Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

ŠTÁTNY PEDAGOGICKÝ ÚSTAV
NATIONAL INSTITUTE FOR EDUCATION

Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

# Internet: princípy a tvorba webu 1

## Predmet: Internet: princípy a tvorba webu

**Línia: Vlastný odborový kontext informatiky a informatickej výchovy**

Operačný program VZDELÁVANIE

EURÓPSKA ÚNIA
Európsky sociálny fond

Európska únia
Európsky sociálny fond

Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je spolufinancovaný zo zdrojov ES

# Internet: princípy a tvorba webu 1

**Garant predmetu:**

PaedDr. Roman Hrušecký
FMFI UK, Bratislava
hrusecky@fmph.uniba.sk

**Autori:**

Mgr. Miroslav Wagner, FMFI UK, Bratislava
PaedDr. Roman Hrušecký, FMFI UK, Bratislava

## Identifikácia modulu

| | |
|---|---|
| **Aktivita projektu:** | 1.2 Vzdelávanie nekvalifikovaných učiteľov informatiky na 2. stupni ZŠ a na SŠ |
| **Línia aktivity:** | Vlastný odborový kontext informatiky a informatickej výchovy |
| **Predmet:** | Internet: princípy a tvorba webu |

## Zaradenie modulu


Modul tvorí prvú časť predmetu Internet: princípy a tvorba webu a nadväzuje na predmet Digitálna gramotnosť učiteľa.

## Abstrakt modulu

Účastníci vzdelávania sa oboznámia s najbežnejšími službami z pohľadu používateľa internetu, spôsobom ich fungovania a využívania. Oboznámia sa aj s ich variantmi pre bezpečnejší prenos osobných údajov prostredníctvom internetu.

# Obsah

# Úvod

## Softvérové a hardvérové požiadavky a odporúčania

- počítač s pripojením na internet
- povolené porty na komunikáciu smerom do internetu 20, 21, 22, 80, 443, 465, 993, 995, 8182
- softvér v slovenských mutáciách: prehliadač Mozilla Firefox 3.5+, Internet Explorer 7+, e-mailový klient Mozilla Thunderbird 3+ (najlepšie portable verzia), FTP klient FileZilla alebo iný s podobnou funkcionalitou.

# Cieľ modulu

Modul je úvodným modulom predmetu Internet: princípy a tvorba webu. V rámci tohto modulu účastníci vzdelávania získajú poznatky o základných internetových službách a ich základných princípoch fungovania. Oboznámia sa s dôležitosťou a spôsobom zabezpečenia bezpečnej komunikácie pri využívaní internetových služieb. V závere sa účastníci oboznámia so základnými možnosťami vlastnej prezentácie na internete.

# Vstupné vedomosti

## Požadované prerekvizity

Pred absolvovaním modulu musí mať účastník absolvované moduly *Základná digitálna gramotnosť* (2DG1), *Základy hardvérového a softvérového vybavenia počítača* (2DG3), *Digitálny svet* (2MŠ1), *Digitálne technológie pre učiteľa 2* (2DG5).

## Predpokladané vstupné vedomosti, skúsenosti a zručnosti

Účastník vie pracovať s prehliadačom webových stránok a e-mailovým klientom.

# Úvod do problematiky

Bežnou súčasťou nášho života sa čoraz viac stáva každodenné využívanie služieb internetu. Či už sa jedná o bankové služby (*internet banking*), posielanie elektronických listov (*e-mail*), vzájomnú komunikáciu prostredníctvom hlasu, textu a obrazu (*Skype, Google Talk, ICQ, Jabber, ...*), prístup k informáciám rôzneho druhu (*on-line encyklopédie, spravodajské portály, ...*) a podobne, vždy pri tom využívame nejakú službu internetu. V predchádzajúcich moduloch (*Digitálny svet* (2MŠ1), *Základná digitálna gramotnosť* (2DG1), *Základy hardvérového a softvérového vybavenia počítača* (2DG3)) sme sa dozvedeli základné informácie o vzniku a vývoji internetu a používali sme niektoré z jeho služieb. V nasledujúcom texte sa dozvieme základné princípy fungovania najrozšírenejších služieb internetu.

## Komunikácia a IP adresa

Počítače ako aj všetky ostatné zariadenia pripojené do počítačovej siete sú rôzneho hardvérového ako aj softvérového vybavenia, a napriek tomu dokážu vzájomne komunikovať. Vzájomná komunikácia je zabezpečená využívaním presne definovaných pravidiel a štandardov. Tieto pravidlá a štandardy označujeme ako **komunikačné protokoly**. V rámci internetu sa na vzájomnú komunikáciu využíva sada protokolov označovaná ako **sada protokolov TCP/IP** *(Transmission Control Protocol/Internet Protocol)*.

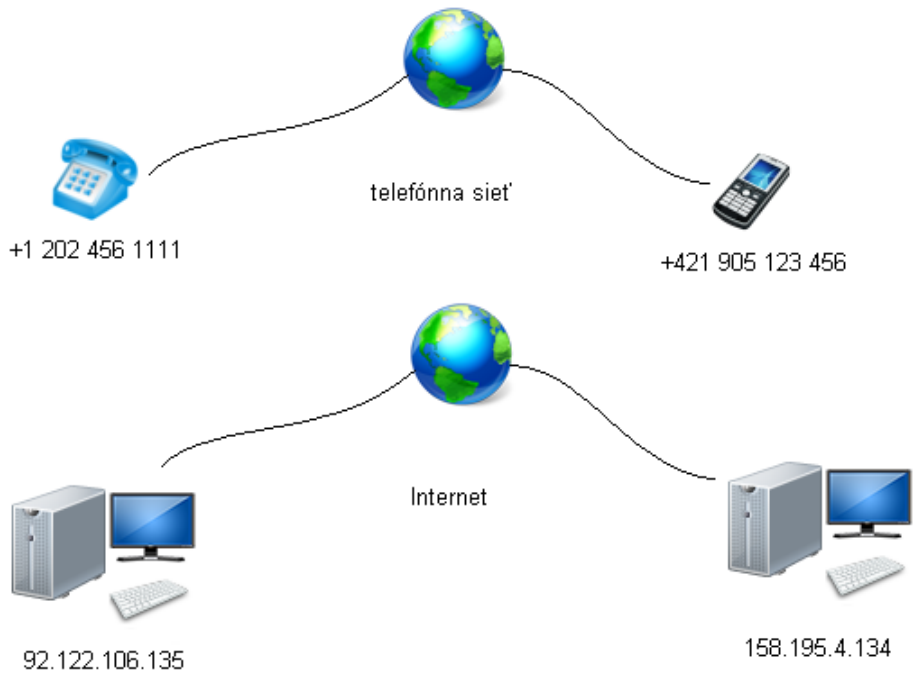
**Protokol** je sada preddefinovaných pravidiel, ktoré určujú ako budú dve a viac zariadení vzájomne komunikovať a vymieňať si údaje.

Aby mohli zariadenia v sieťach postavených na protokoloch TCP/IP vzájomne komunikovať, je potrebné zabezpečiť jedinečnú adresu pre jednotlivé zariadenia. Túto adresu označujeme ako **IP adresa** zariadenia.

IP adresu predstavuje **32 bitové číslo** zapísané po jednotlivých bajtoch v dekadickom tvare oddelených bodkou – napr. **158.195.4.134**. IP adresu si môžeme predstaviť ako telefónne číslo pre konkrétny telefónny prístroj v telefónnej sieti. Rovnako ako nemôžu mať dva rôzne telefóny rovnaké číslo, tak aj dve rôzne zariadenia na internete nemôžu mať rovnaké IP adresy.

1 bajt=8 bitov a teda 32 bitov=4 bajty, **1 bajt** predstavuje decimálne hodnoty 0..255

Uvedený zápis IP adresy označujeme aj ako IPv4 adresa. V prípade používania IPv4 sa v súčasnosti stále viac prejavuje nedostatok voľných IP adries. Preto sa už niekoľko rokov pripravuje prechod na IPv6. Adresy v IPv6 predstavuje 128 bitové číslo (adresy v IPv4 predstavuje 32 bitové číslo) zapísané ako osem skupín štyroch hexadecimálnych čísel oddelených dvojbodkou – napr. 2001:0DB8:0000:CD30:0123:4567:89AB:CDEF.

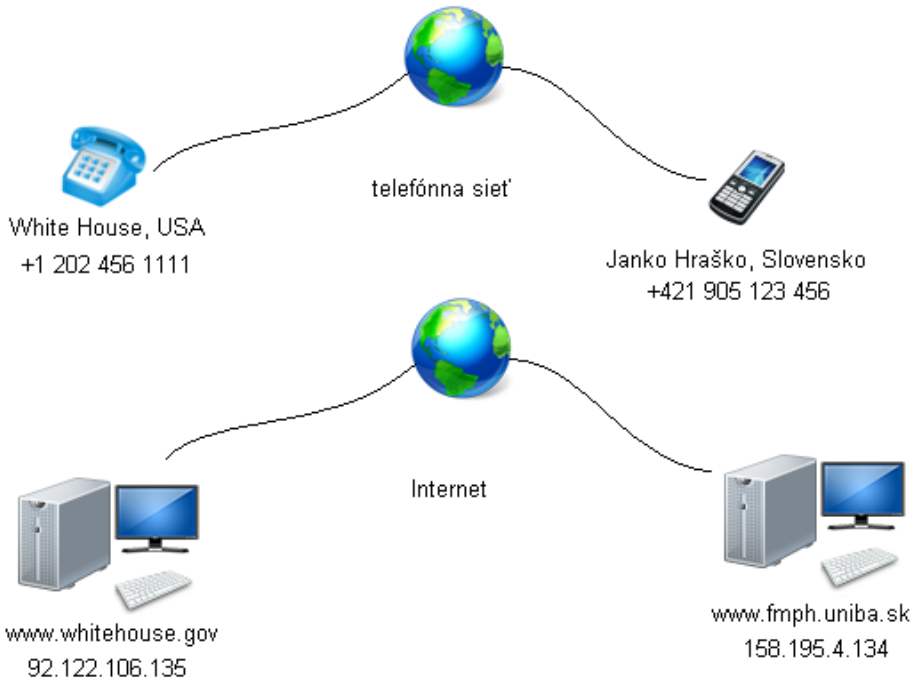



*Obrázok 1 - Adresovanie zariadení v telefónnej sieti vs. v internete*

Ak potrebujeme zistiť pod akou IP adresou v internete vystupuje náš počítač, stačí sa pozrieť na stránku www.whatismyip.com.

## Menné adresy a služba DNS

Pre ľahšie zapamätanie si adresy cieľového zariadenia namiesto čísel používame **menné adresy** tzv. **hostname** - napr. **www.fmph.uniba.sk** namiesto IP adresy **158.195.4.134**.




*Obrázok 2 – Pomenovanie zariadení v telefónnej sieti vs. v internete*

V malej sieti svoj hostname propagujú samotné zariadenia. V takom prípade sa používajú skrátené názvy (napr. *pc01*, *sekretariat*, *jankopc* ...), ktoré sú uvedené v nastavení operačného systému zariadenia ako názov počítača. Vzhľadom na rozľahlosť internetovej siete však takéto propagovanie nie je reálne. Preto sa používajú jednoznačné celé názvy zariadení pripojených do internetovej siete, tzv. **internetové domény** alebo **doménové mená** (napr. *www.fmph.uniba.sk*, *www.whitehouse.gov*, ...).

Doménové meno zariadenia označuje zariadenie v sieti internet.
Hostname zariadenia môže označovať zariadenie v lokálnej sieti.

Aby sme mohli používať doménové mená namiesto IP adries, existuje služba **DNS** (*Domain Name System*), ktorá zadané doménové meno prekladá na IP adresu. Teda, ak do webového prehliadača zadáme adresu *www.fmph.uniba.sk*, prehliadač za pomoci služby DNS zistí jej IP adresu a potom kontaktuje zariadenie na požadovanej adrese. Môžeme si tento postup predstaviť ako súbor telefónnych zoznamov, v ktorom program vyhľadá požadované číslo podľa zadaného mena a potom toto číslo zavolá. Pre fungovanie internetu je služba DNS kľúčová.

Vzhľadom na dôležitosť služby a na veľké množstvo záznamov je služba DNS navrhnutá ako decentralizovaný hierarchický systém so stromovou štruktúrou. Jednotlivé časti štruktúry sú spravované rôznymi servermi. Tieto servery sa nazývajú **name servery**. V prípade výpadku name servera nedôjde ku kompletnému výpadku celej služby DNS, ale iba časti spravovanej vypadnutým name serverom. Aby sa obmedzili aj výpadky jednotlivých častí, kópie týchto častí štruktúry sa distribuujú na iné name servery. Tieto servery označujeme ako sekundárne name servery. V prípade výpadku hlavného (primárneho) name servera jeho úlohu prevezmú sekundárne name servery.

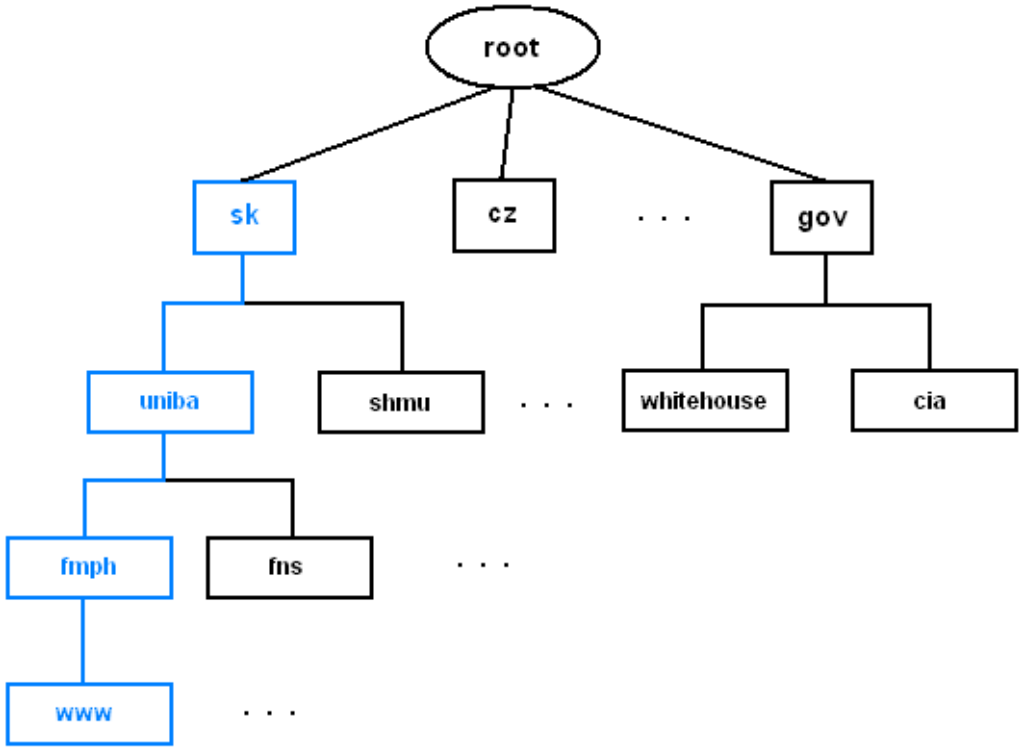
Na vrchole stromovej hierarchie DNS je **koreň (root)**, ktorý spravujú tzv. *koreňové servery* (*root servers*). Pod koreňom sa nachádzajú domény prvej úrovne tzv. **domény najvyššej úrovne** (**top-level domains, TLD**). Existujú tri typy domén najvyššej úrovne:

Aktuálny zoznam domén najvyššej úrovne môžete nájsť na stránke http://www.iana.org/domains/root/db/

- *národné* – dvojznakový kód pridelený jednotlivým krajinám (*sk* pre Slovensko, *at* - pre Rakúsko, *cz* pre Českú republiku, ...),
- *generické* - všeobecné domény nezviazané s konkrétnou krajinou určené jednotlivým typom organizácií (*gov* - vládne, *org* - neziskové organizácie, *mil* - vojenské, …),
- *infraštruktúrne* - využívané pre vnútorné internetové mechanizmy (*arpa*, *test*, ...).

Po doménach najvyššej úrovne nasledujú domény druhej úrovne atď. Pre doménové meno *www.fmph.uniba.sk* predstavuje doménu najvyššej úrovne *sk*, druhej úrovne *uniba*, tretej úrovne *fmph* atď.

V doménových menách sa donedávna mohli používať len niektoré znaky (písmena a až z, čísla a pomlčky). V súčasnosti sa plánuje rozšíriť množinu povolených znakov aj o národné znaky jednotlivých krajín (písmena s diakritikou, čínske znaky a podobne).




*Obrázok 3 - Interpretácia doménového mena www.fmph.uniba.sk v stromovej štruktúre služby DNS*

| | |
|---|---|
| **Zadanie 1** | Otvorte webový prehliadač a zadajte adresu 158.195.4.134. Potom zadajte adresu www.fmph.uniba.sk. Porovnajte rozdiel.<br><br>Rovnako postupujte s dvojicou adries 81.89.48.15 a www.shmu.sk. |
| **Cieľ** | Zistiť, ako spolu súvisí IP adresa a menná adresa stránky. |

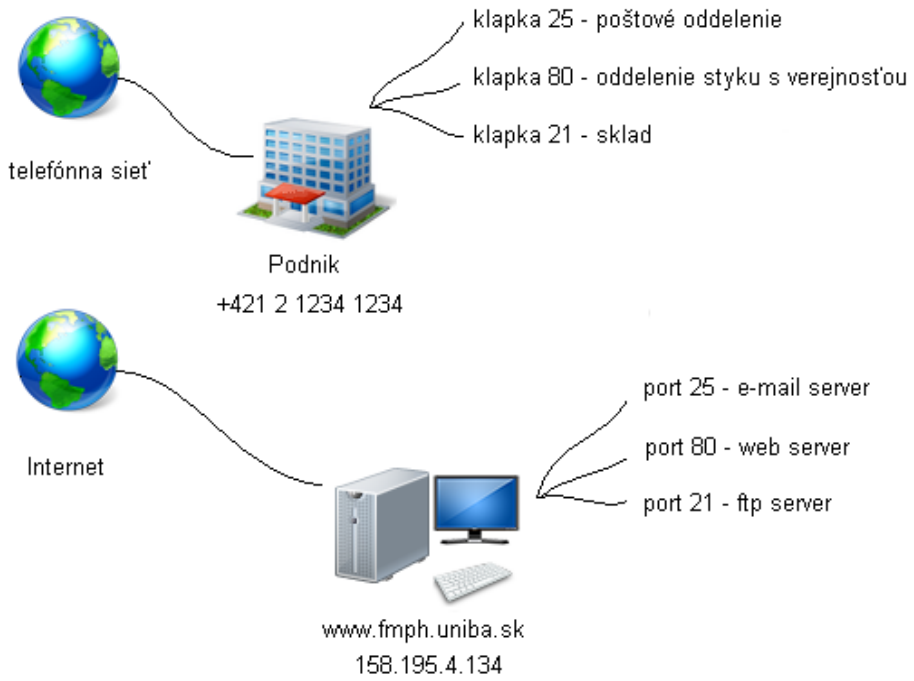
Pojem **server** používame často v spojení označujúcom hardvér počítača, no pojem server označuje aj softvér poskytujúci nejakú sieťovú službu.

## Server a port služby

Aby sme mohli využiť nejakú službu na internete, musíme sa spojiť so zariadením, ktoré túto službu poskytuje. Tieto zariadenia zvyčajne označujeme pojmom **server**. Pojem server sa používa aj na označenie softvéru poskytujúceho nejakú sieťovú službu.

Na jednom fyzickom zariadení môže byť súčasne spustených niekoľko takýchto softvérov – serverových služieb, napríklad webový server, poštový server, súborový server a podobne. Tak ako jednoznačne určujeme adresu zariadenia, tak musíme jednoznačne určiť, o ktorú službu na danom zariadení máme záujem. Každá serverová služba na zariadení má svoju vlastnú identifikáciu označovanú ako **port služby**.

Pri určení cieľového spojenia sa zadá konkrétna adresa zariadenia (IP alebo hostname) a číslo portu požadovanej služby tohto zariadenia. Týmto sa určí, o ktorú službu na danom zariadení máme skutočne záujem. Ak by sme to chceli uviesť v už spomínanej analógii s telefónnou sieťou, tak je to ako telefónne číslo (to predstavuje IP adresu) do nejakého podniku. V podnikoch sa zvyčajne používajú telefónne ústredne, ktoré umožňujú spojenie na jednotlivé oddelenia podniku zadaním *telefónnej klapky* daného oddelenia. Táto klapka predstavuje port požadovanej služby na danej IP adrese (telefónne číslo podniku).




*Obrázok 4 - Viac poskytovaných služieb jedným zariadením*

Niektoré štandardné internetové služby majú preddefinované porty, napríklad webový server zvyčajne používa port 80, e-mailový server na odosielanie správ port 25 a podobne. To je dôvod prečo často pri určení požadovaného cieľa nemusíme zadávať port služby. Vtedy program automaticky použije štandardný port.

| | |
|---|---|
| **Zadanie 2** | Vo webovom prehliadači zadajte cieľovú adresu www.statpedu.sk:80 – zápis **:80** v prehliadači znamená použitie služby na porte 80 zadanej adresy. Pri štandardných portoch prehliadač automaticky hodnotu portu v paneli s adresou odstráni.<br><br>Potom zadajte adresu www.statpedu.sk. Porovnajte zobrazené stránky. |
| **Cieľ** | Zistiť, že v niektorých prípadoch pri štandardných portoch príslušné programy číslo portu služby automaticky použije. |

| | |
|---|---|
| **Zadanie 3** | Vo webovom prehliadači zadajte cieľovú adresu virgo.nw.fmph.uniba.sk:8182 - zápis **:8182** v prehliadači znamená použitie služby na porte 8182 zadanej adresy.<br><br>Potom zadajte adresu virgo.nw.fmph.uniba.sk. Porovnajte zobrazené stránky. |
| **Cieľ** | Zistiť, že v prípade neštandardných portov je nutné číslo portu danej služby doplniť. V tomto prípade na porte 8182 čaká na spojenie iný webový server ako na štandardnom porte 80. |

## Bezpečnosť

Pri využívaní internetových služieb často potrebujeme po sieti prenášať aj údaje, ktoré by nemali byť videné nepovolanými osobami. Najčastejšie je to prihlasovacie meno a heslo (napríklad do internet bankingu, e-mailu, prístupu k rozličným službám a podobne). Niekedy potrebujeme prenášať aj naše osobné údaje (napr. pri komunikácii s úradmi, vytvorenie účtu v nejakej internetovej službe), prípadne osobné údaje iných ľudí (napr. ekonómovia vo firmách pri komunikácii s poisťovňami), ekonomické údaje, údaje platobnej karty pri internetových obchodoch a mnohé ďalšie. Kým tieto údaje dorazia k serveru, ktorému sú určené, prechádzajú množstvom rozličných sieťových zariadení zabezpečujúcich chod internetu. Tieto údaje je teda možné na mnohých miestach po trase prenosu odchytiť a následne ich zneužiť. Preto je potrebné prenos týchto údajov ochrániť, napríklad vytvorením šifrovaného spojenia medzi komunikujúcimi zariadeniami. Ukážeme si, ako môžeme používať zabezpečenú komunikáciu pri mnohých internetových službách. V kapitole *Princíp dôveryhodnej komunikácie* si vysvetlíme princíp zabezpečenia dôveryhodnej komunikácie. V kapitole *Elektronický podpis* si vysvetlíme spôsob, akým je možné pri elektronických dokumentoch zabezpečiť náhradu podpisu z bežného života v elektronickom svete.

Bezpečnosť v internete nie je len o zabezpečení prenášaných údajov, ale aj o zabezpečení jednotlivých zariadení pripojených do siete. S niektorými rizikami a spôsobom ochrany sme sa zaoberali v predchádzajúcich moduloch (*Základy hardvérového a softvérového vybavenia počítača* (2DG3), *Základná digitálna gramotnosť* (2DG1)). V tomto module sa zameriame len na bezpečnosť z pohľadu prenášaných údajov.

| | |
|---|---|
| **Zadanie 4 – diskusia** | Používanie zabezpečenej komunikácie chráni údaje len po trase spojenia. Údaje je však možné neoprávnene získať aj priamo z našich počítačov. Kedy sa tak môže stať a ako sa tomu brániť? |
| **Návod** | Niektoré riziká a spôsoby ochrany sme si už spomínali v predchádzajúcich moduloch. Využite nasledujúce indície: aktualizácia, antivírus, anti-spyware, firewall, spúšťanie a inštalácia dôveryhodných programov a internetových služieb, voľba vhodného hesla a jeho bezpečné uloženie, používanie rôznych hesiel a podobne. |

# Služby internetu

Internet ponúka veľké množstvo rozličných služieb a ich počet sa neustále rozrastá. Keďže nie je reálne sa v rámci tohto modulu so všetkými službami oboznámiť, povieme si o najbežnejšie používaných službách internetu. K využívaniu jednotlivých internetových služieb potrebujeme mať na svojom počítači nainštalovaný špecializovaný program tzv. **klient**, ktorý zabezpečí komunikáciu so serverom poskytujúcim určenú službu a tiež zabezpečí vhodnú prezentáciu požadovaných údajov. Medzi takéto programy patria webový prehliadač, e-mailový klient, klient pre posielanie a príjem krátkych správ, ftp klient a podobne. Súčasné operačné systémy už často obsahujú väčšinu z týchto klientov. Niektoré je však nutné doinštalovať, rovnako ako je možné nainštalovať k existujúcim programom ich alternatívy od iných výrobcov.

**Služba** je úloha alebo operácia, ktorá je dostupná cez aplikáciu alebo program systému.

## WWW

V súčasnosti najpoužívanejšou službou internetu je **WWW** (*World Wide Web*), označuje sa aj ako webová služba.

**Vedeli ste, že...?**

World Wide Web vymyslel Tim Berners-Lee v roku 1989.

Ako sme sa už v predchádzajúcich moduloch dozvedeli, pre zobrazenie webových stránok potrebujeme špecializovaný program – webový prehliadač. Pomocou neho zašleme presnú požiadavku na zobrazenie požadovanej webovej stránky, tzv. **URI** (*Uniform Resource Identifier* - univerzálny identifikátor zdrojov).

**URI** - reťazec znakov s definovanou štruktúrou, ktorý presne určuje umiestnenie zdroja informácie na internete. Určuje komunikačný protokol, adresu servera, port služby, umiestnenie zdroja na serveri a prípadné parametre. Napríklad pre konkrétnu webovú stránku môže URI vyzerať napríklad takto: http://www.kezmarok.sk/navstevnik/o_meste/fotogaleria.htm

Prehliadač kontaktuje webový server (označuje sa aj ako web server, http server alebo httpd – http démon), ktorý mu potom požadovanú webovú stránku odošle. Prehliadač následne túto webovú stránku zobrazí. Komunikáciu medzi prehliadačom a webovým serverom zabezpečuje protokol **HTTP** (*Hypertext Transfer Protocol*). Z predchádzajúceho vyplýva, že HTTP protokol funguje na princípe požiadavka na server – odpoveď servera. Jedná sa o službu typu **klient-server**.

Spolu s požiadavkou na webovú stránku môže prehliadač odoslať aj niektoré doplňujúce informácie pre webový server – označenie a verziu prehliadača, spôsob kódovania národných znakov a podobne.

Ukážme si, čo sa deje, keď do webového prehliadača zadáme adresu www.nw.fmph.uniba.sk/dvui/demo.html. Po jej zadaní webový prehliadač zašle webovému serveru na adrese www.nw.fmhp.uniba.sk nasledujúcu požiadavku:

**Klient-server** popisuje vzťah medzi dvoma programami alebo sieťovými zariadeniami. Prvý, tzv. klient, žiada o nejakú službu druhý program alebo zariadenie. Druhý, tzv. server, je ten, ktorý nejakú službu poskytuje.

```
GET /dvui/demo.html HTTP/1.1
Host: www.nw.fmph.uniba.sk
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; sk;
rv:1.9.2) Gecko/20100115 Firefox/3.6
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
=0.8
Accept-Language: sk,cs;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
```

V požiadavke prehliadač oznámi, o ktorú stránku má záujem (*/dvui/demo.html*), z akého servera (*www.nw.fmph.uniba.sk*), oznámi informácie o sebe a o svojich vlastnostiach (podpora jazyka, kódových stránok atď.), prípadne ďalšie doplňujúce informácie (napr. cookies).

Po prijatí požiadavky ju server spracuje a odpovie na ňu:

```
HTTP/1.1 200 OK
Date: Sat, 06 Feb 2010 21:37:13 GMT
Server: Apache/2.0.59 (NETWARE) mod_jk/1.2.21
```

```
Last-Modified: Sat, 06 Feb 2010 20:46:47 GMT
ETag: "524f88-124-aaa67bc0"
Accept-Ranges: bytes
Content-Length: 292
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=WINDOWS-1250
Content-Language: cs
```

Zoznam HTTP stavových kódov nájdete na stránke www.ietf.org/rfc/rfc2616.txt, prípadne v češtine na stránke interval.cz/clanky/stavove-kody-a-hlaseni-v-odpovedi-protokolu-http/.

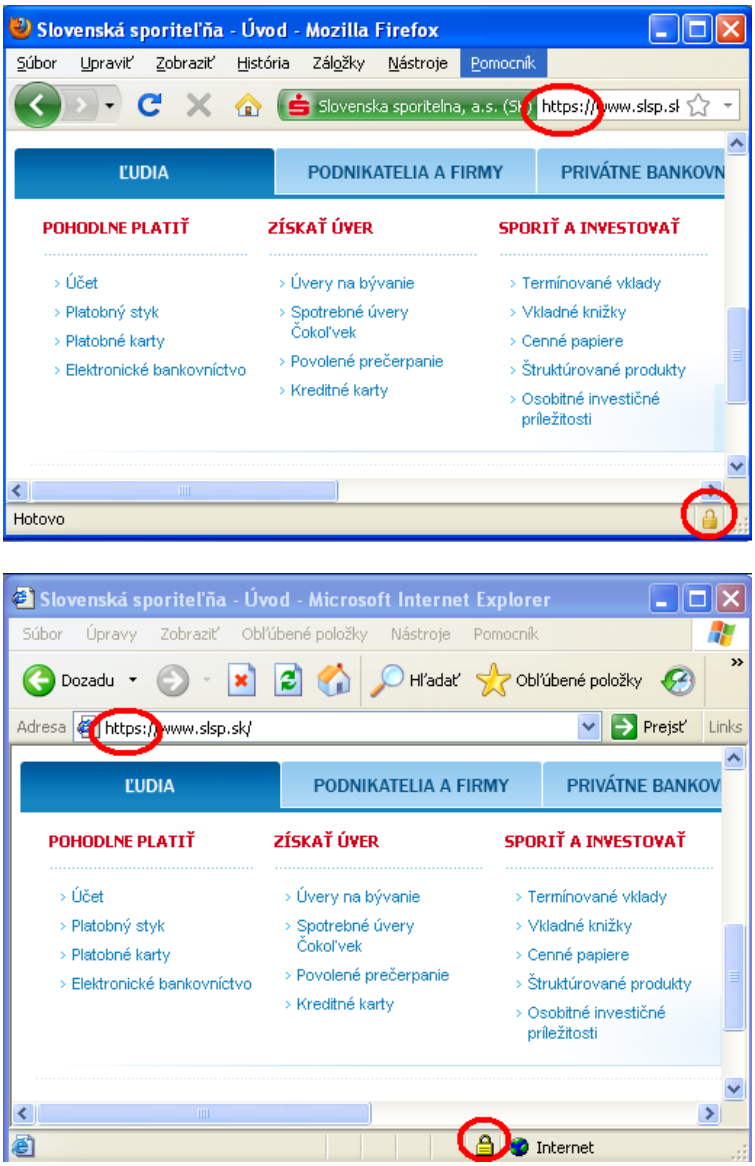
Odpoveď obsahuje stavový kód (*200 OK* – požiadavka bola spracovaná bez chyby) a doplňujúce informácie, tzv. metadata (dátum servera, posledná aktualizácia dokumentu, veľkosť, jazyk, kódová stránka atď.). Po týchto základných údajoch nasleduje samotný obsah dokumentu (v tomto prípade zdrojový kód webovej stránky):

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN">
<html>
<head>
  <title>Demo webovej stránky</title>
  <meta http-equiv="Content-Type" content="text/html;
charset=windows-1250">
</head>
<body>
Toto je demo stránka pre ukážku http komunikácie.
</body>
</html>
```

Spomínali sme, že jedno fyzické zariadenie môže súčasne ponúkať niekoľko rôznych služieb. Jednotlivé služby preto majú pre svoju identifikáciu určený port služby. V prípade webových služieb je to zvyčajne port 80. Na jednom zariadení pod jednou IP adresou môže fungovať aj viac webových serverov. Niektoré môžu fungovať ako tzv. virtuálne hosty, ktoré sa pri požiadavke rozlišujú na základe hodnoty *host* v požiadavke (pozri ukážku komunikácie – požiadavka webového prehliadača). Iné zasa môžu fungovať ako webové služby na rôznych portoch (pozri zadanie 3).

Pri využívaní webových služieb niekedy potrebujeme prenášať citlivé údaje (prihlasovacie meno, heslo, osobné údaje a podobne). V takom prípade je nutné tieto údaje pri prenose medzi prehliadačom a webovým serverom chrániť. Na tento účel sa najčastejšie využíva zabezpečená verzia protokolu HTTP označovaná aj ako **HTTPS** (*Hypertext Transfer Protocol Secure*). Zabezpečená verzia webovej služby zvyčajne využíva port 443. Pri HTTPS komunikácii sa prenášané údaje medzi klientom a serverom zakódujú (zašifrujú) tak, aby sa nedali prečítať pri ich neoprávnenom odchytení.

| | |
|---|---|
| **Zadanie 5** | Vo webovom prehliadači otvorte stránku s adresou http://www.slsp.sk/ a v druhom okne stránku s adresou https://www.slsp.sk/. Aký je rozdiel medzi týmito stránkami? Ako zistíme, ktorá využíva zabezpečenú komunikáciu medzi klientom a serverom? |
| **Riešenie** | Výsledné stránky sú rovnaké. Stránka v druhom okne (https://www.slsp.sk/) však prešla cez internet v zašifrovanom tvare (s využitím protokolu HTTPS). Rozpoznať sa to dá analýzou adresy - adresa začínajúca **https** používa šifrovanie. Prehliadače Internet Explorer a Mozilla Firefox v prípade šifrovanej stránky zobrazia symbol zamknutého zámku. V prípade nešifrovanej stránky sa symbol zámku nezobrazuje, alebo sa zobrazuje symbol odomknutého zámku. |




## Elektronická pošta

Služba elektronickej pošty (e-mail) je po službe WWW druhou najpoužívanejšou službou internetu. E-mail slúži na posielanie elektronických správ ako elektronická obdoba klasickej pošty, ktorú poznáme z bežného života. Výhodou e-mailu oproti klasickej pošte je jednoduchosť odoslania správy, nižšie náklady na odoslanie a hlavne rýchlosť jej doručenia do schránky adresáta. Doba doručenia elektronickej správy sa počíta v rádoch sekúnd až minút a to do ktoréhokoľvek kúta sveta. Preto priaznivci e-mailu zvyknú označovať klasickú poštu ako *Snail mail* (*slimačia pošta*). Na posielanie a prijímanie správ potrebujeme špeciálny program - e-mailový klient (napr. Mozilla Thunderbird, Outlook Express, Pegasus Mail, The Bat!...). Môže mať aj podobu webovej aplikácie. E-mailový klient komunikuje s e-mailovým serverom pri odosielaní správy protokolom **SMTP** (*Simple Mail Transfer Protocol*).

Ukážme si, čo sa deje, keď z e-mailového klienta odošleme e-mail. V uvedenom príklade adresu odosielateľa predstavuje *odosielatel@priklad.sk* a adresu pre doručenie správy predstavuje *adresat@priklad.sk*.

**Vedeli ste, že...?**

E-mail je starší ako internet. Prvý e-mail napísali v roku 1965 Tom Van Vleck a Noel Morris v MIT (Massachusetts Institute of Technology).

Najprv klient nadviaže spojenie so serverom a v úvode sa vzájomne predstavia, klient oznámi kto je odosielateľ správy a komu je správa určená. Na základe týchto informácií sa server rozhodne správu prijať alebo zamietnuť (napr. keď na serveri schránka uvedeného adresáta neexistuje). V prípade, že sa server rozhodne správu prijať, nasleduje telo samotnej správy vrátane jej hlavičiek (hlavičky predstavujú informácie o odosielateľovi a adresátovi, čas odoslania správy, predmet správy a pod.) V uvedenej komunikácii predstavuje **C=klienta** a **S=server**:

Zoznam riadiacich príkazov a kódov protokolu SMTP nájdete na stránke www.ietf.org/rfc/rfc2821.txt

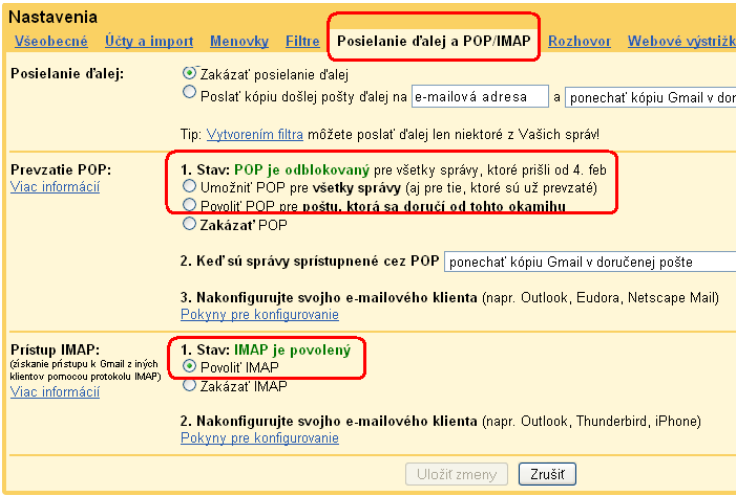
```
C: nadviazanie spojenia so serverom
S: 220 mail.priklad.sk Mercury 1.48 ESMTP server ready.
C: EHLO [192.168.1.1]
S: 250-mail.priklad.sk Hello [192.168.13.10]
C: MAIL FROM:<odosielatel@priklad.sk>
S: 250 Sender OK - send RCPTs.
C: RCPT TO:<adresat@priklad.sk>
S: 250 Recipient OK - send RCPT or DATA.
C: DATA
S: 354 OK, send data, end with CRLF.CRLF
C: Date: Fri, 01 Jan 2010 00:00:00 +0100
C: From: Meno Priezvisko <odosielatel@priklad.sk>
C: To:  adresat@priklad.sk
C: Subject: skuska mailu
C:
C: Dobry den,
C:
C: toto je skusobny mail.
C:
C: Dovidenia.
C: .
S: 250 Data received OK.
C: QUIT
S: 221 mail.priklad.sk Service closing channel.
```

Protokol POP3 sa niekedy skrátene označuje ako POP. Protokol IMAP sa niekedy označuje ako IMAP4 (*Internet Message Access Protocol version 4*).

Pri prístupe k doručeným správam e-mailový klient komunikuje so serverom pomocou protokolu **POP3** (*Post Office Protocol version 3*) alebo **IMAP** (*Internet Message Access Protocol*). Protokol POP3 slúži na stiahnutie správ z e-mailového servera na lokálny počítač, kde je možné s nimi ďalej pracovať. Ďalšie spracovanie týchto e-mailov je potom možné už len na počítači, na ktorý boli stiahnuté. Protokol IMAP naopak umožňuje obojstrannú komunikáciu a tým ponúka pokročilé možnosti ako práca s priečinkami, presúvanie správ a podobne priamo na e-mailovom serveri z prostredia e-mailového klienta. Keďže e-maily ostávajú na serveri, je možné s nimi ďalej pracovať z ľubovoľného miesta – z domáceho počítača, počítača v zamestnaní, mobilného telefónu, PDA, notebooku a podobne. Na ďalšie spracovanie teda nie sme odkázaní na počítač, na ktorý boli správy predtým stiahnuté. Niektoré e-mailové servery umožňujú prístup k e-mailom aj prostredníctvom webového prehliadača, tzv. **Webmail**. Služba elektronickej pošty je taktiež službou typu klient-server.

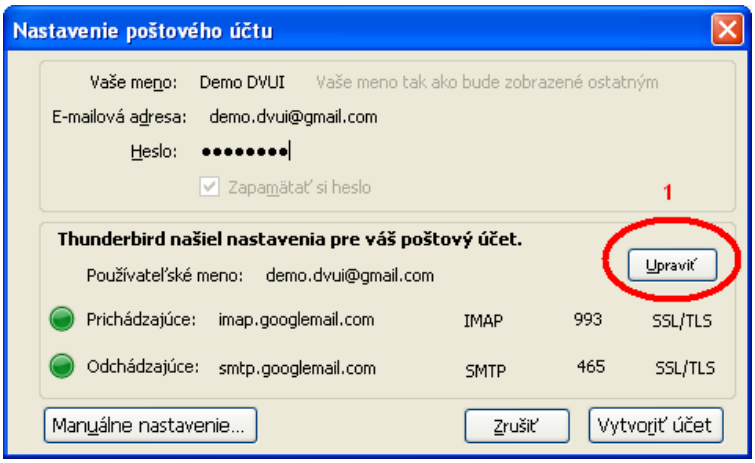
**Zadanie 6**

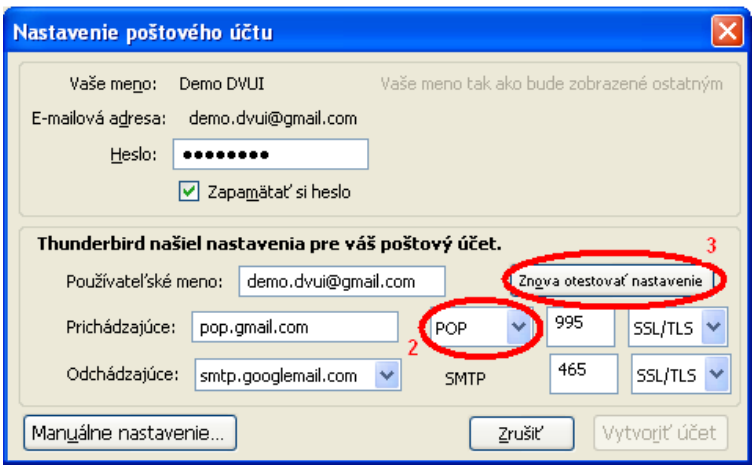
Vytvorte si nový účet v službe Gmail (www.gmail.com), ktorý využijeme aj v ďalších zadaniach. Prihláste sa do tejto služby v prehliadači a cez voľbu *nastavenia* v záložke *Posielanie ďalej a POP/IMAP* povoľte POP3 a IMAP.




Spustite e-mailového klienta Mozilla Thunderbird Portable a v ňom pridajte *nový poštový účet*. Parametre účtu zadáme podľa účtu Gmail, ktorý sme si vytvorili. V nastaveniach cez voľbu *upraviť* nastavte pre prichádzajúce správy POP prístup podľa nasledujúcich obrázkov:

Mozilla Thunderbird Portable (www.mozilla.sk/download/prenosne/)




Po nastavení účtu pošlite svojim susedom e-mail. Vytvorte si priečinky. Stiahnite si nové správy a presuňte si ich do vytvorených priečinkov.

Vo webovom prehliadači sa prihláste do Gmailu a skúste

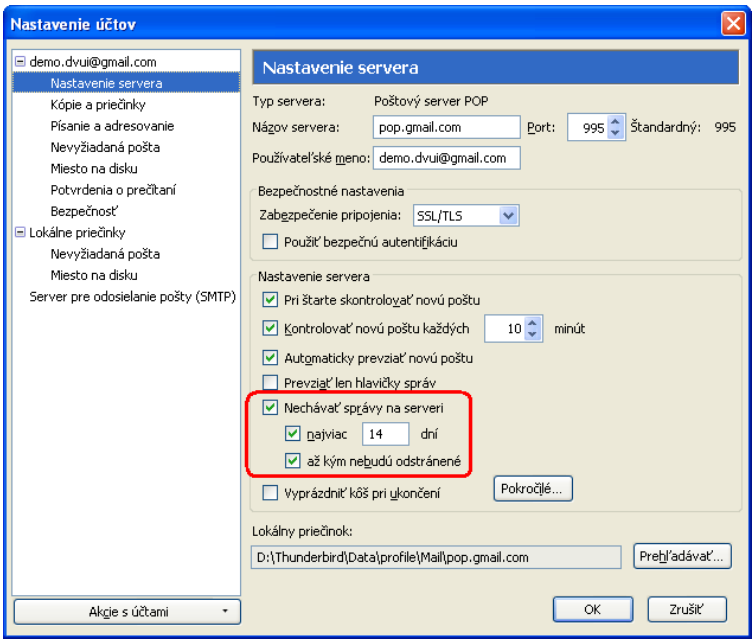
v ňom nájsť vami vytvorené priečinky a v nich presunuté e-maily.

Prečo ste vami vytvorené priečinky nenašli?

**Riešenie**

Dôvodom je použitie protokolu POP3.

V klientovi je možné taktiež nastaviť, aby e-maily stiahnuté POP3 prístupom boli zo servera zmazané. V takom prípade by sme cez webový prehliadač našli schránku doručenej pošty prázdnu. Zmeniť toto nastavenie môžete v nastaveniach účtu podľa nasledujúceho obrázka.




Niektorí e-mailoví klienti majú voľbu zmazania správ zo servera prednastavenú.

**Zadanie 7**

V Mozilla Thunderbird Portable zrušíme účet zo zadania 6 a vytvoríme nový. Pri vytvorení nového účtu postupujte rovnako ako v zadaní 6, ale bez zmeny nastavenia (vynecháme kroky 1, 2, 3) vytvoríme účet s prístupom IMAP.

Po nastavení účtu pošlite svojim susedom e-mail. Vytvorte si priečinky. Stiahnite si nové správy a presuňte si ich do vytvorených priečinkov.

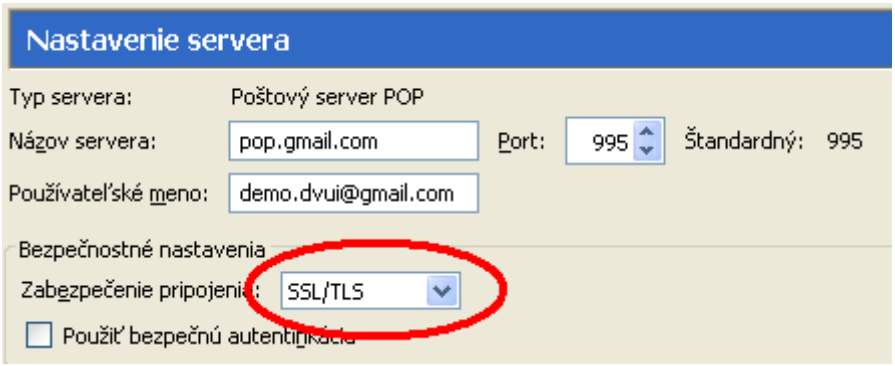
Vo webovom prehliadači sa prihláste do Gmailu a skúste v ňom nájsť vami vytvorené priečinky a v nich presunuté e-maily.

**Cieľ**

V tomto prípade už priečinky aj s e-mailami cez web nájdeme. Takto máme plný prístup k účtu na serveri z nášho e-mailového klienta.

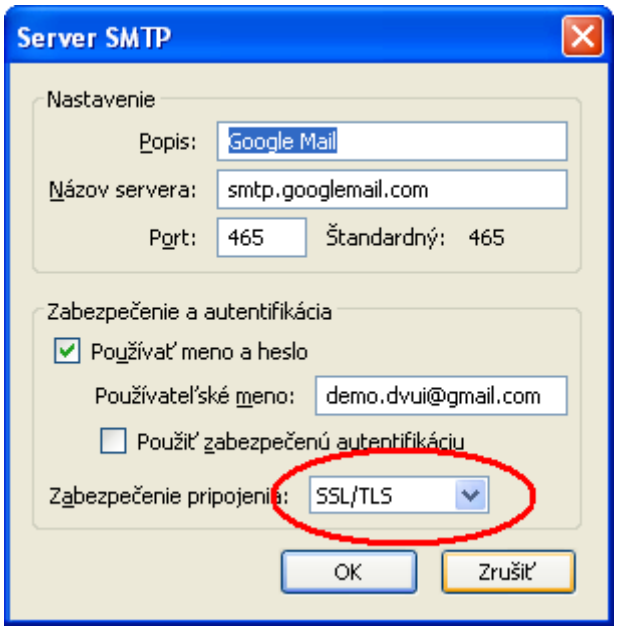
Aby sme mohli z e-mailového servera prevziať svoje správy, je potrebné sa voči serveru identifikovať a to svojim prihlasovacím menom a heslom. Pridelené prihlasovacie meno je previazané s príslušnou e-mailovou schránkou. Pri prihlasovaní sa posiela serveru prihlasovacie meno a heslo. Zvyčajne sa tieto údaje posielajú

v nezašifrovanej podobe. Ak by sa nejakému útočníkovi (neoprávnenej osobe) podarilo odchytiť túto komunikáciu, mohol by naše prihlasovacie údaje zneužiť. Brániť sa môžeme používaním zabezpečeného pripojenia k serveru. V prípade prístupu k e-mailom cez webový prehliadač, je vhodné používať zabezpečený prístup prostredníctvom HTTPS. Pri používaní e-mailového klienta je vhodné v nastaveniach k účtom nastaviť zabezpečené pripojenie pre POP3 alebo IMAP, čo vytvorí šifrovaný kanál pre komunikáciu klienta so serverom.




*Obrázok 5 - Nastavenie zabezpečeného POP pripojenia v programe Mozilla Thunderbird*

Niektoré e-mailové servery vyžadujú pri odosielaní e-mailu z klienta protokolom SMTP prihlásenie. Aj v tomto prípade je vhodné nastaviť zabezpečené pripojenie.




*Obrázok 6 - Nastavenie zabezpečenej autentifikácie SMTP pripojenia v programe Mozilla Thunderbird*

## Interaktívna komunikácia

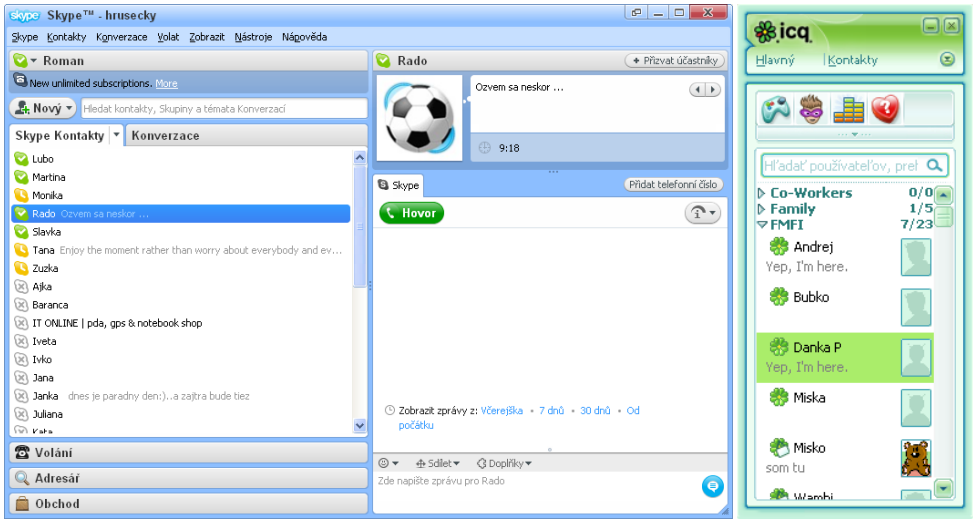
Populárnosť služieb interaktívnej komunikácie v súčasnosti stále narastá. Interaktívna komunikácia, označuje sa anglickým pojmom **Instant messaging** (IM), umožňuje používateľom ešte rýchlejšie vzájomne komunikovať ako pri využívaní služby e-mail, a to posielaním krátkych správ, alebo v súčasnosti veľmi populárnou hlasovou a obrazovou komunikáciou. Vzhľadom na lepšiu dostupnosť internetového pripojenia sa tieto služby používajú stále častejšie ako náhrada telefónnej komunikácie medzi rodinnými príslušníkmi a priateľmi.

**proprietárny** = uzatvorený, teda taký, ktorého špecifikácia nie je verejne prístupná, a tým je jeho použitie viazané k použitiu konkrétneho licencovaného softvéru

Medzi najznámejšie IM služby patria ICQ, Skype, Google Talk, Jabber, Live Messenger. Niektoré tieto služby využívajú tzv. **proprietárny komunikačný protokol**, a tak vyžadujú klienta priamo od poskytovateľa tejto služby, napr. Skype.

Niektoré služby však využívajú všeobecne známy komunikačný protokol a v takom prípade je možné používať klientov rôznych výrobcov nezávisle od poskytovateľa služby. Medzi najznámejšie programy, ktoré podporujú viacero komunikačných protokolov (napr. ICQ, Google Talk, Jabber a ďalšie), patria Miranda, Pidgin, Trillian, SIM, Kopete a QIP. Zároveň títo klienti umožňujú použitie jedného klienta na pripojenie viacero účtov k rovnakej, ale aj rôznej IM službe súčasne. Nie je teda nutné použiť pre každý účet a IM službu samostatného klienta.

Názov služby sa často zhoduje s názvom klienta, napr. ICQ, Skype.




*Obrázok 7 – Ukážka prostredia IM klientov Skype a ICQ*

Pri službách IM sa využívajú spojenia typu klient-server ako aj peer-to-peer, teda spojenia kde komunikujú dva klientske programy priamo medzi sebou bez servera. Server pri IM slúži prevažne na sprostredkovanie informácie o pripojení jednotlivých používateľov danej služby. Server pri posielaní krátkych správ môže slúžiť aj ako sprostredkovateľ a v prípade, že používateľ nie je pripojený, tak server dočasne ukladá správy určené neprihláseným používateľom.

S niektorými službami IM sme sa prakticky oboznámili v predchádzajúcich moduloch (*Základná digitálna gramotnosť* (2DG1), *Základy hardvérového a softvérového vybavenia počítača* (2DG3), *Digitálne technológie pre učiteľa 2* (2DG5)).

## Peer-to-peer

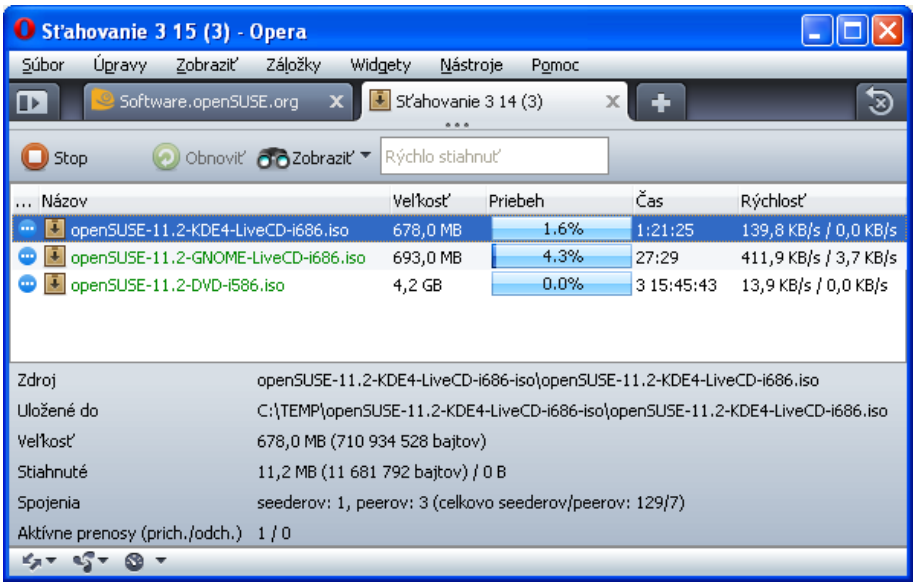
**Peer-to-peer** popisuje rovnocenný vzťah medzi sieťovými programami alebo sieťovými zariadeniami. Každý program alebo zariadenie funguje súčasne aj ako klient aj ako server.

**Peer-to-peer** (alebo P2P, v preklade *rovný s rovným*) poskytuje služby výmeny súborov medzi skupinami používateľov internetu. Vymieňať možno ľubovoľné súbory – text, obrázky, hudbu, videá, softvér atď. Peer-to-peer popisuje vzťah komunikácie, keď jednotliví klienti komunikujú vzájomne medzi sebou bez potreby servera. Pri P2P komunikácii sa server vôbec nepoužíva, alebo slúži len ako sprostredkovateľ zoznamu vzájomne komunikujúcich klientov. Sústava takto vzájomne komunikujúcich P2P klientov sa zvykne označovať aj ako **P2P sieť**.

P2P siete sú vo veľkej obľube najmä u domácich používateľov, ktorí takýmto spôsobom sťahujú najčastejšie hudbu, filmy, hry a rôzny softvér. Napriek tomu, že sa ich pomocou sťahujú súbory prevažne v rozpore s autorskou legislatívou, neboli a nie sú P2P siete vyvíjané pre tento účel. Pomocou P2P sietí sa umožňuje sťahovanie voľne dostupných linuxových distribúcií, inštalačných balíkov voľne dostupného softvéru, ovládačov pre rôzny hardvér a podobne. Pri klasickom sťahovaní súborov kontaktujú jednotliví klienti server, na ktorom sú tieto súbory uložené. Pri vyššom počte týchto klientov sa môže server alebo jeho prístup do internetu zahltiť množstvom súčasných spojení. Pri sťahovaní súborov pomocou

klientov P2P siete sa aj títo klienti zároveň stávajú zdrojom týchto súborov po ich stiahnutí. Niektoré P2P siete túto možnosť vylepšili tak, že sa nesťahuje kompletne celý súbor výhradne z jedného zdroja, ale súbor sa sťahuje po častiach a to aj z rozličných zdrojov toho istého súboru. V takom prípade sa klient stáva zdrojom už stiahnutej časti súboru. Po stiahnutí všetkých časti súboru sa súbor u klienta skompletizuje. Týmto sa dosiahlo ešte lepšie využitie voľného výkonu a prenosovej kapacity liniek jednotlivých klientov a v konečnom dôsledku sa týmto spôsobom dajú súbory stiahnuť rýchlejšie ako pri ich sťahovaní z jedného zahlteného zdroja.

Medzi najznámejšie protokoly P2P sietí patria *BitTorrent*, *Napster*, *Direct Connect*, *Gnutella*, *ed2k*, *FastTrack*. Pre využívanie P2P sietí je potrebný príslušný program – klient, ktorý ovláda príslušný komunikačný protokol. Niektoré protokoly P2P sietí ovláda napríklad aj webový prehliadač Opera.



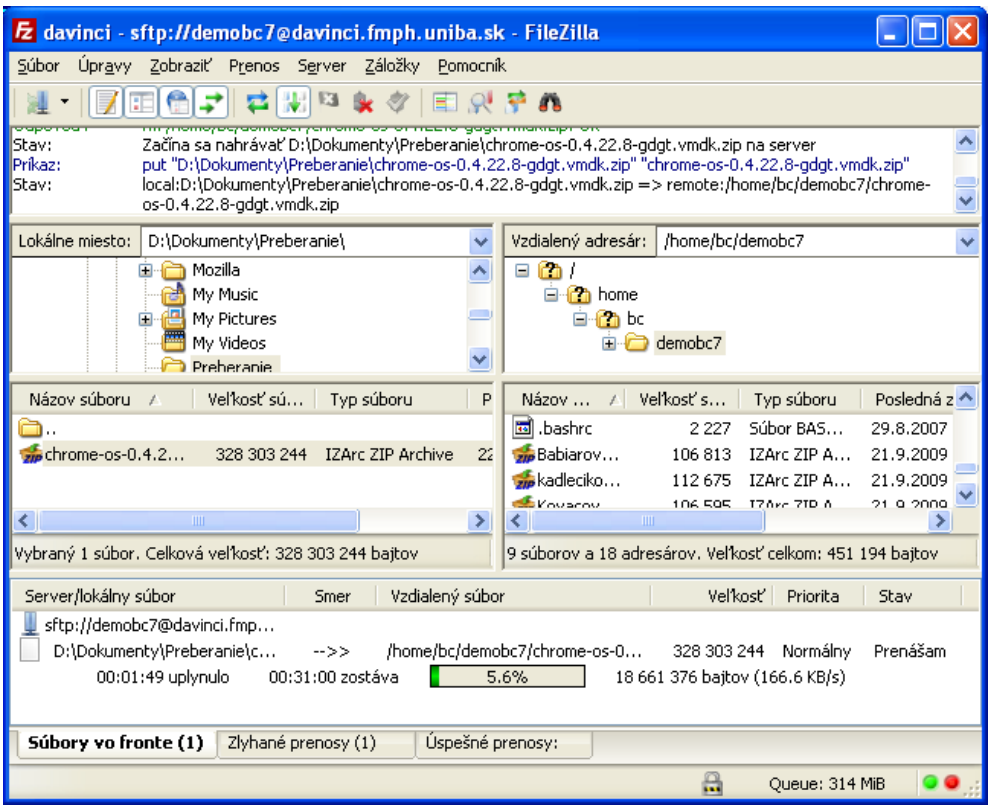

*Obrázok 8 -Sťahovanie súborov P2P protokolom BitTorrent v prehliadači Opera*

Podľa štatistík celosvetovo objem prenesených dát pomocou najpopulárnejšej P2P siete BitTorrent predstavuje približne tretinu celého dátového prenosu v internete. Vzhľadom na množstvo takto prenesených dát a vzhľadom na časté zneužívanie P2P sietí na prenos súborov v rozpore s autorskou legislatívou sa pristúpilo v niektorých organizáciách na blokovanie P2P sietí. Taktiež niektorí poskytovatelia internetového pripojenia môžu používanie P2P sietí, v záujme ochrany pred značným zahltením svojich internetových liniek, obmedzovať a to napríklad na možnosť ich využívania iba v istom časovom úseku, obmedzením ich prenosovej rýchlosti a podobne.

## FTP

**FTP** služba slúži na prenos súborov medzi zariadeniami v sieti. Jedná sa o službu typu klient-server. Pomocou FTP služby môžu používatelia ukladať (upload) alebo sťahovať (download) súbory zo servera. Na ukladanie a sťahovanie súborov sa však v súčasnosti viac využívajú webové služby a P2P siete.

Pre využívanie FTP služieb potrebujeme klientský program. Klientský program komunikuje s ftp serverom za pomoci protokolu **FTP** (*File Transfer Protocol*). FTP protokol pre komunikáciu využíva spojenia na portoch 20 a 21. Port 21 slúži pre príkazy a kontrolu prenášaných dát, port 20 slúži na samotný prenos súborov. Medzi najznámejšie klientské programy patria FileZilla (www.filezilla-project.org) a WS_FTP Lite.




*Obrázok 9 - Sťahovanie súboru v prostredí FTP klienta FileZilla*

Podporu pre FTP však má zabudovanú aj väčšina programov pre správu súborov (súborový manažér), ako napríklad FAR manager (www.farmanager.com), FreeCommander (www.freecommander.com) a Total Commander (www.ghisler.com).

Ukážme si, čo sa deje, keď sa pomocou ftp klienta pripojíme na ftp server a potom stiahneme súbor *help.txt*. Po nadviazaní spojenia ftp klienta so serverom sa klient na server prihlási (USER, PASS), zistí aktuálny priečinok (PWD), nastaví priečinok kde sa nachádza požadovaný súbor (CWD), požiada o výpis zoznamu súborov v danom priečinku (LIST) a požadovaný súbor stiahne (RETR), po skončení sa komunikácia ukončí (QUIT). V uvedenom príklade predstavuje **C=klienta** a **S=server**:

Zoznam riadiacich príkazov protokolu FTP nájdete na stránke www.ietf.org/rfc/rfc0959.txt

```
C: nadviazanie spojenia so serverom
S: 220-FileZilla Server version 0.9.34 beta
S: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
S: 220 Please visit
       http://sourceforge.net/projects/filezilla/
C: USER demo
S: 331 Password required for demo
C: PASS heslo
S: 230 Logged on
C: SYST
S: 215 UNIX emulated by FileZilla
C: PWD
S: 257 "/" is current directory.
C: TYPE I
S: 200 Type set to I
C: REST 0
S: 350 Rest supported. Restarting at 0
C: CWD /
S: 250 CWD successful. "/" is current directory.
C: PORT 192,168,0,1,7,189
S: 200 Port command successful
C: TYPE A
```

```
S: 200 Type set to A
C: LIST
S: 150 Opening data channel for directory list.
S: 226 Transfer OK
C: TYPE I
S: 200 Type set to I
C: PORT 192,168,0,1,7,190
S: 200 Port command successful
C: RETR /help.txt
S: 150 Opening data channel for file transfer.
S: 226 Transfer OK
C: QUIT
S: 221 Goodbye.
```

V uvedenej ukážke vidieť, že pri pripojení na ftp server zadávame aj prihlasovacie meno (*user*) a heslo (*pass*). Prihlásenie slúži pre zabezpečenie autorizovaného prístupu k súborom určeným danému používateľovi. Ftp server ale môže poskytovať aj voľný prístup k vybraným súborom. Tento prístup sa označuje ako anonymný (anglicky *anonymous*). Pri anonymom prístupe zadávame ako meno *anonymous* (prípadne *ftp*) a ako heslo e-mailovú adresu (prípadne necháme prázdne, niekedy sa však vyžaduje aspoň znak @).

Podporu pre sťahovanie súborov pomocou protokolu FTP majú integrovanú aj webové prehliadače. Požiadavku v prehliadači zadávame rovnako ako pre webové stránky, zadaním adresy. V zadanej adrese namiesto protokolu *http* zadávame *ftp*, napríklad: ftp://ftp.ietf.org/rfc/rfc1925.txt. Táto adresa je pre anonymný prístup. Pokiaľ je potrebné sa k danému ftp serveru prihlásiť, adresa má tvar: *ftp://meno:heslo@adresa_servera/cesta_k_súboru/názov_suboru*.

Pri používaní štandardného FTP protokolu sa posielajú prihlasovacie údaje v čitateľnej podobe, a teda hrozí, že odchytením komunikácie môže neoprávnená osoba získať prístup k našim súborom. V takom prípade je vhodnejšie použiť zabezpečené pripojenie k serveru. Najčastejšie sa používa protokol **SFTP** (*SSH File Transfer Protocol*). Protokol SFTP pre zabezpečenie komunikácie využíva protokol SSH-2 (Secure Shell), ktorý komunikuje na porte 22. Protokol SFTP podporujú napríklad klienti FileZilla a WinSCP, taktiež ho podporuje aj súborový manažér Total Commander a FAR s pluginom WinSCP.

**Zadanie 8**

Stiahnite súbor *rfc1925.txt* z priečinka *rfc* nachádzajúceho sa na FTP serveri ftp.ietf.org.

Využite webový prehliadač, ale aj FTP klienta (napr. FileZilla).

# Princíp dôveryhodnej komunikácie

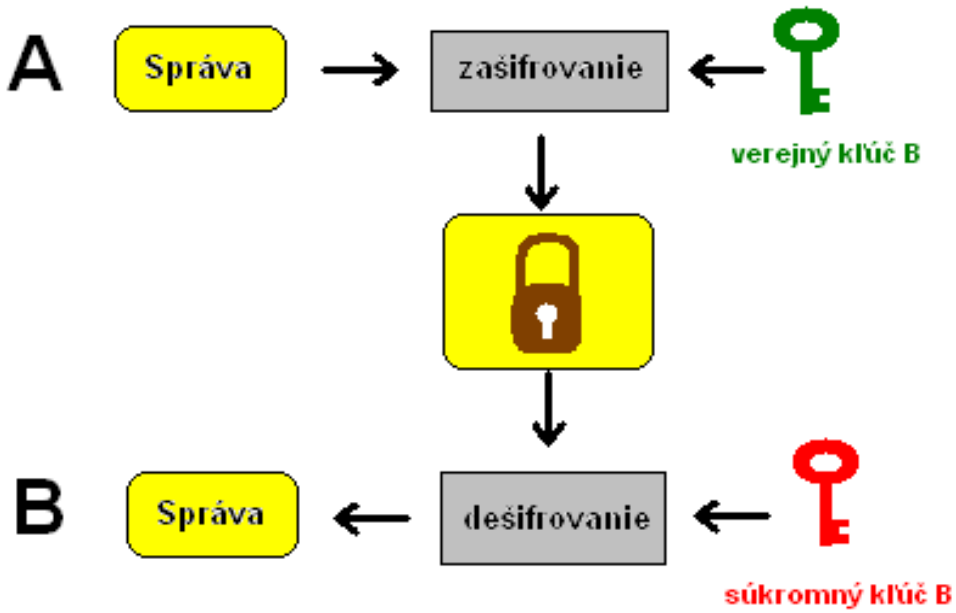
V predchádzajúcich kapitolách sme si spomínali dôležitosť utajovania internetom prenášaných údajov. Utajenie prenášaných údajov sa zabezpečuje vytvorením tzv. bezpečnej komunikácie. Pre vytvorenie bezpečnej komunikácie sa najčastejšie využíva spôsob, ktorý je postavený na **infraštruktúre verejných kľúčov** (***PKI - public key infrastructure***). PKI využíva výhody asymetrického šifrovania, digitálneho certifikátu a elektronického podpisu.

## Asymetrické šifrovanie

**Symetrické šifrovanie** je šifrovanie, pri ktorom sa používa rovnaký kľúč pri zašifrovaní aj dešifrovaní.

Asymetrické šifrovanie, označuje sa aj ako *šifrovanie verejným kľúčom*. Toto šifrovanie funguje na princípe dvojice kľúčov – súkromný a verejný kľúč. Súkromný kľúč ostáva vždy utajený a verejný kľúč je verejne dostupný. Pokiaľ používateľ **A** chce odoslať používateľovi **B** zašifrovanú správu, použije na zašifrovanie verejný kľúč používateľa **B**. Takto zašifrovanú správu odošle používateľovi **B**. Používateľ **B** potom k dešifrovaniu správy použije svoj súkromný kľúč. Neoprávnenej osobe k dešifrovaniu správy nestačí znalosť verejného kľúča, algoritmu a ani prenášanej zakódovanej správy, pretože jej chýba súkromný kľúč.

Teoreticky existuje spôsob ako bez znalosti súkromného kľúča dešifrovať zakódovanú správu. Pri tomto spôsobe je snaha *uhádnuť* súkromný kľúč a to tak, že sa útočník pokúša dešifrovať správu vyskúšaním všetkých možných kombinácií aké môže šifrovací kľúč predstavovať. Tento spôsob sa označuje *brutal force*. Táto metóda zisťovania súkromného kľúča je však výpočtovo a teda časovo veľmi náročná. Napríklad použitie kľúča dĺžky 2048bitov predstavuje $2^{2048}$ možných kombinácií kľúča, a preto tento spôsob pri výkone súčasného hardvéru nedáva zmysel.

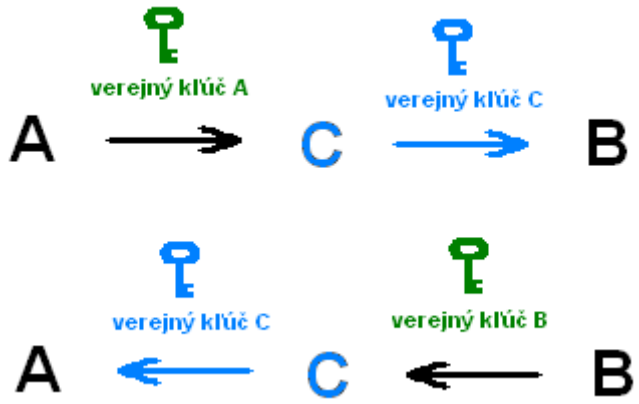



*Obrázok 10 - Schéma asymetrického šifrovania*

Asymetrické šifrovanie používa tzv. jednocestné funkcie, teda operácie, ktoré je možné vykonať len v jednom smere: zo vstupu sa ľahko vypočíta výstup, ale z výstupu je veľmi zložité nájsť vstup.

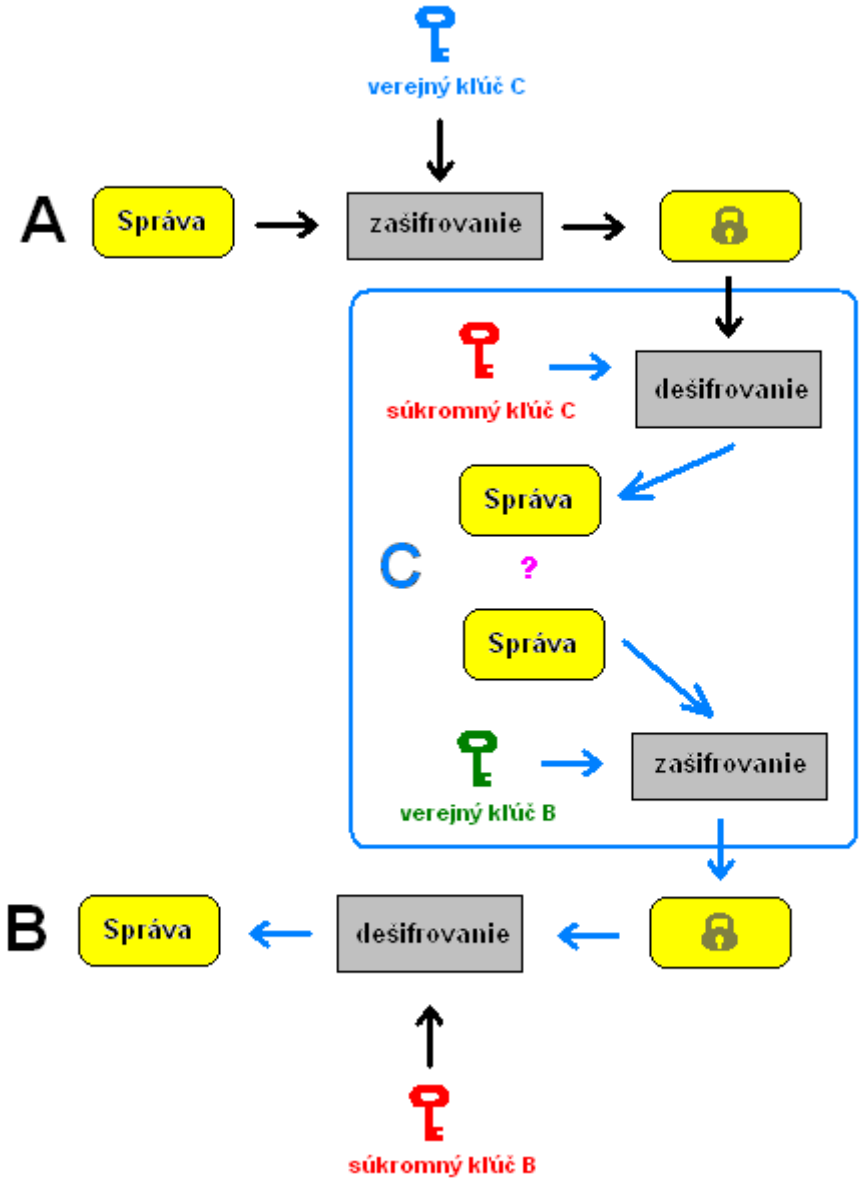
## Digitálny certifikát a certifikačná autorita

Samotné šifrovanie z predchádzajúcej kapitoly síce ochráni komunikáciu pred odpočúvaním, ale bez overenia autentickosti verejných kľúčov sa komunikujúce strany môžu stať obeťou tzv. útoku **Man in the middle** (z angličtiny *človek uprostred*). Podstatou tohto útoku je snaha útočníka odpočúvať komunikáciu tak, že sa stane jej aktívnym prostredníkom. Pri počiatočnej vzájomnej výmene verejných kľúčov získa verejné kľúče účastníkov odpočúvanej komunikácie a podsunie im namiesto nich svoj verejný kľúč:




*Obrázok 11 – Schéma výmeny verejných kľúčov pri útoku Man in the middle*

Následnú šifrovanú komunikáciu preposiela cez seba ako sprostredkovateľ, pričom pôvodnú správu dokáže nielen prečítať, ale môže túto správu aj pozmeniť:

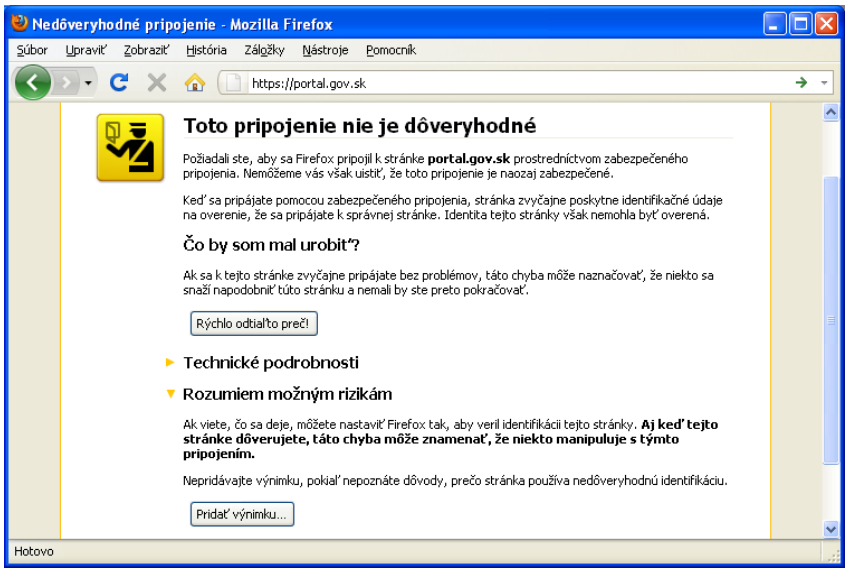



*Obrázok 12 – Schéma odpočúvania komunikácie pri útoku Man in the middle*

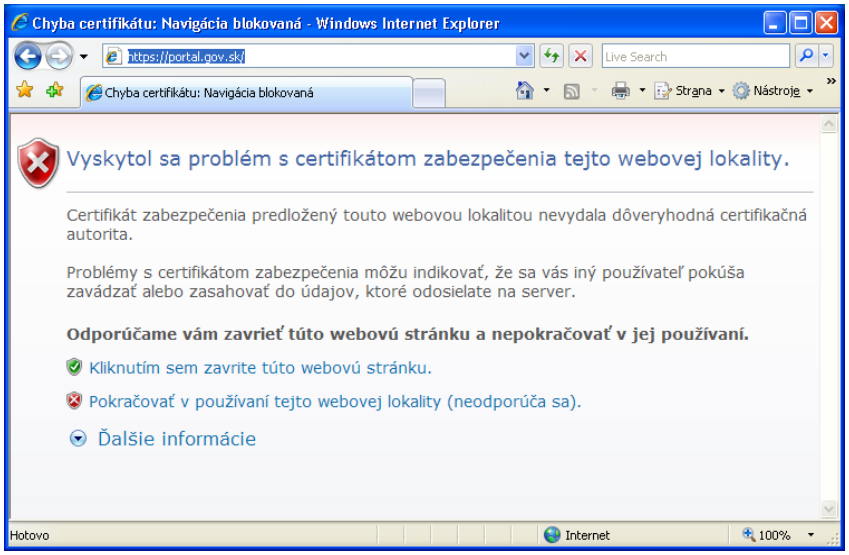
Princíp prenosu dôvery sa bežne využíva v reálnom živote. Dôverujeme informáciám od svojich blízkych priateľov, seriózných novín, odborných relácií v televízii a podobne. Naopak s rezervou berieme informáciu od tzv. zdroja JPP („Jedna pani povedala“), alebo vôbec nedôverujeme zdroju, ktorý preukázateľne v minulosti nehovoril pravdivé informácie.

Preto je potrebné zabezpečiť overenie autentickosti verejných kľúčov. Na tento účel sa využíva princíp prenosu dôvery, kedy predmetný verejný kľúč sa doručí spolu s digitálnym certifikátom vystaveným dôveryhodnou certifikačnou autoritou. **Digitálny certifikát** je elektronicky podpísaný verejný kľúč, ktorý obsahuje údaje svojho majiteľa, za ktorých pravosť sa zaručila certifikačná autorita.

**Certifikačná autorita** je subjekt, ktorý vydáva digitálne certifikáty, a tým potvrdzuje pravosť údajov uverejnených vo verejnom kľúči. Dôvera v túto certifikačnú autoritu je preto veľmi dôležitá. Certifikačná autorita musí adekvátnym spôsobom dbať o svoju dôveryhodnosť. Dôveryhodnosť konkrétnej certifikačnej autority môžeme posúdiť na základe jej webových stránok, mechanizmu overenia údajov žiadateľa o digitálny certifikát, odporúčaní (články v tlači a elektronických médiách, vyjadrení národných bezpečnostných úradov a podobne). Certifikačné autority majú taktiež svoj vlastný digitálny certifikát. Pokiaľ je tento digitálny certifikát uložený v dôveryhodnom úložisku certifikátov nášho počítača (operačný systém, webový prehliadač a podobne) automaticky dôverujeme všetkým certifikátom vydaným touto certifikačnou autoritou. V opačnom prípade program odmietne spojenie s varovaním, že dané spojenie je nedôveryhodné.

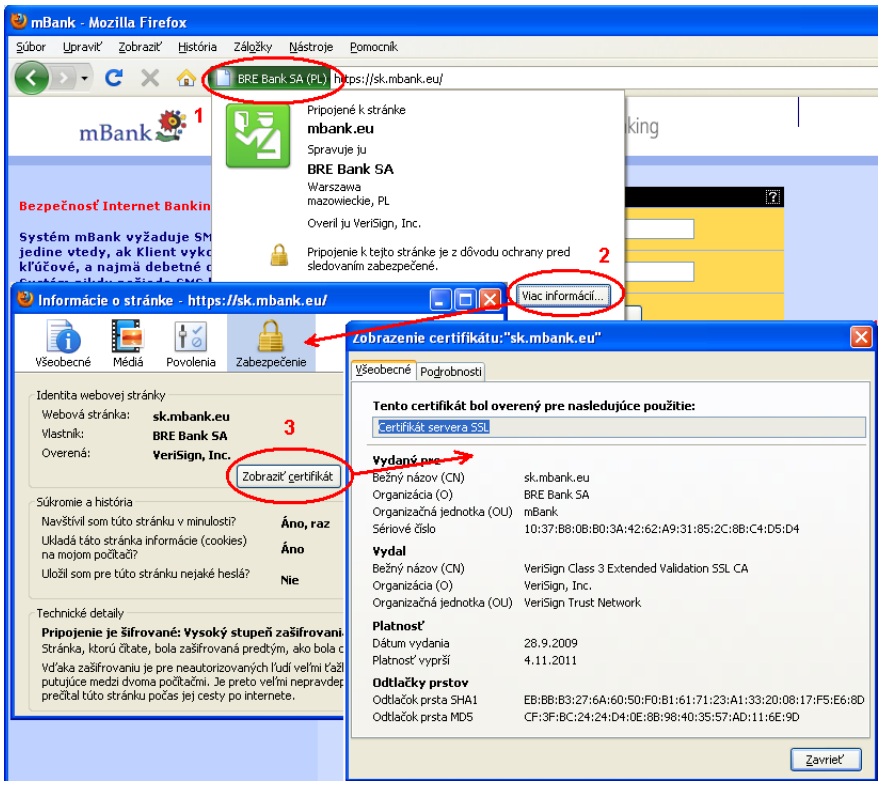



*Obrázok 13 - Zobrazenie oznámenia o nedôveryhodnom certifikáte v prehliadači Mozilla Firefox*

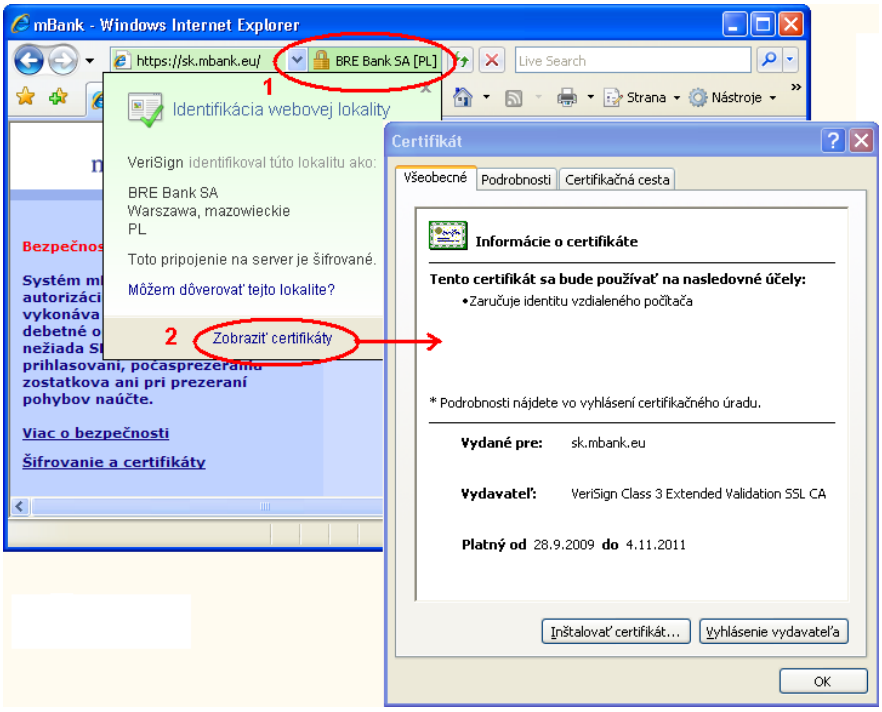



*Obrázok 14 - Zobrazenie oznámenia o nedôveryhodnom certifikáte v prehliadači Windows Internet Explorer*

Štandardnou súčasťou dôveryhodného úložiska súčasných operačných systémov a klientov internetových služieb sú certifikáty najznámejších svetových certifikačných autorít *VeriSign*, *Thawte*, *GeoTrust* a podobne. Preto spoločnosti, ktoré ponúkajú internetové služby vyžadujúce zabezpečené spojenie, si pre zabezpečenie dôveryhodnosti nechávajú do týchto certifikačných autorít vystaviť potrebný certifikát. Najčastejšie sa jedná o spoločnosti ponúkajúce bankové služby, elektronický obchod a podobne.




*Obrázok 15 – Zobrazenie dôveryhodného certifikátu v prehliadači Mozilla Firefox*




*Obrázok 16 - Zobrazenie dôveryhodného certifikátu v prehliadači Windows Internet Explorer*

| | |
|---|---|
| **Zadanie 9** | Otvorte stránku s **dôveryhodným** certifikátom (napr. internet banking niektorej z bánk) a zistite informácie o certifikáte. Vyskúšajte to v prehliadačoch Mozilla Firefox aj Internet Explorer. |
| **Zadanie 10** | Otvorte stránku s **nedôveryhodným** certifikátom (napr. https://cpr.ii.fmph.uniba.sk/moodle/) a zistite informácie o certifikáte. Vyskúšajte to v prehliadačoch Mozilla Firefox aj Internet Explorer. Ako si môžeme túto stránku pozrieť? Ako si nainštalujeme certifikát tejto stránky, aby sa označil ako dôveryhodný? |
| **Zadanie 11 – diskusia** | Aké sú riziká pri prístupe na stránku s nedôveryhodným certifikátom? |

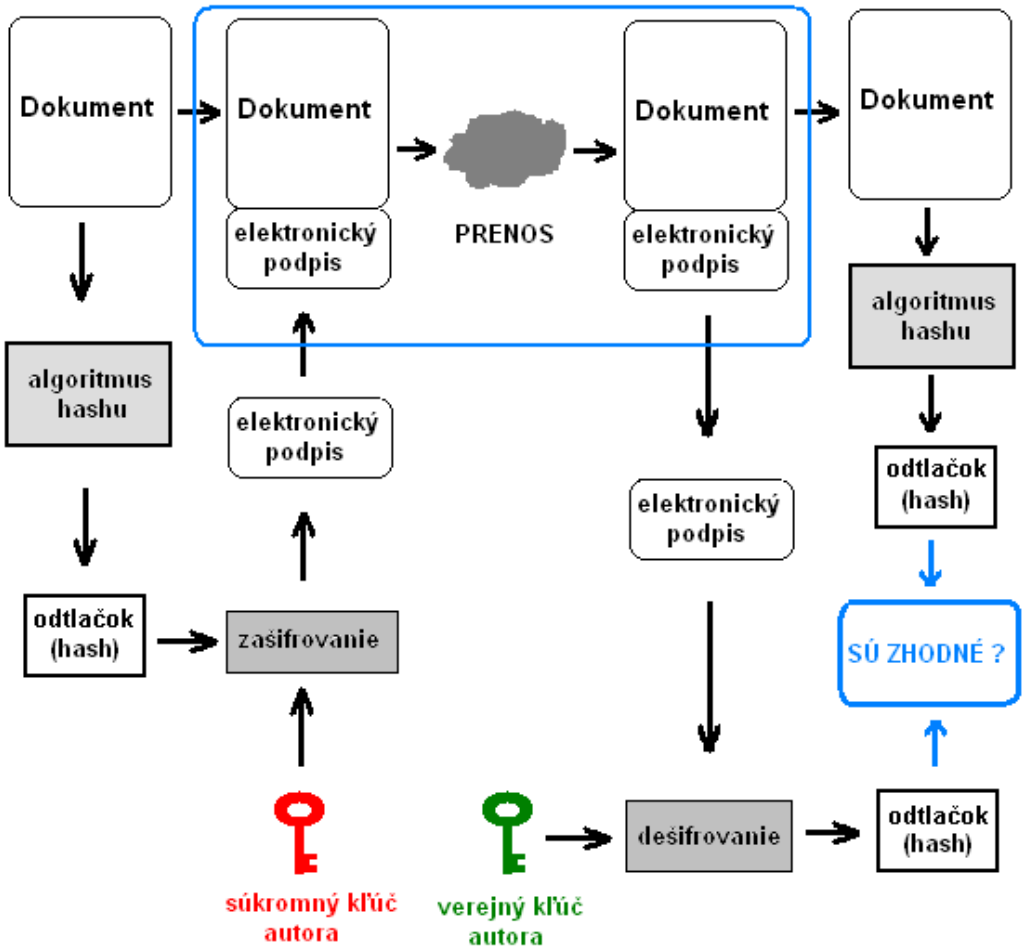
# Elektronický podpis

**Elektronický podpis** je elektronická obdoba tradičného vlastnoručného podpisu, ktorý poznáme z bežného života. Základné vlastnosti elektronického podpisu sú:

- *autenticita* – identifikácia autora (umožňuje spoľahlivo určiť osobu, ktorá podpis vyhotovila),
- *integrita* – neporušenosť dokumentu (overený podpis preukazuje, že po podpise nebol dokument zmenený, upravovaný alebo poškodený),
- *nepopierateľnosť autorstva* - jednoznačné priradenie autorstva dokumentu podpisovateľovi (autor nemôže tvrdiť, že podpísaný dokument nevytvoril),
- *nemožnosť podpísať prázdny (tzv. bianco) dokument* - princíp elektronického podpisu toto vylučuje vzhľadom na vlastnosť integrity.

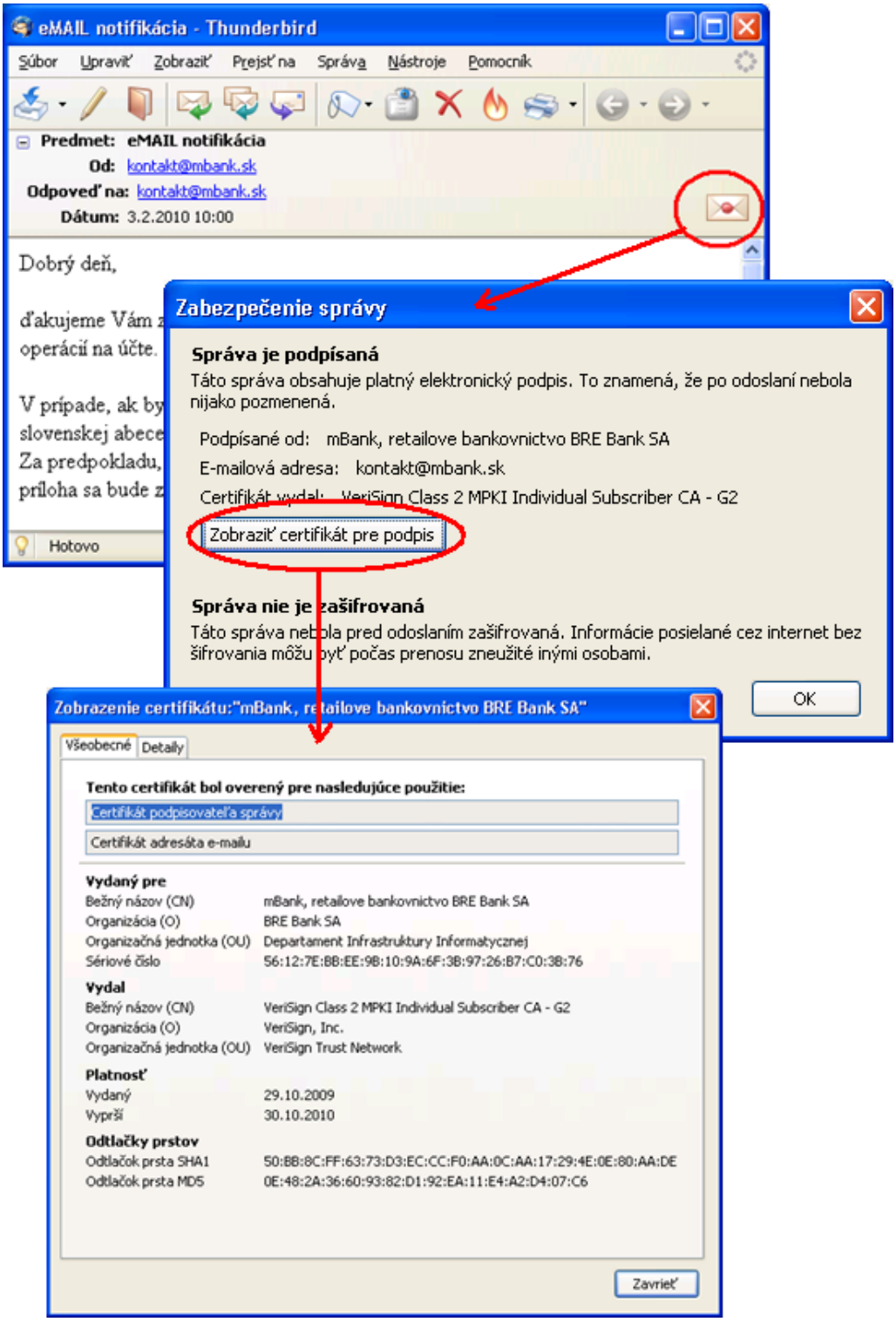
Pri elektronickom podpise sa taktiež využíva asymetrické šifrovanie ako sme opisovali v predchádzajúcej kapitole. Elektronický podpis funguje nasledujúcim spôsobom: z obsahu dokumentu sa vytvorí tzv. odtlačok (**hash**) – krátky (typicky niekoľko stoviek bitov) výťah vytvorený pomocou špecializovaných algoritmov (**hašovacie funkcie**) a takto získaný odtlačok sa následne zašifruje súkromným kľúčom autora. Zašifrovaný odtlačok predstavuje elektronický podpis, ktorý sa k podpisovanému dokumentu priloží. Pri overovaní podpisu sa z dokumentu opäť vytvorí rovnakým algoritmom nový odtlačok a z priloženého elektronického podpisu sa pomocou verejného kľúča autora dešifruje pôvodný odtlačok dokumentu. Novozískaný odtlačok sa porovná s dešifrovaným odtlačkom, a ak sú identické, tak sa týmto zaručila integrita podpísaného dokumentu. Úspešným dešifrovaním elektronického podpisu konkrétnym verejným kľúčom je jednoznačne určený autor podpisu.

**Hašovacia funkcia** je jednosmerná matematická funkcia (algoritmus) na prevod vstupného reťazca dát na krátky výstupný reťazec.

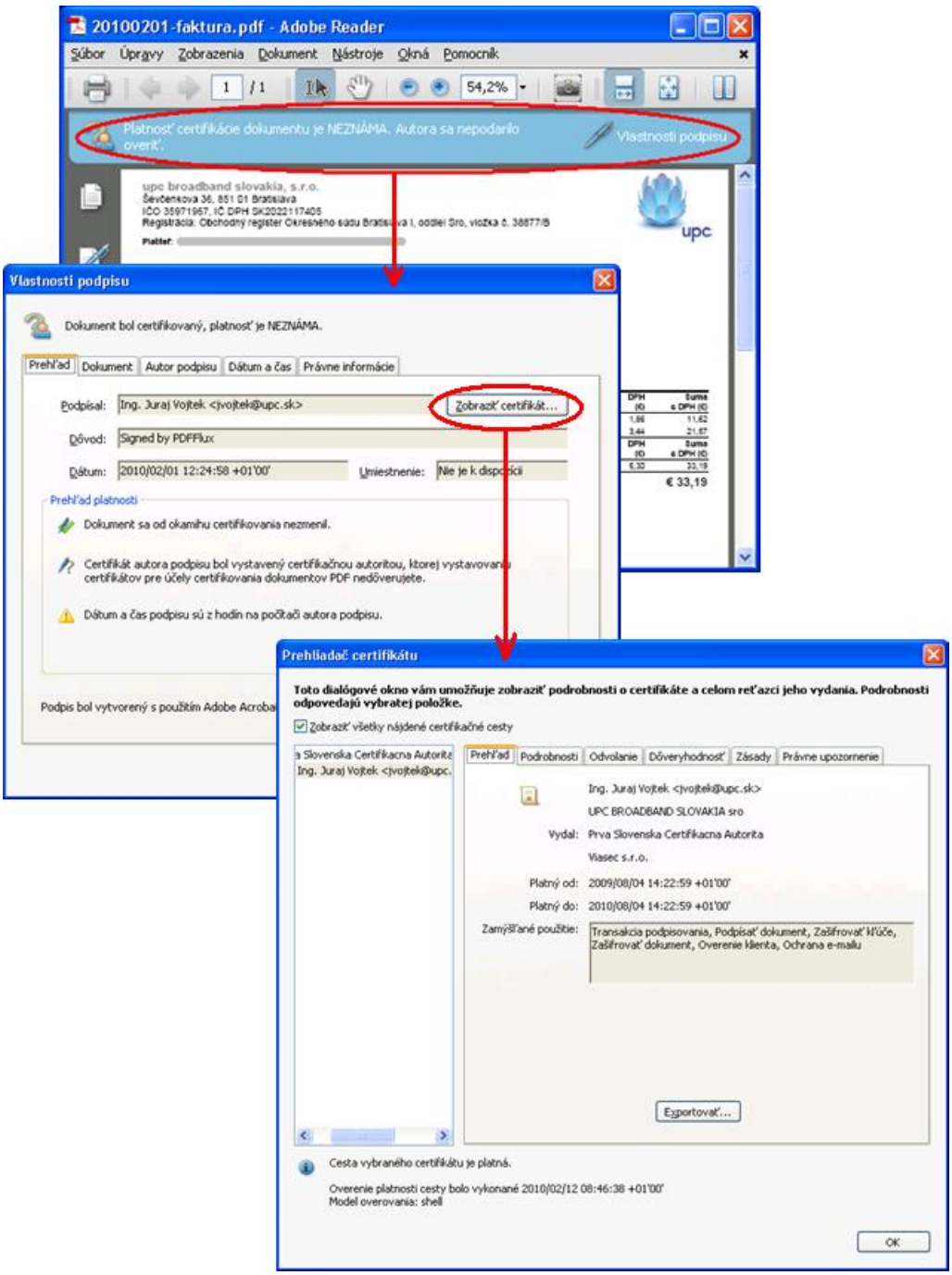



*Obrázok 17 - Vkladanie a overovanie elektronického podpisu dokumentu*

Je dôležité, aby súkromný kľúč ostal vždy súkromným, teda utajeným. V prípade straty alebo odcudzenia súkromného kľúča je dôležité okamžite zrušiť certifikát k príslušnému verejnému kľúču (predčasne ukončiť jeho platnosť). Certifikát na požiadanie vydáva, obnovuje a taktiež zneplatňuje certifikačná autorita. Vydaný certifikát k verejnému kľúču má definovanú dobu platnosti, zvyčajne jeden rok.




*Obrázok 18 - E-mail podpísaný elektronickým podpisom a jeho potvrdenie*




*Obrázok 19 - Elektronická faktúra podpísaná elektronickým podpisom a jeho potvrdenie*

## Zaručený elektronický podpis

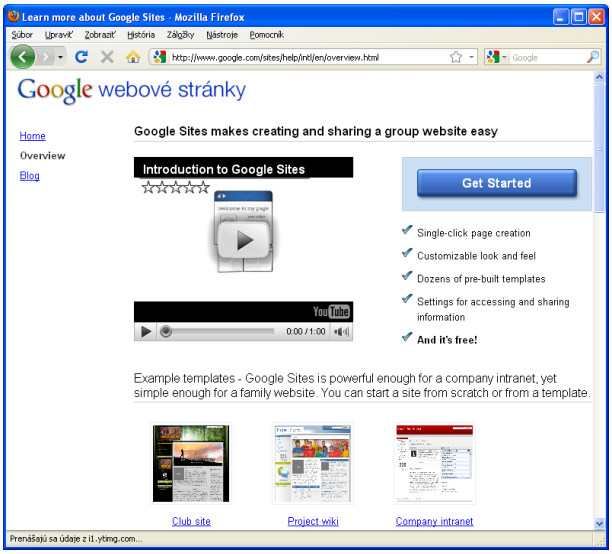
Aby bolo možné elektronický podpis použiť všade tam, kde sa vyžaduje vlastnoručný podpis, je potrebné použiť tzv. **zaručený elektronický podpis**. Zákon o elektronickom podpise (zákon číslo 215/2002 Z.z. v aktuálnom znení) zrovnoprávňuje zaručený elektronický podpis s vlastnoručným notársky overeným podpisom. To znamená, že všade tam, kde sa vyžaduje vlastnoručný podpis, a ak to dovoľujú predpisy, možno použiť zaručený elektronický podpis. V zmysle zákona kvalifikovaný certifikát, ktorý je potrebný pre zaručený elektronický podpis, môže vydať iba certifikačná autorita akreditovaná NBÚ (Národný bezpečnostný úrad). Aktuálny zoznam akreditovaných certifikačných autorít pre zaručený elektronický podpis nájdeme na stránkach NBÚ (www.nbusr.sk).

# Publikovanie na internete

Tak ako existujú webové stránky rôznych spoločností a organizácií, môžeme sa na internete prezentovať aj sami, či už svoju školu, záujmové združenie alebo sami seba.

Skôr, ako začneme na internete niečo publikovať, musíme sa rozhodnúť, akú formu zvolíme. Najrozšírenejšími spôsobmi sú:

- **Klasické webové stránky**. Môžeme ich vytvárať
  - priamo, pomocou **programov na tvorbu webových stránok**, napr. NVU (www.net2.com/nvu/), Kompozer (www.kompozer.net), 1stPage (www.evrsoft.com), Adobe DreamWeaver (www.adobe.com) atď.
  - pomocou rôznych systémov a nástrojov ako **systémov správy obsahu** (Content Management System, CMS), **WIKI nástrojov** a pod. Medzi najznámejšie patria Joomla (www.joomla.org), Google webové stránky (sites.google.com), Meu (meu.zoznam.sk), eStránky.sk (www.estranky.sk).




*Obrázok 20 – Stránka o službe Google webové stránky*

- **Blog** (napr. http://blog.sme.sk/, http://blog.matfyz.sk/). Blogy sme spomenuli v module *Základná digitálna gramotnosť* (2DG1). Pripomeňme, že blog je tiež určitá forma webovej stránky, ktorá je zameraná hlavne na publikovanie vlastných článkov, informácií, fotografií, skúseností, príbehov a názorov. Môžeme naň vkladať obrázky, videá, tagy,...
- **Profil v rámci sociálnej siete** (napr. Facebook, MySpace, Twitter, hi5). Sociálne siete patria k fenoménu doby - umožňujú spojiť sa so svojimi známymi, komunikovať, zdieľať fotografie a videá, hrať sa, ale aj prezentovať seba či svoju prácu. Profil v rámci sociálnej siete môže plniť funkciu osobnej stránky.

V prípade, že vytvárame webové stránky priamo alebo pomocou nejakého systému, budeme potrebovať webový server, na ktorom budú stránky uložené. Webový server môžeme použiť vlastný, alebo si ho môžeme prenajať.

Prenájom webového servera môže byť realizovaný viacerými spôsobmi:

- *Webhosting*
  - Freehosting – prenájom bezplatného webového priestoru
  - Komerčný – prenájom webového priestoru za úhradu, zvyčajne poskytuje aj pridanú hodnotu
- *Serverhosting* – prenájom fyzického servera (hardvér)

- *Server Housing* – umiestnenie vlastného fyzického servera u poskytovateľa internetového pripojenia

Pri prenájme webového priestoru (webhosting) využívame služby webového servera s vlastnosťami, ktoré nevieme ovplyvniť a sú určené prenajímateľovou inštaláciou. V niektorých prípadoch získame s webovým priestorom aj iné služby, napr. e-mail.

Pri prenájme fyzického servera (serverhosting) sa jedná o prenájom počítača, ktorý si môžeme sami nainštalovať. Celá réžia servera je v našich rukách a je len na nás, čo si a ako sami nainštalujeme (vrátane operačného systému, aplikácií...). Inštaláciu servera môže previesť aj prenajímateľ na základe našich požiadaviek.

Server Housing umožňuje umiestniť náš vlastný fyzický server u poskytovateľa internetového pripojenia, ktorý má zvyčajne lepšie pripojenie (priepustnosť siete) a zabezpečenie serverovne (klimatizácia, záložné zdroje, zálohovanie...) ako my.

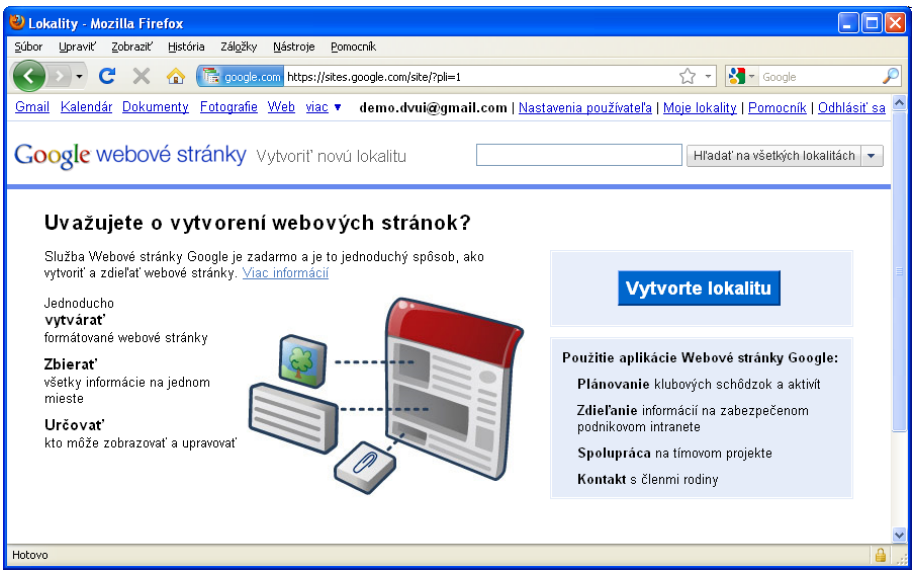
S publikovaním na internete súvisia aj iné oblasti, ktorým by sme mali venovať pozornosť, a to napr.:

- Prístupnosť publikovaných informácií
- Autorské práva publikovaných informácií

Téme **prístupnosti informácií na webe** sme sa venovali v module *Digitálne technológie pre učiteľa 2* (2DG5). Pripomeňme, že **prístupné webové miesto** je použiteľné pre každého používateľa internetu bez ohľadu na: zdravotný stav, znalosti, skúsenosti, zobrazovacie možnosti. Problém prístupnosti informácií na webe sa netýka iba zdravotne postihnutých, ale aj používateľov rôznych alternatívnych prostredí. Malo by byť v našom záujme, aby nami publikované informácie boli prístupné čo najväčšiemu okruhu ľudí.

Pri publikovaní na webe by sme sa mali zaujímať o **autorské práva** získavaných aj publikovaných informácií. Medzi pravidlami **netikety** nájdeme pravidlo (viac pozri v [32]): *Rešpektujte autorské práva iných. Nepublikujte cudzí text pod svojim menom, vždy uvádzajte meno pravého autora a zdroj odkiaľ je text prevzatý.*

V kapitole *Služby elektronickej pošty* sme si vytvorili Gmail účet, ktorý môžeme využiť aj pre iné služby spoločnosti Google, napr. pre Google webové stránky.




*Obrázok 21 – Vytvorenie lokality v službe Google webové stránky*

V úvode materiálu sme spomenuli, že toto je prvý modul zo série o princípoch a tvorbe webu. V nasledujúcich dvoch moduloch sa budeme zaoberať predovšetkým tvorbou webových stránok (napr. aj v Google webové stránky).

# Čo sme sa naučili v tomto module

## Zhrnutie

Dozvedeli sme sa o najpoužívanejších internetových službách (web, elektronická pošta, IM, P2P siete, ftp) a základných princípoch fungovania týchto služieb. Pri internetových službách sme sa zamerali aj na potrebu zabezpečenej komunikácie a oboznámili sme sa so základnými princípmi jej dosiahnutia.

Oboznámili sme sa s princípom fungovania digitálnych certifikátov a digitálnych podpisov.

Oboznámili sme sa so základnými možnosťami prezentácie na internete a využívaním hostingových služieb.

## Preverenie výstupných vedomostí

Preverovanie vedomostí prebieha priebežne. Účastníci riešia úlohy, ktoré preukážu ich zručnosti, a tiež sa zapájajú do diskusií.

# Príloha: Čísla portov sieťových služieb

Čísla portov slúžia k identifikácii požadovanej služby a odpovedajúceho komunikačného protokolu. Čísla portov môžu mať hodnotu celých čísel v rozsahu **0 až 65535** a prideľujú sa z troch intervalov:

Všetky známe čísla portov môžeme nájsť na adrese www.iana.org/assignments/port-numbers

- *známe porty* - hodnoty v rozsahu **0 až 1023**, pevne pridelené pre jednotlivé služby (prideľuje organizácia IANA),
- *registrované porty* – hodnoty v rozsahu **1024 až 49151**, registrované pre bežné používateľské procesy a aplikácie (registruje IANA),
- *dynamické porty* - hodnoty v rozsahu **49152 až 65535**, nie sú nikde registrované a volia sa náhodne (dynamicky) pre klientské procesy.

Zoznam čísel portov internetových služieb používaných v tomto materiáli:

| | | |
|---|---|---|
| **Port 20** | FTP | prenos dát z alebo na FTP server |
| **Port 21** | FTP | riadenie FTP komunikácie |
| **Port 22** | SSH Secure shell | bezpečné prihlásenie, kopírovanie súborov |
| **Port 25** | SMTP | prenos e-mailov |
| **Port 53** | DNS | preklad doménových mien a IP adries |
| **Port 80** | HTTP | webové servery |
| **Port 110** | POP3 | prístup k e-mailovým schránkam |
| **Port 143** | IMAP | prístup k e-mailovým schránkam |
| **Port 443** | HTTPS | zabezpečený HTTP prístup |
| **Port 465** | SMTP over TLS/SSL | zabezpečený SMTP |
| **Port 993** | IMAP over TLS/SSL | zabezpečený IMAP |
| **Port 995** | POP3 over TLS/SSL | zabezpečený POP3 |

# Literatúra a použité zdroje


[1] HUNT, C.(1997) Konfigurace a správa sítí TCP/IP, Brno: Computer Press, 457 strán, ISBN 80-7226-024-3
[2] PUŽMANOVÁ, R. (2004) TCP/IP v kostce, České Budějovice: Koop nakladatelství, 607 strán, ISBN 80-7232-236-2
[3] IP Version 6 Addressing Architecture, RFC 4291, [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc4291.txt>
[4] Internetová doména, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Doménové_jméno>, február 2010
[5] Doména nejvyššího řádu, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Doména_nejvyššího_řádu>, február 2010
[6] Facts About W3C – history, [online]. Dostupné na internete: <http://www.w3.org/Consortium/facts#history>, január 2010
[7] Uniform Resource Identifier (URI), RFC 3986, [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc3986.txt>
[8] Hypertext Transfer Protocol, [online]. Dostupné na internete: <http://sk.wikipedia.org/wiki/HTTP>, január 2010
[9] Hypertext Transfer Protocol – HTTP/1.1, RFC 2616, [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc2616.txt>
[10] HTTPS, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/HTTPS, http://en.wikipedia.org/wiki/HTTP_Secure>, január 2010
[11] E-mail, [online]. Dostupné na internete: <http://sk.wikipedia.org/wiki/E-mail>, január 2010
[12] Simple Mail Transfer Protocol, RFC 821 a 2821, [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc0821.txt>, http://www.ietf.org/rfc/rfc2821.txt>
[13] Post Office Protocol - Version 3, RFC 1939, [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc1939.txt>
[14] Internet Message Access Protocol – Version 4, RFC 1730 a 3501 , [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc1730.txt>, http://www.ietf.org/rfc/rfc3501.txt>
[15] The History of Electronic Mail, [online]. Dostupné na internete: <http://www.multicians.org/thvv/mail-history.html>, január 2010
[16] www.skype.com
[17] www.icq.com
[18] Peer-to-peer, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/P2P>, http://en.wikipedia.org/wiki/Peer-to-peer>, január 2010
[19] BitTorrent pod paľbou, PC Revue január 2010, strana 20-24
[20] File Transfer Protocol, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Ftp>
[21] File Transfer Protocol (FTP), RFC 959, [online]. Dostupné na internete: <http://www.ietf.org/rfc/rfc0959.txt>
[22] SSH file transfer protocol, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/SSH_file_transfer_protocol>, http://en.wikipedia.org/wiki/SSH_file_transfer_protocol>, január 2010
[23] www.filezilla-project.org
[24] PKI (Public Key Infrastructure), [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/PKI, http://en.wikipedia.org/wiki/Public_key_infrastructure>, február 2010
[25] Asymetrická kryptografie (Public-key cryptography), [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Asymetrická_kryptografie, http://en.wikipedia.org/wiki/Public-key_cryptography>, február 2010
[26] Man in the middle attack, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Man_in_the_middle, http://en.wikipedia.org/wiki/Man-in-the-middle_attack>, február 2010
[27] Certifikační autorita, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Certifikační_autorita>, február 2010
[28] Elektronický podpis, [online]. Dostupné na internete: <http://cs.wikipedia.org/wiki/Elektronický_podpis>, február 2010
[29] NBÚ: Elektronický podpis - Základy EP, PKI, Legislatíva, [online]. Dostupné na internete: <http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/ep.pdf>, február 2010 (68 strán, dátum dokumentu 17.12.2008)
[30] NBÚ: Koreňová certifikačná autorita, [online]. Dostupné na internete: <http://ep.nbusr.sk/kca/>, február 2010
[31] ÚPVS: Čo je elektronický podpis a časová pečiatka?, [online]. Dostupné na internete: <http://portal.gov.sk/Portal/sk/Default.aspx?CatID=17&eventid=1677>, február 2010
[32] prispievatelia Wikipédia (2009) *Netiketa*. Wikipédia, *Slobodná encyklopédia, 2009, http://sk.wikipedia.org/w/index.php?title=Netiketa&oldid=2513815*

Tento študijný materiál vznikol ako súčasť národného projektu Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika v rámci Aktivity „Vzdelávanie nekvalifikovaných učiteľov informatiky na 2. stupni ZŠ a na SŠ“.

Autori © Mgr. Miroslav Wagner
PaedDr. Roman Hrušecký

Názov Ďalšie vzdelávanie učiteľov základných škôl a stredných škôl v predmete informatika

Podnázov Internet: princípy a tvorba webu 1

Študijný materiál prešiel recenzným pokračovaním.

Recenzenti Mgr. Ján Skalka, PhD.
RNDr. Peter Gurský, PhD.

Počet strán 32

Náklad 300 ks

**Prvé vydanie, Bratislava 2010**



Vydal Štátny pedagogický ústav, Pluhová 8, 830 00 Bratislava, v súčinnosti s Univerzitou Pavla Jozefa Šafárika v Košiciach, Univerzitou Komenského v Bratislave, Univerzitou Konštantína Filozofa v Nitre, Univerzitou Mateja Bela v Banskej Bystrici a Žilinskou univerzitou v Žiline

Vytlačil BRATIA SABOVCI, s r.o., Zvolen

**ISBN 978-80-8118-035-4**