Elektronický podpis: od návrhu zákona k realite

Ing. Radovan Semančík

BUSINESS @GLOBAL SYSTEMS, a.s.

BGS

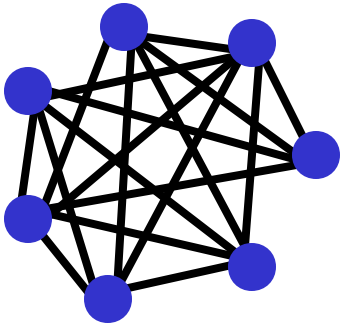
Obsah

- Úvod
- Základy PKI
- PKI v praxi
- Budúcnosť
- Záver

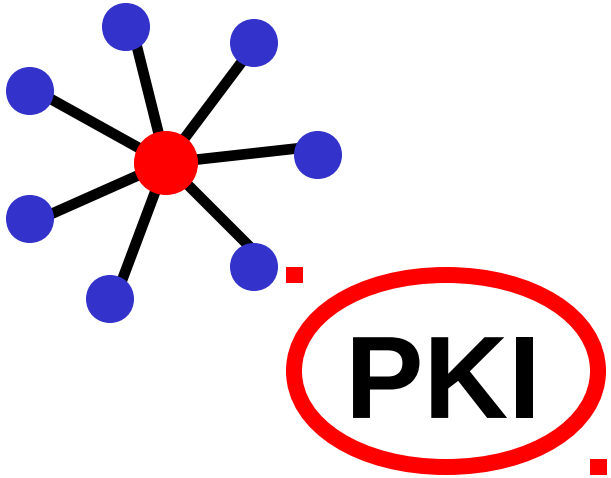
Úvod

- eCommerce, eBusiness, eGovernment, eČokoľvek
- Internetové aplikácie, mail, ...
- Bezpečnosť? na internete?
- Distribuované aplikácie = zložitá správa bezpečnosti
- PKI = public key infrastructure

Úvod - PKI



- Heslá - tradícia
- Symetrické šifry
- n(n-1)/2 spojení

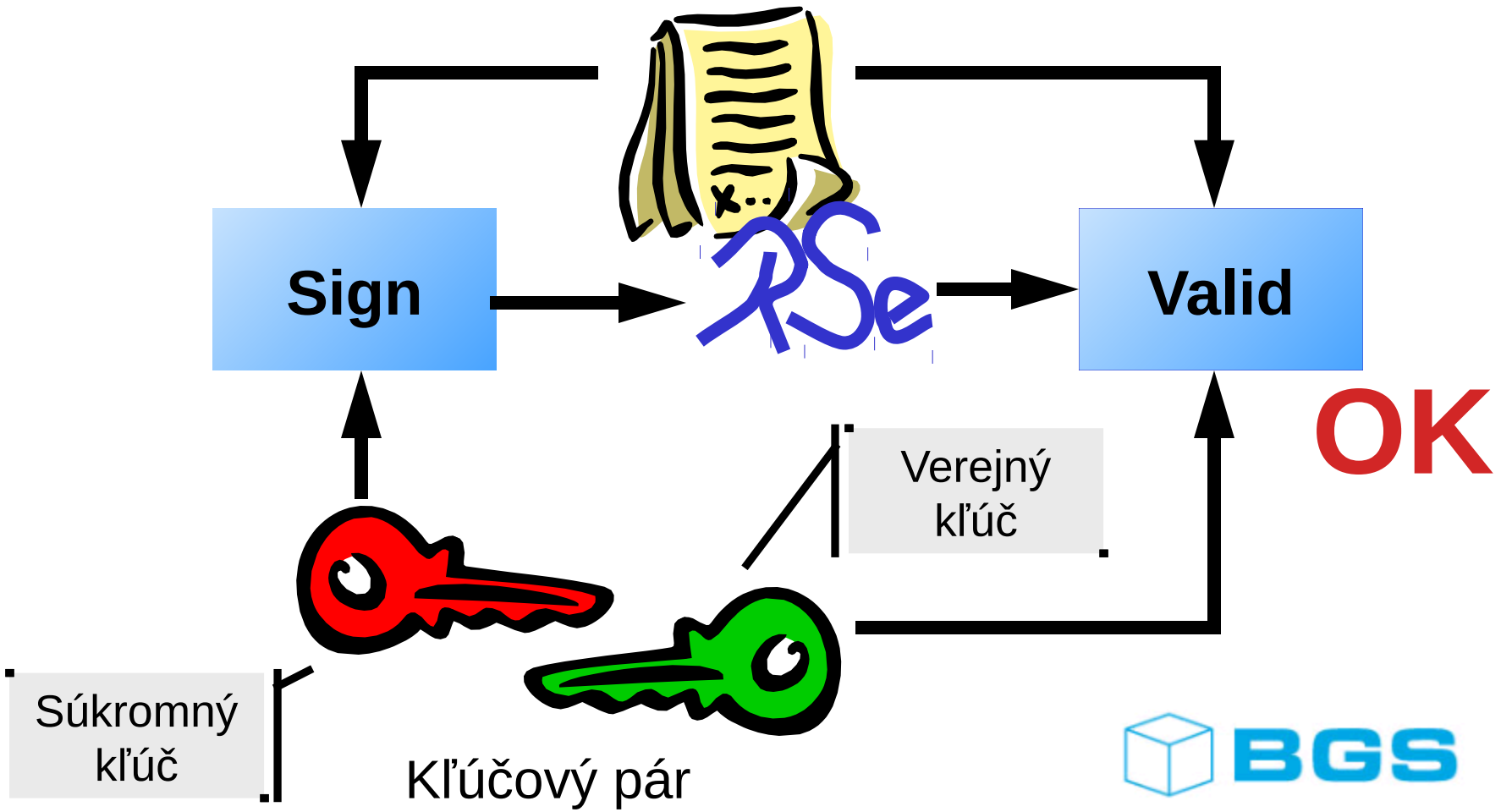


- Centralizácia
- Dôveryhodná tretia strana
- n spojení

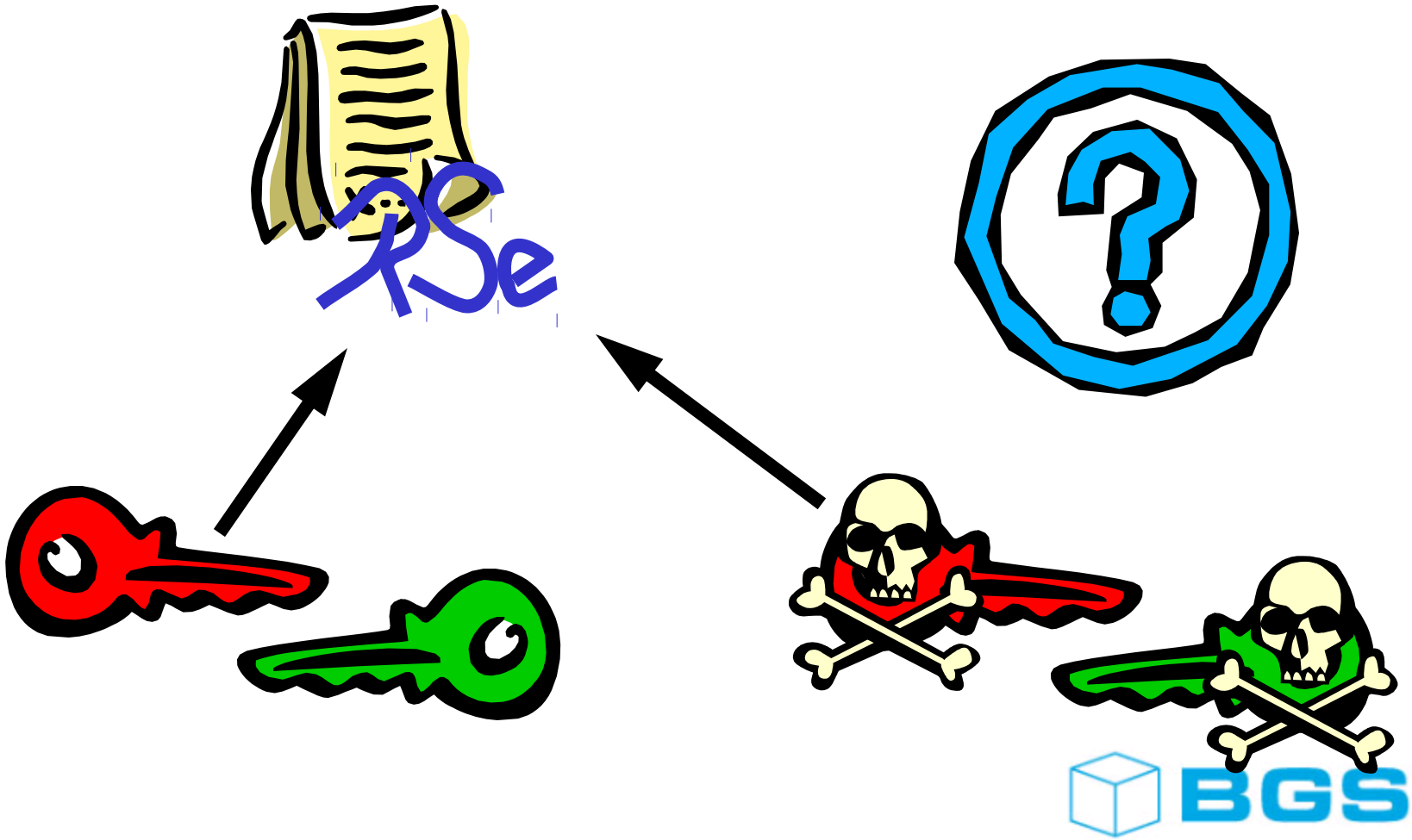
Obsah

- Úvod
- Základy PKI
  - Elektronický podpis
  - Certifikačná autorita
  - Štruktúra
- PKI v praxi
- Budúcnosť
- Záver

Elektronický podpis

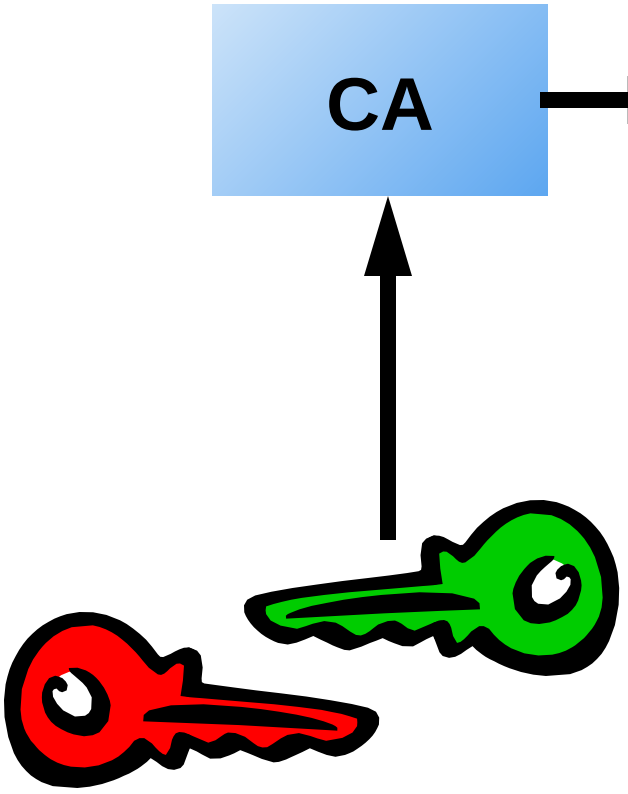


Identita



Certifikát

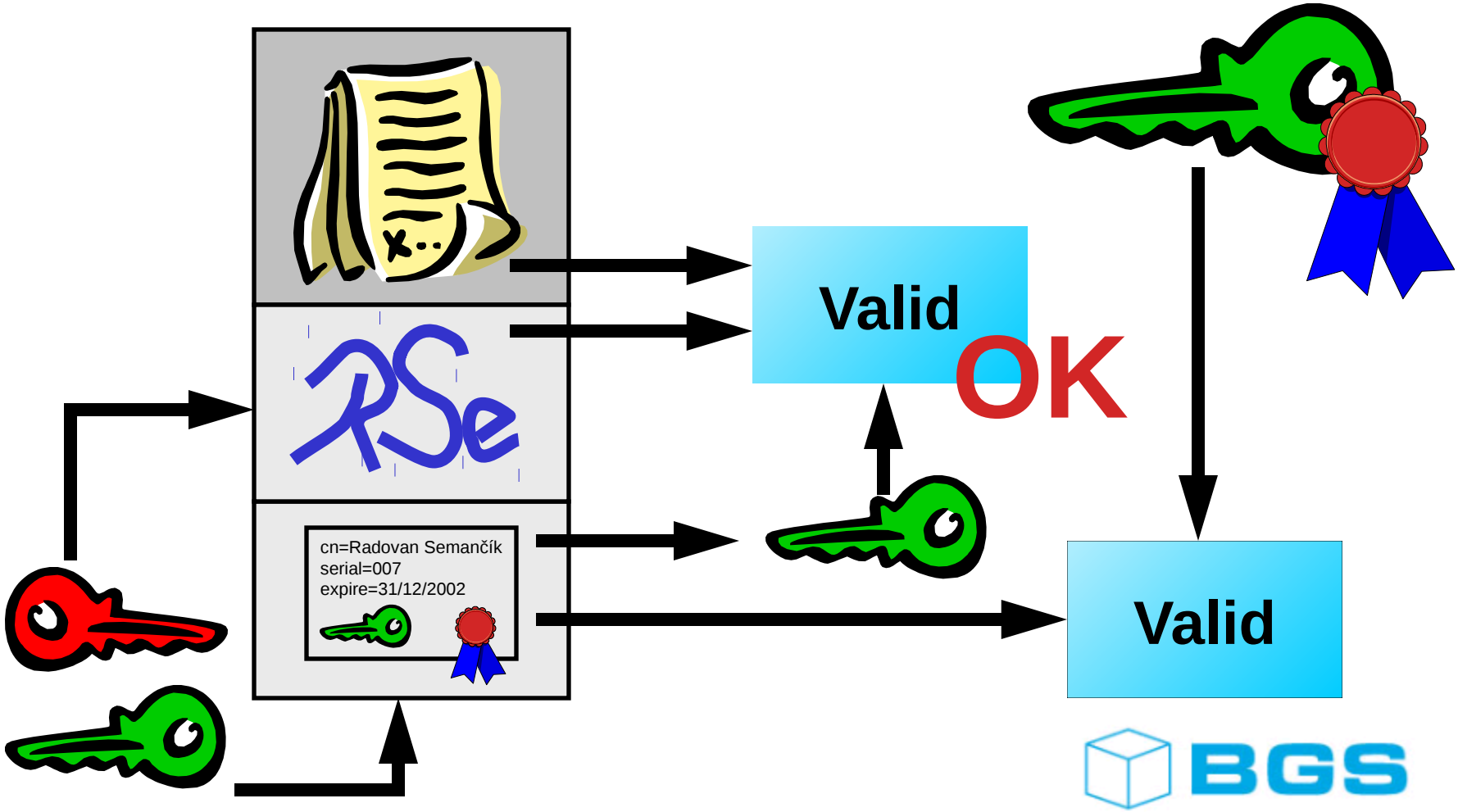
“Dôveryhodná tretia strana”



X.509

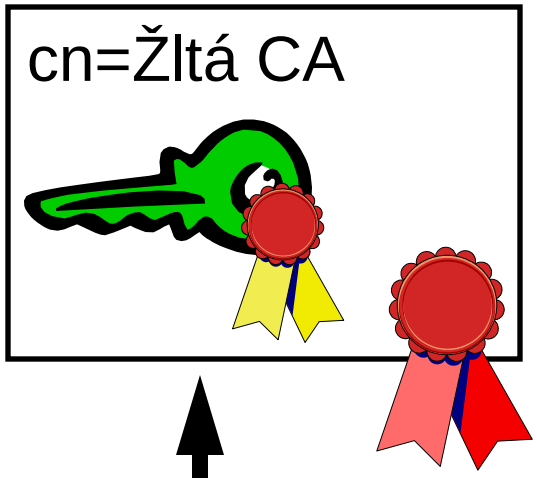
BGS

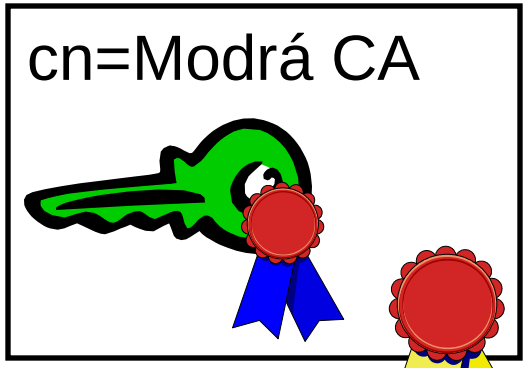
Overovanie certifikátu



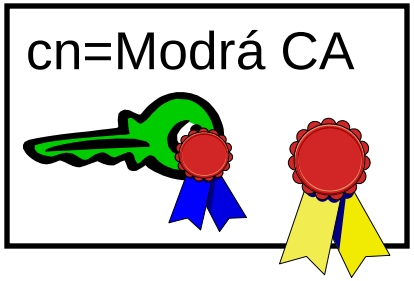
Hierarchia CA

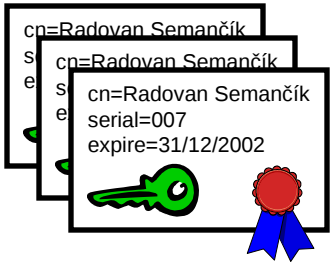
- Veríme …
- Preveríme!

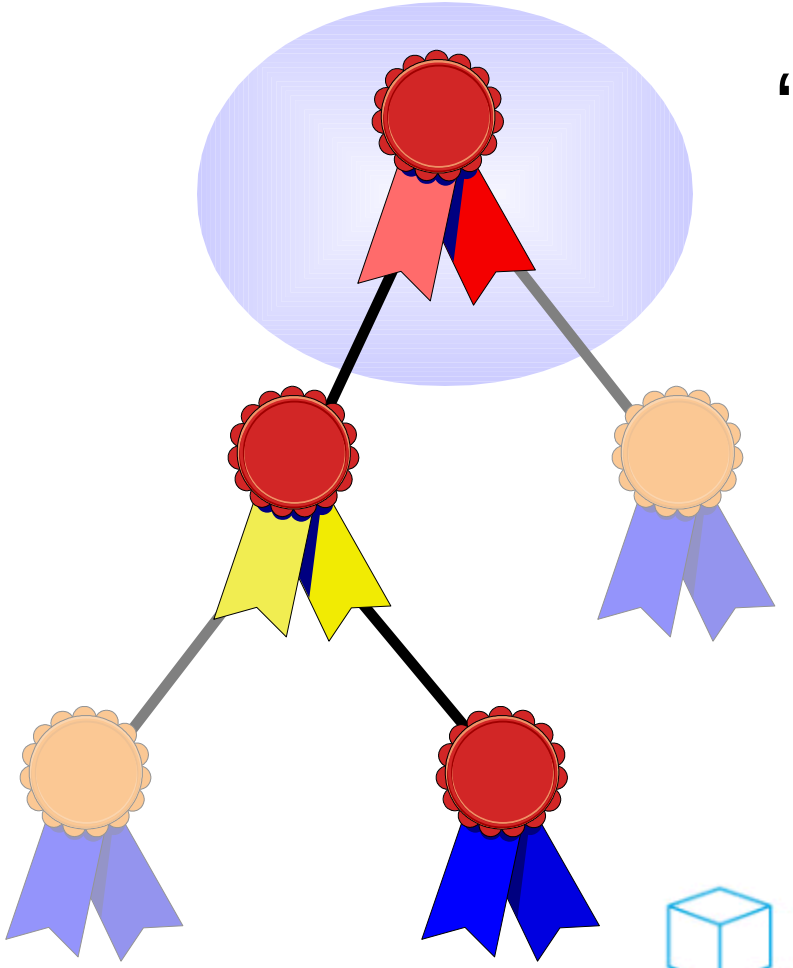




Hierarchia CA



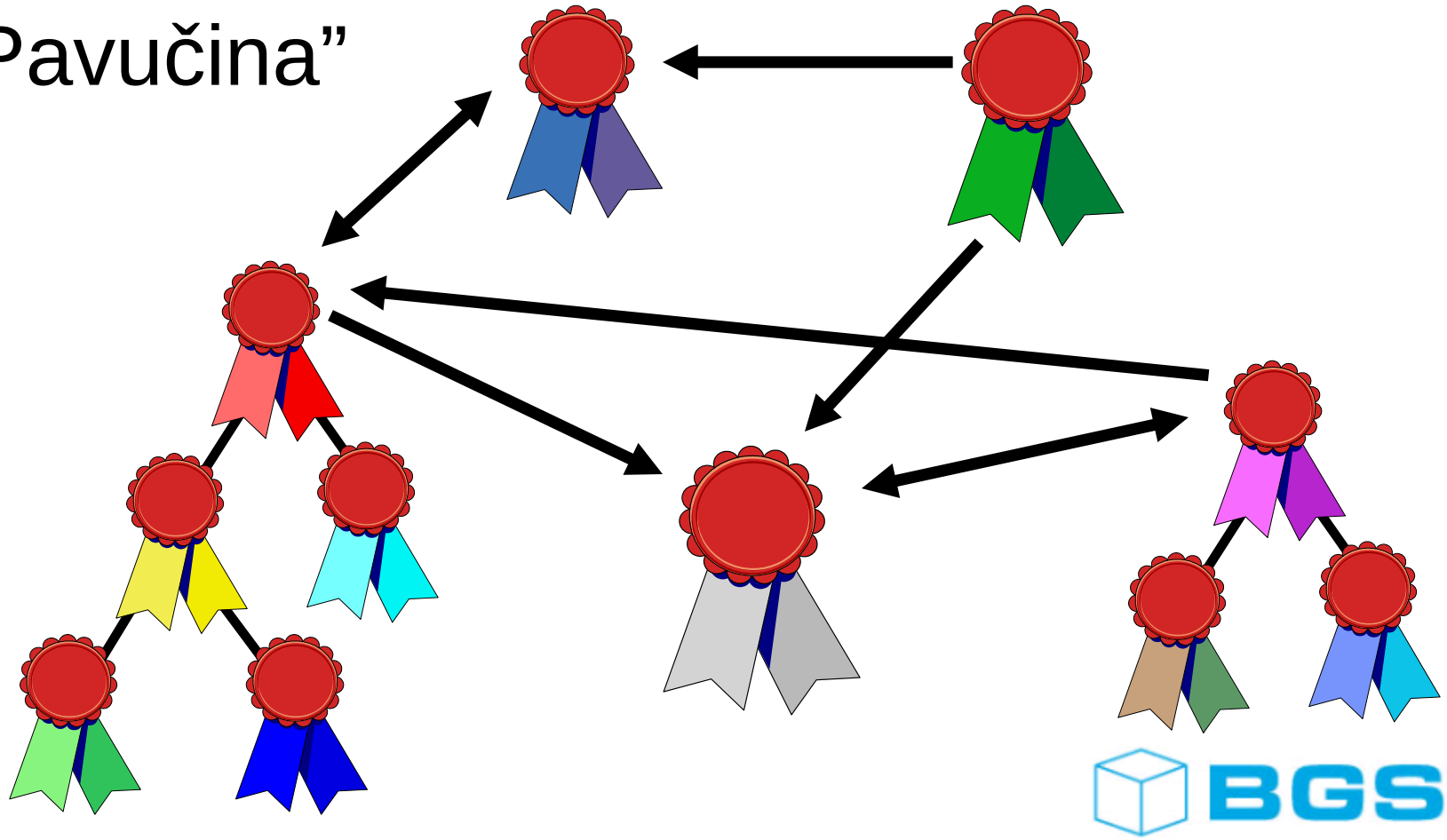




“Strom”

Krížová certifikácia

“Pavučina”

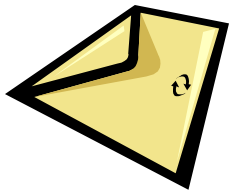


Strom vs Pavičina

- Strom
  - Dobre stanovená organizačná štruktúra
  - Podnikové prostredie, štátna správa, …
- Pavučina
  - Nejasná štruktúra, meniace sa podmienky
  - eBusiness, medzinárodné vzťahy, ...
- Realita: Hybrid

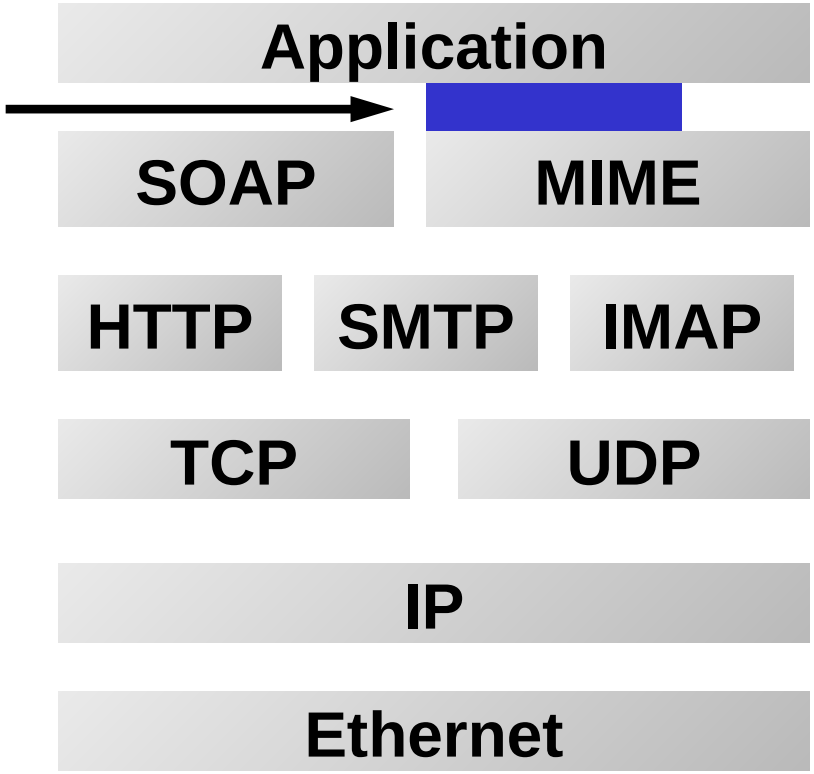
Obsah

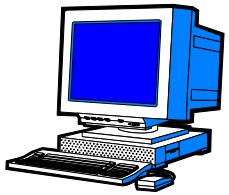
- Úvod
- Základy PKI
- PKI v praxi
  - S/MIME, TLS, IPsec
  - LDAP directory
- Budúcnosť
- Záver



X.509 PKI a S/MIME

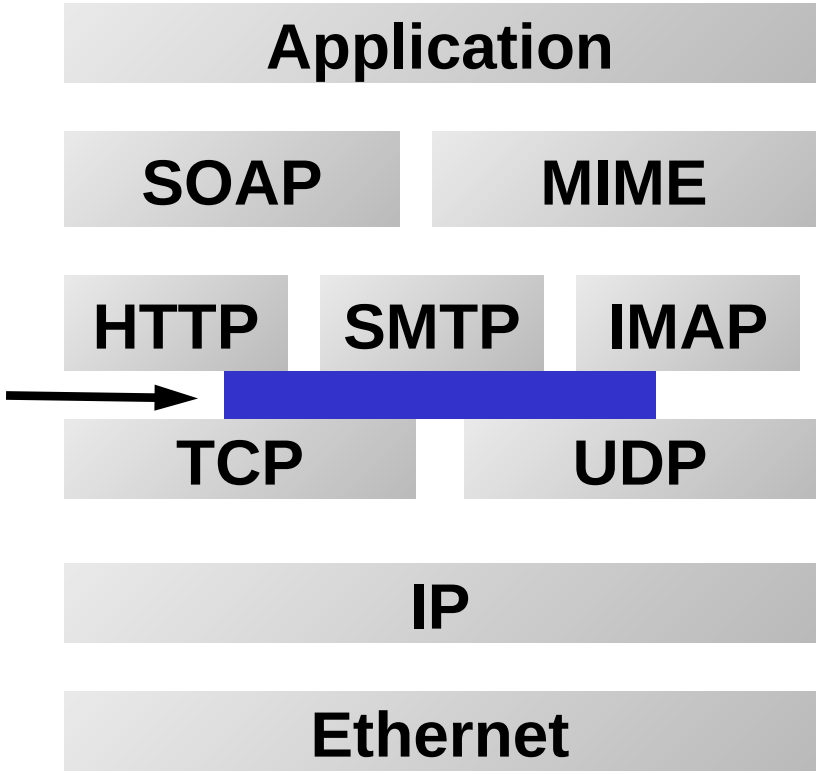
- **S/MIME** - Secure MIME
- Protokol pre zabezpečnenie e-mailu
- Podpisovanie a šifrovanie správ
- Vznik: RSA labs
- RFC2311, RFC2633, …
- Netscape, Outlook, ...

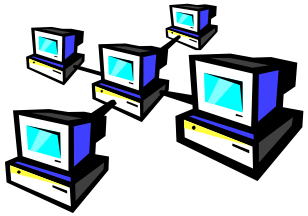




X.509 PKI a TLS

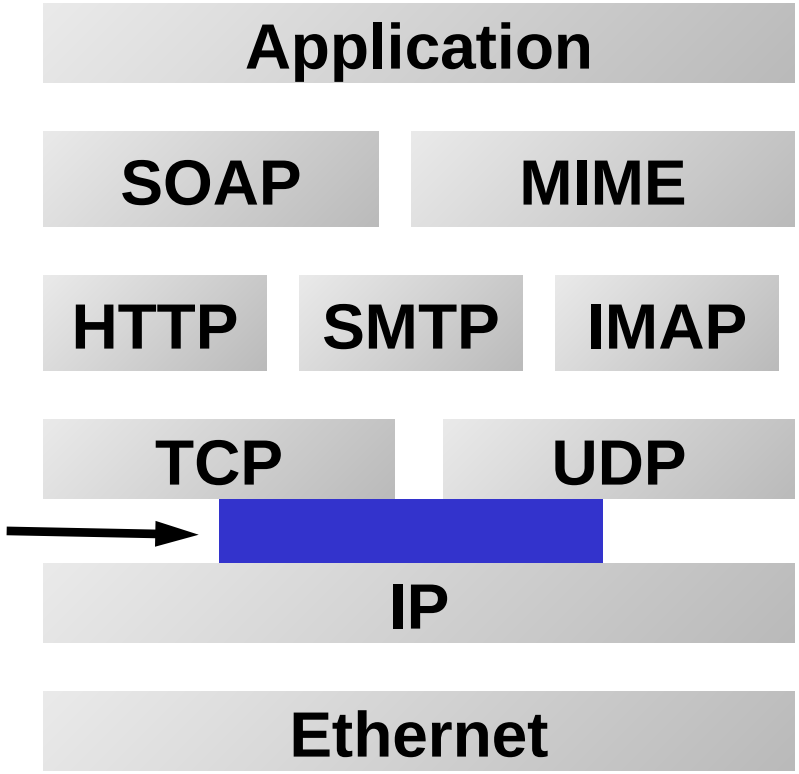
- **TLS** - Transport Layer Security
- Pôvodne SSL
- zabezpečenie transp. vrtsvy
- šifrovanie, autentifikácia
- najčastejšie HTTPS
- RFC2246
- Netscape, MSIE, Apache, ...





X.509 PKI a IPsec

- **IPsec** - IP Security
- Použitie pre VPN
- zabezpečenie sieťovej vrtsvy
- šifrovanie, autentifikácia
- RFC2401
- Sun, Cisco, Lucent, MS, ...

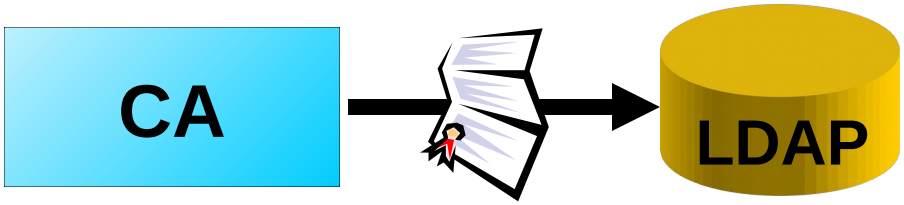


X.509 PKI a LDAP

- Meno v X.509 = LDAP (X.500) DN
  - Globálne meno, ľahko uložiteľné v LDAP

```
uid=semancik,ou=people,o=bgs,c=sk
```

- CA publikuje certifikáty a CRL do LDAP



- **LDAP je integrálnou súčasťou PKI**

Ďalšie služby CA

- Obnovovanie certifkátov
- Zneplatňovanie certifikátov
- CRL - Certificate Revocation List
  - Zoznam zneplatnených certifikátov
  - Vydáva CA pravideľne, aj občasne
- OCSP - Online Certificate Status Protocol
  - Okamžité zisťovanie stavu certifikátu

Obsah

- Úvod
- Základy PKI
- PKI v praxi
- Budúcnosť
  - Čo poskytne PKI?
  - Aplikácie
- Záver

Čo prinesie PKI?

- Silná autentifikácia
  - Už žiadne heslá. Nástup HTTPS, biometria, …
- Neodmientuteľnosť *(non-repudiation)*
  - Spoľahlivý elektronický podpis
  - potrebný timestamping, data certification
- Privátnosť údajov
  - Šifrovanie údajov, bezpečné pre všetkých
  - Key recovery

Aplikácie

- Smartcard, Token device = Nutnosť!
- Interperabilita = problém
- JavaCard standard
- Multi-application cards
  - Vstup do budovy + PKI + network login
  - Banking + PKI + loyalty
- eBusiness
  - globálny charakter PKI

Problémy

- Súčasné zavedené PKI = špeciálne PKI
  - Monolitická architektúra, málo prispôsobivé
  - Rôzne X.509 profily, malá interoperabilita
- Budúcnosť = všeobecné PKI
  - Modulárna architektúra, platformová nezávislosť
  - Štandardizácia (ITU-T, IETF, ISO, …)
- Nasadzovať PKI opatrne
  - Marketing je na škodu, ale odborníci pomôžu

Záver

- PKI je dnes výhoda, zajtra nutnosť
- Pozor na výber vhodných riešení
- PKI nie je samo o sebe riešenie, veľa treba prispôsobiť, integrovať

PKI = technológia + ľudia + procesy

Ďakujem za pozornosť

Ing. Radovan Semančík
<semancik@bgs.sk>