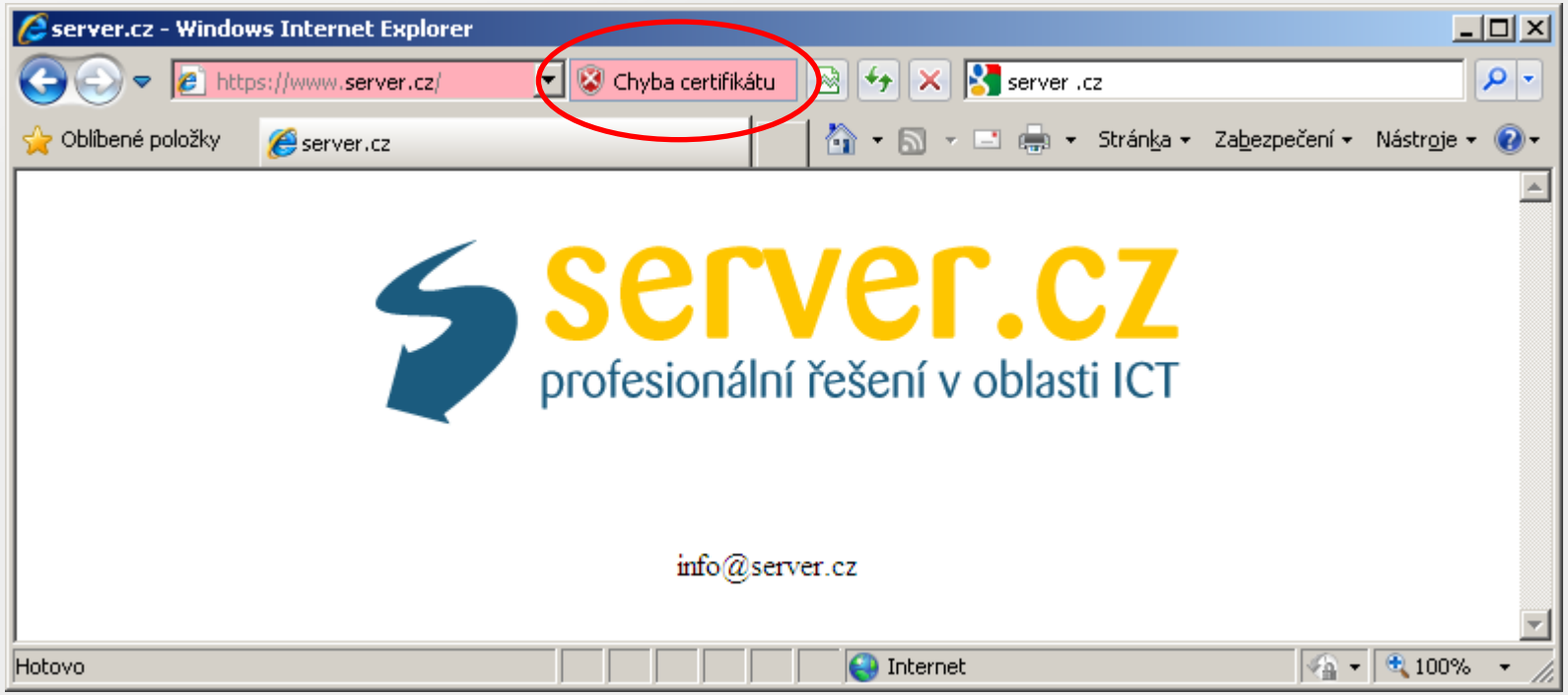


Certifikát určen pro jiný web…

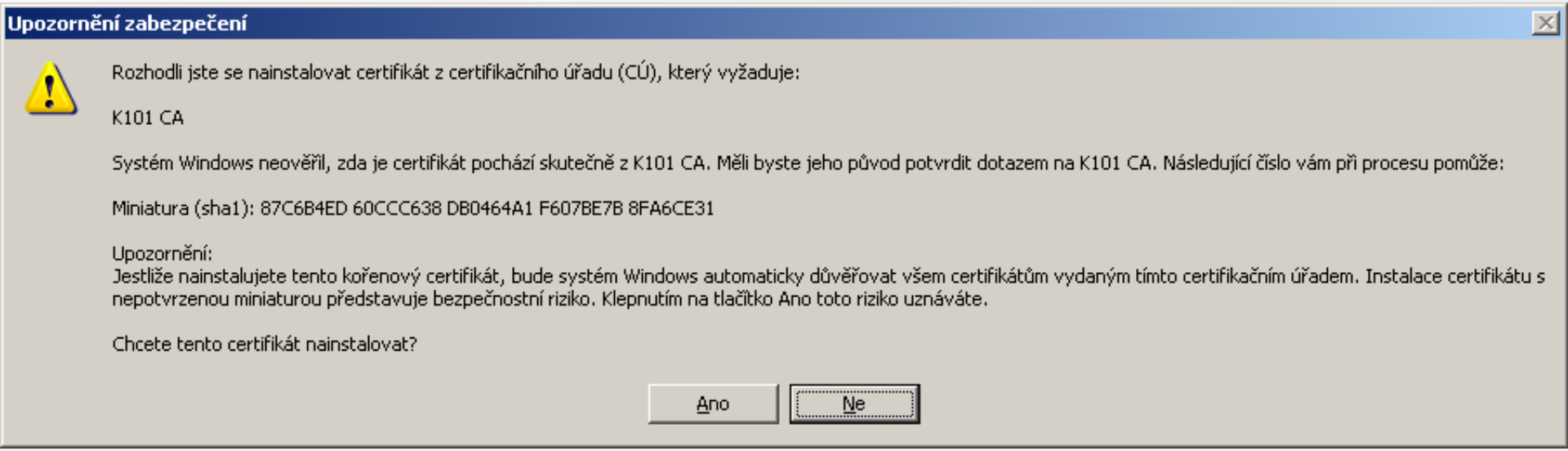


Certifikát nepodepsán důvěryhodnou CA

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

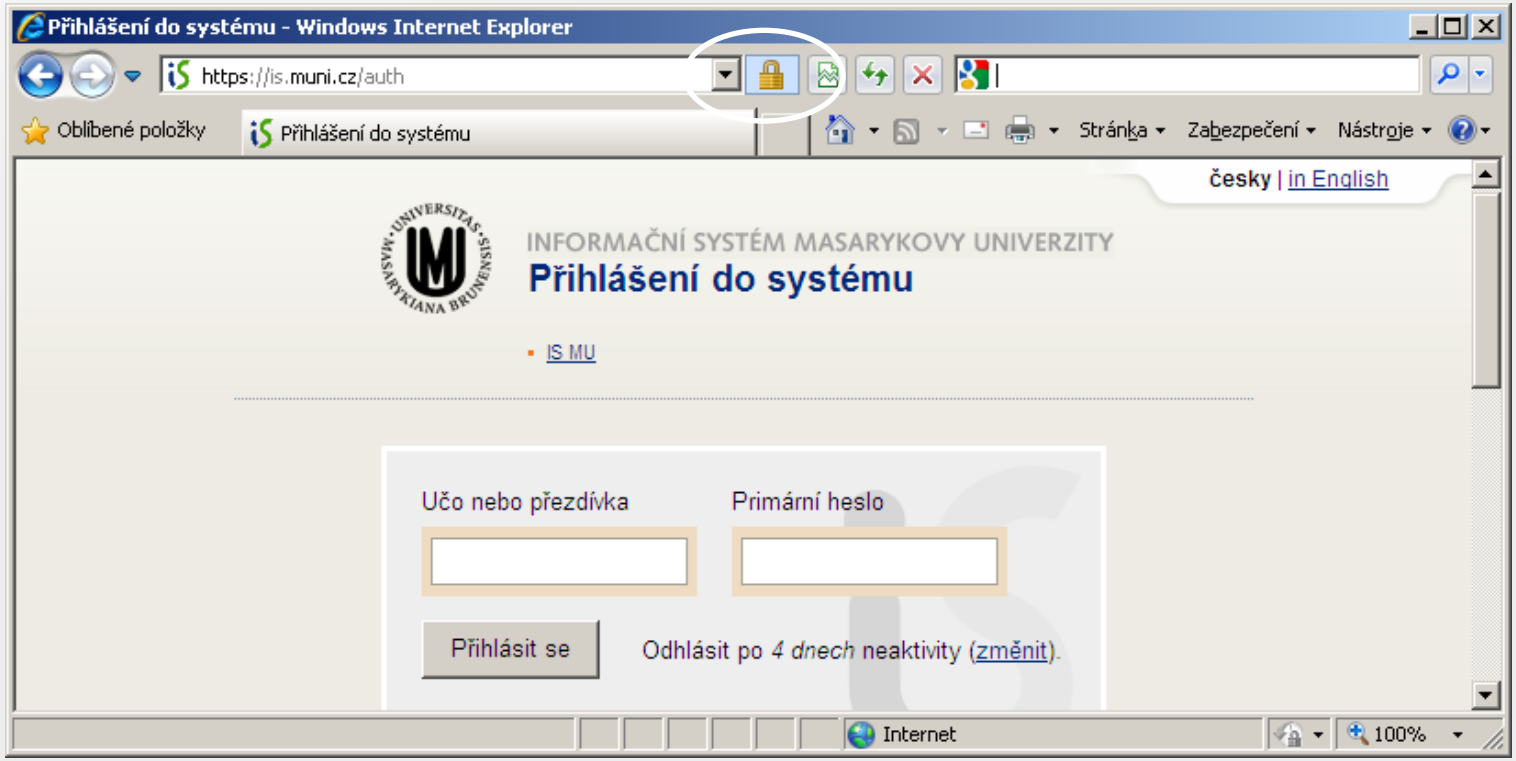


CA lze přidat mezi důvěryhodné



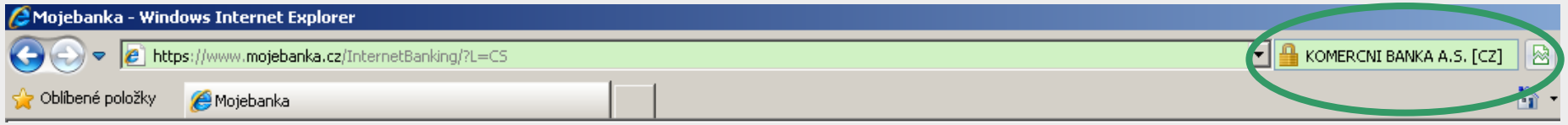
Certifikát podepsán důvěryhodnou CA

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



EV certifikát podepsán důvěryhodnou CA

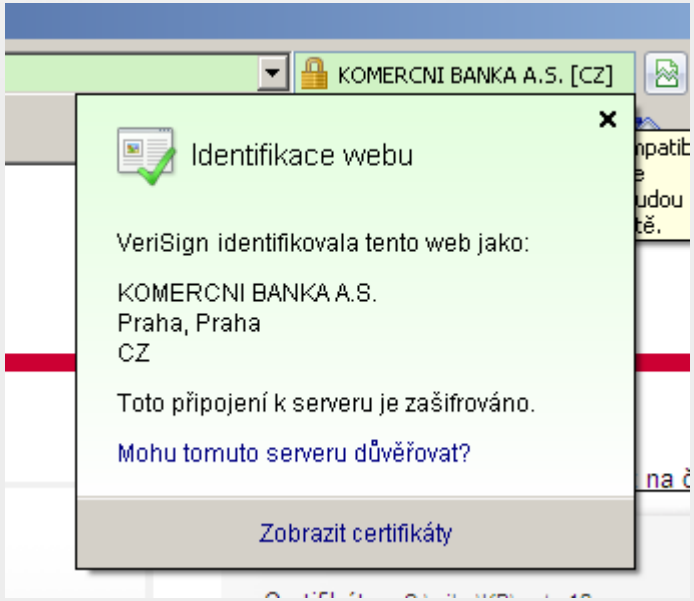
- EV (extended validation) certifikát má vyšší míru důvěry ve shodu vlastníka domény s webovým serverem.
- Technicky ten stejný X.509 (s drobnou poznámkou), ale CA si více žadatele o EV certifikát „proklepne“.

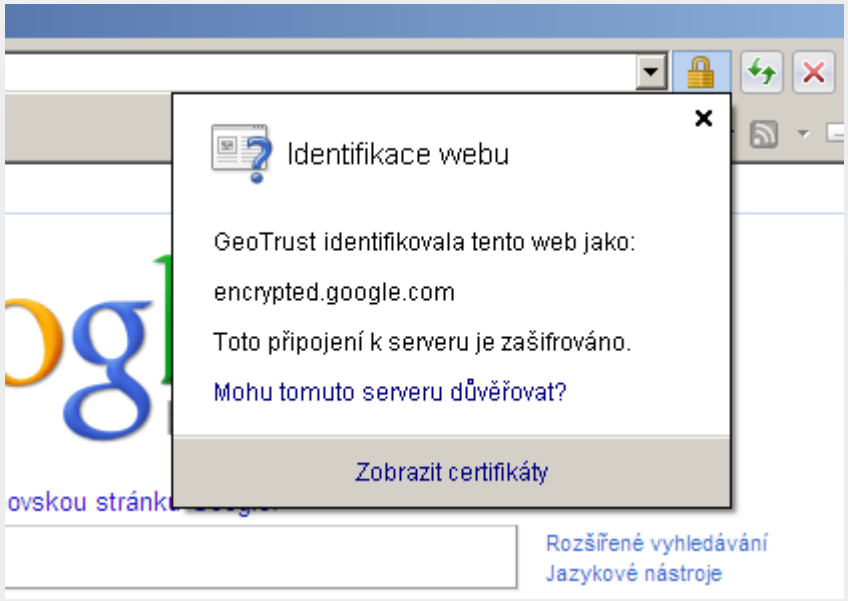


Důvěra nebo nedůvěra

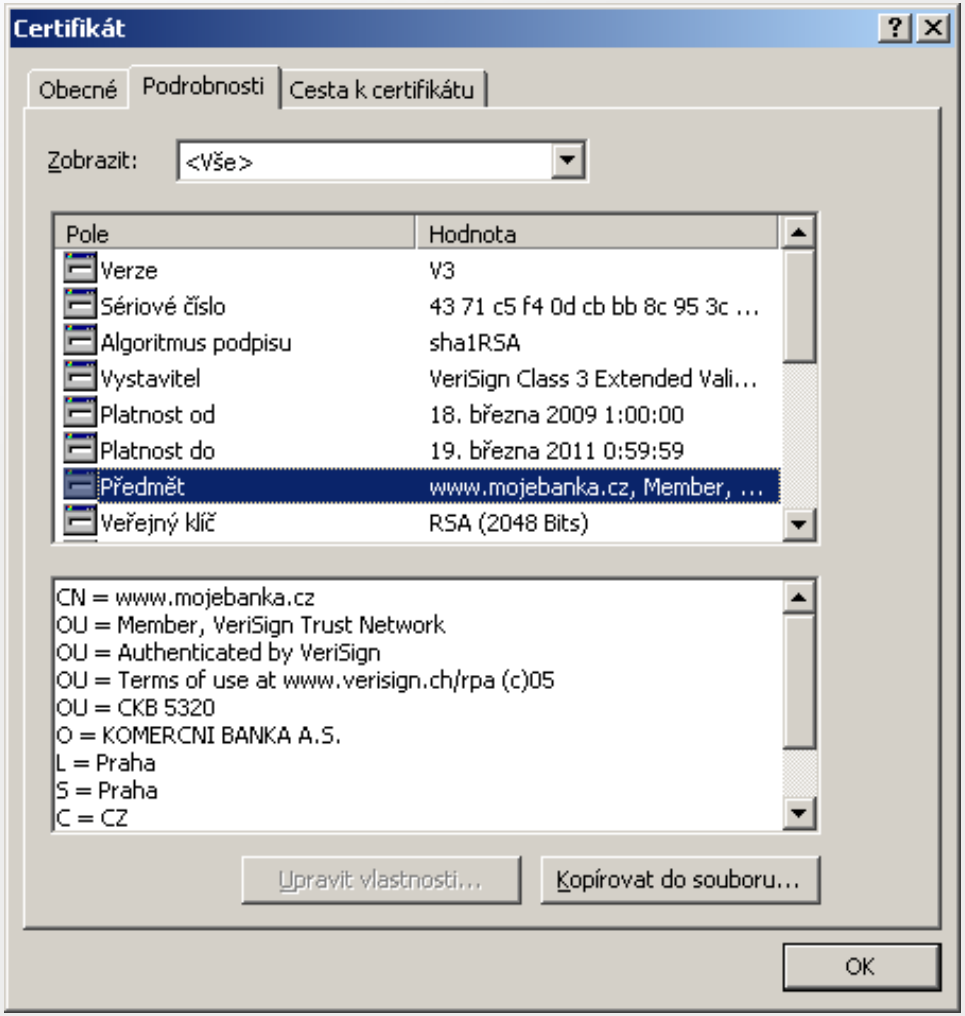
- Pokud certifikát není podepsán důvěryhodnou CA nemusí to automaticky znamenat špatnou stránku.
- Naopak certifikát podepsaný důvěryhodnou CA nemusí znamenat, že na webové stránce nemůže být nějaký malware.
- Jednoduché řešení/návody pro uživatele neexistují.

Jak zjistit, jaká CA podepsala certifikát serveru?



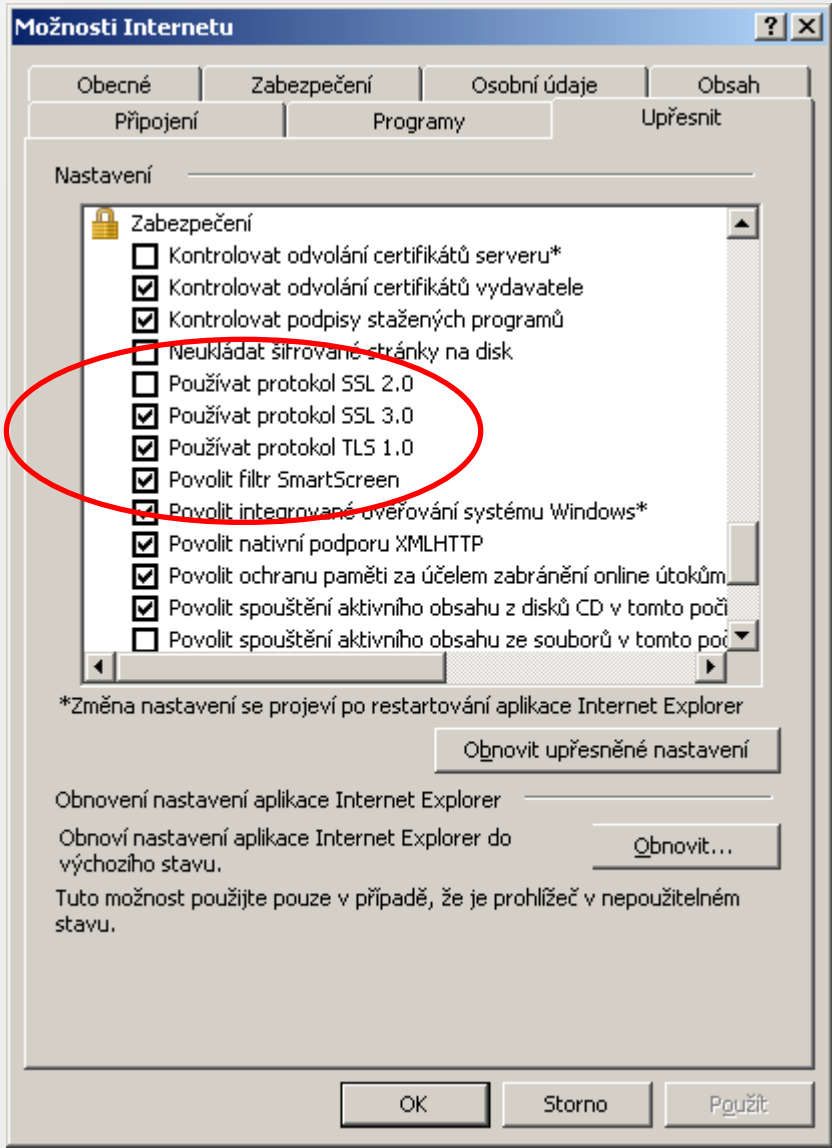


Můžete si i prohlédnout certifikáty…

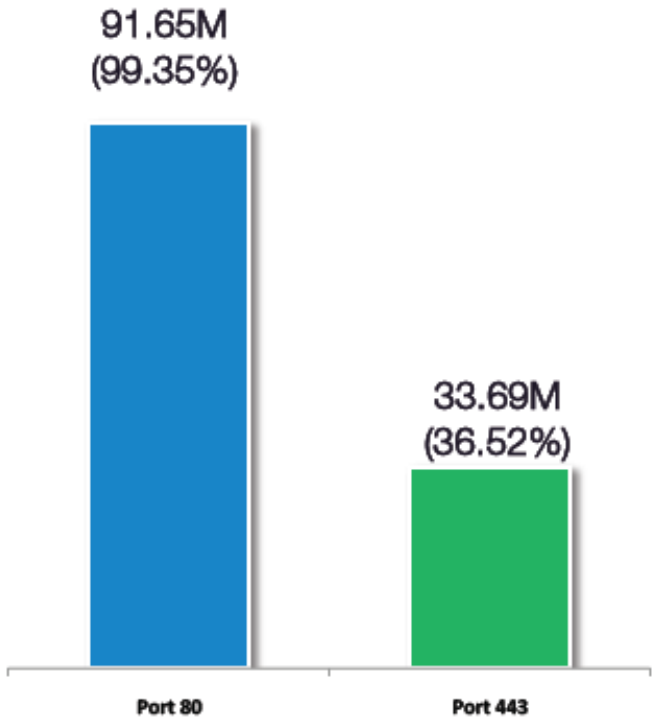


SSL/TLS Verze

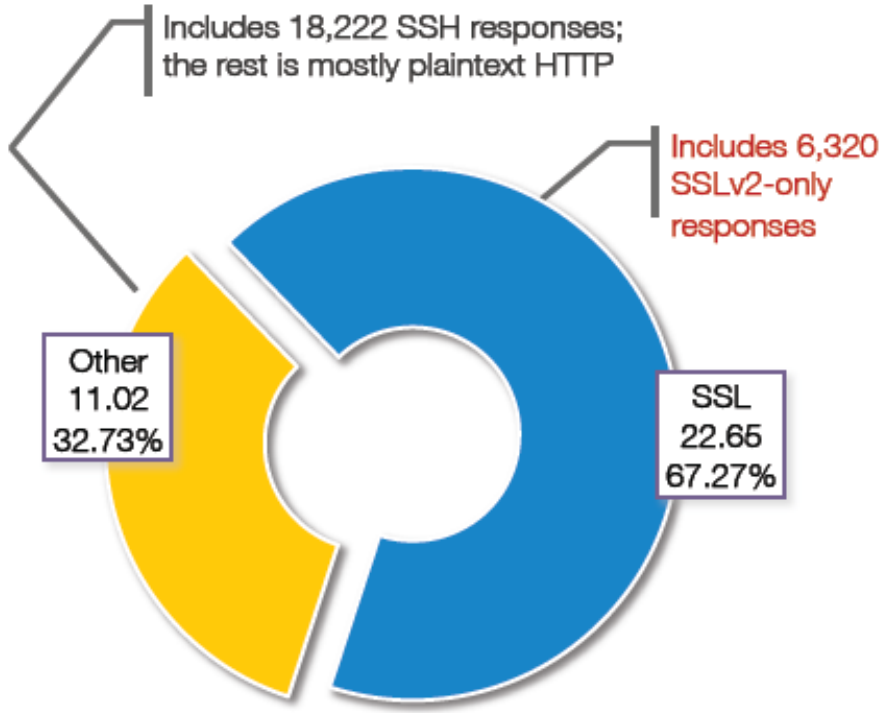
- Existuje několik verzí SSL/TLS
- SSL v2.0 není bezpečné
  - Nepoužívejte



Pár statistik

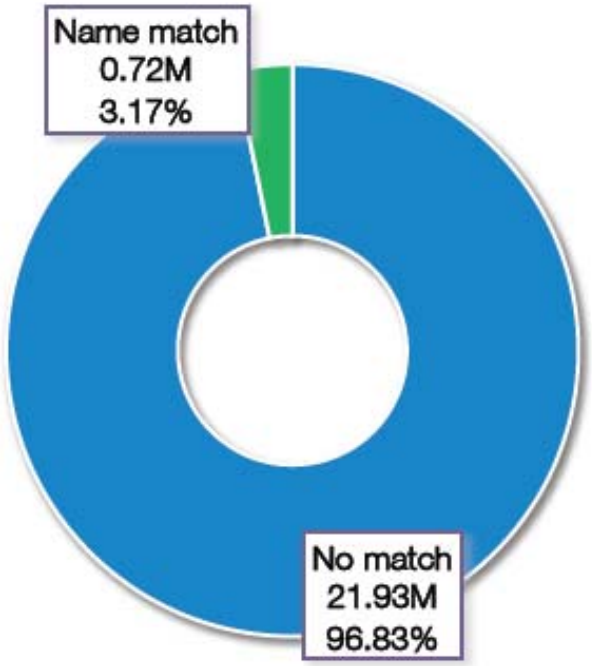


Domain responses on ports 80 and 443

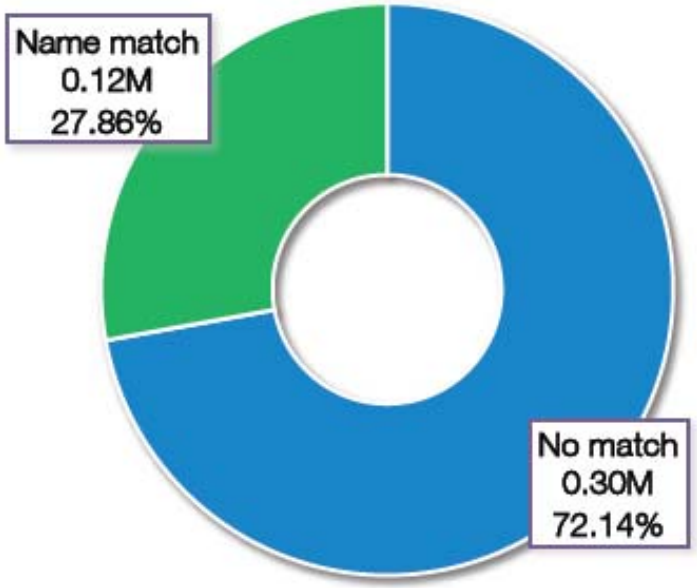


Protocols on port 443 (in millions)

Pár statistik



Out of 22.65M domain names with SSL enabled

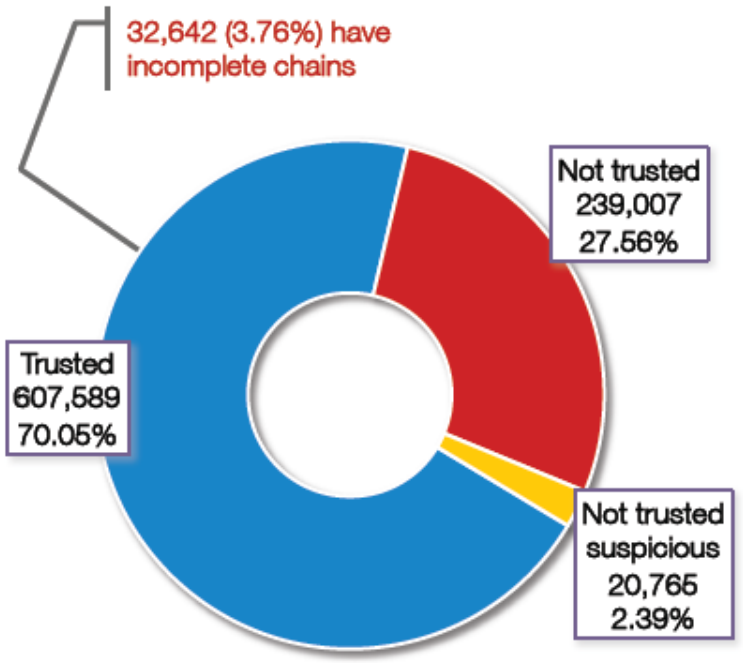


Alexa's Top 1M domain names

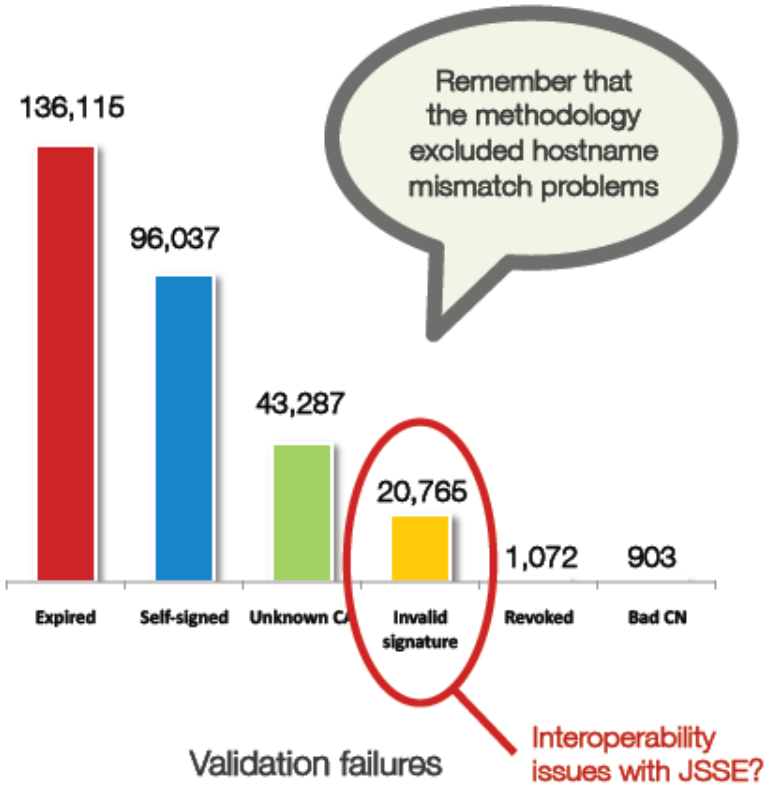
Kontrola certifikátu

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

Pár statistik



Trusted versus untrusted certificates



Validation failures