Otázka 2 - Informační etika, šifrování

Petr Šťastný

2019-09-21

Otázka 2 - Informační etika, šifrování

Ergonomie a hygiena práce s PC

Informační etika

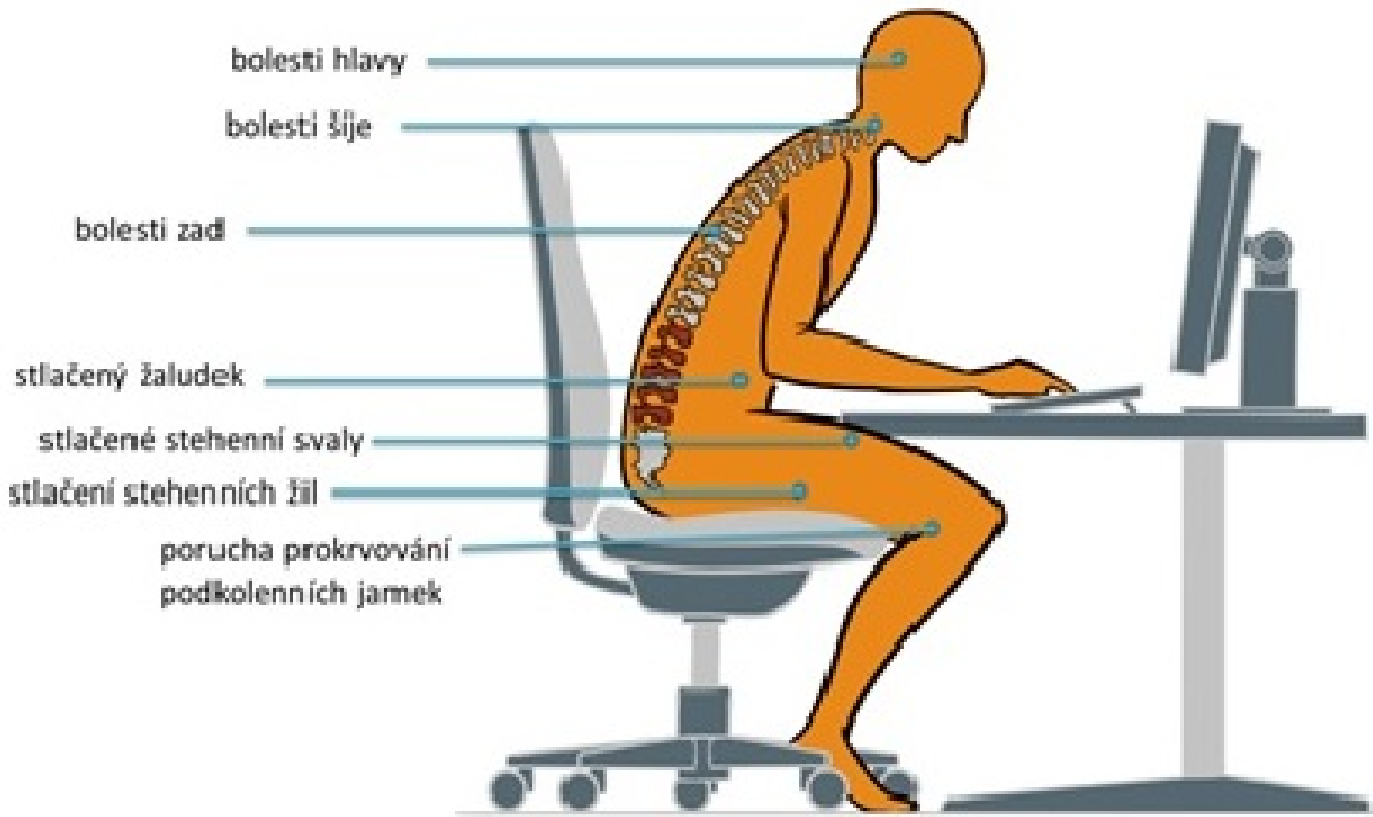
Licence, DRM

Bezpečnost komunikace, kyberšikana

Šifrování

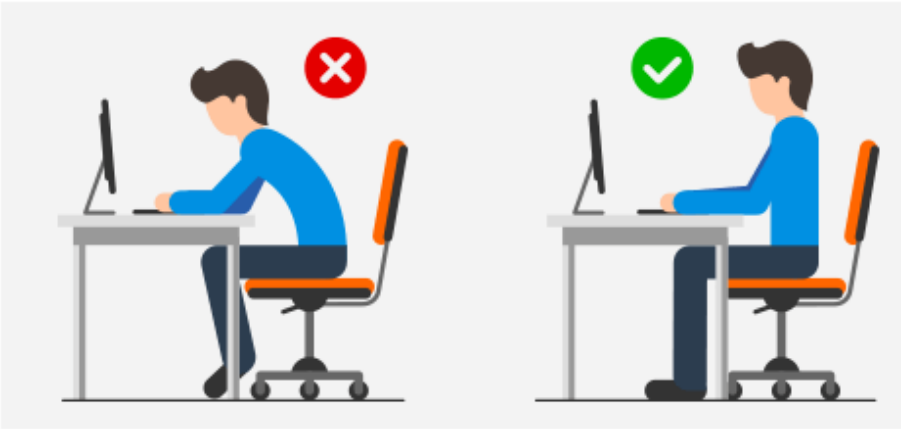
Hygiena práce s PC

- Bolest páteře
- Bolest zad
- Bolest zápěstí
- Bolest očí

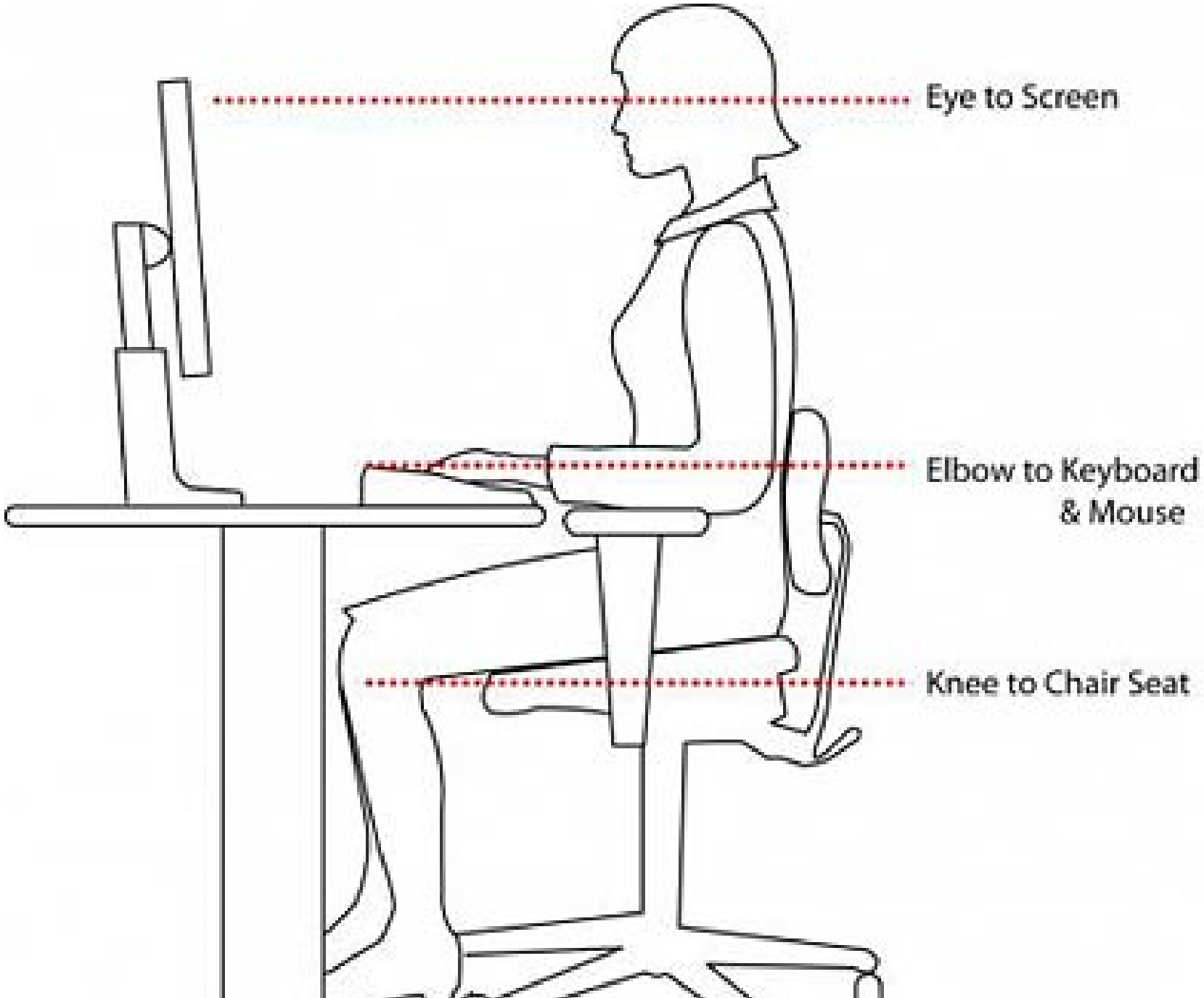


Základní pravidla

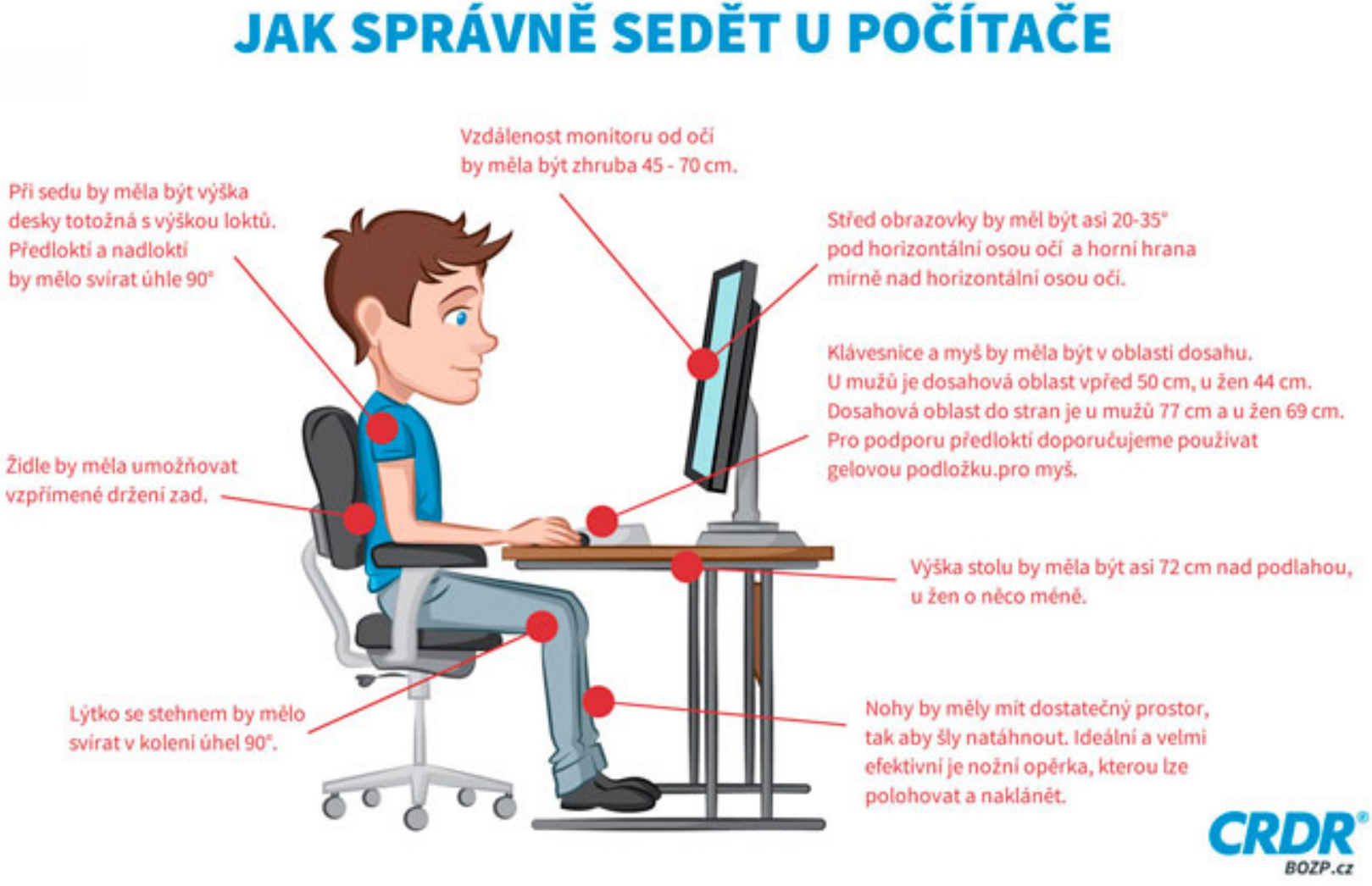
- Horní část monitoru ve výši očí
- Monitor vzdálený min. 30cm (ideálně 60-100cm)
- Rozmístění monitorů a programů rovnoměrně
- Pro notebook - stojan, aby byla obrazovka ve výši očí
- Výška židle - mezi stehnem a lýtkem pravý úhel
- Podložka pro myš nebo klávesnici, aby ruce byly v jedné rovině
- Vertikální myš pro úlevu zápěstí
- Podložka pro nohy



Sezení



Sezení


JAK SPRÁVNĚ SEDĚT U POČÍTAČE
Vzdálenost monitoru od očí
by měla být zhruba 45 - 70 cm.
Při sedu by měla být výška
desky totožná s výškou loktů.
Předloktí a nadlokti
by mělo svírat úhle 90°
Střed obrazovky by měl být asi 20-35°
pod horizontální osou očí a horní hrana
mírně nad horizontální osou očí.
Klávesnice a myš by měla být v oblasti dosahu.
U mužů je dosahová oblast vpřed 50 cm, u žen 44 cm.
Dosahová oblast do stran je u mužů 77 cm a u žen 69 cm.
Pro podporu předloktí doporučujeme používat
gelovou podložku.pro myš.
Židle by měla umožňovat
vzpřímené držení zad.
Výška stolu by měla být asi 72 cm nad podlahou,
u žen o něco méně.
Lýtko se stehnem by mělo
svírat v koleni úhel 90°.
Nohy by měly mít dostatečný prostor,
tak aby šly natáhnout. Ideální a velmi
efektivní je nožní opěrka, kterou lze
polohovat a naklánět.
CRDR
BOZP.cz

Informační etika

- Etika = jak se správně chovat
- Vědecké práce, knihovnictví, novinařina
- Získávání/tvorba/šíření informací
- Nepoužívejte obrázky co nejsou vaše (nebo pod vhodnou licencí)
- To samé platí o hudbě a podobných zdrojích
- Když vaší aplikaci člověk svěřuje informace - neprodávejte je
- Vše co vaše aplikace dělá s osobními údaji napsat do privacy policy
- Stahování pro vlastní potřebu - a P2P (torrent)

Licence, DRM

- Licence - definuje možnost zacházení s produktem
- SW - MIT, GNU GPLv3, Apache 2, WTFPL
- Data, media - CC-BY, CC0, CC-BY-SA
- Fonty - SIL Open Font License
- ChooseALicense.com

- DRM - Digital Right Management (Defective by Design)
- Technologie co zamyká možnosti jak pracovat s daty
- eKnihy nejdou kopírovat
- Hudba nejde přehrávat mezi zařízeními
- Filmy z Netflixu nejdou stahovat

Bezpečnost komunikace

- Všude šifrovat! - na webu protokol https
- Další šifrované varianty protokolů: sftp, ssh
- Adblocky, blokátory trackerů - uBlock Origin, uMatrix
- Prohlížeč co poskytuje dostatečnou ochranu - Firefox
- Blokace na síťové úrovni - PiHole
- Používat aktualizovaný SW - ať už FOSS nebo placený
- Citlivé emaily šifrovat (Thunderbird, Enigma)
- Soubory na cloudu šifrovat (GPG)
- Citlivá data na počítači? Full disk encryption (dm-crypt, eCryptfs)
- Případně jednotlivé soubory pomocí GPG

Kyberšikana

- Šikana prostřednictvím elektronických médií - internet, telefon
- Kyberstalking - pronásledování (FB)
- Kyberharašení - opakované zasílání nepříjemných zpráv
- Ostrakizace - vyloučení z (např. FB) skupiny
- Flaming - nepřátelské chování ve virtuálním světě

Šifrování

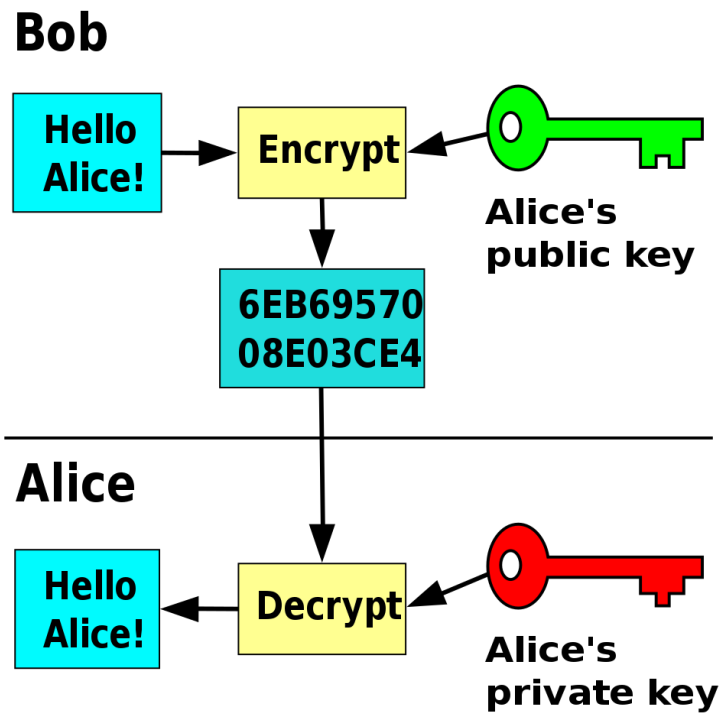
- 2 druhy: symetrický klíč, public/private klíč
- Užití: tajná komunikace
- Užití: potvrzení autenticity informací
- Užití: elektronický podpis (smlouvy, ...)

Symetrické šifrování

- Klíč pro šifrování/dešifrování stejný
- Password manager: heslo
- Šifrování disku
- Enigma
- Alg: AES, Blowfish
- Bezpečný klíč: fráze

Asymetrické šifrování

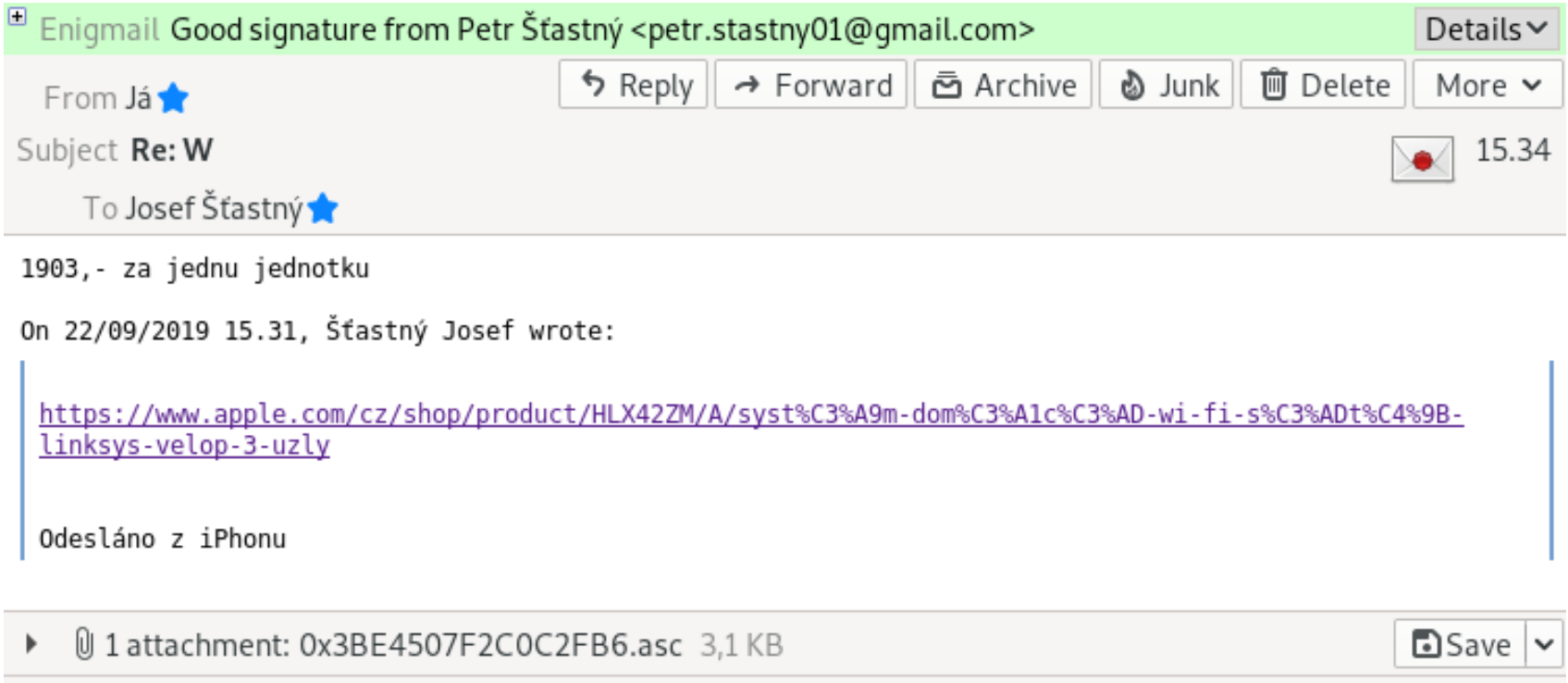
- Uživatel si vygeneruje dva klíče - veřejný a soukromý
- Veřejný vydá ostatním. Jde použít jenom k zašifrování zprávy.
- Soukromý si nechá. Jde použít jenom k rozšifrování zprávy.
- Každý může odeslat zašifrovanou zprávu, ale nikdo si ji nepřečte



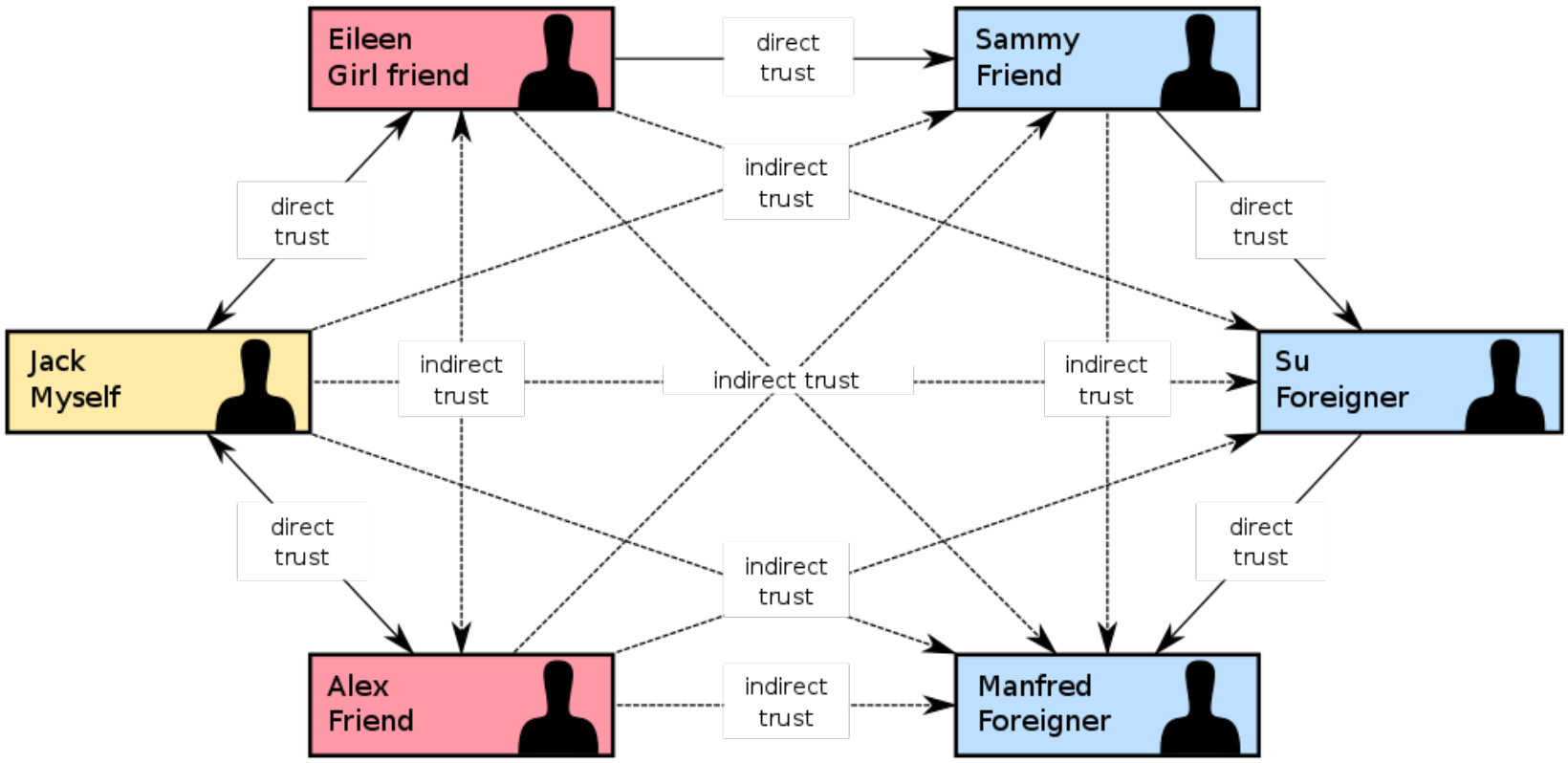
Elektronický podpis

- Pomocí soukromého klíče označíme data (dokument)
- Každý může pomocí veřejného klíče ověřit, že data nebyla změněna
- Pokud se data změní, podpis se stane nevalidní
- Může nahradit fyzický podpis např. na smlouvách
- Používá se k důkazu toho, že zpráva pochází ode mě
- Mohu podepsat email, a tím dokázat, že s ním nebylo manipulováno
- PGP / GPG - Thunderbird (Enigma)

Enigmail


Enigmail Good signature from Petr Šťastný <petr.stastny01@gmail.com>
Details
Reply
Forward
Archive
Junk
Delete
More
From Já
Subject Re: W
15.34
To Josef Šťastný
1903,- za jednu jednotku
On 22/09/2019 15.31, Šťastný Josef wrote:
https://www.apple.com/cz/shop/product/HLX42ZM/A/syst%C3%A9m-dom%C3%A1c%C3%AD-wi-fi-s%C3%ADt%C4%9B-linksys-velop-3-uzly
Odesláno z iPhonu
1 attachment: 0x3BE4507F2C0C2FB6.asc 3,1 KB
Save

Web of trust


Eileen
Girl friend
direct
trust
Sammy
Friend
indirect
trust
direct
trust
direct
trust
Jack
Myself
indirect
trust
indirect trust
indirect
trust
Su
Foreigner
direct
trust
indirect
trust
direct
trust
Alex
Friend
indirect
trust
Manfred
Foreigner

Zdroje

- Ergonomie a hygiena používání PC: interní wiki Alza.cz
- Informační etika: wikisofia.cz/wiki/Informační_etika
- Wen: Information ethics
- Lincence: ChooseALicense.com
- Wen: Digital rights management
- GPG manpage
- Wcz: Kyberšikana
- Wen: Web of Trust
- Wen: Public key encryption