Problematické aspekty elektronického podepisování

Jiří Peterka

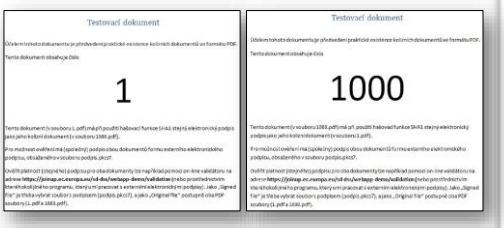
Praha, 17.6.2019

1

2009: MV ČR „zavelelo“ k přechodu na SHA-2

- nařídilo to certifikačním autoritám
  - ostatním to „důrazně doporučilo“
- problém:
  - mnozí uživatelé dodnes používají SHA-1
  - přestože SHA-1 již je slabá a kolizní dokumenty reálně existují


Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu


Testovací dokument

1

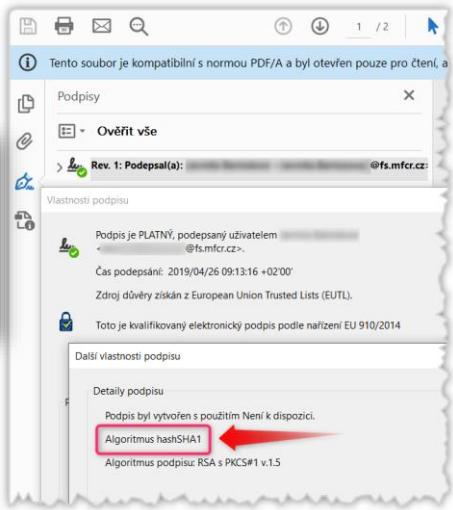
Testovací dokument

1000

SHA-256:
61809BC85C4287185035138E
F0E212989BE4F198AADAA77E
96DDD399AFC3E3D0

SHA-256:
2F224F3D79A506E178F7E84C
25209C7DD6266F4527A2A557
639652DE7F357815

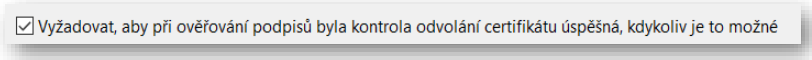
SHA1:
087DD6660A05F1C5729C6F1BF589CE0EF1C35941



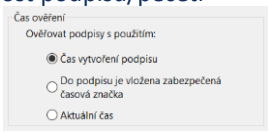
2

problémy s nastavením programů

- používané programy (např. Adobe Acrobat/Reader) mají mnoho možností nastavení
  - které zásadně ovlivňují výsledek ověření
- příklady (pro Adobe Reader):
  - lze vypnout kontrolu revokace (předčasného zneplatnění)
    - důsledek: podpis, vytvořený až po revokaci, bude vyhodnocen jako platný !!!



  - lze volit 3 různé varianty volby tzv. rozhodného okamžiku
    - ke kterému se vyhodnocuje splnění podmínek pro platnost podpisu/pečeti
      - „od výrobce“ je nastavena varianta „čas vytvoření podpisu“
        - tj. mělo by se důvěřovat deklarovanému času podepsání
          - který je přebírán ze systémových hodin počítače



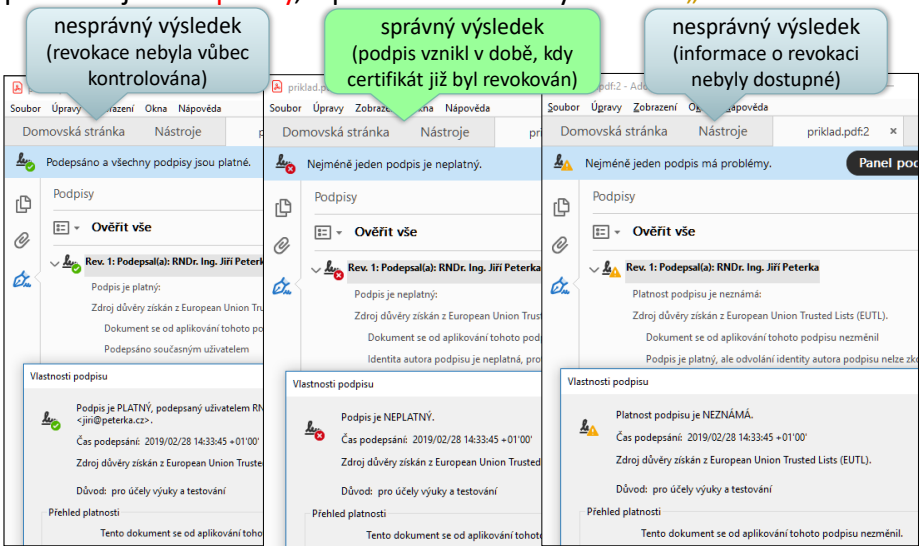
  - lze nastavit obsah úložiště důvěryhodných certifikátů
    - a tím určit, kterým certifikátům bude program důvěřovat
      - problematické u nekvalifikovaných certifikátů
      - pro kvalifikované certifikáty (z EU) vyřešeno vazbou na unijní seznam LOTL (resp. EUTL)

obsah úložiště nastavuje primárně Adobe, resp. Microsoft

3

odstrašující příklad

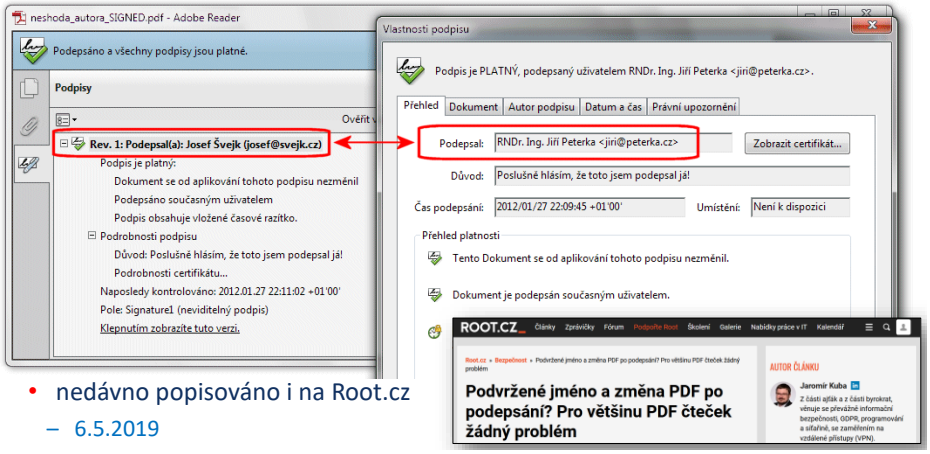
- Adobe Reader (i Acrobat) lze nastavit tak, aby stejný elektronický podpis na stejném dokumentu vyhodnotil jednou jako platný, podruhé jako neplatný, a potřetí skončil s výsledkem „nevím“



4

jiný problém: neshoda podepsané osoby

- při určitém nastavení Adobe Reader uvádí nesprávné jméno podepsané osoby
  - zobrazuje obsah položky Name (z podpisového slovníku), nikoli z certifikátu
    - děje se tak, pokud Reader el. podpisy nevyhodnocuje automaticky při otevírání dokumentu, ale až na žádost

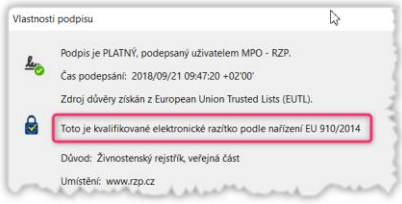


- nedávno popisováno i na Root.cz
  - 6.5.2019

5

jak poznat „český“ uznávaný el. podpis?

- problém:
  - zahraniční programy neznají tuzemskou legislativu, a tudíž nedokáží poznat (a uživateli správně indikovat) „české“ varianty el. podpisů a pečetí
    - uživatel si to musí vydedukovat sám (a musí vědět jak) !!!!
- příklad: Adobe Reader
  - pozná kvalifikovaný elektronický podpis a kvalifikovanou elektronickou pečeť
    - u pečeti nesprávně říká, že jde o „kvalifikované elektronické razítko“
      - při lokalizaci do CZ byl anglický termín „seal“ přeložen jako „razítko“ (místo „pečeť“)



  - nepozná „český“ uznávaný elektronický podpis
    - tj. „zaručený el. podpis, založený na kvalifikovaném elektronickém certifikátu“
      - je nutné „ručně“ ověřit, že certifikát je kvalifikovaný !!!

6

rozhodný okamžik (dle eIDAS)

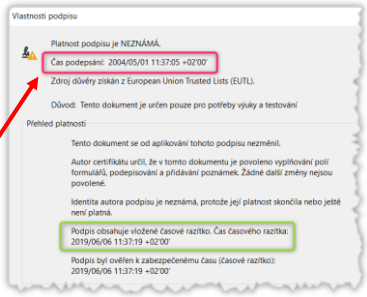
- aneb: okamžik, ke kterému se vyhodnocuje splnění podmínek pro platnost
  - to je naprosto klíčové pro správný výsledek ověření !!!

- dříve: postup ověřování byl popsán ve vyhlášce
  - vyhláška 212/2012 Sb. (zrušena k 19.9.2016)
    - ne úplně správně, ale nikoli chybně
      - *„… nejprve okamžik doručení, a když to nevychází tak okamžik z časového razítka …“*

správně by to bylo obráceně, protože časové razítko je starší

- nyní: postup ověřování platnosti předepisuje přímo nařízení eIDAS
  - říká: **rozhodný okamžik = okamžik podepsání**
    - článek 32 Nařízení: podmínky se ověřují *„k okamžiku podepsání“*

mají se ignorovat časová razítka?



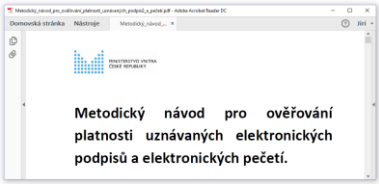
- ale to nejde aplikovat – nemá to smysl !!!
  - protože okamžik podepsání neznáme !!
    - přesněji: nějaký časový údaj k dispozici máme, ale nevíme, zda je správný – zda se na něj můžeme spoléhat
      - ale: systémové hodiny lze libovolně přetočit

7

metodický návod MV ČR

- připomenutí:
  - nařízení eIDAS (nesprávně) trvá na ověřování k okamžiku podepsání – který neznáme (dostatečně spolehlivě)
    - dodržení tohoto požadavku může vést k zásadním pochybením

- v ČR se snaží řešit (až, pouze) Metodický návod MV ČR
  - za okamžik vzniku elektronického podpisu MV doporučuje zvolit okamžik, kdy spoléhající se strana může prohlásit, že zaručený elektronický podpis již existoval:

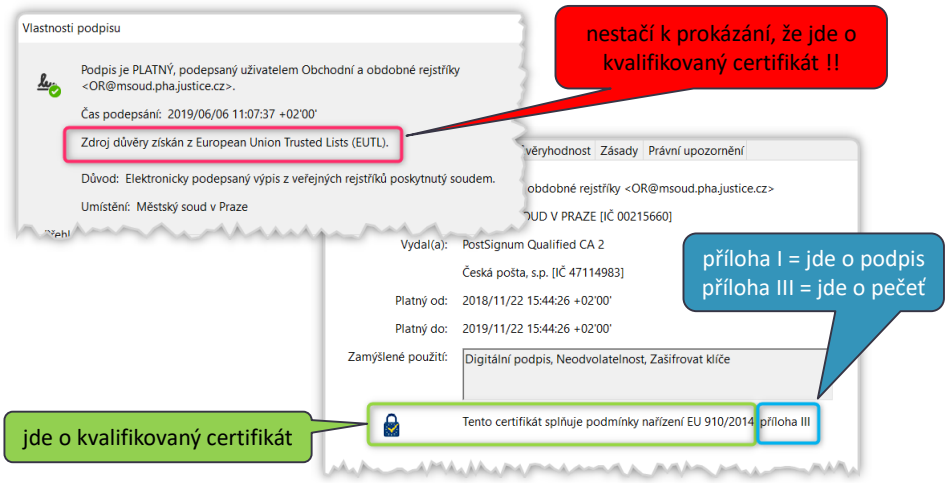


a) datum a čas doručení elektronicky podepsaného dokumentu nebo
b) nejčasnější časový okamžik, ve kterém již prokazatelně existoval zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, jehož platnost je ověřována (čas připojení důvěryhodného elektronického časového razítka, v případě existence více důvěryhodných elektronických časových razítek čas připojení nejstaršího z nich).

8

jak poznat „český“ uznávaný el. podpis/pečeť?

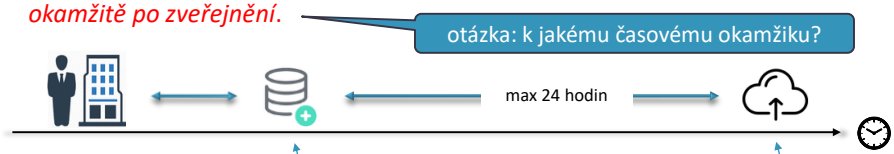
- uživatel si musí vše správně vydedukovat:
  - o jaký druh certifikátu se jedná
  - zda jde o podpis či pečeť
    - když nejde o kvalifikovanou el. pečeť, Adobe Reader to prezentuje jako podpis



9

ještě jeden problém z eIDAS-u

- jak rozumět čl. 24, odst. 3:
  - *Jestliže se kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty rozhodne určitý certifikát zneplatnit, zaeviduje toto zneplatnění ve své databázi certifikátů a zneplatnění certifikátu včas a v každém případě do 24 hodin od obdržení žádosti zveřejní. Zneplatnění nabývá účinku okamžitě po zveřejnění.*



- názor 1:
  - ke zneplatnění došlo k okamžiku zaevidování do databáze
  - důsledky:
    - \+ držitel začíná být chráněn dříve
    - \- spoléhající se strana by (někdy) měla čekat až 24 hodin
      - zda se nedozví o revokaci k dřívějšímu okamžiku (zaevidování do databáze)
- názor 2:
  - ke zneplatnění došlo k okamžiku zveřejnění
  - důsledky:
    - \- držitel začíná být chráněn později
      - rozdíl jsou v reálu jednotky sekund
    - \+ spoléhající se strana nemusí čekat

10

jiný problém: jednoznačná identifikace

- otázka:
  - chceme, aby elektronický podpis sloužil k (jednoznačné) identifikaci podepsané osoby?
    - slouží k tomu vlastnoruční podpis? viz podpis „Jan Novák“ — ale který Jan Novák?
  - ještě záleží na tom, zda chceme:
    - **aktuální identifikaci** — jako u úředně ověřených podpisů
      - kdy přímo z podpisu poznáme, o kterého konkrétního Jana Nováka jde
    - **potenciální identifikaci** — jako u vlastnoručních podpisů
      - aby v případě sporu existovala možnost, jak (dodatečně) zjistit, zda jde či nejde o podpis jednoho konkrétního Jana Nováka
        - u vlastnoručního podpisu: přes posudek písmoznalce (složité, drahé)
- odpověď:
  - pro kvalifikované / “české“ uznávané podpisy je **potenciální identifikace** možná:
    - jsou založeny na kvalifikovaném certifikátu
      - certifikační autorita, která vydala kvalifikovaný certifikát, zná identitu svého zákazníka (držitele certifikátu) zcela přesně
        - ví, o kterého Jana Nováka jde (musel se prokázat 2 osobními doklady)
      - jen tuto (detailní, konkrétní) informaci nedává do certifikátu !!!
        - soud se může autority zeptat !!!
  - pro **aktuální identifikaci** se nabízí:
    - atributové certifikáty
    - „legalizace el. podpisu“
      - koncept navržený v zákoně o právu na digitální služby

11

co je uvedeno v certifikátu?

- každý certifikát má své (jednoznačné) sériové číslo
  - podle něj se lze ptát u vydavatele (certifikační autority)
- kvalifikovaný certifikát
  - musí povinně obsahovat: jméno (ve smyslu: jméno, příjmení)
  - další údaje obsahovat může, ale nemusí
    - nesmí být po něm vyžadováno, aby je obsahoval !!!
      - například: emailová adresa, adresa bydliště, zaměstnavatel, funkce, ...
  - v ČR: další (možné) údaje určí MV ČR vyhláškou, půjde zřejmě o AIFO
- původně (zákon č. 227/2000 Sb. o el. podpisu)
  - certifikát vydaný v tuzemsku musí obsahovat *„údaje jednoznačně identifikující podepsanou osobu“*
    - v praxi: jde o IK MPSV (upřesňuje vyhláška 212/2012 Sb.)
- dnes: požadavek nařízení eIDAS (910/2014/ES), článek 32
  - při ověřování je spoléhající se straně *„řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu“*
    - žádný požadavek na IK MPSV apod.
    - výklad MV ČR: nejde o žádná „data navíc“ — stále je to jen „potenciální identifikace“
      - ale o ta, která již v certifikátu jsou (jméno, sériové číslo certifikátu, vydavatel, ….), a tato musí být spoléhající se straně řádně zobrazena

12

autorizované konverze

- původně se doložka opatřovala uznávaným el. podpisem či značkou
  - tj. nebyl nutný kvalifikovaný prostředek
- od 20.9.2016 zákon explicitně požaduje připojení kvalifikovaného podpisu či kvalifikované pečeti

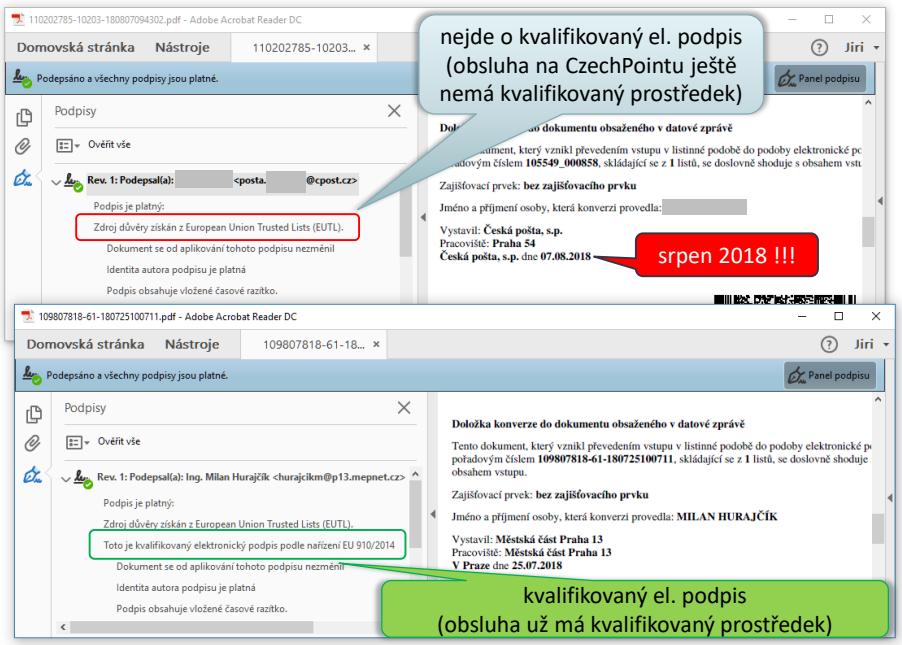
§ 25 zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi
Doložka
(1) Doložka konverze do dokumentu obsaženého v datové zprávě se považuje za součást výstupu a obsahuje
.....
h) kvalifikovaný elektronický podpis osoby, která konverzi provedla, nebo kvalifikovanou elektronickou pečeť subjektu, který konverzi provedl, byla-li konverze provedena automatizovaně.

- problém:
  - řada CzechPointů ani po 20.9.2016 neměla kvalifikovaný prostředek a nemohla opatřovat doložky kvalifikovaným podpisem !!!

výmluva: i na doložky se vztahovala 2-letá výjimka (§ 19 odst. 1 zákona č. 297/2016 Sb.):
„Po dobu 2 let ode dne nabytí účinnosti tohoto zákona lze k podepisování podle § 5 použít rovněž zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis“

13

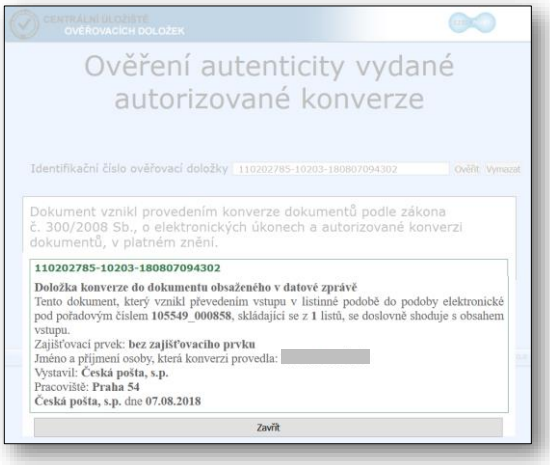
autorizované konverze



14

autorizované konverze

- konverzní doložky se evidují (archivují) a jsou veřejně dostupné



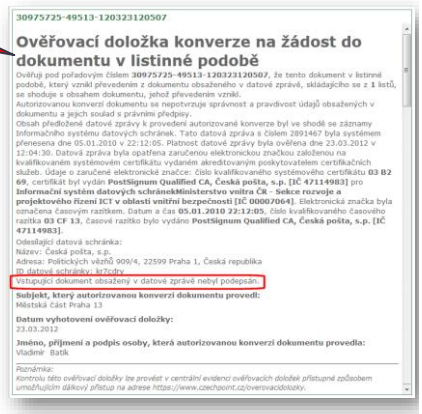
- ale:
  - nepozná se, k jakému dokumentu se vztahují
    - nezahrnují ani otisk (hash) el. dokumentu, ani určení jeho obsahu (čeho se týká)
  - doložka hovoří o počtu listů – ale (u listinného dokumentu): kolik měl stránek?

15

autorizované konverze

- zákon (do 19.9.2016) říkal:
  - konvertovat se dá pouze (platně) podepsaný el. dokument
    - „§ 24 odst. 4 písm. f) zákona č. 300/2008 Sb.: *Konverze se neprovádí … v případě provedení konverze na žádost, nebyl-li dokument obsažený v datové zprávě podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil ….*
  - přesto se konvertovaly i zcela nepodepsané el. dokumenty
    - pokud se „protáhly“ datovou schránkou
- od 20.9.2016
  - zákon byl upraven tak, aby el. dokument mohl být podepsán *„způsobem, se kterým jiný právní předpis spojuje při právním jednání vůči státu v souvislosti s výkonem jeho působnosti účinky vlastnoručního podpisu“*
    - tedy i pomocí tzv. fikce podpisu
      - ale nikdo nekontroluje, zda o fikci podpisu šlo !!

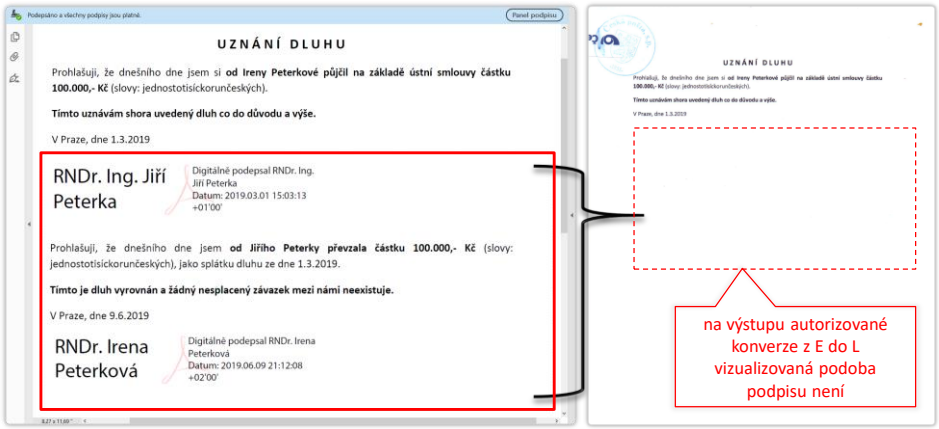
příklad z roku 2012



16

autorizované konverze

- problém s vizualizovanou podobou el. podpisů a pečetí
  - může to být jakýkoli obrázek, i takový který mění jeho význam či vyznění
  - otázka: má být vizualizovaná podoba podpisu/pečeti součástí listinného výstupu?
- realita: CzechPointy vizualizovanou podobu nekonvertují !
  - názor: a je to tak asi dobře (je to méně nebezpečná varianta)



17

celkový trend

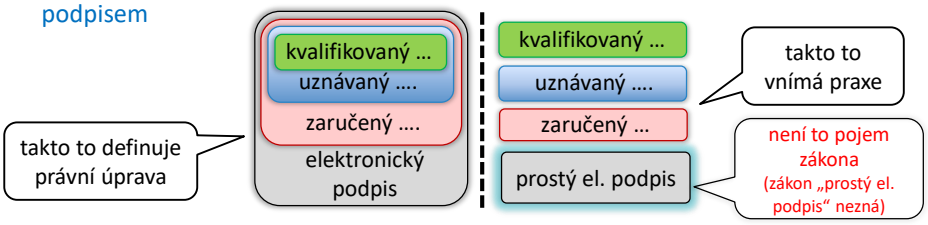
- „svět IT“:
  - trendem je zvyšování bezpečnosti
    - přihlašování:
      - přechod na vícefaktorovou autentizaci
    - podepisování:
      - používání „vyšších“ druhů elektronických podpisů
        - viz přechod od uznávaných el. podpisů ke kvalifikovaným
      - přechod na „dokonalejší“ hashovací funkce a větší klíče
      - .....
    - obecně:
      - používání antivirů, firewallů, VPN, ...
      - osvěta uživatelů
- „svět práva“:
  - snahy o zjednodušení, i za cenu obětování dosud vyžadovaných vlastností
    - ztráta prokazatelnosti, možnosti spoléhat se, možnosti „mít co zkoumat“
  - podepisování
    - snahy prosadit používání tzv. prostých elektronických podpisů
      - které nemusí mít vůbec žádné vlastnosti a schopnosti ....

Zákon č. 297/2016 Sb.
§ 7
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.

18

co jsou prosté elektronické podpisy?

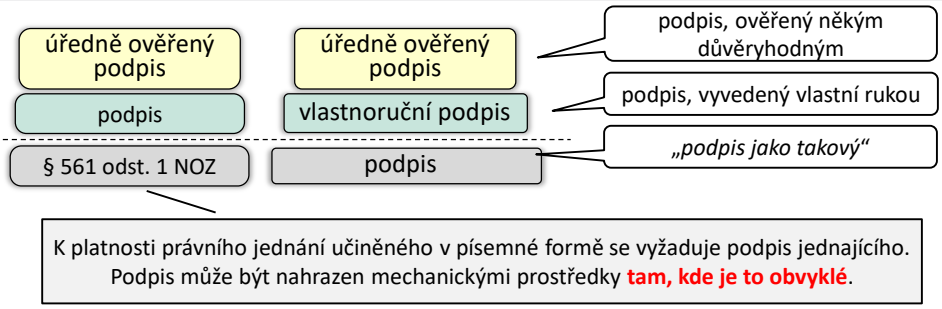
- je to „zbytková kategorie“ – pro jiné než kryptografické podpisy
  - podpis, který „je z nul a jedniček“, ale ještě není kryptografickým (zaručeným) el. podpisem



- nařízení eIDAS se touto kategorií nijak konkrétněji nezabývá:
  - neklade na ni žádné požadavky, nepřisuzuje jí žádné právní účinky
- nařízení eIDAS řeší jen „kryptografické“ elektronické podpisy
- názor:
  - nařízení nepředpokládá reálné používání jiných než kryptografických podpisů
  - ale u nás jsme si takovéto používání uzákonili
    - viz §7 zákona č. 297/2016 Sb.: v soukromoprávních vztazích lze používat i prosté el. podpisy (a důvodová zpráva jim dává účinky vlastnoručních podpisů !!!)

19

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*“ !!!
  - připomenutí: §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“

20

(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 ....

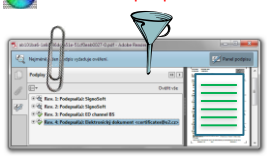
protože po nich není nic požadováno !!

21

příklad: dynamický biometrický podpis

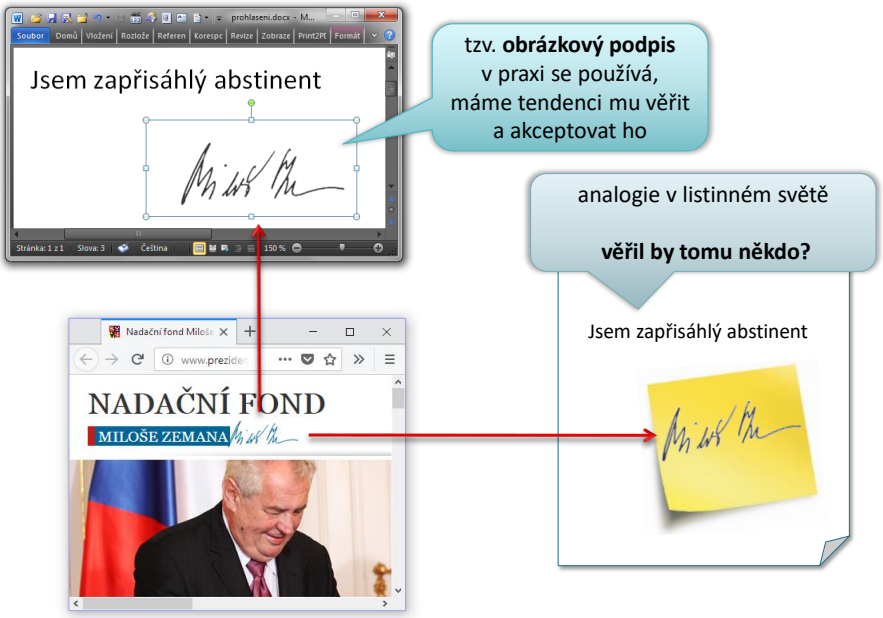
- vyhovuje definici prostého elektronického podpisu
  - je to vlastně „vzorek podepisující osoby“
    - podobně, jako otisk prstu, vzorek DNA (krev, sliny, ...), ...
  - získává se pomocí úkonu, který má charakter odběru
    - obdobně, jako odběr vzorku krve, vzorku slin, otisku prstů .....

- 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



22

příklad: „obrázkový“ el. podpis

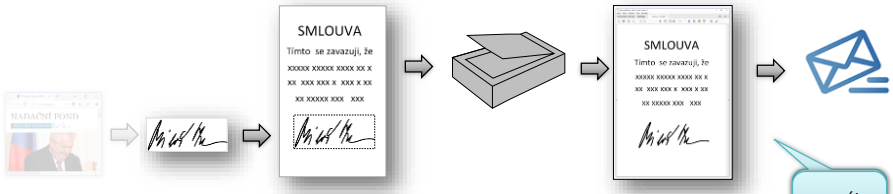


23

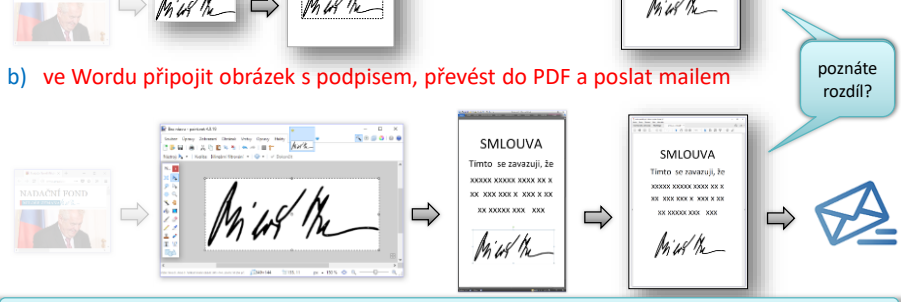
obrázkový podpis: příklad z praxe

- *… 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)

24

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?

25