Elektronické podpisy a pečetě ve světle nařízení eIDAS a zákona 297/2016 Sb.

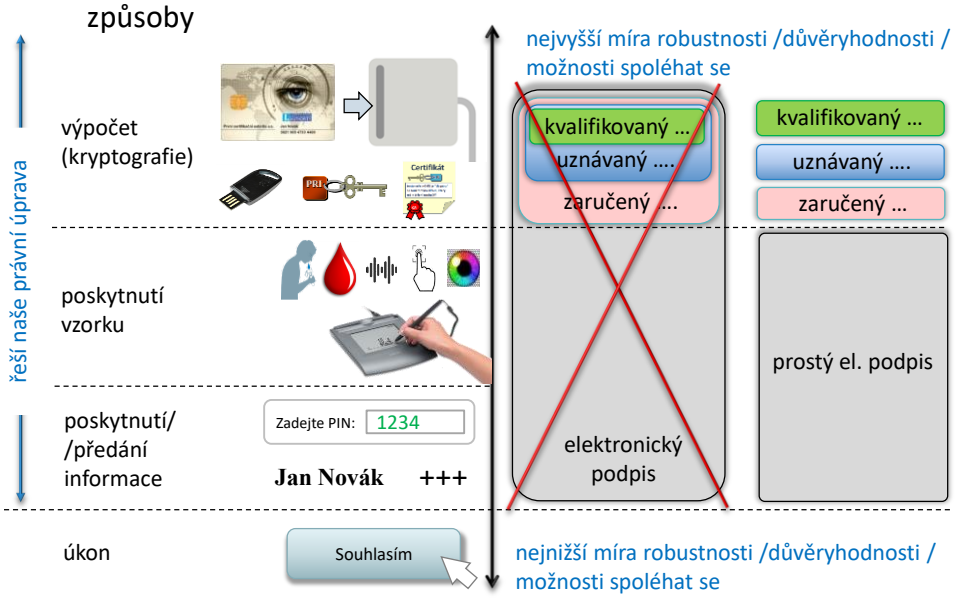
Jiří Peterka

21.2.2019

1

není (el.) podpis jako (el.) podpis

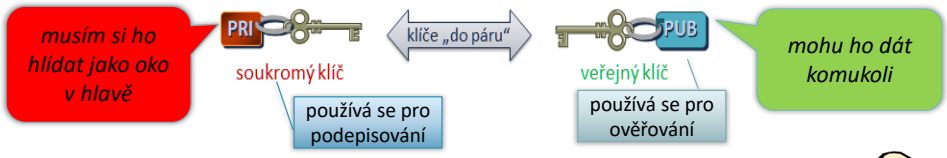
- lidé dnes chtějí/mohou/musí projevovat svou vůli různými způsoby



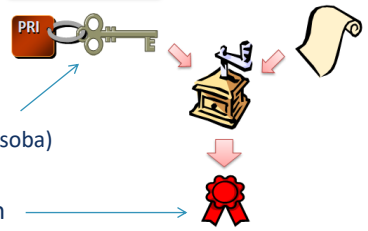
2

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



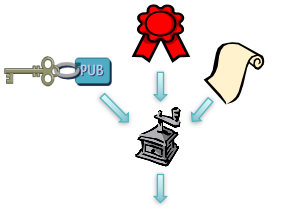
  - **jsou „počítané“**
    - vznikají výpočtem
      - zjednodušená představa: vznikají semletím
        - soukromého klíče (který má jen podepisující osoba)
        - podepisovaného dokumentu
    - samotné podpisy jsou (jedním velkým) číslem



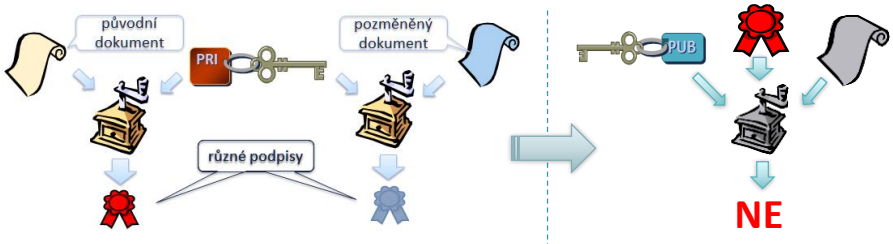
3

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



  - 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)

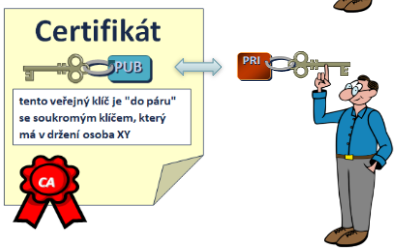


4

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
        - el. podpis není možné vytvořit bez příslušného soukromého klíče / s jiným klíčem
    - 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



5

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**

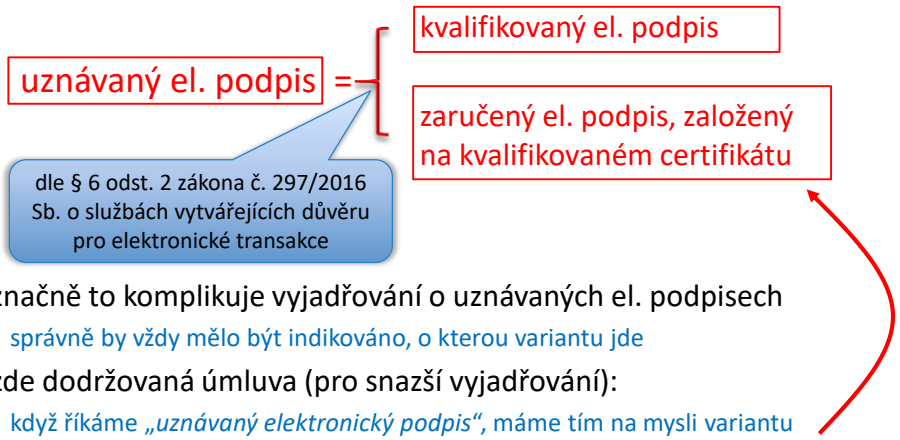
      - jak pro uchovávání klíče
      - tak i pro vytváření el. podpisů
  - **zaručený** a **uznávaný** el. podpis
    - není kladen žádný požadavek
      - soukromý klíč si držitel může uchovávat kde chce
        - je to hlavně otázka bezpečnosti

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

6

odbočení: terminologický problém

- uznávaný elektronický podpis (dnes) není jeden !!!
  - ale jsou to dva různé druhy elektronických podpisů
    - dříve (před eIDAS) to byl jen jeden druh el. podpisu – ale aby se kvůli eIDAS nemuselo měnit tolik legislativních předpisů, zavedla se tato „legislativní zkratka“

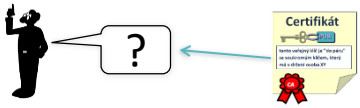


- značně to komplikuje vyjadřování o uznávaných el. podpisech
  - správně by vždy mělo být indikováno, o kterou variantu jde
- zde dodržovaná úmluva (pro snazší vyjadřování):
  - když říkáme „*uznávaný elektronický podpis*“, máme tím na mysli variantu „*zaručený el. podpis, založený na kvalifikovaném certifikátu*“

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 ….“*

soukromý klíč musí být uložen v kvalifikovaném prostředku

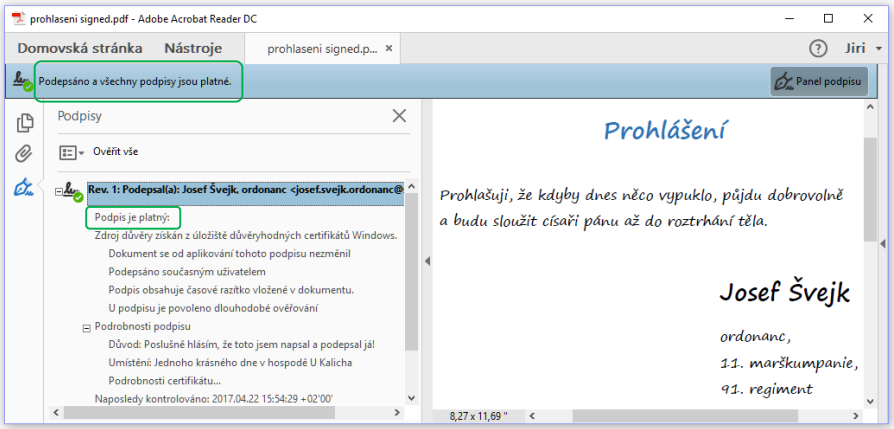
soukromý klíč může být uložen kdekoli

certifikát může být jakýkoli

8

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

9

srovnání (možností ověřování podpisů)

- **vlastnoruční podpis**
  - nemusí vypovídat o identitě podepsané osoby (viz nečitelný „klikyhák“)
  - „napoprvé“ mu důvěřujeme bez ověření (nezkoumáme ho)
    - ověřujeme ho až ex-post (v případě sporu), protože je to drahé a pomalé
      - ověření dělá písmoznalec, potřebuje více vzorků (s již zjištěným původem - identitou),
      - fakticky se ověřuje míra shody mezi vzorky, verdikt je statistický (na X%)
- **zaručený elektronický podpis**
  - *něco o identitě vypovídá, ale nelze se na to spoléhat …….*
  - pokud máme více vzorků, můžeme jednoznačně ověřit, že patří stejné osobě
    - že byly vytvořeny stejným soukromým klíčem
    - nepotřebujeme písmoznalce (provádí program), výsledek je ANO/NE/NELZE
- **uznávaný elektronický podpis**
  - vypovídá o identitě podepsané osoby (lze se na to spoléhat)
  - ke spolehlivému ověření stačí jediný el. podpis (jediný vzorek / exemplář)
    - ověření může být rychlé, levné, automatické (program), výsledek ANO/NE/NELZE
  - důsledek: ověření lze dělat dopředu („napoprvé“), ne až ex-post (v případě sporu)

10

el. podepisování vs. pečetění

- nařízení eIDAS zavedlo **elektronické pečeti** (Electronic Seals)
- pečeti a podpisy se **shodují** po technické stránce:
  - jsou „kryprografické“ a mají stejné vlastnosti jako podpisy
    - používají jiné certifikáty: certifikáty pro el. podpisy vs. certifikáty pro el. pečeti
      - právě druh certifikátu určuje, zda se jedná o podpis nebo pečeť

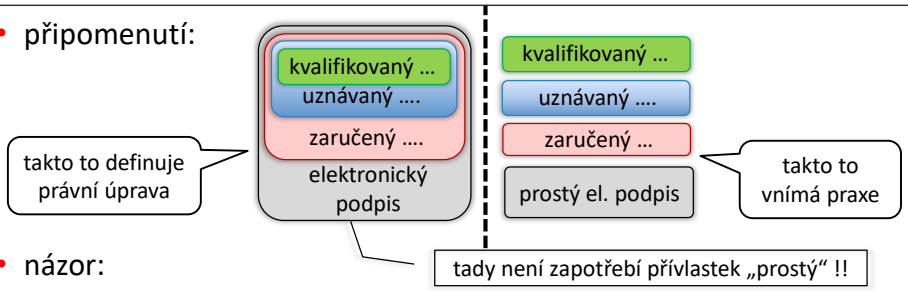
- pečeti a podpisy se **liší** po právní stránce:

– podpisy		– pečeti
• vytváří je (podepisují se) pouze fyzické osoby	⟷	• vytváří je (pečetí) pouze právnické osoby
• podpis je projevem vůle fyz. osoby	⟷	• pečeť je vyjádřením původu
• lze podepsat i cizí dokument	⟷	• pečetí lze opatřit pouze vlastní dokument – jehož je právnická osoba původcem
• podpisy se obvykle vytváří „ručně“ – kvalifikované prostředky (QSCD) jsou relativně levné (stovky Kč)	⟷	• pečeti se nejčastěji vytváří strojově – kvalifikované prostředky (QSealCD/HSM) jsou hodně drahé

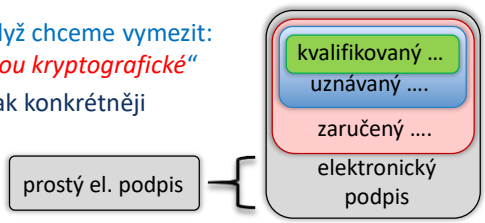
11

(prosté) elektronické podpisy

- připomenutí:

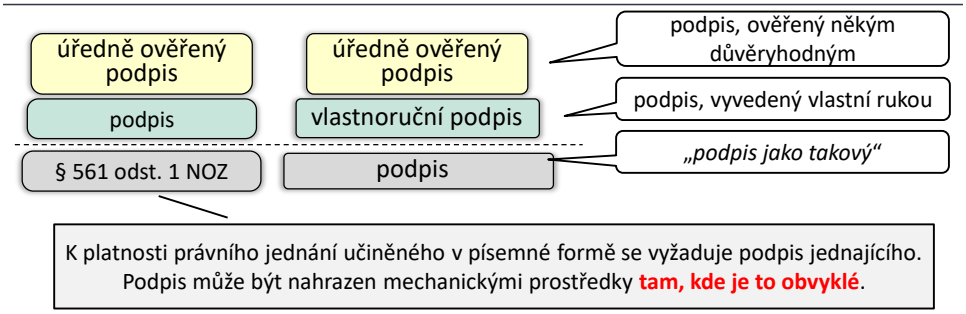


- názor:
  - pojem **elektronický podpis** je spíše určitý „definiční základ“ (nejširší kategorie), umožňující vymezit specifičtější („užší“) kategorie s konkrétnějšími vlastnostmi
    - má za cíl říci: *má to sloužit jako podpis, ale být „z nul a jedniček“*
  - přívlastkem „prostý“ si pomáháme, když chceme vymezit: *„ty podpisy z nul a jedniček, které nejsou kryptografické“*
    - nařízení eIDAS se touto kategorií nijak konkrétněji nezabývá:
      - neklade na ni žádné požadavky,
      - nepřisuzuje žádné právní účinky
    - nařízení eIDAS řeší jen „kryptografické“ elektronické podpisy



12

analogie z listinného světa



- názor:
  - prosté elektronické podpisy odpovídají „podpisům, které nejsou vyvedeny vlastní rukou“ (resp.: *nahrazení podpisu mechanickými prostředky (NOZ)*“)
- ale: jejich využití není omezeno jen na „*tam, kde je to obvyklé*“ !!!
  - §7 zákona č. 297/2016 Sb.:
    - K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, **případně jiný typ elektronického podpisu**, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1.

„veřejnoprávní jednání“

13

(prosté) elektronické podpisy

- definice elektronického podpisu v nařízení:
  - data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání
- přeloženo do češtiny:
  - mohou to být „jakékoli nuly a jedničky“, které jsou „nějak provázány“ s „podepisovanými nulami a jedničkami“, a podepisující osoba je považuje za svůj podpis

- důsledek:
  - je to tak obecná definice, že jí vyhoví úplně cokoli .....
    - jakýkoli způsob určení/získání „nul a jedniček“, představujících podpis
    - jakýkoli způsob „provázání“ podpisu a podepisovaných dat
- prostý elektronický podpis:
  - vyloučíme asymetrickou kryptografii ....

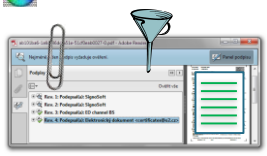
protože po nich není nic požadováno !!

14

příklad: dynamický biometrický podpis

- vyhovuje definici prostého elektronického podpisu
  - je to vlastně „vzorek podepisující osoby“
    - podobně, jako otisk prstu, vzorek DNA (krev, sliny, …), …
  - získává se pomocí úkonu, který má charakter odběru
    - obdobně, jako odběr vzorku krve, vzorku slin, otisku prstů …..

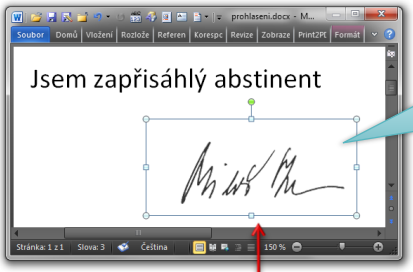
1100101010
el. podpis



- výhody:
  - odběr vzorku vytváří iluzi podepisování
  - je to „elektronické řešení pro masy“
  - vzorek je dostatečně charakteristický
    - lze znalecky zkoumat, zda patří příslušné osobě
      - **ale nelze z něj poznat, z jakého důvodu (v souvislosti s čím) byl vzorek odebrán !!**
- nevýhody:
  - další osud odebraného vzorku není v rukou „podepisující“ osoby
    - ona nemá kontrolu nad tím, k čemu je její vzorek připojen – musí se spoléhat na korektnost druhé strany
  - podepisující se tímto způsobem nemůže podepsat sám
    - potřebujete na to druhou (smluvní) stranu, není to pro jednostranné úkony

15

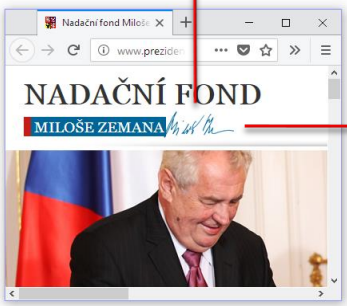
příklad: „obrázkový“ el. podpis



tzv. **obrázkový podpis** v praxi se používá, máme tendenci mu věřit a akceptovat ho

analogie v listinném světě

věřil by tomu někdo?



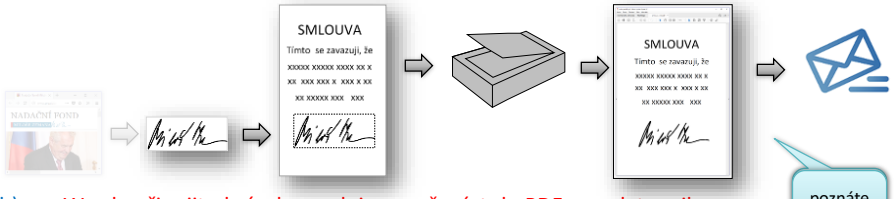
Jsem zapřisáhlý abstinent

16

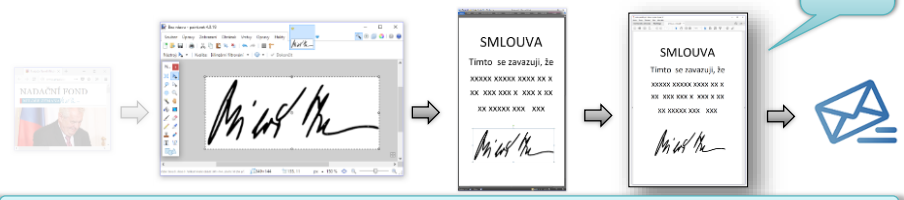
obrázkový podpis: příklad z praxe

- *… posílám návrh smlouvy ve Wordu …. prosím podepište, naskenujte a pošlete zpět mailem …..*

  - lze udělat různými způsoby:
    a) skutečně vytisknout, vlastnoručně podepsat, naskenovat (do PDF) a poslat mailem
      - nebo: nepodepisovat, ale přiložit lístek s podpisem, naskenovat a poslat mailem



    b) ve Wordu připojit obrázek s podpisem, převést do PDF a poslat mailem



otázka: proč to vůbec posílat? Postup dle b) si může udělat druhá strana sama (stačí „vzít“ podpis z jiné smlouvy)

17

příklady prostých el. podpisů

- jak by vypadaly v tradičním papírovém (listinném) světě …….

- je zde stále zachována písemná forma?
  - která vyžaduje podpis, nikoli jen nějaké znamení, "razítko", ústní odsouhlasení apod.
- lze určit podepsanou osobu?
  - kdo je Pepa? Kdo je ☺ ? Kdo je 1?
    - může to být více osob – a jak poznáme – či dokonce ověříme, v případě sporu – o kterou konkrétní osobu jde?
    - extrém: všichni jsme jedničky, a proto se podepisujeme stejně, jako 

- co se bude zkoumat v případě sporu? Jak se bude dokazovat pravost?

18

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.)

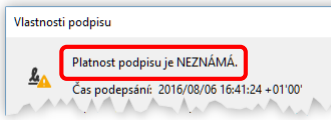
výhoda „kryptografických“ el. podpisů: složitost (výpočtu / prolomení) lze zvyšovat podle potřeby

pozor, neplatí to pro prosté el. podpisy !!

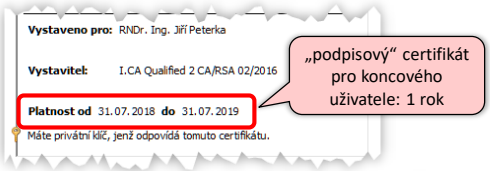
19

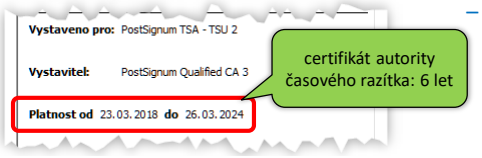
výhoda „kryptografických“ el. podpisů

- 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 časovým razítkem
      - lze ověřit jen to té doby, než skončí řádná doba platnosti certifikátu autority časového razítka
        - tj. *„kolik zbývá do 6 let ….“*

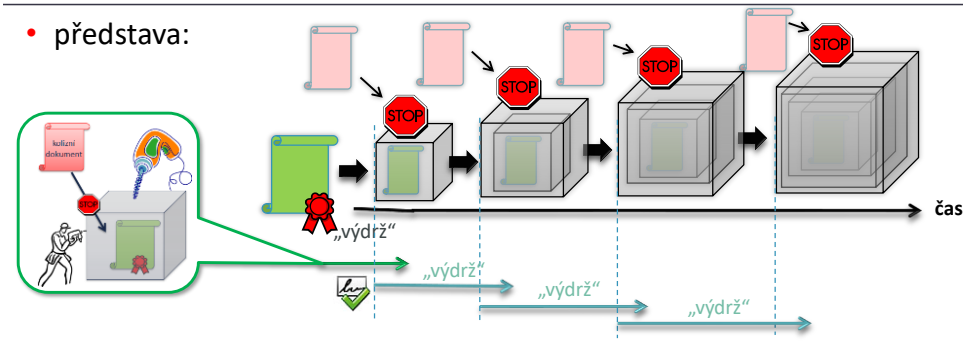




20

princip zajištění digitální kontinuity

- 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
      - technicky je to stejné, jako podepsání (opatření „kryptografickým“ podpisem)
        - ale: právní účinky jsou vhodnější – nejde o projev vůle, ale o „zafixování v čase“

21

děkuji za pozornost

Jiří Peterka

jiri@peterka.cz
www.earchiv.cz

22