Má elektronický podpis identifikovat podepsanou osobu?

A pokud ano: jak?

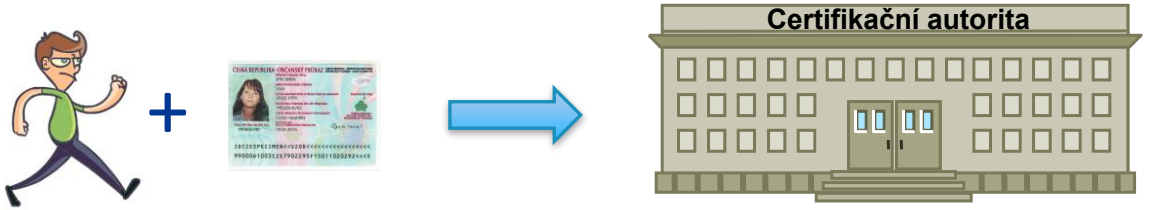
Jiří Peterka

nezávislý konzultant a publicista

pedagog na MFF UK

jak funguje (uznávaný) el. podpis?

- pro vystavení kvalifikovaného certifikátu se musíte dostavit osobně
  - a předložit certifikační autoritě (CA) své osobní doklady



- důsledek:
  - vydavatel certifikátu (CA) zná vaši identitu
- otázka:
  - „kolik“ ze svých znalostí vaší identity má CA přenést do certifikátu?

co je v silách el. podpisu?

- upřesnění:
  - bavíme se o uznávaném el. podpisu (a komunikaci s veř. správou)
    - od 1.7.2016: půjde o kvalifikovaný el. podpis (nařízení 910/2014: eIDAS)

- princip fungování:
  - identita (fyzické) osoby je zjištěna dostatečně spolehlivě a přesně
    - jednorázově, při žádosti o vydání kvalifikovaného certifikátu (provádí CA)
    - může být přenesena (vložena) do certifikátu

  - certifikát je veřejný a je připojen ke každému el. podpisu
    - důsledek: jednoznačná informace o identitě držitele certifikátu může být k dispozici spoléhající se straně (příjemci podepsaného dokumentu)
      - a za správnost identifikace ručí certifikační autorita

- důsledek:
  - **uznávaný el. podpis může mít „stejnou sílu“ jako úředně ověřený (vlastnoruční) podpis**

srovnání „síly“ různých podpisů

	Vlastnoruční	Ověřený (vlastnoruční)	Uznávaný (kvalifikovaný) el. podpis
Existence podpisu	ANO	ANO	ANO
Identifikace podepsané osoby	NE	ANO (znovu při každém podpisu)	ANO (jednorázově, při vydání certifikátu)
Pravost / neodmítnutelnost	NE	ANO (ručí za to ověřující)	ANO (dáno technicky/asymetr. kryptogr.)

- vlastnoruční podpis
  - nezajišťuje (vždy) identifikaci podepsané osoby
    - z „klikyháku“ nic nepoznáme
      - není předepsána podoba podpisu
  - ověření (pravosti) musí provádět (písmo)znalec
    - je to drahé, dělá se až při sporu

zásadní otázky

- má být (uznávaný) elektronický podpis postaven na roveň
  a. ověřenému (vlastnoručnímu) podpisu?
  b. vlastnoručnímu podpisu?

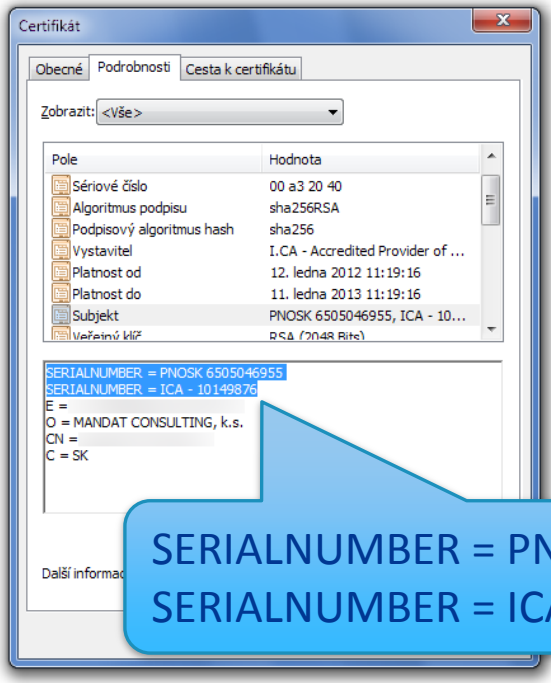
Situace:	Uznávaný el. podpis odpovídá:
dnes v ČR	není definováno (v praxi: vlastnoručnímu, ale jsou výjimky)
dnes na Slovensku	ověřenému podpisu (je-li připojeno časové razítko)
od 1.7.2016 (nařízení 910/2014, eIDAS)	vlastnoručnímu podpisu

- jiná otázka:
  - má el. podpis vůbec sloužit k identifikaci podepsané osoby?
    - část „lidí kolem el. podpisů“ se domnívá, že NE
      - je to konzistentní s tím, že vlastnoruční podpis také nezajišťuje identifikaci podepsané osoby (viz *„z klikyháku nepoznáme nic“*)

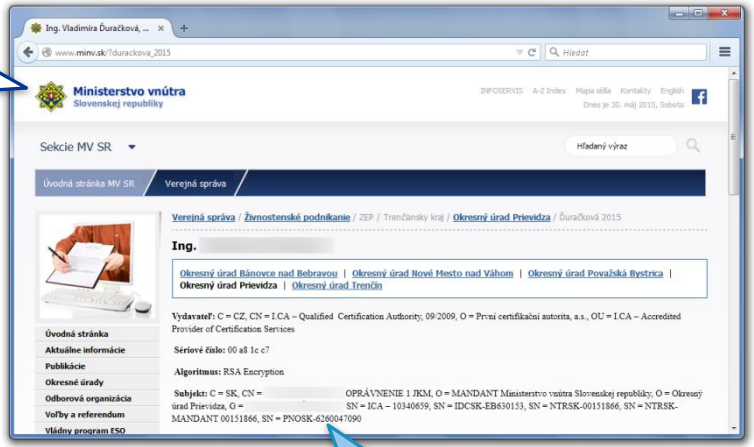
jak to řeší na Slovensku?

- vkládají do certifikátu rodné číslo držitele
  - přitom: certifikát je (musí být) veřejný !!!
    - pokud má být veřejný i podepsaný dokument

§ 5 zákona č. 215/2002 Sb. (o elektronickom podpise):
Ak sa v styku s orgánmi verejnej moci používa zaručený elektronický podpis, kvalifikovaný certifikát musí byť vydaný akreditovanou certifikačnou autoritou a musí obsahovať **rodné číslo držiteľa certifikátu**.



Ministerstvo vnitra (SK) zveřejňuje certifikáty úředníků



rodné číslo držitele

SERIALNUMBER = PNOSK 6505046955
SERIALNUMBER = ICA - 10149876

SN = PNOSK 6260047090

současný stav v ČR

- „tuzemský“ kvalifikovaný certifikát (pro uznávaný podpis):
  - musí obsahovat údaje, které umožňují jednoznačnou identifikaci

§11 odst. 3 zákona č. 227/2000 Sb.: Uznávaným elektronickým podpisem se rozumí *a)* zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a **obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby**

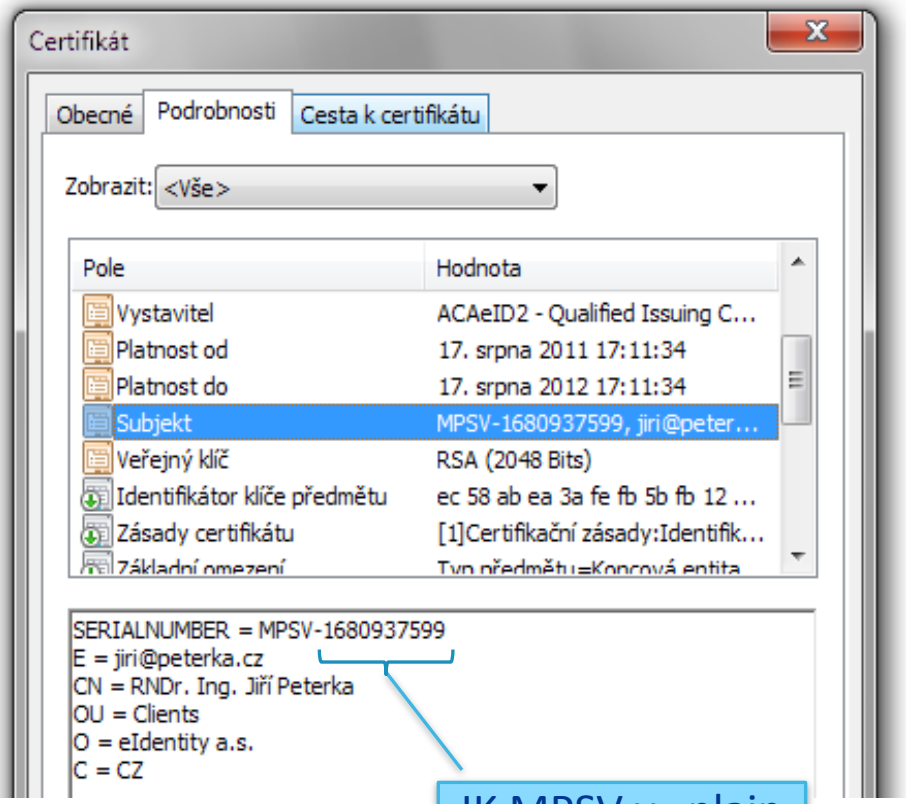
- o jaké údaje se jedná?
  - to říká vyhláška č. 212/2012 – ale špatně !!!!

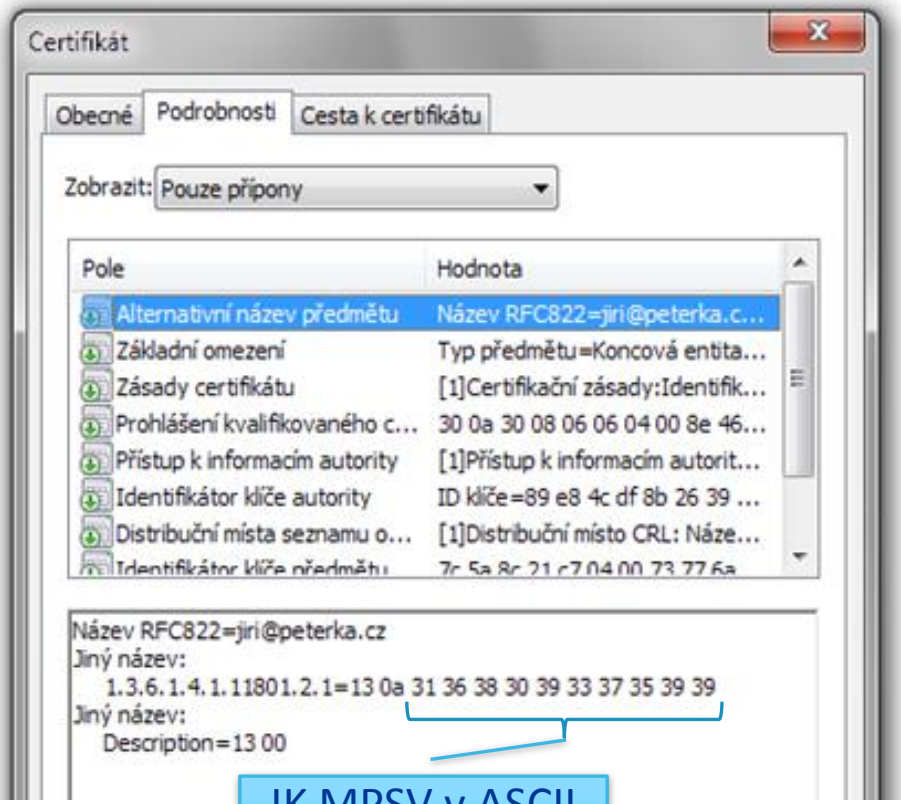
údaj, který umožňuje jednoznačnou identifikaci podepisující osoby, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295.

  - neříká, co má toto číslo znamenat – jaký identifikátor to má být
    - když si do certifikátu napíšu 1 111 111 111, bude to OK (ale k ničemu) !!

současná praxe v ČR

- do certifikátů se vkládá IK MPSV
  - přímo v CN (eIdentity)
  - v ASCII kódu v jiné položce (I.CA a PS)





v certifikátu je vždy uvedeno jméno a příjmení držitele (nebo pseudonym)

znovu základní otázka:

- CA zná (zcela přesně) identitu držitele certifikátu
- ale: „jak moc“ má tuto identitu znát spoléhající se strana?
  - tj. příjemce podepsaného dokumentu
    - což může být i soukromá osoba (nebo privátní subjekt) !!!
- možnosti:

a. nemusí ji znát vůbec (a musí si poradit nějak jinak)
   - jako u vlastnoručního podpisu
     - ale proč se pak v certifikátu vůbec uvádí jméno a příjmení?

b. zná ji „jen rámcově“, a jednoznačně pouze „potenciálně“
   - zná jen jméno a příjmení (což nepostačuje pro jednoznačnou identifikaci)
   - další údaje o identitě (nutné k jednoznačné identifikaci) může získat:
     - OVM: může se kdykoli „zeptat“ na držitele IK MPSV
     - soukromá osoba, privátní subjekt: musí vyvolat soudní spor
       - soud se pak může „zeptat“ CA, komu certifikát vydala

c. zná ji jednoznačně („aktuálně“, nikoli jen „potenciálně“)

nařízení 910/2014 (eIDAS)

- říká:
  - *„chci, aby kvalifikovaný el. podpis měl stejnou váhu jako vlastnoruční podpis“*
    - názor: je to krok zpět – způsobený tím, že některé členské země neznají ověřený (vlastnoruční) podpis
  - v kvalifikovaném certifikátu má být jméno (a příjmení) držitele
    - další položky tam mohou být, ale jen dobrovolně
      - nesmí být povinné, a celkový „efekt“ musí být stejný, jako když tam nejsou
- požaduje:
  - aby spoléhající se strana mohla ověřit (kvalifikovaný) el. podpis jako platný, musí jí být (řádně) poskytnuta unikátní data, identifikující držitele certifikátu (a tím i podepsanou osobu)

provided that …… the unique set of data representing the signatory in the certificate is correctly provided to the relying party

jak rozumět nařízení eIDAS?

- požaduje pro spoléhající se stranu „jednoznačnou identifikaci“, nebo jen „unikátní identifikátor“?
  - spíše jde o unikátní identifikátor (viz „a unique set of data …“)
- požaduje „aktuální“ možnost jednoznačné identifikace, nebo jen „potenciální“ možnost (pro případ sporu)?
  - vypadá to spíše na „potenciální“ možnost
    - tedy v zásadě stejně, jako je to dnes
- jaké údaje má mít k dispozici spoléhající se strana?
  - jak konkrétně má vypadat onen „unique set of data“?
    - mají to být jiná data než ta, která jsou již obsažena v certifikátu?
      - možná interpretace: *certifikát může obsahovat něco jako IK MPSV (či AIFO nebo VIFO), ale nepovinně. Pokud jej neobsahuje, musí jej podepsaná osoba dodat spoléhající straně nějak jinak*.
      - protiargument: pro potenciální identifikaci (při sporu, který řeší soud) postačuje sériové číslo certifikátu a identita vydavatele !!!!

děkuji za pozornost

Jiří Peterka

http://jiri.peterka.cz

http://www.earchiv.cz

http://www.bajecnysvet.cz

http://www.muzeuminternetu.cz