

DCGI

KATEDRA POČÍTAČOVÉ GRAFIKY A INTERAKCE

Základy webových aplikací ZWA

Přednáška č. 1

Martin Klíma

Kontakt

Martin Klíma

xklima@fel.cvut.cz

Místnost: KN-E321

Tel +420 224 35 7362

Konzultační hodiny: kdykoli po objednání

Web předmětu:

<https://cw.fel.cvut.cz/wiki/courses/B6B39ZWA/start>





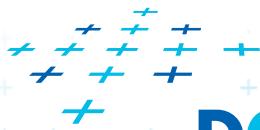
Cíl a náplň předmětu

Cíl předmětu:

- Absolvent předmětu bude schopen navrhnut, realizovat a spravovat klientskou i serverovou část webové aplikace.

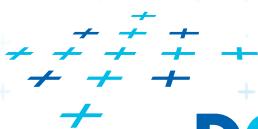
Náplň předmětu:

- programování na straně webového klienta
- programování na straně webového serveru
- návrh webové aplikace (architektura, technologie, vzory)



Organizace přednášek

1. Základy Internetu, protokol HTTP
2. HTML, jazyky pro definici struktury dokumentu
3. Tvorba formulářů na klientské straně
4. Přednáška CSS
5. Skriptování na straně klienta
6. Jazyk PHP
7. Obsluha fomulářů
8. Praktická ukázka obsluhy formuláře
9. Udržení stavu aplikace (session)
10. Autentizace a autorizace, zápis do souboru
11. Struktura serverové části kódu, MVC
12. Databáze úvod
13. PHP a databáze
14. Rezerva (typicky odpadá)



DCGI



Organizace předmětu

- Zápočet + zkouška
- Body ze semestru



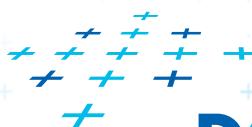
DCGI



Hodnocení

	Max	Min
Semestrální práce	50	30
Test v semestru	15	8
Aktivita	10	0
Zkoušková písemka	25	15
Ústní zkouška	10	-10
Celkem	110	

A (výborně)	≥ 99
B (velmi dobře)	88 až 98
C (dobře)	77 až 87
D (uspokojivě)	66 až 76
E (dostatečně)	55 až 65
F (nedostatečně)	< 55



DCGI



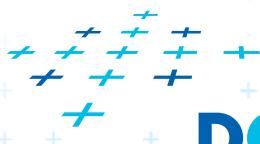
Internet – základní principy

- Počítačová síť tvořená počítači a routery
- Jednotlivé prvky jsou na sobě nezávislé
- Datagramová síť (posílání packetů)
- Packet obsahuje adresu zdroje a cíle
- Doručení packetu není zaručeno
- Není žádná centrální autorita, která by řídila provoz v síti

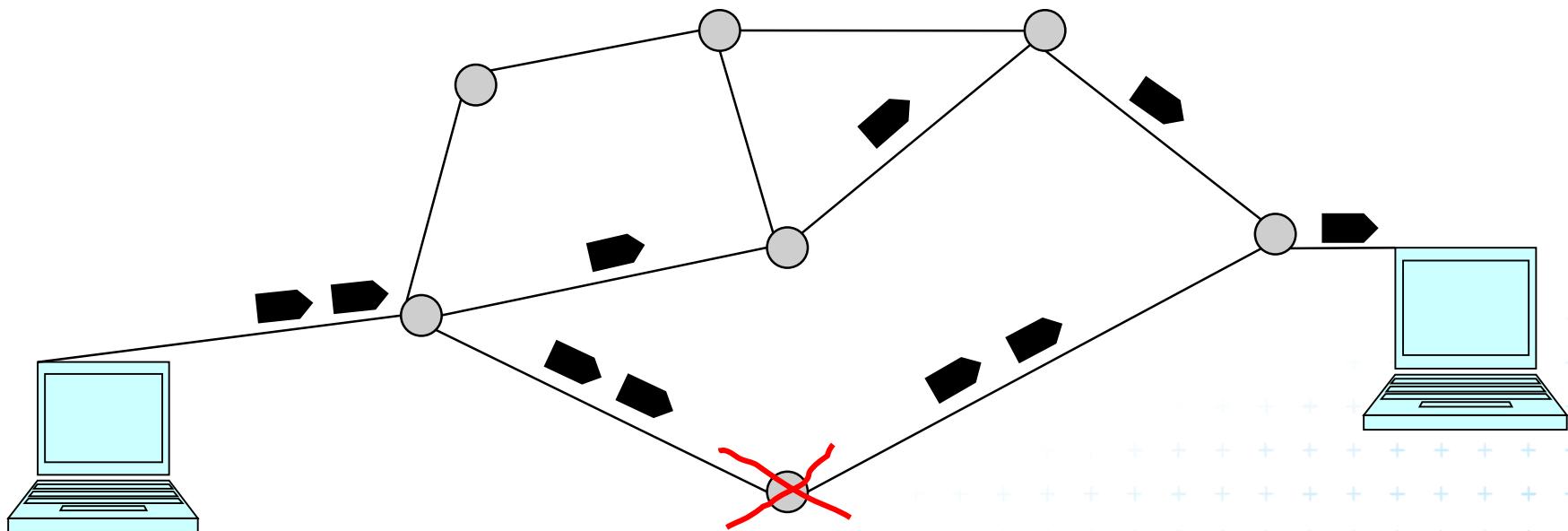
Packet - elementární datová jednotka procházející přes síť

Základní protokoly:

- Internet Protocol (IP) a Transmission Control Protocol (TCP)



Přenos paketů



DCGI



Směrování packetů

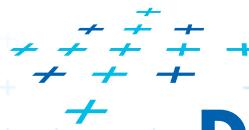
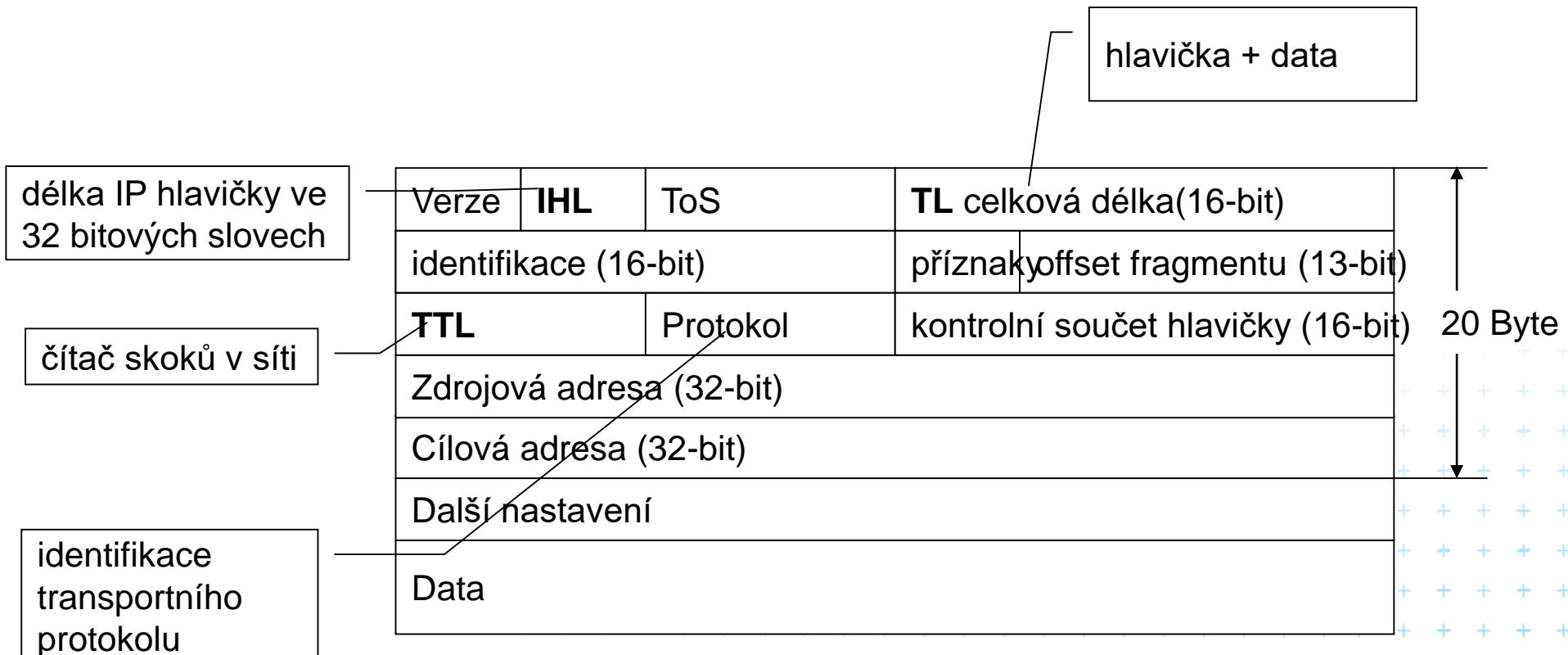
- Routery rozhodují o posílání packetů podle své lokální znalosti
- Ta je uložena v routovací tabulce
- Tabulka je buď statická nebo dynamicky se měnící
- Aktualizaci tabulky zajišťují speciální protokoly
- Většina routerů má statickou konfiguraci



DCGI



Struktura IP paketu



IP adresa

- 4 byte = 32 bit => ~~2³² možných adres~~
- zápis po jednom byte
 - 192.168.27.11
 - 147.32.80.132
- adresa má části, které adresují konkrétní počítač a podsít'
- 3 základní třídy IP adres





Struktura IP adresy

Třída	Formát	Zaměření	Bity vyšších řádů	Rozsah adres	Max počet zařízení
A	N.H.H.H	Několik velikých organizací	0	1.0.0.0 až 126.0.0.0	16 777 214 ($2^{24} - 2$)
B	N.N.H.H	Středně veliké organizace	1, 0	128.1.0.0 až 191.254.0.0	65 543 ($2^{16} - 2$)
C	N.N.N.H	Malé organizace	1, 1, 0	192.0.1.0 až 223.255.254.0	254 ($2^8 - 2$)
D	N/A	Multicast	1, 1, 1, 0	224.0.0.0 až 239.255.255.255	N/A
E	N/A	Experimentální	1, 1, 1, 1	240.0.0.0 až 254.255.255.255	N/A



DCGI



Speciální IP adresy

Tvar adresy	Význam
0.0.0.0	Tento počítač v rámci této sítě. Tato adresa se běžně nepoužívá a není většinou implementována
0...0.počítač	Některý počítač na této síti
síť.0...0	Adresa sítě samotné
síť.1...1	Všechny počítače v rámci dané sítě. Na místě adresy počítače jsou samé jedničky. Lze zaslat i na vzdálenou síť.
111....1 (samé jedničky)	Broadcast, neboli oběžník všem počítačům v rámci lokální sítě. Routery tento oběžník nepředávají dále, aby tím zabránily zahlcení Internetu broadcasty.
127.cokoliv	Loopback, neboli programová smyčka. Adresuje počítač samotný. Paket není propagován síťovým rozhraním mimo počítač samotný. Obvykle se používá pouze adresa 127.0.0.1.



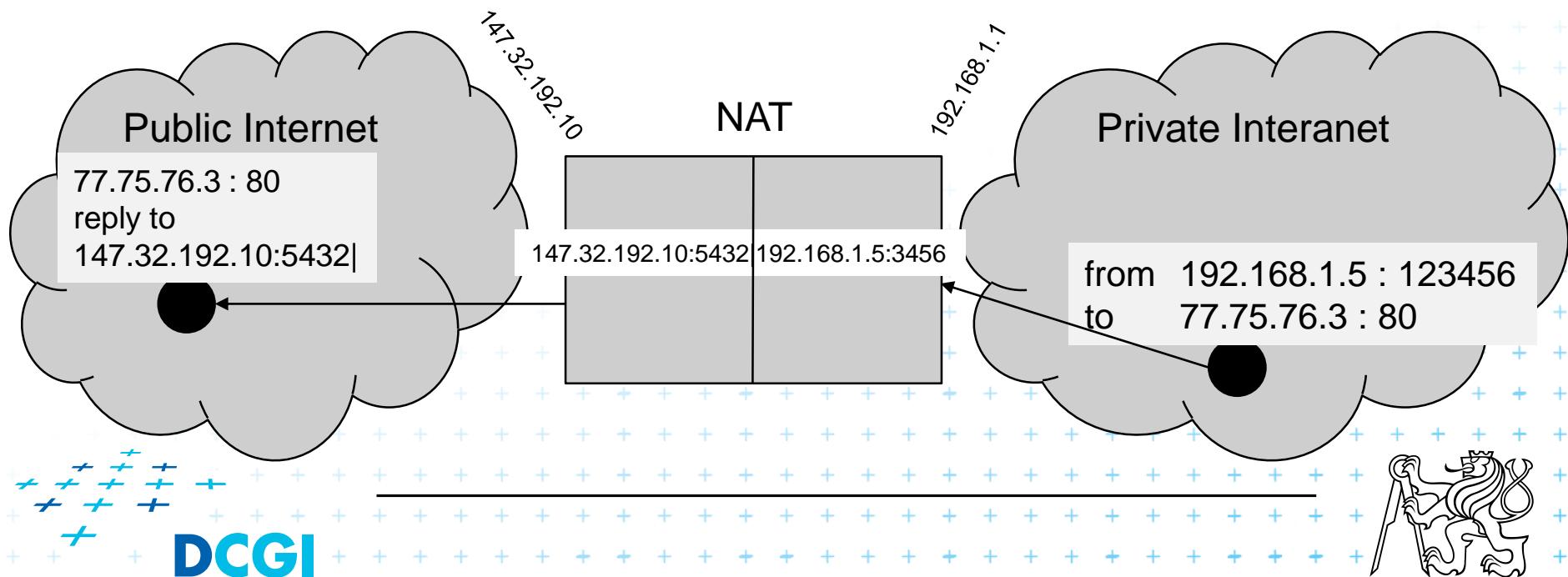
Speciální IP adresy II

- Některé IP adresy nejsou předávány routery dále
 - Umožňuje to vytvářet nezávislé lokální sítě, intranety
 - Adresy z těchto rozsahů nejsou propagovány routery
-
- 192.168.x.x
 - 172.16.x.x
 - 10.x.x.x



Jak komunikují stroje s privátní adresou?

- V rámci své sítě podle adresy
- V rámci internetu jsou vidět pod stejnou veřejnou adresou (NAT – masquerading)



Protokoly vyšších vrstev

■ TCP (Transmission Control Protocol)

- Zavádí porty (16 bit). Aplikace poslouchá na IP adresu a TCP portu.
- Vytváří virtuální okruhy
- Zaručuje doručení data, v případě ztráty paketu
- Zaručuje pořadí doručení paketů
- Je základním protokolem pro většinu aplikací

■ UDP (User Datagram Protocol)

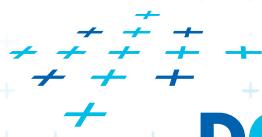
- Zavádí porty (16 bit). Stejný princip jako u TCP, ale čísla portů UDP a TCP jsou nezávislá
- Nezaručuje doručení dat
- Nezaručuje pořadí
- Vhodný pro aplikace typu video streaming, voice over IP



TCP versus UDP

TCP zaručuje doručení paketů. Příjemce paketu odpovídá odesilateli potvrzující paket. Datový tok pro aplikaci je zastaven do doby, než jsou k dispozici kompletní data. Je vhodný pro aplikace, kde je třeba zajistit správné a kompletní doručení dat.

UDP nezaručuje doruční ani správné pořadí paketů. Pakety se nepotvrzují. Vhodný je pro aplikace, které jsou orientované na datový tok a nesmějí čekat na vyřešení problémů. Příkladem jsou streaming zvuku a videa.



TCP protokol

■ TCP (Transmission Control Protocol)

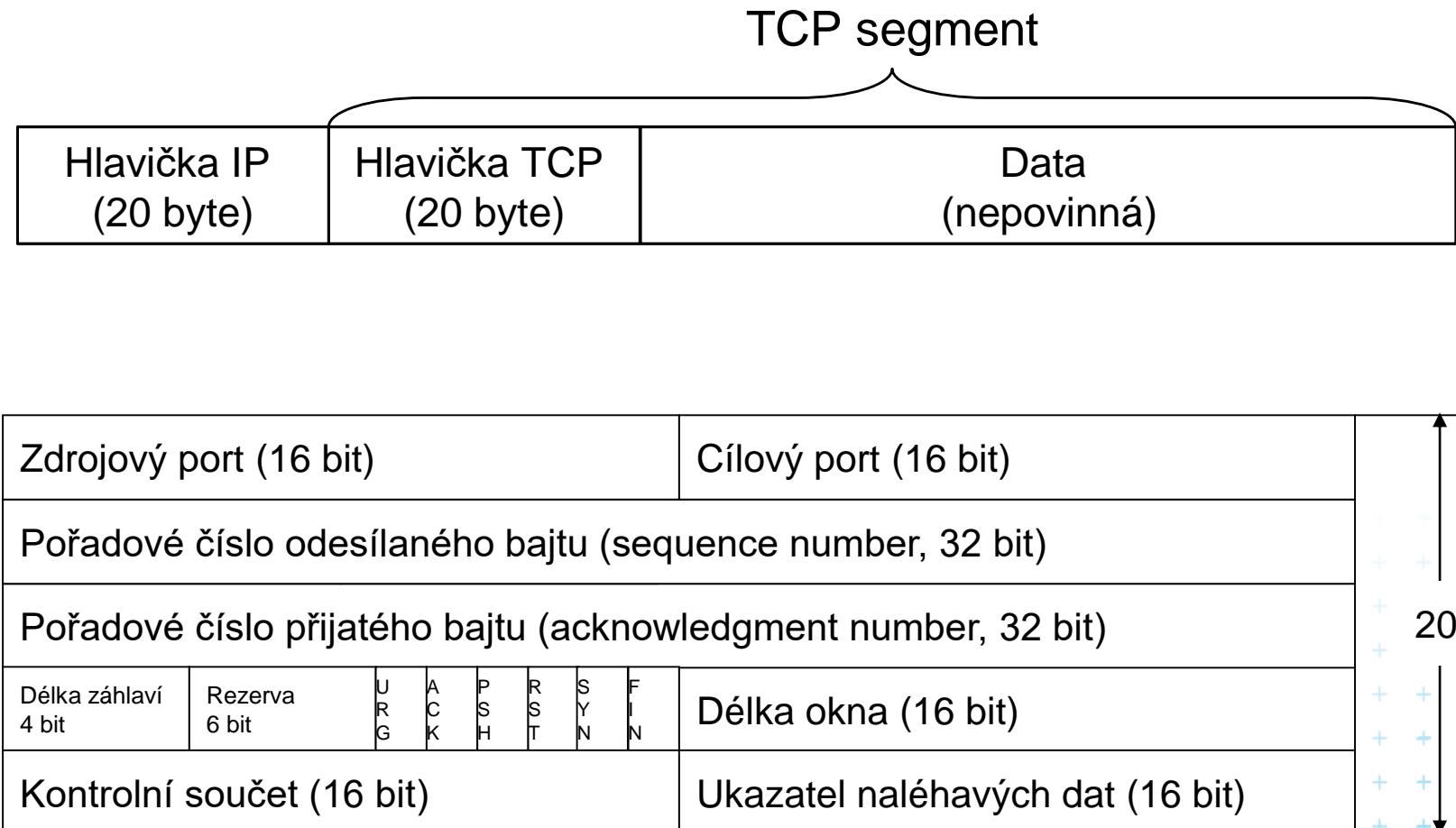
- Zavádí porty (16 bit). Aplikace poslouchá na IP adresu a TCP portu.
- Vytváří virtuální okruhy
- Zaručuje doručení data, v případě ztráty paketu
- Zaručuje pořadí doručení paketů
- Je základním protokolem pro většinu aplikací

■ Další protokol nad IP je UDP (User Datagram Protocol):

- Nezaručuje doručení dat a pořadí
- Vhodný pro aplikace typu video streaming, voice over IP



Struktura TCP paketu

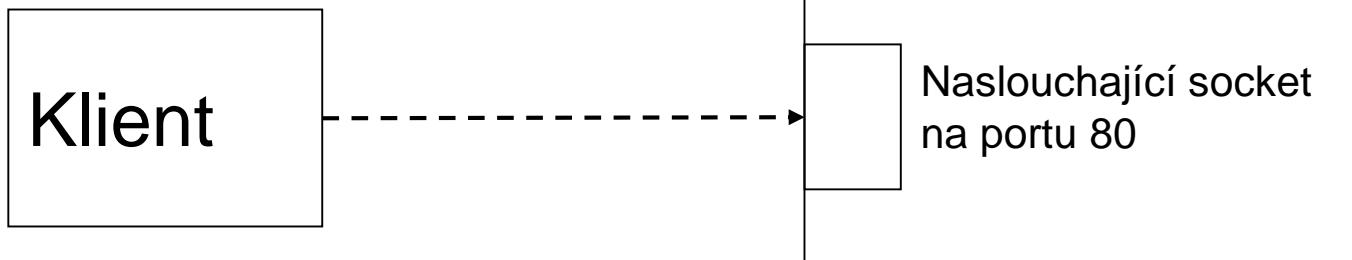


DCGI

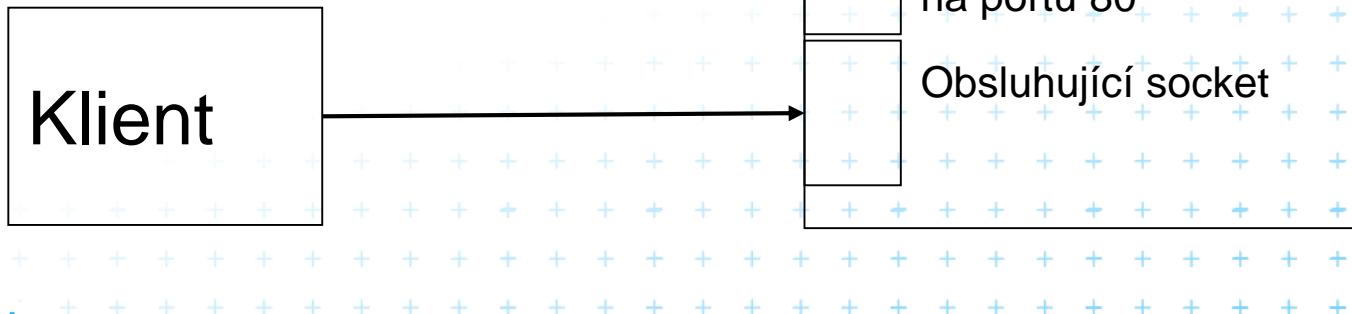


Navazování spojení

1. Navázání spojení

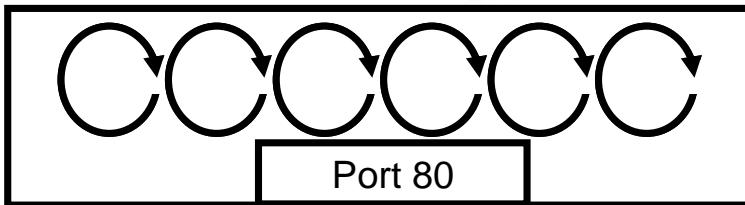


2. Vlastní komunikace



Obsluha požadavků serverem

Jeden Server

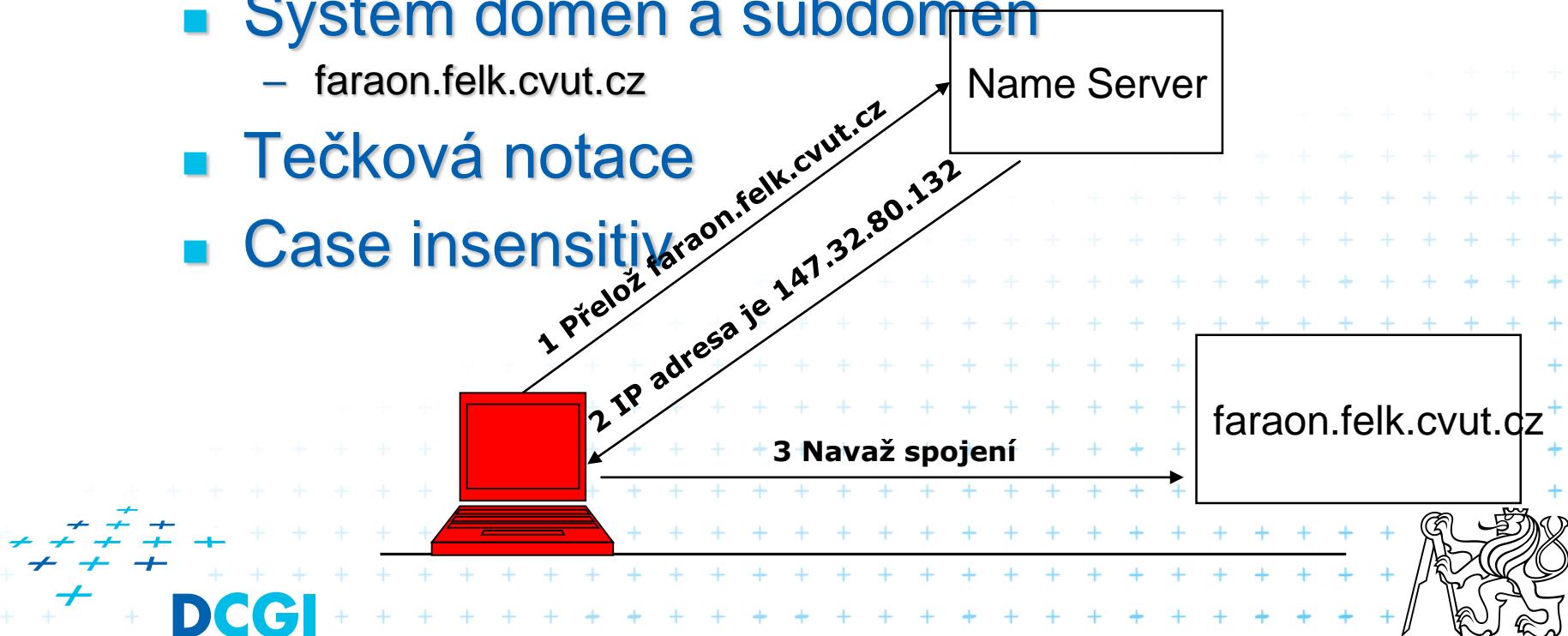


Více Klientů



Systém DNS

- Domain Name System
- Celosvětově distribuovaná databáze jmen
- Překládá textově zapsaná jména na IP adresy
- Systém domén a subdomén
 - faraon.felk.cvut.cz
- Tečková notace
- Case insensitivity



HTTP protokol

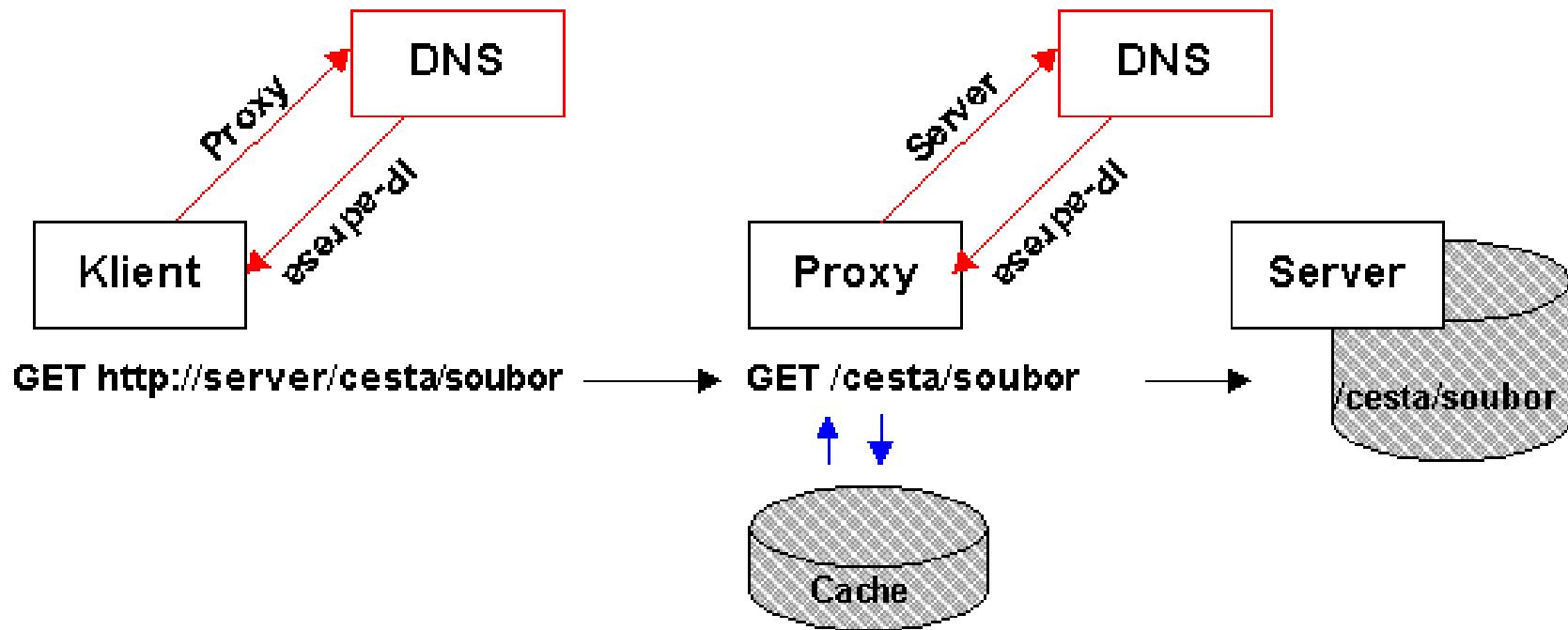
- Základní protokol pro službu WWW
- HTTP → TCP → IP
- Textový protokol
- Bezestavový
 - Dotaz
 - Odpověď
 - Nikdo si nic nepamatuje



DCGI



Proxy



DCGI



World Wide Web (WWW)

- Počátek služby v roce 1989
- Jednoduché principy + nízké náklady = masové rozšíření
- Bouřlivý rozvoj: mnoho rozšíření a aplikací
- Základní prvky:
 - HTTP – protokol pro komunikaci (klient/server)
 - URL – schéma pro lokalizaci zdrojů
 - HTML – jazyk pro zápis hypertextových dokumentů



DCGI



HTTP dotaz

- dotazovací řádek (hlavička, cesta, protokol)
- hlavičky blíže popisující dotaz
- prázdný řádek
- tělo dotazu

Hlavičky:

- GET
- POST
- PUT
- HEAD
- ...

```
GET /index.html HTTP/1.0
Accept: */
Accept-Language: cs
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1; ....)
Host: www.google.com
Connection: Keep-Alive
Cookie: PREF=ID=6ce8e13:.....
* prázdný řádek *
```



DCGI



HTTP odpověď

- stav
- informace
- prázdný řádek
- tělo odpovědi
(HTML dokument)

Stavy:

- 200 - OK
- 403 – Forbidden
- 404 - Not found
- ...

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Content-Encoding: gzip
Server: GWS/2.1
Content-Length: 1385
Date: Mon, 28 Feb 2005 22:11:05 GMT
* prázdný řádek *
<html><head><title>Webing</title></head>
<body>
....
</body>
</html>
```

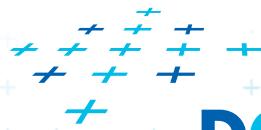


DCGI



URL (Uniform Resource Locator)

- Identifikace zdrojů uložených na serverech
- Syntax definována v RFC 1738 jako podmnožina Uniform Resource Identifier (URI)
- Obecná syntaxe: <scheme>:<scheme specific part>
 - Možná schémata (<scheme>):
ftp, gopher, http, mailto, news, nntp, telnet, wais...
 - <scheme specific part>:
//<user>:<password>@<host>:<port>/<url-path>
 - <user> & <password> jsou nepovinné a následované @
- Syntax pro <url-path> závisí na schématu



URL pro HTTP (tj. pro web)

<schema>//<user>:<password>@<host>:<port>/<url-path>

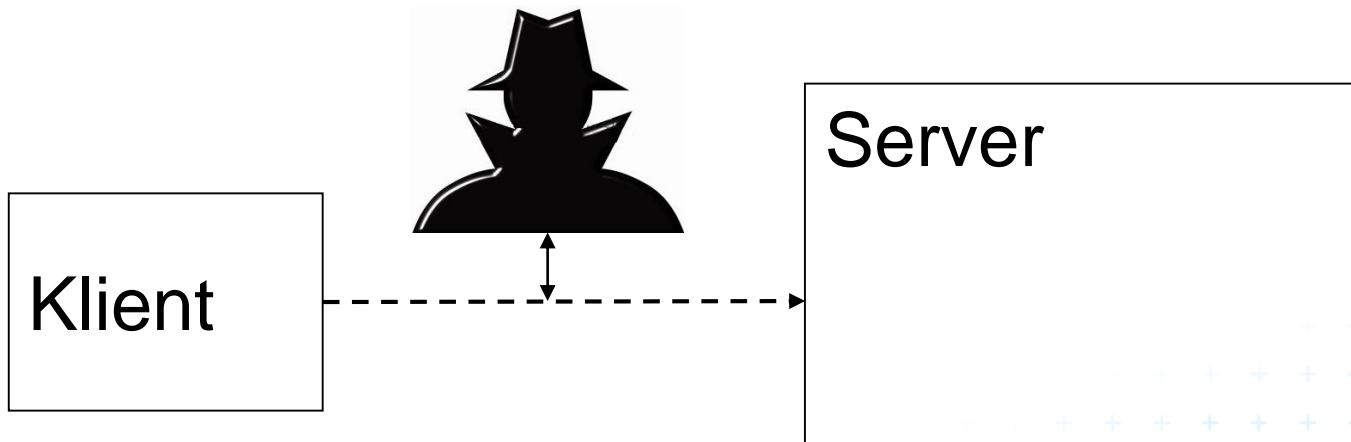
- <schema>: http (případně https)
- <host> - adresa (IP alebo domain name) serveru, na kterém je zdroj
- <port> - obykle 80
- <url-path> - cesta k zdroji na webovém serveru

<https://cw.fel.cvut.cz/wiki/courses/b6b39zwa/classification/start>



HTTP vs HTTPS

- HTTP nezabezpečuje spojení, problém s „man in the middle“.



Řešení je zašifrovat skomunikaci. Jak?

Klasický přístup je sdílené tajemství – šifrovací klíč,
tzv. symetrická šifra

1. Klient vygeneruje šifrovací klíč
 2. Klient ho pošle serveru
 3. Oba poté šifrují komunikaci.
-
4. ...pomůže to?
... moc ne, protože „man in the middle“ problém přetrhává



DCGI



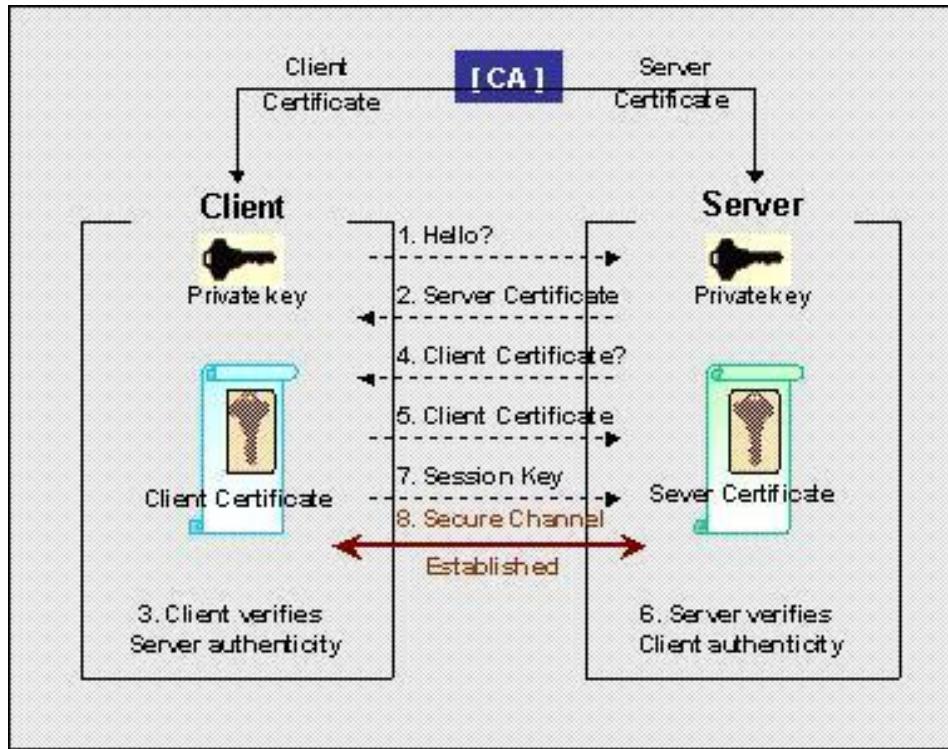
Jiný přístup

Asymetrická šifra je založena na matematickém postupu, kdy se vygenerují dva klíče. Jedním se dá zpráva zašifrovat, druhým rozšifrovat.

1. Strana A vygeneruje oba klíče. Ten k zašifrování se nazývá veřejný, ten k odšifrování je privátní.
2. A pošle straně B veřejný klíč.
3. B ho použije k zašifrování sdíleného tajemství.
4. A pomocí svého privátního klíče získá tajemství.
5. A i B přejdou na symetrickou šifru na základě sdíleného tajemství.



Asymetrické šifrování



Zdroj: <https://tender.eprocurement.gov.in/DigitalCertificate/faqs/gfaqs.htm>

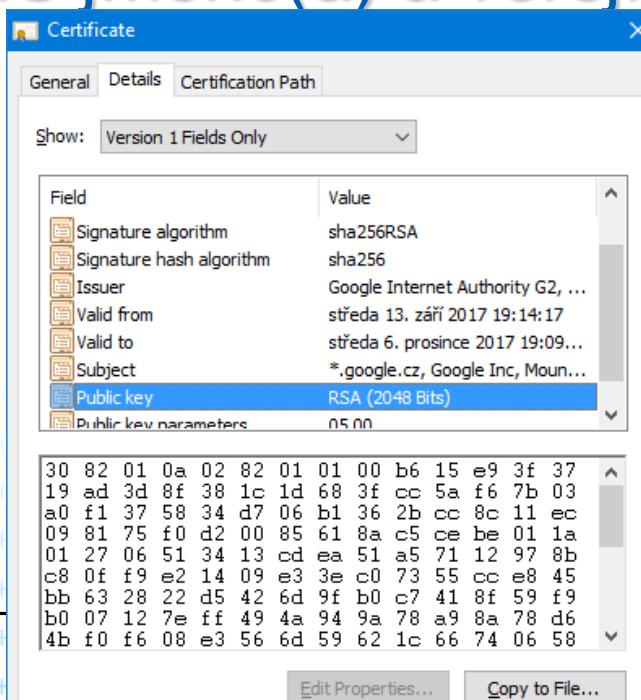


DCGI



Co to jsou certifikáty

- Certifikát je dokument, ve kterém je spojen veřejný klíč se jmény.
- Je vystaven někým, komu věříme (veřejná autorita).
- Obsahuje DNS jméno(a) a veřejný klíč, má platnost atd.



Důsledky

1. Bezpečné, šifrované spojení.
2. Man in the middle není možné.
3. Důvěra v to, že mluvím s ověřeným protějškem.
 1. Certifikát je vydán důvěryhodnou autoritou.
 2. Certifikát říká, že ten, s kým mluvím, se nějak jmenuje.
4. Lze ověřit jak server, tak klienta.
5. V prohlížeči se zobrazuje zámek v adresním řádku.



Ověřeno od CA

6. Seznam důvěryhodných CA je zabudován v OS

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Start
AddTrust External CA Root	AddTrust External CA Root	30.05.2020	Server Authentication...	ServerAuthenticat...	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13.05.2025	Server Authentication...	DigiCert Baltimore ...	
Certum CA	Certum CA	11.06.2027	Server Authentication...	Certum	
Certum Trusted Network CA	Certum Trusted Network CA	31.12.2029	Server Authentication...	Certum Trusted Net...	
Class 3 Public Primary Certificate...	Class 3 Public Primary Certificate...	02.08.2028	Secure Email, Client...	VerSign Class 3 Pu...	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31.12.1999	Time Stamping	Microsoft Timesta...	
Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	10.07.2019	Secure Email, Serve...	Deutsche Telekom ...	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10.11.2031	Server Authentication...	DigiCert	
DigiCert Global Root CA	DigiCert Global Root CA	10.11.2031	Server Authentication...	DigiCert	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Ro...	10.11.2031	Server Authentication...	DigiCert	
DST Root CA X3	DST Root CA X3	30.09.2021	Secure Email, Serve...	DST Root CA X3	
Entrust Root Certification Auth...	Entrust Root Certification Authority	27.11.2026	Server Authentication...	Entrust	
Entrust Root Certification Auth...	Entrust Root Certification Authority	07.12.2030	Server Authentication...	Entrust.net	
Entrust.net Certification Author...	Entrust.net Certification Authority	24.07.2029	Server Authentication...	Entrust (2048)	
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	22.08.2018	Secure Email, Serve...	GeoTrust	
GeoTrust Global CA	GeoTrust Global CA	21.05.2022	Server Authentication...	GeoTrust Global CA	
GeoTrust Primary Certification ...	GeoTrust Primary Certification Authority	17.07.2036	Server Authentication...	GeoTrust	
GeoTrust Primary Certification ...	GeoTrust Primary Certification Authority	02.12.2037	Server Authentication...	GeoTrust Primary C...	
GlobalSign	GlobalSign	18.03.2029	Server Authentication...	GlobalSign	

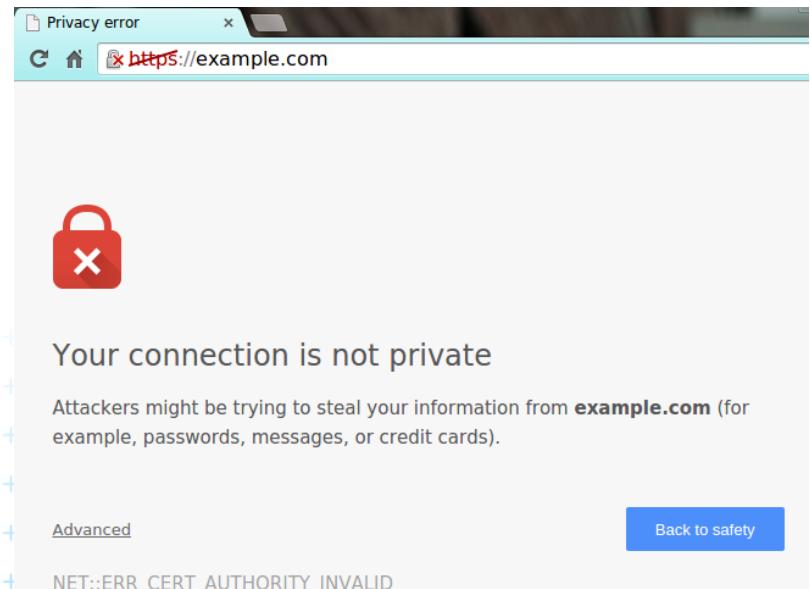
Trusted Root Certification Authorities store contains 55 certificates.



Problémy a výhody

■ Self signed certificate

- certifikát není ověřen důvěryhodnou autoritou
- ale šifrování funguje
- nemohu tedy ověřit, že ten, s kým hovořím, je opravdu ten pravý
- používá se v případech, kdy si věříme, např. v intranetu



■ Výhody

- Google dává kladné body za důvěryhodné weby
- https je dnes standardem



DCGI

