MUNI MED

Institut biostatistiky a analýz

Uživatel počítačové sítě

Daniel Klimeš, Roman Šmíd, Jan Krejčí

Organizace kurzu

- Podmínky zápočtu
  - Registrace v is.muni.cz
  - Účast na teoretické části
  - Zvládnutí elektronického testu

    (po skončení přednášky)

Osnova

- Pojmy, termíny
- Připojení k síti
  - Možnosti připojení, co je zapotřebí, srovnání
- Síťové služby
  - HTTP, FTP, Email, vzdálený přístup
- Bezpečnost na síti
  - Hesla a průzkumník vůbec, Firewall, email, spyware, phishing
  - Mobilní zařízení
- Šifrování a elektronický podpis
- Český E-government

Pro DPS studium

- Elektronické zdravotnictví ČR

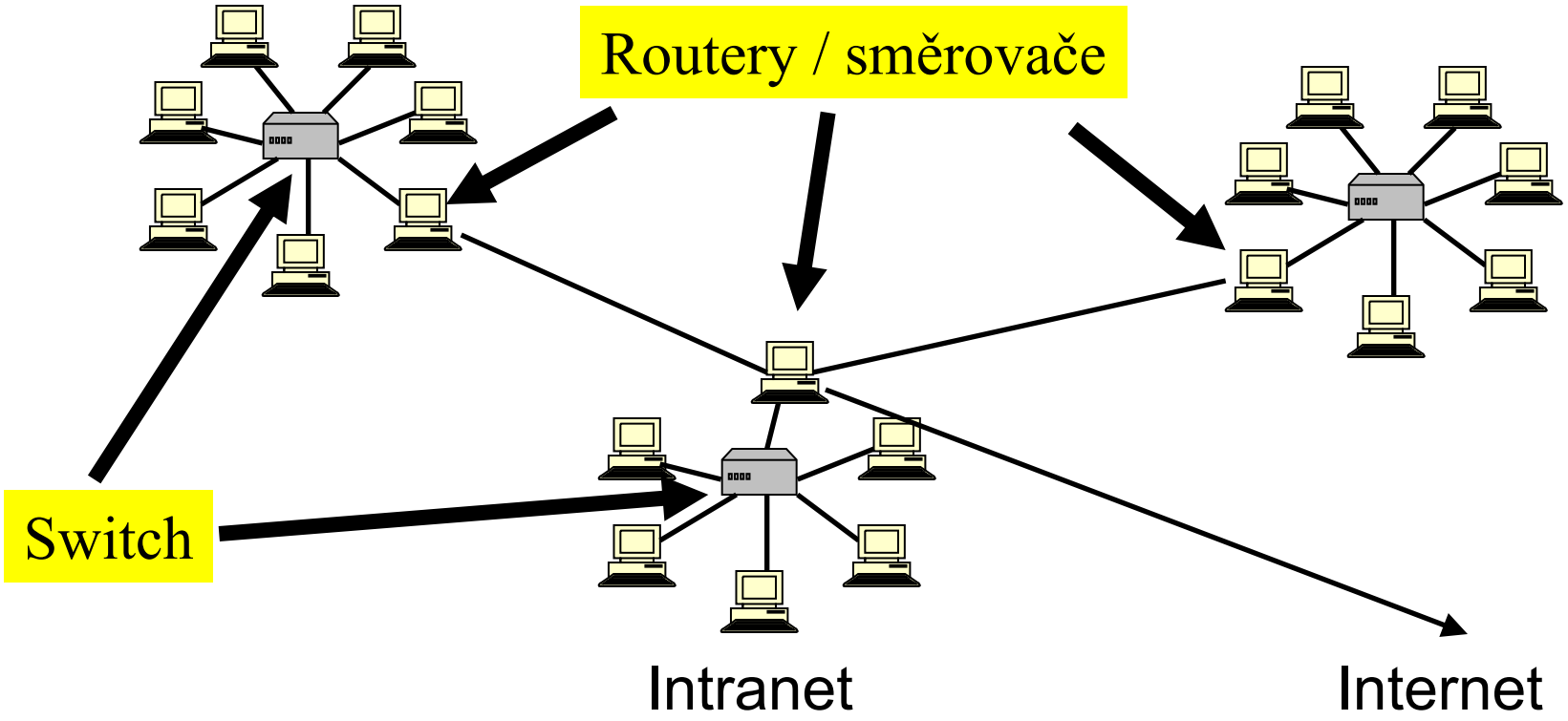
Data a jejich objem

- Jak vyjádřit informaci
- **1 bit (b) - základní informační jednotka 1/0**
- **1 Byte (B) – 8 bitů, celé číslo od 0 do 255,**
  - **1 textový znak (ASCII), např. "A" = 65**
- 1 Kb = 1024 bitů
- 1 KB = 1024 Bytů

Počítačová síť

- Propojení dvou a více počítačů
- Součástí sítě jsou síťové prvky
  - Počítač (zařízení) se síťovou kartou, modemem, wifi adaptér
  - Kabeláž (metalická, optická)
  - Rozbočovače, směrovače a přepínače, wifiroutery, antény
  - Zařízení poskytující síťové služby, síťové tiskárny…
- Kvalitu sítě, respektive konkrétní cesty v síti, lze hodnotit podle
  - **Propustnosti** (rychlosti) sítě - (K/M/G) bity za sekundu (**b/s**)
  - **Rychlosti odezvy** (milisekundy) – program **ping**

Propojení lokálních sítí



Identifikace PC v síti

- Identifikace síťové karty

  Celosvětově „jedinečná“ MAC adresa (fyzická adresa)
  00-0A-E4-C0-36-81

- IP adresa (obdoba IČO nebo telefonu)

  Celosvětově „jedinečné“
  147.251.147.76

- Internetové jméno (obdoba pošt. adresy) - URL

  Celosvětově jedinečné
  www.iba.muni.cz

IP adresa

IPv4 x IPv6

- IPv4: 32b = 2^{32} IP adres => cca 4 * 10^{9} adres
- IPv6: postupně zaváděna 128b => 3,4 * 10^{38} adres

Stejný počítač
přenesený do jiné sítě
má zpravidla jinou IP
adresu!

IP adresa

- Pevná x dynamická IP adresa
- Veřejná x neveřejná IP adresa

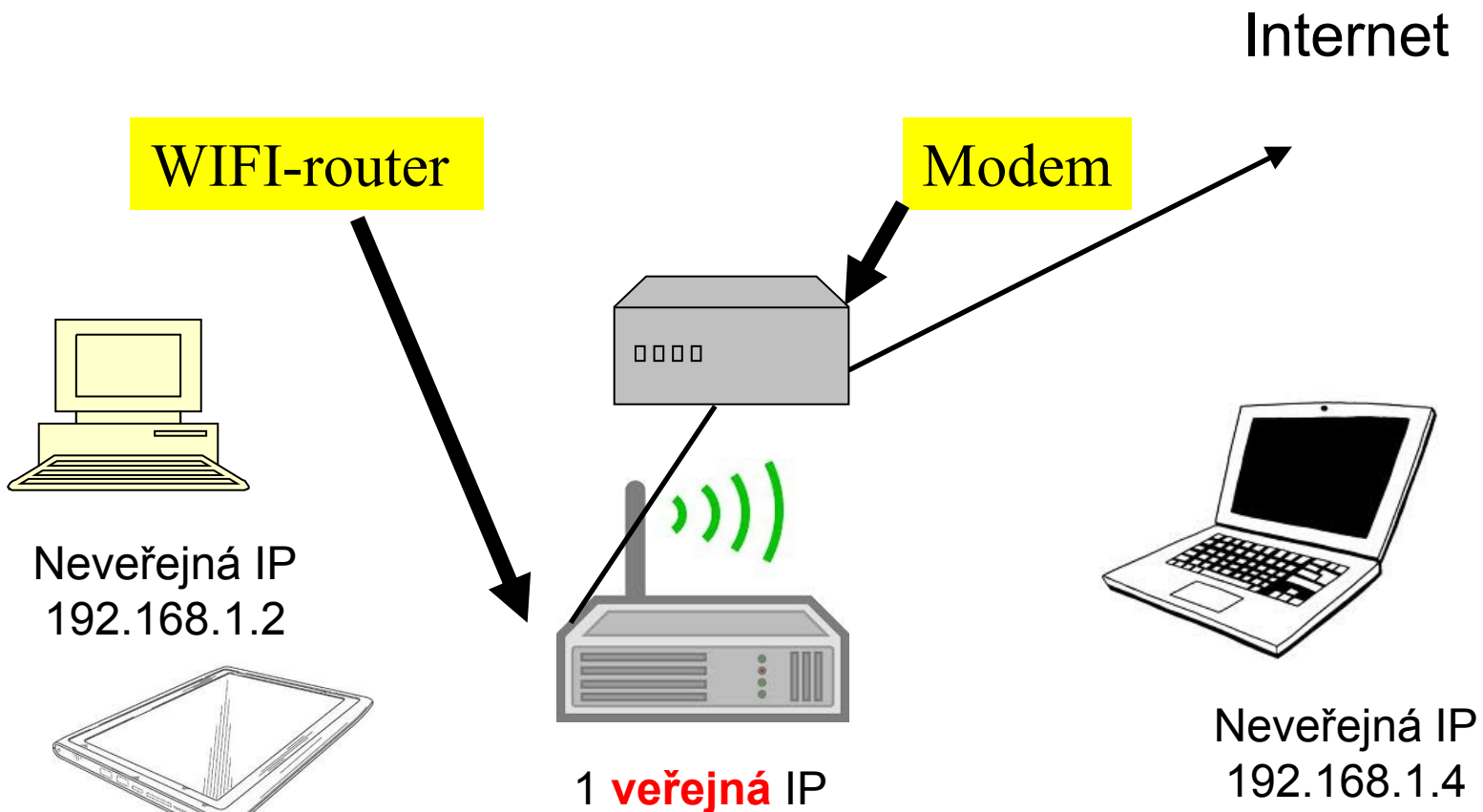
  - Neveřejná IP není celosvětově unikátní – pouze v rámci lokální podsítě
  - Neveřejné adresy nemívají přiřazené internetové jméno
  - Dynamická + neveřejná IP – typický konzument služeb
  - Pevná + veřejná IP – typický poskytovatel služeb

http://www.ip-adress.com/

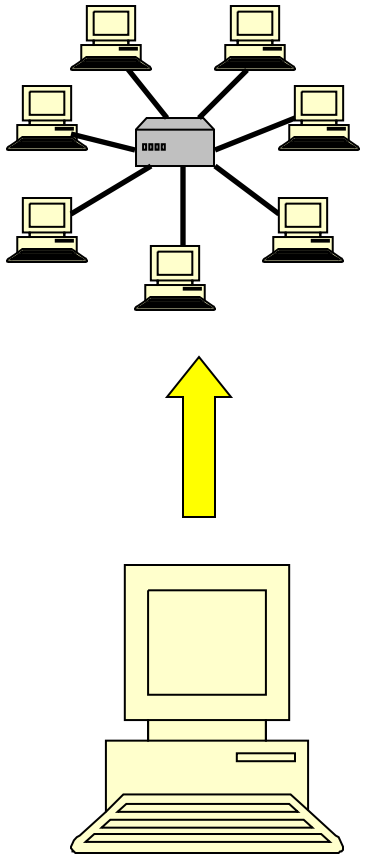
cmd - ipconfig

Neveřejné IP adresy

192.168.*.*

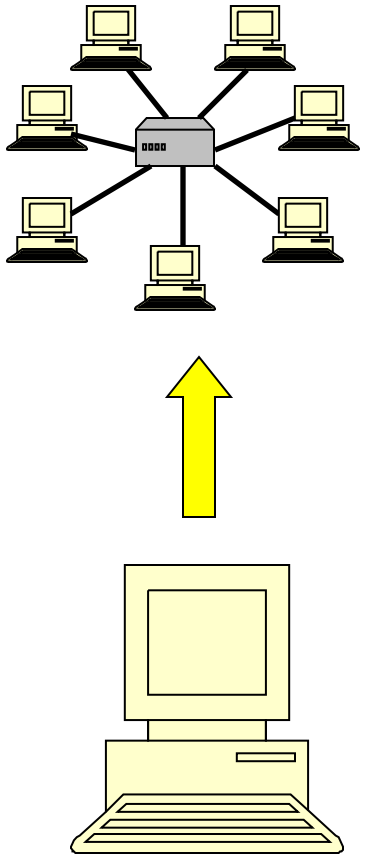


Fyzické připojení PC do sítě



- Kabelová televize
  - Modem, metalická síť x optická síť
- Telefonní linka
  - ADSL modem
- Mobilní připojení
  - Modem nebo mobilní telefon
- Bezdrátové připojení – WIFI
  - Speciální zařízení/karta, anténa

Kabelová televize



- V místech dostupnosti kabelové televize
- Rychlost až 500 Mb/s
- Metalické x optické připojení
  - Metalické má výrazně horší upload
- Speciální modem
- http://www.upc.cz
- http://www.netbox.cz
- http://www.selfnet.cz
- http://rychlost.cz/pripojeni-internetu/kabelova-tv/

Rychlost připojení v pevných optických sítích

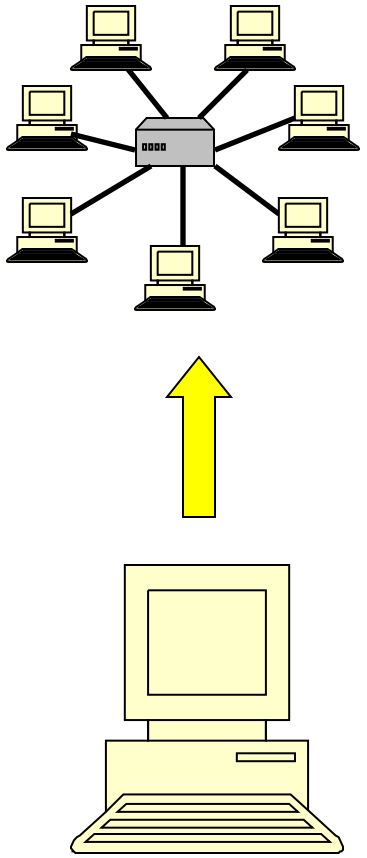
Prosinec 2018

Poskytovatel	Rychlost v Mb/s	Meziroční změna
Centrio	29,62	-1 %
Cesnet	40,58	6 %
Kabel1	28,85	4 %
Netbox.cz	27,50	-2 %
TETAnet	34,69	38 %
T-Systems	52,62	79 %
Celkem	30,08	4 %

zdroj: www.dsl.cz

MUNI MED Institut biostatistiky a analýz

Telefonní linka



- ~~Vytáčené připojení (až 56 kb/s)~~
- ~~ISDN (až 128 kb/s)~~
- ADSL (až 16 Mb/s)
- VDSL (teroreticky až 100 Mb/s)
  - Nabízeno do 1,3 km od ústředny

- Každý typ vyžaduje specifický modem

xDSL připojení - rychlost

Prosinec 2018

Poskytovatel	Rychlost v Mb/s
AVONET	20,68
Český Bezdrát	17,49
GTS	15,86
O2	19,16
T-Mobile	17,61
Vodafone	17,99
Celkem	18,89

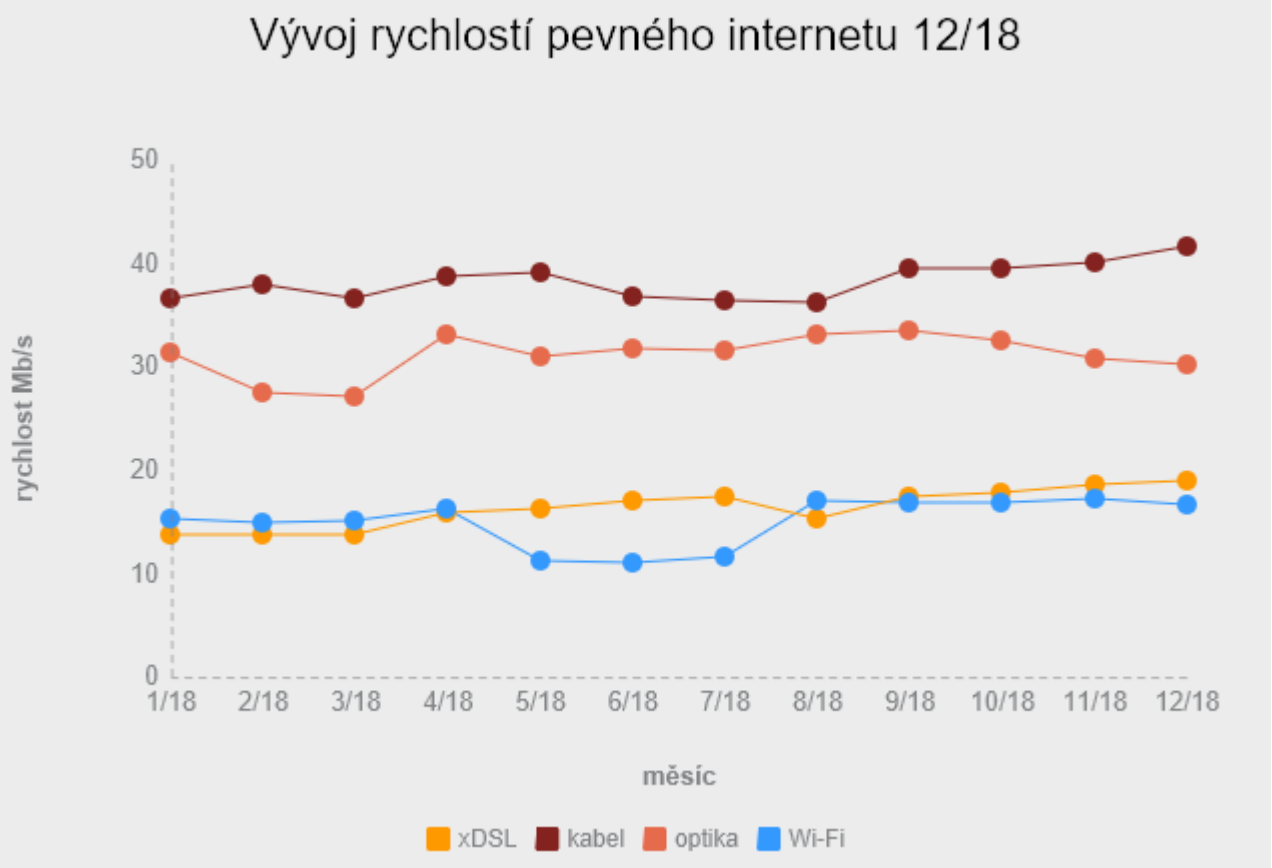
zdroj: www.dsl.cz

WiFi-připojení

- Outdoor/indoor
- Komerční/komunitní sítě
- Rychlost až 54 Mb/s
- Speciální cenově dostupné vybavení
- Zabudované v notebooku - indoor
- Riziko rušení, odposlouchávání, neoprávněného připojení
- Přístupový bod /Access point/ hot spot
- http://www.internetprovsechny.cz/wifi/
- https://it.muni.cz/sluzby/wifi
  - Eduroam

Wi-Fi připojení - rychlost

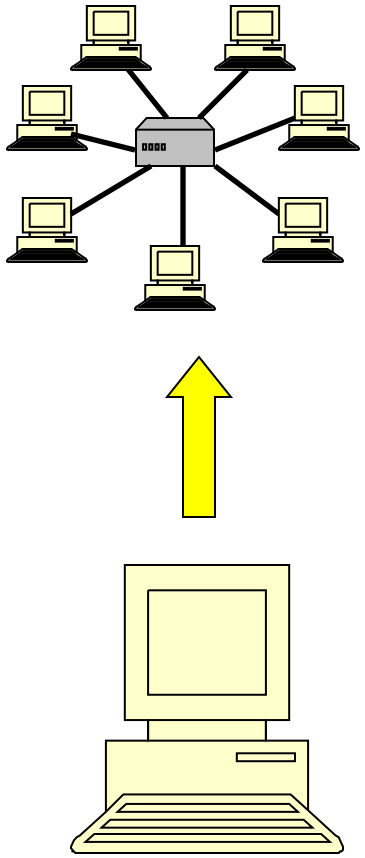
- **V rozmezí 5 – 21 Mb/s**
- **Průměr kolem 15 Mb/s**



zdroj: www.dsl.cz

MUNI MED Institut biostatistiky a analýz

Mobilní připojení



- GPRS (až 128 kb/s)
- 2G - EDGE (až 512 kb/s)
- 3G - UMTS/HSDPA (1024 kb/s a více)
- **4G - LTE (80 Mb/s a více)**
  - **Větší pokrytí než 3G**
  - Novější smartphony a modemy

Mobilní připojení - rychlost

Prosinec 2018

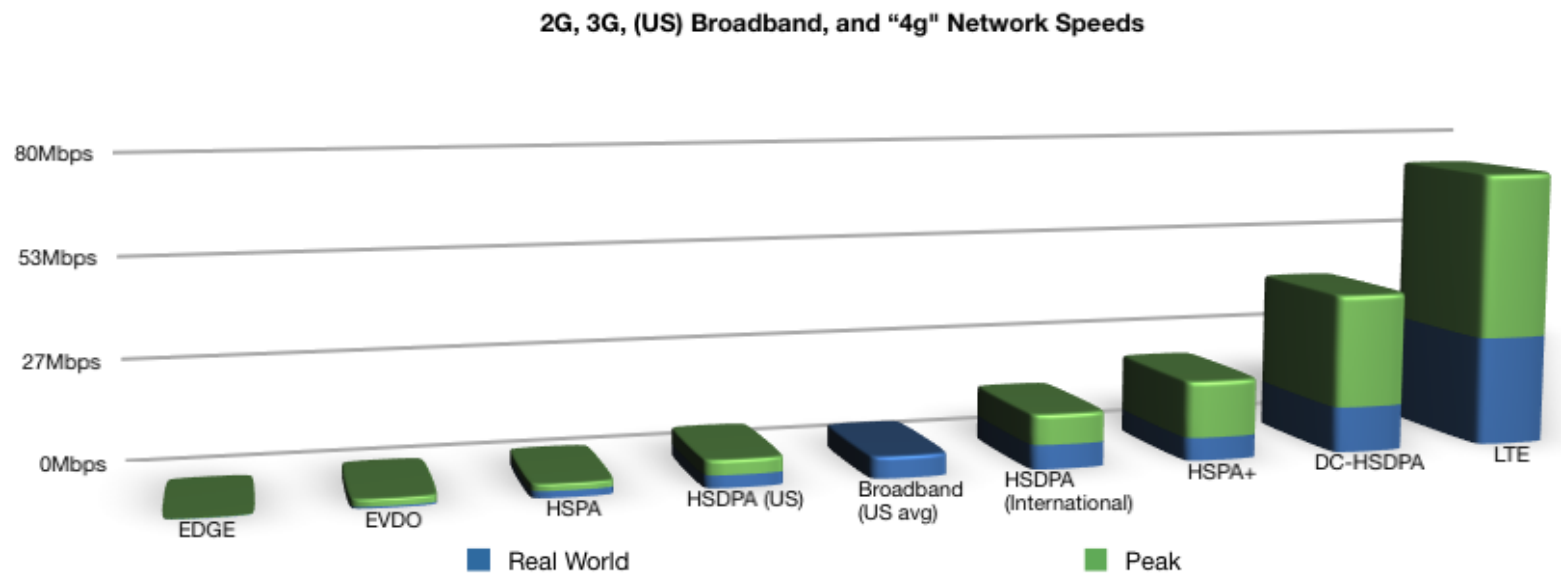
Technologie	Poskytovatel	Rychlost v Mb/s	Meziroční změna
LTE	O2	33,70	12 %
LTE	T-Mobile	46,29	22 %
LTE	Vodafone	45,43	6 %
3G	O2	11,36	16 %
3G	T-Mobile	5,86	-45 %
3G	Vodafone	7,37	28 %
2G	O2	0,10	6 %
2G	T-Mobile	0,10	-4 %
2G	Vodafone	0,07	-29 %

zdroj: www.dsl.cz

MUNI MED Institut biostatistiky a analýz

Rychlost připojení přes GSM

- Mnoho termínů a zkratek – GPRS, EDGE, UMTS, HSPA, HSPA+, HSDPA, HSUPA, WCDMA, 3G, 4G, LTE….



Zdroj: tasel.wordpress.com

LTE pokrytí

- Velká dynamika
- Stránky poskytovatelů nebo
- http://lte.ctu.cz/pokryti/
- Pro všechny operátory

- LTE pásma
  - LTE-800 = základní pro ČR

Výběr připojení k internetu

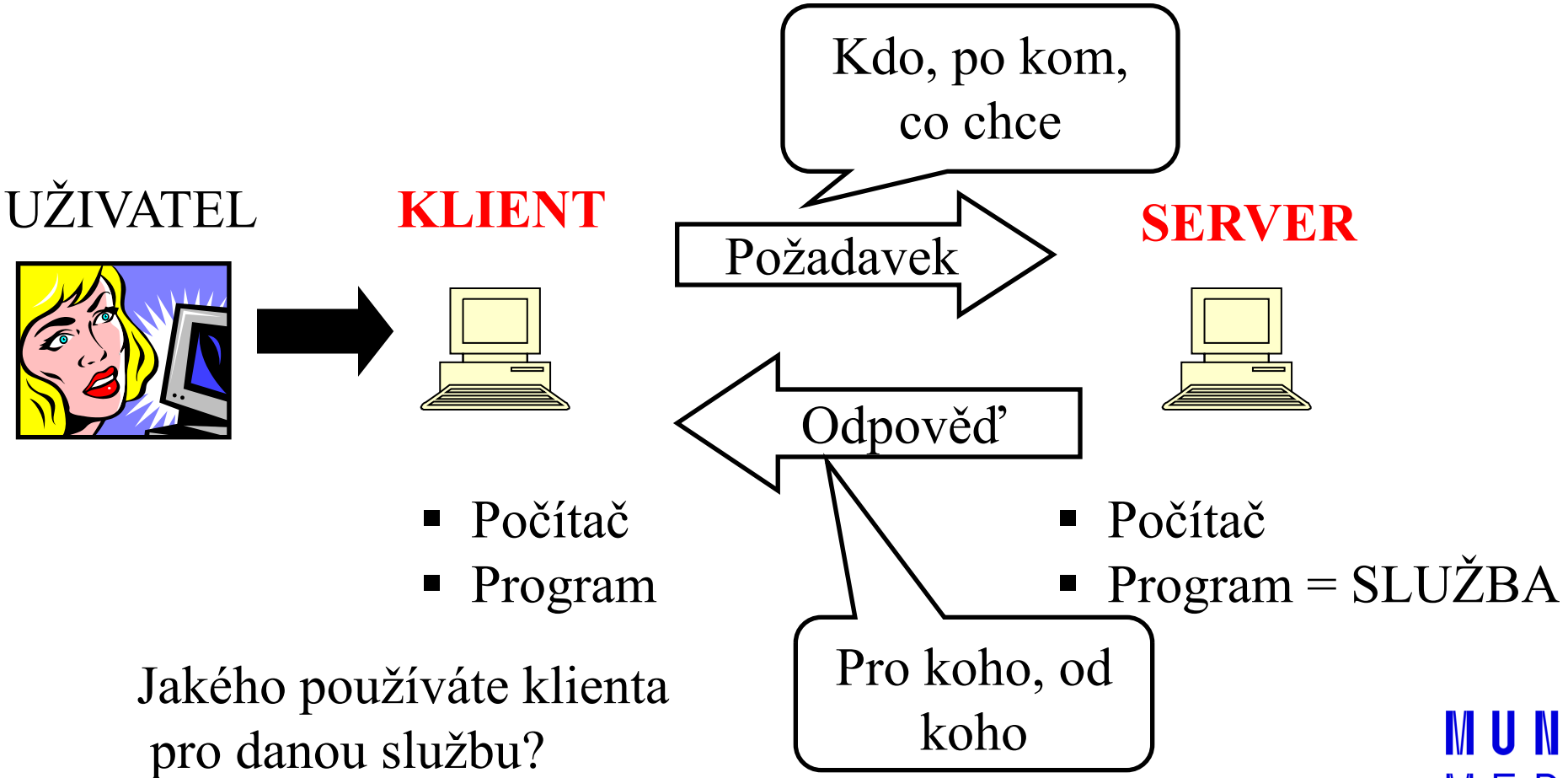
- Způsob použití – pevné PC x notebook
- Dostupnost v daných lokalitách, pokrytí
- Rychlost, většinou v Mb/s
  - symetrické x **asymetrické** (download, upload)
  - (např.: 20/2 Mb/s)
  - Skutečnou rychlost ověřit v praxi
- Fair user policy (FUP) – omezení rychlosti po přenesení určitého množství dat
- Agregace (např.: 1:32) – (ADSL, bezdrátové připojení)

Aktuální rychlost mezi dvěma počítači lze orientačně změřit pomocí speedmetrů

Např.: http://nastroje.lupa.cz/mereni-rychlosti/, www.dsl.cz

Vzájemná komunikace počítačů v síti

Model Klient – Server



- Počítač
- Program

- Počítač
- Program = SLUŽBA

Jakého používáte klienta pro danou službu?

Síťové služby

- DHCP, DNS
- HTTP, FTP, SSH, POP3, IMAP, SMTP
- Typicky jeden server poskytuje více služeb
- Server je identifikován IP adresou (tel. číslo), služba svým číslem zvaným port (klapka)
- Kompletní adresa služby je IP adresa serveru + číslo portu
- Každá služba má definovaný standardní port, např. HTTP port č. 80

Zobrazení aktuálně využívaných služeb – **cmd** + **netstat**

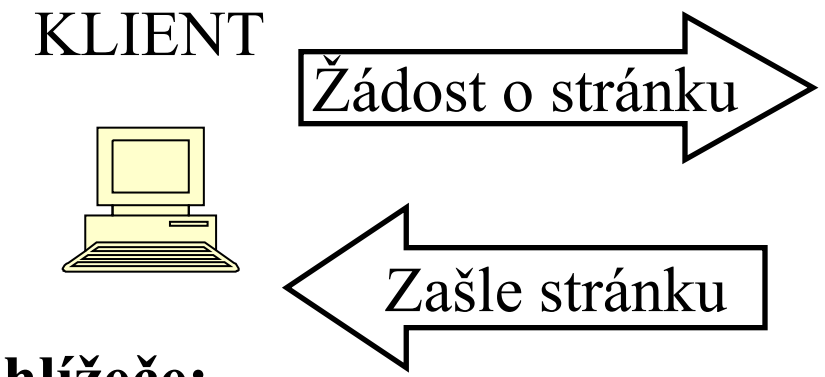
Služba DHCP

- Automatická konfigurace síťového připojení vašeho počítače v lokální síti
- DHCP protokol nastavuje veškeré parametry nutné pro připojení PC do sítě, zejména
  - **IP adresa** PC (147.251.147.250)
  - **Maska sítě** (255.255.255.0)
  - **IP adresa brány** (gateway) (147.251.147.1)
  - **IP adresy DNS serveru** (147.251.26.1)
- Připojení počítače (síťové karty = MAC adresy) může povolit/zakázat administrátor sítě

DNS služba

- Překlad internetových jmen na IP adresy
- Ne každá IP adresa má definováno internetové jméno
- Překlad realizují DNS servery, které udržují seznam známých internetových jmen a případně se dotazují dalších DNS serverů na neznámá jména
- Bez dostupnosti této služby nelze využívat internetová jména, pouze IP adresy

Webové stránky HTTP(S)



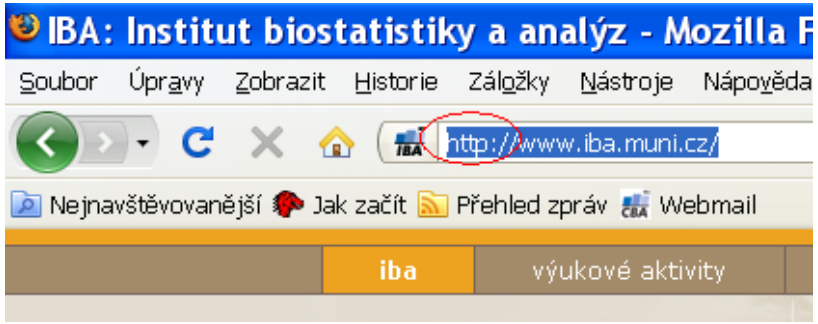
Prohlížeče:
Internet Explorer
Mozilla Firefox
Chrome
Edge
Safari

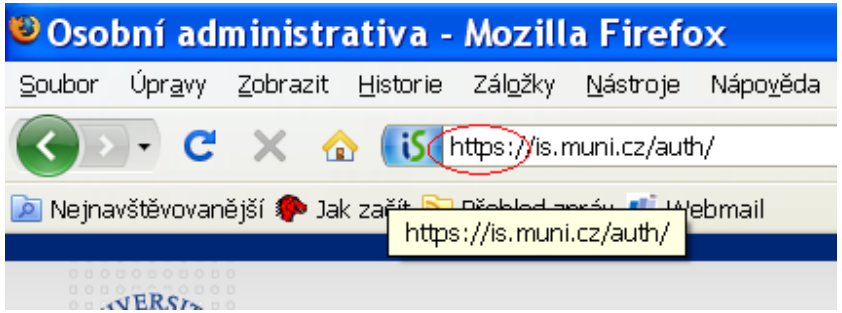
Servery:
IIS
Apache

Porty:
HTTP – 80
HTTPS - 443

HTTP x HTTPS

- Veškerá komunikace klienta se serverem je šifrována – data jsou během přenosu nečitelná
- HTTPS má vlastní port 443
- Server musí podporovat službu HTTPS





MUNI MED Institut biostatistiky a analýz

COOKIES

- Malé soubory ukládané na vašem počítači
- Svázané s konkrétním serverem
- Prohlížeč je zasílá s požadavkem na server
- Server je tvoří/upravuje, posílá prohlížeči
- Server si vás "pamatuje„
- Kampaň k ochraně soukromí
- Riziko převzetí spojení po vašem přihlášení ke službě
  - otevřená WIFI, při nešifrovaném spojení

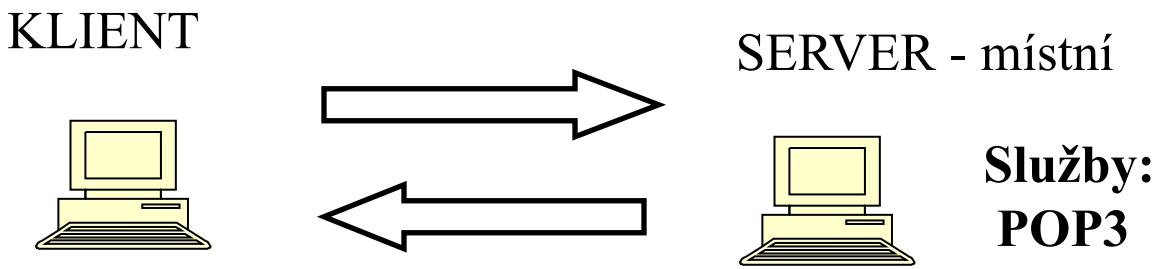
Odstranění uložených cookies

- IE
  - Možnosti Internetu – Obecné
    Odstranit…
- Firefox
  - Nabídka Možnosti – Soukromí
    Odebrat soubory cookies
- Chrome
  - Nastavení – Ochrana soukromí
    Vymazat údaje o prohlížení
- Edge
  - Nastavení – Vymazat údaje o procházení

Emailové služby

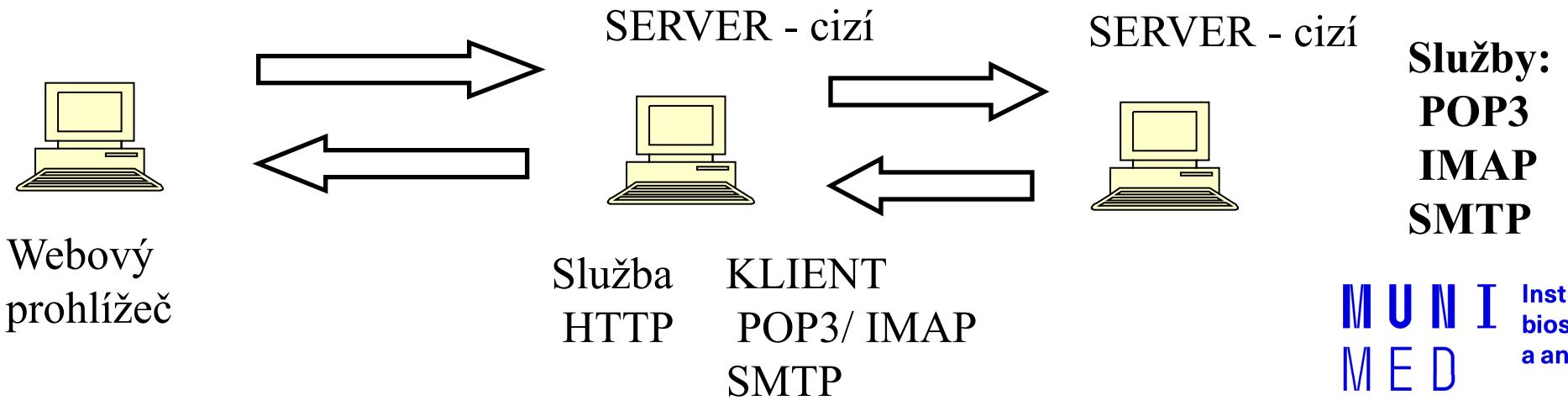
- E-mailová schránka = soubor(y) primárně ležící na poštovním serveru
- Poštovní servery spolu komunikují – přeposílají maily
- E-mailové programy x e-mail přes webové rozhraní
- Služby pro čtení pošty
- Služba pro odesílání pošty

Email přes lokálního klienta



Email přes webové rozhraní

Seznam.cz, centrum.cz, email.cz, gmail, …

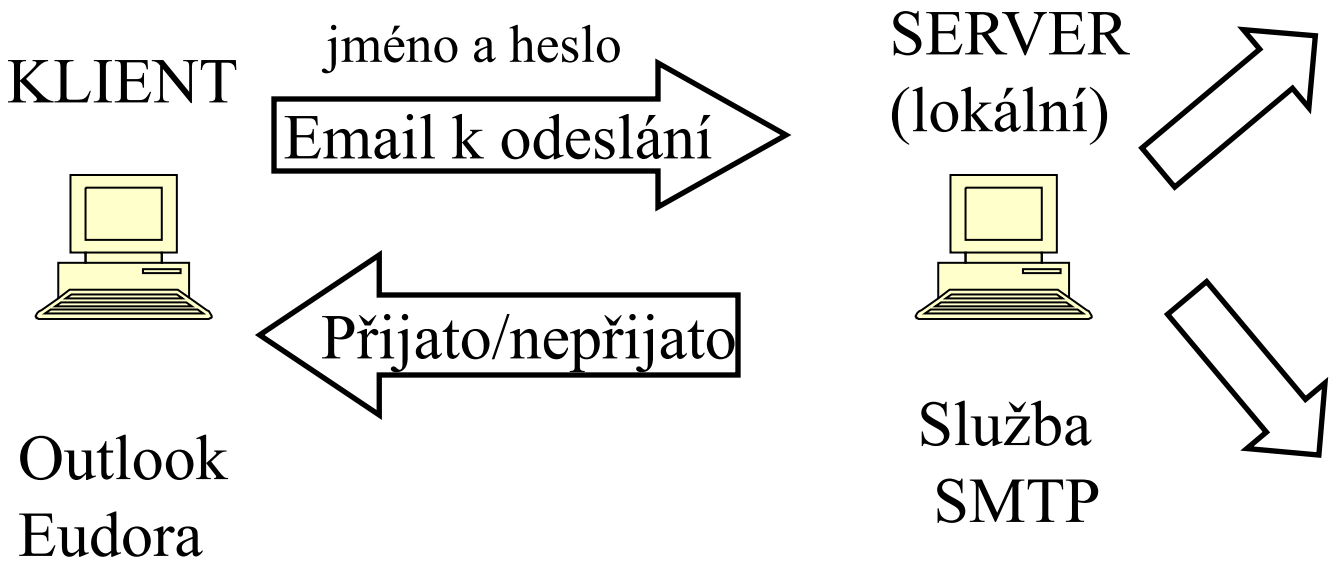


MUNI MED Institut biostatistiky a analýz

Služby POP3 a IMAP

POP3	IMAP
Zašle všechny nové emaily – celé Odstraní je ze serveru	Zašle pouze hlavičky emailů Obsah emailu zašle až na vyžádání
Třídění emailů do složek na lokálním počítači	Všechny emailové složky na serveru
Vhodné pro off-line čtení	Vhodné při čtení pošty z více počítačů

Odesílání pošty služba SMTP



VPN (Virtual private network)

- Služba simuluje připojení vzdáleného počítače do lokální sítě
- „Tunel“ do vzdálené sítě
- Vzdálenému počítači je přidělena lokální IP adresa
- Vzdálené PC se pak stává „téměř“ plnohodnotnou součástí vnitřní sítě
- http://vpn.muni.cz/ (OpenVPN)
- Nutná instalace, administrátorská oprávnění
- UČO + sekundární heslo

VPN MU

Popis služby

- VPN (virtual private network) poskytuje zaměstnancům i studentům přístup do univerzitní sítě například z domu, zahraničí nebo jiné univerzity. Po připojení k VPN se počítač bude chovat tak, jako by byl připojen přímo k univerzitní síti.
- Studenti a zaměstnanci mohou tak využívat služeb, které jsou dostupné pouze z univerzitní sítě, i když v této síti zrovna nejsou. Po připojení k VPN získáte veřejnou adresu z rozsahu MU a tím například:
  - přístup k placeným informačním zdrojům MU odkudkoliv (seznam dostupných zdrojů pro MU: http://ezdroje.muni.cz/prehled/abecedne.php?lang=cs),
  - přístup ke službám dostupným pouze ze sítě MU (např. specializovaná zařízení a přístroje nebo přístup k univerzitním licencím).
- Připojit k VPN můžete například PC s Windows, Mac OSX, Linux nebo jiným, mobilním zařízení s OS Android nebo iOS.

MUNI MED Institut biostatistiky a analýz

Bezpečnostní zásady při práci s PC

Rizika při práci v počítačové síti

Co nám hrozí?

- Ztráta dat
  - V případě selhání hardware, ztráty nebo odcizení PC, zavirování

Následky ztráty dat jsou individuální, záleží na povaze dat.

- Možnosti zálohování
  - CD/DVD
  - Jiný počítač
  - USB disk
  - NAS (**N**etwork **A**ttached **S**torage – „datové úložiště na síti“)
  - Cloudové úložiště
    - OneDrive
    - GoogleDrive

Co nám hrozí?

- Útok hackera
  - **Automatizovaný a plošný** (e-mail, www, IM, sociální sítě)
    Cílem hackera je ovládnout váš PC, získat z něj citlivé údaje (čísla kreditních karet, hesla…), odcizit hotovost z účtu nebo jej použít k dalším útokům
  - Cílený přímo na Vás
    Cílem může být získání citlivých firemních dat (konkurenční boj, diskreditace)

Možné následky útoku:

- Přímá finanční ztráta (odcizení peněz z účtu přes kreditní kartu)
  Správné nastavení limitů na kartě
- Policejní stíhání (obvinění z použití PC k nelegálním aktivitám)
- Problémy v zaměstnání (zablokovaný email, VPN, …)
- Vydírání a diskreditace (zveřejnění citlivých informací, fotografií, e-mailů…)
- Ztráta dat (**RansomWare**)
  WannaCry (květen 2017)

Úvod – jak se bránit?

- PC jako pracovní nástroj: je nutné dodržovat bezpečnostní pravidla jako s každým jiným nástrojem, zejména v těchto oblastech:
  - Práce s emailem a přílohami
  - Instant messaging (Skype, ICQ, Jabber…)
  - Sociální sítě (Facebook, Google+, LinkedIn, Twitter…)
- Je třeba **rozumět hlášením operačního systému** a dalších programů, které vyžadují uživatelskou akci a adekvátně reagovat
- Je třeba udržovat OS, antivir a všechny používané aplikace aktualizované
- Data jsou často důležitější než samotný hardware – je důležité **zálohovat**:
  - Vím, co se z mého PC zálohuje, kam a v jakých intervalech?
  - Umím si zkontrolovat, zda zálohování funguje?
  - Umím si zálohovaná data v případě potřeby obnovit?
- Přístupové údaje k různým službám – jaká mám kde hesla? Kam je ukládám?
- Správně zabezpečená WiFi síť

Bezpečnost E-mailu

- Hrozby:
  - SPAM – nevyžádané zprávy posílané za účelem:
    - Rozesílání reklamy
    - Sběru aktivních emailových adres
    - Distribuce škodlivého kódu
    - Vylákání peněz
  - Phishing – nevyžádaná zpráva, hromadně rozesílaná za účelem:
    - Vylákání přístupových údajů k různým službám
    - Vylákání soukromých informací
  - Spear Phishing – nevyžádaná zpráva cílená a upravená pro konkrétního uživatele
    - Převážně na objednávku
    - Cílem bývá zavlečení škodlivého kódu do vnitřní sítě organizace za účelem získání přístupu k citlivým firemním datům
    - Jde o velmi zákeřný útok, na který se mohou nachytat i zkušení uživatelé

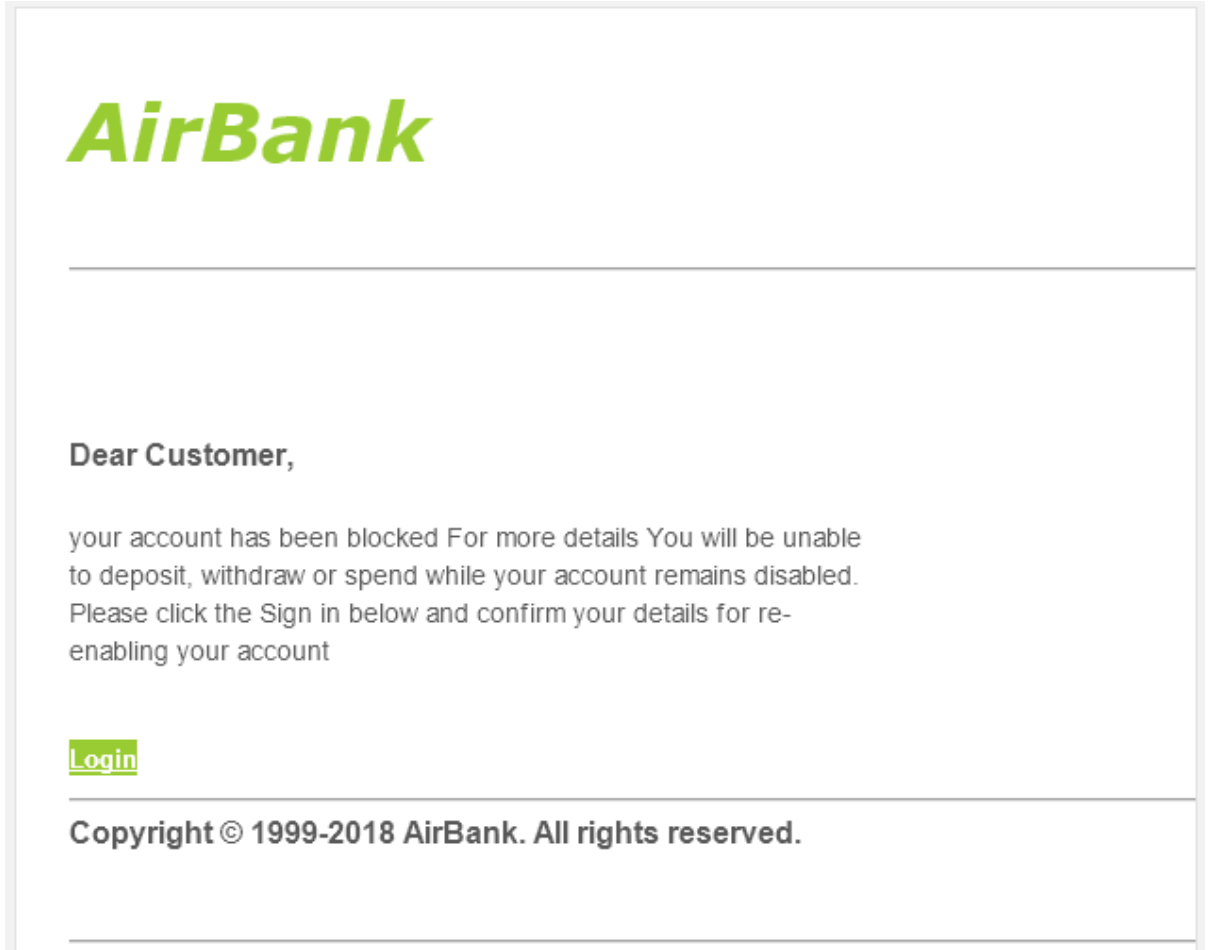
Bezpečnost E-mailu

- Pravidla:
  - Neklikat na odkazy v neznámých zprávách (nebezpečí podvržení adresy, nasměrování na stránku se škodlivým kódem)
  - Neotvírat přílohy v neznámých a podezřelých zprávách
  - Nikam neposílat loginy a hesla, čísla kreditních karet
  - Všímat si podezřelých rysů ve zprávách (strojově přeložený text, odkazy vedou jinam než jejich popis, zprávy předstírající že pocházejí od masově používaných služeb (Facebook, banky atd…), podezřelá adresa odesílatele
  - Neignorovat případná varování antivirových programů
  - Nenechat se zastrašit (Pokud nenainstalujete software X.Y., váš počítač bude ohrožen…)

Příklad zavirovaného emailu

- Vážená paní, vážený pane,
- děkujeme za projevenou důvěru v internetové obchody obchody24.cz.
- Tímto emailem potvrzujeme, že jsme v pořádku přijali vaši objednávku.
-
- Číslo objednávky (variabilní symbol): JCBDF729B439057 Datum a čas objednávky: 11.01.15 00:45 Kontaktní údaje:
- Barbora Záňová
- +420 604 920 148
-
- Vaše objednávka:
- ----------
- SONY DSC-F828 Cyber-Shot 8 mil. obraz.bodu, bílá: 1 x 23 549,00 Kč =23 549,00 Kč
- Doúprava PPL: 113 Kč
- ----------
- Celková cena nákupu vč. DPH: 23 662,00 Kč Způsob platby: Platba předem – platební karta
- Poznámka: Potvrzení platby a fakturu najdete v přiloženém souboru (ucet111D535.zip)
- -
- Nyní prosím vyčkejte na našeho operátora, který se s vámi spojí maximálně do 1 pracovního dne a dohodne podrobnosti ohledně Vaší objednávky.

Fishing


AirBank
Dear Customer,
your account has been blocked For more details You will be unable to deposit, withdraw or spend while your account remains disabled. Please click the Sign in below and confirm your details for re-enabling your account
Login
Copyright © 1999-2018 AirBank. All rights reserved.

Cloudové služby (OneDrive, Google Disk,…)

- Hrozby: odevzdání vašich dat cizímu subjektu
  - U většiny cloudových služeb jejich používáním souhlasíte s tím, **že data tam nahraná může firma použít k jakýmkoli účelům**, předávat je dalším subjektům, publikovat, analyzovat atd.
  - Týká se to drtivé většiny nešifrovaných cloudových poskytovatelů i poskytovatelů emailových služeb –
    - Google Disk,
    - Microsoft OneDrive,
    - Seznam,
    - Volny.cz atd.
  - **Tyto služby jsou nevhodné pro jakkoliv citlivá data – osobní údaje, vědecké publikace….**
  - Možné řešení – **šifrované cloudové služby** – takové, kde poskytovatel služby do Vašich dat nevidí, protože se ukládají na jejich serverech šifrovaně a klíč má pouze uživatel.
    - Emailové služby – Protonmail, Lavabit,…
    - Služby pro ukládání dat – SpiderOak, Mega (?),…

  Pokud nechcete odevzdat svá data cizí firmě, používejte pouze šifrované cloudové služby. Vždy je vhodné číst podmínky použití dané služby.

Sociální sítě

- **Facebook** – zneužíván pro šíření spamu, hoaxů, škodlivého kódu
  - Nebezpečná je důvěra v přátele: kliknu na cokoli, co postne někdo z mých přátel
  - Obtížná orientace v prostředí, které se často mění – pasti na neznalé uživatele
  - Clickjacking – kombinace sociálního inženýrství a tlačítek To se mi líbí

    Příklad: Klikněte postupně na všechna tlačítka To se mi líbí pro zobrazení videa apod. Na konci často pouze webová stránka se škodlivým kódem, stránka tahající z lidí peníze nebo zvyšující si uměle návštěvnost
- **Google+** - platí obdobná pravidla jako pro Facebook, zatím méně rozšířené
- **Twitter** – šíření adres stránek obsahujících škodlivý kód

Základní pravidlo – neklikat na cokoli, přemýšlet. I počítače vašich přátel mohou být napadeny škodlivým kódem, který na jejich FB profilu posílá příspěvky…

Na sociální sítě přistupujeme většinou přes internetový prohlížeč – tedy platí zásady zabezpečení prohlížeče (viz. dále)

Antivirus a antispyware

Pokud nepoužíváme nějaký **placený antivirový program**, je vhodné použít **zdarma dostupné antivirové produkty.**

Pro domácí nekomerční použití jsou to například

- **Microsoft Security Essentials** – produkt Microsoftu, distribuovaný přes Microsoft Update. Nenáročný, dostačující, v češtině
- **Avast Free Antivirus** – produkt české firmy AVAST Software, velmi oblíbený, automatické aktualizace, mírně náročnější na systémové zdroje, nutná obnova bezplatné registrace po 1 roce
- **AVG Antivirus FREE** – další český produkt, také vhodný pro běžné použití
- **Panda Cloud Antivirus FREE** – antivir pracující na cloudové bázi, menší zátěž PC
- **Comodo Antivirus** – základní ochrana od firmy Comodo

Antiviry si většinou automaticky aktualizují své virové databáze, je třeba nechat tuto funkci povolenou!

Antispyware – software na odstranění a blokování spyware (programy, které odesílají data o uživateli třetí straně bez jeho vědomí)

- **Spybot Search & Destroy** – zdarma pro nekomerční účely, český překlad
- **Spyware Terminator** – zdarma i pro komerční účely, český překlad
- **Ad Aware SE Personal Edition** – zdarma pro nekomerční účely
- **Windows Defender** – standardní součást Windows Vista a vyšších verzí

Antispyware není většinou nutné používat stále, ale je vhodné občas nějaký nainstalovat a nechat proskenovat počítač.

Přístupová hesla

Běžně využíváme mnoho různých internetových služeb – máme mnoho přístupových údajů

- Nebezpečné tendence – všude používat stejné a jednoduché heslo
- Známé služby čelí častým útokům hackerů s cílem ukrást přístupové údaje uživatelů (často úspěšně)
- Pokud mám všude stejný login a heslo, hacker najednou získá přístup do všech mých účtů!
- Zásady:
  - do důležitých služeb (přístupy do banky atd.) používat **unikátní přístupové údaje**
  - Jako přístupové údaje jsou často vyžadovány e-mail a heslo. **Nikdy nezadávat stejné heslo, jako máme do emailu!!** Při vyzrazení těchto údajů hackeři začnou využívat váš e-mail k šíření spamu a virů, hrozí zablokování účtu.
  - Pokud máme hesel mnoho, zvážit použití **softwarového správce hesel**

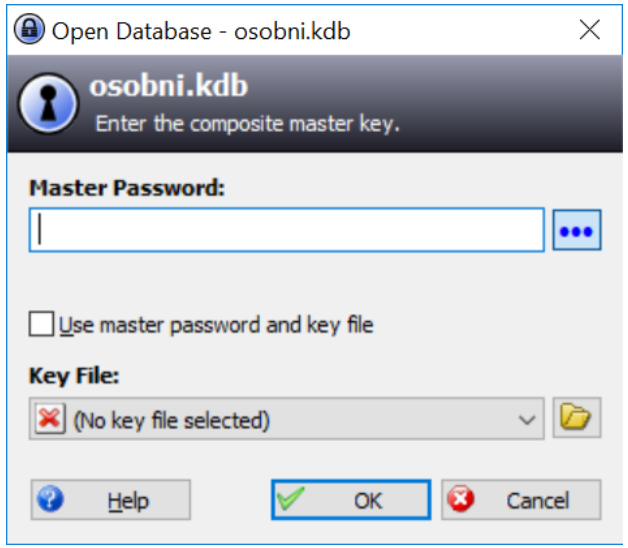
Přístupová hesla – správce hesel

Správce hesel – užitečný pomocník pro bezpečnou práci s hesly

Je třeba si pamatovat pouze jedno hlavní heslo, ostatní hesla jsou bezpečně a přehledně uloženy v programu.

Mezi nejznámější software této kategorie patří:

- **KeePass Password Safe** – přehledný správce hesel, zdarma i pro komerční použití, existuje i verze pro mobilní telefony
- **LastPass** – doplněk pro internetové prohlížeče, předvyplní internetové formuláře, generuje hesla
- **Password Agent** – umí uchovat hesla a další informace, možnost instalace na USB klíčenku



Zabezpečení domácí sítě

Vstupní branou do domácí sítě je často **domácí router**. Jeho kvalita a adekvátní zabezpečení zásadně ovlivňuje bezpečnost celé domácí sítě.

Problémem levných routerů bývá nedostupnost sw. aktualizací od výrobce a nekvalitní software – tyto routery bývají nebezpečné.

Základní pravidlo je **neponechávat** AP ve výchozím nastavení od výrobce!! Nastavit administrátorské heslo a zvolit vhodné zabezpečení Wi-Fi:

Existující formy zabezpečení domácích AP (Access point, bezdrátový router):
- Otevřená síť (bez zabezpečení) (nepoužívat ani omylem, kom. není šifrována)
- Šifrování WEP (zastaralé, dávno prolomeno)
- **Šifrování WPA-PSK nebo WPA2-PSK**
- Šifrování WPA(2) – Enterprise (Eduroam, podnikové)

Nekvalitně zabezpečený AP vystavuje nebezpečí vás!!

zdroj: www.dsl.cz

MUNI Institut biostatistiky a analýz
IBA

Zabezpečení domácí sítě

V domácích podmínkách preferujeme zabezpečení **WPA2-PSK** v kombinaci se šifrováním **AES** (někdy označováno jako CCMP)

- nabízí rozumnou míru bezpečnosti
- je nutné zvolit **kvalitní PSK** (rozumně dlouhé a složité heslo)
  - doporučuje se **alespoň 13 znaků**
  - kombinace písmen a číslic
  - nepoužívat známá hesla (existují seznamy nejpoužívanějších hesel)
- **vypnout WPS (QSS)** (WiFi Protected Setup) na AP (prolomeno v prosinci 2011)
- Pokud má router přednastavené jméno sítě a náhodné heslo od dodavatele, je nutné jej změnit na vlastní, bezpečné (časté například u UPC)

Vhodné je nelitovat vyšší investice a koupit kvalitní router, který kromě vyšší rychlosti nabídne i kvalitní software a bezpečnostní aktualizace. Těchto routerů však není na trhu mnoho (Turris Omnia od CZ NIC).

Nekvalitně zabezpečený router vystavuje nebezpečí vás!!

zdroj: www.dsl.cz

MUNI Institut biostatistiky a analýz

Mobilní zařízení

- Obyčejné x chytré telefony
- OS telefonů a kompatibilita
- Internet v telefonu, tabletu
- Bezpečnost a rizika plynoucí z mobility

Obyčejné x chytré telefony

- Chytrý telefon (smartphone) – obsahuje pokročilý operační systém, umožňuje instalaci a úpravy dalších programů, které dále rozšiřují možnosti telefonu.
- Příklady OS pro smartphony: **Android, iOS**, Windows Phone, Firefox OS, Tizen, Symbian, MeeGo
- Výhody: velké množství aplikací a tím i možností, co lze s telefonem dělat (kancelář, hry, čtení knih, internetové aplikace, navigace atd.)
- Nevýhody: typicky kratší výdrž baterie, často větší rozměry, různá bezpečnostní rizika (viry, vyzrazení soukromých informací), cena
- V roce 2013 se poprvé prodalo celosvětově více smartphonů než obyčejných telefonů.

Tablety

- Dotyková zařízení, OS často stejný jako na smartphonech, mohou mít i telefonní funkce.
- Tvoří mezičlánek mezi smartphony a klasickými osobními počítači. Některé novější tablety jsou plnohodnotnými počítači se standardním OS
- Používané OS: **Android, iOS,** Linux, Windows
- Prodeje klesají, nastupují menší „phablety“

Kompatibilita

- Různé OS mobilních zařízení NEJSOU mezi sebou kompatibilní (nelze spouštět programy pro Android např. na iPhonech)
- Nejvíce používané programy však bývají napsány pro nejpoužívanější OS (např. Skype existuje pro Android, iOS i Symbian nebo Windows)
- Z pohledu uživatele tedy absence kompatibility nepředstavuje většinou problém, je však třeba na to myslet při koupi nového zařízení – programy koupené pro iOS nelze instalovat na Android – nutné zakoupit znovu.

Internet v mobilních zařízeních

- Přípojení je bezdrátové (WiFi, GSM).
- Obsahují plnohodnotný internetový prohlížeč, emailový klient, komunikátory, VoIP klienty, VPN, terminálové klienty, vzdálenou plochu atd.).
- Při připojení přes GSM může být limitujícím faktorem datový tarif. Po vyčerpání datového limitu se připojení zpomalí a práce s internetem se stává nepohodlná nebo nefunguje prakticky vůbec. Důležitý je správný výběr datového tarifu.

Bezpečnost mobilních zařízení

- Hlavní problémy:
  - Operační systémy a jejich aktualizace

    Ze strany výrobců zařízení je aktualizace OS v reakci na nové bezpečnostní zranitelnosti často pomalá nebo žádná. Hlavně starší modely telefonů bývají často výrobcem ponechány bez aktualizací a tedy zranitelné vůči dávno známým chybám.
  - Nepozornost uživatele

    Při instalaci nových aplikací se OS vždy ptá uživatele, zda smí aplikaci udělit oprávnění k určitým činnostem v rámci systému (např. čtení/posílání SMS, přístup na internet atd.). Uživatelé by měli dávat pozor, jaká oprávnění aplikaci udělí a jaké aplikace instalují.

Bezpečnost mobilních zařízení

- Data a přístupy v mobilních zařízeních

  Zařízení často obsahují důvěrná data uživatelů nebo přístupy k různým službám (email, bankovnictví apod.). Často však nebývají adekvátně zabezpečena pro případ ztráty zařízení. **PIN ani odemčení gestem nestačí!!** Dostačující ochranou je **šifrování** celého zařízení včetně SD karty. Tuto možnost dnes nabízí většina současných modelů. Vhodná je i aktivace možnosti **vzdáleného vymazání** zařízení v případě ztráty.

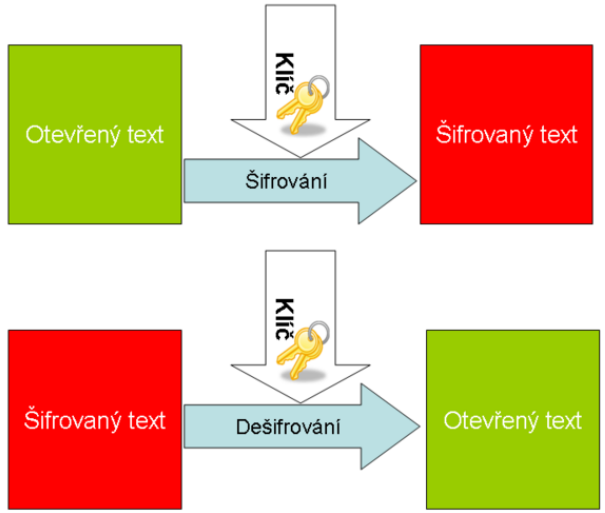
MUNI MED

Institut biostatistiky a analýz

Šifrování a elektronický podpis

Šifrování

- Změna podoby (zakódování) textu a dat do formy, která je bez znalosti dešifrovacího klíče (hesla) nečitelná



- Lze šifrovat např.
  - Dokumenty (7zip, winrar - symetricky)
  - Emaily (podpora emailových klientů, veřejný klíč adresáta)
  - Síťovou komunikaci (https, sftp, imaps, ssh)
  - Disky (truecrypt, realcrypt, bitlocker)
- Utajení obsahu komunikace a dokumentů

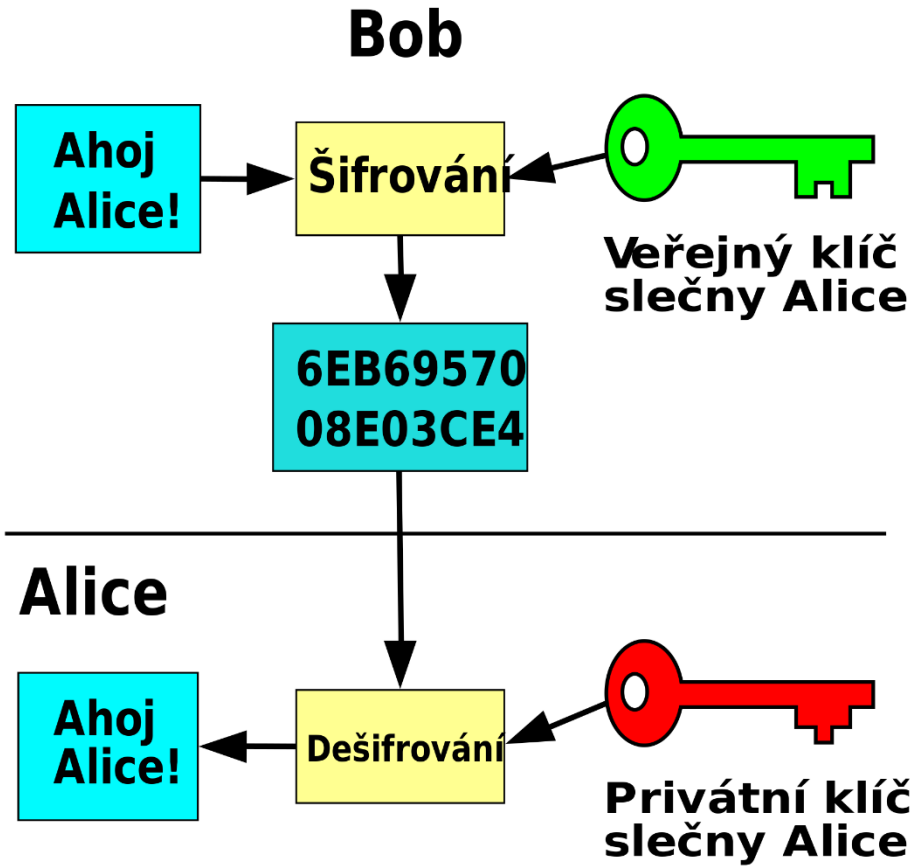
Typy šifrování

- Symetrické šifrování
  - Jednodušší podoba, pro šifrování i dešifrování je použit jediný klíč - heslo

- Asymetrické šifrování
  - Klíč má dvě části, **soukromou** a **veřejnou**

    Pokud mi chce někdo zaslat **šifrované** informace, zašifruje je pomocí **veřejné části klíče příjemce**.
    Jediný, kdo dokáže tato data dešifrovat je vlastník privátní části klíče, tedy já

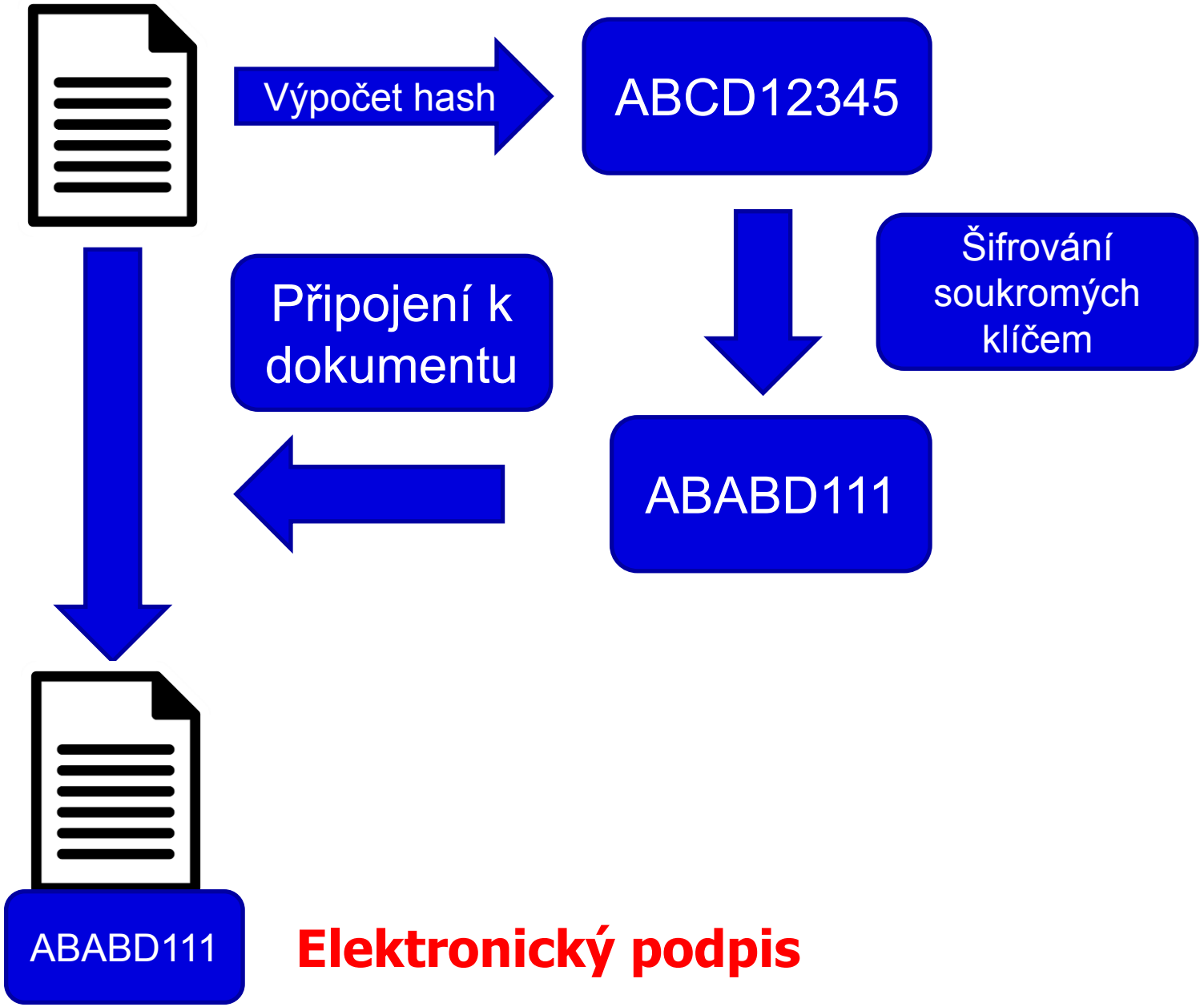
Asymetrické šifrování



Elektronický podpis

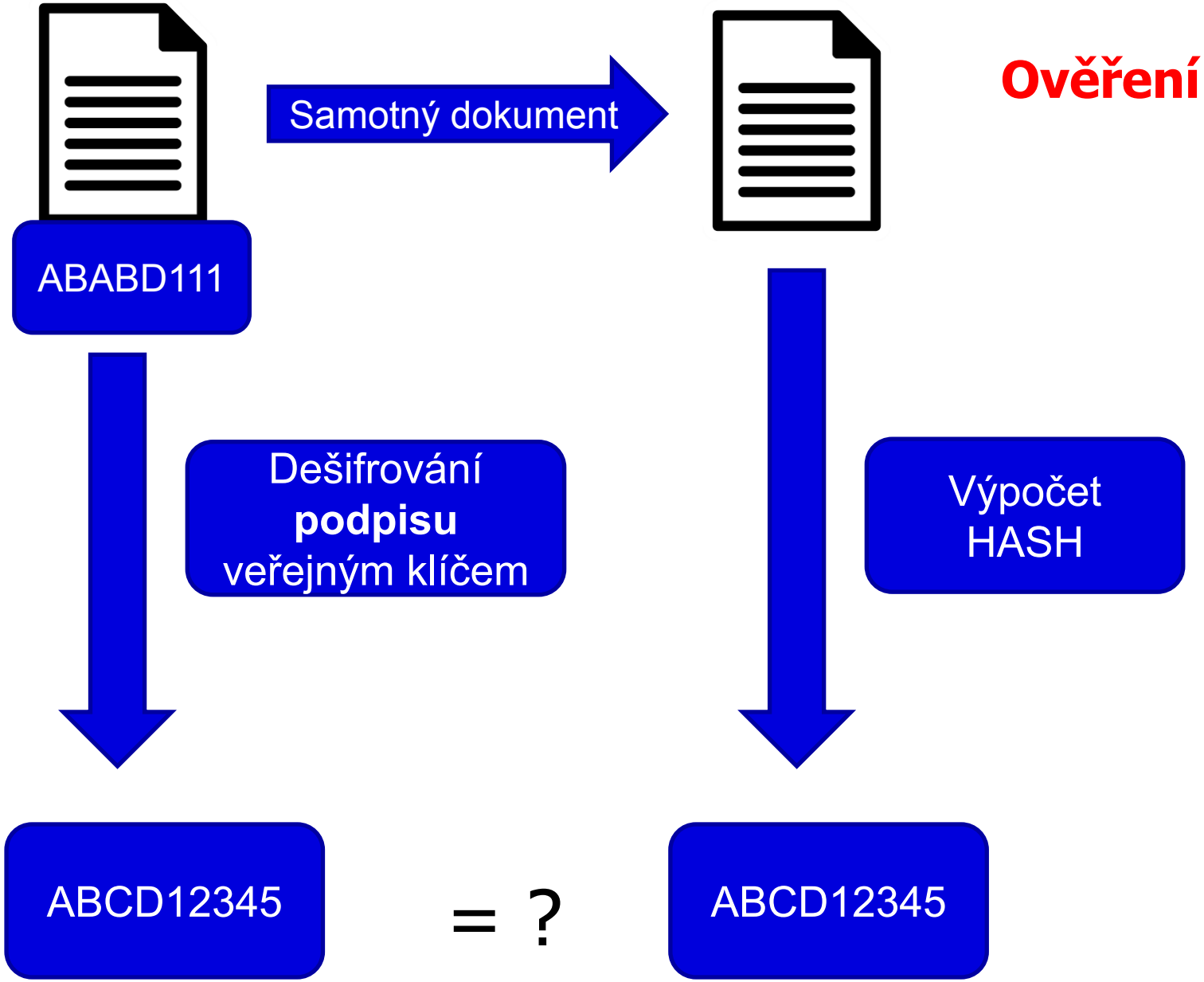
- **Využívá prvky asymetrického šifrování**
- Pokud chci nějaký text digitálně **podepsat**, stačí pro podepsání použít **soukromou** část klíče (provede emailový klient, PDF editor)
- Každý, kdo zná veřejnou část mého klíče (je odesílána automaticky s podepsaným emailem) pak může mnou digitálně podepsaný text
  - Přečíst
  - **Ověřit, zda jsem autorem/odesílatelem**
  - **Ověřit, zda nebyl text někým neoprávněně pozměněn**
- Podepsaný email/dokument **není šifrovaný!!**

- Nemusíte nic „počítat“ nebo si pamatovat, provede emailový klient nebo jiná aplikace (pdf reader)



Elektronický podpis

Ověření podpisu



Digitální certifikát

- Fyzicky = počítačový soubor od certifikační autority
  - Vydává certifikační autorita
  - Omezená platnost certifikátu (obvykle 1 rok)
- Obsahuje
  - **Údaje o subjektu** (uživatel, server)
    - Jméno
    - E-mailová adresa
    - Další identifikační údaje
  - **Veřejný klíč subjektu**
- **Oddělenou komponentou je příslušný soukromý klíč**
- Lze odvolat (revokovat) v případě vyzrazení soukromého klíče
- **Kvalifikovaný** x komerční certifikát

Kvalifikovaný x komerční certifikát

- **Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce**
- Kvalifikovaný certifikát
  - **Vydává kvalifikovaný poskytovatel** služeb vytvářejících důvěru
  - **https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx**
  - Česká pošta (PostSignum)
  - První certifikační autorita, a. s.
  - eIdentity a. s.

Digitální certifikát – jak získat prakticky

- Vydávají tzv. certifikační autority (např. Česká pošta)

1. Přihlášení do webové (případně stažení off-line) aplikace
2. Vlastnoruční vygenerování a uložení páru klíčů s heslem
3. Vyplnění žádosti
4. Návštěva pobočky s žádostí, ověření údajů
5. Zařazení veřejné části klíče certifikační autoritou do seznamu ověřených klíčů
6. Obdržení podepsaného certifikátu s veřejným klíčem a identifikací

- Lze snadno integrovat do používaných emailových aplikací ve formě certifikátu = zaručený digitální (elektronický) podpis

- Na MU lze získat osobní digitální certifikát pro uživatele zdarma na adrese http://pki.cesnet.cz/cs/tcs-personal.html

Elektronický podpis a eIDAS

- elektronický podpis (FO) – vyjadřuje souhlas
- elektronickou pečeť (PO)
- elektronickou značku - vyjadřuje původ (PO)

a. kvalifikovaný elektronický podpis (QES, Qualified Electronic Signature):

- Musí být založen na kvalifikovaném certifikátu pro elektronický podpis
- Musí být vytvořen pomocí kvalifikovaného (bezpečného) prostředku pro vytváření elektronických podpisů (čipová karta a USB token = **QSCD** (od: Qualified Signature Creation Device).

b. zaručený elektronický podpis, založený na kvalifikovaném certifikátu

- Musí být založený na kvalifikovaném certifikátu
- Není nutný kvalifikovaný prostředek (certifikovaná čipová karta/token).

c. zaručený elektronický podpis (AdES, Advanced Electronic Signature)

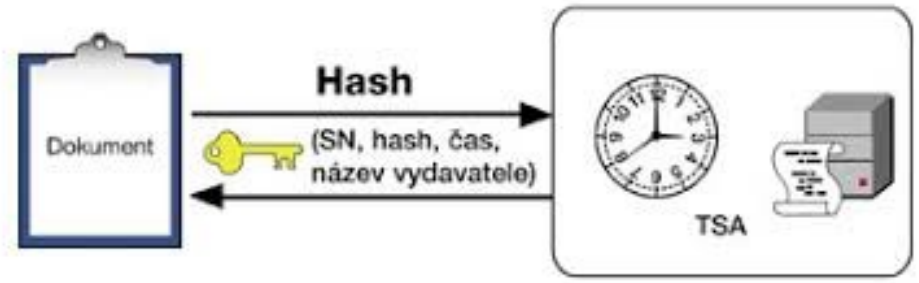
- Bez specifických požadavků na certifikát

Uznávaný elektronický podpis = společné označení pro a. i b.

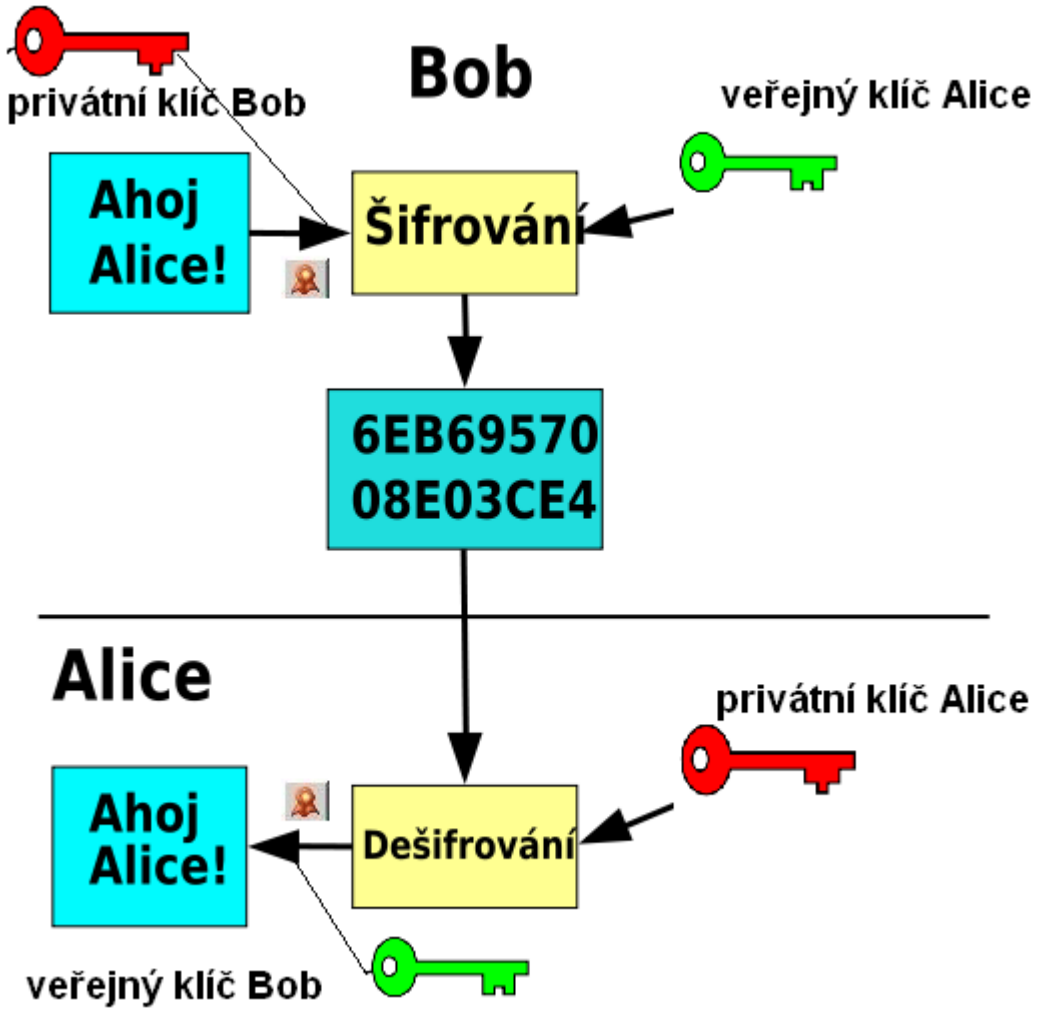
- úroveň B, T, LT či LTA
  - T jako Time (časové razítko)
  - LT jako long term

Elektronické časové razítko

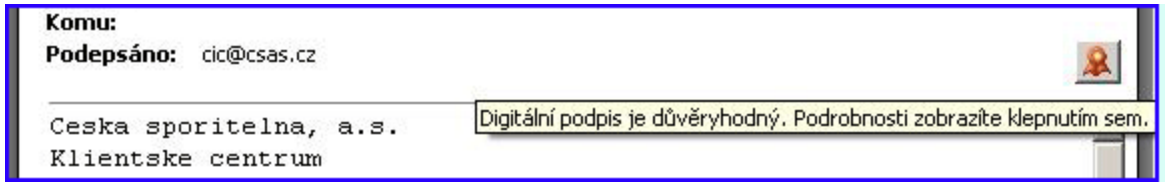
- Doložení, že dokument v daném okamžiku existoval v příslušné podobě.
- Kombinuje se s elektronickým podpisem
  - „Prodlužují“ platnost el. podpisu
- Omezená platnost, ale delší než el. podpis
- Prosté a kvalifikované razítko



Šifrovaný email



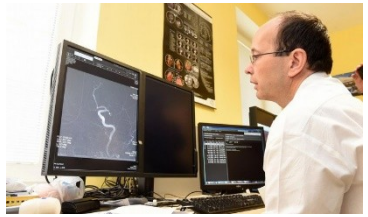
- Bob **podepíše** zprávu Alici svým soukromým klíčem
- E-mail **zašifruje** veřejným klíčem Alice
- Alice **dešifruje** zprávu svým privátním klíčem
- **Ověří** Bobův podpis pomocí jeho veřejného klíče



MUNI MED Institut biostatistiky a analýz

Vzdálené ověřování osoby

… aneb jak se vzdáleně prokázat, že jsem to já



1) Něco jedinečného vím

2) Něco jedinečného mám

→ **Prostředky prokazování identity**

Úroveň důvěryhodnosti (Level of assurance)

- **Nízká**
- **Střední**
- **Vysoká**

eidentita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM

Bezpečnostní úroveň prokázání elektronické identity

- Prostředky dle úrovně důvěryhodnosti:
  - Low - např.: login + heslo
  - Substantional - dvoufaktorová autentizace = potvrzovací SMS, OTP = One Time Password
  - High (čipová karta, elektronický občanský průkaz)

Prostředky prokazování identity

- **Hesla**
- **Tokeny**
- **Karty**
- **Biometrika**
- **Mobilní telefony**

O vydávání těchto prostředků a vlastní ověřování přístupů se stará

- **A) Poskytovatel cílové služby**

- **B) Dle NIA konceptu „Identity provider“ Poskytovatel identitních prostředků**

Poskytovatel identitních prostředků

- **Stát**
  - **Elektronický občanský průkaz od 1. 7. 2018**
  - **Heslo + jednorázový SMS kód**

- **Soukromý poskytovatel**
  - **Běží certifikace**

Český E-government

- Datové schránky
- Základní registry
- Elektronický občanský průkaz
- Portál občana

Datové schránky

- V komunikaci se státní správou lze použít ke stejnému účelu jako elektronický podpis
- Zřízení a komunikace se státní správou zdarma
- Není omezena platnost jako u certifikátů
- Uchovává dokumenty pouze 90 dnů
- Funguje jako „webový email“, místo emailové adresy je kód datové schránky
- Komunikace mimo orgány státní moci je zpoplatněna
- Zřízení na poště, jednoduchý formulář a OP

Základní registry

- ROB – registr obyvatel
  - Propojené s evidencí obyvatel a cizinců
  - Omezený přístup
- ROS – registr osob (podnikatelských)
- RUIAN – Registr územní identifikace, adres a nemovitostí

- Rodné číslo x AIFO (agendový identifikátor fyzické osoby)
  - Různá identifikace občana v různých agendách

Elektronický občanský průkaz

- Vydávaný od 1.7. 2018
- Kontaktní technologie
- Umožňuje přihlášení k elektronickým službám státu
- Nutná aktivace na úřadu
- Umožňuje nahrát podpisový certifikát
- Potřebujete čtečku karet (v notebooku či externí)
- Přístupové kódy (PIN)
  - BOK, IOK, DOK, PIN, PUK, QPIN

Portál občana

- https://obcan.portal.gov.cz
- Přihlášení přes eOP nebo datovou schránku
- Postupný náběh služeb
- Přehled dokladů
- e-Recept

MUNI MED

Institut biostatistiky a analýz

Elektronické zdravotnictví

Národní registr zdravotnických pracovníků

- Dle zákona 372/2011 Sb.
- Lékařští i nelékařští pracovníci
- Záznam zakládá vzdělavatel automaticky po ukončení vzdělání
  - Základní obor, specializace, certifikační kurzy
- Registrace zaměstnanců zaměstnavatelem (poskytovatelem zdravotních služeb)
- **Pracovník** = nahlíží, doplňuje kontaktní údaje, pořizuje výpis
  - http://www.uzis.cz/node/7131
  - http://www.uzis.cz/registry-nzis-vstup
- **Poskytovatel** – povinnost registrovat zaměstnané zdravotnické pracovníky

E-recept

- Centrální úložiště receptů
- Probíhá ztotožňování pacientů oproti ROB (není nutné)
- Kolem 5 mil. e-receptů měsíčně
- Serverový certifikát (za poskytovatele = za IČ)
- Uznávaný elektronický podpis (lékař)
- Login a heslo lékaře, lékárníka
- https://www.epreskripce.cz/

Výměna klinických dat v ČR

- Typy komunikace
  - Mezi informačními systémy v rámci zařízení
  - Mezi zdravotnickými zařízeními (ZZ)
    - Obrazová data
      - PACS, DICOM
    - Klinická data
      - Kraj Vysočina, MEDICAL NET (CGM), MISE (STAPRO), E-zpráva
  - Mezi ZZ a pojišťovnami
    - K-Dávky
    - Portály zdravotních pojišťoven (komerční certifikáty)
  - Mezi ZZ a státní správou
    - EREG
      - Statistická zjišťování
      - Národní registry

Struktura dat

- Laboratorní data
  - NČLP – Národní číselník laboratorních položek
  - Dělení: Systém (krev), komponenta(ERY), druh veličiny(počet), jednotka, procedura(FLOWCYT)
- Léky
  - Kód SÚKL - odpovídá kódu v číselníku VZP
    - 7místné číslo
    - Konkrétní výrobek
    - 0046224 – Panadol - POR TBL FLM 24X500MG
    - http://www.sukl.cz/modules/medication/search.php
  - ATC klasifikace
    - Účinná látka
    - Anatomicko-terapeuticko-chemické skupiny
    - Hierarchické uspořádání kódu
    - N02BE01 - Paracetamol (N Nervový systém)
    - L01BC02 - Fluorouracil (L **Cytostatika a imunomodulační léčiva)**
    - www.whocc.no, http://www.sukl.cz/modules/medication/atc_tree.php

Struktura dat

- Plátci zdravotní péče
  - Standard VZP (K Dávky)
  - Metodika pro pořizování a předávání dokladů VZP ČR
  - www.vzp.cz – Poskytovatelé
  - Číselníky
    - Číselník výkonů
    - HVLP – hromadně vyráběné léčivé přípravky
    - Zdravotní prostředky
    - MKN-10 – Mezinárodní klasifikace nemocí verze 10

MKN 10

- Český překlad ICD – 10
- International Statistical Classification of Diseases and Related Health Problems
- Cca 14 tis. položek
- Hierarchická struktura kódu
  - Xnnn, Xnn – onemocnění
  - A, B – Infekční onemocnění
  - C – zhoubné nádory
    C50 karcinom prsu
    C502 karcinom prsu - horní vnitř.kvadrant prsu
- http://www.uzis.cz/cz/mkn/index.html

Klasifikace v onkologii

- Klasifikace MKN – O
  - Aktuálně verze 3
  - Překlad mezinárodní klasifikace ICD - O
  - Morfologický kód

    M - 8140/ 3 1

    histologie/chování (grade)
  - Topografický kód

    C50.2 Horní vnitřní kvadrant prsu
- TNM klasifikace
  - Rozsah nádorového onemocnění

    T – velikost vlastního tumoru (T1 až T4)

    N – postižení sousedících lymfatických uzlin (N0 – N3)

    M – metastatické postižení (M0/M1)

DASTA

- Datové rozhraní
  - DASTA
    - Datový standard MZČR
    - Český standard budovaný „ze zdola“
    - http://www.dastacr.cz/
    - Svázán s NČLP
    - Zaštiťuje ČSZIVI ČLS JEP
    - Nejen formát dat, ale oboustranná komunikace

DASTA verze 3

- Umožňuje přenos
  - identifikační data pacienta
  - základní informace o pacientovi (nacionále, r.č., adresy, výška, hmotnost atd.)
  - urgentní informace (alergie, dg.)
  - platební vztahy, pojišťovny, pracovní neschopnosti
  - anamnéza
  - léky
  - očkování
  - dg. trvalé a aktuální
  - **Laboratorní vyšetření**

DASTA verze 4

- Klinické události
  - RDG vyšetření (RTG, CT, SONO…)
  - EKG vyšetření
  - Příjem pacienta
  - Operační zpráva
  - Konzilium
  - Dekurz
  - Propouštěcí zpráva
  - Ambulantní zpráva
  - Výpis zpráv z archivu

DASTA - omezení

- Rozhraní není závazné
- Firemní mutace
- Firemní bloky
- Položky mimo NČLP
- Neexistuje přehled o skutečném využívání
- Národní specifikum bez vazby na mezinárodní standardy
- Neřeší vlastní přenos dat
- Neřeší zabezpečení

HL7

- Health level 7
- Celosvětové rozšíření
- Centrum v USA
  - www.hl7.org
- Pobočky v jednotlivých zemích
  - www.hl7.cz
- „Fabrika“ na standardy komunikace ve zdravotnictví
- V České republice omezené rozšíření

CDA

- Clinical document architecture
  - Aplikace HL7
  - Formalizovaný klinický dokument (lékařské zprávy)
  - 3 úrovně formalizace
    - Formalizovaná hlavička + nestrukturovaný text
    - Hlavička + rozčleněný text do bloků
    - Plně strukturovaný strojově zpracovatelný obsah
  - Pro konkrétní dokumenty připraveny CDA šablony (templates)
  - Aplikováno např. v Rakousku, Polsku

SNOMED

- Klinická terminologie
- Spravován International Health Terminology Standards Development Organisation (IHTSDO)
- Nejen termíny, ale hlavně vazby
- Multiosové uspořádání
- Základní jednotka = koncept
- Základní struktura
  - Koncept (Concept)
  - Popis (Description)
    FSN - **Fully Specified Name**
    Preferred Term
    Synonyms
  - Vazby (Relationship)

SNOMED

- Cca 300 tisíc konceptů
- **19 kořenových konceptů**
  - Observable entity (otázky)
  - Clinical finding (odpovědi)
  - Procedure
  - Body structure
  - Organism
  - Substance
  - Pharmaceutical products
  - Physical force
  - Physical object
  - ..
- **Název konceptu (**“semantic tag“**)**
- Fracture of foot (disorder)

Test

- V ISu:
- Student – vybrat předmět UPS – Odpovědníky
- Vybrat odpovědník Test UPS –
  - Chci sestavit první sadu otázek
  - Na konci „Uložit a vyhodnotit“
- 20 otázek
- 60 minut – Nelze přerušit
- 5 pokusů provedení hodnocení
- U některých je více správných odpovědí (každá za bod)
- Odečítání bodů za chybnou odpověď
- Minimum pro splnění je 15 bodů