Problematické aspekty elektronického podepisování

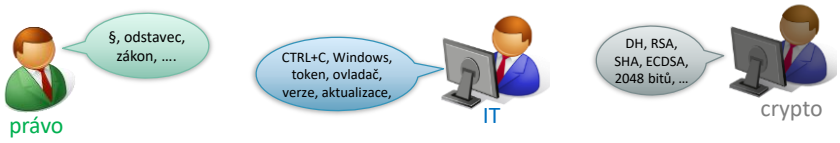
Jiří Peterka

Praha, 26.11.2019

1

co je největším problémem el. podpisů?

- jejich značně mezioborový charakter !!
  - aby el. podpisy fungovaly, dalo se na ně spoléhat a mohly se v běžném životě používat, musí vzájemně spolupracovat lidé (nejméně) ze 3 oborů

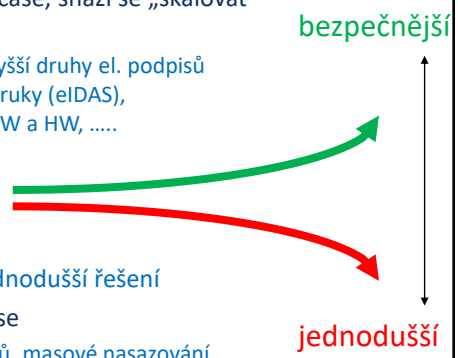


  - problém: každý obor má svůj „pohled na svět“ (své priority, zájmy, terminologii, ..)
    - a vzájemná domluva mezi lidmi z těchto oborů je ..... „složitá“
  - je nutné naučit lidi (širší uživatelskou veřejnost) el. podpisy používat
    - je nutná (srozumitelná, správná, široká ....) osvěta
      - dnes zcela chybí
    - je zapotřebí pozitivní motivace
      - dnes existuje spíše negativní motivace – vymáhání, tresty za nedodržení .....
    - stát by neměl prosazovat (problematické) alternativy k el. podepisování
      - jako je fikce podpisu v ISDS (§18 odst. 2 zák. 300/2008 Sb., či právo na nahrazení el. podpisu (§6 navrhovaného zákona o právu na digitální služby)

2

problém divergence

- různé obory reagují na současný trend (masové elektronizace / digitalizace) různě:
  - crypto a IT cítí potřebu posilovat spolehlivost a bezpečnost používaných řešení
    - vnímají (stále větší) ohrožení a vývoj v čase, snaží se „škálovat složitost“ (zneužití, prolomení, …)
      - mají potřebu používat „silnější crypto“, vyšší druhy el. podpisů (kvalifikovaný, uznávaný), vyšší úrovně záruky (eIDAS), vícefaktorovou autentizaci, bezpečnější SW a HW, …..
  - právo (hlavně soukromé) hledá co nejjednodušší řešení
    - (tolik) nevnímá ohrožení ani vývoj v čase
      - tendence k používání prostých el. podpisů, masové nasazování dynamických biometrických podpisů, ….
        - nešťastný §7 zákona č. 297/2016 Sb: …. *lze použít jakýkoli druh el. podpisu …*



3

problém terminologie

- jak se mají uživatelé v celé problematice orientovat, když není ani vyjasněna a sjednocena terminologie?
- například:
  - …. *písemně nebo elektronicky* …
    - např.: správní řád, zákon o ochraně spotřebitele, …..
  - …. *písemně, a to buď elektronicky nebo v listinné podobě* ….
    - např. o.s.ř, t.ř., ….
- například:

dokument „na papíře“ je:	dokument „z nul a jedniček“ je:
analogový (z. č. 499/2004 Sb.)	obsažený v datové zprávě (z. č. 300/2008 Sb.)
	digitální (z. č. 499/2004 Sb.)
listinný (jinde)	elektronický (jinde)

jinde též: **digitální podpis**

- nebo když je terminologie matoucí:
  - **zaručený elektronický podpis** (AdES, Advanced Electronic Signature)
    - je charakteristický tím, že nezaručuje identitu podepsané osoby
      - mate to uživatele, legislativce, justici, …..
  - **uznávaný elektronický podpis** (naše národní specialita, EU nezná)
    - je charakteristický tím, že v zahraničí (EU) jej neznají a tedy neuznávají
    - jde ve skutečnosti o „legislativní zkratku“ pro dva různé druhy el. podpisů
      - buď: kvalifikovaný elektronický podpis,
      - nebo: zaručený elektronický podpis, založený na kvalifikovaném certifikátu

4

problém: *ono to neumí …..*

- používané programy/služby často neumí (neřeší, nepodporují, neindikují) důležité věci

kvalifikovaný …

3	*PAdES T-level kvalifikovany.pdf*	
Podpis je platný (platnost prodloužena čas. razítkem)		*RNDr. Ing. Jiří Peterka / ae1880 / 31.07.2018 - 31.07.2019*
4	*PAdES T-level uznavany viditelny.pdf*	
Podpis je platný (platnost prodloužena čas. razítkem)		*RNDr. Ing. Jiří Peterka / 2dfdeb / 22.02.2018 - 14.03.2019*

kvalifikovaná pečeť v referenčním formátu

12	*pecet_kval_ref_razitko.pdf*	
Podpis je platný	*CRL z 23.03.2019 05:51:02*	*MPO - RZP / ae5542 / 13.09.2018 - 13.09.2019*
13	*pecet_uznav_basic_bezrazitka.pdf*	
Podpis je platný	*CRL z 23.03.2019 09:20:14*	*Obchodní a obdobné rejst / 3db03d / 22.11.2018 - 22.11.2019*

- příklady:

„český“ uznávaný …

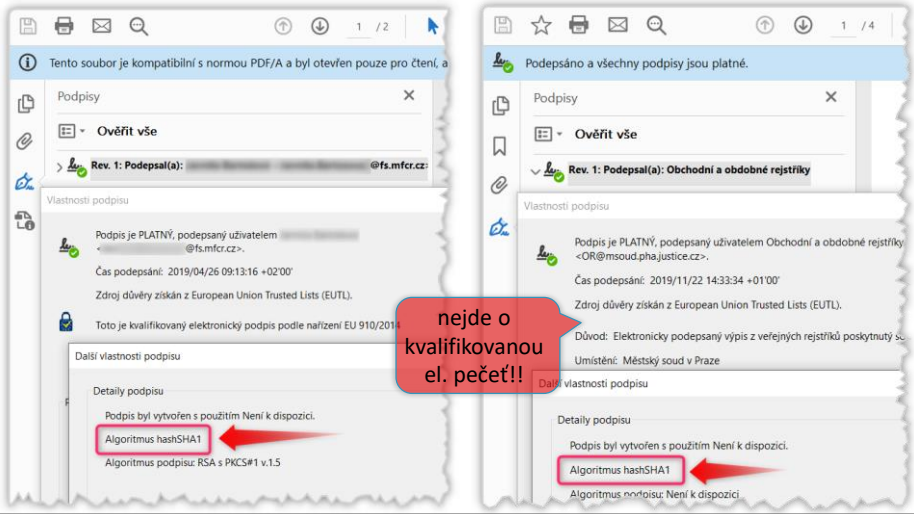
„česká“ uznávaná pečeť v ne-referenčním formátu

  - elektronické podatelny na soudech:
    - do 20.3.2019 nepodporovaly referenční formáty dle eIDAS (PAdES Baseline), neznaly zahraniční certifikáty, nepodporují archivní časová razítka (B-LTA), ……
    - od 20.3.2019 již podporují referenční formáty a zahraniční certifikáty (z EU)
      - stále ještě: nerozlišují kvalifikované vs. uznávané el. podpisy, nerozlišují podpisy vs. pečeti, neinformují o hashovací funkci ani formátu el. podpisu, neumí eliptické křivky, ..
  - kvalifikovaná služba (ověřování) SecuSign
    - neověřuje podpisy bez časového razítka, neinformuje o hashovací funkci
  - CzechPOINTy:
    - neřeší hashovací funkce, referenční formáty, neumí eliptické křivky, ….

5

problém s chováním uživatelů

- 2009: MV ČR „zavelelo“ k přechodu z SHA1 na SHA-2
  - pro certifikační autority to bylo povinné, pro ostatní jen „důrazné doporučení“
- 2019: SHA1 se (někde, ve veřejné správě) stále používá

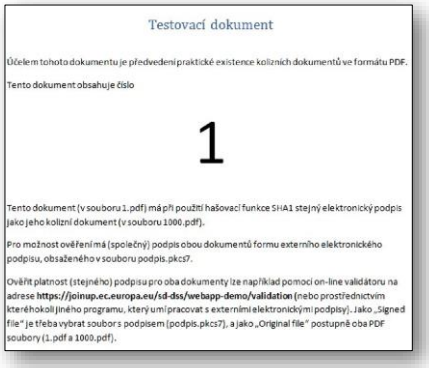


6

proč je nutné „silnější crypto“

- hashovací funkce SHA1 již dnes není bezpečná
  - kolizní dokumenty (1. řádu) reálně existují
  - příklad z roku 2017: dva různé dokumenty se stejným otiskem dle SHA1

https://www.earchiv.cz/down/koliznibalicek.zip


Testovací dokument

Účelem tohoto dokumentu je předvedení praktické existence kolizních dokumentů ve formátu PDF.

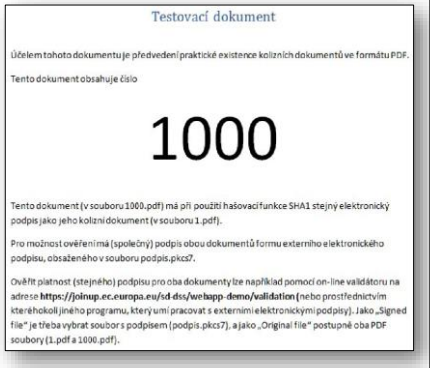
Tento dokument obsahuje číslo

1

Tento dokument (v souboru 1.pdf) má při použití hašovací funkce SHA1 stejný elektronický podpis jako jeho kolizní dokument (v souboru 1000.pdf).

Pro možnost ověření má (společný) podpis obou dokumentů formu externího elektronického podpisu, obsaženého v souboru podpis.pkcs7.

Ověřit platnost (stejného) podpisu pro oba dokumenty lze například pomocí on-line validátoru na adrese **https://joinup.ec.europa.eu/sd-dss/webapp-demo/validation** (nebo prostřednictvím kteréhokoli jiného programu, který umí pracovat s externími elektronickými podpisy). Jako „Signed file“ je třeba vybrat soubor s podpisem (podpis.pkcs7), a jako „Original file“ postupně oba PDF soubory (1.pdf a 1000.pdf).


Testovací dokument

Účelem tohoto dokumentu je předvedení praktické existence kolizních dokumentů ve formátu PDF.

Tento dokument obsahuje číslo

1000

Tento dokument (v souboru 1000.pdf) má při použití hašovací funkce SHA1 stejný elektronický podpis jako jeho kolizní dokument (v souboru 1.pdf).

Pro možnost ověření má (společný) podpis obou dokumentů formu externího elektronického podpisu, obsaženého v souboru podpis.pkcs7.

Ověřit platnost (stejného) podpisu pro oba dokumenty lze například pomocí on-line validátoru na adrese **https://joinup.ec.europa.eu/sd-dss/webapp-demo/validation** (nebo prostřednictvím kteréhokoli jiného programu, který umí pracovat s externími elektronickými podpisy). Jako „Signed file“ je třeba vybrat soubor s podpisem (podpis.pkcs7), a jako „Original file“ postupně oba PDF soubory (1.pdf a 1000.pdf).

SHA1: 087DD6660A05F1C5729C6F1BF589CE0EF1C35941

SHA-256:
61809BC85C4287185035138EF0E212989BE4F19
8AADAA77E96DDD399AFC3E3D0

SHA-256:
2F224F3D79A506E178F7E84C25209C7DD6266F4
527A2A557639652DE7F357815

7

problém: *ono to neřeší …..*

- praktický problém: většina používaných nástrojů/služeb neřeší, jaká hashovací funkce byla použita při vytváření el. podpisu/pečeti
  - Adobe Acrobat (Reader) DC aspoň indikuje

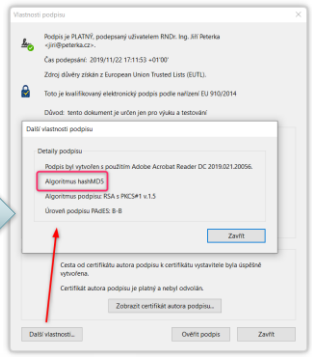

Příklad dokumentu s elektronickým podpisem

pro potřeby výuky a testování

Tento dokument je opatřen kvalifikovaným elektronickým podpisem. Při jeho vytváření byla použita hashovací funkce MD5.

RNDr. Ing. Jiří Peterka

Důvod: tento dokument je určen jen pro výuku a testování
Datum: 2019.11.22 17:11:53 +01'00'


Vlastnosti podpisu

Podpis je PLATNÝ, podepsaný uživatelem RNDr. Ing. Jiří Peterka <jiri@peterka.cz>.

Čas podepsání: 2019/11/22 17:11:53 +01'00'

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

Toto je kvalifikovaný elektronický podpis podle nařízení EU 910/2014

Důvod: tento dokument je určen jen pro výuku a testování

Další vlastnosti podpisu

Detaily podpisu

Podpis byl vytvořen s použitím Adobe Acrobat Reader DC 2019.021.20056.

Algoritmus hashMD5

Algoritmus podpisu: RSA s PKCS#1 v.1.5

Úroveň podpisu PAdES: B-B

Zavřít

Cesta od certifikátu autora podpisu k certifikátu vystavitele byla úspěšně vytvořena.

Certifikát autora podpisu je platný a nebyl odvolán.

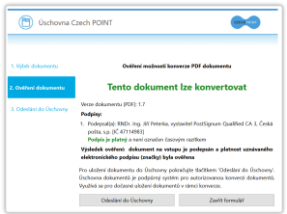
Zobrazit certifikát autora podpisu...

Další vlastnosti...

Ověřit podpis

Zavřít

- příklad: použití MD5
- CzechPOINT (bez problémů) zkonvertuje


Úschovna Czech POINT

Ověření možností konverze PDF dokumentu

Tento dokument lze konvertovat

Verze dokumentu (PDF): 1.7

Podpisy:

1. Podepsal(a): RNDr. Ing. Jiří Peterka, vystavitel PostSignum Qualified CA 3, Česká pošta, s.p. (IČ 47114983)

Podpis je platný a není označen časovým razítkem

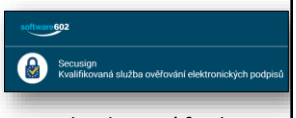
Výsledek ověření: dokument ne vstupu je podepsán a platnost uznávaného elektronického podpisu (značky) byla ověřena

Pro uložení dokumentu do Úschovny pokračujte tlačítkem 'Odeslání do Úschovny'. Úschovna dokumentů je podpůrný systém pro autorizovanou konverzi dokumentů. Využívá se pro dočasné uložení dokumentů v rámci konverze.

Odeslání do Úschovny

Zavřít formulář

o hashovací funkci informuje „hodně hluboko“ (Diagnostic Tree)

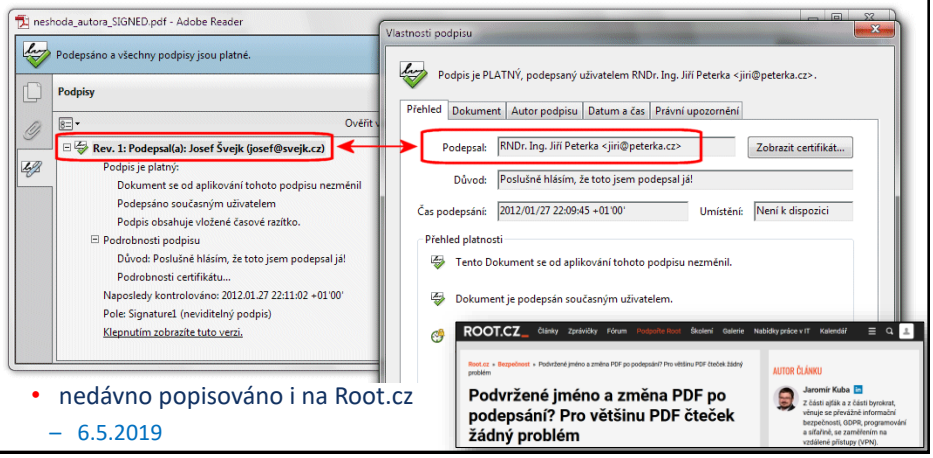


o hashovací funkci neinformuje vůbec

8

problém chyb v programu

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

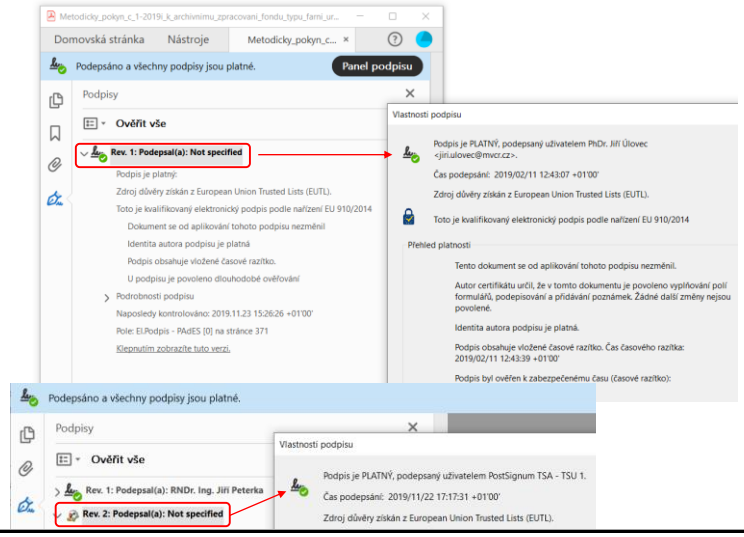


- nedávno popisováno i na Root.cz
  - 6.5.2019

9

problém chyb v programu

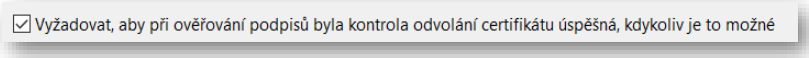
- některé kombinace nástrojů (pro vytváření a ověřování el. podpisů) stále nefungují korektně
  - tak, aby se řádně zobrazovala identita podepsané osoby



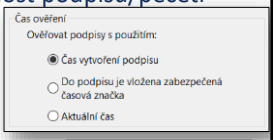
10

problémy s nastavením programů

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



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



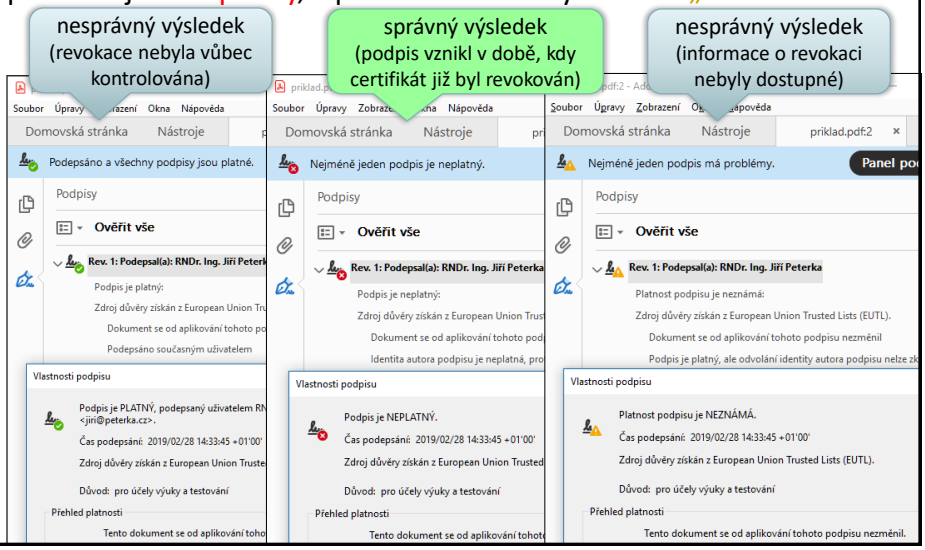
  - lze nastavit obsah úložiště důvěryhodných certifikátů
    - a tím určit, kterým certifikátům bude program důvěřovat
      - problematické u nekvalifikovaných certifikátů
      - pro kvalifikované certifikáty (z EU) vyřešeno vazbou na unijní seznam LOTL (resp. EUTL)

obsah úložiště nastavuje primárně Adobe, resp. Microsoft

11

odstrašující příklad

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



12

problém rozhodného okamžiku

- tj. okamžiku, ke kterému se vyhodnocuje splnění podmínek pro platnost
  - to je naprosto klíčové pro správný výsledek ověření !!!

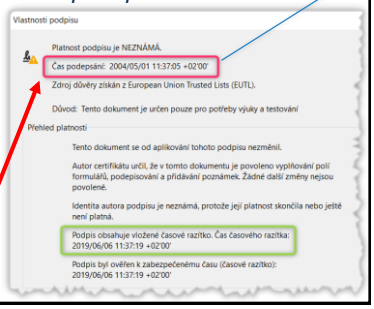
- dříve: postup ověřování byl popsán ve vyhlášce
  - vyhláška 212/2012 Sb. (zrušena k 19.9.2016)
    - ne úplně správně, ale nikoli chybně
      - *„… nejprve okamžik doručení, a když to nevychází tak okamžik z časového razítka …“*

správně by to bylo obráceně, protože časové razítko je starší

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

ve smyslu: deklarovaného

znamenalo by to ignorovat časová razítka



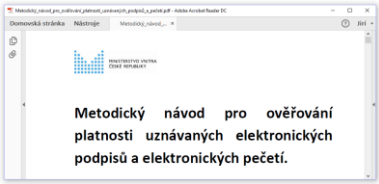
- ale to nejde aplikovat – nemá to smysl !!!
  - protože okamžik podepsání neznáme !!
    - přesněji: nějaký časový údaj k dispozici máme, ale nevíme, zda je správný – zda se na něj můžeme spoléhat
      - protože systémové hodiny lze libovolně přetočit !!

13

metodický návod MV ČR

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

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

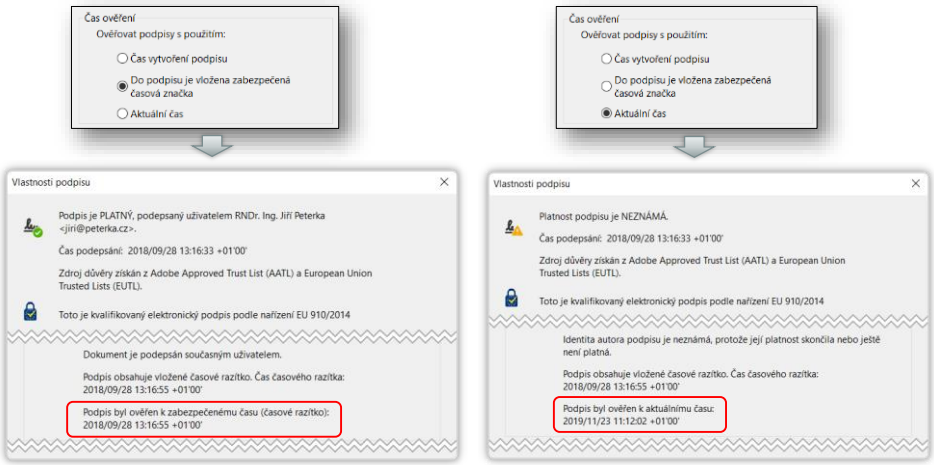


a) datum a čas doručení elektronicky podepsaného dokumentu nebo
b) nejčasnější časový okamžik, ve kterém již prokazatelně existoval zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, jehož platnost je ověřována (čas připojení důvěryhodného elektronického časového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

14

Adobe Reader: vliv nastavení na výsledek

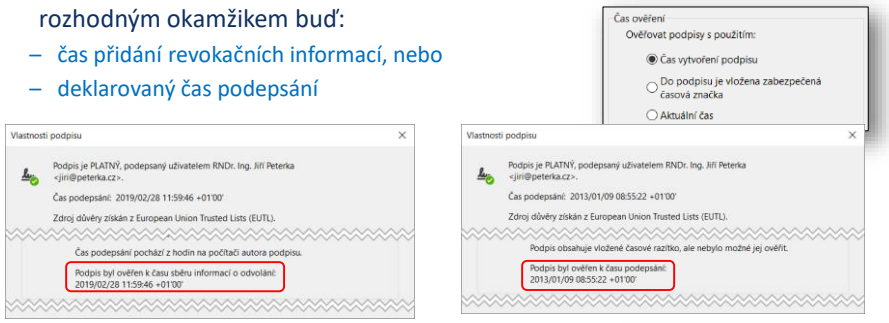
- volba způsobu určení rozhodného okamžiku (v Adobe Readeru) významně ovlivňuje výsledek ověření
  - volba „Aktuální čas“ způsobí ignorování časových razítek
    - nutno udělat tam, kde razítko není kvalifikované (což Reader nepozná)

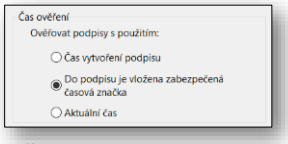


15

Adobe Reader: vliv nastavení na výsledek

- volba „Čas vytvoření podpisu“ (defaultní nastavení)
  - pokud je platné časové razítko, je rozhodným okamžikem čas přidání časového razítka (tedy stejně jako u „Do podpisu je vložena zabezpečená časová značka“)
  - pokud časové razítko není (nebo není možné ho ověřit jako platné), pak je rozhodným okamžikem buď:
    - čas přidání revokačních informací, nebo
    - deklarovaný čas podepsání



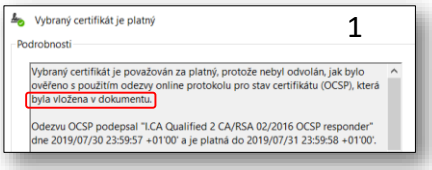


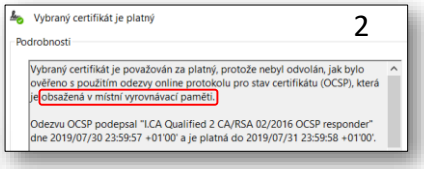
- „Do podpisu je vložena zabezpečená časová značka“
  - Reader se pokouší ověřit k času časového razítka
  - pokud se mu to nepovede, zkouší to ještě k aktuálnímu času !!!!

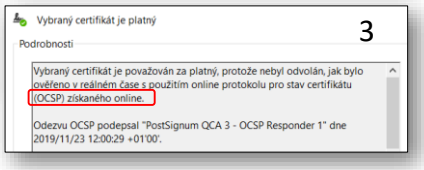
16

Adobe Reader: hledání revokačních informací

- pro ověření platnosti podpisu Reader potřebuje zjistit, zda certifikát nebyl revokován
  - pokud mu tato možnost nebyla v nastavení zakázána (vypnuta)
- Reader hledá revokační informace (CRL, OCSP) vždy v tomto pořadí:
  1. vložené do dokumentu
  2. umístěné v jeho cache paměti
  3. on-line







- praktické důsledky:
  - pokud jsou revokační informace vloženy v dokumentu, Reader nehledá novější („čerstvější“) informace on-line – viz dále
  - pokud dojde na volbu ad 2), je výsledek závislý na obsahu jeho cache paměti
    - **tedy na dřívějším používání daného exempláře programu Adobe Reader !!!!**

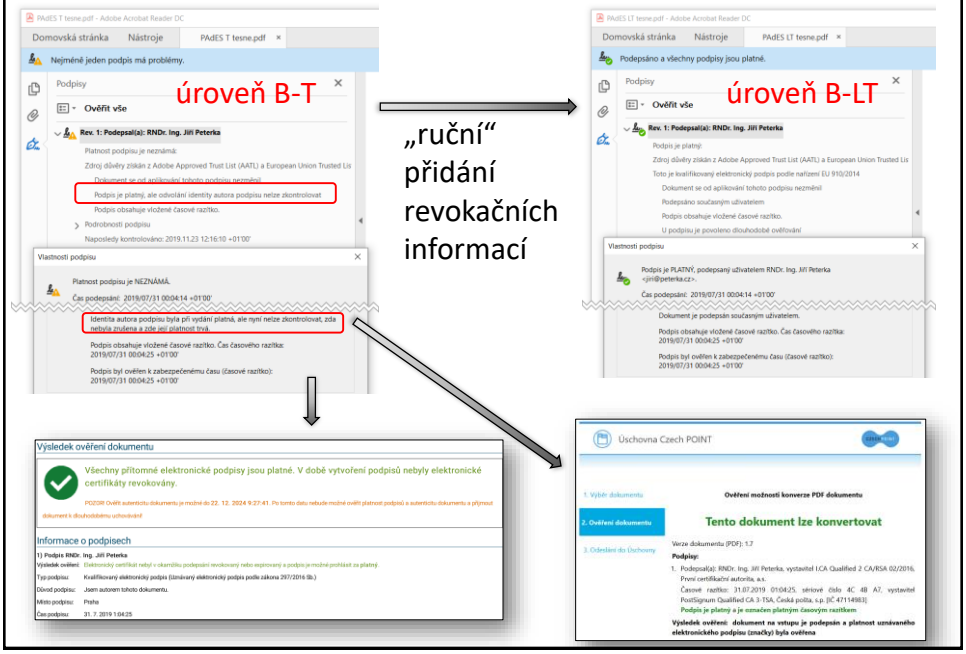
17

problém volby mezi úrovní B-T a B-LT

- OVM dnes mají povinnost používat úroveň B-T
  - používat referenční formáty (PAdES Baseline pro PDF) a připojovat časové razítko
    - nemají povinnost připojovat revokační informace (CRL či OCSP)
- příklad negativních důsledků:
  - podpisový certifikát má platnost do dne/času X
  - dokument je podepsán před okamžikem X (několik týdnů/dní …) na úrovni B-T
    - tj. je připojeno (kval.) časové razítko, ale nejsou vloženy revokační informace
- očekávání příjemce dokumentu (občana, firmy):
  - že díky časovému razítku bude možné ověřit platnost podpisu i dlouho po okamžiku X (několik let – dnes minimálně po dalších 5 let)
  - realita:
    - na CzechPOINTU lze konvertovat (používá vlastní revokační informace)
    - kvalifikované služby pro ověřování (SecuSign, I.CA Verify, Obelisk) také ověří
    - Adobe Reader (po okamžiku X) nedokáže platnost ověřit !!!!
      - nebo: dokáže, pokud revokační informace najde ve své cache paměti !!!!

18

konkrétní příklad: B-T vs. B-LT



19

ještě jeden problém z eIDAS-u

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

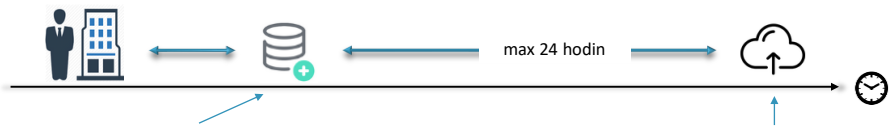
otázka: k jakému časovému okamžiku?

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

20

důsledky (okamžiku revokace)

- jaké jsou důsledky pro podpis bez časového razítka
  - nebo s razítkem "mladším" 24 hodin
- jak se mají chovat el. podatelny, CzechPOINTy, služby ověřování, … ??

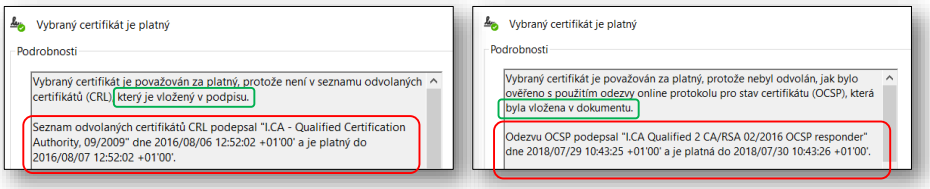


- názor 1 (platí čas zapsání do db)
  - příjemce dokumentu by měl čekat 24 hodin, než může konstatovat, že podpis je platný
    - resp. tolik hodin, kolik zbývá do 24 hodin od připojení (kvalifikované-ho) časového razítka
  - CzechPOINTy to dříve řešily disclaimerem:
    - *„v době od uveřejnění seznamu zneplatněných kvalifikovaných certifikátů …. do provedení autorizované konverze dokumentů mohlo dojít k zneplatnění kvalifikovaného certifikátu"*
- názor 2 (platí čas zveřejnění)
  - příjemce dokumentu nemusí čekat
    - získá aktuálně dostupné revokační informace a podle nich vyhodnotí platnost podpisu

21

související problém (24 hodin)

- CRL seznamy byly často vydávány s platností na 24 hodin
  - a některé odpovědi OCSP serverů dnes také

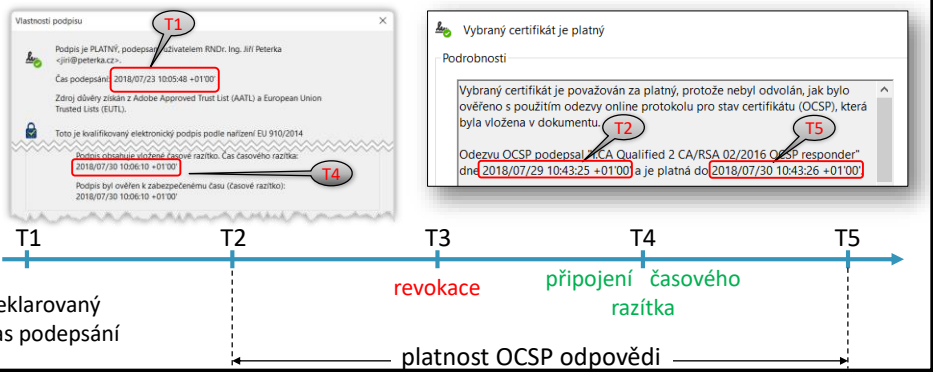


- problém:
  - některé programy se řídí CRL seznamy/OCSP odpověďmi, které byly vloženy do dokumentu (k podpisu)
    - a nekontrolují, zda nejsou dostupné novější revokační informace
- důsledek:
  - hodnotí jako platný i takový podpis, který byl vytvořen až po revokaci certifikátu
    - třeba i několik hodin (do 24 hodin)
- týká se to:
  - Adobe (Acrobat) Readeru i CzechPOINT-ů (do poloviny roku 2018)

22

konkrétní příklad (7/2018)

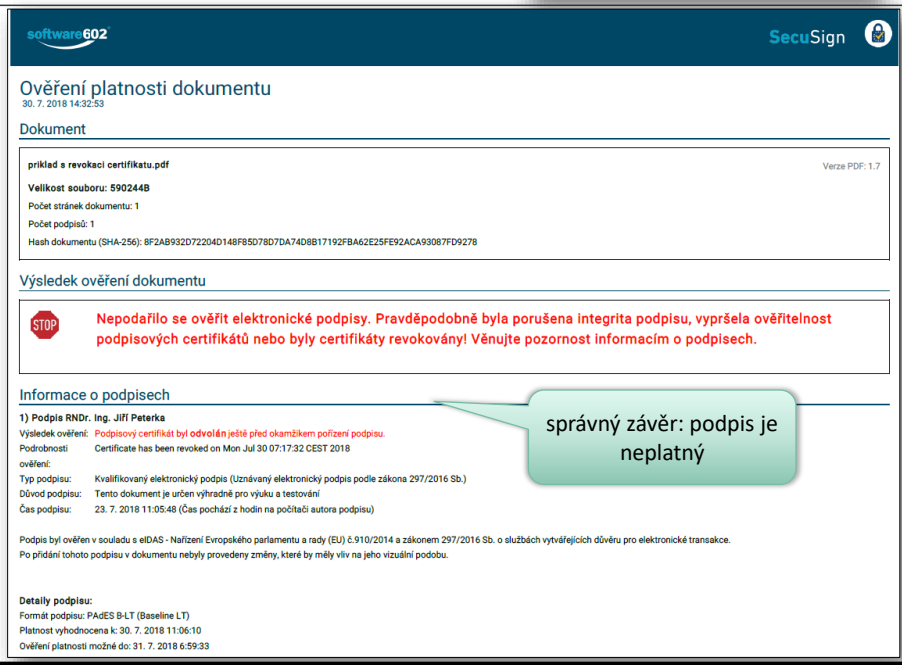
- dokument v souboru priklad s revokaci certifikatu.pdf
  - (kvalifikovaný) certifikát od I.CA byl platný do 31.7.2018, 05:59:33 (+1:00)
  - T1: deklarovaný čas podepsání: 23.7.2018, 10:05:48 (+1:00) (přetočené hodiny)
  - T3: k revokaci došlo **30.7.2018, 07:17:32** (+1:00) → skutečné podepsání
  - T4: (kvalifikované) čas. razítko připojeno **30.7.2018, 10:06:10** (+1:00)
    - do dokumentu byla vložena odpověď OCSP serveru z 29.7.2018, 10:43:25 (+1:00) (T2), platná do 30.7.2018, 10:43:26 (+1:00) (T5)



23

jak to dopadlo?

priklad s revokaci certifikatu.pdf

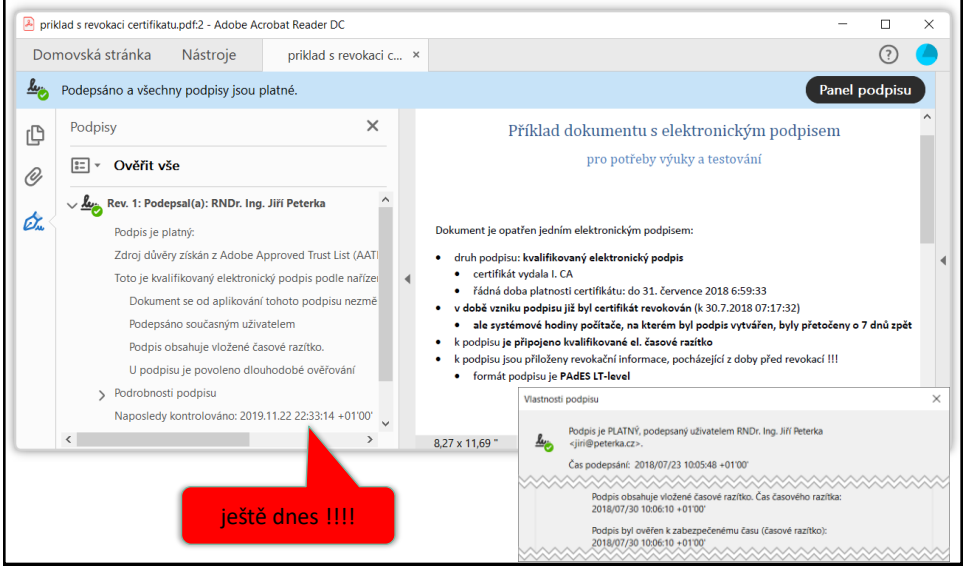


24

jak to dopadlo?

priklad s revokaci certifikatu.pdf

- Adobe Acrobat Reader:
  - důvěřuje vložené odpovědi OCSP serveru, která byla vydána před revokací !!



25

jak to dopadlo?

priklad s revokaci certifikatu.pdf

generováno 30.7.2018 14:41

...nether they are Advanced electronic Signatures (AdES), AdES ...) or a Qualified electronic Signature (QES). All certificates and their ...alidated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps).

Signature id-809398238e43a4538c8d8b33284d9ff1c1e2c1641883c0bac6cb8445663f116e

Signature Level :	QESig
Indication :	TOTAL_PASSED
	The trusted certificate doesn't match the trust service
Signature Format :	PAdES-BASELINE-LT
Certificate chain:	RNDr. Ing. Ji#í Peterka I.CA Qualified 2 CA/RSA 02/2016
On claimed time :	2018-07-23T09:05:48
Best signature time :	2018-07-30T09:06:10
Signature position :	1 out of 1
Signature scope:	Partial PDF (PdfByteRangeSignatureScope) The document byte range: [0, 541942, 573302, 1220]

Document Information

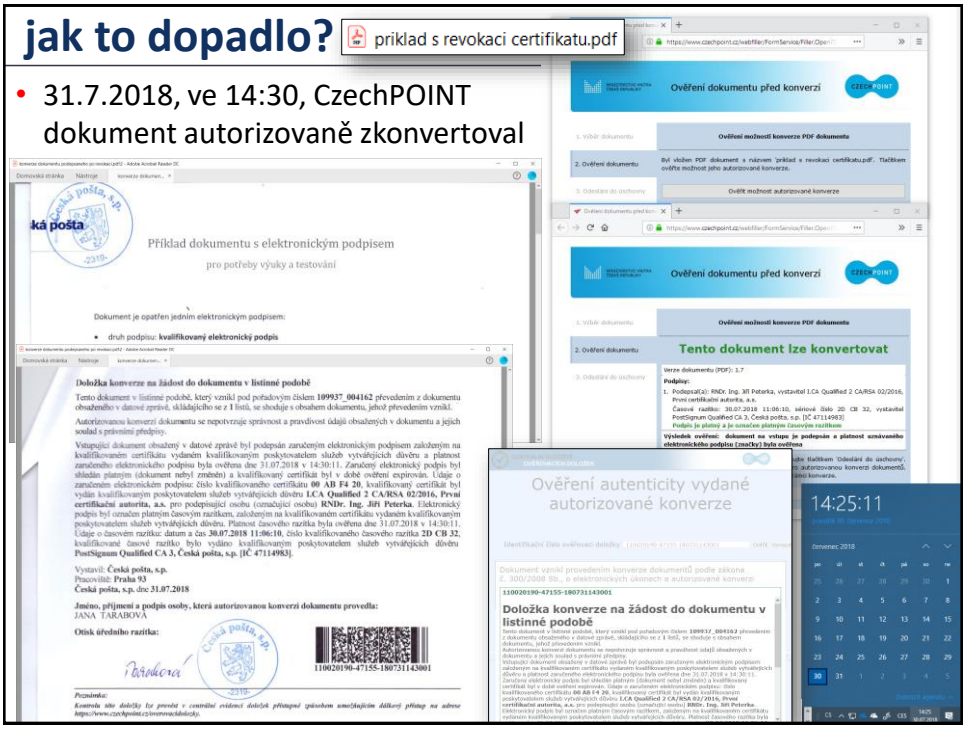
Signatures status :	1 valid signatures, out of 1
Document name :	priklad s revokaci certifikatu.pdf

26

jak to dopadlo?

priklad s revokaci certifikatu.pdf

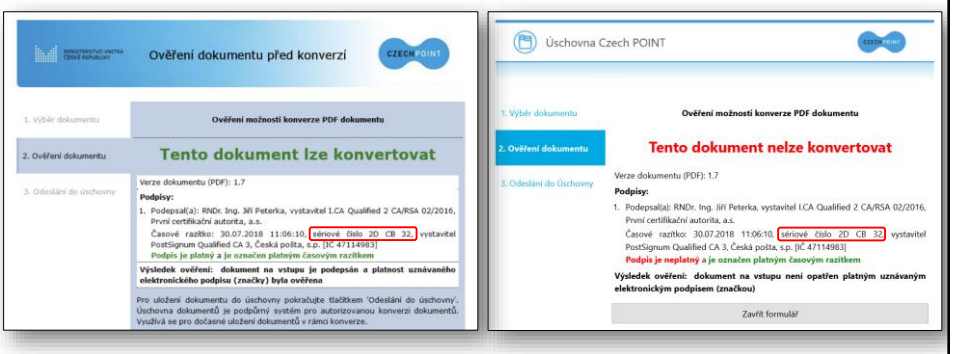
- 31.7.2018, ve 14:30, CzechPOINT dokument autorizovaně zkonvertoval



27

jak by to dopadlo dnes?

- po upozornění byla chyba v CzechPOINTu opravena, dnes by stejný dokument nebyl konvertován
  - podpis je vyhodnocen jako neplatný



dříve dnes

28

jiný problém: jednoznačná identifikace

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

29

co je uvedeno v certifikátu?

- každý certifikát má své (jednoznačné) sériové číslo
  - podle něj se lze ptát u vydavatele (certifikační autority)
- kvalifikovaný certifikát
  - musí povinně obsahovat: jméno (ve smyslu: jméno, příjmení)
  - další údaje obsahovat může, ale nemusí
    - nesmí být po něm vyžadováno, aby je obsahoval !!!
      - například: emailová adresa, adresa bydliště, zaměstnavatel, funkce, ...
  - v ČR: další (možné) údaje určí MV ČR vyhláškou, půjde zřejmě o AIFO

- původně (zákon č. 227/2000 Sb. o el. podpisu)
  - certifikát vydaný v tuzemsku musí obsahovat *„údaje jednoznačně identifikující podepsanou osobu“*
    - v praxi: jde o IK MPSV (upřesňuje vyhláška 212/2012 Sb.)
- dnes: požadavek nařízení eIDAS (910/2014/ES), článek 32
  - při ověřování je spoléhající se straně *„řádně poskytnut jedinečný soubor dat identifikujících podepisující osobu v certifikátu“*
    - žádný požadavek na IK MPSV apod.
    - výklad MV ČR: nejde o žádná „data navíc“ — stále je to jen „potenciální identifikace“
      - ale o ta, která již v certifikátu jsou (jméno, sériové číslo certifikátu, vydavatel, ….), a tato musí být spoléhající se straně řádně zobrazena

30

navrhovaná řešení

- návrh zákona o právu na digitální služby připravuje 2 různá řešení problému nejednoznačné identifikace
  - v §6: Právo na nahrazení úředně ověřeného podpisu nebo uznávaného elektronického podpisu

- na principu legalizace (odst. 1):
  - podepisující osoba (jakkoli) elektronicky podepíše svůj dokument
    - může se jednat i o prostý el. podpis
      - tedy například jen napsané jméno
  - poté se dostaví za „někým jiným“, kdo ověří její identitu a přidá své dobrozdání (doložku)
    - může to být oprávněná osoba (člověk) nebo IS VS (stroj)
  - výsledek může nahradit
    - úředně ověřený podpis
    - uznávaný elektronický podpis

- na principu „*veřejného přihlášení se k držení certifikátu*“ (odst. 2):
  - držitel kvalifikovaného certifikátu jej zveřejní
    - nechá jej přidat ke svým údajům v základním registru obyvatel
    - tím doplní chybějící vazbu na svou konkrétní osobu
      - ta pak „bude vidět“ skrze PVS
  - uznávaný elektronický podpis držitele pak bude moci nahradit jeho úředně ověřený podpis

31

autorizované konverze

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

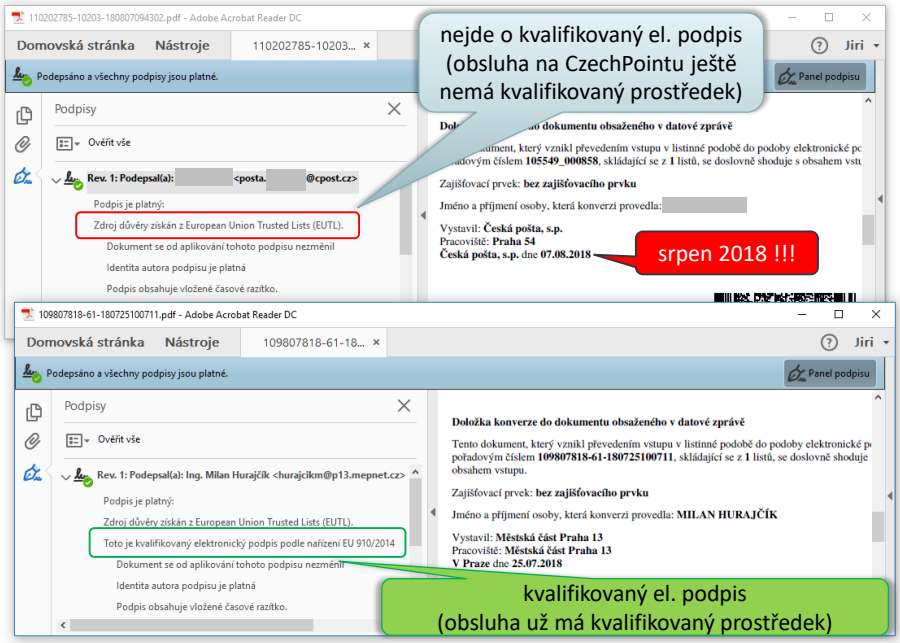
§ 25 zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi
Doložka
(1) Doložka konverze do dokumentu obsaženého v datové zprávě se považuje za součást výstupu a obsahuje
.....
h) kvalifikovaný elektronický podpis osoby, která konverzi provedla, nebo kvalifikovanou elektronickou pečeť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

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

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

32

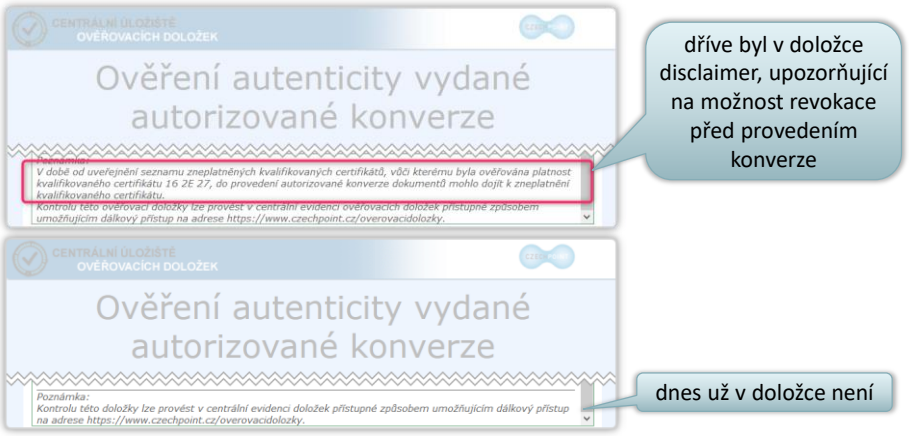
autorizované konverze



33

doložky autorizovaných konverzí

- doložky se evidují (archivují) a jsou veřejně dostupné



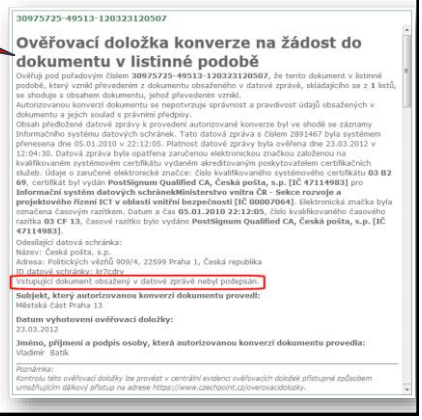
- ale stále:
  - nepozná se, k jakému vstupnímu dokumentu se doložky vztahují !!!
    - nezahrnují ani otisk (hash) el. dokumentu, ani určení jeho obsahu (čeho se týká)
  - doložka hovoří o počtu listů – ale (u listinného dokumentu): kolik měl stránek?

34

autorizované konverze

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

příklad z roku 2012


30975725-49513-120323120507

Ověřovací doložka konverze na žádost do dokumentu v listinné podobě

Ověřuji pod pořadovým číslem **30975725-49513-120323120507**, že tento dokument v listinné podobě, který vznikl převedením z dokumentu obsaženého v datové zprávě, skládajícího se z **1** listů, se shoduje s obsahem dokumentu, jehož převedením vznikl.

Autorizovanou konverzí dokumentu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.

Obsah předložené datové zprávy k provedení autorizované konverze byl ve shodě se záznamy Informačního systému datových schránek. Tato datová zpráva s číslem 2891467 byla systémem přenesena dne 05.01.2010 v 22:12:05. Platnost datové zprávy byla ověřena dne 23.03.2012 v 12:04:30. Datová zpráva byla opatřena zaručenou elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Údaje o zaručené elektronické značce: Číslo kvalifikovaného systémového certifikátu **03 B2 69**, certifikát byl vydán **PostSignum Qualified CA, Česká pošta, s.p. [IČ 47114983]** pro **Informační systém datových schránekMinisterstvo vnitra ČR - Sekce rozvoje a projektového řízení ICT v oblasti vnitřní bezpečnosti [IČ 00007064]**. Elektronická značka byla označena časovým razítkem. Datum a čas **05.01.2010 22:12:05**, číslo kvalifikovaného časového razítka **03 CF 13**, časové razítko bylo vydáno **PostSignum Qualified CA, Česká pošta, s.p. [IČ 47114983]**.

Odesílající datová schránka:
Název: Česká pošta, s.p.
Adresa: Politických vězňů 909/4, 22599 Praha 1, Česká republika
ID datové schránky: keaaaby

Vstupující dokument obsažený v datové zprávě nebyl podepsán.

Subjekt, který autorizovanou konverzi dokumentu provedl:
Městská část Praha 13

Datum vyhotovení ověřovací doložky:
23.03.2012

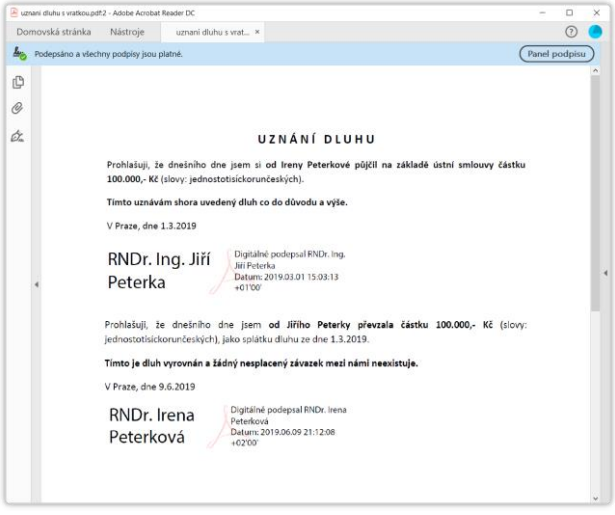
Jméno, příjmení a podpis osoby, která autorizovanou konverzi dokumentu provedla:
Vladimír Batík

Poznámka:
Kontrolu této ověřovací doložky lze provést v centrální evidenci ověřovacích doložek přístupné způsobem umožňujícím dálkový přístup na adrese https://www.czechpoint.cz/overovacidolozky.

35

autorizované konverze

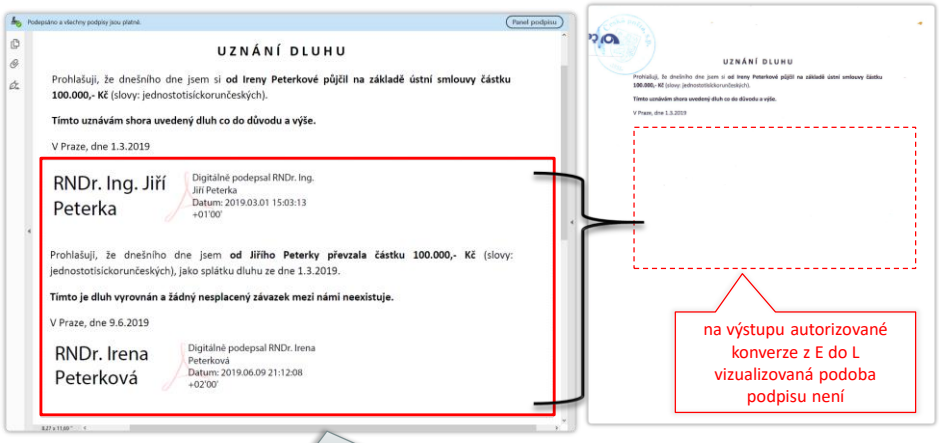
- problém s vizualizovanou podobou el. podpisů a pečetí
  - může to být jakýkoli obrázek, i takový který mění jeho význam či vyznění
  - otázka: má být vizualizovaná podoba podpisu/pečeti součástí listinného výstupu?
- příklad:
  - kolik je na dokumentu podpisů?
  - byl dluh vyrovnán, nebo nikoli?



36

autorizované konverze

- realita: CzechPointy vizualizovanou podobu nekonvertují !
  - názor: a je to tak asi dobře (je to méně nebezpečná varianta)



37

děkuji za pozornost

Jiří Peterka
jiri@peterka.cz
http://jiri.peterka.cz

38