

# Aktuální stav a perspektivy elektronického podpisu

Jiří Peterka

# otázka na úvod:

- **mají být zákony technologicky neutrální?**
  - dnes obecná odpověď: ano, *zákon nemá předepisovat konkrétní technologii* (technologické řešení)
- **ale: platí to i v případě elektronického podpisu?**

možnosti:

- **zákon se nebude ptát, jak technologie fungují**
  - ale vytvoří si určitou konstrukci a tu kodifikuje
  - teprve pak se bude hledat technologické řešení, které tuto konstrukci naplní
    - možná se ani nenajde
- **zákon bude vycházet z toho, jak konkrétní technologie fungují**
  - a bude kodifikovat to, jak má být daná technologie používána
    - aby byly naplněny další konkrétní požadavky
  - zákon bude vytvářet právní rámec pro konkrétní technologii

příklady technologií: PGP, digitální podpis na bázi asymetrické kryptografie a PKI, ....

# z historie el. podpisu v ČR:



- první návrh zákona o el. podpisu byl „technologicky neutrální“

*Jsou tady dvě cesty, kterými se dá jít:*

- *Jednou je téměř doslova přijmout legislativu EU. To je cesta, kterou chce jít vláda.*
- *Druhá cesta je vytvořit něco, co by bylo pro nás, jako nečlena EU, mnohem jednodušší a nebylo vázané přímo direktivu EU.*
- *To, co chce přejmout vláda, totiž direktivu EU, obsahuje přesné technické specifikace. V případě, že přijdou nové techniky identifikace - identifikace lidí z DNA či očních duhovek - direktiva se jednoduše změní. Náš zákon ale nikoliv.*
- *Proto my navrhujeme zákon, který by nepočítal s ničím technicky konkrétním. Byl by přesně pro situaci v ČR a přesně by ho vymezil až Úřad pro elektronický podpis.*

*poslanec Vladimír Mlynář, v interview pro MF Dnes, 22.12.1999*

# principiální představy „technologicky neutrální“ právní úpravy el. podpisu

## „jako známka“



- někdo mi vydá můj elektronický podpis
  - ten existuje „sám o sobě“
  - je specifický pro mne
  - a já ho pak opakovaně používám
    - „nalepím“ na dokument, tím podepíši
- zákon požaduje:
  - „*nakládat s elektronickým podpisem s náležitou péčí*“

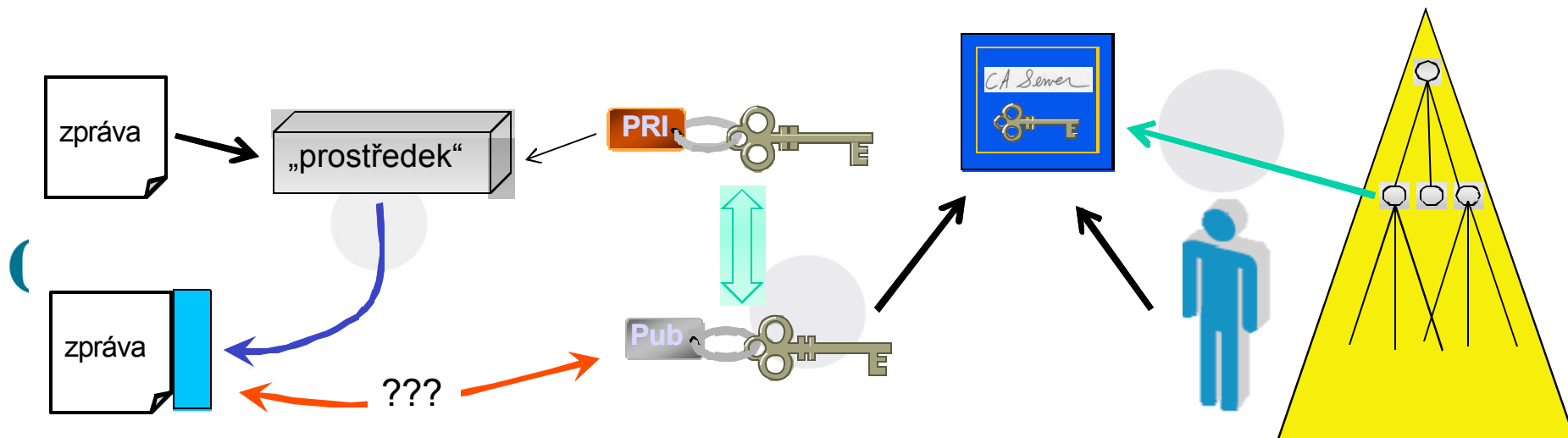
## „jako razítko“



- někdo mi vydá můj prostředek pro vytváření mých elektronických podpisů
  - prostředek existuje „sám o sobě“
  - je specifický pro mne
  - a já ho pak opakovaně používám
- zákon požaduje:
  - „*nakládat s elektronickým prostředkem s náležitou péčí*“

# historie a současnost

- „technologicky neutrální“ návrh zákona o el. podpisu prošel v lednu 2000 prvním čtením v PSP
  - ale před druhým čtením byl nahrazen „technologicky závislým“ zákonem, který vycházel ze směrnice 1999/93/EC z 30.11.1999
- dnes platný zákon o el. podpisu (č. 227/2000 Sb.) kodifikuje jeden konkrétní druh „elektronického podpisu“
  - a to „digitální podpis na bázi asymetrické kryptografie“, opírající se o infrastrukturu PKI



# a jaká je dnes realita?

- **názor: *princip (uzákoněného) elektronického podpisu nebyl širší veřejností (a mnohdy ani tou odbornou) dostatečně pochopen***
- **v médiích se ozývají hlasy:**
  - „*elektronický podpis neuspěl !!!*“
- **konstatují to i politici**
  - ministr vnitra Ivan Langer:  
„*nevyvolali jsme poptávku po el. podpisu*“
- **volá se po zjednodušení el. podpisu**
  - europoslankyně Zuzana Roithová na ISSS 2009: „*musí se zjednodušit ....*“
- **problém je i v osvětě:**
  - ta často propaguje elektronický podpis sice zjednodušeně (pro laiky),
    - ale věcně nesprávně!!!
  - ve smyslu technologicky neutrální varianty:
    - „**jako známka**“, či „**jako razítko**“
  - zájemci se nabízejí „**vydání jeho elektronického podpisu**“

Datoveschranky.info



**Kde si zřídím elektronický podpis?**

**V ČR jsou pouze tři certifikační autority, které vydávají e-podpisy.**

# co se povedlo a co se nepovedlo

## povedlo se:

- **zavést elektronické značky**

- vlastně: strojový elektronický podpis
  - umožňuje generovat různé výpisy z databází/rejstříků
  - například pro Czech Pointy

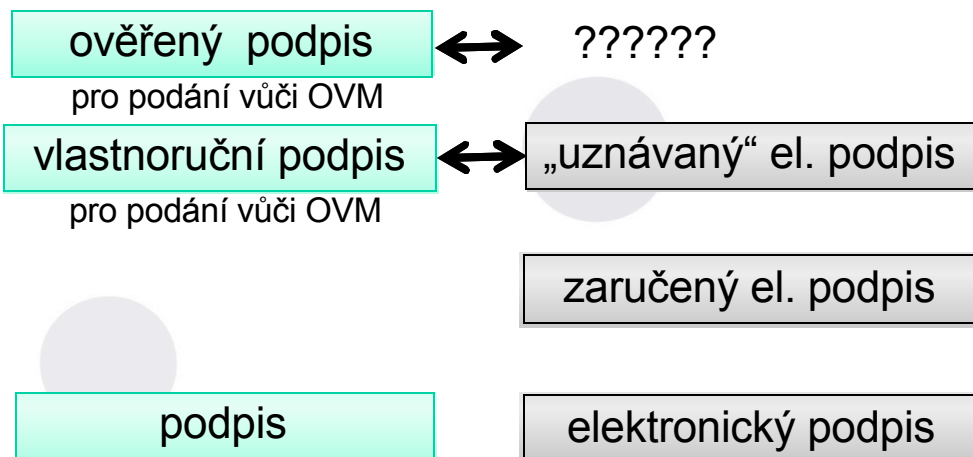
- **zavést časová razítka**

- samotný podpis neuvádí dobu svého vzniku
  - časové razítko garantuje, že podepsaný dokument existoval „někdy předtím“

## nepovedlo se:

- **najít elektronický ekvivalent pro (úředně, notářsky) ověřený podpis**

- „legalizaci“ vlastnoručního podpisu



# (pokus o) legalizaci elektronického podpisu

- byl proveden v prvním návrhu zákona o eGovernmentu, ještě z dílny eStátu
  - legalizace podpisu = jeho ověření notářem či jiným pověřeným orgánem
- u vlastnoručního podpisu na listině:
  - podepisující se dostaví před notáře, podepíše se před ním a notář to osvědčí
  - výsledek: ověřený podpis má větší „právní sílu“ než neověřený vlastnoruční podpis
- otázka:
  - má smysl vůbec smysl ověřovat elektronický podpis?
    - před kýmkoli?
    - když už jednu došlo k ověření před certifikační autoritou?
- eStát v roce 2006 navrhl elektronickou legalizaci
- princip:
  - žadatel se dostaví před orgán, provádějící legalizaci, s elektronicky podepsaným dokumentem
  - žadatel uzná elektronický podpis za vlastní
  - orgán, provádějící legalizaci, to osvědčí
    - připojí legalizační doložku a vše opatří svým elektronickým podpisem
- stanovisko tehdejšího MI ČR:
  - je to koncipováno „zcela bez respektu k právní úpravě uznávaného el. podpisu“

# co se chystá? od 1.7.2009

Datoveschranky.info

## • datové schránky

– možnosti přihlašování:

- pomocí jména a hesla, nebo
- pomocí technik elektronického podpisu

– důsledek (pro právnické a fyzické osoby):

- úkon, učiněný skrze datovou schránku, „**má stejné účinky jako úkon učiněný písemně a podepsaný**“

– i když se uživatel přihlásil k datové schránce jen pomocí jména a hesla

– **tj. uživatel nemusí připojovat svůj elektronický podpis, ale efekt je stejný jako kdyby ho připojil**

- **pouhé „jméno a heslo“ zde umožňuje dosáhnout stejného efektu jako elektronický podpis!!!!**



ale jak podepsaný?  
jen „podpis“? vlastnoruční podpis? ověřený podpis?

# v čem je problém?

- **u (uznávaného) elektronického podpisu:**

- svá podepisovací data (privátní klíč) mám pouze já, nedostává je ani certifikační autorita
- na certifikát, způsob jeho vydávání i fungování autority jsou kladeny přísné podmínky
  - ověřované při akreditaci

- **u jména a hesla:**

- moje přístupové údaje měl někdo druhý
  - ten, kdo je generoval, odesílal, ....
- nevím podle jakých pravidel mé přístupové údaje vznikly
  - jak funguje ten, kdo je generoval, odesílal, ....
- nevím, zda je nemá dosud
  - ani co všechno s nimi mohl (také) udělat ....

přesto mohu s pouhým jménem a heslem dosáhnout stejného efektu (platně se podepsat, v rámci úkonu ....), jako se svým privátním klíčem

# jiný problém s datovými schránkami

- když skrze datovou schránku získám (od orgánu veřejné moci) dokument v elektronické podobě, tento:
  - je (musí být) opatřen platným elektronickým podpisem či elektronickou značkou
  - může (ale nemusí být) opatřen časovým razítkem
- co se stane, až expiruje (skončí platnost) certifikátu, použitého při podepisování dokumentu?
- názor:
  - bez časového razítka nepůjde ověřit autenticita (pravost) dokumentu
    - neprokáži, kdy podpis vznikl
  - nepůjde provést autorizovaná konverze na žádost
    - podmínkou je platný elektronický podpis (v době konverze)
  - nepůjde použít jako součást (příloha) jiného podání, pokud má být podepsána
    - v okamžiku podání nebude elektronický podpis platný

Datoveschranky.info



# co se chystá? od 1.7.2009

- **mění se i celý systém doručování od soudů k občanům**
  - pro dokumenty v listinné i elektronické podobě
- **novinky:**
  - změna principu:
    - příjemce je odpovědný za to, aby soud měl vždy správnou a aktuální adresu, na kterou mu lze doručit
  - fikce doručení po 10 dnech i pro listinné dokumenty
    - doručované (Českou) poštou
  - doručuje se například skrze datovou schránku
    - pokud ji příjemce má zřízenu
  - příjemce může soud požádat, aby mu doručoval klasickým emailem
    - a on musí do tří dnů potvrdit příjem konkrétní zásilky
    - potvrzení musí být podepsáno zaručeným elektronickým podpisem
    - soudu musí dopředu sdělit svého akreditovaného poskytovatele certifikačních služeb
      - nebo přímo poskytnout svůj kvalifikovaný certifikát

???

děkuji za pozornost

Jiří Peterka

[jiri.peterka.cz](http://jiri.peterka.cz)  
[www.earchiv.cz](http://www.earchiv.cz)