Elektronický podpis

Podpis obecně

- slouží k doložení projevu vůle osoby
- v závislosti na právním systému jím může být jakýkoliv znak, symbol či kresba
- dle občanského zákoníku je **písemný** právní úkon platný, je-li **podepsán** jednající osobou
- bez ohledu na formu jde o zachycení obsahu právního úkonu a určení osoby, která jej učinila

Proč elektronický podpis (EP)

- anonymita internetu => možnost vydávat se za někoho jiného
- digitální informaci nelze jednoznačně spojit s jejím autorem
- potřeba ekvivalentu fyzického podpisu u digitálních dokumentů

- Hlavní úkoly EP:
  - **možnost zjistit následnou změnu podepsaných dat (dokumentu)**
  - **jednoznačně spojit podpis s konkrétní osobou**

Rozdíl mezi vlastnoručním a elektronickým podpisem

- Vlastnoruční podpis
  - existuje „sám o sobě“.
  - můžeme podepsat např. čistý papír, na který pak někdo později může cokoli připsat (ať již s naším vědomím či bez něj).
- Elektronický podpis (EP)
  - neexistuje sám o sobě
  - je přímo závislý na tom, co podepisuje (obsahu). Když jedna osoba podepisuje dva dokumenty, její elektronický podpis bude vždy *odlišný*.
  - je pouhé *číslo*
- Mohu si EP koupit?
  - Ne, el. podpis vzniká aplikací kryptografických funkcí a dat pro vytváření el. podpisu na podepisovaný dokument

Asymetrická kryptografie

- El. podpis funguje na principu **asymetrické kryptografie**
- K podepisování a ověřování podpisu se používají 2 rozdílné klíče (symetrická kryptografie = 1 klíč, který musím protistraně poskytnout, což je riskantní)
- Důvod:
  - bezpečnost – eliminuje se potřeba výměny klíčů
  - praktická nemožnost ze znalosti šifrovacího klíče spočítat dešifrovací
  - snadná ověřitelnost protistranou

Klíče

- jsou čísla, která se generují na počátku procesu vydání EP (tzv. **pár klíčů**) a jsou vzájemně kryptograficky spjaty

1. **soukromý klíč** (data pro vytváření elektronického podpisu)
   - slouží k podepisování
   - uložen na tokenu, kartě, v PC…
   - je určen pouze pro použití svým majitelem, který jej musí držet v tajnosti a bezpečí

2. **veřejný klíč**
   - slouží k vyhodnocování platnosti (ověřování) EP
   - je veřejně dostupný komukoliv
   - říká se mu certifikát

- PKI (Public key infrastructure) - Infrastruktura veřejného klíče

Certifikát

- v asymetrické kryptografii**: veřejný klíč + data o jeho majiteli** a vydavateli podepsaná EP vydavatele (CA)
- slouží k ověřování platnosti EP
- je **volně** k dispozici komukoliv, kdo má zájem navázat bezpečné spojení s majitelem příslušného soukromého klíče
- certifikáty jsou zveřejňovány na webech svých vydavatelů
- vydává jej certifikační autorita (CA)
- pro vytváření zaručeného EP je nezbytné jej připojit ke každému vytvořenému EP
- musí být nainstalovaný v počítači
- má omezenou platnost na (obvykle) 1 rok od vydání
- Kvalifikovaný (zaručený)
- Komerční

Bezpečnost

Stejně jako u většiny jiných elektronických služeb i u elektronického podpisu panují **obavy z jeho zneužití**. Soukromý klíč musí být proto chráněn:

- **fyzicky** (token)
- **PIN**
- možností **zneplatnění**

- Srovnej: vzdálené podepisování

Zneplatnění (revokace) certifikátu

- V případě kompromitace soukromého klíče (odcizení tokenu atp.) nelze „zablokovat“ jeho certifikát, protože certifikát je volně k dispozici a není možné jej „stáhnout z oběhu“ (x platební karta)
- Na zneplatnění se musíme **dotázat vydavatele** (CA) prostřednictvím:
  - CRL – Certificate Revocation List
  - OCSP – Online Certificate Status Protocol – eIDAS: povinné!
- Dělá program (eSSL, Adobe Reader, Signer…)
- Musíme ale vědět, **kdy** se dotázat (problém pouze, pokud není časové razítko
- „Kámen úrazu“ ověřování platnosti EP

Seznam zneplatněných certifikátů
(CRL – Certificate Revocation List)

- pokud je certifikát na CRL, znamená to, že mu již **nelze důvěřovat**, i když je nadále **platný**
- **zveřejnění na CRL neznamená zrušení či zablokování certifikátu – lze jej i nadále používat k tvorbě EP!**
- informace o zneplatnění je dostupná pouze **u vydavatele, z certifikátu ji nelze vyčíst!**
- CRL vydává CA **minimálně** jednou za 24 hodin
- zneplatněný certifikát bude zveřejňován na CRL do konce své platnosti, pak už ne!
- OCSP - Online Certificate Status Protocol – zjišťování revokace v reálném čase

Časové razítko

- Čas podpisu hraje při **ověřování** podpisu klíčovou roli
- Při „běžném“ podepisování se datum a čas bere z hodin na počítači autora podpisu
- Tyto hodiny lze však libovolně nastavit – údaj o čase podpisu pak **není důvěryhodný**
- Poskytuje **důvěryhodný údaj o existenci podepsaného dokumentu v čase**
- Absence časového razítka = problémy s ověřením podpisu **podle eIDAS**

Časové razítko

- Založeno na stejném principu jako EP
- na rozdíl od něj je v něm uveden pouze garantovaný údaj o čase jeho vzniku
- údaj o čase poskytuje důvěryhodná třetí strana – poskytovatel časových razítek (srovnej s certifikační autoritou)
- poskytuje se zpravidla online (přes internet)
- Připojuje se k již podepsanému dokumentu => **další zabezpečovací prvek**
- platnost časového razítka: 3 – 5 let => **významným způsobem pozitivně ovlivňuje (= prodlužuje) možnost ověření EP**

Platnost EP v čase

- certifikát pro vytváření EP platí nejčastěji 1 rok od vydání
- po tuto dobu jsme schopni učinit **všechny** kroky pro ověření jeho pravosti a tím i pravosti EP, který je na něm založen
- to, že vypršela platnost certifikátu (expirace) neznamená, že by dokument byl automaticky považován za nepravý
- znamená to však, že již nejsem schopen učinit **všechny** kroky k ověření jeho pravosti
- viz např. zkontrolovat, zda nebyl zneplatněn certifikát EP
- ale nadále jsem schopen kontrolovat integritu (neporušenost obsahu)

Elektronická pečeť

- Technicky obdobný prostředek jako el. podpis
- Prokazuje **původ dokumentu** (x podpis)
- lze vydat **pouze právnickým osobám**
- problém vytváření:
  - čipová karta nebo token – nutno vždy zadat PIN, v praxi obtížně použitelné
  - HSM modul (Hardware security module) – drahé
  - vzdálené pečetění – služba

eIDAS

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu

Článek 25

Právní účinky elektronických podpisů

1. **Elektronickému podpisu nesmějí být upírány právní účinky** a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.

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**.

Hierarchie el. podpisů dle eIDAS

- Kvalifikovaný (Qualified, QES)
  - Musí být založen na kvalifikovaném certifikátu
  - Musí jej vydat kvalifikovaná certifikační autorita
  - **Musí** být na kvalifikovaném prostředku (QSCD, tj. kartě, tokenu, HSM)

- Zaručený (Advanced, AES)
  - Musí být založen na kvalifikovaném certifikátu
  - Musí jej vydat kvalifikovaná certifikační autorita
  - **Nemusí** však být na kvalifikovaném prostředku (může být uložen v PC)

- „Jiný“ („prostý“, „simple“)
  - Jakýkoli jiný, třeba i podpis „Jan Novák“ v e-mailu

Kvalifikovaný certifikát

- vydavatel - **certifikační autorita -** ověřuje identitu osoby, která si chce certifikát pořídit a **ručí** za její správné ověření
- může jej vydávat pouze **kvalifikovaná certifikační autorita** (QCA), která musí splňovat požadavky kladené zákonem o el. podpisu
- Orgán dohledu v ČR: Digitální informační agentura (DIA) (do 2023 MV)

Kvalifikovaná certifikační autorita
(Qualified CA, QCA)

- vydává certifikáty (kvalifikované) na základě podmínek stanovených právními předpisy
- V ČR:
  - První certifikační autorita, a. s. (ICA)
  - Česká pošta, s. p. (PostSignum)
  - eIdentity a. s.

+ cca 245 dalších v celé EU (např. Itálie 50, Španělsko 40)

- k vytvoření kvalifikovaného elektronického podpisu lze použít certifikát **jakékoli** kvalifikované CA splňující nařízení eIDAS
- List of Trusted Lists (LOTL) – seznam kvalifikovaných poskytovatelů v EU

Zk. č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

- Tzv. adaptační zákon nařízení eIDAS
- **národní** pojem **uznávaný el. podpis** = kvalifikovaný nebo zaručený (založený na kvalifikovaném certifikátu)
- **Veřejnoprávní podepisující** (VP): stát, **ÚSC**, PO zřízená zákonem nebo zřízená či založená státem, ÚSC nebo PO zřízenou zákonem nebo jejich orgán anebo jiná jejich součást.
- VP smí použít **pouze kvalifikovaný** EP při podepisování dokumentu, kterým činí úkon nebo právně jedná.
- Soukromoprávní podepisující (SP) vůči VP: **pouze uznávaný** podpis
- VP *musí* opatřit podepsaný dokument **časovým razítkem,** SP nikoli

Kvalifikované časové razítko

- Hierarchie obdobná podpisu
- **VP musí označit kvalifikovaný časovým razítkem každý podepsaný dokument** (viz 297/2016 Sb. + eIDAS)
- Poskytuje se vzdáleně **jako služba** (nutné připojení k internetu)
- Kde získám: koupím balíček časových razítek od poskytovatele (TSA)

Kvalifikovaná el. pečeť

- Zk č. 297/2016 Sb.:

  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.

Komerční certifikát

- Public (x Qualified)
- legislativní, nikoli technický rozdíl vůči kvalifikovanému
- slouží zejména k bezpečné komunikaci, tj. k bezpečnému přihlašování, k šifrování, k elektronickému podepisování e-mailů apod.
- Je vydáván bez jakýchkoli **legislativních** záruk, podmínky stanovuje CA

Ověřování EP

- z EP není pouhým pohledem patrné, zda je či není platný
- smyslem je zjistit, zda dokument nebyl po podepsání změněn
- klíčový prvek pro to, aby podepsané elektronické dokumenty mohly být považovány za pravé
- Nařizuje:
  - čl. 32 eIDAS
  - vyhl. č. 259/2012 Sb., o podrobnostech výkonu spisové služby

Ověřování

Vyhláška č. 259/2012 Sb.:

Zaznamenanými údaji o výsledku zjištění podle odstavce 4 a výsledku ověření podle odstavce 5 jsou alespoň

- a) **název nebo obchodní firma kvalifikovaného poskytovatele služeb vytvářejících důvěru** nebo akreditovaného poskytovatele certifikačních služeb,
- b) **údaj o době, na kterou byl certifikát vydán**, popřípadě, pokud jsou známy, datum a čas jeho zneplatnění,
- c) **identifikační číslo** certifikátu,
- d) **jméno, popřípadě jména, a příjmení**, název nebo obchodní firma podepisující, označující nebo pečetící osoby, popřípadě pseudonym, byl-li použit,
- e) **údaj o tom, zda se jedná o kvalifikovaný elektronický podpis nebo zaručený elektronický podpis** založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovanou elektronickou pečeť nebo zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu pro elektronickou pečeť,
- f) **datum a čas rozhodné pro ověření platnosti** uznávaného elektronického podpisu nebo uznávané elektronické pečetě, a certifikátů, na nichž jsou založeny,
- g) **výsledek, datum a čas ověření platnosti** uznávaného elektronického podpisu, uznávané elektronické pečetě, uznávané elektronické značky, kvalifikovaného elektronického časového razítka a certifikátů, na nichž jsou založeny, a
- h) **číslo seznamu zneplatněných certifikátů, vůči kterému byla platnost certifikátu ověřována**, nebo způsob, jakým byla platnost certifikátu ověřována, nebylo-li seznamu zneplatněných certifikátů k ověření platnosti certifikátu užito.

Ověřování

Aby bylo možno konstatovat, že je podpis platný musí být splněna 3 kritéria **současně**:

- **integrita** podepsaného dokumentu nebyla porušena
- **certifikát**, na kterém je podpis založen, byl k posuzovanému okamžiku **platný** (ve smyslu: ještě neuplynula doba jeho řádné platnosti).
- **certifikát**, na kterém je podpis založen, **nebyl** k posuzovanému okamžiku **revokován** (zneplatněn). Totéž musí platit i pro všechny nadřazené (kořenové) certifikáty, které **musím** mít nainstalované v PC.

Ověřování a platnost elektronických podpisů

- Platnost **certifikátu** obvykle 1 rok – bezpečnost
- Platnost el. podpisu **nekončí** okamžikem, kdy skončila platnost jeho certifikátu. **Subjekt (před rokem) zamýšlel podepsat platně.**
- Po uplynutí platnosti certifikátu je omezena pouze schopnost ověřit platnost podpisu
- Řešení: **časové razítko** (viz 297/2016 Sb., eIDAS)

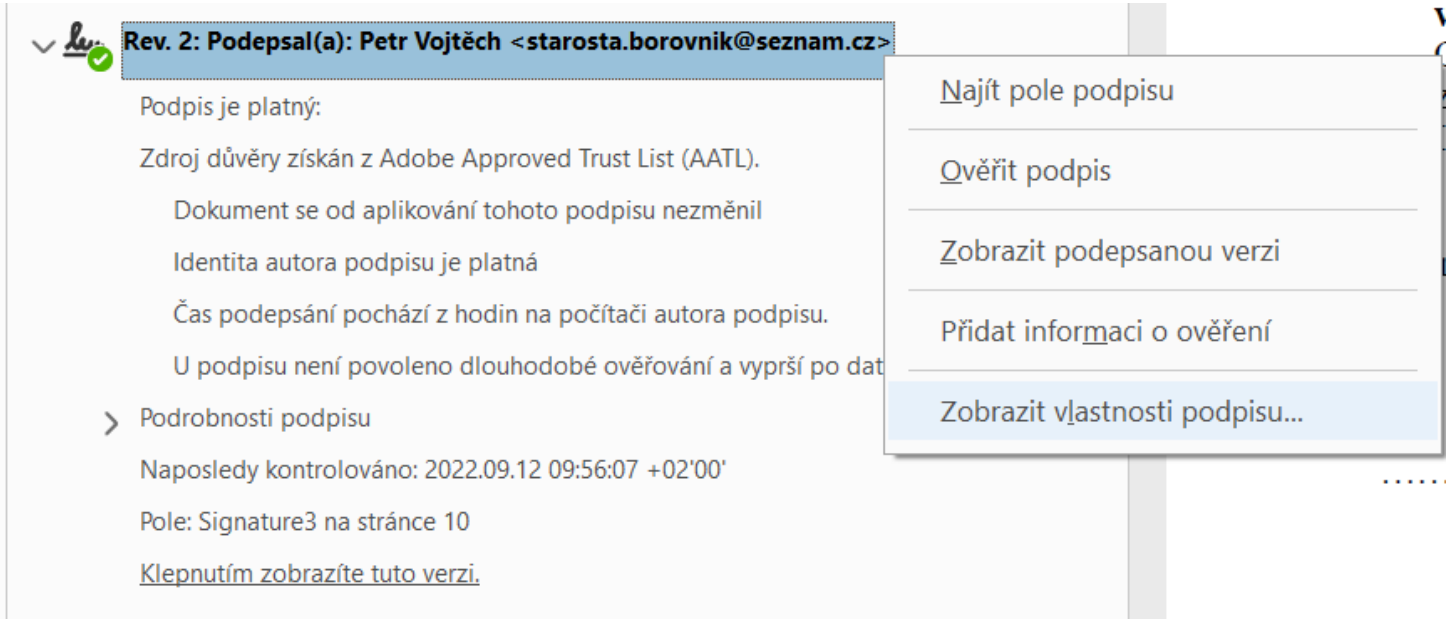
Ověřování

- Doporučení: ověřovat přes specializovanou aplikaci/službu
- Čl. 33 eIDAS: Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí
- Ověřování EP musí být součástí eSSL (el. systému spisové služby):
  - eSSL při příjmu nebo vložení komponenty automatizovaně zajistí ověření platnosti zajišťovacích prvků, které jsou ke komponentám připojeny.
  - eSSL při ověření zajišťovacích prvků v době příjmu nebo vložení zaznamená do metadat údaje stanovené právním předpisem upravujícím podrobnosti výkonu spisové služby nebo k dokumentu připojí samostatnou komponentu, která údaje o ověření obsahuje.
- Adobe Reader není zcela vhodný ověřovací nástroj pro laiky

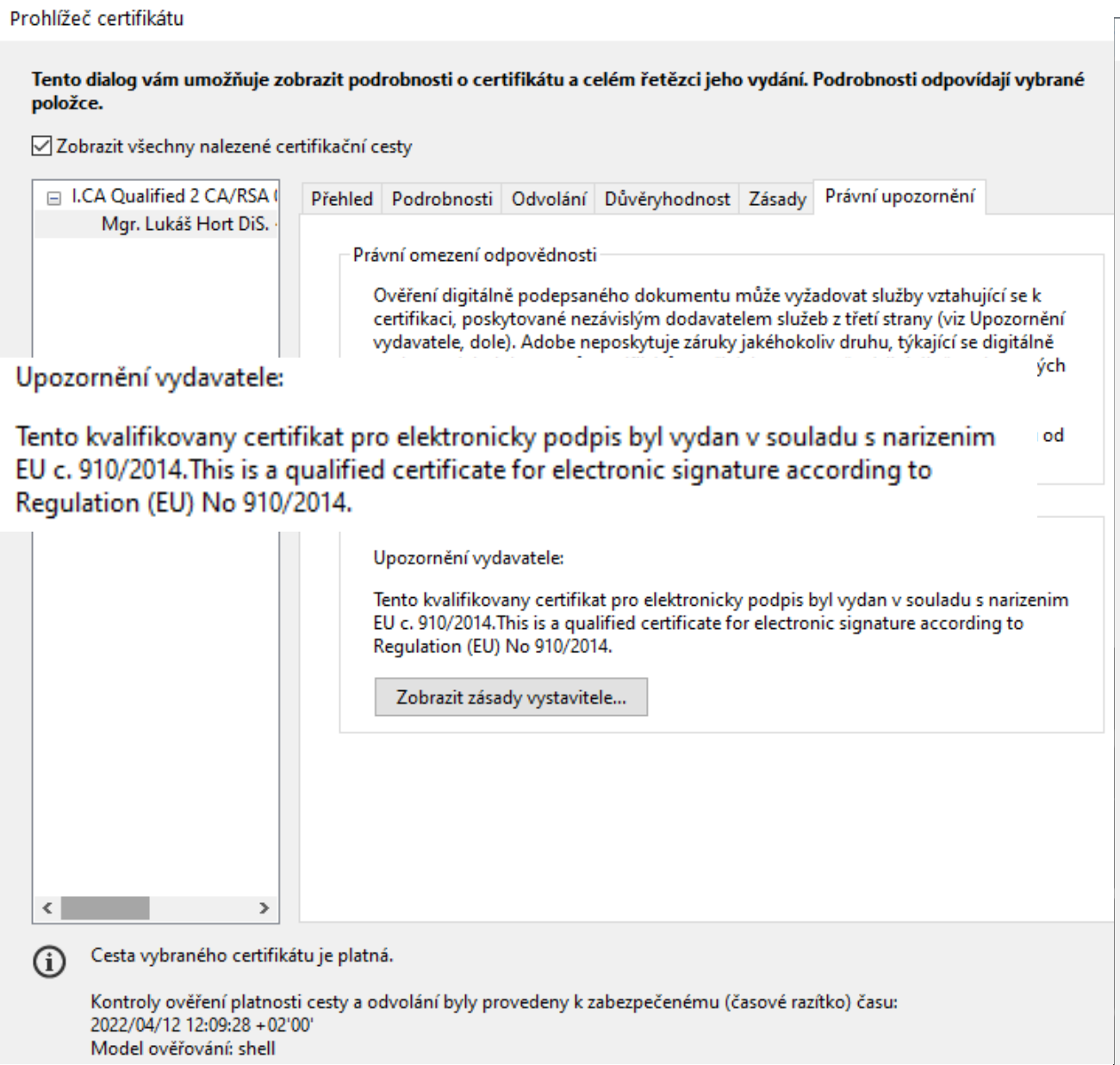
Informace o podpisu v Adobe Reader

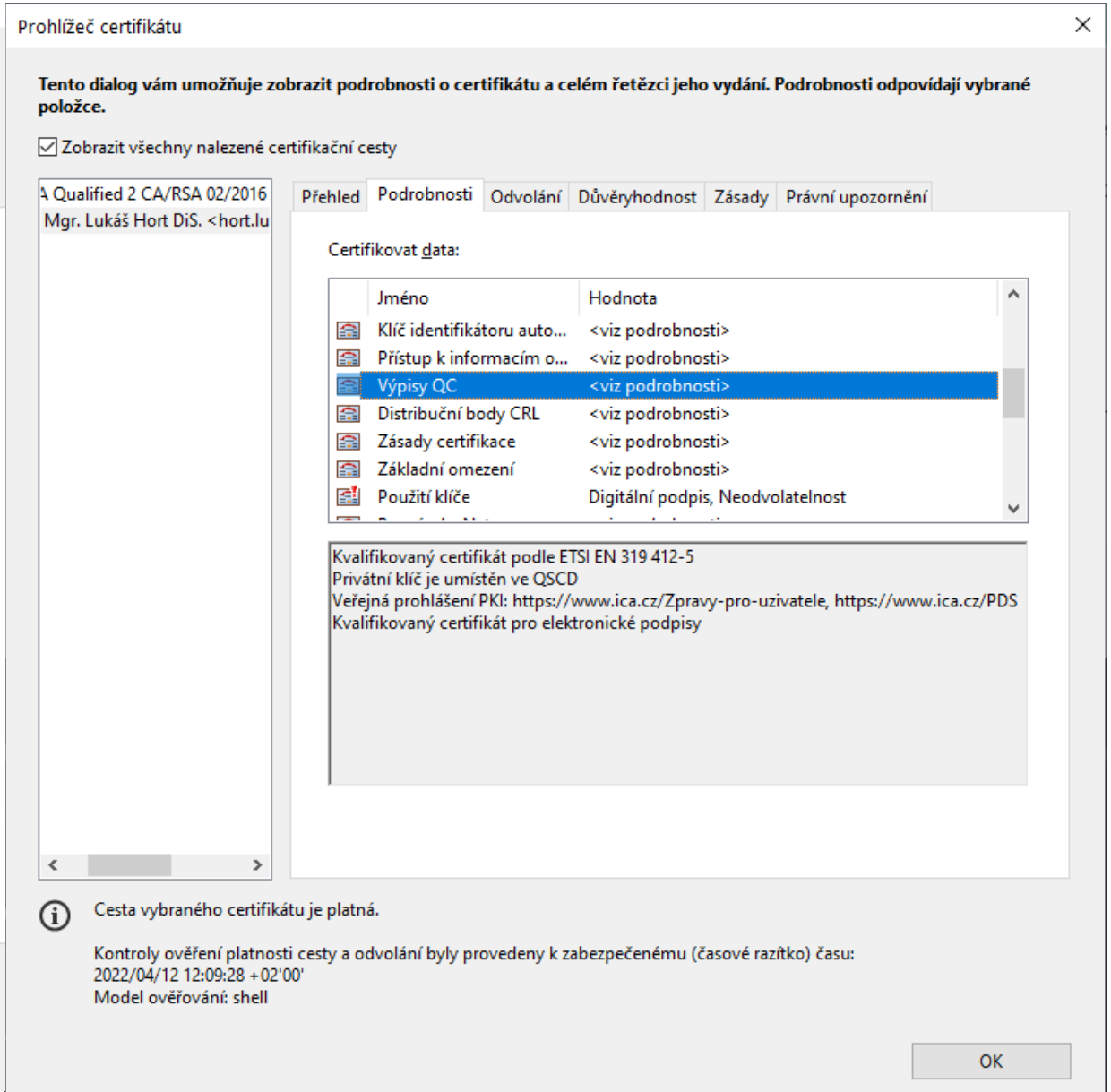
značí přítomnost elektronického podpisu/pečetě, otevře okno podpisů

- Kliknutím pravým tlačítkem myši na podpis lze zobrazit jeho vlastnosti



Jak poznáme kvalifikovaný el. podpis





Vizualizovaný podpis

- Nezaměňovat s vlastním EP !
- Zcela na libovůli autora
- „Ikona“ či link vedoucí k vlastnostem podpisu

Ověřování podpisu v Adobe Reader

- Musí být uživatelem správně nastaven
- Nevhodným/záměrným nastavením jej lze přimět k tomu, aby i neověřitelný podpis hodnotil jako platný (rozdílné nastavení dává rozdílné výsledky)
- Vyžaduje instalaci kořenových certifikátů autorit
- Není vhodným nástrojem pro ověřování **dle eIDAS** pro laiky, vyžaduje odborné znalosti

Nastavení Adobe Reader DC pro ověřování el. podpisu

Zapnutí integrace se systémovým uložištěm certifikátů

0. Musím mít importované kořenové certifikáty certifikačních autorit.
1. Spusťte Adobe Reader DC.
2. Otevřete menu Úpravy/Předvolby.
3. Zvolte Kategorie/Podpisy.
4. Panel Ověření, tlačítko Další.
5. Panel Integrace s Windows
6. Ověřování podpisů, zaškrtnout.
7. Ověřování certifikovaných dokumentů, zaškrtnout.

Časté problémy s ověřením

- Porušení integrity dat = změna dat po podpisu => podpis VŽDY neplatný – nemá smysl dále ověřovat
- Často nejde o úmysl, ale může způsobit např. antivirus nebo podpisující protistrana nevhodným nastavení aplikace
- V okamžiku ověření nejsou dostupné informace o revokaci podpisu („Platnost podpisu neznámá“)
  - Neuplynula potřebná lhůta
  - Není důvěryhodný čas (časové razítko)
  - SW se nedokáže získat CRL nebo OCSP (např. z důvodu nastavení místní sítě)

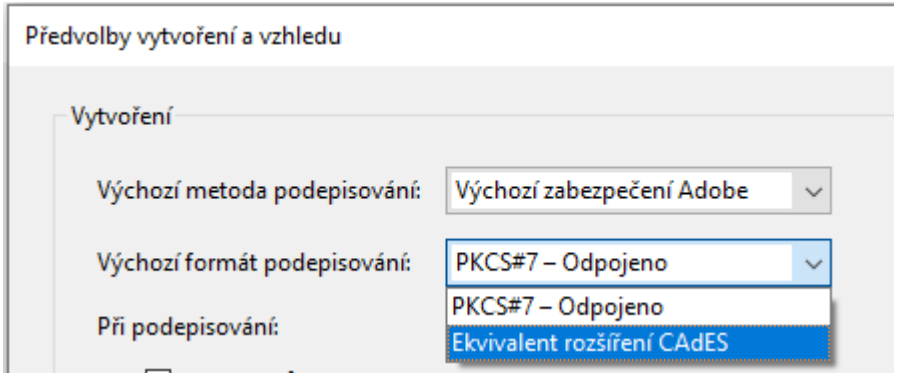
Vytváření kvalifikovaného el. podpisu

- Co potřebuji k podepsání dokumentu:
  - Dokument v **PDF**
  - Prostředek pro vytváření kvalifikovaných podpisů (**kvalifikovaný certifikát na tokenu**)
  - **Časové razítko**
  - **Program**, který umožňuje dokument **podepsat** a **označit časovým razítkem** (Adobe Reader*, eSSL, 602 Signer…)
  - Při podpisu **vybrat** správný certifikát (Qualified, nikoli Public!)

* nutno správně nastavit

Vytváření kvalifikovaného el. podpisu dle nařízení eIDAS v Adobe Reader DC

- Pouze pokud není k dispozici sofistikovanější nástroj
- Bez dodatečného nastavení produkuje pouze formát podpisu PKCS# 7/PAdES Basic, který není součástí eIDAS
- potřebujeme alespoň formát PAdES B
- Nutno nastavit: menu Úpravy -> Předvolby -> Podpisy -> Vytvoření a vzhled - Další... -> Výchozí formát podepisování změnit z PKCS#7 - Odpojeno na Ekvivalent rozšíření CAdES



Nastavení časových razítek v Adobe Reader

- Ideální je nastavení časových razítek ve spisové službě.
- Pokud chcete používat časová razítka i bez spisové služby, je potřeba si objednat službu časových razítek od kvalifikovaného poskytovatele.

Nastavení časových razítek v Adobe Readeru:

1. Otevřete menu Úpravy/Předvolby.
2. Zvolte Podpisy.
3. Panel Přidání časového razítka do dokumentu, tlačítko Další.
4. Tlačítkem [+] přidáme server TSA. Název a přihlašovací údaje dodá poskytovatel časových razítek.
5. Uložit.

- Pokud jste vše zadali správně, při každém elektronickém podpisu bude automaticky přidáno i časové razítko.