Jak podepisovat, pečetit a uchovávat elektronické dokumenty v praxi dle eIDAS

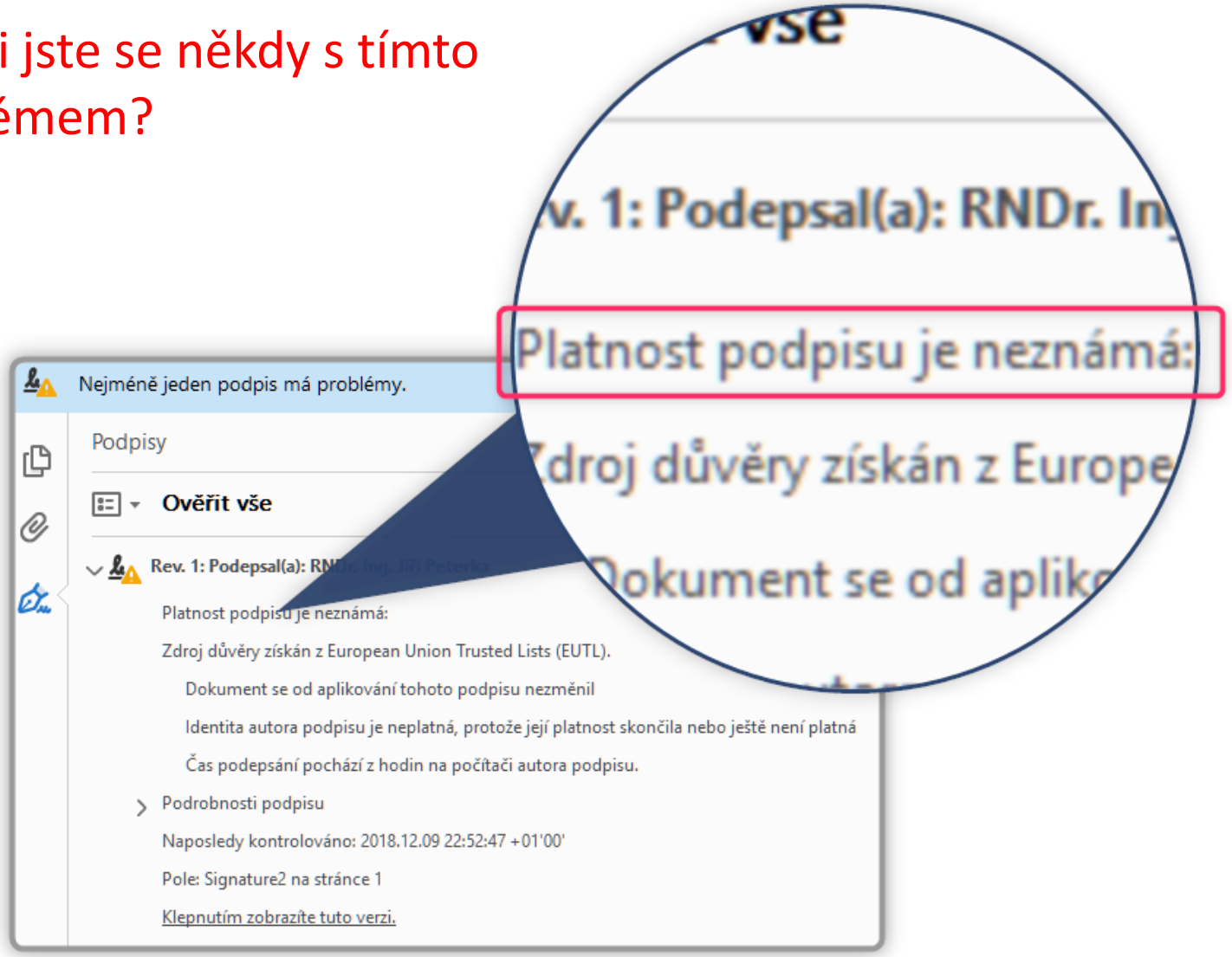
Jiří Peterka

Střelničná 1861/8a, Praha 8, 13.12.2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Motivace účastníků a Cíl semináře

setkali jste se někdy s tímto problémem?

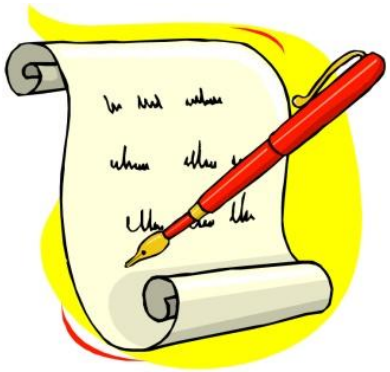


dnes se dozvíte, proč k němu dochází a jak mu předcházet

Osnova přednášky

- Blok 1: Podepisování a pečetění (9:00 – 11:00)
  - vymezení prvního rámce
  - kvalifikovaný statut (služeb, poskytovatelů, prostředků)
  - vlastnosti kvalifikovaných, uznávaných a zaručených elektronických podpisů a pečetí,
  - ověřování elektronických podpisů a pečetí
  - povinnosti OVM při el. podepisování a pečetění
  - povinnosti FO a PO (nejenom) při el. komunikaci s OVM
- Blok 2: Uchovávání elektronických podpisů a pečetí (11:15 – 13:00)
  - problém digitální kontinuity
  - koncept dlouhodobě ověřitelných podpisů (koncept LTV)
  - možné přístupy k dlouhodobému uchovávání el. podpisů a pečetí
  - praktické řešení:
    - ukázka uchovávání pomocí programu Adobe Acrobat Reader
    - pomocí kvalifikované služby pro uchovávání
    - pomocí Informačního systému datových schránek (ISDS)

Blok 1: Podepisování a pečetění



vývoj právní úpravy

- období 1999-2000:
  - evropská směrnice 1999/93/ES
    - *„o zásadách Společenství pro elektronické podpisy ….“*
  - v ČR transponována zákonem č. 227/200 Sb. o elektronickém podpisu
    - s významnou odchylkou/výjimkou:
      - *„ani pro nejvyšší formu el. podpisu (uznávaný el. podpis) nemusíme používat bezpečné prostředky“*
        - fakticky: certifikované čipové karty či USB tokeny
    - s postupem času se naše právní úprava vyvíjela
      - zavedení elektronických značek: novinka v rámci EU
    - prováděcí vyhlášky

„původní“ právní úprava

účinnost od 1.7.2016

účinnost od 19.9.2016

- období 2014-2016
  - **evropské nařízení 910/2014 (eIDAS)**
    - „o elektronické identifikaci a službách vytvářejících důvěru ……
    - v ČR i v ostatních členských zemích přímo účinné
      - relevantní pasáže účinné od 1.7.2016
    - (unijní) prováděcí předpisy
  - **„adaptační“ zákon (č. 297/2016 Sb.)**
    - zákon o službách vytvářejících důvěru
    - snaží se zachovat stejnou výjimku:
      - vyhnout se povinnosti používat výhradně bezpečné prostředky
        - pro jednání FO/PO vůči OVM: trvale
        - pro jednání OVM: na 2 roky
  - **změnový zákon (č. 298/2016 Sb.)**
    - tzv. tlusťoch

„nová“ právní úprava

co a kde hledat – v právním rámci

- nařízení eIDAS
  - co jsou elektronické podpisy (kvalifikovaný, zaručený, prostý)
  - co jsou elektronické pečeti (kvalifikované, zaručené, prosté)
  - co jsou elektronická časová razítka (kvalifikovaná, ….)
  - co jsou kvalifikované prostředky (QSCD, QSealCD)
  - co jsou kvalifikované služby vytvářející důvěru
    - pro ověřování platnosti elektronických podpisů
    - co je evropská značka důvěry
  - co jsou důvěryhodné seznamy
  - kdo jsou kvalifikovaní poskytovatelé služeb vytvářejících důvěru

- prováděcí předpisy k nař. eIDAS
  - referenční formáty elektronických podpisů
- adaptační zákon (297/2016 Sb.)
  - co jsou uznávané elektronické podpisy a uznávané elektronické pečeti
  - jaké druhy elektronických podpisů, pečetí a časových razítek mají používat OVM, jaké FO a PO (§5, §6)
  - kdy mají OVM podepisovat a kdy pečetit
  - kdy mají OVM připojovat časová razítka
- metodický pokyn MV ČR
  - jak volit rozhodný okamžik při ověřování platnosti

proč „o službách vytvářejících důvěru“?

- nařízení č. 910/2014 (eIDAS) se v angličtině jmenuje:
  - Regulation …. on electronic identification and trust services for electronic transactions in the internal market …..
- otázka:
  - jak vnímat (a jak přeložit) anglické „trust service“ ?
    - pozor: není to „trusted service“
      - „trusted service“ je důvěryhodná služba = to, čemu můžeme důvěřovat, co funguje důvěryhodným způsobem
        - sem patří např. spisové služby, měly by sem patřit nejrůznější informační systémy atd.
      - zjednodušeně: „trusted“ by mělo být všechno …..
    - ale: nařízení nemá ambice „řešit všechno“ (ani to nedělá)
      - také se (v angličtině) nejmenuje … *on trusted services* …., ale …. *on trust services* …..
- odpověď:
  - nařízení se zabývá jen službami, jejichž výstupem je *„něco, co nám umožňuje něčemu důvěřovat“* (například certifikáty)
    - *„něco, na čem zakládáme svou důvěru“*, resp. *„něco, z čeho odvozujeme svou důvěru“*

BTW: jak by se označovala služba, která nespadá pod eIDAS? Jako nedůvěryhodná?

proto: služby vytvářející důvěru

odbočení: 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
    - kvalifikované elektronické podpisy, kvalifikované elektronické pečeti, časová razítka
    - kvalifikované certifikáty
    - kvalifikované prostředky (pro vytváření el. podpisů a pečetí – QSCD a QSealCD)
    - ……

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, než ze zákona/nařízení
    - obvykle: z toho, kdo je poskytovatelem služby / vydavatelem certifikátu
      - například: důvěřujeme bance, u které máme peníze

není (el.) podpis jako (el.) podpis

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

řeší naše právní úprava

výpočet (kryptografie)

poskytnutí vzorku

poskytnutí/ /předání informace

Zadejte PIN: 1234

Jan Novák +++

úkon

Souhlasím

nejvyšší míra robustnosti /důvěryhodnosti / možnosti spoléhat se

kvalifikovaný …

uznávaný ….

zaručený …

prostý el. podpis

kvalifikovaný …

uznávaný ….

zaručený …

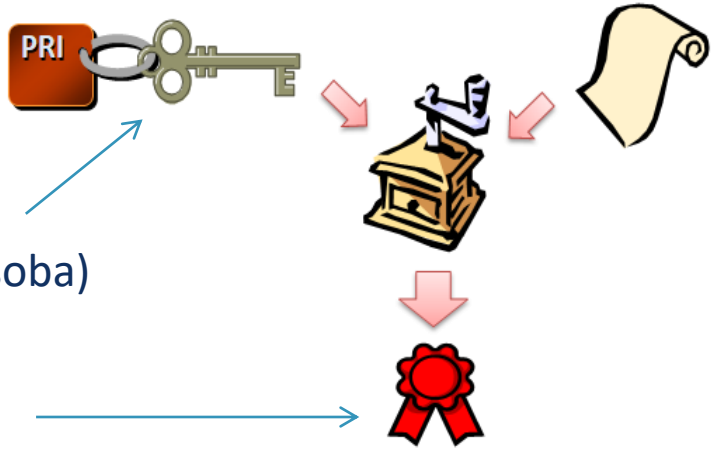
prostý el. podpis

nejnižší míra robustnosti /důvěryhodnosti / možnosti spoléhat se

kvalifikované, uznávané a zaručené ..

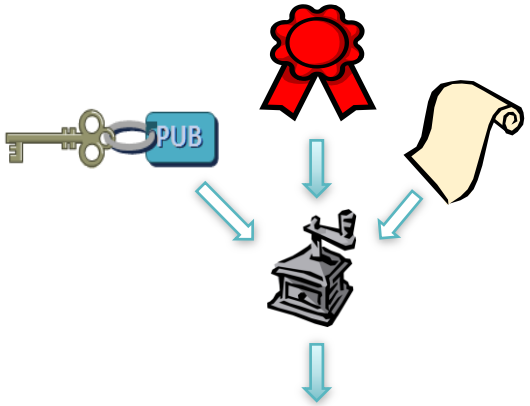
- v čem se shodují tyto druhy elektronických podpisů?
  - **jsou „kryptografické“**
    - tj. jsou založené na poznatcích a metodách matematiky (kryptografie)
      - hlavně: na asymetrické kryptografii
        - kvůli tomu se u nich pracuje s dvojicí klíčů – soukromým a veřejným

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



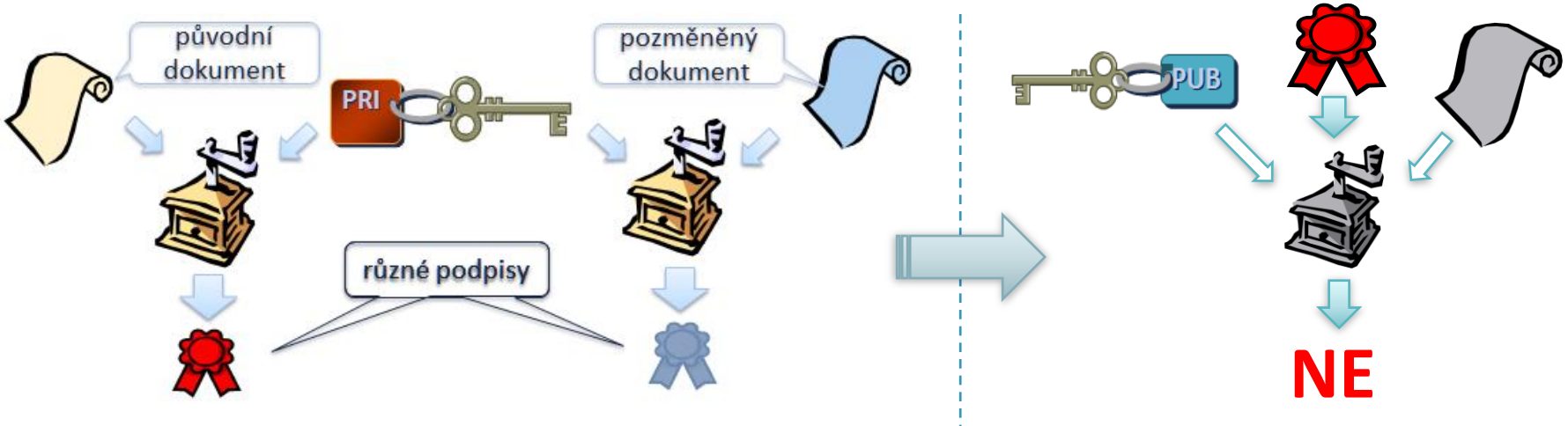
kvalifikované, uznávané a zaručené ..

- 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)



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

kvalifikované, uznávané a zaručené ..

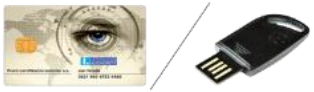
- v čem se liší tyto druhy elektronických podpisů?
  - v požadavcích na:

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

jeho obsah musí být pravdivý !!

jeho obsah nemusí být pravdivý !!

- způsob uložení soukr. klíče:
  - **kvalifikovaný** el. podpis
    - je vyžadován tzv. kvalifikovaný prostředek

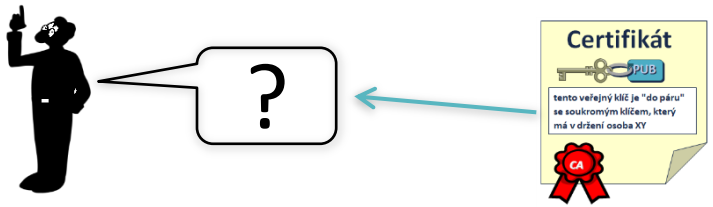


      - jak pro uchovávání klíče
      - tak i pro vytváření el. podpisů
  - **zaručený** a **uznávaný** el. podpis
    - není kladen žádný požadavek
      - soukromý klíč si držitel může uchovávat kde chce
        - je to hlavně otázka bezpečnosti

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

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 ….“

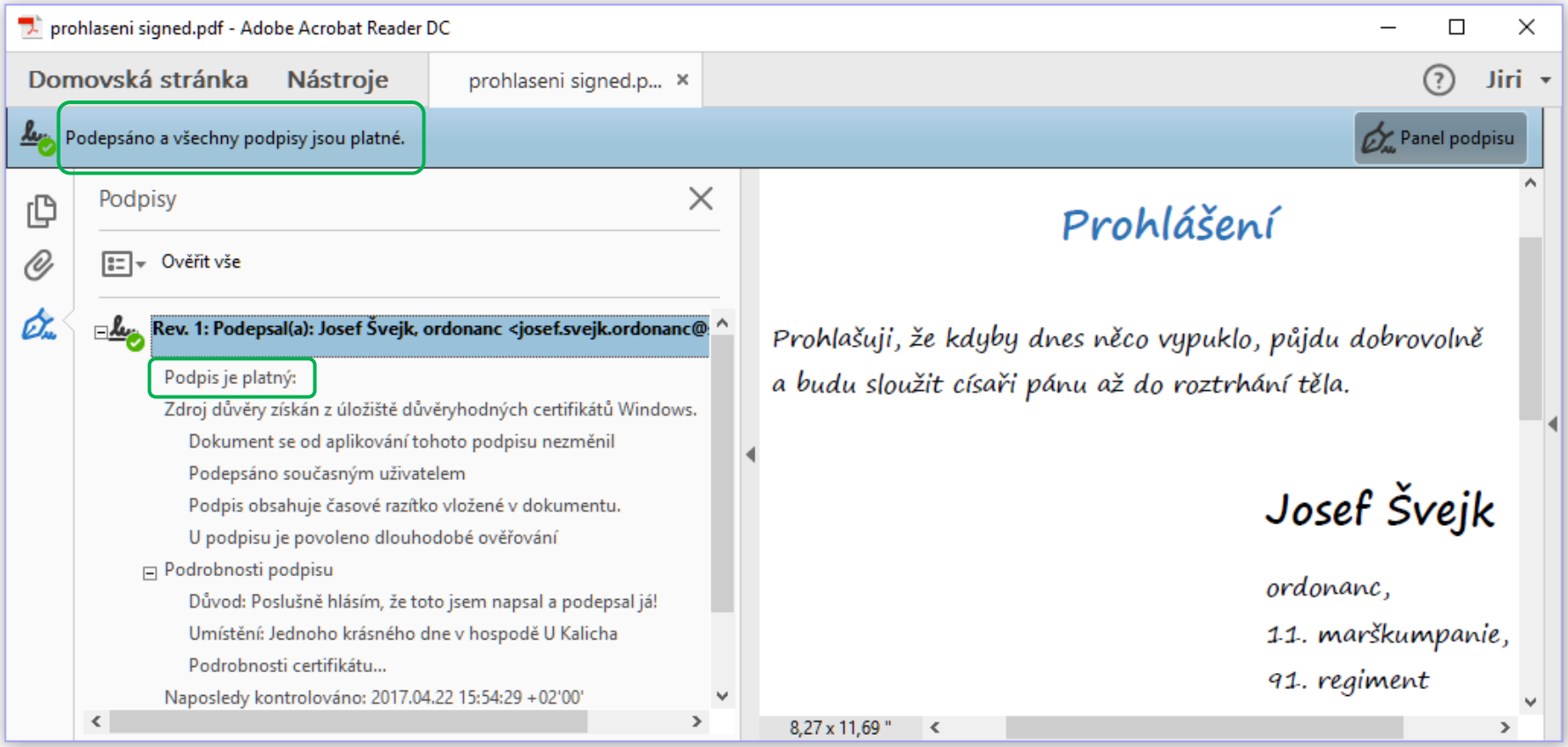
soukromý klíč musí být uložen v kvalifikovaném prostředku

soukromý klíč může být uložen kdekoli

certifikát může být jakýkoli

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

pravost vs. platnost podpisů (a pečetí)

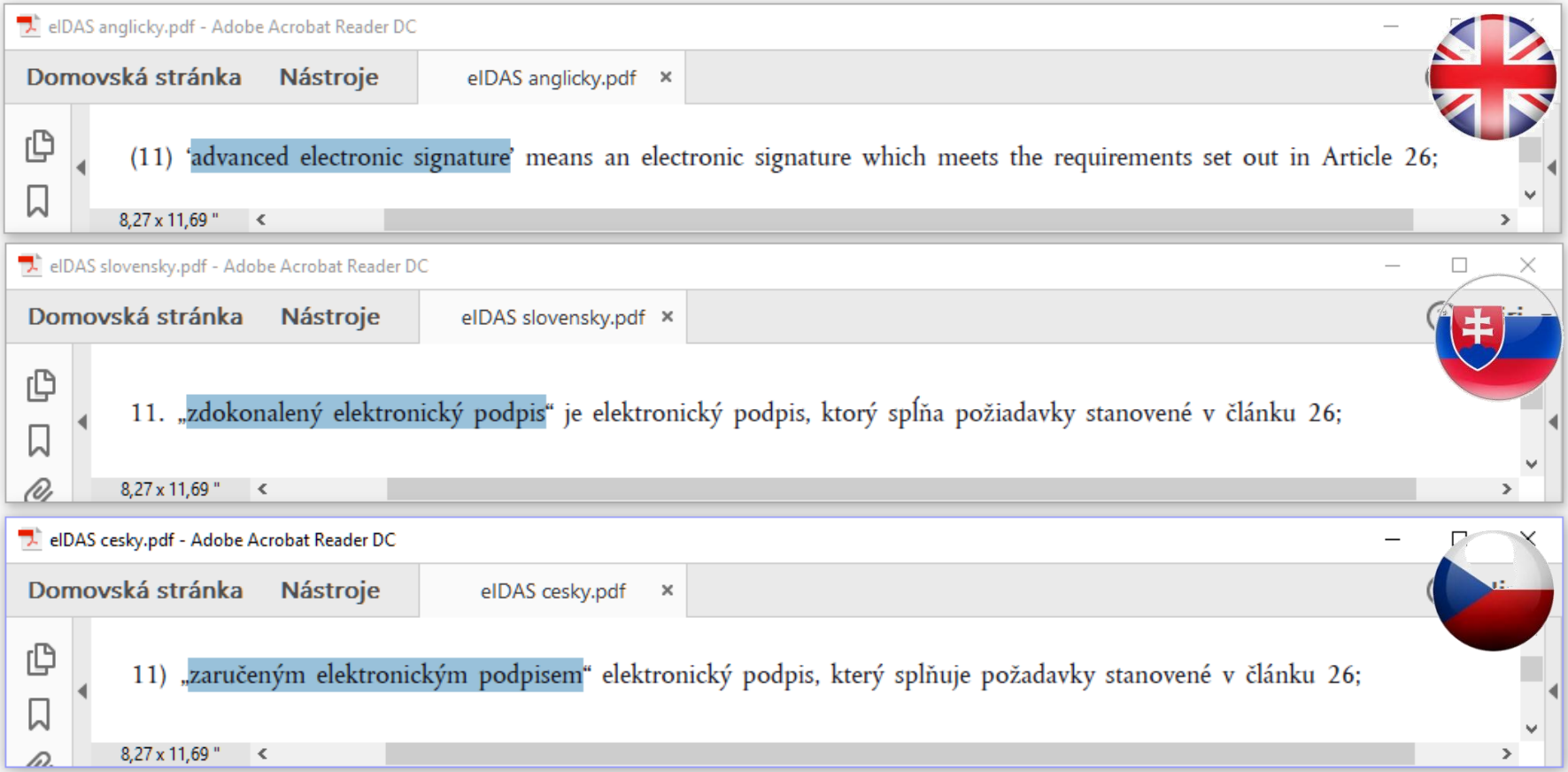
- „lidé od práva“ řeší pravost podpisů:
  - **podpis je pravý** = skutečně jej vytvořila příslušná osoba
    - ta osoba, která je prezentována jako podepsaná osoba
  - „pravost podpisu“ je právní pojem

- 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 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 (a pečetí)
  - **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

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

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.*

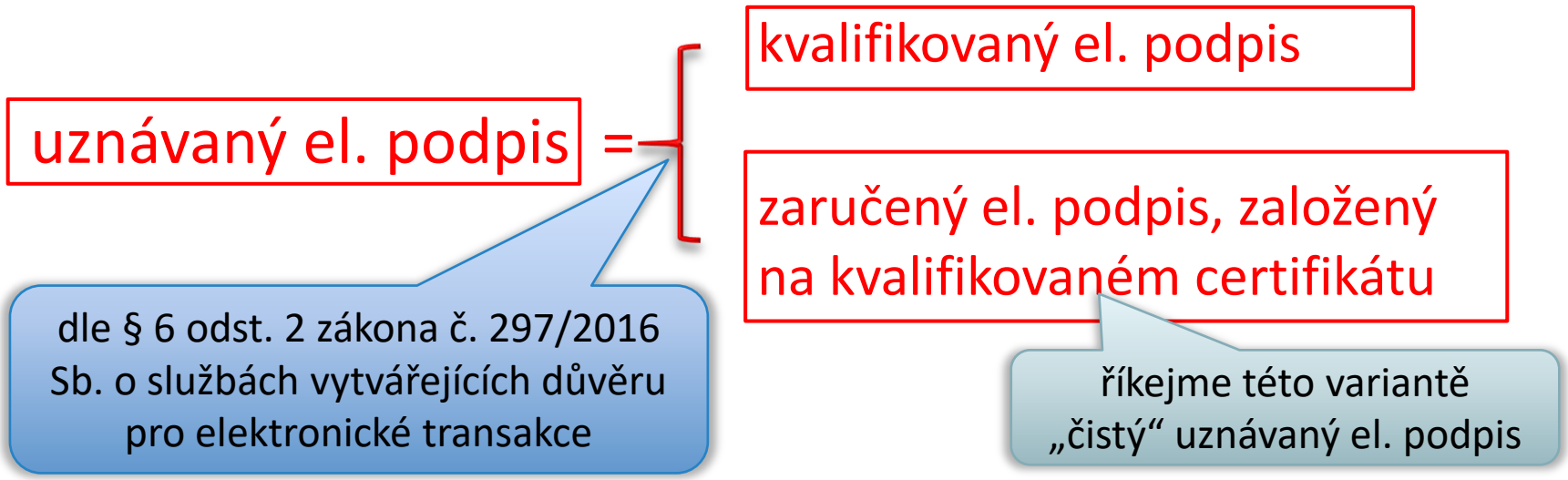
od 1.7.2012: podepsané **uznávaným**

  - 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

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“



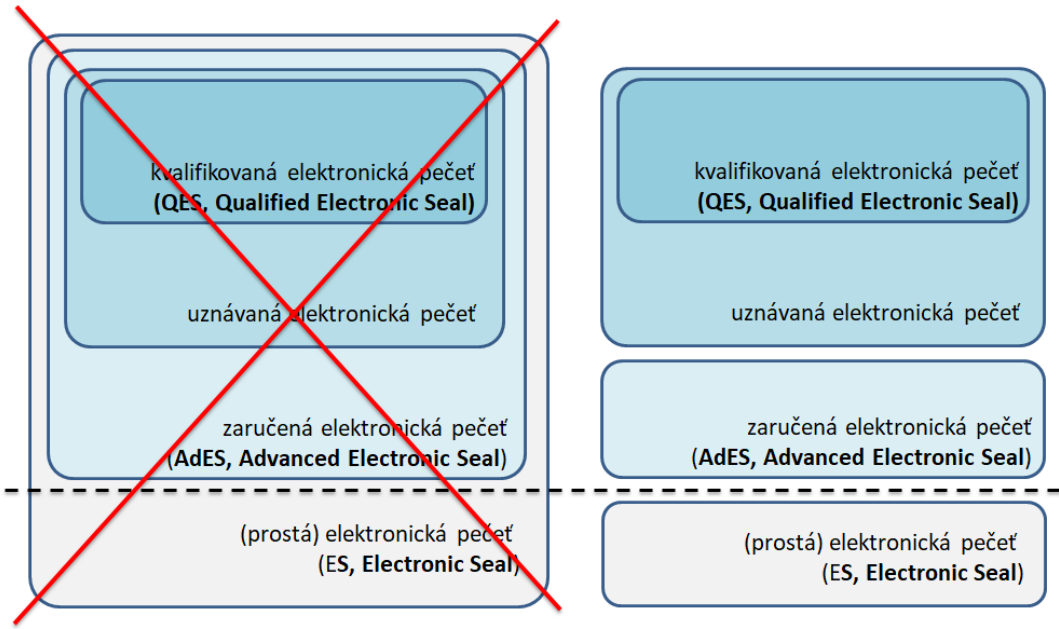
- značně to komplikuje vyjadřování o uznávaných el. podpisech
  - správně by vždy mělo být indikováno, o kterou variantu jde
- úmluva (pro potřeby tohoto semináře – ale i pro běžnou praxi):
  - když budeme říkat „*uznávaný elektronický podpis*“, budeme mít na mysli variantu „*zaručený el. podpis, založený na kvalifikovaném certifikátu*“

co jsou elektronické pečeti?

- nový koncept, zavedený nařízením eIDAS
  - inspirovaný našimi elektronickými značkami – ale trochu jiný
- základní princip:
  - fyzické osoby se podepisují (používají el. podpis)
    - jde o projev vůle fyzické osoby
  - právnické osoby pečetí (používají el. pečeti)
    - nejde o projev vůle, ale o vyjádření původu a integrity (neměnnosti)

důležitý důsledek: pečeť lze přidat jen na něco vlastního (čeho jsem původce) !!!

  - obdobně jako u podpisů platí, že:
- není pečeť jako pečeť !!
  - existuje jich celá hierarchie



podpisy vs. pečeti

- po technické stránce se nijak neliší …..
- liší se po právní stránce:

vytváří se vždy „ručně“

vytváří se buď „ručně“, nebo strojově

– **elektronické podpisy**
  - vytváří je pouze fyzické osoby
    - jde o **podepisující osoby**
  - jde o projev vůle fyzické osoby
    - lze podepisovat i cizí dokumenty
  - jsou založeny na certifikátech pro elektronický podpis
    - jde o osobní certifikáty
  - kvalifikované podpisy vyžadují kvalifikované prostředky (QSCD)
    - pro vytváření elektronických podpisů
  - „uznávaný“ elektronický podpis je legislativní zkratkou, pro
    - kvalifikovaný elektronický podpis
    - zaručený elektronický podpis, založený na kvalifikovaném certifikátu

– **elektronické pečeti**
  - vytváří je pouze právnické osoby
    - jde o **pečetící osoby**
  - jde o vyjádření původu
    - pečetit lze pouze vlastní dokumenty
  - jsou založeny na certifikátech pro elektronické pečeti
    - jde o certifikáty „pro organizaci“
  - kvalifikované pečeti vyžadují kvalifikované prostředky (QSealCD)
    - pro vytváření elektronických pečetí
  - „uznávaná“ elektronická pečeť je legislativní zkratkou, pro:
    - kvalifikovanou elektronickou pečeť
    - zaručenou elektronickou pečeť, založenou na kvalifikovaném certifikátu

co je kvalifikovaný prostředek?

- přesněji:
  - kvalifikovaný prostředek pro vytváření elektronických podpisů
    - zkratkou **QSCD** (Qualified Signature Creation Device), případně **QSigCD**
      - existují též kvalifikované prostředky pro vytváření elektronických pečetí (**QSealCD**)
- je to „zařízení“:

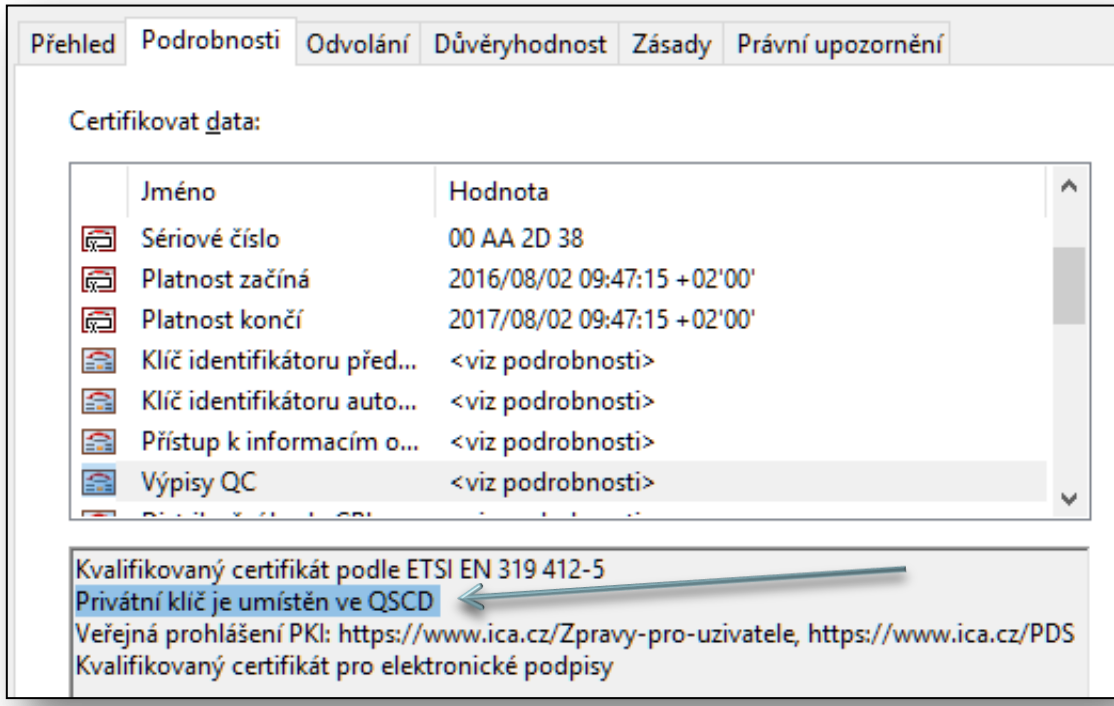
nejčastěji čipová karta či USB token, ale může být například i mobilní (v chytrém telefonu)

  - pro uchovávání soukromých klíčů a certifikátů
    - bez možnosti exportu soukromého klíče
      - bez možnosti „dostat ho ven“
  - pro vytváření elektronických podpisů
    - jelikož soukromý klíč nemůže prostředek opustit, musí podpisy vznikat také uvnitř prostředku
      - „kafemlýnek“ je zabudován přímo v prostředku
  - které je certifikované
    - někdo (k tomu oprávněný) zkontroloval, že prostředek funguje tak jak má
      - že splňuje požadavky zákona (nařízení eIDAS) a technických standardů

QSCD jsou i nové eOP

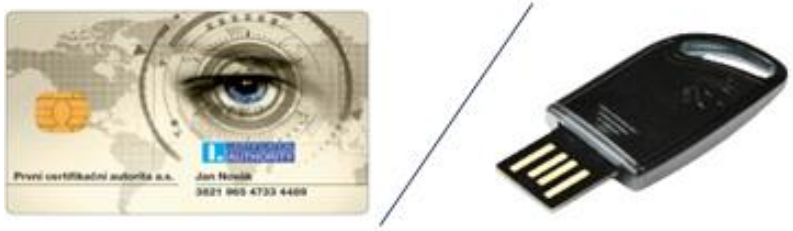
ad kvalifikovaný prostředek (QSCD)

- je zde určitý rozpor:
  - nařízení eIDAS (článek 3, bod 12) požaduje:
    - aby kvalifikovaný el. podpis *„byl vytvořen pomocí kvalifikovaného prostředku“*
  - ale zatím jsme požadovali něco jiného:
    - aby soukromý klíč *„byl uložen (umístěn) na kvalifikovaném prostředku (QSCD), bez možnosti dostat ho ven …..“*
- realita je ještě jiná:
  - aby el. podpis byl kvalifikovaný, musí mít (jeho) kvalifikovaný certifikát nastaven příznak uložení soukromého klíče na QSCD
  - vydavatel certifikátu (autorita) nastaví příznak jen tehdy, pokud má jistotu, že soukromý klíč byl vygenerován přímo v QSCD !!!
    - nikoli dodatečně importován



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**
  - naše národní specialita, 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

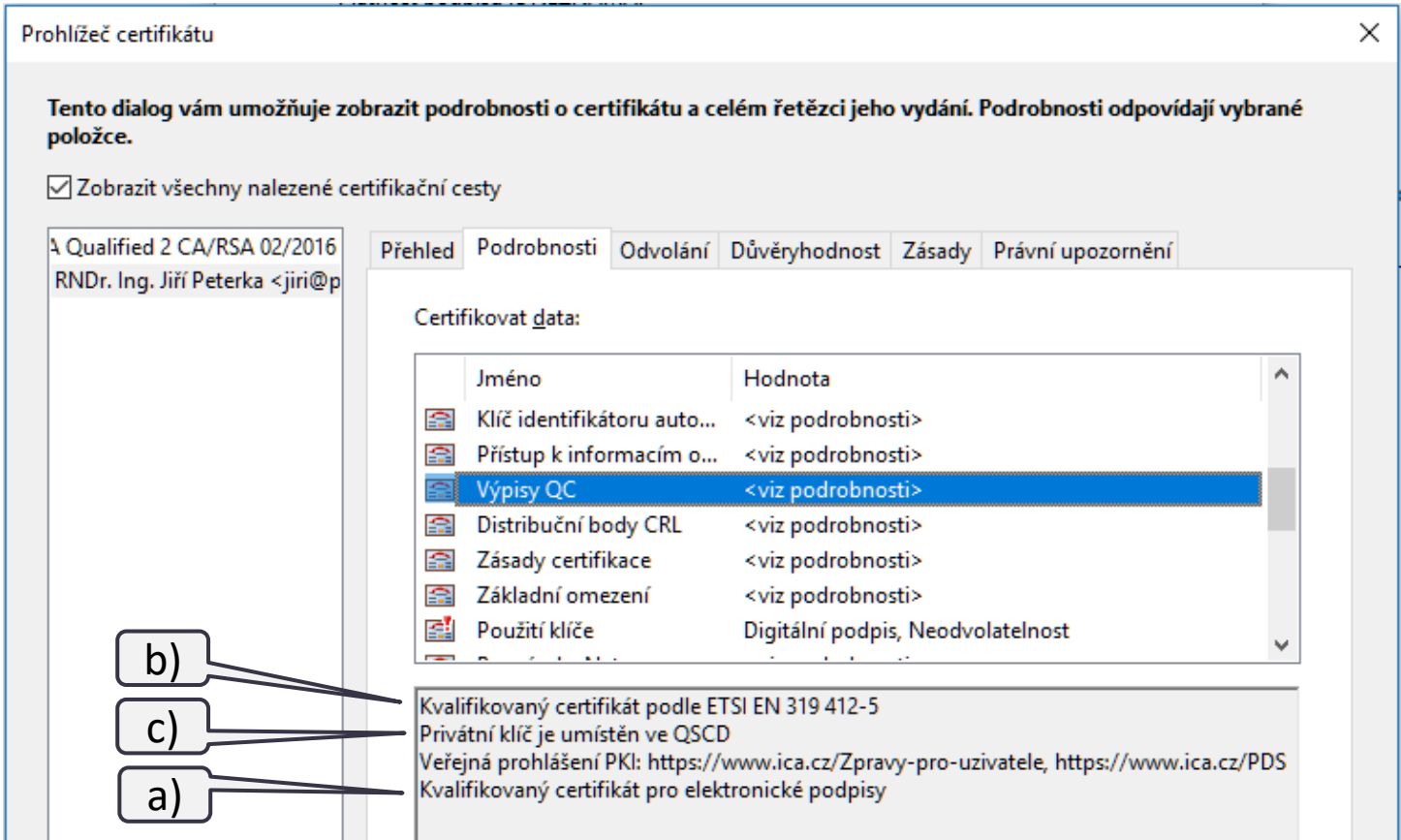
- analogie s platebními kartami:
  - kvalifikovaný el. podpis je jako platba u obchodníka / výběr z bankomatu:
    - je nutné mít kartu (fyzicky) - pokud vám ji neukradnou, je riziko zneužití malé
  - uznávaný el. podpis je jako on-line platba po Internetu
    - není nutné mít kartu (fyzicky), stačí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

jak poznat druh el. podpisu (či pečeti)?

- určující je druh a obsah certifikátu - je v něm uvedeno:
  a) zda jde o certifikát pro elektronický podpis nebo pro elektronickou pečeť
  b) zda jde o kvalifikovaný certifikát (či nikoli)
  c) zda je soukromý klíč uložen na kvalifikovaném prostředku (QSCD)
- tyto údaje jsou uvedeny v položce „QC Statement“ (Výpisy QC)

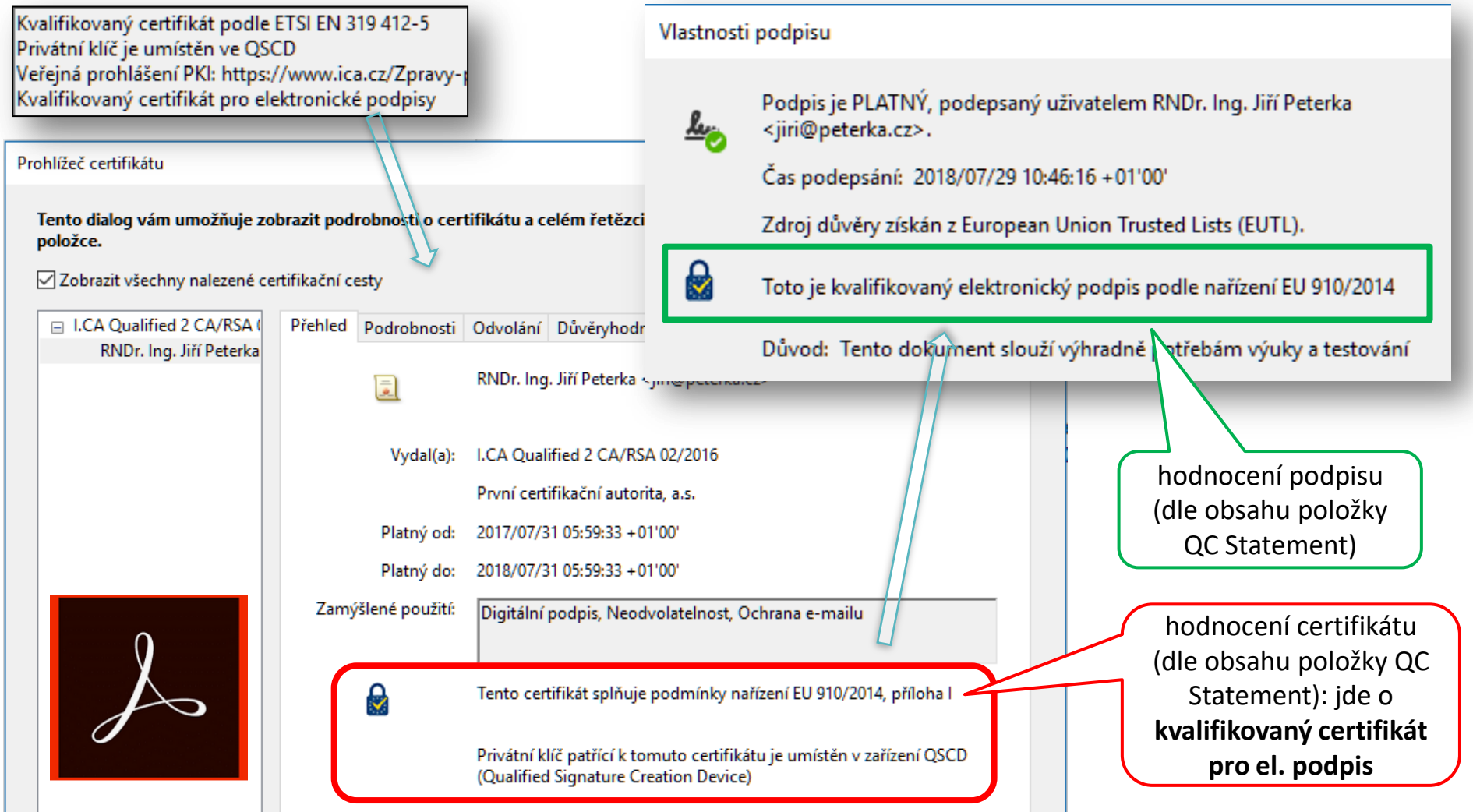
obsah položky QC Statement (Výpisy QC) není určen pro „lidské“ uživatele !!!

vyhodnocují ho programy, které používáme pro práci s elektronickými podpisy



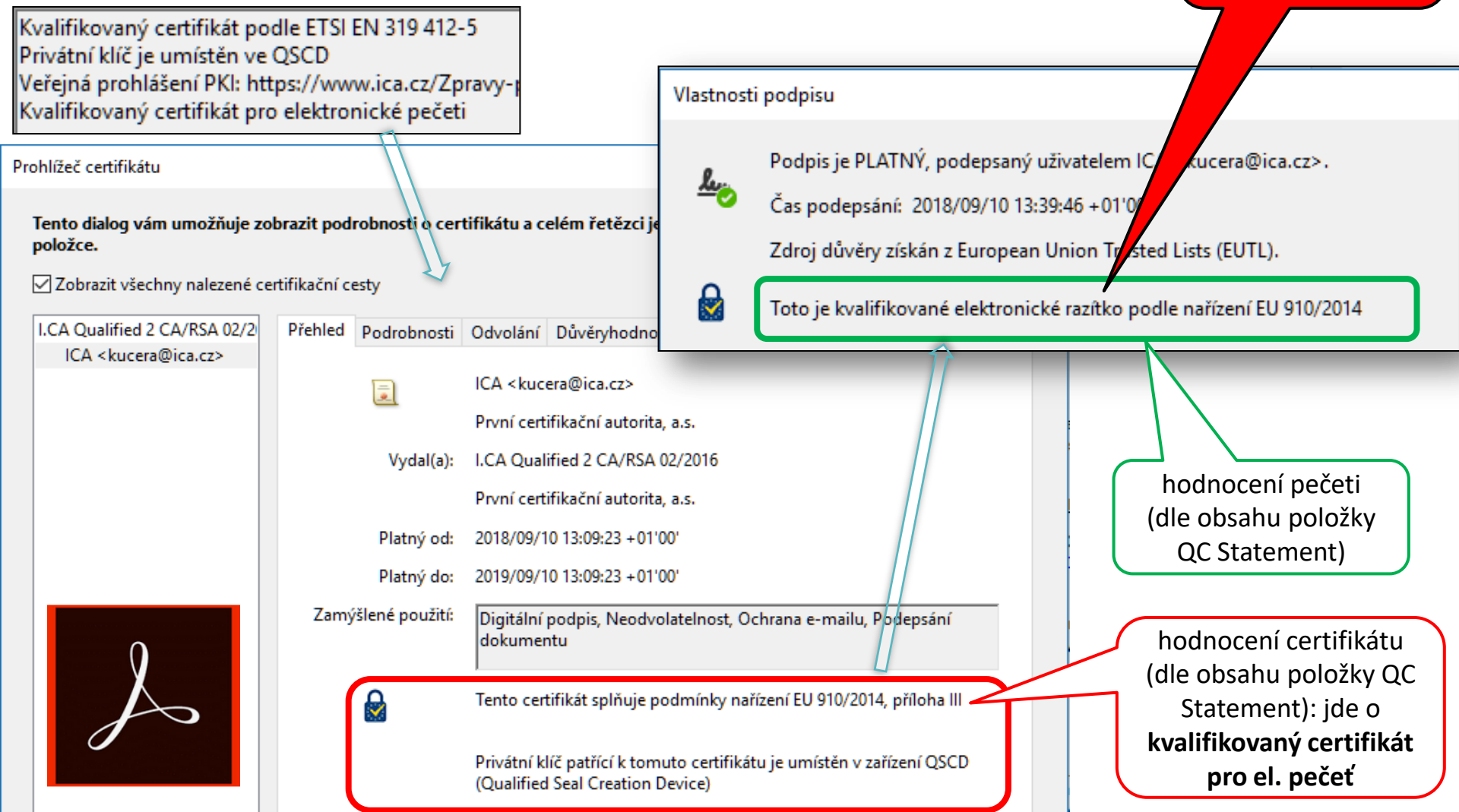
kvalifikovaný elektronický podpis

- aby šlo o kvalifikovaný podpis, musí být splněny tyto podmínky:
  - certifikát je kvalifikovaný a je certifikátem pro elektronický podpis
  - soukromý (nesprávně: privátní) klíč je uložen (umístěn) na QSCD



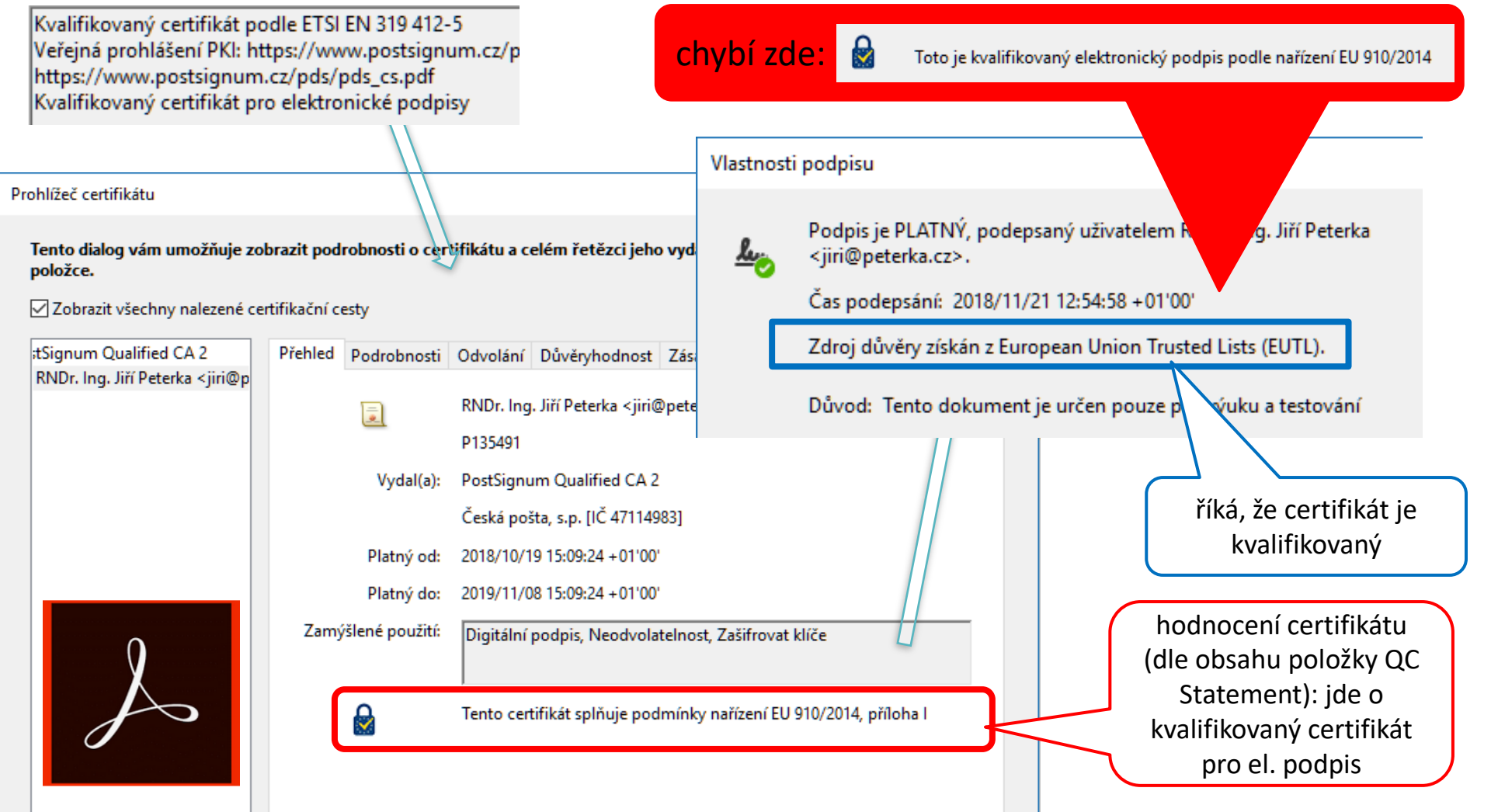
kvalifikovaná elektronická pečeť

- aby šlo o kvalifikovanou pečeť, musí být splněno ….
  - certifikát je kvalifikovaný a pro elektronickou pečeť
  - soukromý (nesprávně: privátní) klíč je uložen (umístěn) na QSCD



uznávaný elektronický podpis

- aby šlo o kvalifikovaný podpis, musí být splněny tyto podmínky:
  - certifikát je kvalifikovaný a je certifikátem pro elektronický podpis
  - ~~soukromý (nesprávně: privátní) klíč je uložen (umístěn) na QSCD~~

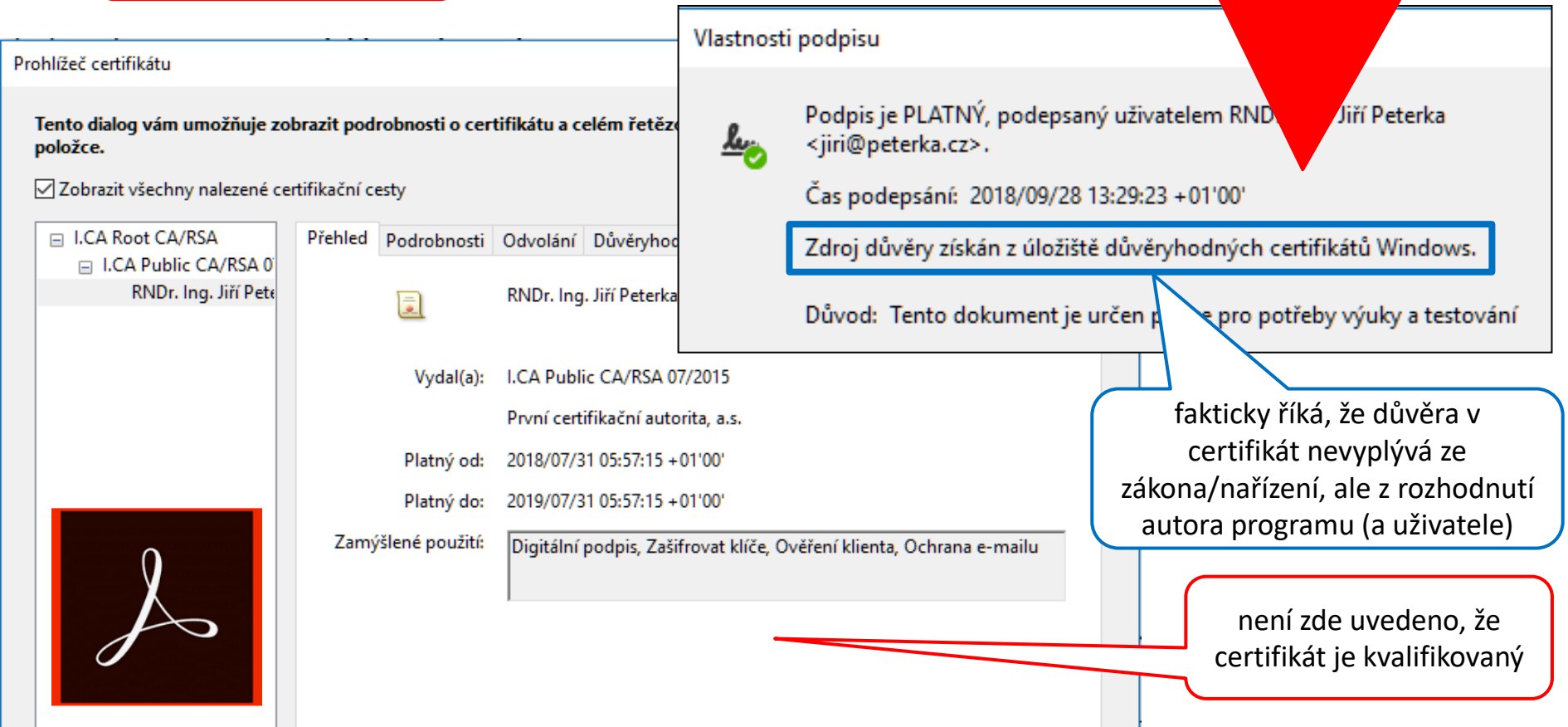


zaručený elektronický podpis

- aby šlo o kvalifikovaný podpis, musí být splněny tyto podmínky:
  - certifikát je kvalifikovaný a je certifikátem pro elektronický podpis
  - soukromý (nesprávně: privátní) klíč je uložen (umístěn) na QSCD

znamená, že **certifikát není kvalifikovaný**

chybí zde: Zdroj důvěry získán z European Union Trusted Lists (EUTL).

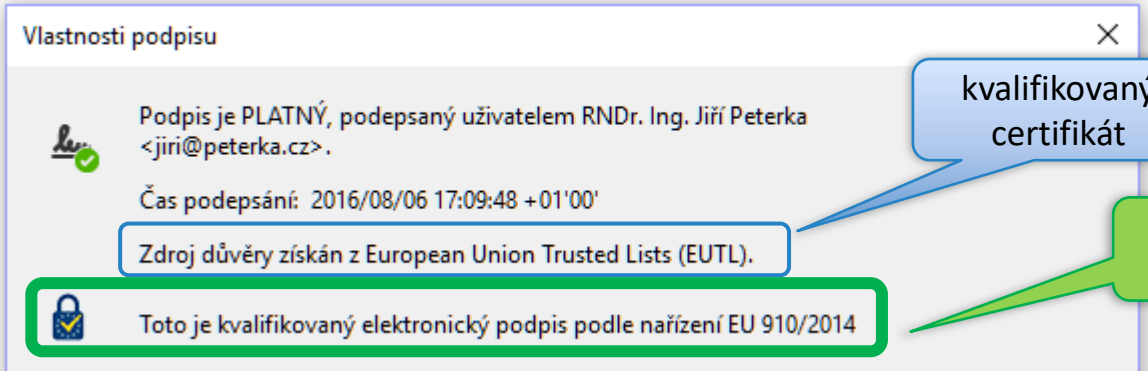


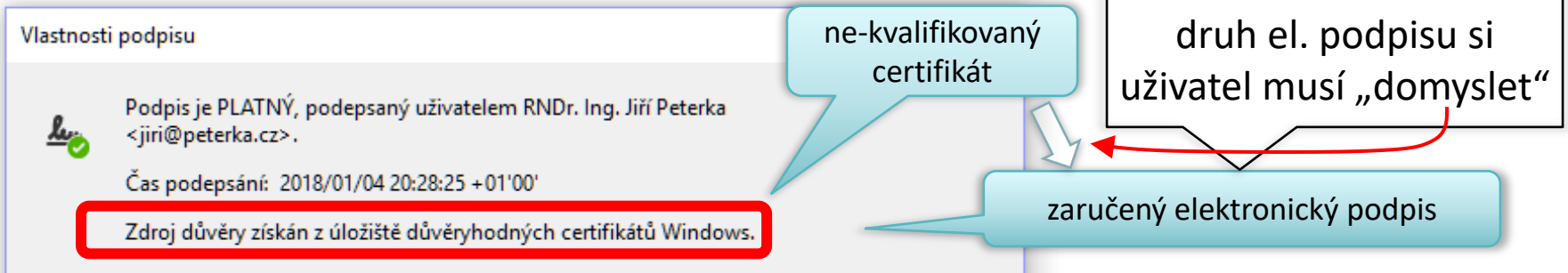
fakticky říká, že důvěra v certifikát nevyplývá ze zákona/nařízení, ale z rozhodnutí autora programu (a uživatele)

není zde uvedeno, že certifikát je kvalifikovaný

rekapitulace: ověřování pomocí Adobe Readeru

- program nám explicitně „ohodnotí“ pouze kvalifikovaný el. podpis
  - ostatní varianty si uživatel musí sám a správně odvodit (domyslet) !!!





tzv. unijní validátor (DSS)

- EU připravila „vzorovou implementaci validátoru“
  - validátor = nástroj pro ověřování platnosti elektronických podpisů a pečetí
- na webu EU je dostupná veřejná (demo) verze tohoto validátoru

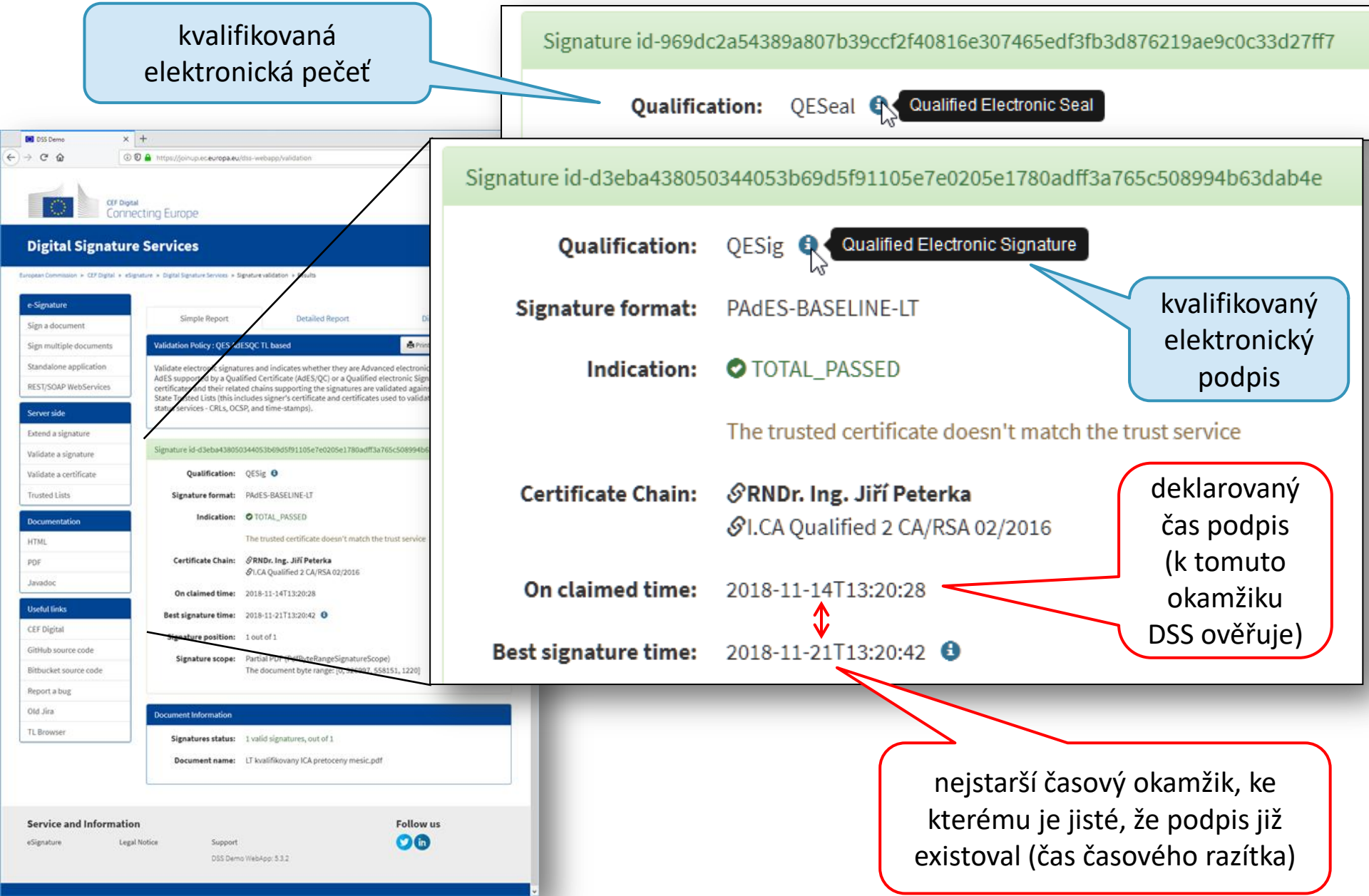
https://joinup.ec.europa.eu/dss-webapp/

  - výhoda: je zdarma
  - nevýhody:
    - k ověření se odesílá se celý dokument s podpisem či pečetí
      - pozor na dokumenty s důvěrným obsahem
    - validátor postupuje striktně podle nařízení eIDAS
      - podporuje pouze tzv. referenční formáty (Baseline), nikoli ty ne-referenční (Basic)
      - neřídí se časovými razítky
        - jako rozhodný okamžik bere deklarovaný čas podpisu (přebíraný ze systémových hodin počítače, na kterém byl podpis/pečeť vytvořen)

- v ČR je na této vzorové implementaci založen validátor Obelisk od společnosti Sefira
  - jde o komerční (placenou) službu

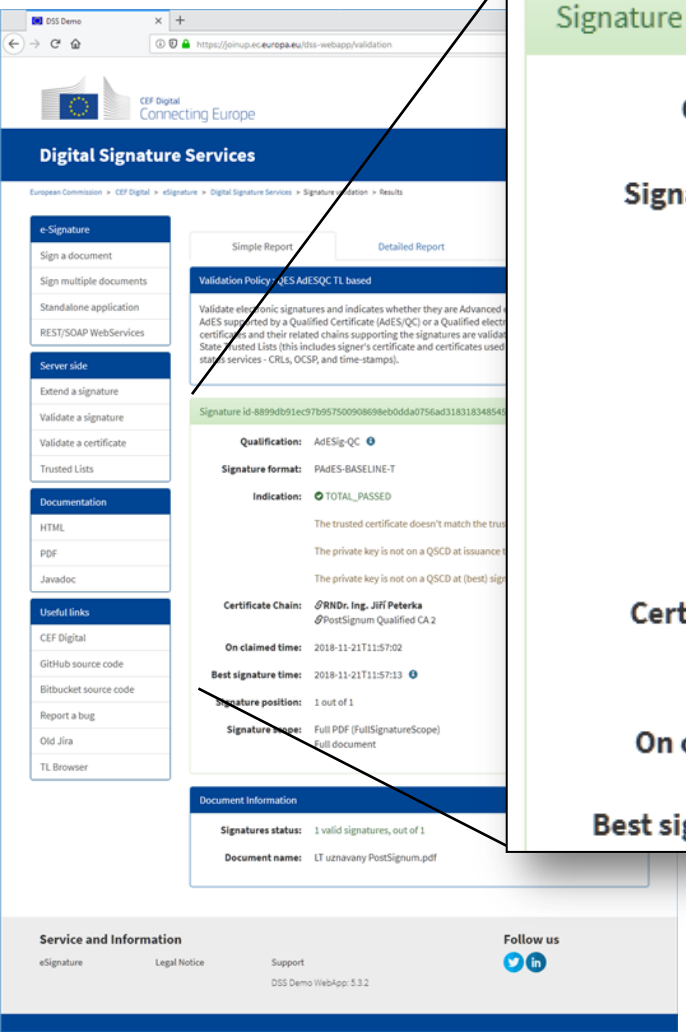
kvalifikovaný elektronický podpis (pečeť)

kvalifikovaná elektronická pečeť



uznávaný elektronický podpis (pečeť)

uznávaná elektronická pečeť



Signature id-cc128877a06feb398a57615c343527a38fdc6d72db3070c234b202724ab36be4

Qualification: AdESeal-QC — Advanced Electronic Seal supported by a Qualified Certificate

Signature id-64ba8aaf4d58895e45dc5837ed87ca757ee6c11a8ad1cb15d80e498b83346842

Qualification: AdESig-QC — Advanced Electronic Signature supported by a Qualified Certificate

Signature format: PAdES-BASELINE-T

Indication: TOTAL_PASSED

The trusted certificate doesn't mat

The private key is not on a QSCD at iss

The private key is not on a QSCD at (best) signing time!

Certificate Chain: RNDr. Ing. Jiří Peterka
PostSignum Qualified CA 2

On claimed time: 2018-11-21T11:54:58

Best signature time: 2018-11-21T11:55:13

uznávaný elektronický podpis (zaručený elektronický podpis, založený na kvalifikovaném certifikátu)

nejstarší časový okamžik, ke kterému je jisté, že podpis již existoval (čas časového razítka)

kvalifikované služby ověřování

- jejich poskytovatel ručí za správnost výsledku ověření
- v ČR takové služby nabízí:
  - Software602: služba SecuSign
  - I.CA: služba I.CA Verify (a I.CA Qverify pro SK)

- existují i služby ověřování bez kvalifikovaného statutu:
  - validátor Obelisk od spol. Sefira

- jak funguje služba SecuSign?
  - má uživatelské rozhraní
    - vlastní webové rozhraní
      - odesílá se celý dokument
    - skrze aplikaci Signer
      - odesílá se jen otisk (hash) dokumentu
  - má „lidsky čitelný“ výstup
    - poskytuje protokol o ověření
      - který lze uchovat …..

- jak funguje služba I.CA Verify?
  - nemá uživatelské rozhraní
    - na straně uživatele je systémová komponenta, určená k zabudování do IS uživatele
    - komponenta odesílá jen otisk (hash) dokumentu, ten se ověřuje na serveru
    - výstup (komponenty) je v XML, interpretuje ho IS uživatele, do kterého je komponenta zabudována

kvalifikovaná služba SecuSign

- zná tuzemskou právní úpravu
  - včetně „legislativních zkratek“, které správně rozepisuje

Informace o podpisech

1) Podpis RNDr. Ing. Jiří Peterka

Výsledek ověření: Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za **platný**.

Typ podpisu: Kvalifikovaný elektronický podpis (Uznávaný elektronický podpis podle zákona 297/2016 Sb.)

Čas podpisu: 6. 8. 2016 18:07:46

Informace o podpisech

1) Podpis RNDr. Ing. Jiří Peterka

Výsledek ověření: Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za **platný**.

Typ podpisu: Zaručený elektronický podpis založený na kvalifikovaném certifikátu (Uznávaný elektronický podpis podle zákona 297/2016 Sb.)

Čas podpisu: 6. 8. 2016 17:50:48

Informace o podpisech

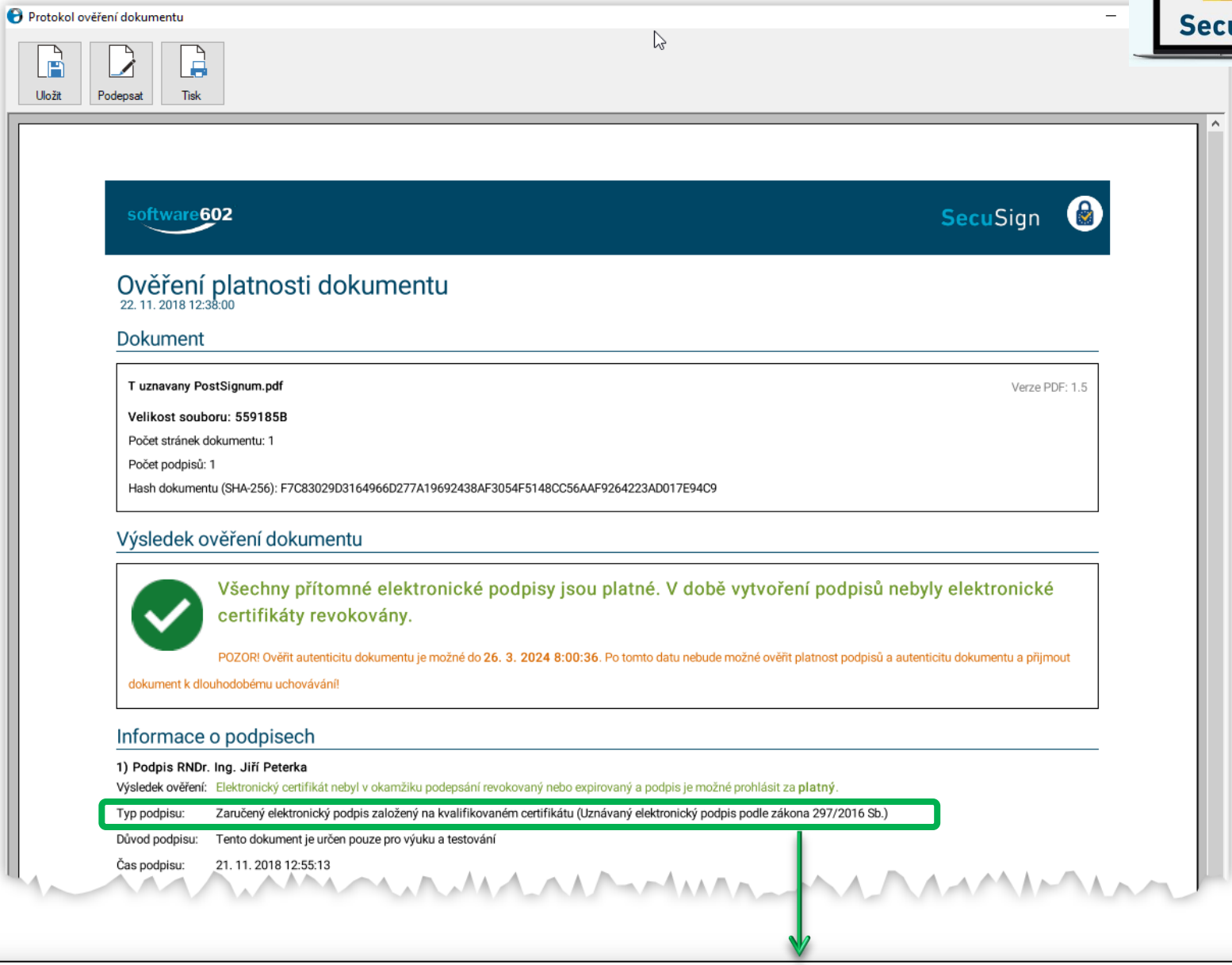
1) Podpis RNDr. Ing. Jiří Peterka

Výsledek ověření: Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za **platný**.

Typ podpisu: Zaručený elektronický podpis

Čas podpisu: 6. 8. 2016 17:50:48

protokol o ověření (SecuSign)



Typ podpisu: Zaručený elektronický podpis založený na kvalifikovaném certifikátu (Uznávaný elektronický podpis podle zákona 297/2016 Sb.)

protokol o ověření (SecuSign)

Detaily podpisu:

Formát podpisu: PAdES B-T (Baseline T)

Platnost vyhodnocena k: 21. 11. 2018 12:55:13

Ověření platnosti možné do: 26. 3. 2024 8:00:36

Informace o certifikátu:

- Typ: kvalifikovaný certifikát pro elektronický podpis vydaný kvalifikovaným poskytovatelem služeb vydávání certifikátů
- Předmět: SERIALNUMBER=P135491, G=Jiří, SN=Peterka, CN=RNDr. Ing. Jiří Peterka, OU=P135491, C=CZ
- Vydavatel: CN=PostSignum Qualified CA 2, O="Česká pošta, s.p. [IČ 47114983]", C=CZ
- Sériové číslo: 3B89E0
- Platnost: 19. 10. 2018 16:09:24 - 8. 11. 2019 15:09:24
- Ověřitelnost do: 26. 3. 2024 8:00:36
- Kontrola odvolání: On-line ověření stavu certifikátu (OCSP) ze 22. 11. 2018 12:37:58
  - Zdroj revokačních dat: Revokační data stažena od vydavatele certifikátu
  - Kontrolní SHA256 otisk: 5FE23B73B753508DBB663A078D51EDFC84FD20F16AB870A3C2D5B5408C4460BE
- Prohlášení vydavatele certifikátu:
  - Evropský kvalifikovaný certifikát (0.4.0.1862.1.1)
  - Zpráva pro uživatele (0.4.0.1862.1.5): https://www.postsignum.cz/pds/pds_en.pdf; https://www.postsignum.cz/pds/pds_cs.pdf
  - Typ certifikátu (0.4.0.1862.1.6): Certifikát pro elektronický podpis dle eIDAS - Nařízení Evropského parlamentu a rady (EU) č. 910/2014

Protokol ověření dokumentu byl vytvořen: 22. 11. 2018 12:38:00

Tento protokol ověření dokumentu byl vytvořen kvalifikovaným poskytovatelem služeb vytvářejících důvěru - Software602 a.s. a službou SecuSign.

protokol o ověření (SecuSign)

Časové razítko: 21. 11. 2018 12:55:13

Výsledek ověření:

Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a razítko je možné prohlásit za **platné**.

Typ razítka: Kvalifikované elektronické časové razítko

Formát razítka: Časové razítko z podpisu (v rámci PKCS7CMS_WITH_TST a CAdES-T a výše)

Informace o certifikátu:

- Typ: kvalifikovaný certifikát pro elektronickou pečeť vydaný kvalifikovaným poskytovatelem služeb vydávání certifikátů
- Předmět: CN=PostSignum TSA - TSU 1, OU=Time Stamping Authority, O="Česká pošta, s.p. [IČ 47114983]", OU=NTRCZ-47114983, C=CZ
- Vydavatel: CN=PostSignum Qualified CA 3, O="Česká pošta, s.p. [IČ 47114983]", C=CZ
- Sériové číslo: 2DCBE7
- Platnost: 23. 3. 2018 10:48:35 - 26. 3. 2024 8:00:36
- Ověřitelnost do: 26. 3. 2024 8:00:36
- Kontrola odvolání: Seznam zneplatněných certifikátů (CRL) vydaný 23. 11. 2018 5:23:08
  - Zdroj revokačních dat: Úložiště kvalifikované služby SecuSign
  - Vydavatel: C=CZ,O=Česká pošta\, s.p. [IČ 47114983],CN=PostSignum Qualified CA 3
  - Sériové číslo: 25BD
  - Vydání následujícího seznamu: 24. 11. 2018 5:23:00
  - Kontrolní SHA256 otisk: DEEC092F2F07C9325EA5082530EC1507B1CD8115A5F20A46695471750600D861
- Prohlášení vydavatele certifikátu:
  - Evropský kvalifikovaný certifikát (0.4.0.1862.1.1)
  - Zpráva pro uživatele (0.4.0.1862.1.5): https://www.postsignum.cz/pds/pdstsa_en.pdf; https://www.postsignum.cz/pds/pdstsa_cs.pdf
  - Typ certifikátu (0.4.0.1862.1.6): Certifikát pro elektronickou pečeť dle eIDAS - Nařízení Evropského parlamentu a rady (EU) č. 910/2014

jak se musí kdo podepisovat?

- **OVM**:
  - do 19.9.2018 (včetně)
    - stačilo používat jen uznávané el. podpisy
      - neboli: kvalifikované prostředky (pro vytváření el. podpisů) nebyly nutné!
        - tento stav platil již od roku 2000 (dle zákona č. 227/2000 Sb. o el. podpisu)
  - po 19.9.2018
    - subjekty veřejné správy se musí podepisovat formou kvalifikovaného elektronického podpisu !!
      - tj. potřebují kvalifikované prostředky, a také „nové“ kvalifikované certifikáty
      - plyne z §5 zákona č. 297/2016 Sb.
    - musí připojovat kvalifikované elektronické časové razítko
      - plyne z §11) zákona č. 297/2016 Sb.

- **FO** a **PO**:
  - při právním jednání s (českými) OVM:
    - stačí používat uznávané elektronické podpisy
      - plyne z §6 zákona č. 297/2016 Sb.
  - při právním jednání se (zahraničními, z EU) OVM:
    - nutno používat kvalifikované elektronické podpisy
      - plyne z nařízení eIDAS
  - při soukromoprávním jednání
    - lze používat jakýkoli elektronický podpis
      - včetně „pouze“ zaručeného či dokonce prostého elektronického podpisu)
      - plyne z §7 zákona č. 297/2016 Sb.

pro pečetění vše obdobně ….

co přesně říká zákon?

- § 5 zákona č. 297/2016 Sb. o službách vytvářejících důvěru
  - K podepisování elektronickým podpisem lze použít pouze kvalifikovaný elektronický podpis, podepisuje-li elektronický dokument, kterým právně jedná
    a) stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem (dále jen „veřejnoprávní podepisující“), nebo
    b) osoba neuvedená v písmenu a) při výkonu své působnosti.

- vymezuje okruh subjektů, kterých se ustanovení týká
  - zavádí nový pojem: „veřejnoprávní podepisující“

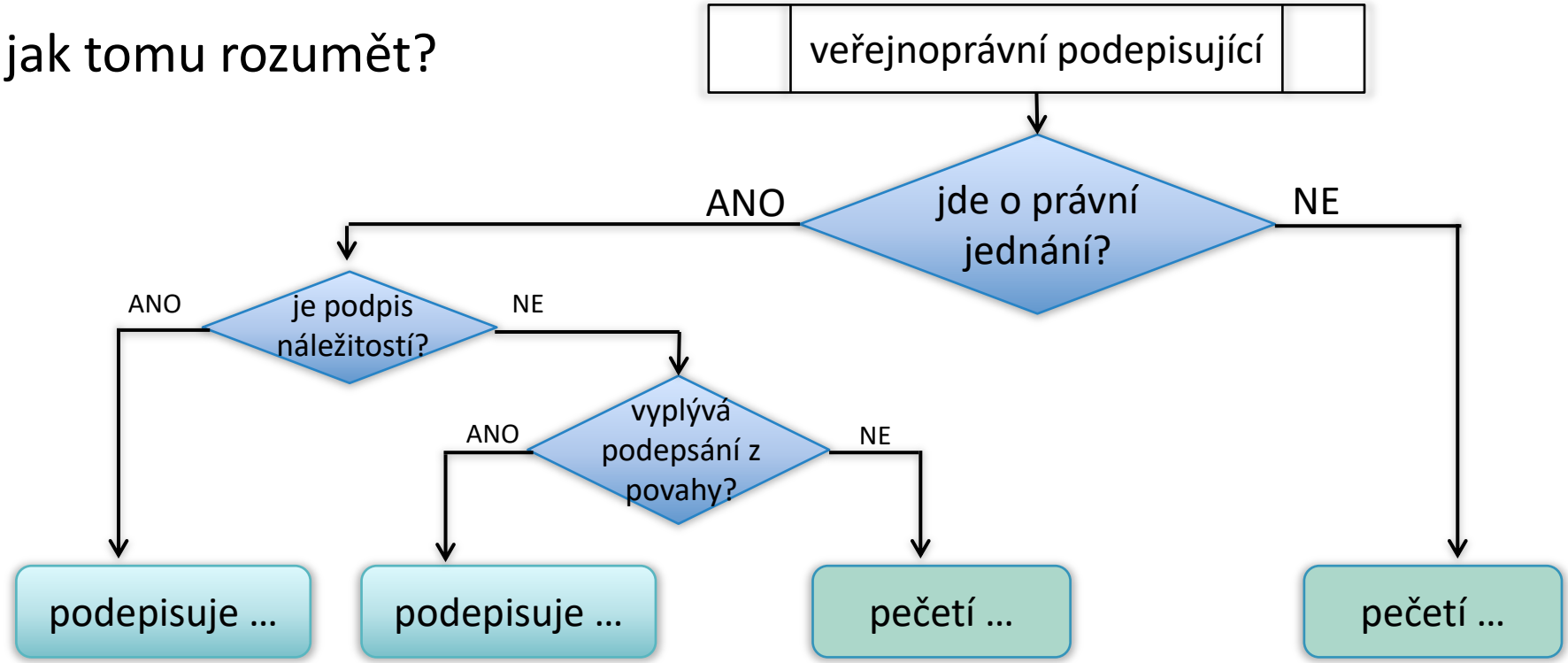
do 19.9.2018 (včetně) platila výjimka (§19 odst. 1): stačil i uznávaný elektronický podpis

- neříká, kdy se má elektronicky podepisovat !!
  - to musí vyplývat „odjinud“ …
- říká pouze to, že:
  - když už „veřejnoprávní podepisující“ má elektronicky podepsat ….
  - ….. pak musí použít kvalifikovaný elektronický podpis

kdy má veřejnoprávní podepisující podepisovat?

- § 8 zákona č. 297/2016 Sb. o službách vytvářejících důvěru
  - Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí.

- jak tomu rozumět?



  - na každém elektronickém dokumentu musí být buď (el.) podpis, nebo (el.) pečeť

veřejnoprávní podepisující a pečetění

- když má „veřejnoprávní podepisující“ povinnost pečetit, musí použít kvalifikovanou elektronickou pečeť
  - vyplývá z §8 zákona č. 297/2016 Sb.

do 19.9.2018 platila výjimka: bylo možné používat i jiné než kvalifikované pečeti

- s kvalifikovanou el. pečetí je spojena presumpce
  - správnosti původu dat (nikoli správnosti obsahu)
    - tj. opak by musel prokazovat ten, kdo ho tvrdí
  - celistvosti, resp. neměnnosti (zajištění integrity)

s kvalifikovanými elektronickými podpisy není spojena žádná (obdobná) presumpce/domněnka

- článek 35, odst. 2 nařízení eIDAS:
  - *u kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena.*

- FO a PO při právním jednání vůči OVM mohou používat uznávané elektronické pečeti (§9)
  - při soukromoprávním jednání mohou použít jakoukoli elektronickou pečeť (§10)

kvalifikované elektronické pečeti

- vyžadují:
  - **kvalifikované certifikáty** pro elektronické pečeti
  - **kvalifikované prostředky** pro vytváření elektronických pečetí (QSealCD)
- možnosti:
  - pro „ruční“ pečetění (tj. jako u podepisování) je od 1.8.2018 dostupný jeden konkrétní kvalifikovaný prostředek (QSealCD)
    - čipová karta ProID+Q od PostSignum
      - lze reálně použít jen pro malé objemy pečetěných dokumentů
        - protože vytvoření pečeti nějakou dobu trvá, a vždy vyžaduje autentizaci uživatele (zadání PINu)
  - pro „strojové pečetění“ je nutný tzv. HSM (Hardware Security Modul), který je velmi drahý
    - a na našem trhu zatím (moc) není
  - další možností je služba „vzdáleného pečetění“
    - služba RemoteSeal od I.CA

(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 ….
  - existují kvalifikovaná 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 …
- veřejnoprávní podepisující a časová razítka:
  - dříve: povinnost připojovat čas. razítka nebyla v zákoně uložena explicitně, odvozovala se z jiných ustanovení
  - dnes: povinnost již je v zákoně zakotvena explicitně (§11)

§ 11 zákona č. 297/2016 Sb. o službách vytvářejících důvěru

(1) Veřejnoprávní podepisující, který podepsal elektronický dokument, kterým právně jedná, způsobem podle § 5, a osoba, která podepsala elektronický dokument, kterým právně jedná při výkonu své působnosti, způsobem podle § 5, opatří podepsaný elektronický dokument kvalifikovaným elektronickým časovým razítkem.

odst. 2 obdobně pro pečetění

- pro FO a PO: nemají povinnost ….
  - ale lze jim vřele doporučit, aby časová razítka používali (viz digitální kontinuita)

co říká nařízení a co náš zákon?

nařízení eIDAS (nařízení 910/2014 EU)

- účinky rovnocenné vlastnoručnímu podpisu má kvalifikovaný el. 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.)

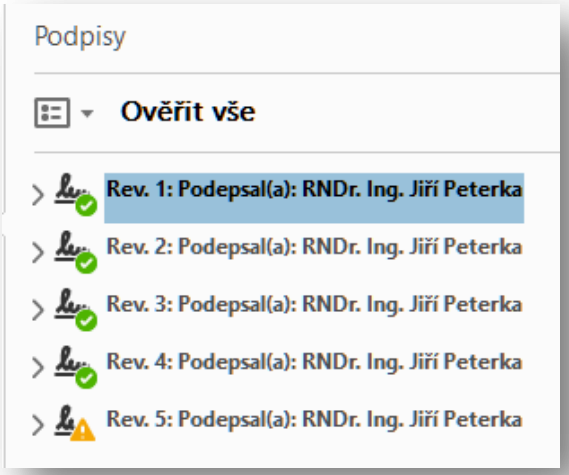
- účinky rovnocenné vlastnoručnímu podpisu mají (v soukromoprávních vztazích) všechny druhy el. podpisů
  - tj. včetně prostého el. podpisu i zaručeného el. podpisu

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.

soubory s příklady k 1. bloku

- **priklad1_1.pdf** (+ priklad1_1_verify.pdf)
  - 5 různých elektronických podpisů:
    - kvalifikovaný v referenčním formátu
    - kvalifikovaný v nereferenčním formátu
    - zaručený, založený na kvalifikovaném certifikátu
      - „český“ uznávaný
    - zaručený
      - certifikát od ICA (důvěryhodný ve Windows)
    - zaručený
      - certifikát od eIdentity



- **priklad1_2.pdf** (+ priklad1_2_verify.pdf)
  - kvalifikovaná elektronická pečeť
    - výpis z RŽP

protokol o ověření kvalifikovanou službou SecuSign

- **priklad1_3.pdf** (+ priklad1_3_verify.pdf)
  - zaručená elektronická pečeť, založená na kvalifikovaném certifikátu
    - výpis z OR