Seznámení s elektronickými podpisy

(v kontextu nařízení eIDAS a zákona č. 297/2016 Sb.)

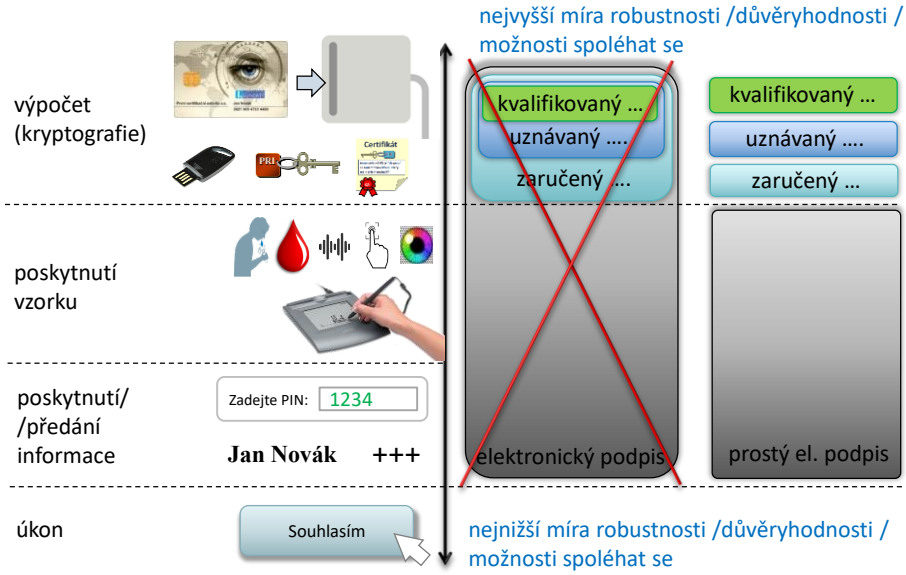
Jiří Peterka

Praha, 17.6.2019

1

není (el.) podpis jako (el.) podpis

- lidé dnes chtějí/mohou/musí projevovat svou vůli různými způsoby



2

kvalifikovaný statut

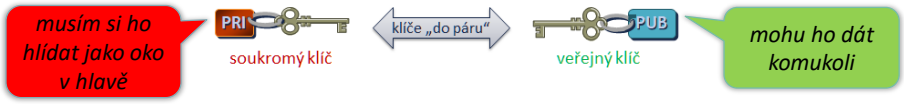
- přívlastkem „*kvalifikované*“ se označuje to, čemu můžeme (musíme) důvěřovat …. již ze zákona (z nařízení)
  - svou důvěru odvozujeme ze zákona (z nařízení)
  - máme:
    - kvalifikované služby (vytvářející důvěru)
      - např. kvalifikované služby uchovávání elektronických podpisů a pečetí
      - kvalifikované služby ověřování platnosti …. podpisů, pečetí
      - ……
    - kvalifikované poskytovatele (služeb vytvářejících důvěru)
      - dnes v ČR: I.CA, PostSignum, eIdentity, Software602, SZR
    - kvalifikované elektronické podpisy, kvalifikované elektronické pečeti, el. časová razítka
    - kvalifikované certifikáty
    - kvalifikované prostředky (pro vytváření el. podpisů a pečetí – QSCD a QSealCD)
    - ……

- to, co není kvalifikované, nemusí být nedůvěryhodné
  - ale: pokud tomu chceme důvěřovat, musíme svou důvěru odvozovat z něčeho jiného, než ze zákona/nařízení
    - obvykle: z toho, kdo je poskytovatelem služby / vydavatelem certifikátu
      - například: důvěřujeme bance, u které máme peníze

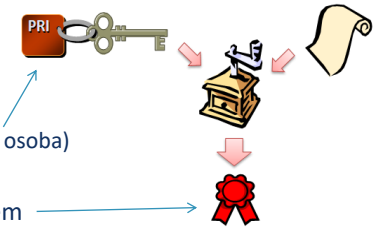
3

kvalifikované, uznávané a zaručené ..

- v čem se shodují tyto druhy elektronických podpisů?
  - jsou **„kryptografické“**
    - tj. jsou založené na poznatcích a metodách matematiky (kryptografie)
      - hlavně: na asymetrické kryptografii
        - kvůli tomu se u nich pracuje s dvojicí klíčů – soukromým a veřejným



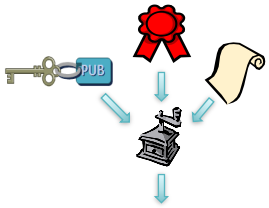
  - jsou **„počítané“**
    - vznikají výpočtem
      - zjednodušená představa: vznikají semletím
        - soukromého klíče (který má jen podepisující osoba)
        - podepisovaného dokumentu
    - samotné podpisy jsou (jedním velkým) číslem



4

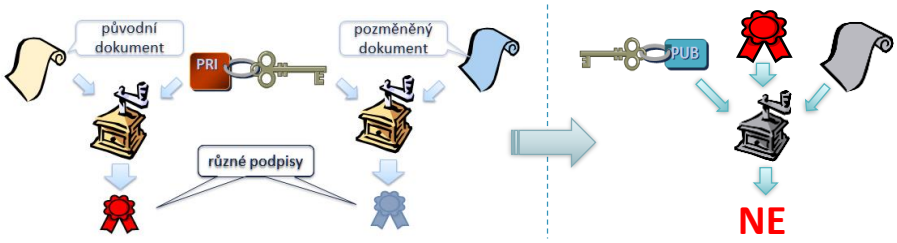
kvalifikované, uznávané a zaručené ..

- v čem se shodují tyto druhy elektronických podpisů?
  - **jsou exaktní** (jednoznačné)
    - platnost se ověřuje (exaktním) výpočtem
    - výsledky ověření platnosti jsou exaktní
      - jen: ANO/NE/nelze ověřit
    - žádné klikyháky
      - jméno podepsané osoby je vždy dokonale čitelné



ANO/NE/nelze ověřit

  - **dokáží chránit proti změně**
    - pokud by došlo ke změně již podepsaného dokumentu, spolehlivě by se to poznalo (původní podpis na pozměněném dokumentu by byl neplatný)

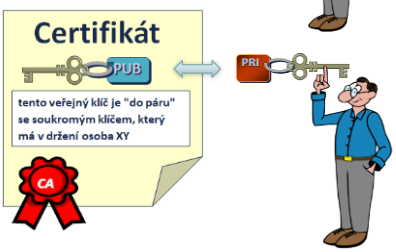


5

kvalifikované, uznávané a zaručené ..

- v čem se shodují tyto druhy elektronických podpisů?
  - to, komu patří (koho máme považovat za podepsanou osobu) se odvozuje od držení soukromého klíče
    - platí zde princip nepopiratelnosti/neodmítnutelnosti (non-repuditation):
      - k vytvoření el. podpisu musel být použit příslušný soukromý klíč
      - resp. el. podpis není možné vytvořit bez příslušného soukromého klíče
  - díky tomu může nastoupit právní fikce:
    - *podepsanou osobou je ten, kdo prohlašuje příslušný soukromý klíč za svůj*

  - k deklaraci toho, že „*tento soukromý klíč je můj*“, slouží **certifikáty**
    - certifikát je osvědčení o držení soukromého klíče
      - » ale sám obsahuje jen veřejný klíč
    - vydává ho tzv. certifikační autorita
      - » dnes: **poskytovatel služeb vytvářejících důvěru**



6

kvalifikované, uznávané a zaručené ..

- v čem se liší tyto druhy elektronických podpisů?
  - v požadavcích na:
    - **„kvalitu“ certifikátu**:
      - kvalifikovaný a uznávaný el. podpis
        - certifikát musí být kvalifikovaný
          - tím je dáno i to, že vydavatel certifikátu musí být kvalifikovaný (poskytovatel služeb vytvářejících důvěru)

jeho obsah musí být pravdivý !!

      - zaručený el. podpis
        - není kladem žádný požadavek
          - ani na druh certifikátu
          - ani na vydavatele certifikátu

jeho obsah nemusí být pravdivý !!

    - **způsob uložení soukr. klíče**:
      - kvalifikovaný el. podpis
        - je vyžadován tzv. **kvalifikovaný prostředek**
          - jak pro uchovávání klíče
          - tak i pro vytváření el. podpisů
      - zaručený a uznávaný el. podpis
        - není kladen žádný požadavek
          - soukromý klíč si držitel může uchovávat kde chce
            - je to hlavně otázka bezpečnosti

druh el. podpisu	kvalita certifikátu	uložení soukromého klíče
kvalifikovaný el. podpis	kvalifikovaný certifikát	kvalifikovaný prostředek
uznávaný el. podpis	kvalifikovaný certifikát	žádný požadavek
zaručený el. podpis	žádný požadavek	žádný požadavek

7

kvalifikované, uznávané a zaručené ..

- důsledky odlišností:
  - týkají se hlavně možnosti spoléhat se na to, komu podpis patří
    - na identitu podepsané osoby

- proč?
  - protože „to, komu podpis patří“ se odvozuje z obsahu certifikátu

- konkrétně:
  - kvalifikovaný el. podpis: zaručuje identitu podepsané osoby
    - s vyšší mírou spolehlivosti, než uznávaný el. podpis
  - uznávaný el. podpis: zaručuje identitu podepsané osoby
    - ale s nižší mírou spolehlivosti, než kvalifikovaný el. podpis
      - kvůli většímu riziku kompromitace soukromého klíče
  - zaručený el. podpis: nezaručuje identitu podepsané osoby
    - *„něco tam sice je napsané, ale to vůbec nemusí být pravda ….“*

8

Odbočení: pravost vs. platnost el. podpisů

- „lidé od práva“ řeší (ověřují) pravost podpisů:
  - podpis je pravý = skutečně jej vytvořila příslušná osoba
    - ta osoba, která je prezentována jako podepsaná osoba
  - „pravost podpisu“ je právní pojem

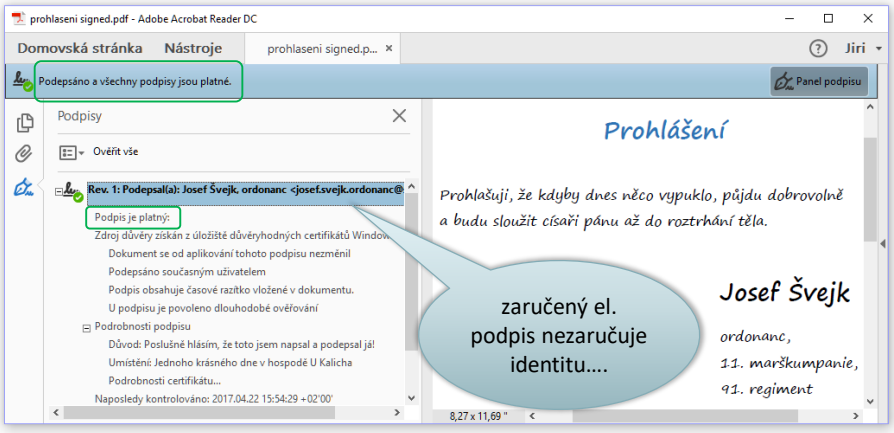
- pravost el. podpisu se odvozuje z jeho platnosti
  - u kvalifikovaného a uznávaného el. podpisu lze presumovat jeho pravost
    - i když to v (současné) právní úpravě není explicitně ošetřeno
    - pro kvalifikovaný el. podpis to bylo ošetřeno v původní právní úpravě
      - § 3 odst. 2 zákona č. 227/2000 Sb. o elektronickém podpisu
  - u zaručeného el. podpisu nikoli !!!

- „lidé od počítačů“ řeší platnost elektronických podpisů
  - podpis je platný = jsou splněny všechny podmínky pro jeho platnost
    - obecně:
      - neporušená integrita
      - certifikát je v době platnosti
      - certifikát nebyl revokován
    - jejich splnění je posuzováno k určitému časovému okamžiku
      - rozhodnému okamžiku, posuzovanému okamžiku
  - „platnost podpisu“ je technický pojem
    - a nemění se v čase
      - protože splnění podmínek se (obecně) posuzuje k rozhodnému okamžiku
    - má smysl jen pro „kryptografické“ podpisy

9

příklad zaručeného el. podpisu

- který je platný, ale není pravý
  - nevytvořil ho ten, kdo je prezentován jako podepsaná osoba

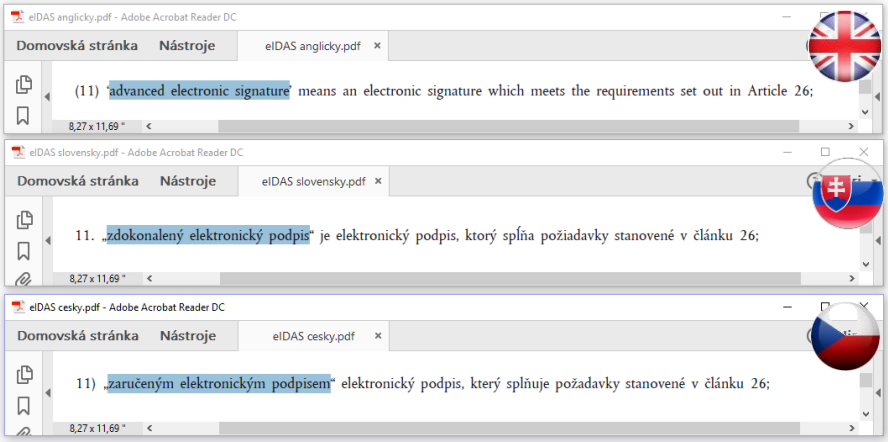


- důvod: tento podpis se opírá pouze o testovací certifikát
  - vyrobený „na koleně“
    - může v něm být napsáno cokoli – i něco, co není pravdou

10

proč „zaručený“ el. podpis?

- je to špatný (jazykový) překlad
  - chyba se stala již v roce 2000, dosud nebyla opravena



- „zdokonalený“ (či: „pokročilý“, „vylepšený“) el. podpis není od toho, aby zaručoval identitu podepsané osoby (pravost podpisu)
  - od toho jsou „vyšší“ varianty el. podpisu – uznávaný a kvalifikovaný el. podpis

11

zaručený el. podpis dlouhodobě mate

- mnoho lidí si stále myslí, že zaručený el. podpis zaručuje identitu podepsané osoby (pravost)
  - a požadují tento druh podpisu tam, kde by měli požadovat „vyšší“ variantu el. podpisu
- příklady z legislativy:
  - zákon č. 99/1963 Sb., Občanský soudní řád
    - § 174a: Elektronický platební rozkaz
      - (1) *Je-li návrh podán na elektronickém formuláři podepsaném ~~zaručeným~~ elektronickým podpisem žalobce a nepřevyšuje-li peněžité plnění požadované žalobcem částku 1 000 000 Kč, soud může vydat na návrh žalobce elektronický platební rozkaz*

teprve od 1.7.2012: **uznávaným**

  - zákon č. 269/1994 Sb., Zákon o Rejstříku trestů
    - § 16a
      - (1) *Žádost o vydání výpisu a o nahlédnutí do opisu může osoba, jíž se údaje týkají, zaslat v elektronické podobě ~~opatřené zaručeným~~ elektronickým podpisem.*

od 1.7.2012: **podepsané uznávaným**

  - vyhláška č. 62/2015 Sb., o provedení některých ustanovení zákona o zdravotnických prostředcích
    - (3) *Výsledek šetření nežádoucí příhody oznamuje výrobce nebo zplnomocněný zástupce Ústavu elektronicky vyplněným a zaručeným elektronickým podpisem podepsaným formulářem pro hlášení nežádoucí příhody*

požadavek na „zaručený“: celkem 6x

12

odbočení: další terminologický problém

- uznávaný elektronický podpis není jeden !!!
  - ale jsou to dva různé druhy elektronických podpisů

- značně to komplikuje vyjadřování o uznávaných el. podpisech
  - správně by vždy mělo být indikováno, o kterou variantu jde
- úmluva (pro potřeby této prezentace):
  - variantu *„zaručený el. podpis, založený na kvalifikovaném certifikátu“* budeme označovat jako **český uznávaný el. podpis**

13

kvalifikovaný vs. uznávaný el. podpis

- kvalifikovaný el. podpis
  - používá se a uznává v celé EU
  - vyžaduje kvalifikovaný certifikát
  - vyžaduje použití certifikované čipové karty nebo USB tokenu
    - tzv. kvalifikovaného prostředku pro vytvářejí el. podpisů
      - reálně: jde o bezpečné uložení soukromého klíče

- „český“ uznávaný el. podpis
  - naše národní specialita
  - vyžaduje kvalifikovaný certifikát
  - nevyžaduje použití certifikované čipové karty nebo USB tokenu
    - reálně: jde o peníze – *„přeci nebudeme nutit lidi pořizovat si čipovou kartu/token“*
      - » dnes za cca 700 Kč

- **analogie s platebními kartami:**
  - kvalifikovaný el. podpis je jako platba u obchodníka / výběr z bankomatu:
    - je nutné mít kartu (fyzicky) - pokud vám ji neukradnou, je riziko zneužití malé ……
  - „český“ uznávaný el. podpis je jako on-line platba po Internetu
    - není nutné mít kartu (fyzicky), stačí znát údaje o kartě. Riziko zneužití je větší ……

14

nejsou jen el. podpisy (ale i pečeti)

- **zásada**: fyzické osoby se podepisují, právnické osoby pečetí

- **elektronický podpis**:
  - je projevem vůle vůči obsahu podepisovaného dokumentu
  - mohu podepsat i cizí dokument
    - nemusím být jeho původcem
      - na jednom dokumentu mohou být podpisy více osob
  - podepsanou osobou je fyzická osoba
- **elektronická pečeť**:
  - je vyjádřením původu
    - a zajištěním integrity
  - opatřit svou pečetí mohu pouze svůj dokument !!!
    - musím být jeho původcem
  - pečetící osobou je právnická osoba
    - včetně organizační složky státu

druh el. podpisu	druh el. pečeti	vyžaduje	zaručuje
kvalifikovaný el. podpis	kvalifikovaná el. pečeť	kvalifikovaný prostředek kvalifikovaný certifikát	identitu integritu
(„český“) uznávaný el. podpis	(„česká“) uznávaná el. pečeť	kvalifikovaný certifikát	identitu integritu
zaručený el. podpis	zaručená el. pečeť	*… vzniká výpočtem ….*	integritu
prostý el. podpis	prostá el. pečeť	*… nevyžaduje se nic ….*	*… nic …*

15

(elektronická) časová razítka

- nejsou projevem vůle (ani vyjádřením původu)
  - jen „fixují“ konkrétní obsah (dokument, podpis, pečeť) v čase
    - ve smyslu: to, co je opatřeno el. časovým razítkem, již existovalo v čase připojení časového razítka ….
  - používají se především kvalifikovaná el. časová razítka
    - u kterých se lze spoléhat na údaj o čase (připojení časového razítka)
      - existují i ne-kvalifikovaná (např. testovací) razítka, u kterých se nelze spoléhat …
  - pomáhají zajistit digitální kontinuitu
    - možnost ověření podpisu/pečeti i po delším čase …….
- kdo má povinnost připojovat (kvalifikovaná) el. časová razítka – k el. podpisům a el. pečetím?
  - veřejnoprávní podepisující (a osoby vykonávající působnost)
    - ukládá jim to § 11 zákona č. 297/2016 Sb. o službách vytvářejících důvěru
- ostatní subjekty nemají povinnost razítka používat
  - **ale lze jim to vřele doporučit, kvůli zajištění digitální kontinuity …..**

16

problém digitální kontinuity (zjednodušeně)

- již dnes:
  - počítače dokáží syntetizovat hlas konkrétní osoby
    - aniž by to mluvila ona, a aniž by se dal poznat rozdíl
- je pouze otázkou času, kdy:
  - počítače dokáží napodobit písmo konkrétní fyzické osoby, včetně jejího vlastnoručního podpisu
    - tak, aby to nedokázal poznat (ani sebelepší) písmoznalec
  - počítače dokáží „prolomit“ (dnešní) elektronický podpis
    - a vytvořit tzv. kolizní dokument (jiný dokument, ale se stejným podpisem)
      - pak nepůjde poznat, který dokument byl původně podepsán
- řešením je „škálování složitosti“
  - zvyšování složitosti toho, co je potřeba překonat („prolomit“, napodobit, …..)
    - musí se dělat proaktivně (dopředu), nikoli reaktivně (až když už dojde k ..)

problém: složitost (napodobení) vlastnoručního podpisu nejde škálovat !!! (nelze chtít, aby se lidé podepisovali 10x složitěji, pak 100x, pak 1000x atd.)

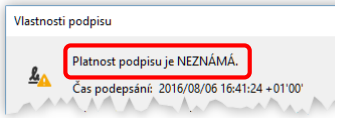
výhoda „kryptografických“ el. podpisů: složitost (výpočtu / prolomení) lze zvyšovat podle potřeby

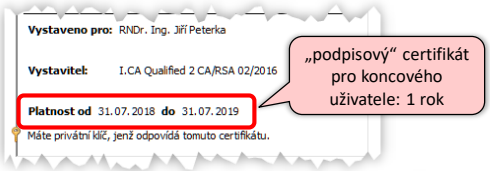
pozor, neplatí to pro prosté el. podpisy !!

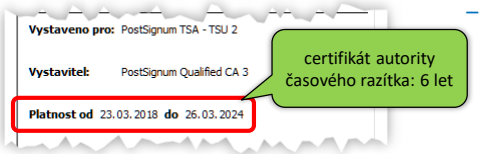
17

výhoda „kryptografických“ el. podpisů

- mají v sobě zabudovánu „časovou pojistku“
  - proti svému „prolomení“
- kde? jak je realizována?
  - jde o časové omezení certifikátů
    - každý certifikát má jen omezenou dobu řádné platnosti
      - určuje vydavatel certifikátu, podle svého odhadu vývoje „výpočetní síly“ počítačů





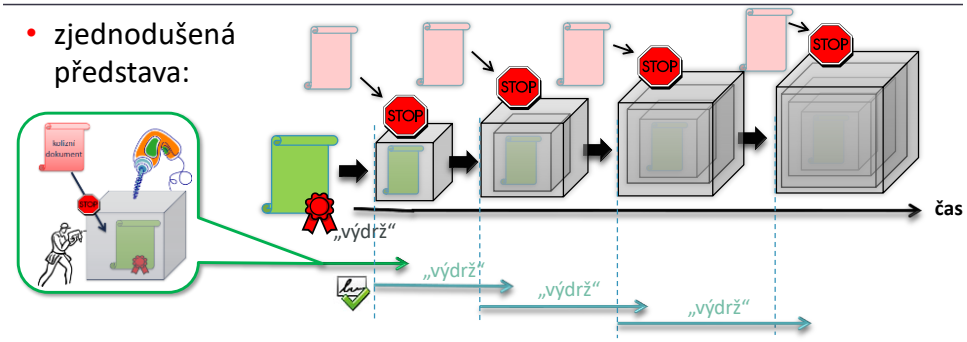


- jak (čím) se projevuje?
  - tím, že po určité době již není možné ověřit platnost konkrétního el. podpisu
    - podpis bez časového razítka
      - lze ověřit jen to té doby, než skončí řádná doba platnosti „podpisového“ certifikátu
        - tj. *„kolik zbývá do 1 roku ….“*
    - podpis s (1) časovým razítkem
      - lze ověřit jen to té doby, než skončí řádná doba platnosti certifikátu autority časového razítka
        - tj. *„kolik zbývá do 6 let ….“*

18

princip zajištění digitální kontinuity

- zjednodušená představa:



- neboli:
  - ještě než skončí možnost ověření (než protistrana stihne „prolomit“), je nutné provést nápravné opatření (analogie: vložit do ještě „bytelnější“ schránky)
    - stačilo by: znovu podepsat „kryptografickým“ elektronickým podpisem
      - protože se použije „aktuálně dostatečně silný/složitý“ elektronický podpis
        - ale: podpis má určité právní účinky (je projevem vůle)
    - lepší řešení: připojí se další časové razítko (+ tzv. validační informace)
      - technicky je to stejné, jako podepsání (opatření „kryptografickým“ podpisem)
        - ale: právní účinky jsou vhodnější – nejde o projev vůle, ale o „zafixování v čase“

19