Praktický pohled na elektronické podpisy a jejich fungování

Jiří Peterka

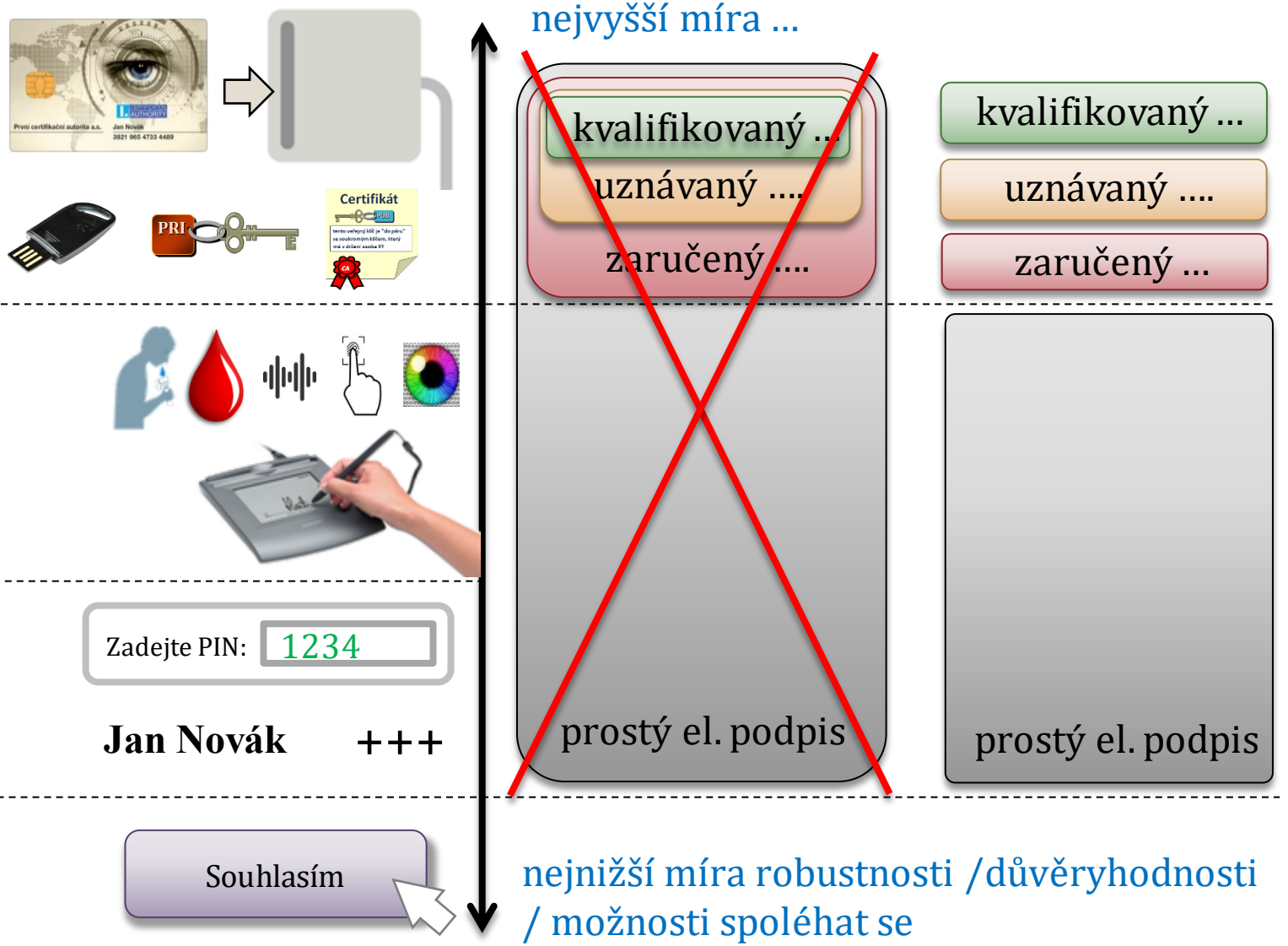
17.1.2018

Tuto prezentaci si můžete již nyní prohlížet (i stáhnout) na

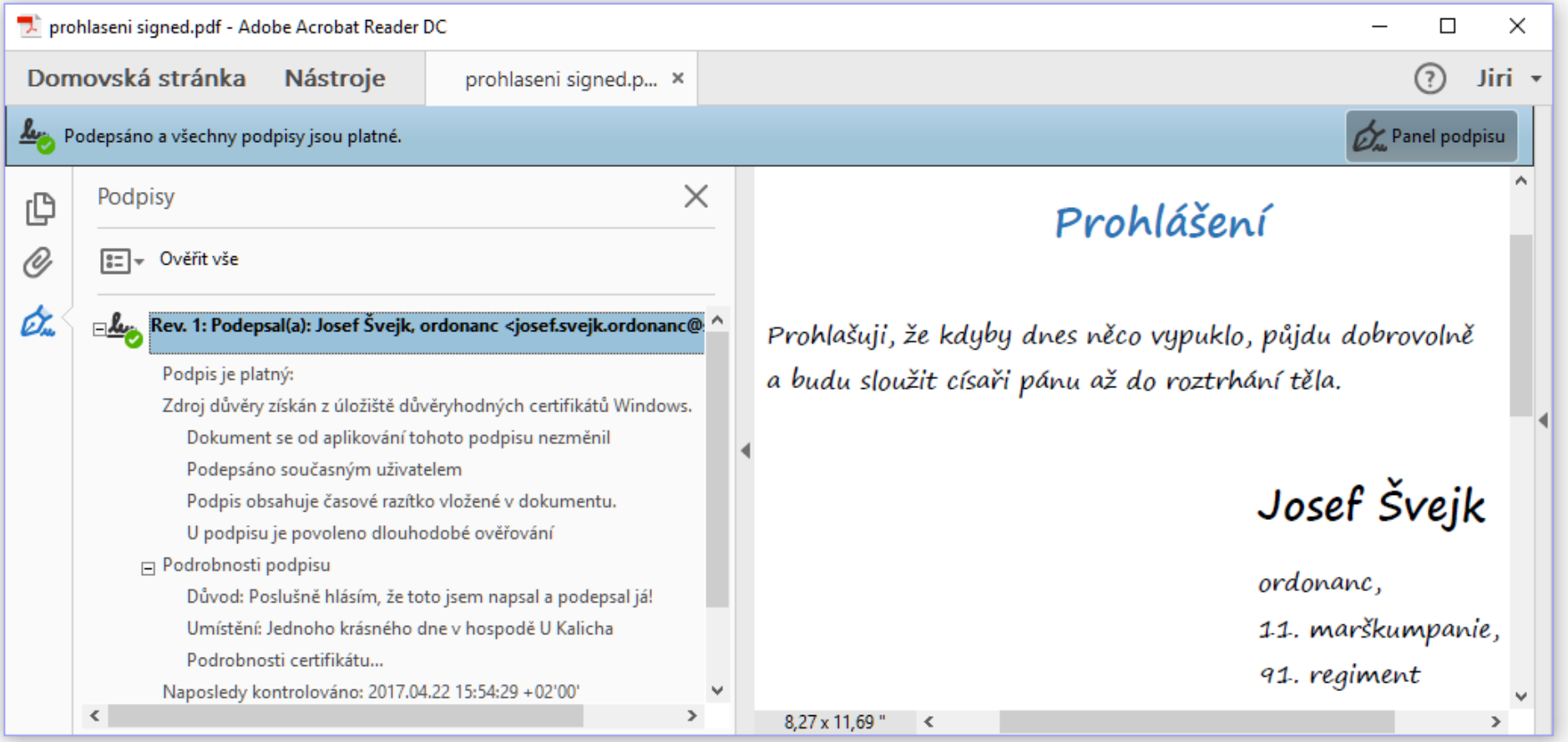
www.earchiv.cz/papers/p81

není (el.) podpis jako (el.) podpis

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

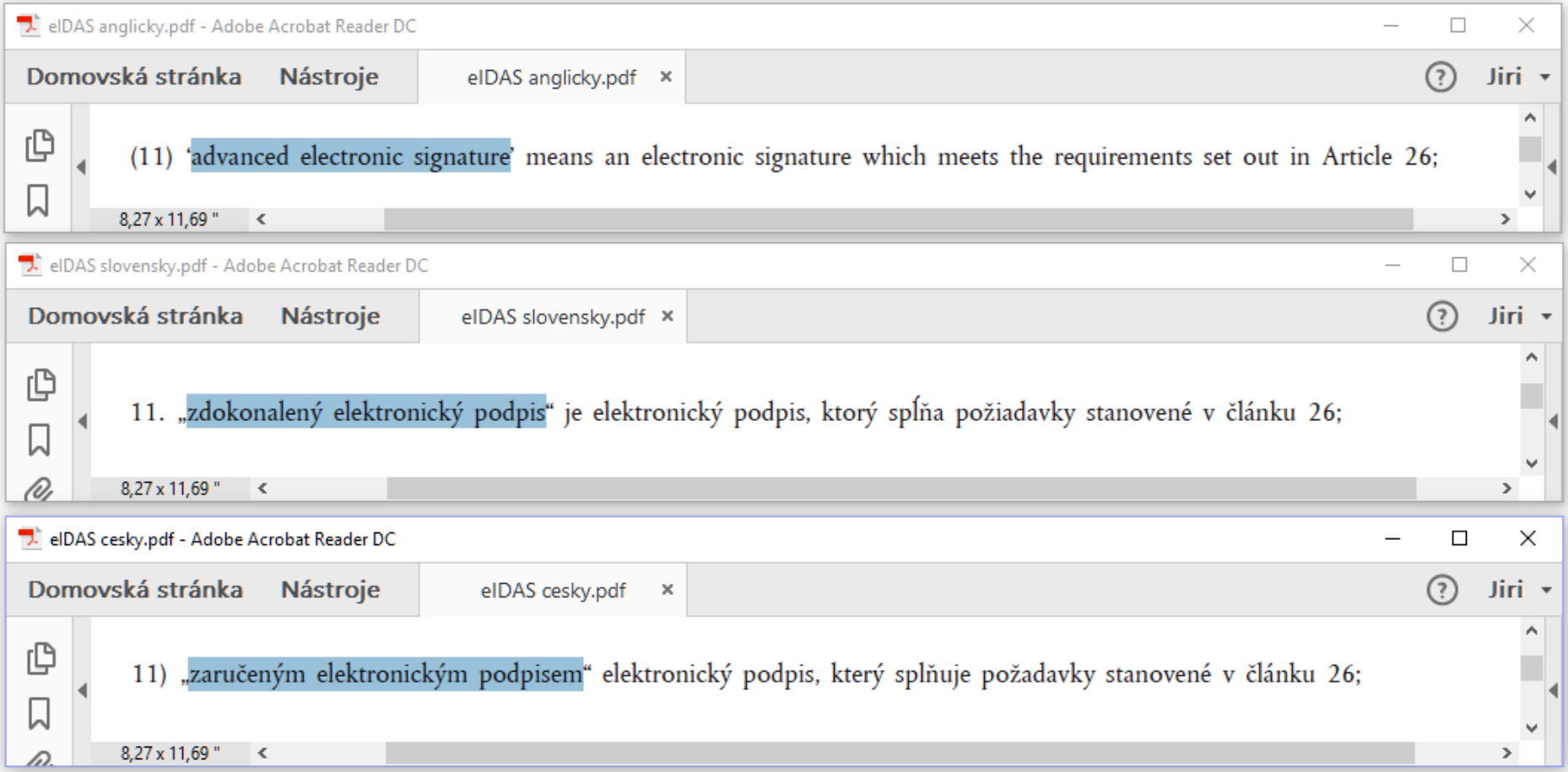


příklad zaručeného el. podpisu



- **pozor: zaručený el. podpis <u>nezaručuje</u> identitu podepsané osoby !!!**
  - formou zaručeného elektronického podpisu se lze (velmi snadno) podepsat za kohokoli jiného
  - zaručený podpis může „patřit“ i někomu, kdo vůbec neexistuje (jako fyzická osoba)
- **zaručuje pouze neměnnost (integritu) toho, co je podepsáno ....**

je to špatný překlad



- **„zdokonalený" (či: „pokročilý", „vylepšený") el. podpis není od toho, aby zaručoval identitu podepsané osoby**
  - od toho jsou „vyšší" varianty el. podpisu – uznávaný a kvalifikovaný el. podpis
- **je od toho, aby zajišťoval neměnnost (integritu) toho, co bylo podepsáno**

zaručený el. podpis dlouhodobě mate

- **mnoho lidí si stále myslí, že zaručený el. podpis zaručuje identitu podepsané osoby**
  - 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

proč zaručený podpis nezaručuje?

- **představa:**
  - zaručený el. podpis vzniká „semletím“ dvou ingredienci

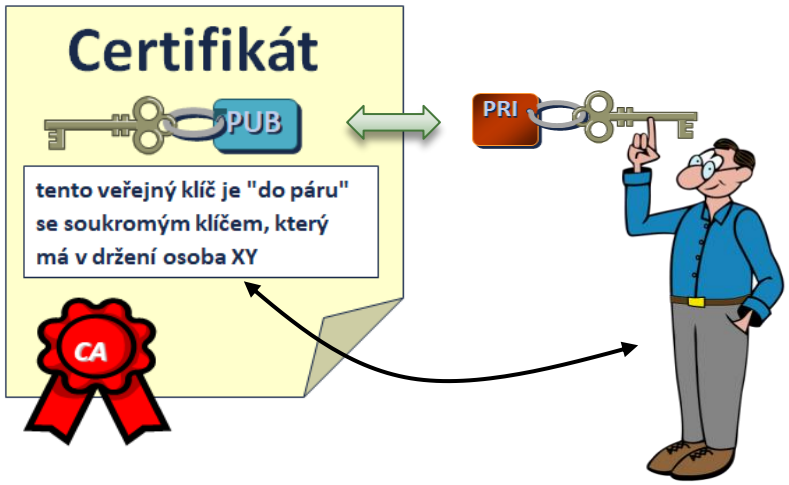
    1. podepisovaného dokumentu
       - tím se podpis stává závislým na tom, co je podepsáno
         - díky tomu dokáže chránit proti změně
       - díky tomu je zaručený el. podpis pokaždé jiný
         - a nelze ho připravit dopředu !!!
    2. soukromého klíče 

       - soukromý klíč je tím, co nemá nikdo jiný, co je specifické pro konkrétní podepisující osobu
       - soukromý klíč je „*tím, co činí můj podpis mým podpisem*“
- **realita:**
  - nevíme, kdo (třeba někde v soukromí) skutečně použil soukromý klíč (kliknul myší ...)
- **nastupuje právní fikce:**
  - podpis patří tomu (za podepsanou osobou považujeme toho), kdo prohlašuje soukromý klíče za svůj
- **certifikát = osvědčení o tom, komu soukromý klíč patří**
  - kdo ho prohlašuje za svůj

u zaručeného el. podpisu není kladen žádný požadavek na důvěryhodnost certifikátu !!!

proč zaručený podpis nezaručuje?

- **shrnutí:**
  - u zaručeného el. podpisu nám nezáleží na tom, od koho pochází osvědčení o vlastnictví soukromého klíče – v podobě certifikátu
    - akceptujeme jakýkoli certifikát, který mohl vydat kdokoli
      - i někdo, kdo nám lže a tvrdí něco, co není pravdou
    - může se jednat třeba i o testovací certifikát
      - jaký si může kdokoli vyrobit „na koleně“ a napsat si do něj, cokoli jen chce
        - viz příklad s literární postavou Josefa Švejka



- **pokud chceme mít jistotu (ohledně toho, komu podpis patří):**
  - musíme požadovat „dostatečně kvalitní“ (důvěryhodný) certifikát
    - takový, u kterého se můžeme spoléhat na správnost jeho obsahu
  - konkrétně tzv. **kvalifikovaný certifikát**
    - který může vydávat jen kvalifikovaná certifikační autorita, splňující požadavky zákona
      - dnes: **kvalifikovaný poskytovatel služeb vytvářející důvěru**
      - dnes v ČR: I.CA, PostSignum, eIdentity

pak už se jedná o **kvalifikovaný** (či **uznávaný**) **elektronický podpis**

kvalifikovaný statut

- **přívlastkem „kvalifikovaný“ se označuje to, čemu můžeme (musíme) důvěřovat / na co se můžeme spoléhat .... ze zákona (nařízení)**
  - svou důvěru odvozujeme ze zákona
  - máme:
    - kvalifikované služby (vytvářející důvěru)
      - např. kvalifikované služby elektronického doporučeného doručování
      - kvalifikované služby ověřování platnosti .... podpisů, pečetí
      - .....
    - kvalifikované poskytovatele (služeb vytvářejících důvěru)
      - dnes v ČR: I.CA, PostSignum., eIdentity, Software602
    - kvalifikované elektronické podpisy, kvalifikované elektronické pečeti
    - kvalifikované certifikáty
    - kvalifikovaná časová razítka
    - kvalifikované prostředky (pro vytváření el. podpisů)
    - .....

to, co je kvalifikované, má právo být označeno touto značkou

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

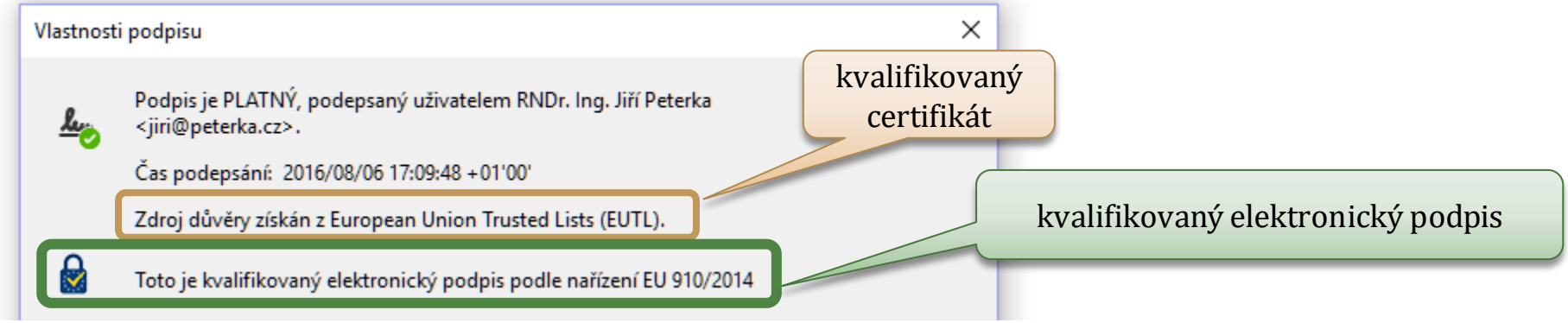
kvalifikovaný vs. uznávaný el. podpis

- **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

- **uznávaný el. podpis**
  - je naší národní specialitou, jinde neznají
  - 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

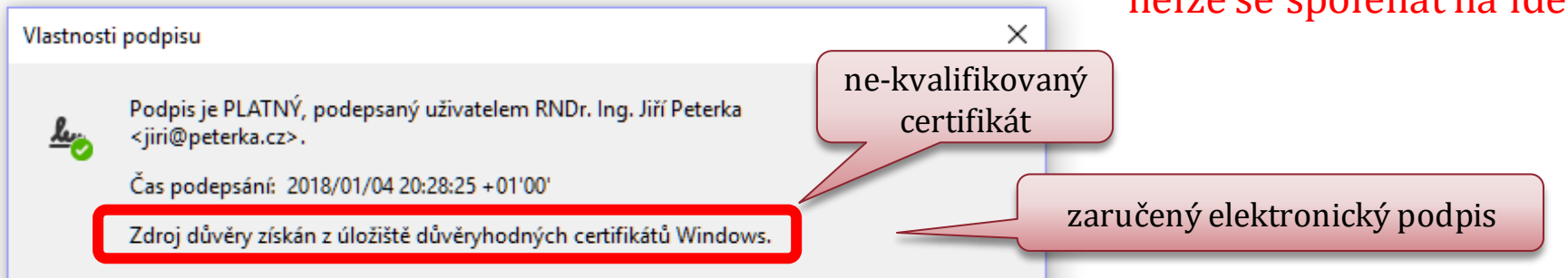
- **analogie s platebními kartami:**
  - kvalifikovaný el. podpis je jako platba u obchodníka / výběr z bankomatu:
    - je nutné mít kartu (fyzicky) - pokud vám ji neukradnou, je riziko zneužití malé ……
  - uznávaný el. podpis je jako on-line platba po Internetu
    - není nutné mít kartu (fyzicky),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

kvalifikovaný vs. uznávaný el. podpis



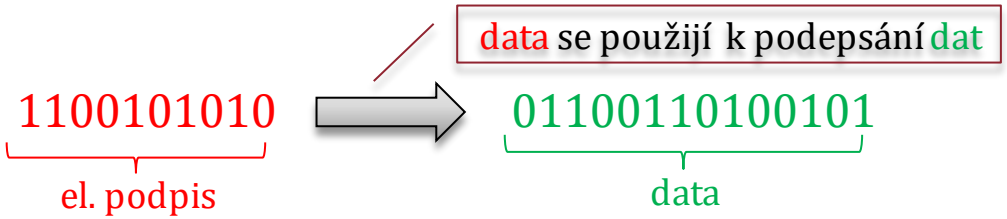
lze se spoléhat na identitu ..

nelze se spoléhat na identitu ...



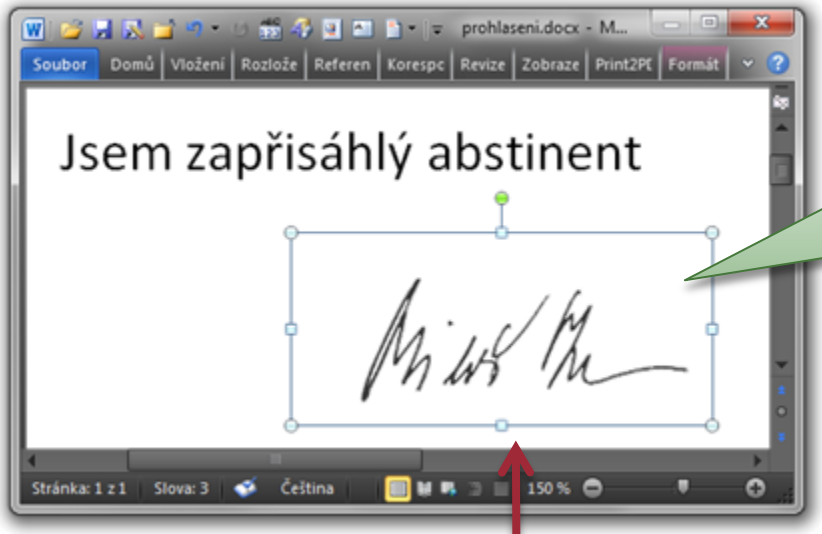
(prostý) elektronický podpis

- **původní definice v AJ (směrnice):**
  - data in electronic form which are attached to or logically associated with other electronic data and which **serve as a method of authentication**
- **původní definice (CZ zákon):**
  - údaje v elektronické podobě, které jsou připojené **k datové zprávě** nebo jsou s ní logicky spojené a které slouží jako **metoda k jednoznačnému ověření identity** podepsané osoby ve vztahu k datové zprávě
- **nová definice (nařízení, 2016):**
  - 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

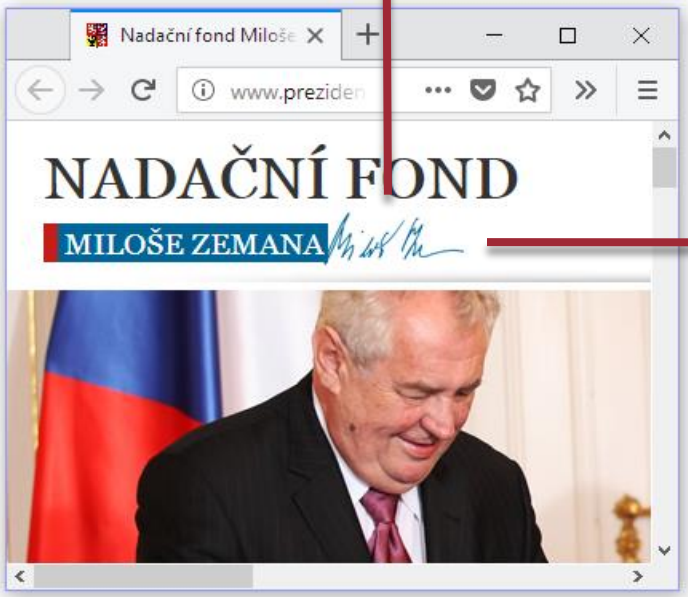


- **rezignuje na jakékoli požadavky**
  - **podpisem může to být cokoli elektronického (data)**
  - **nemluví se o žádném ověřování (či jen možnosti ověření) čehokoli !!!**
  - vazba mezi podpisem a podepsanými daty není specifikována (může být libovolná)

příklad prostého el. podpisu



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



analogie v listinném světě

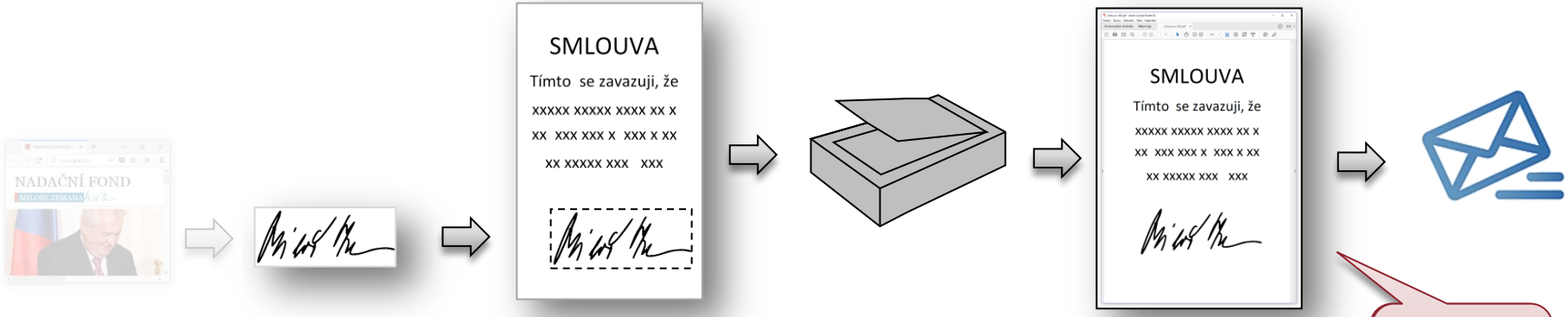
věřil by tomu někdo?

Jsem zapřisáhlý abstinent

obrázkový podpis: příklad z praxe

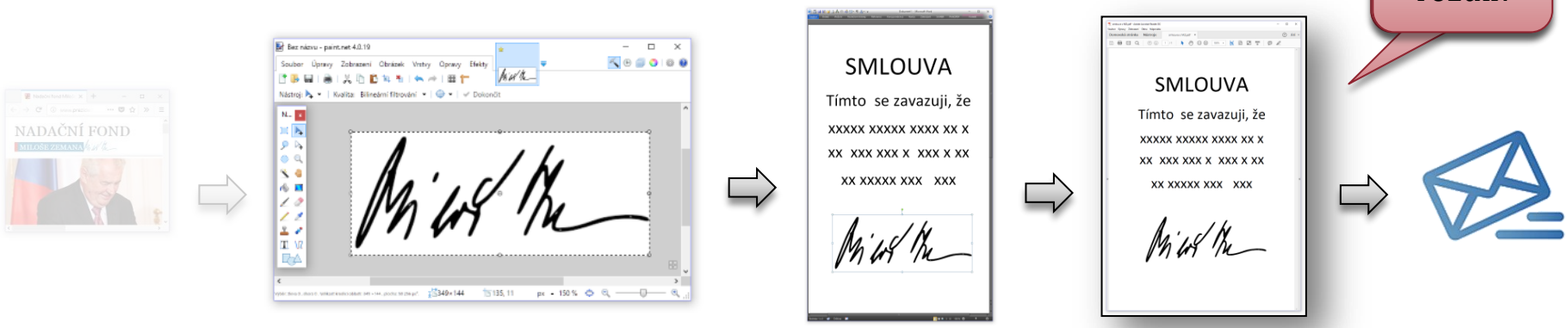
- ***… posílám návrh smlouvy ve Wordu …. prosím podepište, naskenujte a pošlete zpět mailem …..***

  - lze udělat různými způsoby:
    a) skutečně vytisknout, vlastnoručně podepsat, naskenovat (obvykle 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

poznáte rozdíl?



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

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?**

srovnání: vlastnoruční vs. prostý

- **vlastnoruční podpis**
  - není v zákonech definován
  - ale počítáme s tím, že:
    - každý se podepisuje +/- stejně
      - že různé podpisy téže osoby jsou (víceméně) stejné
        - aby se daly porovnávat na shodu
    - různé osoby se podepisují různě
      - vlastnoruční podpis je (nějak) charakteristický a individuální
        - aby se daly rozlišovat různé podepsané osoby
    - podpis je pevně spojen se substrátem (papírem) a nedá se od něj oddělit
      - „vpití inkoustu do papíru“ je nevratné
      - nejde „extrahovat“ podpis z jednoho listu papíru a přenést jej na jiný list papíru
    - nejde se podepsat dopředu (do zásoby) a pak podpis „aplikovat“ (nanést na papír)
      - ale dá se podepsat bianco šek

- **prostý elektronický podpis**
  - je definován v zákoně (nařízení eIDAS)
    - stejná osoba se může podepisovat různě
      - není požadováno, abych používal vždy stejný podpis
        - mohu měnit podpis například podle nálady

    - prosté podpisy různých osob mohou být stejné
      - není požadována žádná různorodost
      - extrém: všichni používají stejný podpis
        - viz „všichni jsme 1“
    - vazba mezi podpisem a „tím, co je podepsáno“ nemusí být pevná
      - může být i jen „logická“
        - (stejný) prostý podpis k podepsání více dokumentů/zpráv
          - podpis coby „jakákoli elektronická data“ lze replikovat (v libovolném počtu)
          - logická vazba může „vést“ od jednoho prostého podpisu k více dokumentům

    - lze se podepsat do zásoby (a pak aplikovat)

co říká nařízení a co náš zákon?

nařízení eIDAS

(nařízení 910/2014 EU)

- **účinky rovnocenné vlastnoručnímu podpisu má kvalifikovaný elektronický podpis**
  - a „cizí“ kvalifikovaný podpis z EU se bere stejně jako „domácí“

Článek 25
Právní účinky elektronických podpisů

2. Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.
3. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

adaptační zákon

(zákon č. 297/2016 Sb.)

- **účinky rovnocenné vlastnoručnímu podpisu mají (v soukromoprávních vztazích) všechny druhy elektronických podpisů**
  - tj. včetně prostého el. podpisu i zaručeného el. podpisu

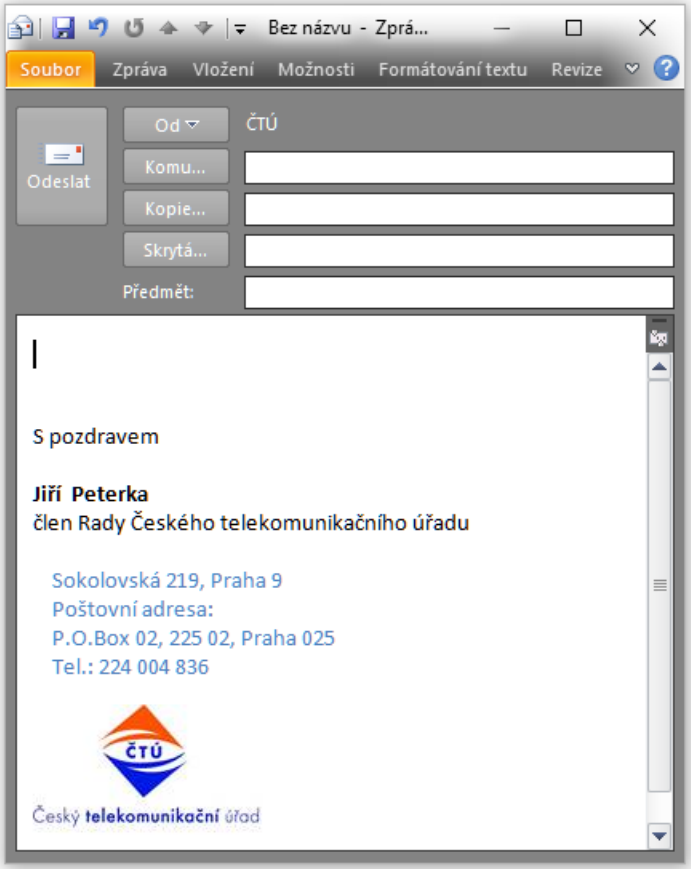
Podepisování dokumentu
§ 7
K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1.

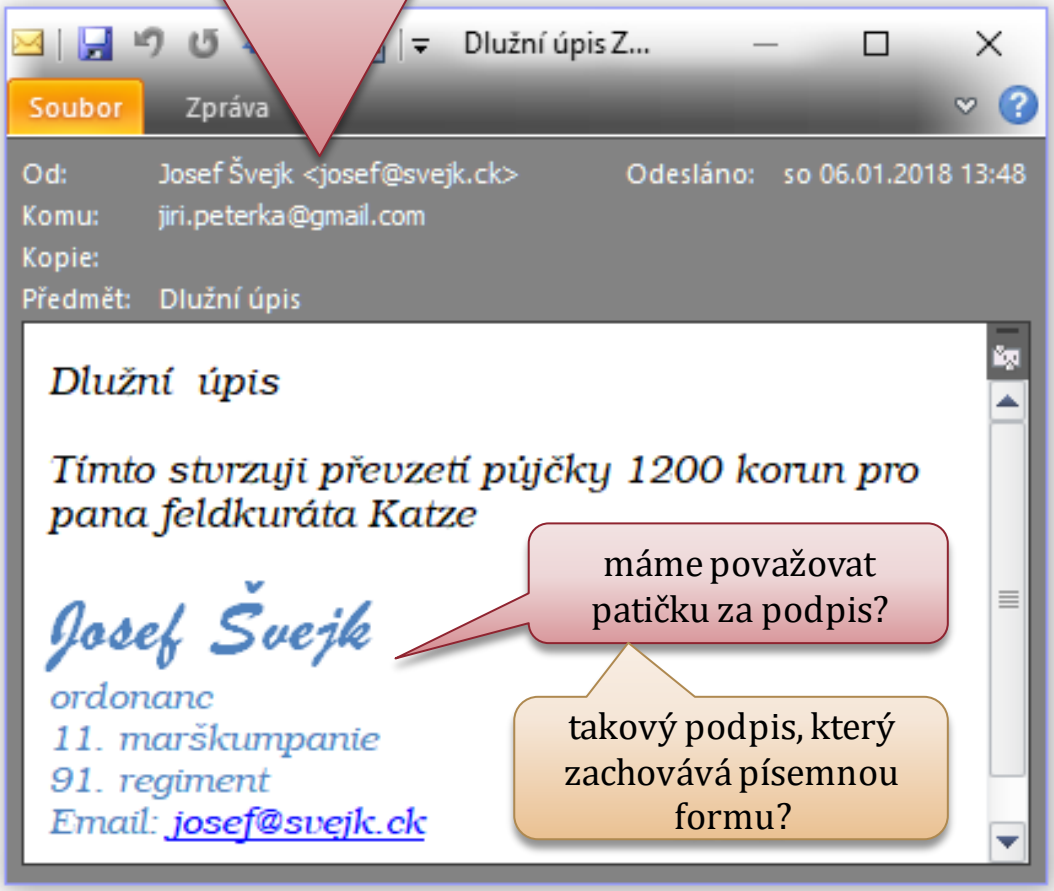
Zákon č. 297/2016 Sb.

další příklad – emailové patičky

- **emailová patička je „kus textu“, který vkládá sám poštovní program**
  - podle nastavení od uživatele
  - jde o informaci
    - která může/nemusí být pravdivá

na pravdivost údajů o odesilateli se nelze vůbec spoléhat (zfalšování – odeslání z libovolné adresy – je triviální)

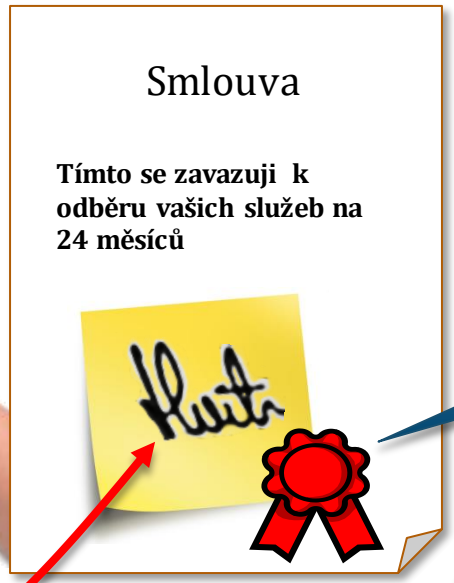




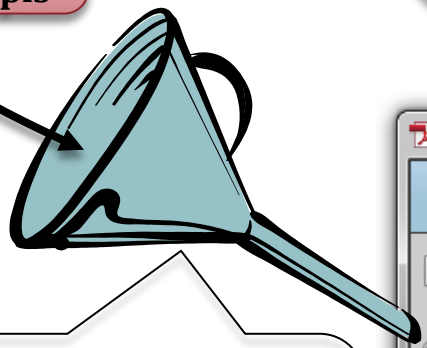
dynamické biometrické podpisy

odebraný „vzorek“ jedné smluvní strany - zákazníka

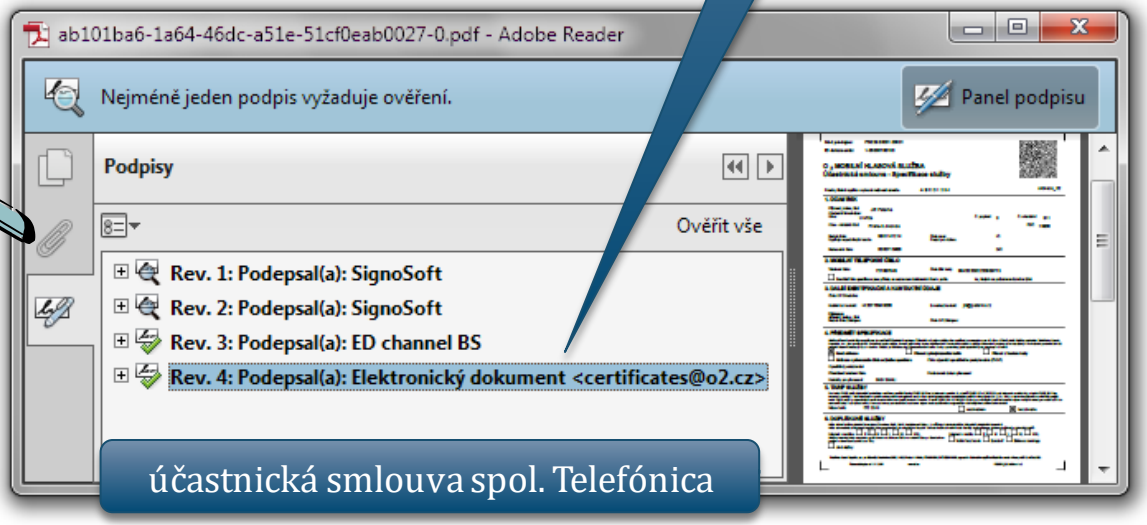
konkrétně tzv. **dynamický biometrický podpis**



uznávaný el. podpis (značka, pečeť) druhé smluvní strany - poskytovatele



odebraný vzorek (dynamický biometrický podpis) druhá smluvní strana přiloží k dokumentu a sama podepíše svým kvalifikovaným či uznávaným el. podpisem (značkou, pečetí)



účastnická smlouva spol. Telefónica

praxe dynamických biometrických podpisů

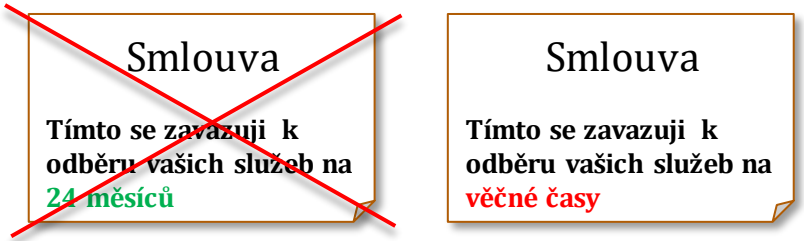
- **jsou využívány pro sjednávání dvoustranných smluvních vztahů**
  - typicky: pro uzavírání zákaznických smluv (zákazník – poskytovatel)
    - kde nevadí, že zákazník nemůže jednat sám (potřebuje na to druhou stranu)
- **zákazník nepodepisuje smlouvu, ale poskytuje vzorek „sebe sama“**

  - konkrétně vzorek svého podpisu
    - včetně „dynamické biometriky“ – rychlosti vedení pera, tlaku, ……
  - obdobně by mohl poskytovat jiné vzorky „sebe sama“, které reprezentují jeho individualitu




    - například (statická biometrika): otisk prstu, vzorek DNA (z krve, slin, ….), vzorek sítnice, …..
    - nebo (dynamická biometrika): vzorek své řeči, vzorek své chůze, …….

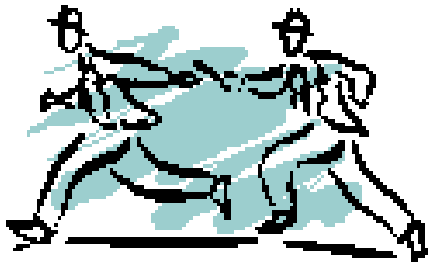
  - odběr vzorku v podobě dynamického biometrického podpisu má velkou přednost: **vytváří zákazníkovi iluzi, že podepisuje konkrétní dokument**
    - ve skutečnosti jen poskytuje vzorek sebe sama



- **nevýhoda / slabé místo / nebezpečí:**
  - manipulace s odebraným vzorkem není v moci jeho držitele (zákazníka)
    - záleží na korektnosti druhé strany, zda vzorek použije jen dohodnutým způsobem
      - že přiloží odebraný vzorek jen k jednomu dokumentu
      - jen k tomu dokumentu, který byl zákazníkovi předložen a se kterým zákazník souhlasí

problém škálování složitosti

- **realita světa IT:**
  - schopnosti výpočetní technicky (velmi) rychle rostou, užitek z toho mají obě strany
    - „hodná strana“: ti, kteří se chtějí chovat korektně, řádně podepisovat ….
    - „zlá strana“: ti, kteří chtějí podvádět, falšovat, prolamovat, chovat se nekorektně ……
  - je pouze otázkou času, kdy „zlá strana“ dokáže prolomit/zneužít/dešifrovat/napodobit řešení, aktuálně používané „hodnou stranou“
    - včetně takového napodobení, aby bylo nerozhodnutelné, zda jde o originál či padělek
      - týká se mj. i vlastnoručních podpisů
        - je pouze otázkou času, kdy umělá inteligence dokáže napodobit vlastnoruční podpis tak, že to nepozná ani sebelepší písmoznalec (a nebude to jeho vinou)
      - týká se i lidské řeči (viz pokroky v počítačové syntéze řeči)
- **důsledek:**
  - „hodná strana“ musí předbíhat „zlou stranu“ …. včas „přitvrzovat“
    - používat čím dál tím „silnější“ řešení, které je obtížnější (výpočetně složitější) prolomit/zneužít/dešifrovat ……



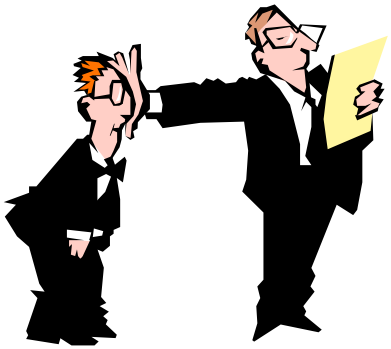
  - **řešení, založená na výpočtu, lze „přitvrzovat“ tak, jak je třeba**
    - kryptografie (zaručené el. podpisy) může používat stále větší klíče a stále sofistikovanější kryptografické algoritmy
  - **řešení, která nejsou založena na výpočtu, nelze „přitvrzovat“**
    - vlastnoruční podpisy ani lidskou řeč nejde „dělat složitějšími“
    - obecně jde o všechny prosté el. podpisy

problém vzájemné komunikace

- **Motto:**
  - elektronické podpisy mají mnoho úžasných vlastností, ale také jeden velký handicap: jsou značně mezioborovou záležitostí

- **vyžadují spolupráci lidí z různých oborů**
  - přinejmenším (v abecedním pořadí):
    - informatiky
    - kryptografie
    - práva

- **realita je taková, že dialog mezi lidmi z různých oborů „není ideální“**
  - řada aspektů kolem elektronických podpisů není kvůli tomu stále dořešena



- **problém je i s osvětou**
  - a celkovou vzdělaností nejširší populace

děkuji za pozornost

Jiří Peterka

jiri@peterka.cz
www.earchiv.cz

Tuto prezentaci najdete na

www.earchiv.cz/papers/p81