Princípy elektronického podpisu

Členovia pracovnej skupiny
Slovenskej informatickej spoločnosti pre prípravu zákona o elektronickom podpise
(http://www.informatika.sk/e-podpis/)

Ing. Vladimír Benček, CSc. • Ing. Pavol Frič, CSc., DITEC • Doc. JUDr. Daniela Gregušová, CSc., PF UK
Mgr. Jaroslav Janáček, MFF UK • RNDr. František Kaščák, AmoNet • Mgr. Ivan Kopáčik, CISA, Gordias
Ing. Emil Kršák, Žilinská univerzita • Ing. Július Lintner, DITEC • Ing. Rastislav Machel, CISSP, META Group CESE
Ing. Miroslav Milán, ICL Slovakia • Doc. RNDr. Daniel Olejár, CSc., MFF UK • RNDr. Igor Prívara, CSc.
Ing. Michal Sasinek • JUDr. Boris Susko, PF UK • Ing. Stanislav Valachovič, COLUMBEX International
RNDr. Jozef Vyskoč, PhD., CISA, VaF

Elektronický podpis

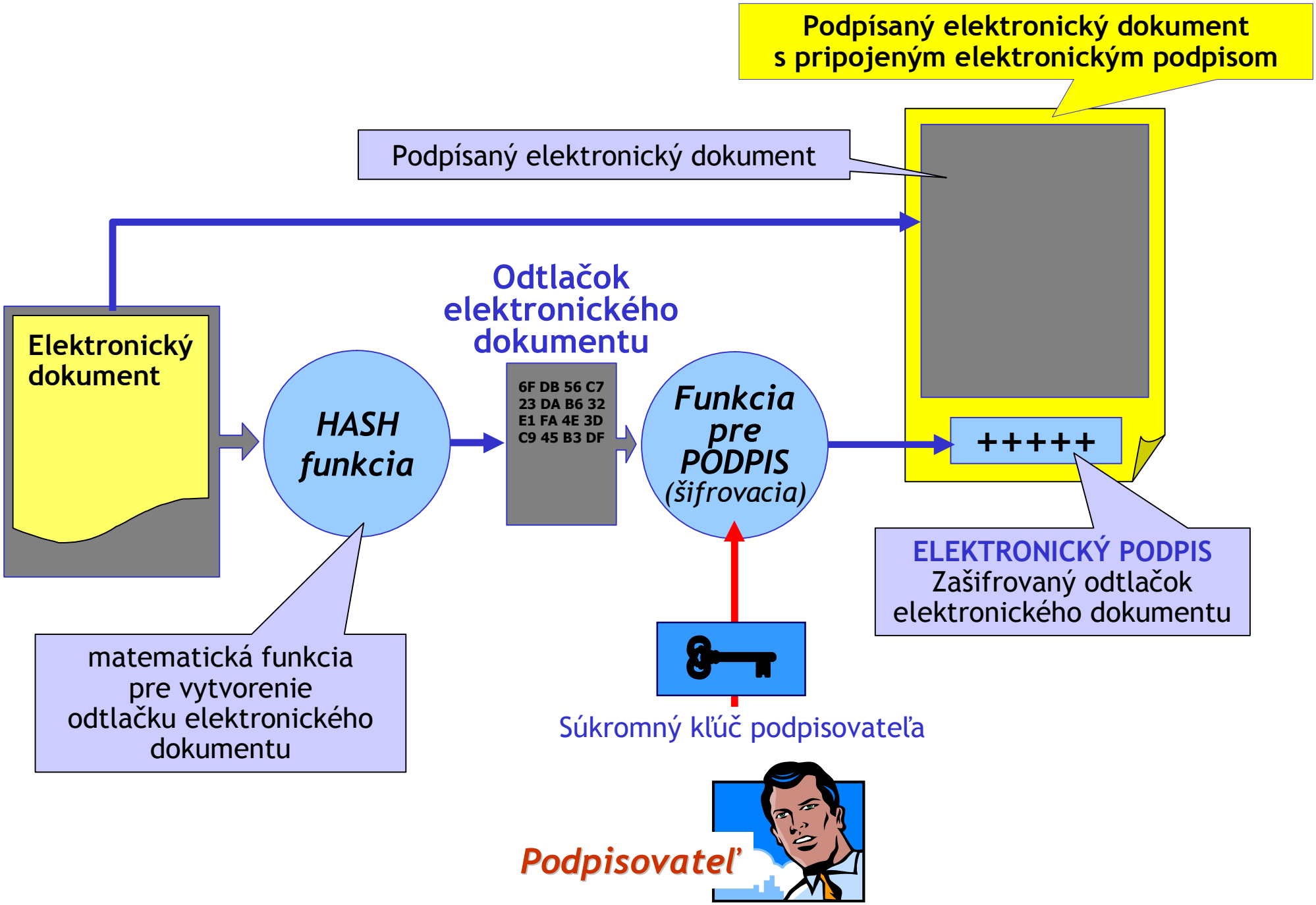
Čo je elektronický podpis?

- Metóda pre bezpečnú komunikáciu, s pomocou ktorej zabezpečujeme, že správa alebo súbor dát nebol nijakým spôsobom modifikovaný (bola zaistená integrita)
- V spojení s elektronickým certifikátom elektronický podpis potvrdzuje, že ide o správu z predpokladaného zdroja

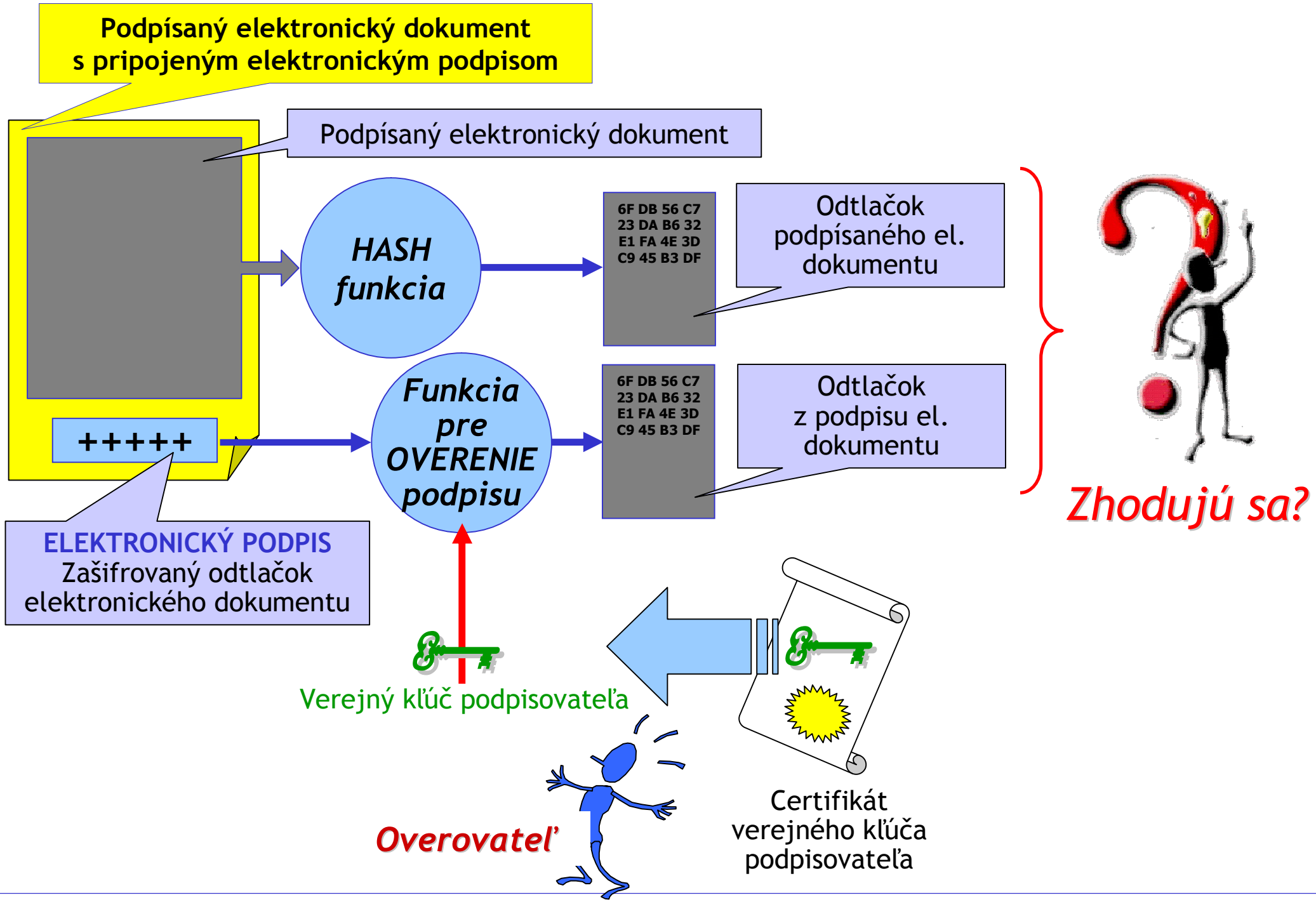
Výhody elektronického podpisu

- Je prakticky nemožné ho sfalšovať
- Relatívne jednoduché overenie pravosti elektronického podpisu
- Zaručuje neporušenosť (integritu) správy
- Nepopierateľnosť (nie je možné podpísať „bianco“ dokument, ktorého obsah by bol doplnený neskôr), t.j. podpísaná osoba nemôže poprieť, že by nebola zoznámená s obsahom podpísanej správy

Vytvorenie elektronického podpisu



Overenie elektronického podpisu

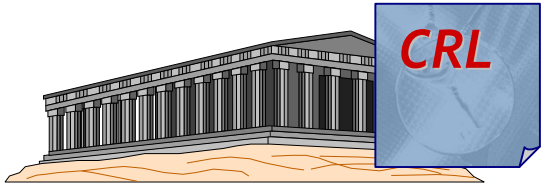


„Obyčajný“ a zaručený elektronický podpis

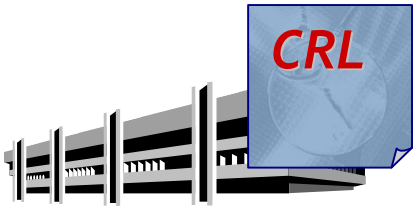
- **Prečo dva druhy elektronického podpisu?**
  - Rozdielne bezpečnostné požiadavky, rozdielne technické nároky a teda aj rozdielna cena
- **„obyčajný“ elektronický podpis**
  - Zabezpečuje **LEN** to, že podpísaný elektronický dokument **nebol zmenený** (t.j. zaistí, že prípadnú zmenu podpísaného elektronického dokumentu odhalíme)
  - Sám o sebe **NEDOKÁŽE SPOĽAHLIVO** určiť podpisovateľa
- **Zaručený elektronický podpis**
  - Zabezpečuje, že podpísaný elektronický **dokument nebol zmenený** a v spojení s **KVALIFIKOVANÝM certifikátom** (vydaným k verejnému kľúču podpisovateľa) **SPOĽAHLIVO určuje podpisovateľa**
  - Kvalifikovaný certifikát k verejnému kľúču podpisovateľa musí byť vydaný **akreditovanou certifikačnou autoritou**
  - Kvalifikovaný certifikát okrem iného **obsahuje tiež ohraničenia na použitie** tohto certifikátu (napr. že zaručený podpis s týmto certifikátom môže byť použitý len na úkony určitého druhu alebo na transakcie do určitej výšky)
  - Je ho možné vytvoriť **iba pomocou bezpečného zariadenia** na vytváranie elektronického podpisu (napr. využitím špeciálnej čipovej karty s mikroprocesorom)
  - Použitie zaručeného elektronického podpisu **nevyžaduje rozsiahle dokazovanie** pri overovaní podpisu a preukazovaní jeho pravosti

Čo potrebujeme pre využívanie elektronického podpisu

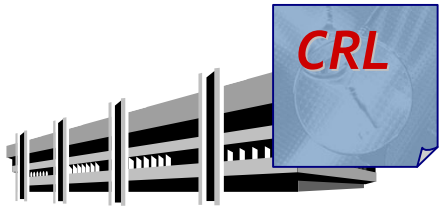
Zoznam zneplatnených certifikátov (Certificate Revocation List)



Úrad pre elektronický podpis



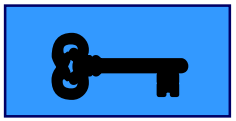
Certifikačná autorita



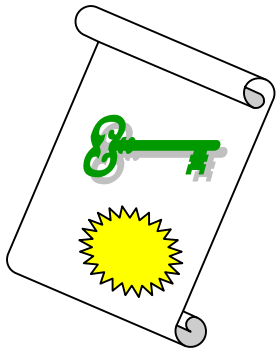
Akreditovaná certifikačná autorita

Registračná autorita

Podpisovateľ



Súkromný kľúč podpisovateľa



Certifikát verejného kľúča podpisovateľa

Overovateľ

Kvalifikovaný certifikát verejného kľúča podpisovateľa

Elektronický podpis a slovenská legislatíva

- **Smernica EÚ 1999/93/EC**
  - Povinnosť členských krajín do 19. Júla 2001 zosúladiť národnú legislatívu s jej požiadavkami/ustanoveniami
- **Potreba zapojenia sa Slovenska do medzinárodnej spolupráce**
  - Národná legislatíva, ktorá nie je v súlade so Smernicou 1999/93/EC môže byť vážnou prekážkou
- **Podmienky používania elektronického podpisu**
  - Prijatý zákon o elektronickom podpise (v súlade s EÚ)
  - Vydané potrebné vykonávacie predpisy (vyhlášky Úradu pre elektronický podpis)
  - Vytvorená potrebná technická infraštruktúra verejného kľúča (PKI)
- **Prečo bol prijatý poslanecký návrh zákona**
  - Je terminologicky jednoznačný
  - Je technologicky neutrálny a prakticky realizovateľný
    (upozorňujeme, že je zásadný rozdiel medzi technologickou neutralitou a vágnymi, nepresnými, pojmami vládneho návrhu zákona kamuflovanými ako „technologická neutralita“)
  - Je v súlade s existujúcimi ako aj pripravovanými zákonmi o e-podpise v iných krajinách (Rakúsko, Nemecko, Poľsko, ...)

Aspekty prijatého zákona o elektronickom podpise

- **Právny aspekt:**
  - Zavedenie elektronického podpisu do slovenského právneho poriadku, stanovenie podmienok, za ktorých je rovnocenný vlastnoručnému podpisu
  - Umožnenie zrovnoprávnenia elektronických dokumentov s dokumentmi papierovými

- **Praktický aspekt:**
  - Technologicky neutrálny - realizácia elektronického podpisu pomocou asymetrického šifrovania a digitálneho podpisu (dnes)
  - Zákon musí byť dostatočne všeobecný aby dovoľoval reagovať na budúci vývoj, ale súčasne technicky jednoznačný a presný aby nepripúšťal rozdielny výklad
  - Dôvera voči elektronickému podpisu založená na spoľahlivosti zariadení a metód
  - Stanovenie bezpečnostných požiadaviek na zariadenia pre elektronické podpisy
  - Popis procedúr, ktoré sa v súvislosti s elektronickým podpisom budú používať
  - Zohľadnenie medzinárodných technických noriem (o.i. formáty dokumentov, procedúry, bezpečnostné kritériá)
  - Potreby a možnosti Slovenska
  - e-obchod, e-government
  - Zlacnenie a zrýchlenie komunikácie s verejnou a štátnou správou, daňovými úradmi, …