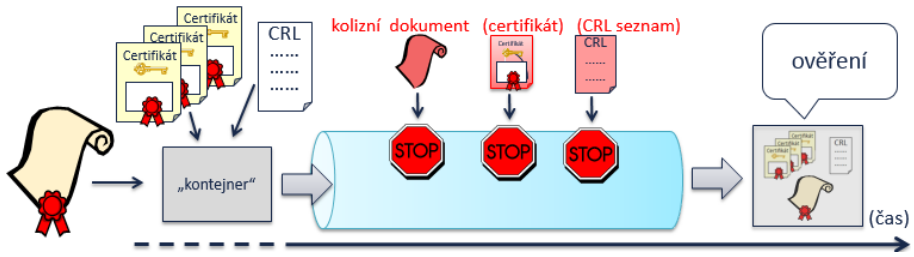
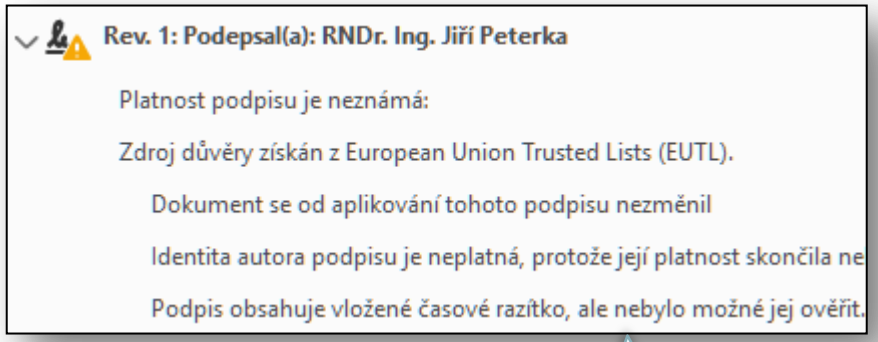
Blok 2: Uchovávání elektronických podpisů a pečetí



problémem je digitální kontinuita

- je to nové klíčové slovo (buzzword)
  - jehož význam není ještě zcela ustálen
    - není to pojem zákona
- intuitivně:
  - jde o zajištění „dlouhověkosti“ el. dokumentů
    - jejich „použitelnosti“, v horizontu měsíců, let, desetiletí, …
- zahrnuje (po technické stránce):
  - možnost seznámit se s jejich obsahem (čitelnost dokumentů)
    - použitelnost/čitelnost technických nosičů (diskety, CD, pásky, …..)
    - otázka formátů el. dokumentů – samostatná kapitola, zde neřešíme
      - lze řešit konverzí do nových formátů, nebo emulací původního prostředí, ve kterém lze pracovat s původními formáty
  - možnost spoléhat se, že jde o původní dokument (zajištění integrity)
    - zabránění jakékoli změně, nebo aspoň: možnost detekce libovolné změny
  - možnost spoléhat se na původ dokumentu (možnost ověření platnosti elektronických podpisů, značek a razítek)
    - možnost identifikovat podepsanou osobu, zjistit a prokázat platnost jejího podpisu či značky, prokázat dobu vzniku/existence podpisu, …..



aby se nám nestávalo toto

je dokument autentický?

je dokument pravý?

co se děje s podpisy, když plyne čas?

- pohled práva:
  - podpis je „napořád“
    - pokud je podpis váš (tj. je pravý), je vaším podpisem (pravým podpisem) už napořád
      - nelze říci „*tento podpis byl můj, ale teď už můj není*“

- vlastnoruční podpisy („na papíře“):
  - možnost jejich ověření se v čase může měnit
    - inkoust vysychá, papír bledne a chátrá, …..
  - ale: možnost ověření není nijak omezována (v čase)
    - nikdo/nic neříká: „po X letech již nelze podpis ověřit“

- elektronické podpisy:
  - možnost jejich ověření je v čase omezována
    - zcela záměrně a programově

dlouhověkost elektronických podpisů

vlastnoruční podpis

podpis je platný

platnost podpisu lze ověřit

čas

????????

elektronický podpis

podpis je platný

platnost podpisu lze ověřit

platnost podpisu nelze ověřit

možnost ověření je nastavena pouze na tuto dobu

jsou podniknuta opatření na prodloužení možnosti ověřit platnost podpisu

elektronický podpis

podpis je platný

platnost podpisu lze ověřit

platnost podpisu lze ověřit

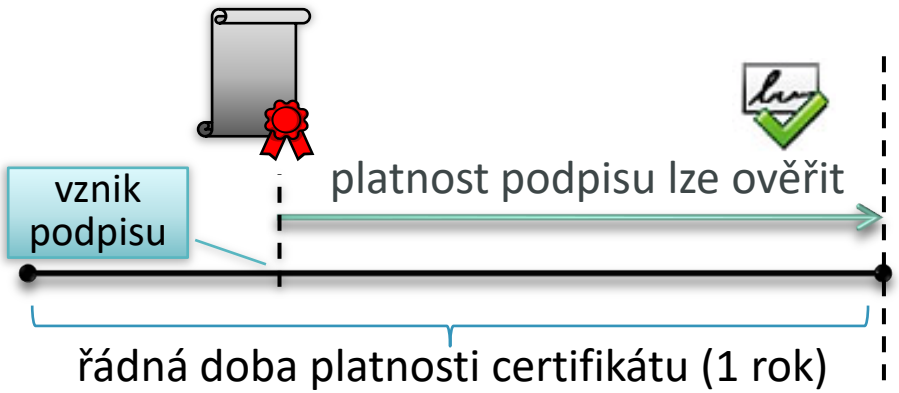
...lze ověřit

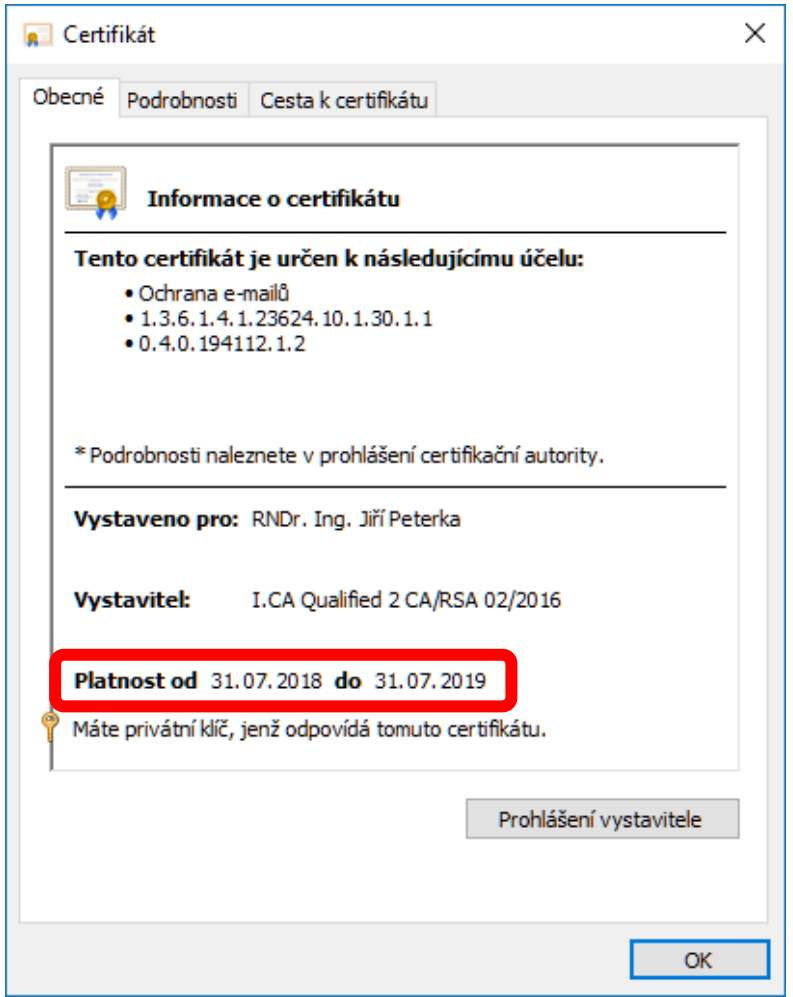
připojení časového razítka

připojení časového razítka

kde je časové omezení implementováno?

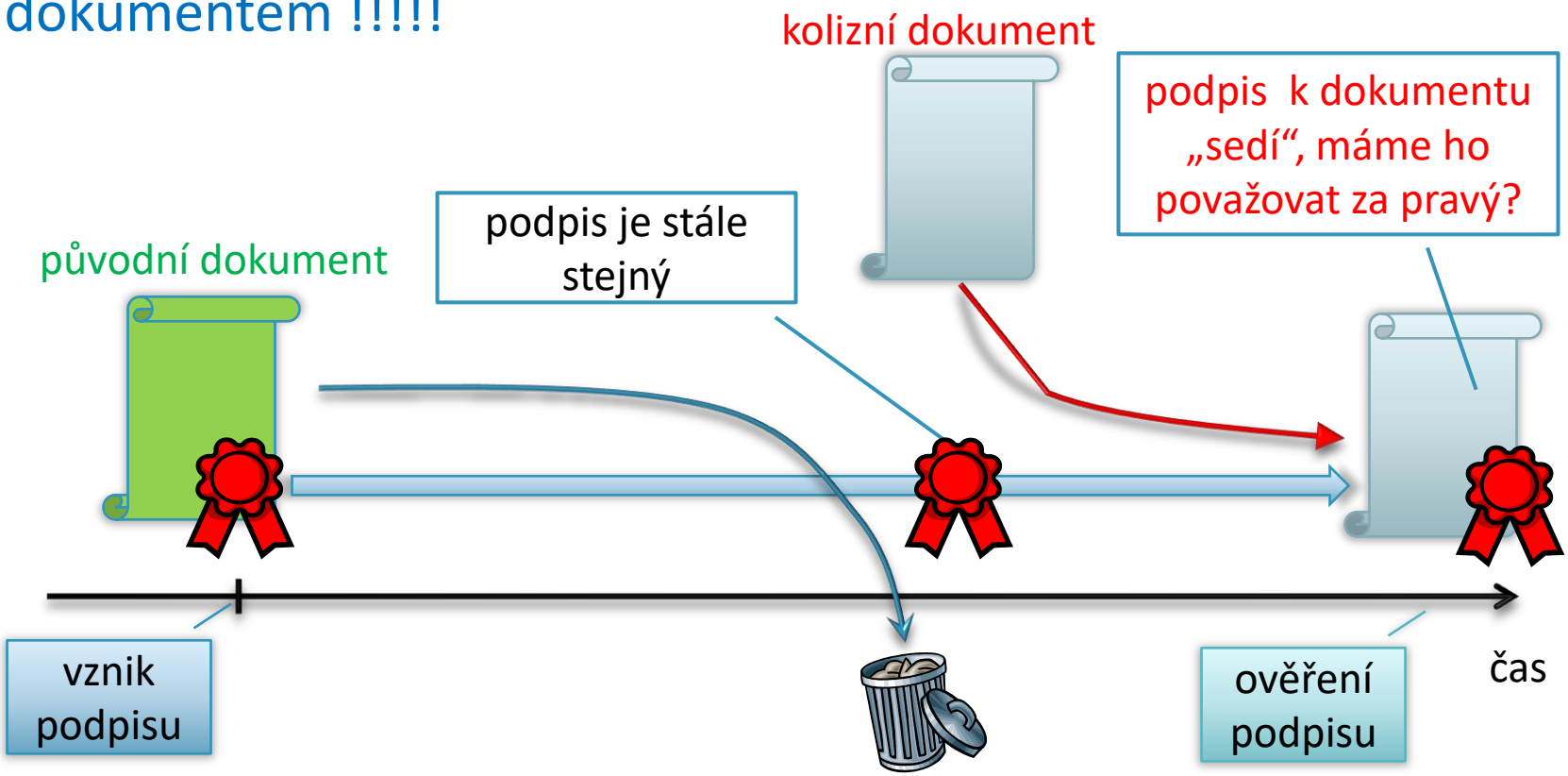
- v certifikátu: řádná doba jeho platnosti je časově omezena
  - tuzemské (podpisové) certifikáty jsou typicky vystavovány na 1 rok
    - řádná doba jejich platnosti trvá 1 rok
  - vydavatel certifikátu ručí za to, co je v něm napsáno, jen po dobu jeho řádné platnosti
- důsledek: certifikáty expirují
  - končí jim řádná doba platnosti
- důsledek (pokud se neprovedou konkrétní „nápravná“ opatření):
  - možnost ověřit platnost el. podpisu končí s koncem řádné doby platnosti (expirací) certifikátu





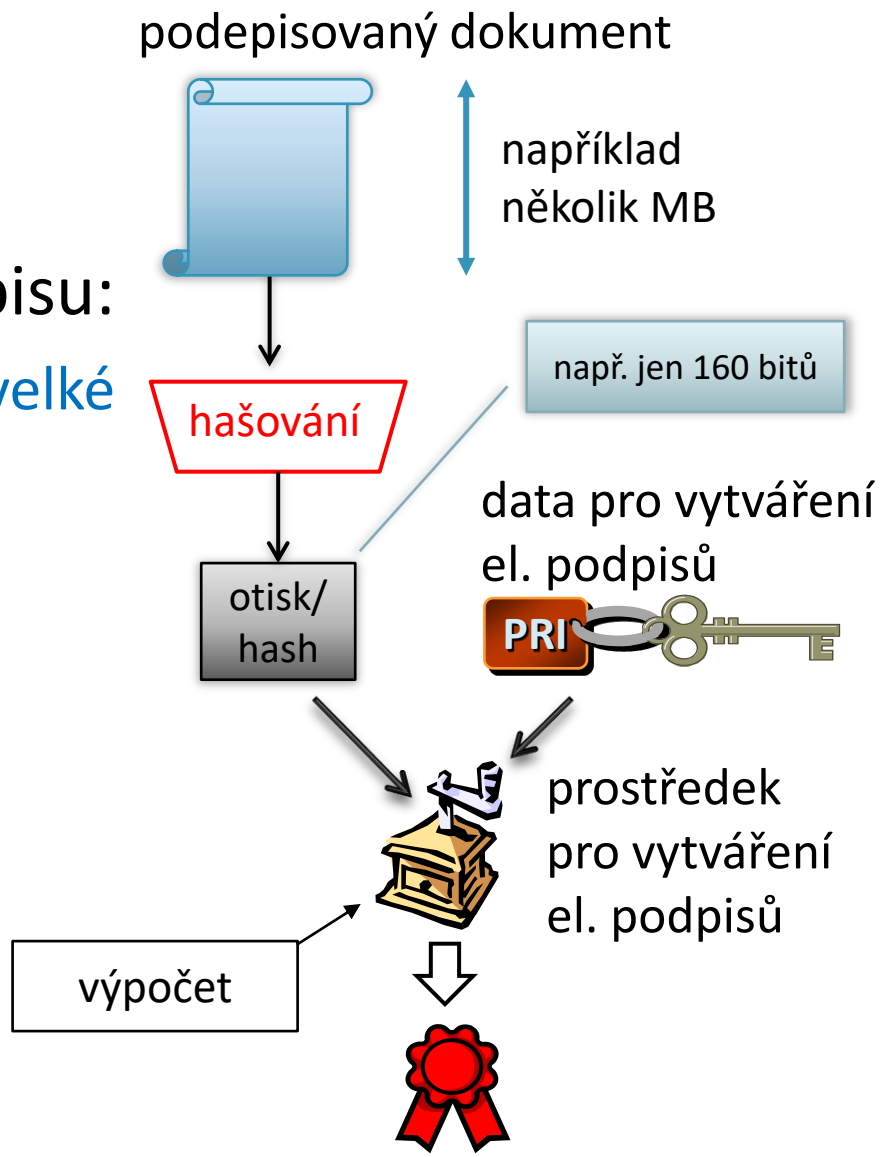
otázka: proč vůbec časové omezení?

- čeho se tak bojíme?
  - nebezpečí tzv. **kolizních dokumentů**
    - definice: dva dokumenty jsou kolizní, pokud jsou jiné, ale mají stejný elektronický podpis či značku
  - hrozí nebezpečí záměny původního dokumentu kolizním dokumentem !!!!!



odbočka: proč hašování?

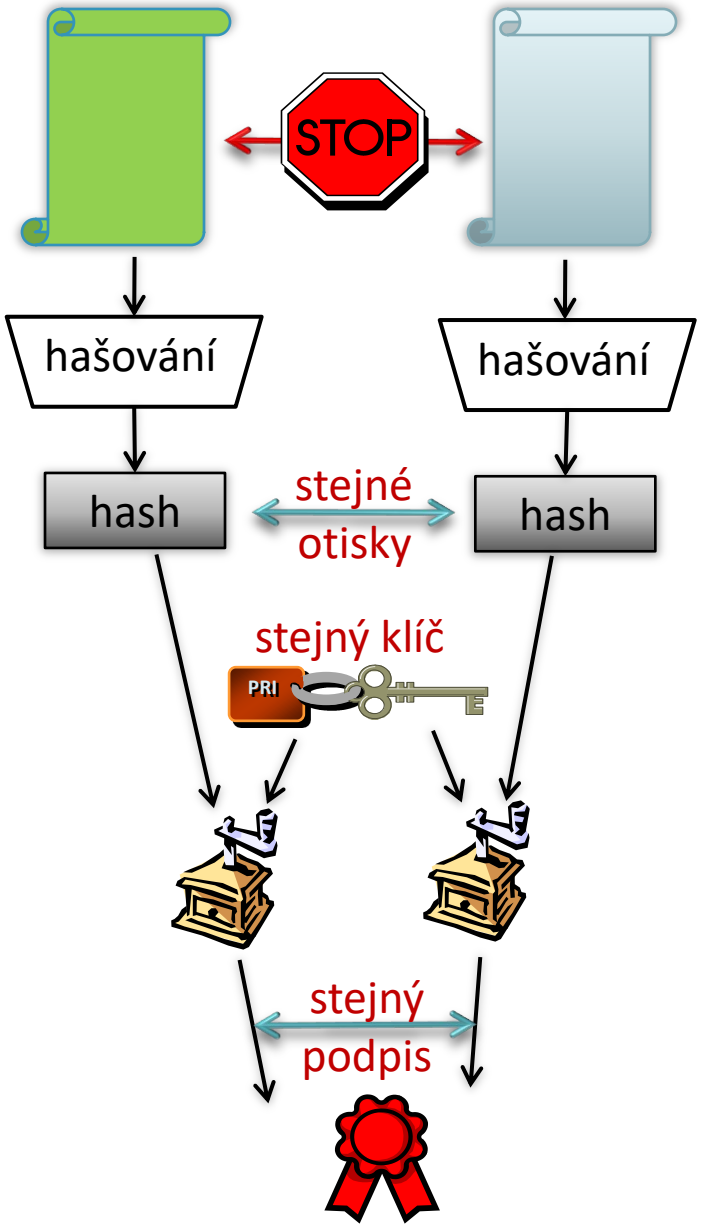
- uživatelé:
  - chtějí podepisovat různě velké dokumenty
- algoritmy elektronického podpisu:
  - dokáží podepisovat pouze pevně velké (malé) bloky dat
- proto:
  - z libovolně velkého dokumentu se nejprve udělá pevně velký **otisk** (tzv. **hash**)
    - pomocí tzv. **hašovací funkce**
      - např. jen 160 bitů, 256 bitů
  - teprve tento otisk se podepíše



problém: existuje nekonečně mnoho různých dokumentů, které mají stejný otisk !!!!

jak může elektronický podpis „fungovat“?

- díky tomu, že hledání kolizních dokumentů (fakticky: jejich výpočet) je neúnosně dlouhé
  - nemůže být kratší, než „nějaké miliony let“
    - a podvodníkovi se nevyplatí je hledat
- ale:
  - je to vztaženo k výpočetní síle našich počítačů
    - a ta velmi rychle roste !!!!
      - co dnešním počítačům trvá miliony let, ty budoucí stihnou třeba za hodinu
- proto:
  - je nutné neustále zvyšovat složitost výpočtu (hledání kolizních dokumentů)
- jak?
  - používání „silnějších“ hašovacích funkcí
  - používáním delších klíčů
  - .....



jak přitvrzovat?

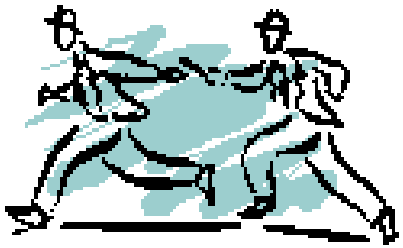
- složitost hledání (výpočtu) kolizního dokumentu je dána především:
  - použitou hašovací funkcí
    - dříve se používala SHA-1, dnes SHA-2, časem SHA-3
  - velikostí použitých klíčů (soukromého a veřejného)
    - dříve 1024 bitů, dnes 2048, časem …….

jde o celou skupinu funkcí:
SHA-256, SHA-384, SHA512

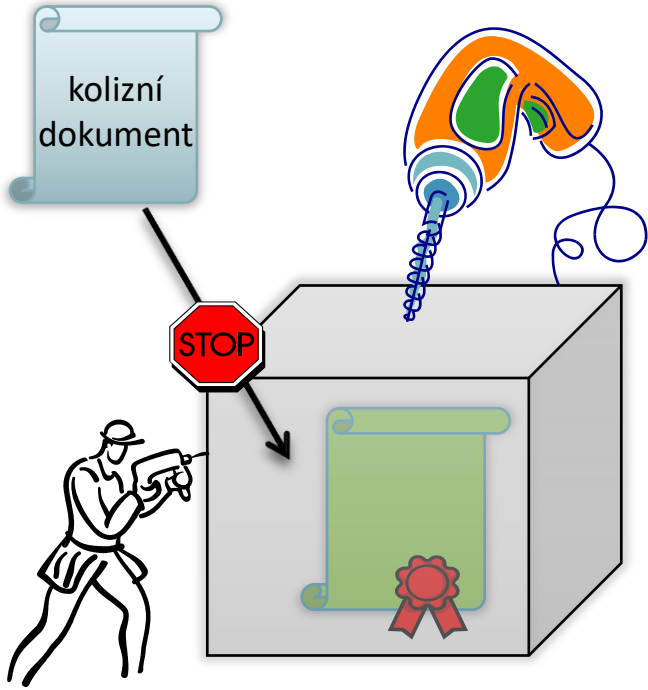
- proto:
  - na elektronický podpis (pečeť) se můžeme spoléhat jen do té doby, než hašovací funkce (a délky klíčů) zastarají
    - než se stanou příliš slabými (vzhledem k výpočetní síle dostupných počítačů)
- řešení:
  - nově zabezpečit (podepsat, opatřit pečetí či časovým razítkem)
    - a přitom použít novější (dostatečně silné) hašovací funkce a klíče !

kdy přitvrzovat?

- aby složitost hledání (výpočtu) kolizního dokumentu vyrovnávala růst schopností počítačů, je nutné
  - **neustále ji předbíhat, nikoli jen dohánět**

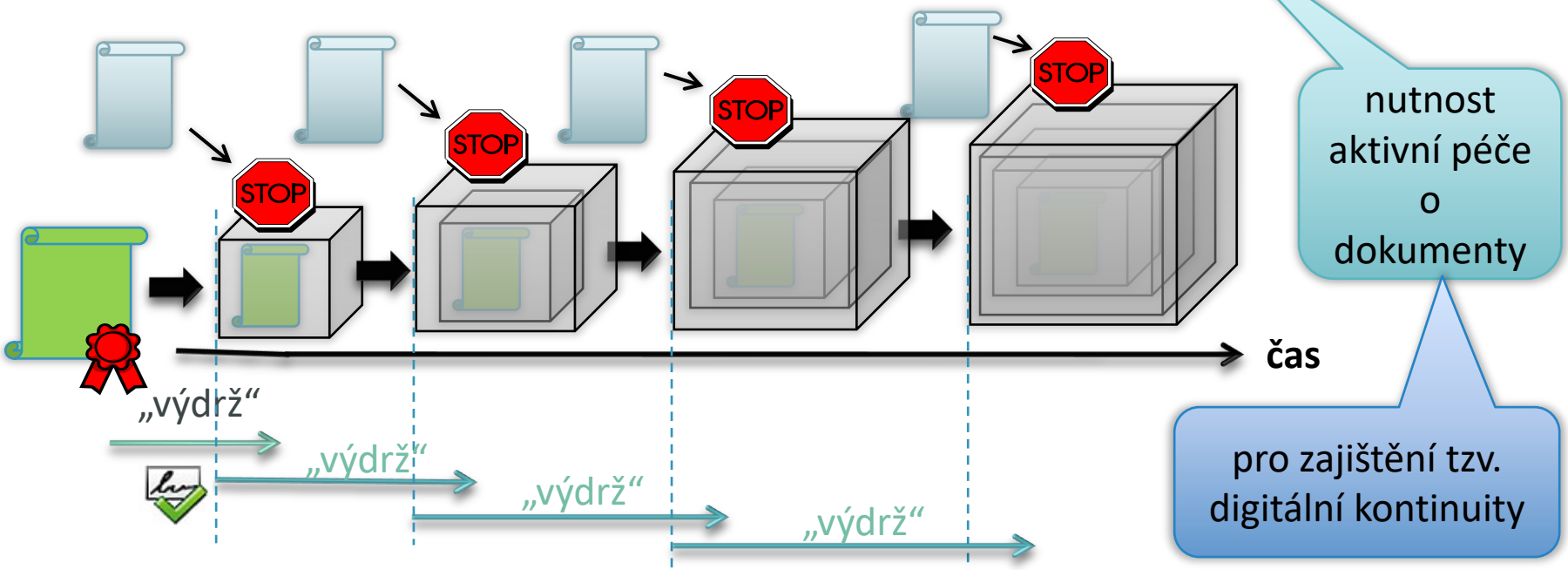


- jinými slovy:
  - chceme-li zachovat možnost ověření platnosti podpisu, musíme neustále a včas (dopředu) „přitvrzovat“
    - používat stále „silnější“ ingredience el. podpisů
      - novější hašovací funkce, větší klíče
- přirovnání:
  - podepsání el. dokumentu je jako jeho uzavření do bezpečnostní schránky
    - její „robustnost“ je pevně dána, nemění se
  - snaha nalézt kolizní dokument odpovídá snaze provrtat tuto schránku a zaměnit dokumenty
    - útočníci mají stále lepší vrtačky a tvrdší vrtáky
      - časem schránku provrtají !!!



koncept postupného přitvrzování

- připomeňme si, že:
  - pomyslná bezpečnostní schránka má jen omezenou „tvrdost“ a protistrana ji časem dokáže „navrtat“ a proniknout do ní
    - najít kolizní dokument a zaměnit ho za původně podepsaný
  - proto schránka (možnost ověření) „vydrží“ jen po omezenou dobu !!!
- řešení:
  - ještě dříve, než skončí „výdrž“ schránky, ji uzavřít do další schránky
    - ještě větší, ještě robustnější



jak zajistit postupné přitvrzování?

- technicky: je nutné
  - vytvořit nový otisk (použít novou - silnější hašovací funkci)
  - „semlít“ otisk s (novým - větším) soukromým klíčem

- může jít o elektronický podpis
  - technicky je to ok
  - ale právně to ok být nemusí

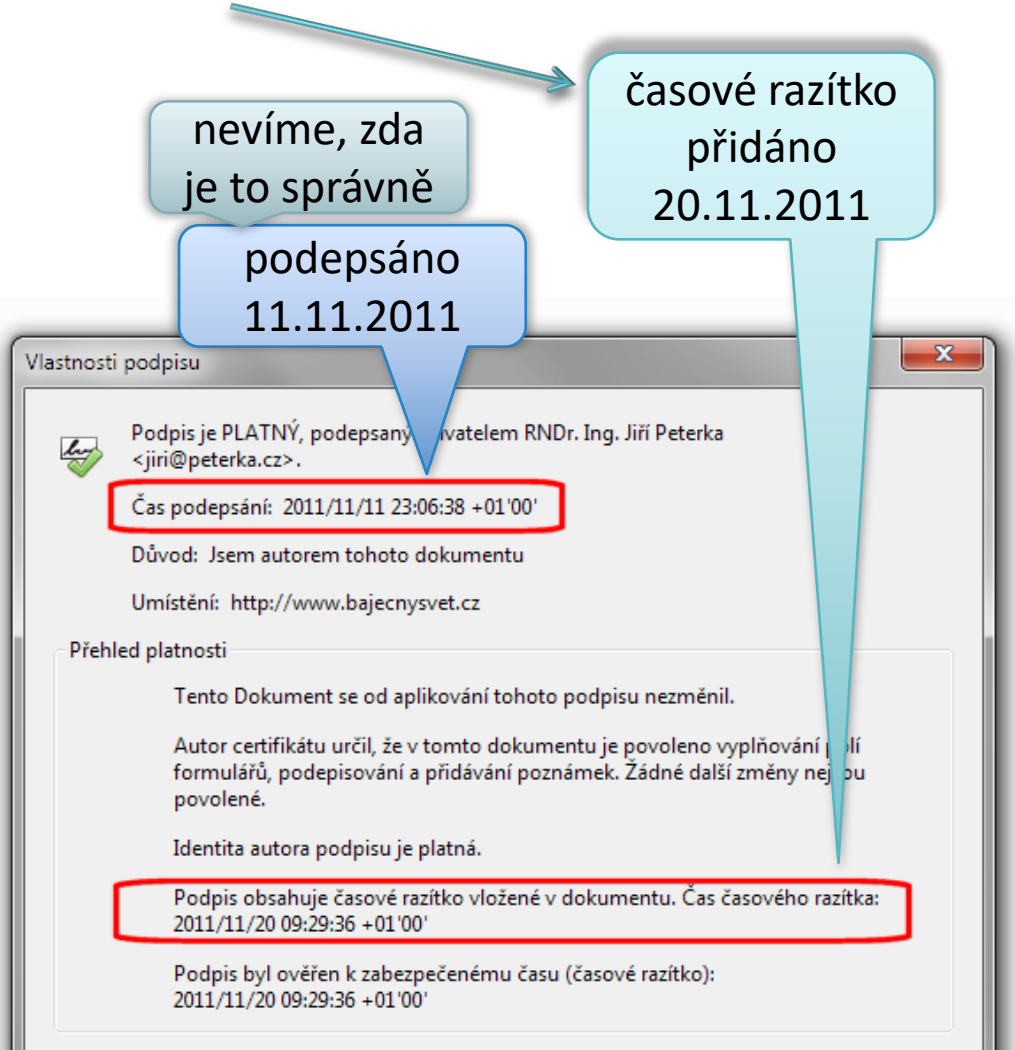
- problém:
  - podpis je projevem vůle vůči dokumentu
    - navíc předpoklad: podepisující osoba se seznámila s obsahem
  - dokument může být v péči třetí osoby
    - která se stará o digitální kontinuitu dokumentů
    - ale ta nemá co projevovat svou vůli vůči dokumentu

- může jít o časové razítko
  - technicky: stejné jako podpis
  - právně: má úplně jiný statut

- výhoda:
  - přidání časového razítka není projevem vůle
    - ani nemůže – ten, kdo razítko vytváří, se nemůže seznámit s obsahem dokumentu
      - pracuje pouze s otiskem
  - fixuje dokument a podpis v čase
    - garantuje, že již existoval v čase, který je v časovém razítku uveden

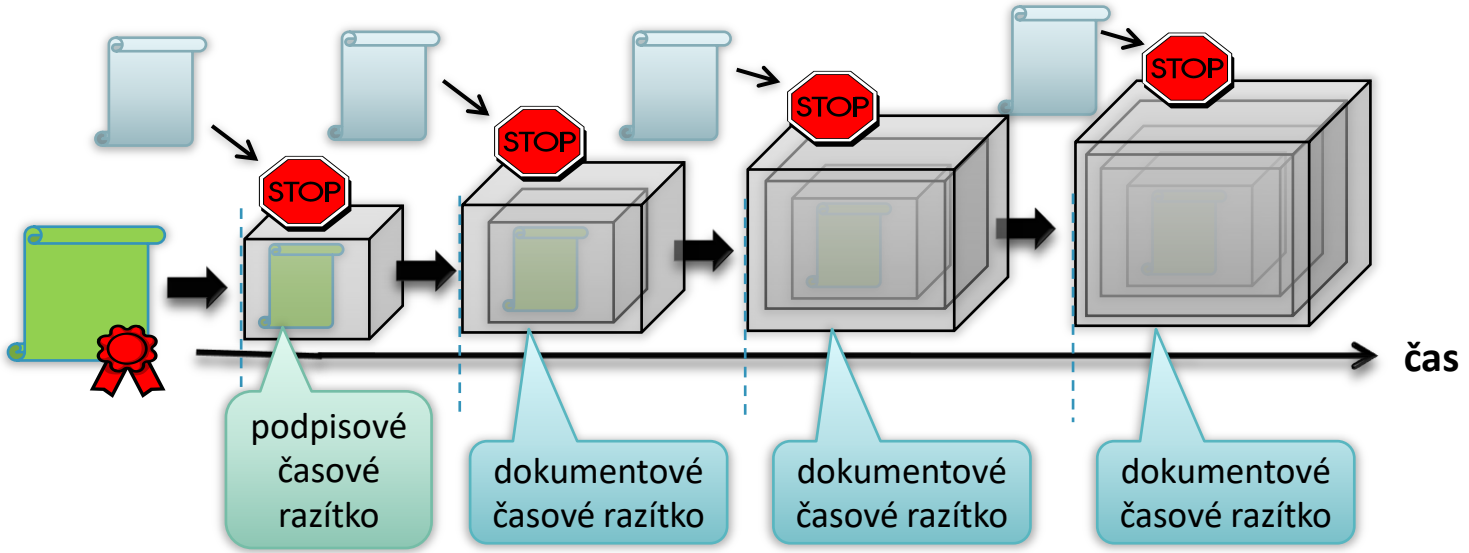
co osvědčuje časové razítko?

- kvalifikované časové razítko (Nařízení eIDAS)
  - platí [pro něj] domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny.
- jak tomu rozumět?
  - neříká, kdy podpis vznikl !!!!
    - jen kdy už existoval !!
  - časové razítko může přidat kdokoli
    - nemusí to být podepisující osoba
  - časové razítko může být přidáno později
    - třeba několik dnů/týdnů/měsíců po vzniku podpisu

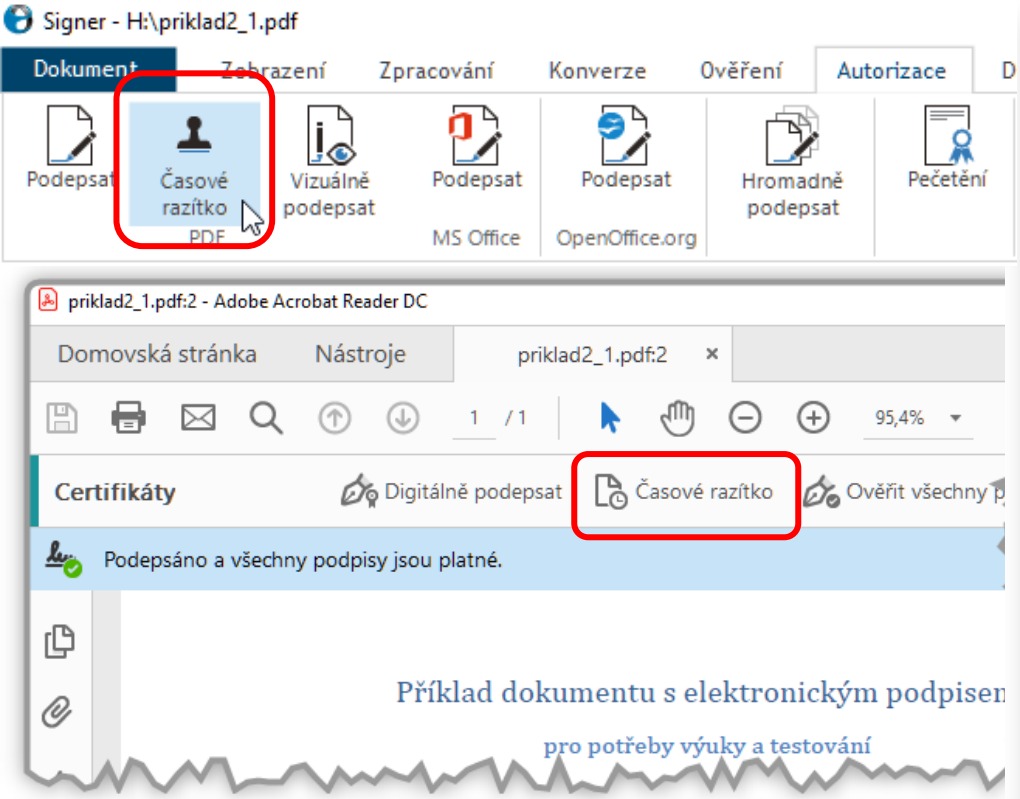


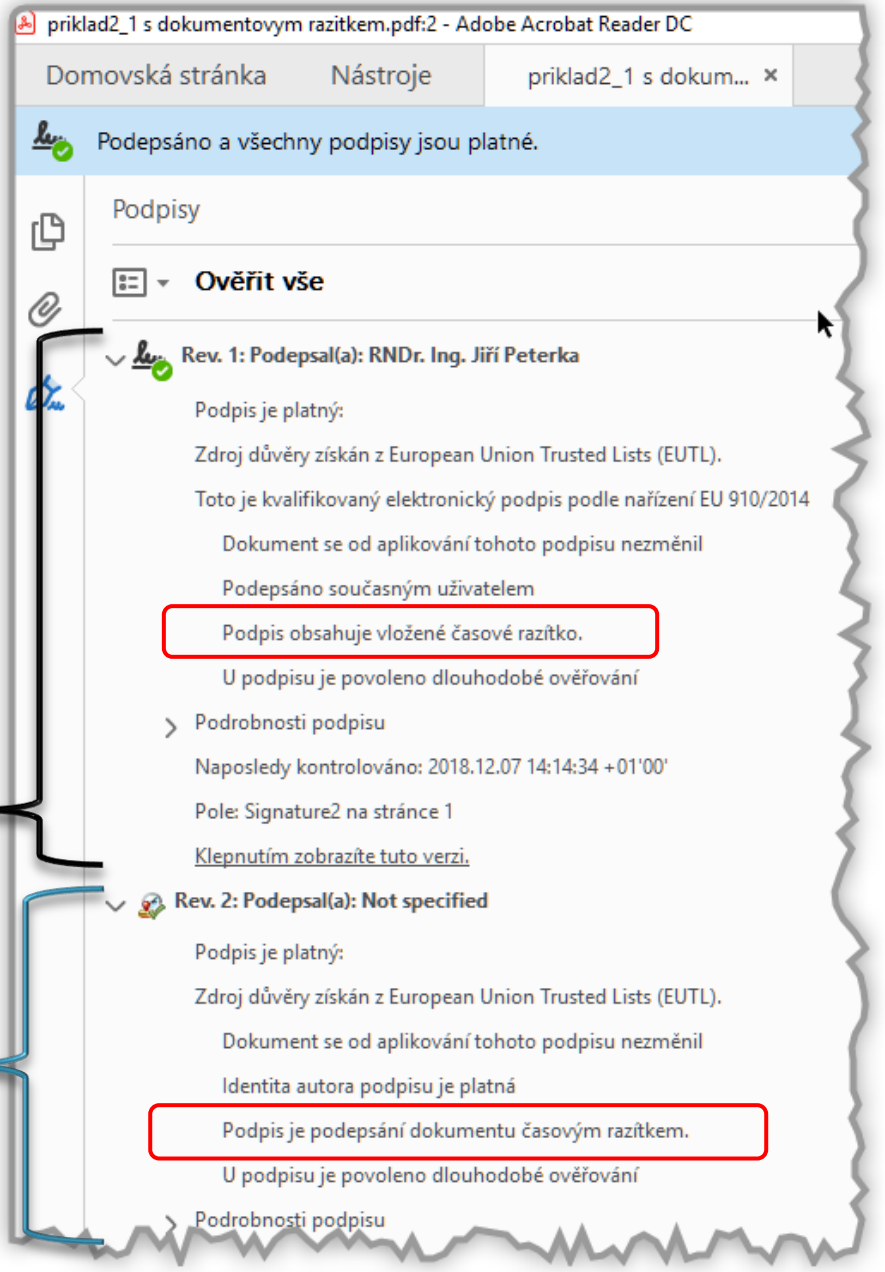
podpisové a dokumentové časové razítko

- právně:
  - časové razítko je samostatným objektem (např. vyhláška 212/2012 Sb.):
    - *…. je-li k datové zprávě podepsané elektronickým podpisem nebo označené elektronickou značkou připojeno platné kvalifikované časové razítko …..*
- technicky existuje:
  - podpisové časové razítko
    - je „vloženo“ přímo do podpisu, vztahuje se k němu
      - ke každému podpisu může být jen 1 podpisové časové razítko !!
  - dokumentové časové razítko (někdy též: archivní)
    - je „vloženo“ do dokumentu, vztahuje se k celému dokumentu i všem jeho podpisům
      - dokumentových časových razítek může být více (libovolně)



podpisové a dokumentové časové razítko

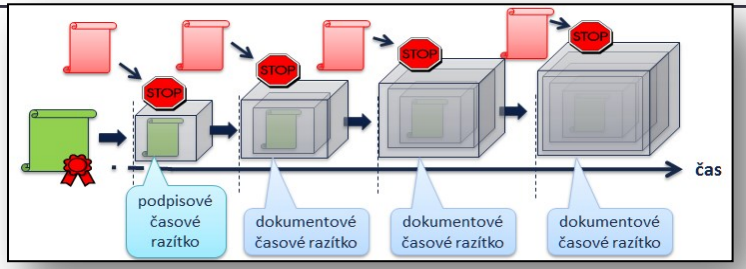




podpis a podpisové časové razítko

dokumentové časové razítko

odbočení: validační informace



- dosud naznačený postup chrání proti nebezpečí kolizních dokumentů
  - ale nemusí stačit
    - …. pro ověření platnosti původního podpisu po nějaké delší době
- problémem může být (bude) ještě něco jiného
  - po delší době již nemusí být (nebudou)dostupné všechny informace, nezbytné pro ověření platnosti konkrétního el. podpisu (značky, pečetě, čas. razítka)
    - jde o tzv. **validační informace** (informace, potřebné pro validaci), které tvoří:

1. certifikáty
   - podpisové certifikáty, certifikáty autorit, …..

zde problém nebývá – certifikáty se obvykle přikládají k samotnému el. podpisu

2. revokační informace
   - informace o (případném) předčasném zneplatnění (tzv. revokaci) některého certifikátu

zde problém bývá – revokační informace s časem přestávají být dostupné podpisu

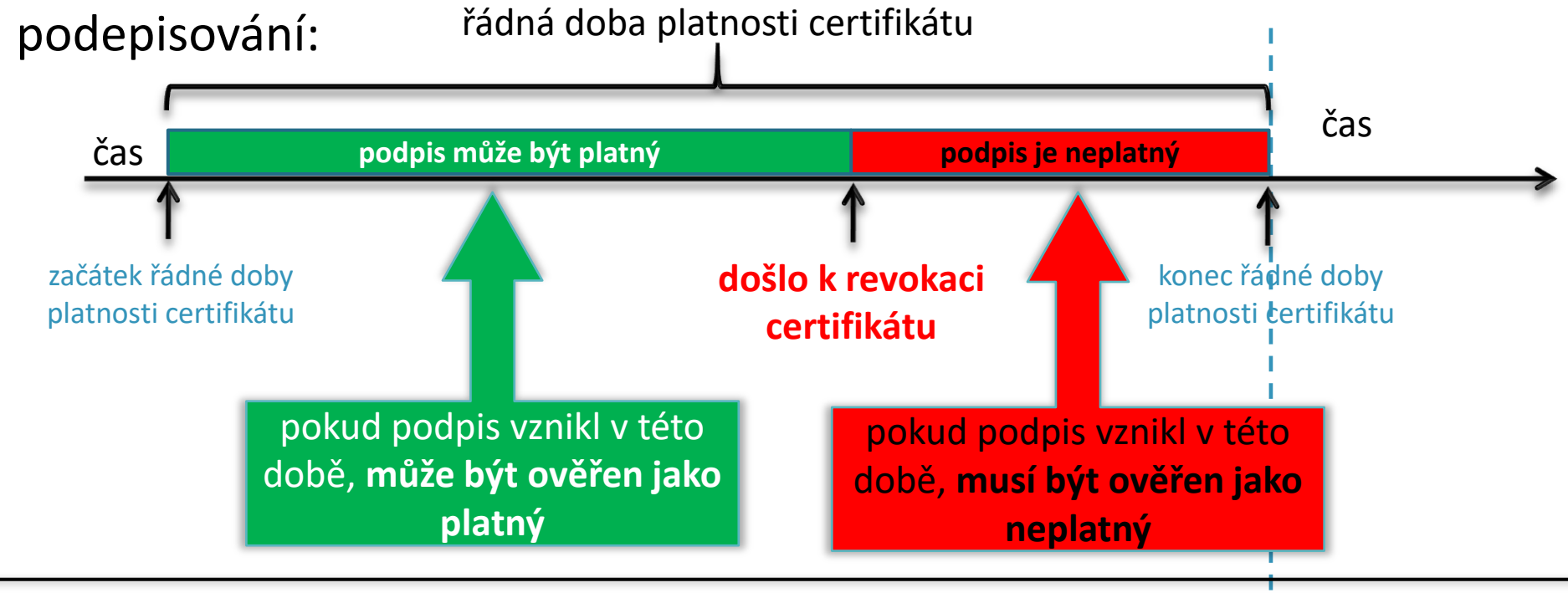
odbočení: co je revokace?

- též: předčasné zneplatnění
- analogie:
  - když ztratíte platební kartu, okamžitě požádáte banku o její zneplatnění
    - obdobně: když ztratíte svůj soukromý klíč (resp. celý kvalifikovaný prostředek), necháte si předčasně zneplatnit (revokovat) certifikát, vydaný k tomuto klíči
      - aby se nový držitel vašeho soukromého klíče nemohl platně podepisovat za vás ….
  - když má úředník (úřední) razítko a odchází do důchodu, razítko odevzdá
    - obdobně: když zaměstnanec přestane být zaměstnancem, zaměstnavatel nechá předčasně zneplatnit (revokovat) certifikát zaměstnance
      - aby se původní držitel nemohl nadále platně podepisovat jako zaměstnanec …..
- praktický problém:

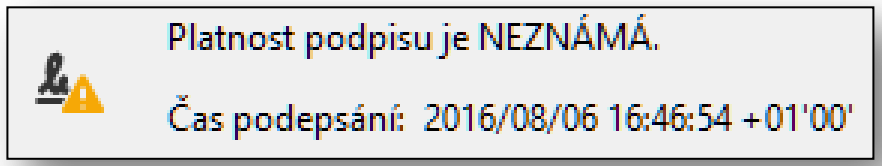
bez jejich dostupnosti se nedá ověřit platnost !!

  - informace o (případné) revokaci se s časem stávají nedostupné !!!
    - jejich dostupnost je garantována jen po dobu řádné platnosti certifikátu
  - analogie: vydavatel certifikátu vyvěšuje tyto informace na nástěnku
    - která ale nemá neomezenou kapacitu – proto jsou informace po čase mazány !!

důsledky revokace certifikátu

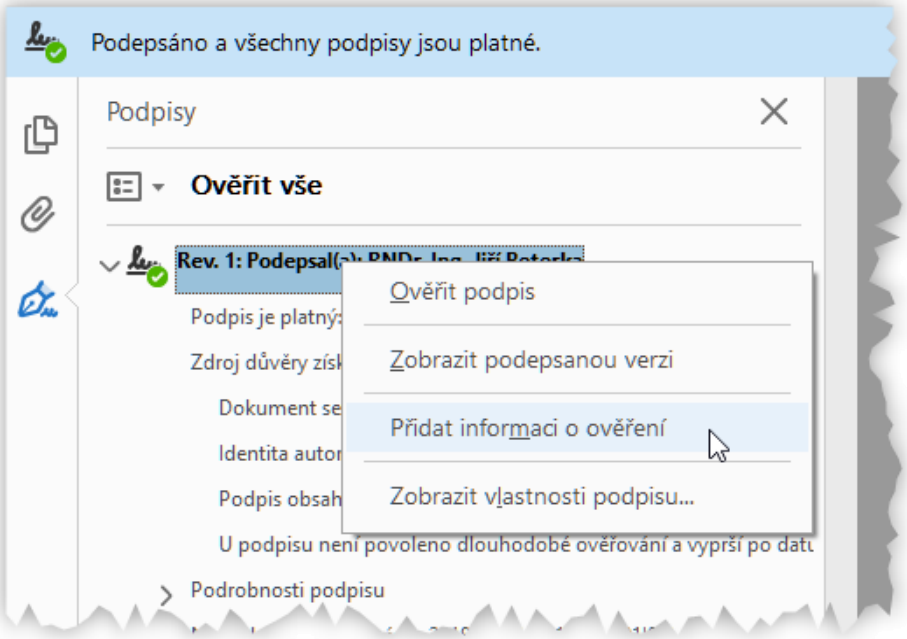


- bez dostupnosti informací o revokaci není možné dokončit proces ověřování platnosti podpisu/pečetě/značky/razítka !!!
  - ověření skončí „pokrčením ramen“
    - výsledkem: platnost je neznámá ....

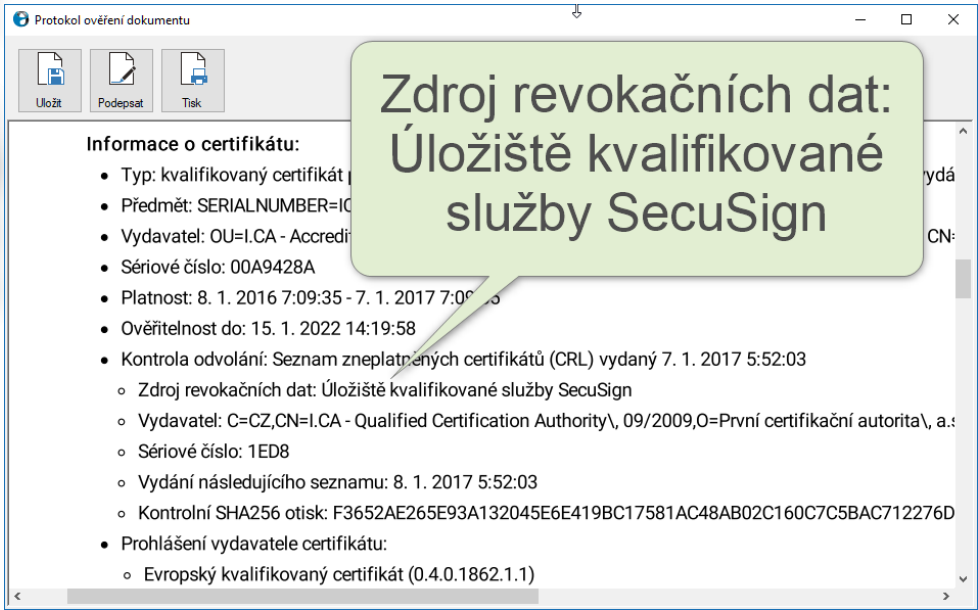


problém s nedostupností revokačních informací

- dá se řešit dvěma způsoby:
  - informace získat ještě v době, kdy jsou dostupné, a přiložit je k podpisu
    - většina používaných programů to umožňuje

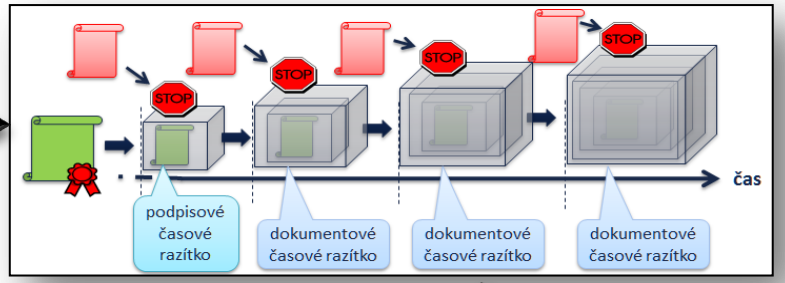


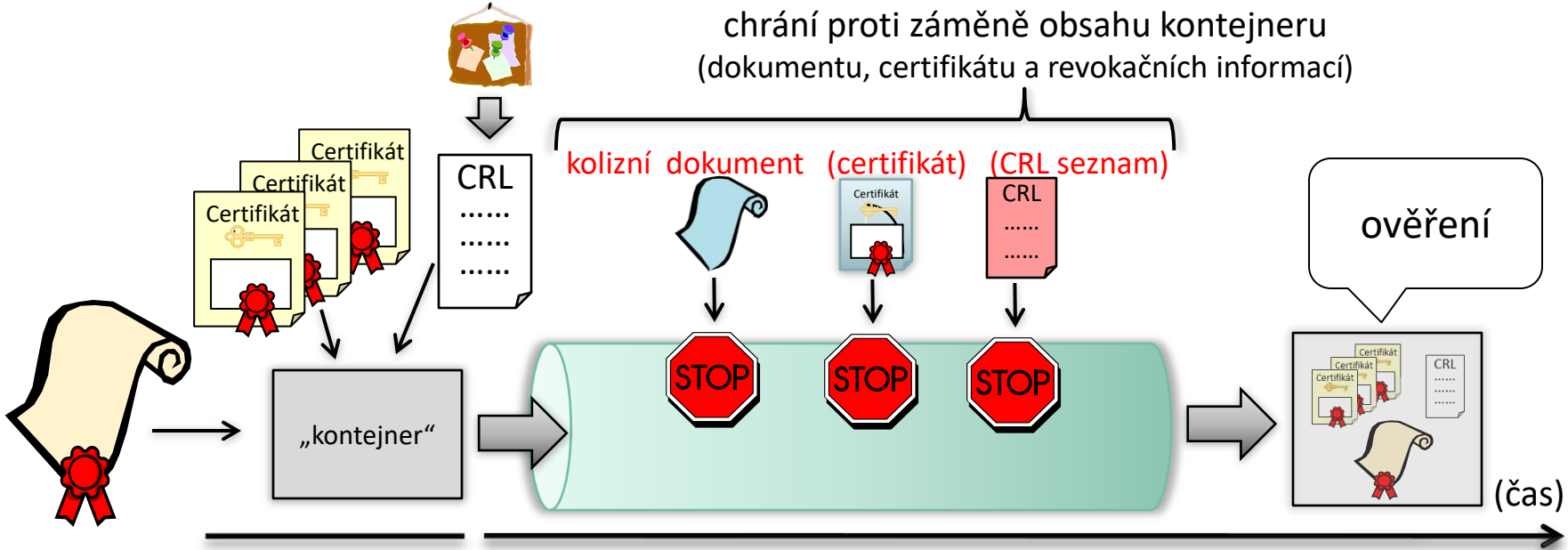
  - správně by to měly být informace, vydané za dobu delší než 24 hodin po podepsání (připojení časového razítka)
  - získat potřebné informace „nějak jinak“
    - například: mít je v zásobě
      - systematicky je sbírat a archivovat, pro pozdější využití
    - takto to dělají (např.):
      - CzechPOINT, některé validátory
      - kvalifikované služby pro ověřování
        - příklad: SecuSign



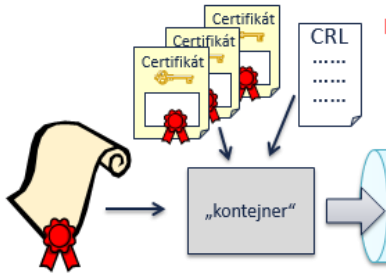
„dlouhodobé“ elektronické podpisy

- musí vyřešit:
  - zajištění integrity (aby nic nemohlo být změněno)
    - řeší se dříve popsaným způsobem
  - dostupnost všech validačních informaci
    - certifikátů a revokačních informací
- princip **LTV (Long Term Validation)** podpisů:
  - všechny nezbytné informace se shromáždí v době, kdy jsou ještě k dispozici
    - a „zabalí“ i s dokumentem a podpisy do vhodného kontejneru
  - kontejner se pak trvale chrání proti jakékoli změně
    - pravidelně opatřuje časovými razítky





referenční formáty

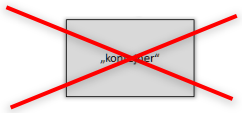
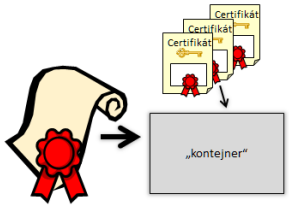
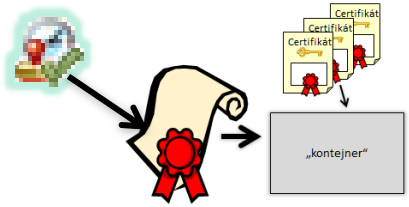
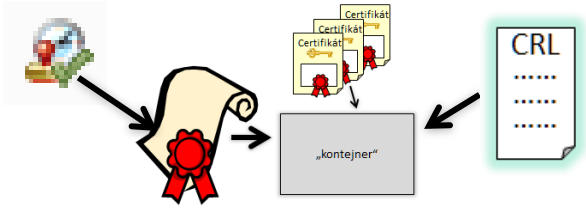
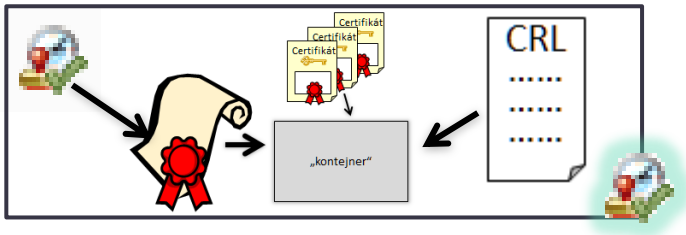


- důležitá podmínka:
  - elektronický podpis (pečeť) se musí chovat jako kontejner
    - do kterého lze „vkládat“ příslušné objekty
      - certifikáty, časová razítka, revokační informace
    - který chrání vložené objekty proti změně/záměně
- předpoklad:
  - musí existovat technické standardy, které definují formáty el. podpisů
    - jde o otázku technických standardů (v EU: standardy ETSI)
- pro el. podpisy (značky, pečetě) na PDF dokumentech
  - jde o formát **PAdES** (**PDF Advanced Electronic Signature**)
    - již v roce 2011 nabylo (přímé) účinnosti Rozhodnutí Komise č. 130/2011/ES, které ukládá (orgánům veřejné moci) používání tzv. referenčních formátů PAdES
    - dnes: používání referenčních formátů (po OVM) požaduje nařízení eIDAS a jeho prováděcí předpisy
  - jde o formáty **XAdES** (pro XML) a **CADES** (pro binární data)

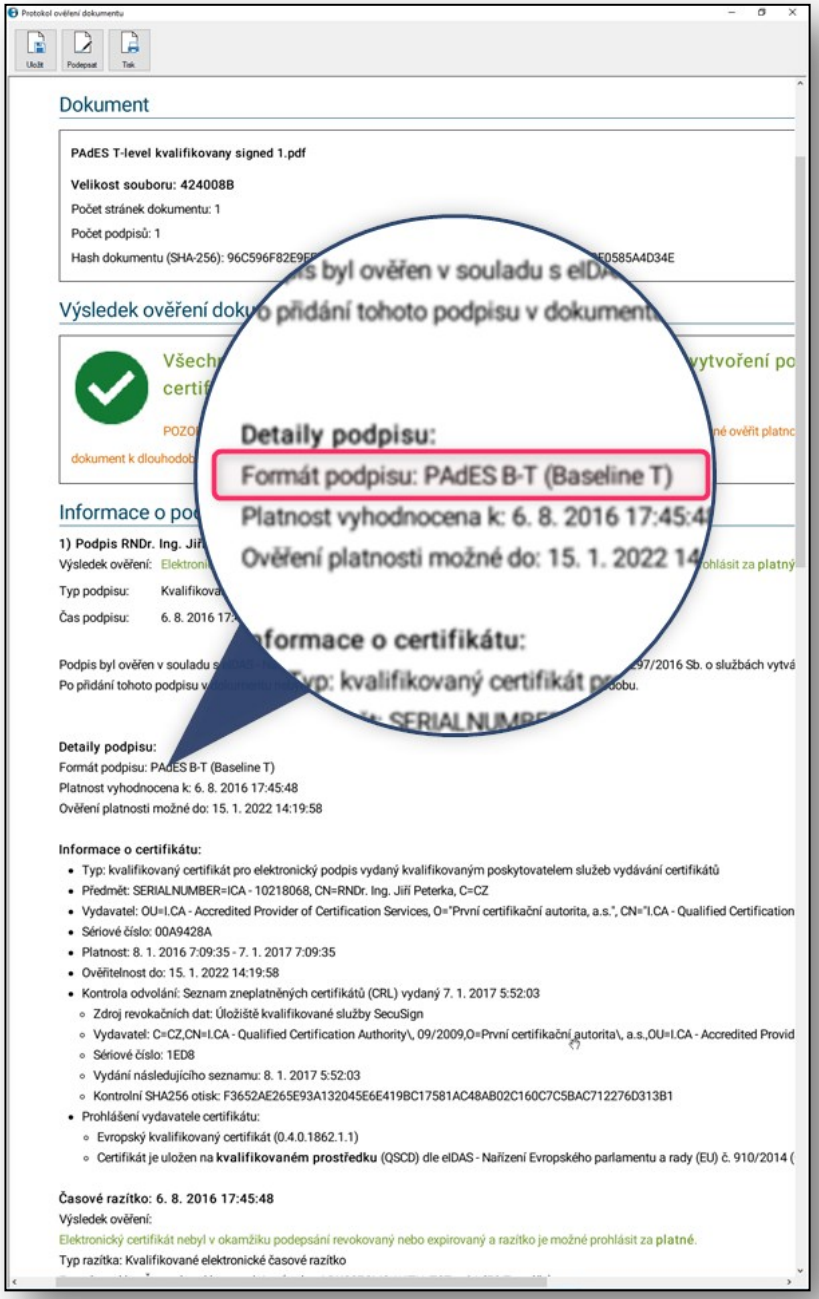
obecně se formáty s požadovanými vlastnostmi označují jako **referenční formáty**

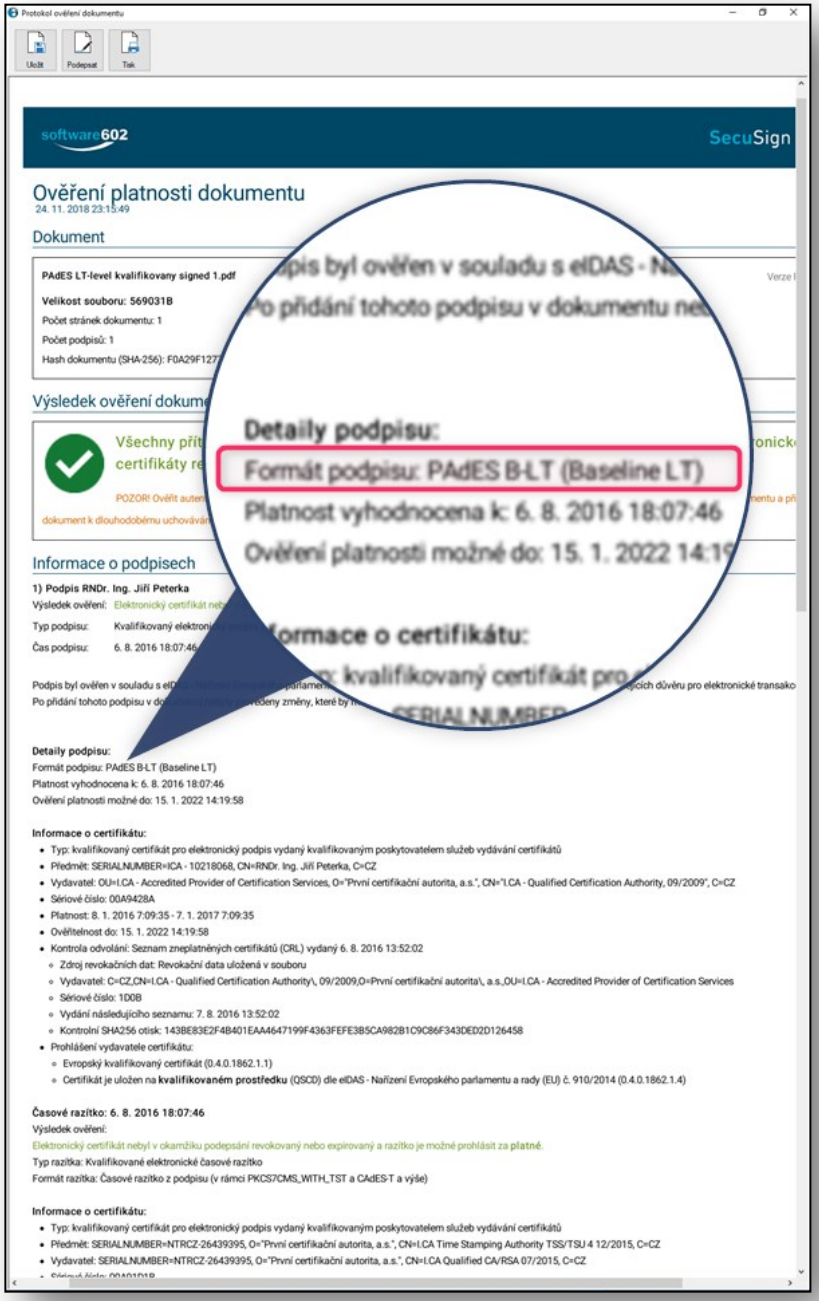
úrovně referenčních formátů

- ref. formáty mají více úrovní, podle toho, *„co se do kontejneru nasype“*

PAdES Basic nejde o referenční formát	 *nechová se jako kontejner s požadovanými vlastnostmi*
PAdES Baseline-B (úroveň B-B) B od: *„Basic“*	 jen samotný podpis
PAdES Baseline-T (úroveň B-T) T od: *„Timestamp“*	 podpis + časové razítko
PAdES Baseline-LT (úroveň B-LT) LT, od: *„Long Term“*	 podpis + časové razítko + revokační informace
PAdES Baseline-LTA (úroveň B-LTA) *„Long Term Archival“*	 podpis + časové razítko + revokační informace + dokumentové (archivní) časové razítko

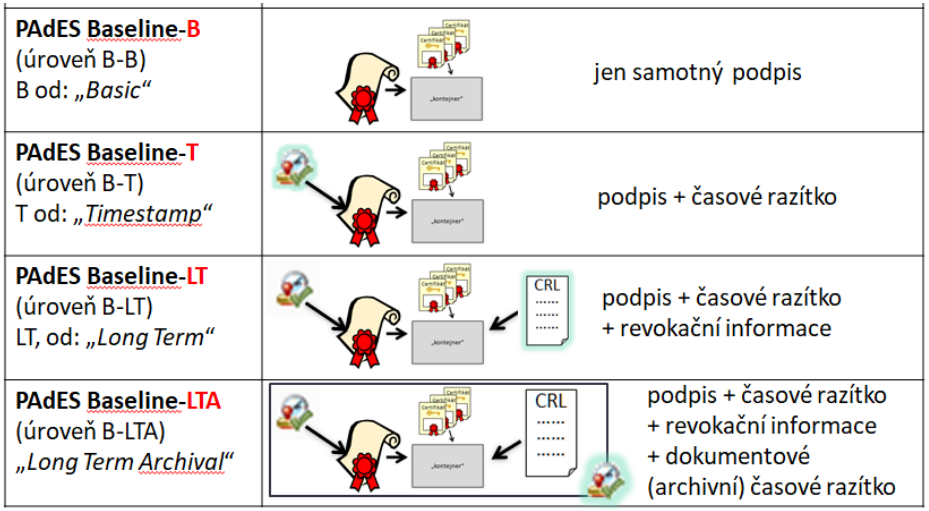
příklad: formát dle SecuSign





co se rozumí „uchováním“ el. podpisu?

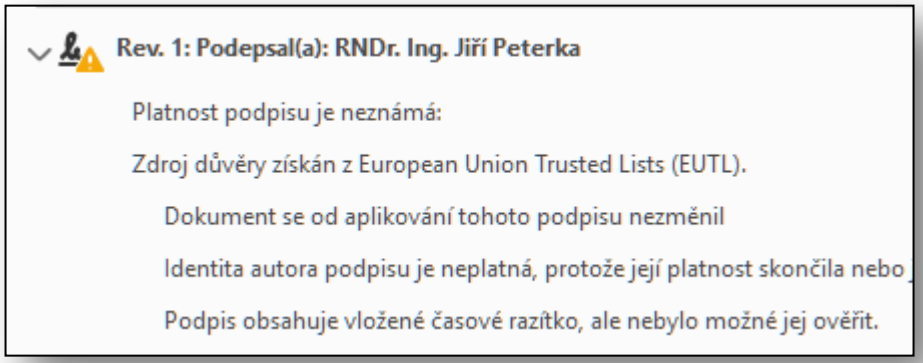
- nejde o „uchování“ ve smyslu uskladnění
  - zajištění dostupnosti i po delší době ….
- jde o „uchování“ ve smyslu zachování možnosti ověření platnosti !!!
  - provádí se „nápravná opatření“ pro eliminaci časových omezení
- reálně:
  - jde o přidávání dalších (dokumentových, archivních) časových razítek
    - včetně přidávání nezbytných validačních informací
      - certifikátů a revokačních dat
    - případně o (jednorázové) přidání podpisového časového razítka (pokud není)
      - a případně o změnu formátu podpisu na referenční
        - pokud je to nutné a možné – konkrétně v ISDS (datové schránky)



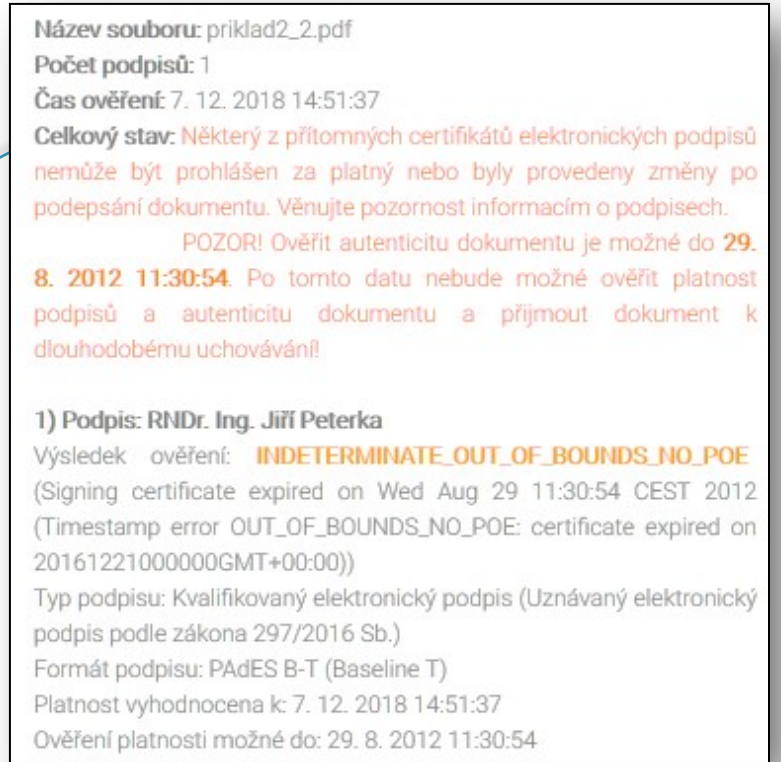
poprvé jde o převod do úrovně LTA, a pak o přidávání dalších dokumentových (archivních) časových razítek

příklad (priklad2_1.pdf)

- PDF dokument s elektronickým podpisem ve formátu PAdES-T:
  - certifikát podepisující osoby měl řádnou platnost od 30.8.2011 do 29.8.2012
  - podpis je opatřen „podpisovým“ časovým razítkem, které bylo přidáno 20.1.2012
    - razítko se opírá o certifikát s řádnou dobou platnosti od 21.12.2011 do 21.12.2016
  - k podpisu jsou připojeny revokační informace (ale k časovému razítku nikoli)
- platnost podpisu bylo možné ověřit jen do 21.12.2016 !!!!
  - do konce doby řádné platnosti certifikátu časového razítka



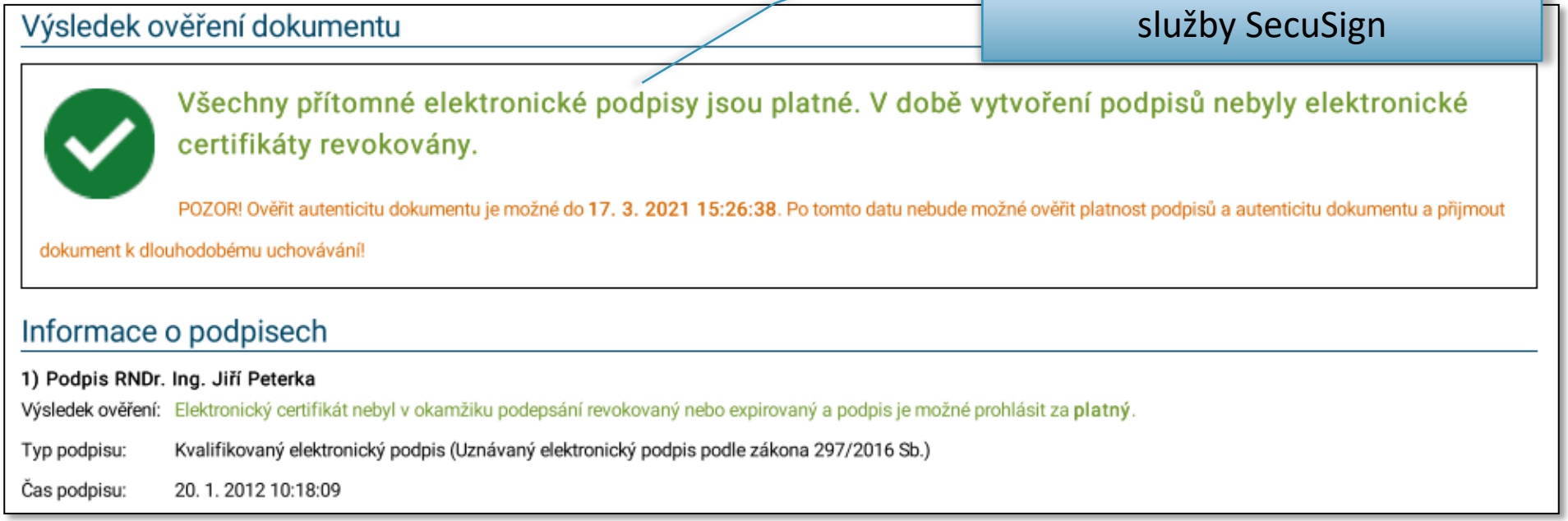
dnešní pokus o ověření pomocí kvalifikované služby SecuSign



příklad (priklad2_1_uchovany.pdf)

- původně: stejný dokument z roku 2012 (jako na předchozím slidu)
  - s možností ověření platnosti podpisu do 21.12.2016
- „uchování“ provedeno 2.8.2016 (tedy včas: před 21.12.2016)
  - připojeno kvalifikované dokumentové (archivní) časové razítko
    - opírá se o certifikát s platností od 17.3.2015 do 17.3.2021
- důsledek:
  - digitální kontinuita je zachována (možnost ověření platnosti byla prodloužena) do 17.3.2021

ověření pomocí kvalifikované služby SecuSign



Výsledek ověření dokumentu

Všechny přítomné elektronické podpisy jsou platné. V době vytvoření podpisů nebyly elektronické certifikáty revokovány.

POZOR! Ověřit autenticitu dokumentu je možné do **17. 3. 2021 15:26:38**. Po tomto datu nebude možné ověřit platnost podpisů a autenticitu dokumentu a přijmout dokument k dlouhodobému uchovávání!

Informace o podpisech

1) Podpis RNDr. Ing. Jiří Peterka

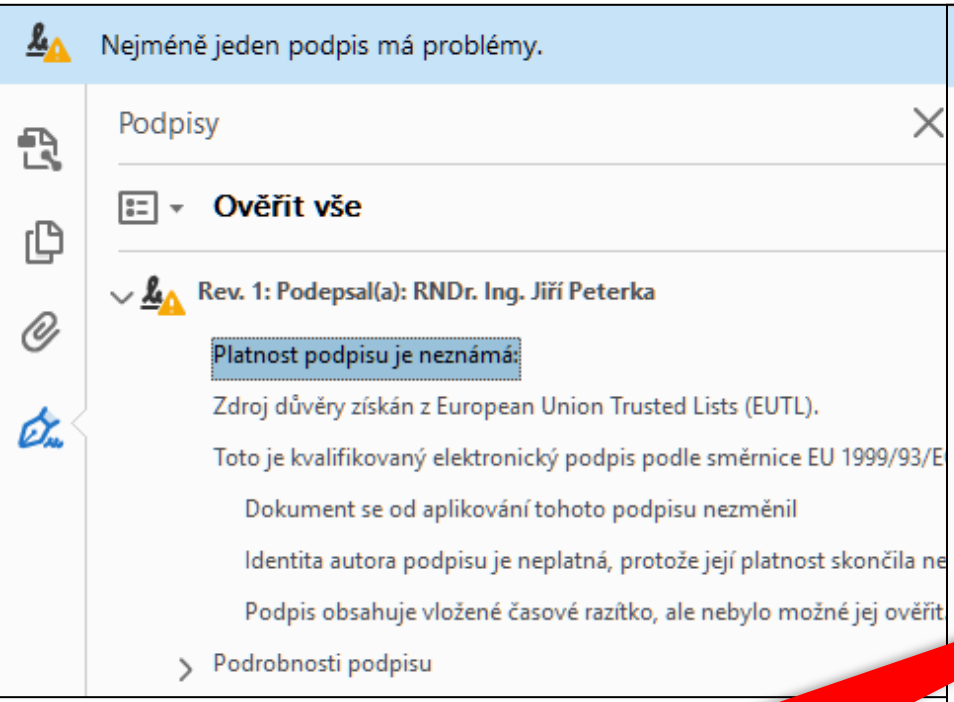
Výsledek ověření: Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za **platný**.

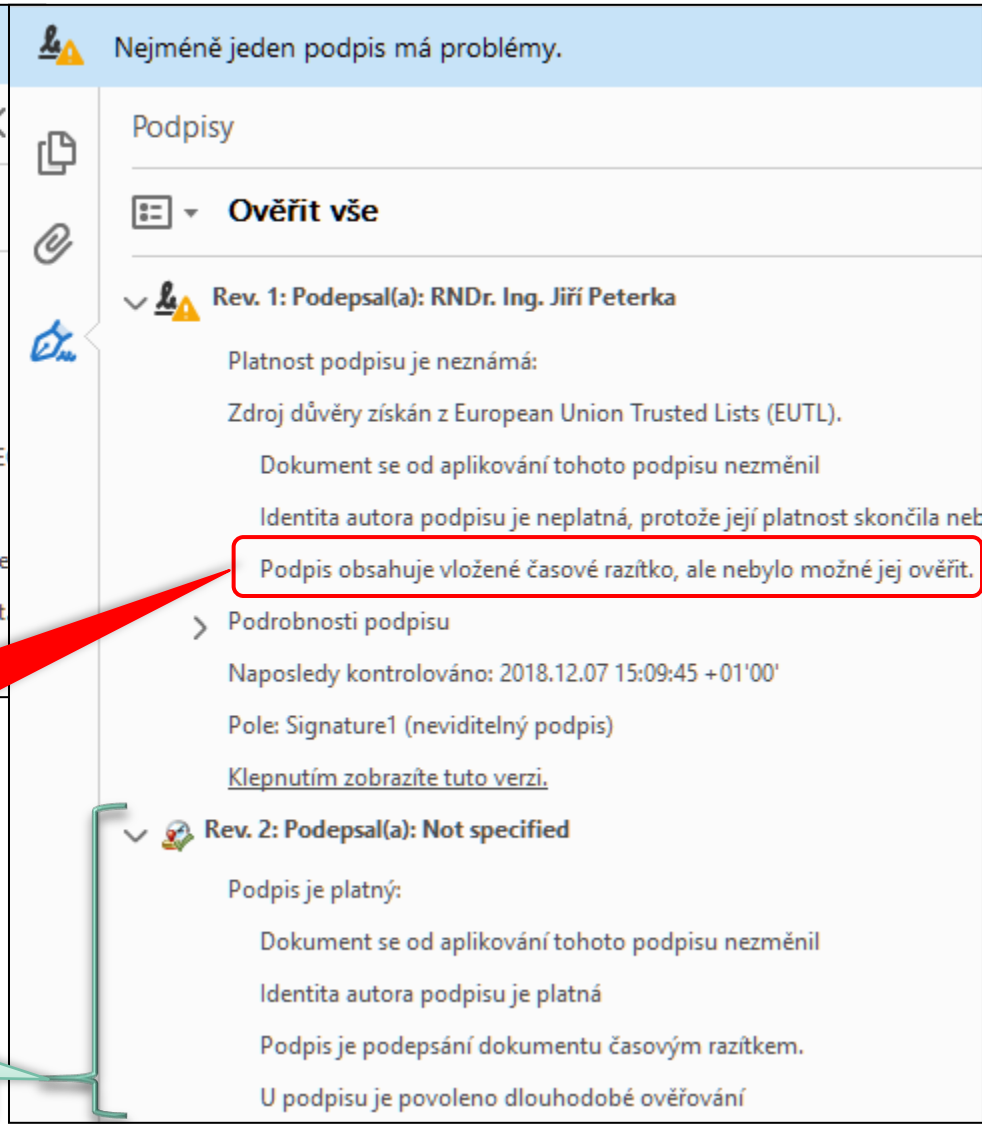
Typ podpisu: Kvalifikovaný elektronický podpis (Uznávaný elektronický podpis podle zákona 297/2016 Sb.)

Čas podpisu: 20. 1. 2012 10:18:09

příklad ověření (Adobe Reader)

- původní dokument z roku 2012
  - priklad2_1.pdf
- „uchovaný“ dokument (2016)
  - priklad2_1_uchovany.pdf



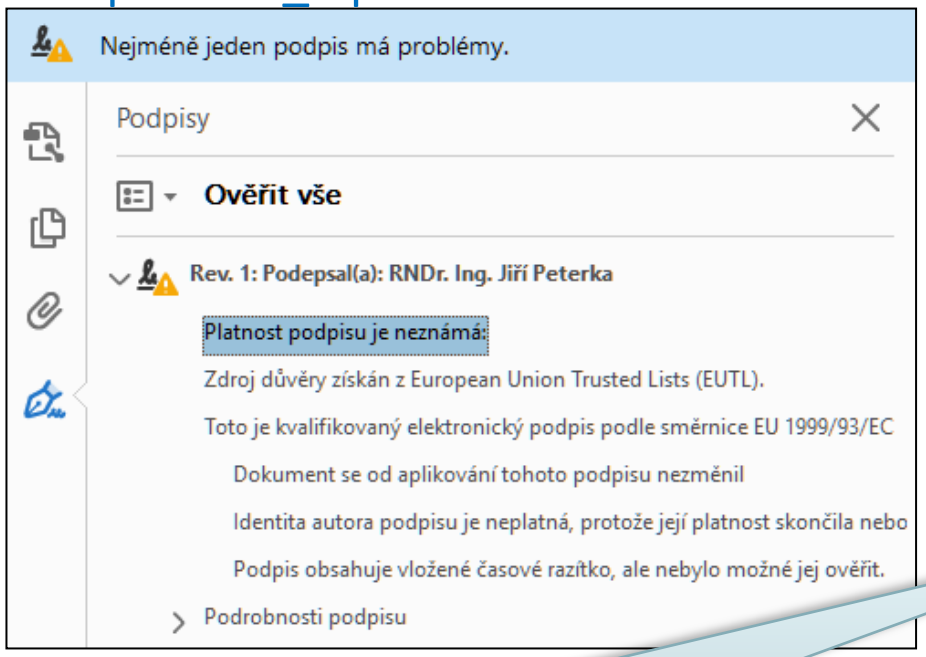


problém: Adobe Acrobat Reader stále nebere v úvahu (platné) dokumentové časové razítko (pro ověření podpisového razítka)

dokumentové (archivní) časové razítko

příklad ověření (Adobe Reader)

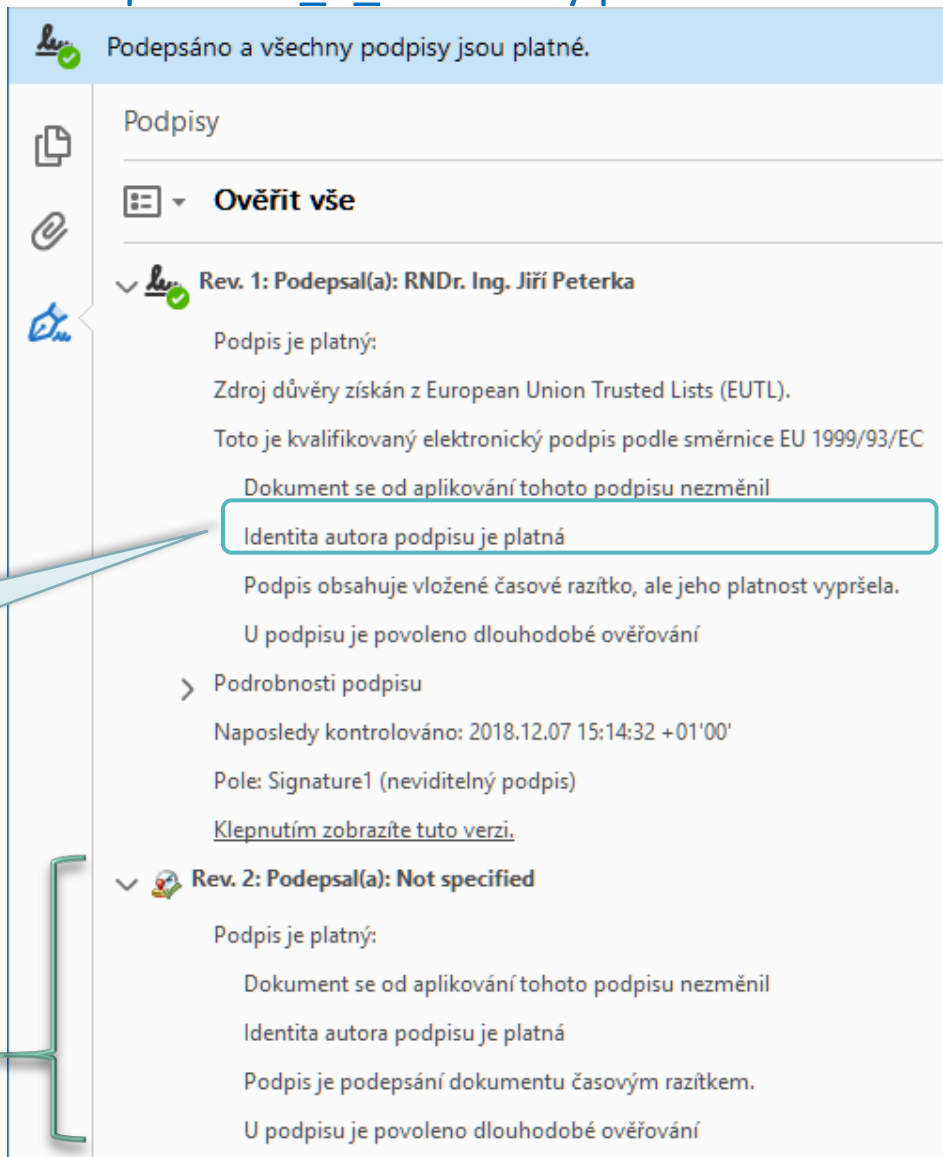
- původní dokument z roku 2012
  - priklad2_1.pdf



v nastavení (Předvolby, Podpis) lze Readeru předepsat, že má důvěřovat i „starším“ časovým razítkům

☑ Použít časová razítka ukončené platnosti

- „uchovaný“ dokument (2016)
  - priklad2_1_uchovany.pdf



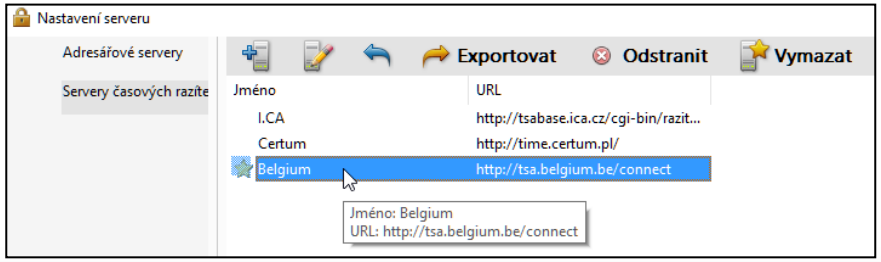
dokumentové (archivní) časové razítko

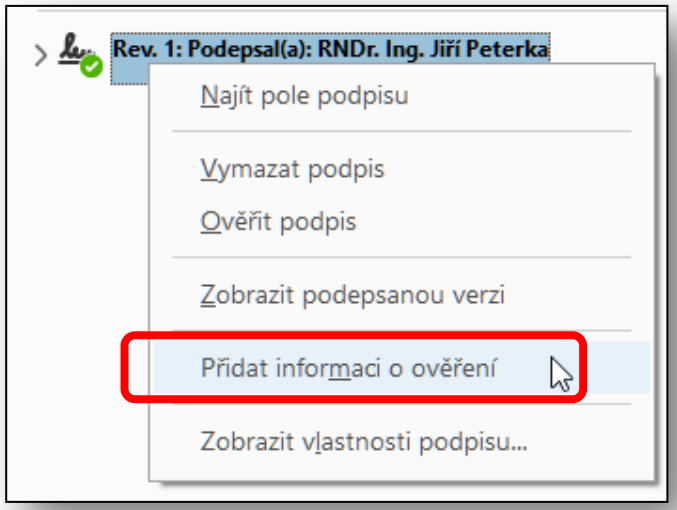
jak a kde provádět uchovávání?

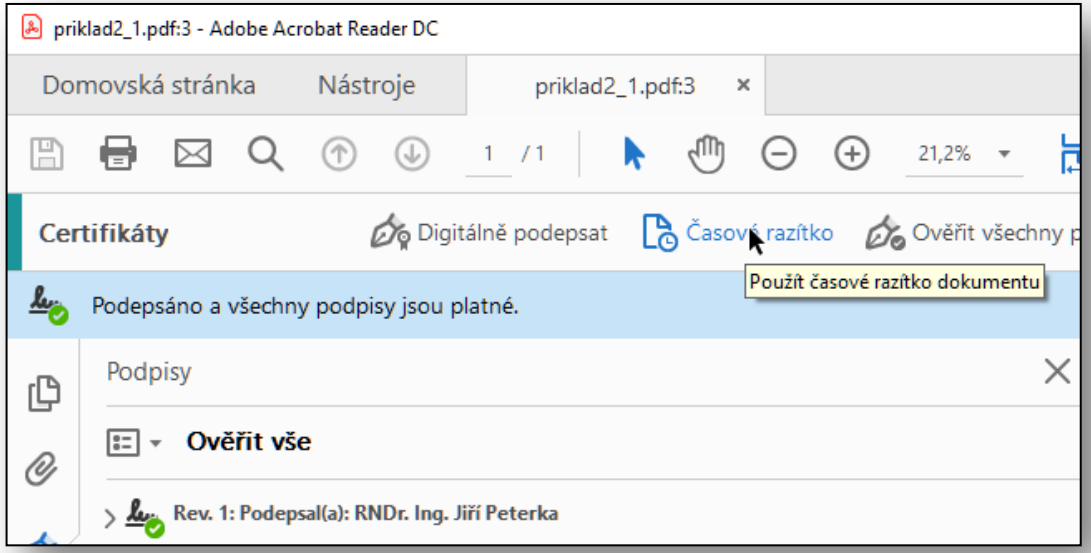
- připomenutí:
  - nejde o „uchovávání dokumentu“ ve smyslu ukládání (archivace, zajištění dostupnosti celého dokumentu), ale o „uchovávání podpisu/pečeti“ ve smyslu zachování možnosti ověřit platnost (a tím i možnost spoléhat se ….)
- principiální možnosti:
  - **„ručně“** (pro malé objemy dokumentů)
    - uživatelé sami iniciují provedení potřebných kroků
      - připojování časových razítek a revokačních informací
    - pomocí:
      - „univerzálních“ programů
        - např. Adobe Reader, …..
      - specializovaných programů
        - asi teprve vzniknou
      - (kvalifikovaných) služeb pro uchovávání
  - „strojově“
    - organizace si sama upraví svůj IS (např. spisovou službu) tak, aby včas přidávala k elektronickým dokumentům další (dokumentová) časová razítka a revokační informace
      - do budoucna: mělo by to být standardní funkčností IT systémů, které nakládají s elektronickými dokumenty
    - napojením svého IS na (kvalifikovanou) službu uchovávání
      - přes Api této služby

„ruční“ uchování (Adobe Reader)

- bezplatný Adobe Acrobat Reader umožňuje:
  - přidání revokačních informací (CRL seznamu či odpovědi OCSP)
    - pokud je podpis (či pečeť) ověřen jako platný
      - kliknout pravým tlačítkem na řádek s podpisem
      - zvolit „přidat informace o ověření“
    - umožňuje to ověření i v době, kdy revokační informace již nejsou dostupné
  - přidání samostatného (dokumentového) časového razítka
    - je nutné mít nastaven zdroj (kvalifikovaných) časových razítek
      - např. http://tsa.belgium.be/connect

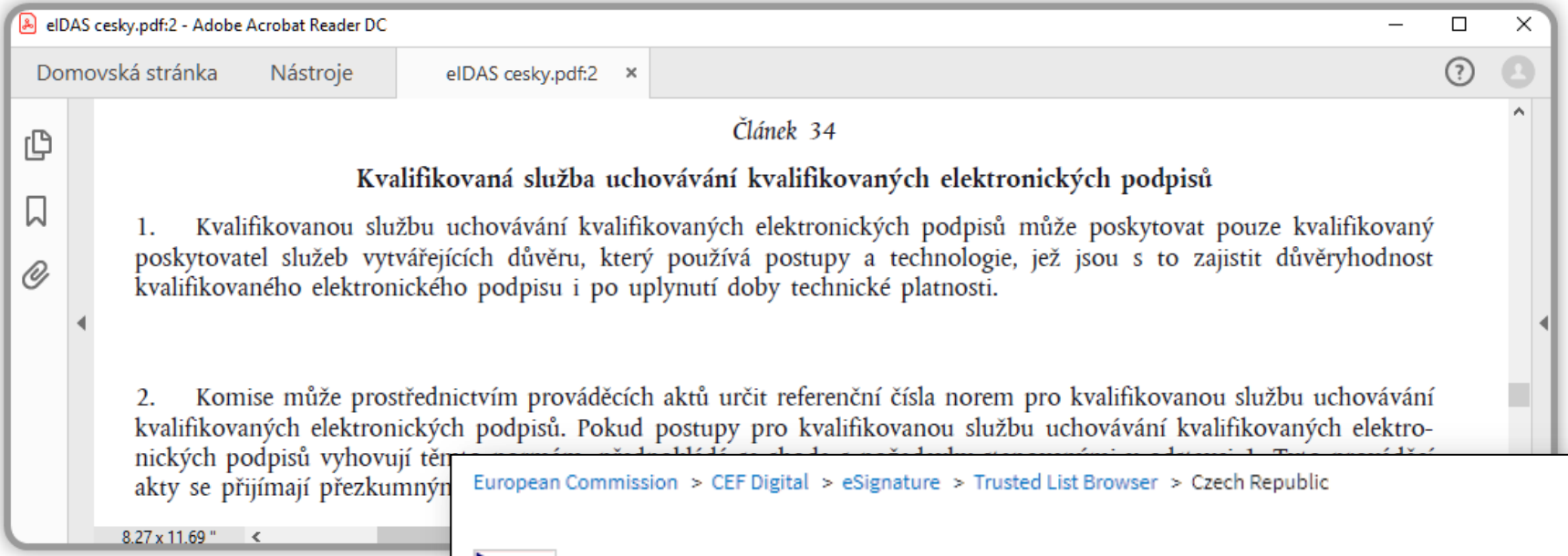






kvalifikované služby pro uchovávání

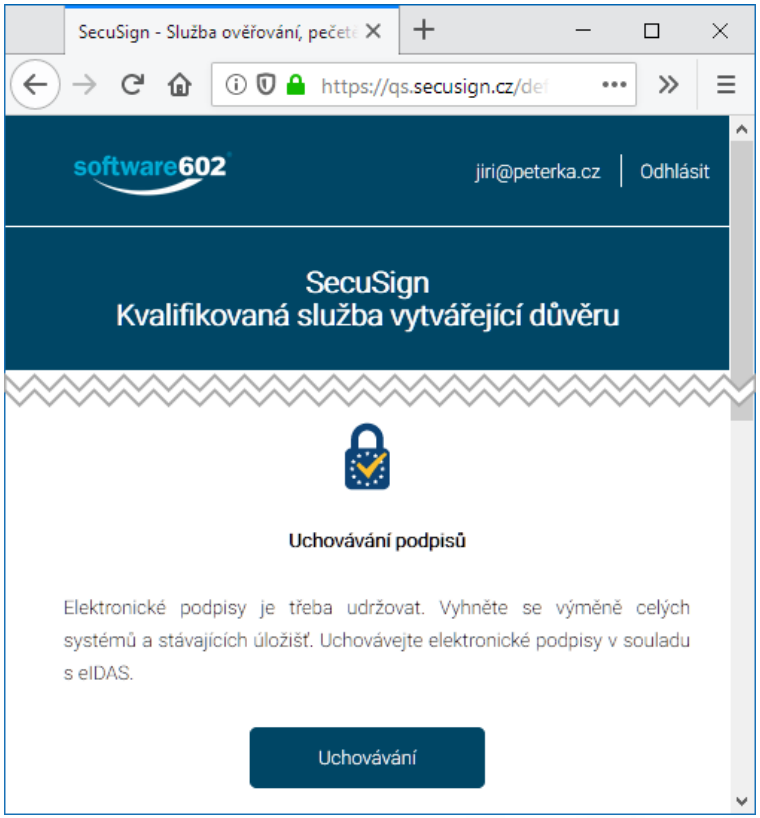
- nařízení eIDAS počítá s existenci kvalifikovaných služeb pro uchovávání kvalifikovaných elektronických podpisů a pečetí

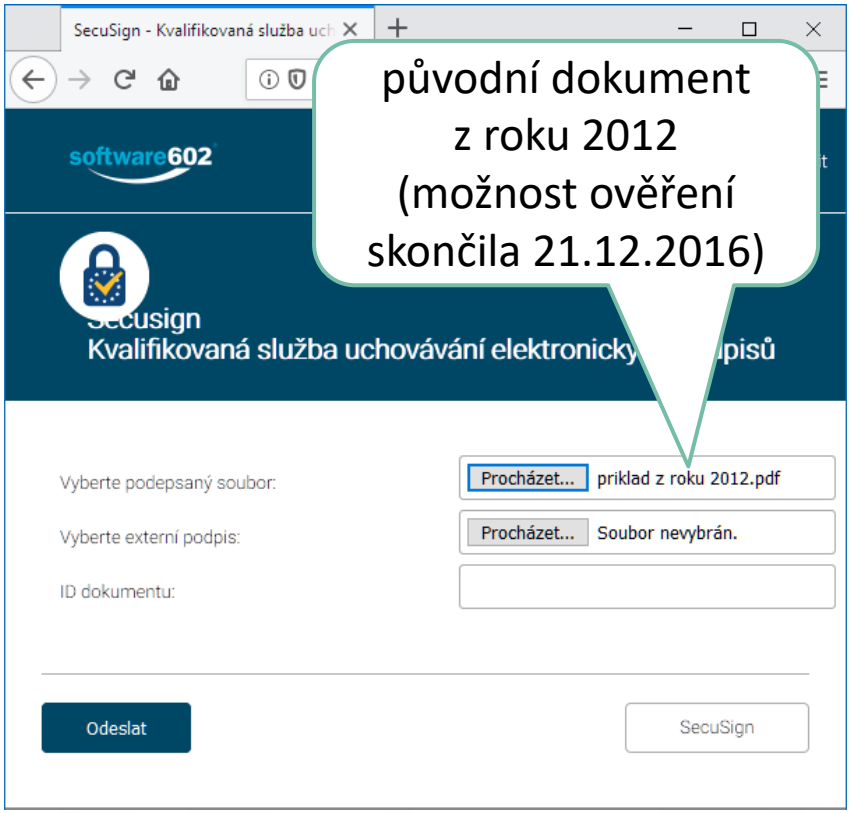


- v ČR je t.č. jen jedna taková služba
  - SecuSign od SW602

Jak funguje služba SecuSign?

- podmínkou pro „uchování“ je možnost ověřit podpis jako platný
  - v okamžiku, kdy je dokument služba předkládán



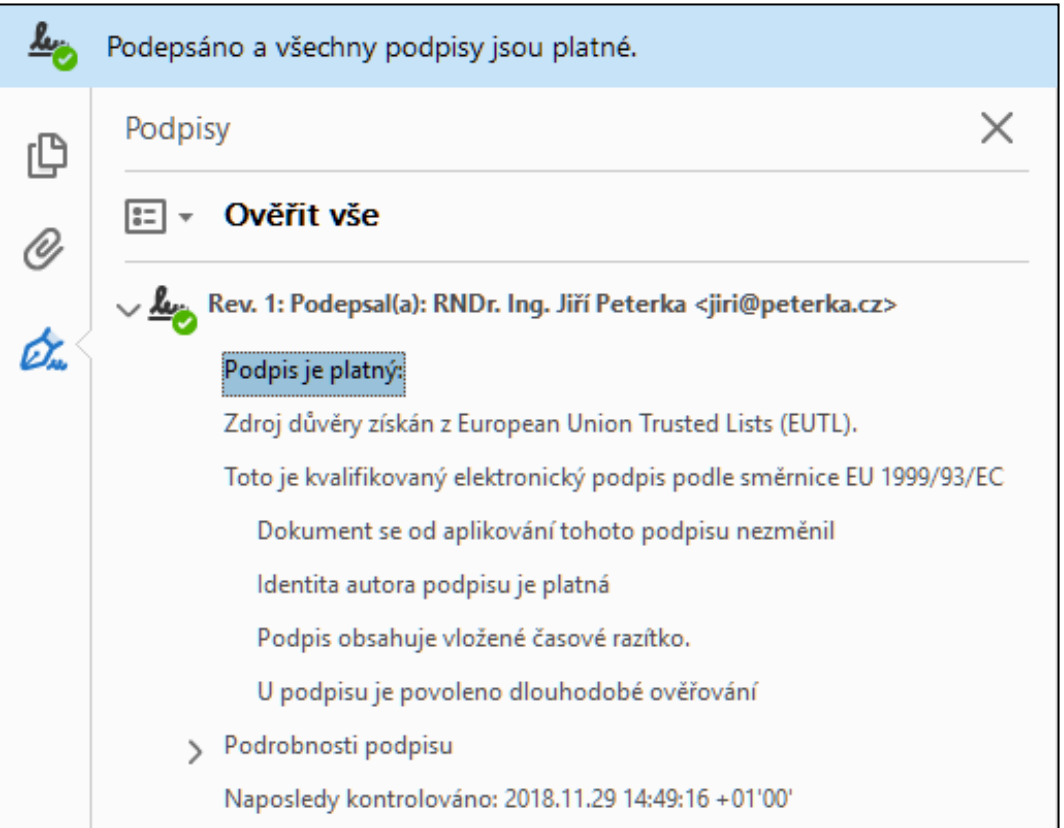


uchování není možné

Dokument nesplňuje podmínky pro službu uchovávání kvalifikovaných podpisů. Alespoň jeden podpis musí být vyhodnocen jako PLATNÝ, případně podpisový certifikát jako revokovaný.

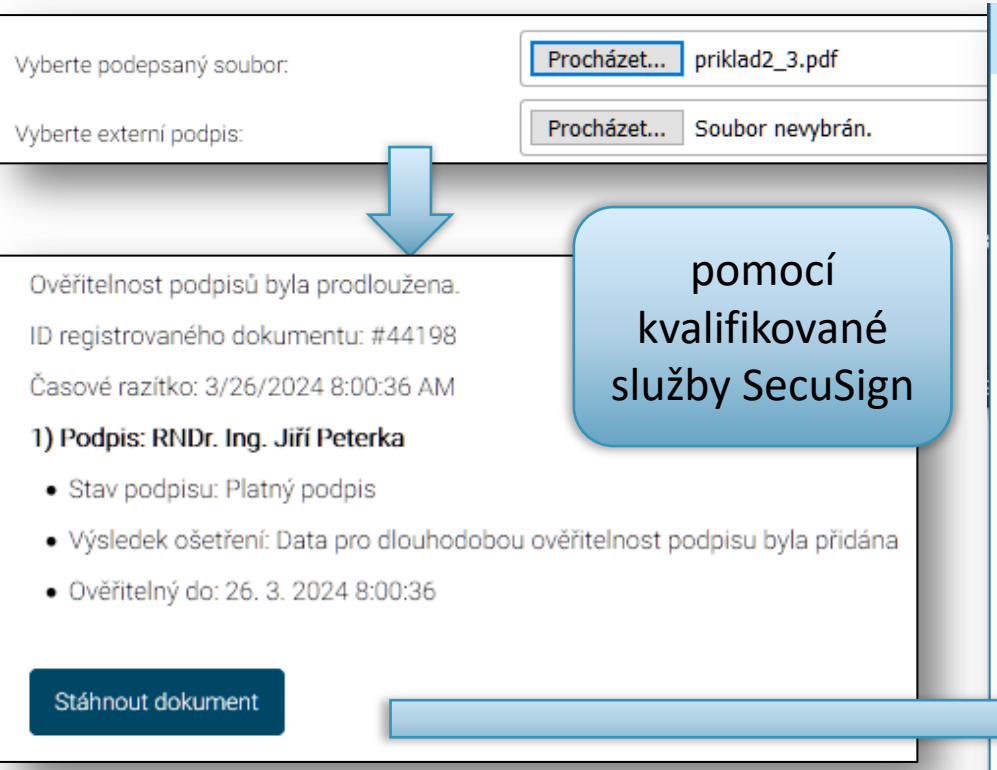
příklad (priklad2_2.pdf)

- DPF dokument s kvalifikovaným elektronickým podpisem
  - založený na certifikátu s dobou platnosti od 22.1.2014 do 22.1.2015
  - opatřený kvalifikovaným časovým razítkem, připojeným 19.1.2015
    - které je založené na certifikátu s dobou platnosti od 25.8.2014 do 2.10.2020
  - k podpisu jsou připojeny revokační informace (vložen CRL seznam)
    - jde o elektronický podpis ve formátu PAdES Baseline-LT (B-LT)

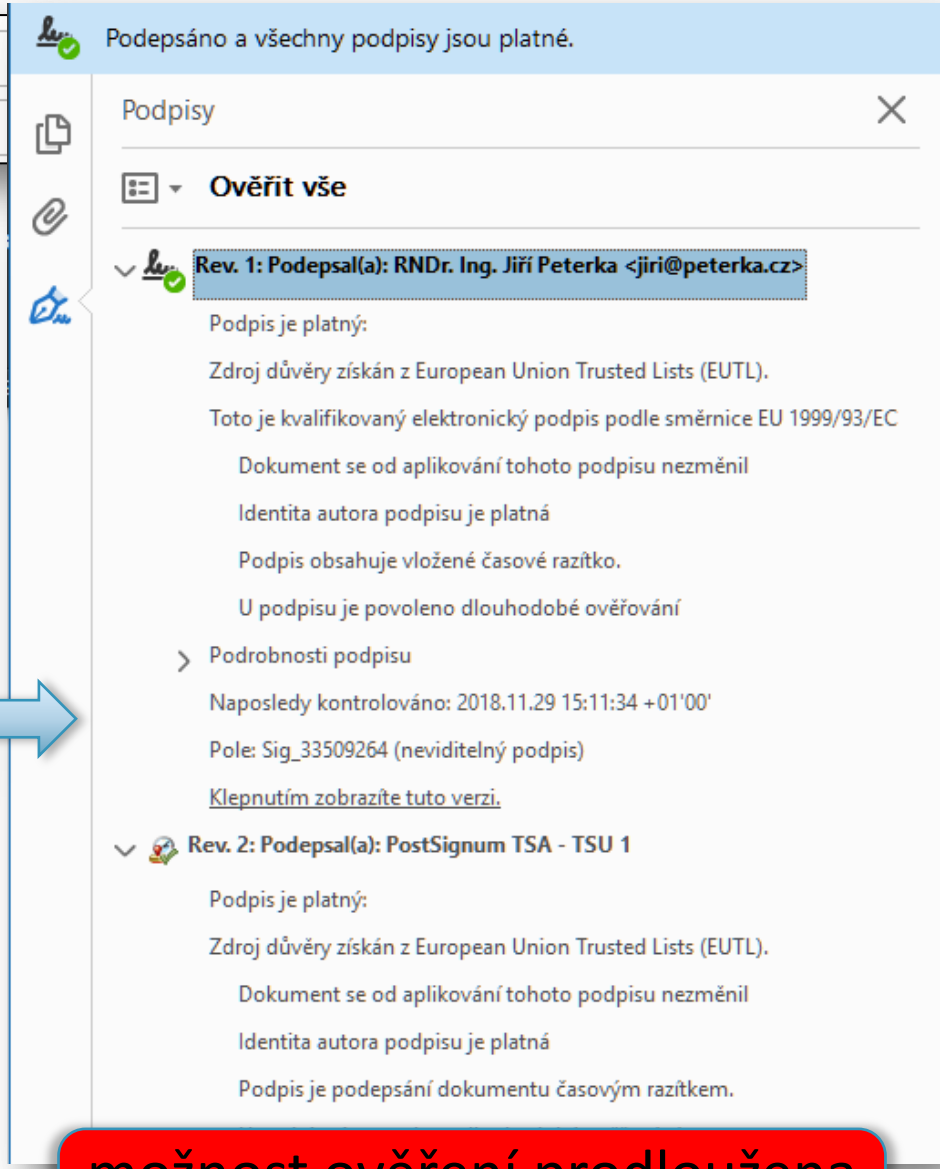


- možnost ověření platnosti podpisu je do 2.10.2020

„uchování“ (priklad2_2_uchovany.pdf)



pomocí kvalifikované služby SecuSign



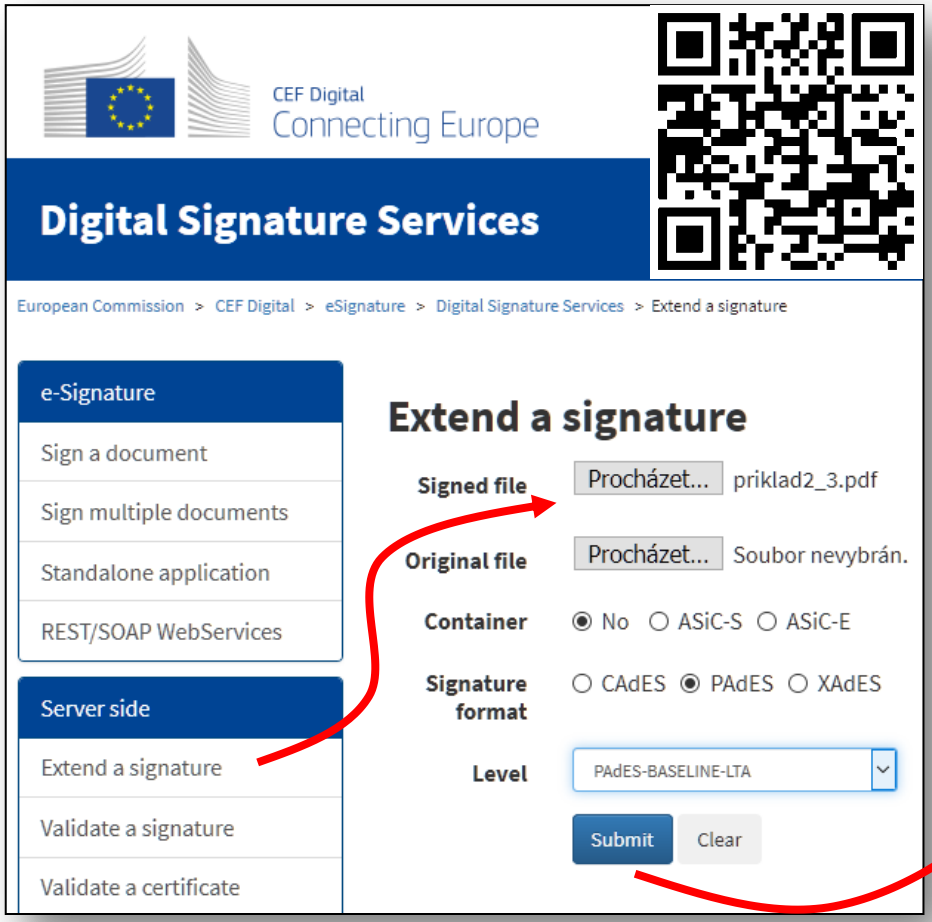
- bylo přidáno další časové razítko
  - dokumentové (archivní)
  - založené na certifikátu s platností do 26.3.2024
- formát podpisu se změnil z **B-LT** na **B-LTA**

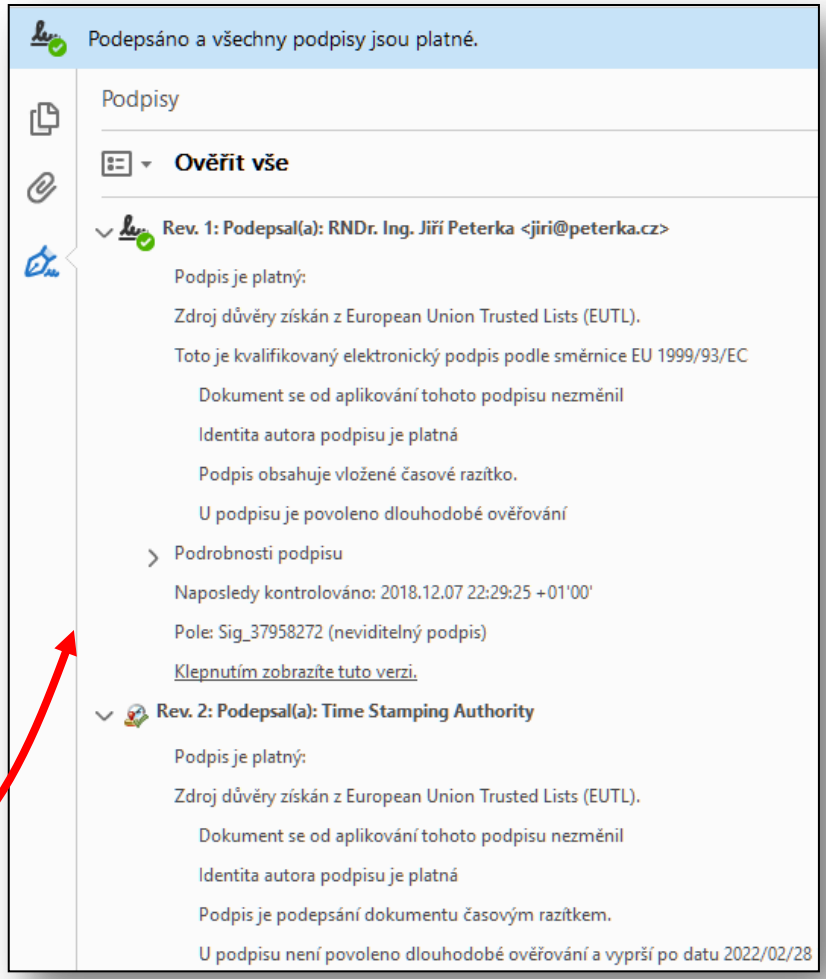
Úroveň podpisu PAdES: B-LTA

možnost ověření prodloužena do 26.3.2024

„uchování“ (priklad2_3_extended.pdf)

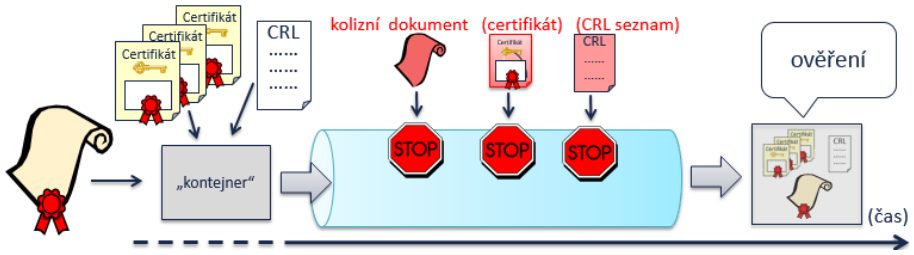
- také „unijní validátor“ nabízí možnost uchovávání
  - označovanou jako „extend a signature“
  - fakticky přidá dokumentové (archivní) el. časové razítko od belgické autority
    - které Adobe Reader hodnotí jako kvalifikované, ale SecuSign i CzechPOINT ne ..





možné přístupy k digitální kontinuitě

- existuje více principiálních možností:
  - aktivně se starat se o své dokumenty, využívat konceptu LTV
    - „technické“ řešení, vyžaduje přerazítkovávání
      - popisovali jsme si až dosud
      - takto fungují kvalifikované služby pro uchovávání
        - dle nařízení eIDAS
  - svěřit své dokumenty do úschovy
    - „institucionální“ řešení: institucionální archiv, elektronický notář
      - svěřit své dokumenty někomu, kdo na počátku ověří jejich stav (platnost podpisů, pravost, ….) a pak dlouhodobě uchovává
      - pak dokumenty vydá a k nim připojí své dobrozdání o jejich původním stavu
      - v ČR zatím neexistuje, nejsou vytvořeny podmínky



jiný pohled na digitální kontinuitu

- podstatou je názor, že „přerazítkovávání je zbytečné“
  - že podpisy a značky stačí „jednorázově ošetřit“, a že to „vydrží navěky“
    - že po celou dobu „života“ el. dokumentů není potřeba se o ně jakkoli aktivně starat – že stačí je opatřit jen jedním podpisem a jedním časovým razítkem
- problém:
  - nebere to v úvahu vývoj výpočetní techniky
    - „výpočetní síly“ počítačů
  - ignoruje to nebezpečí vzniku kolizních dokumentů
- má (mělo) to i oporu v zákoně
  - zákon č. 499/2004 Sb. o archivnictví a spisové službě
    - *§69a/5: Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou …. a …. opatřen kvalifikovaným časovým razítkem.*

označováno jako tzv. **vyvratitelná domněnka** (fikce) **pravosti**

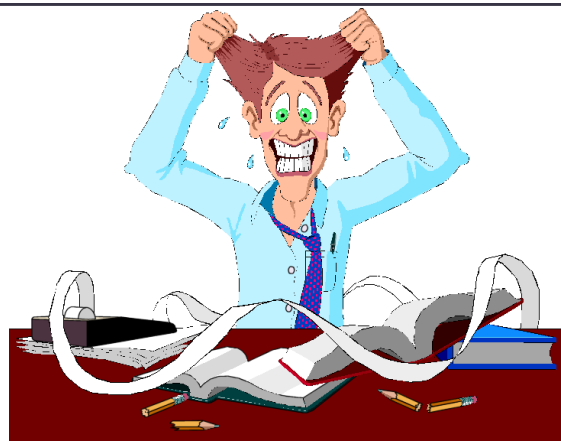
jiný pohled na digitální kontinuitu

- podstatou je názor, že „přerazítkovávání je zbytečné“
  - že podpisy a značky stačí „jednorázově ošetřit“, a že to „vydrží navěky“
    - že po celou dobu „života“ el. dokumentů není potřeba se o ně jakkoli aktivně starat
- má (mělo) to i oporu v zákoně
  - zákon č. 499/2004 Sb. o archivnictví a spisové službě
    - *§69a/5: Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou …. a …. opatřen kvalifikovaným časovým razítkem.*

označováno jako tzv. vyvratitelná domněnka (fikce) pravosti

- problém:
  - nebere to v úvahu vývoj výpočetní techniky („výpočetní síly“ počítačů)
  - ignoruje to nebezpečí vzniku kolizních dokumentů
- možné vysvětlení:
  - má to smysl uvnitř zabezpečených archivů, které (jinými prostředky) brání záměně podepsaného dokumentu za kolizní dokument – ale ne mimo archivy!!!

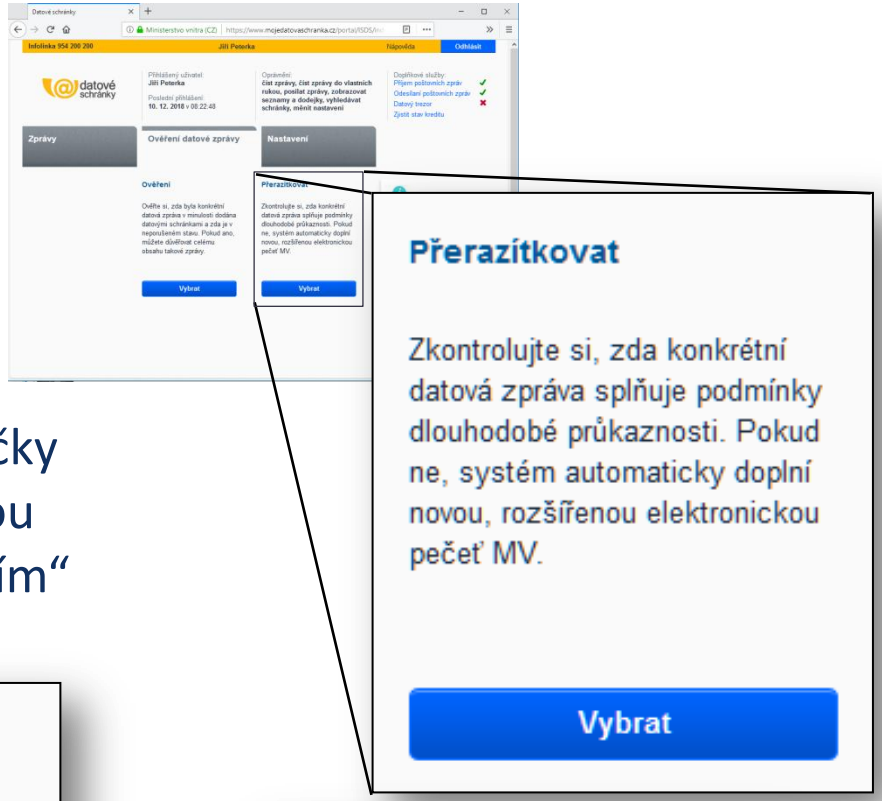
jiný pohled na digitální kontinuitu

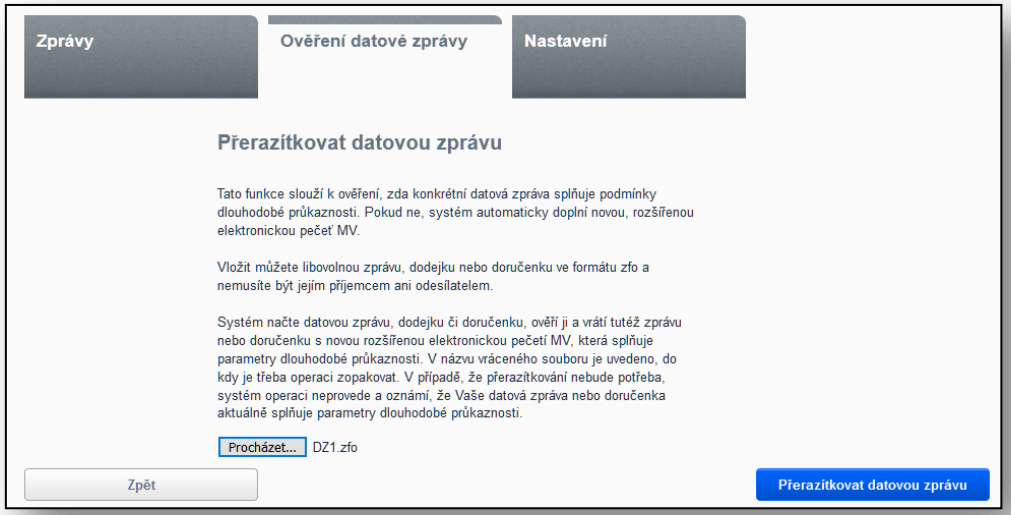


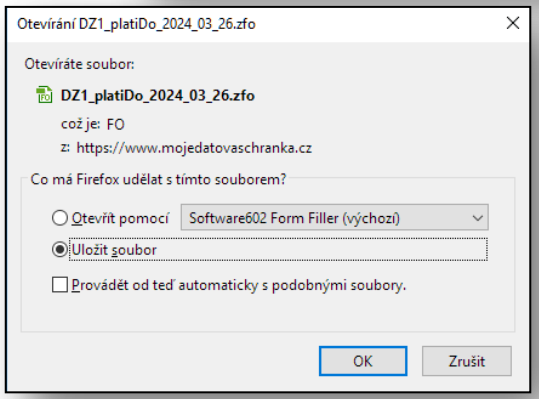
- byl to nesprávný (a nebezpečný) přístup
  - kdo se spoléhal na tuto domněnku, měl smůlu
  - v roce 2016 byla vyvratitelná domněnka pravosti (§69a odstavec 5 zákona č. 499/2004 Sb.) zrušena
    - v souvislosti s nařízením eIDAS
      - konkrétně „tlusťochem“ k adaptačnímu zákonu
        - zákonem č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce
- celá myšlenka (že stačí jen 1 podpis + 1 časové razítko) mohla mít svůj význam v „řízeném a kontrolovaném prostředí“
  - např. u elektronického notáře, který si jednorázově ověří platnost podpisů při příjmu, pak se o neměnnost (neporušenost) dokumentu stará jinak, a na konci vydává své dobrozdání ohledně toho, jaký byl dokument při příjmu („na vstupu“)
    - podobně u (spolehlivých) archivů …..
- ale stejně neřešila nedostupnost revokačních informací
  - které je nutné průběžně přidávat k uchovávaným dokumentům …..

uchovávání datových zpráv (ISDS)

- digitální kontinuita se týká i datových zpráv, přenášených mezi datovými schránkami
- od 29.1.2012 nabízí ISDS možnost „uchovávání“
  - prezentována je jako „přerazítkování“
  - ve skutečnosti funguje jinak:
    - jako náhrada původní elektronické značky (a „výstupního“ časového razítka) novou elektronickou pečetí a novým „výstupním“ časovým razítkem





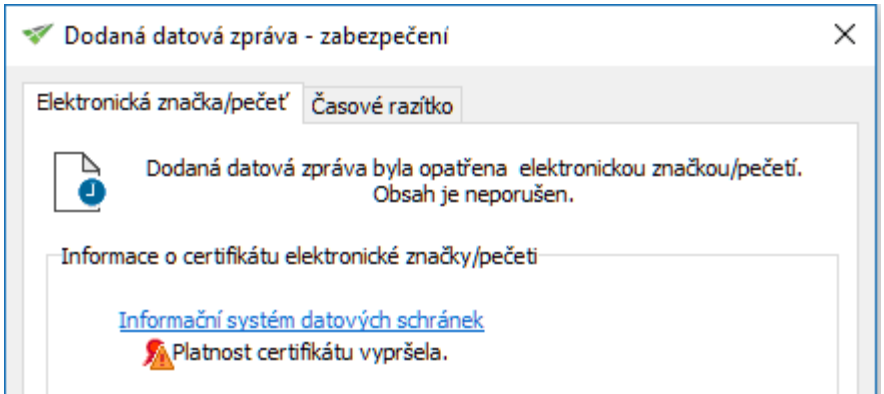


uchovávání datových zpráv (ISDS)

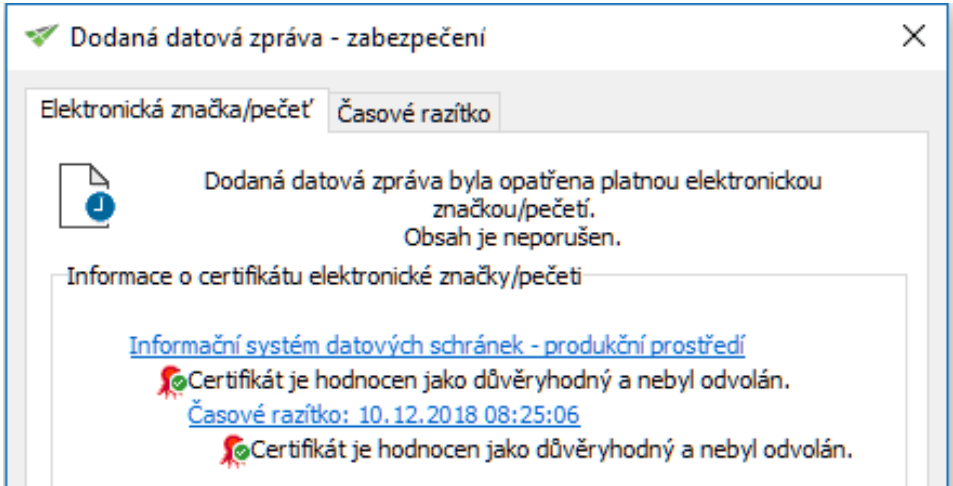
- další odlišnost (oproti obecnému postupu):
  - nemusí být dodržena časová souslednost
    - „uchování“ je možné provést kdykoli !!!!
      - není nutné jej provést dříve, než dojde ke ztrátě ověřitelnosti
        - protože ISDS „poznává“ autenticitu datové zprávy podle dalších atributů !!

není veřejně známo, jakých ….
(security through obscurity)

- příklad: DZ z roku 2010
  - soubor: **priklad2_4.zfo**
  - ještě bez „výstupního“ časového razítka
  - el. značka byla založena na certifikátu s platností od 9.4.2010 do 9.4.2011
    - tj. ověření bylo možné do 9.4.2011

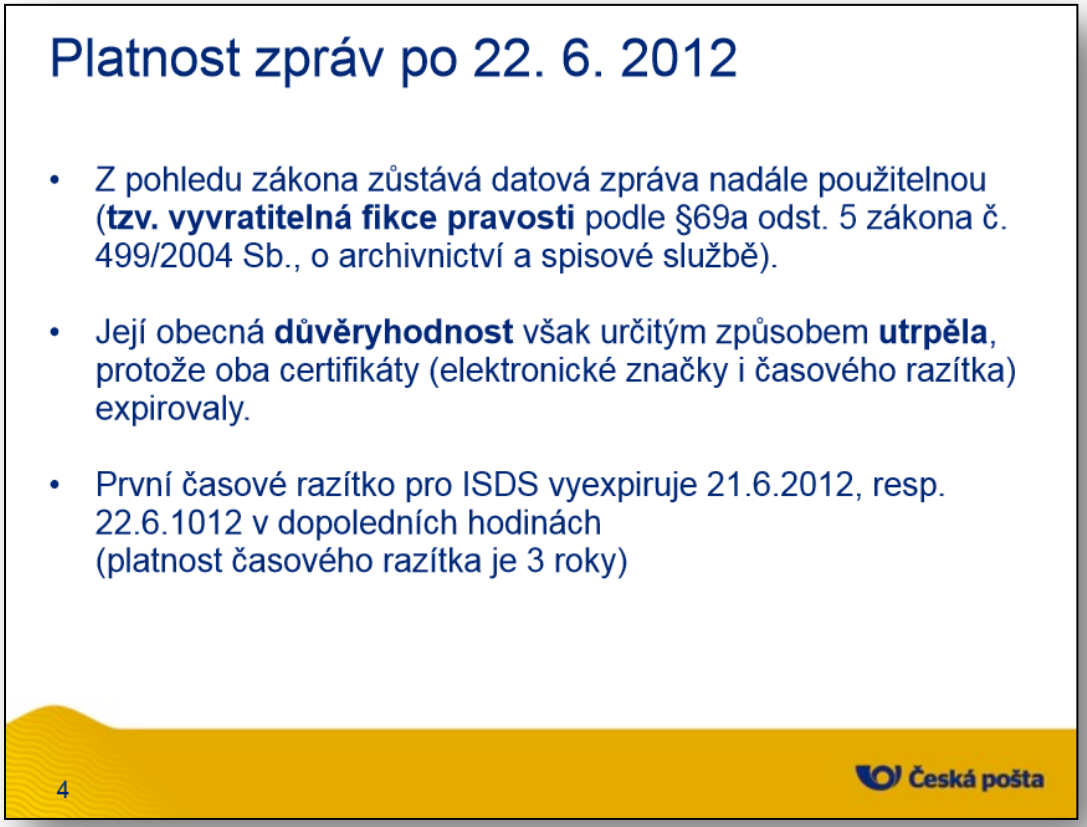


- stejná DZ, „uchovaná“ 12/2018
  - soubor: **priklad2_4_uchovany.zfo**
  - připojena nová (uznávaná) el. pečeť
  - připojeno nové „výstupní“ čas. razítko
    - ověření je možné do 26.3.2024



problém chybějící osvěty

- problém digitální kontinuity (nutnosti pravidelného „uchovávání“) zůstává stále nedoceněn
  - spíše: je bagatelizován, ignorován, či přímo popírán
- osvěta kolem tohoto problému je nulová
  - až místy záporná …..
- příkladem jsou i datové schránky:
  - když byla v roce 2012 možnost „uchovávání“ datových schránek zavedena, byla prezentována jako (v zásadě) zbytečná



závěrečné shrnutí

- chcete-li zachovat použitelnost svých elektronických dokumentů
  - možnost spoléhat se na jejich autenticitu i po delší době
    - možnost ověřit platnost jejich elektronických podpisů, pečetí a časových razítek

- musíte pro to něco aktivně dělat !!!!
  - včas podnikat nápravná opatření
    - ať již sami, nebo na principu outsourcingu

Děkuji za pozornost!

Tento seminář pořádá
Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz