3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

Proč dnešní elektronické podpisy nejsou věčné?

Jiří Peterka

2011

3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

omyl !!!!!

- elektronické podpisy jsou věčné !!!!
  - stejně jako všechny (ostatní) druhy podpisů
    - i vlastnoruční podpisy na listinných dokumentech

- důvod?
  - právní řád nezná „podpis na dobu určitou“, resp. „podpis s omezenou platností v čase“
    - vůbec nepočítá s tím, že by platnost podpisu byla omezena v čase
      - ve smyslu: tento podpis pozbývá platnosti po X dnech/měsících/letech
    - časově omezené mohou být právní úkony, stvrzené podpisem
  - podpis nelze revokovat (ukončit jeho platnost)
    - nelze říci: „*tento podpis byl můj, ale teď už můj není*“
    - lze revokovat (odvolat, zneplatnit) právní úkon, stvrzený podpisem
    - lze revokovat certifikát ….

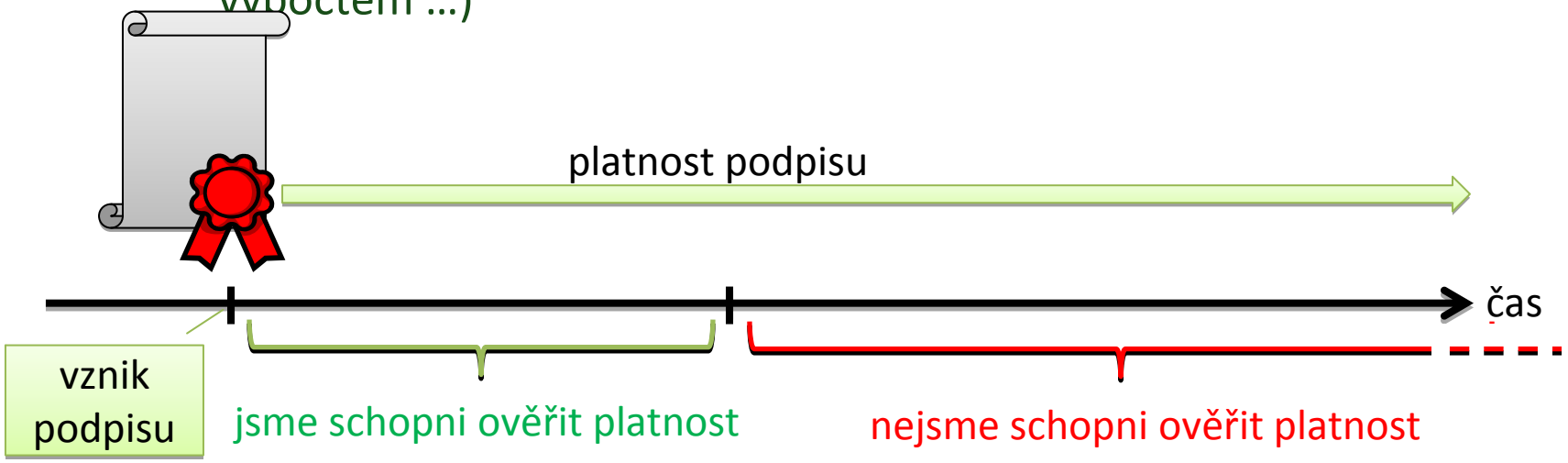
3A2E 5665 6E6F 7661 6E69 2E3A 0D0 A 5475 746F 206B 6E69 6875 2076 656E 756A 6920 7376 6520 7A65 6E65 2049 7265 6E65 2C20 7379 6E6F 7669 204A 6972 696D 7520 6120 6463 6572 6920 4576 652E 0D0 A562 0507 2617 A652 C204 C503 2303 1302 04A6 9726 9205 0657 4657 26B6 1

co tedy není věčné?

- u elektronických podpisů:
  - časově omezena je možnost ověřit (a prokázat) platnost podpisu !!!!
- důsledek:
  - (elektronický) podpis platí stále, i když už nejsme schopni ověřit (a prokázat) jeho platnost
    - není to tak, že: platnost podpisu končí okamžikem, kdy přestaneme být schopni ověřit jeho platnost (elektronicky, výpočtem …)

přesvědčit sami sebe

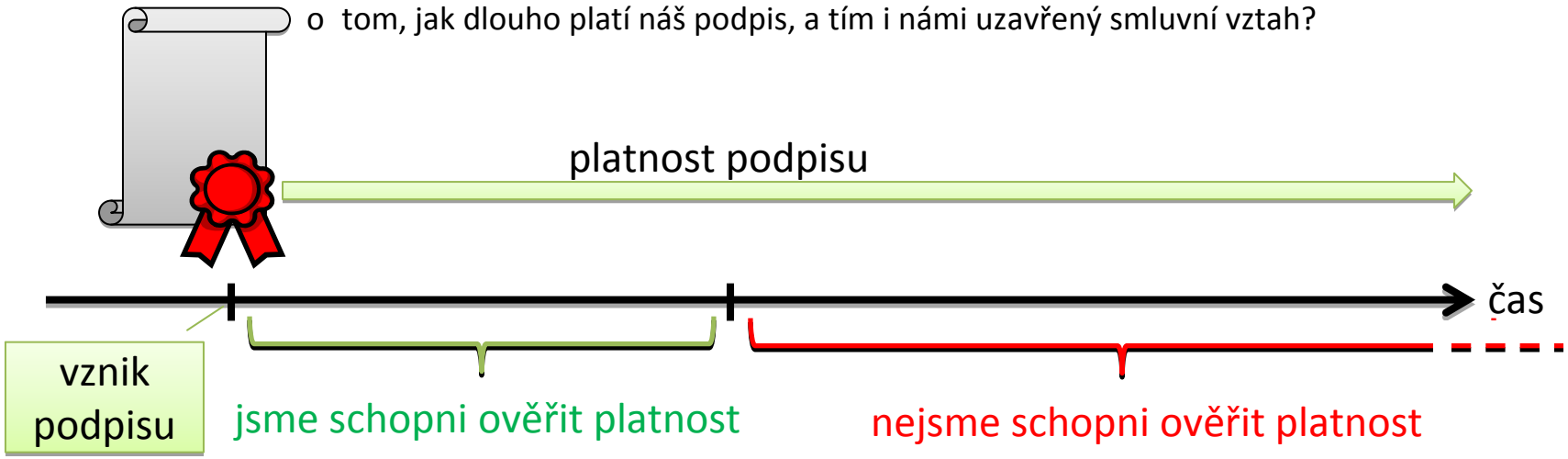
přesvědčit někoho jiného



3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

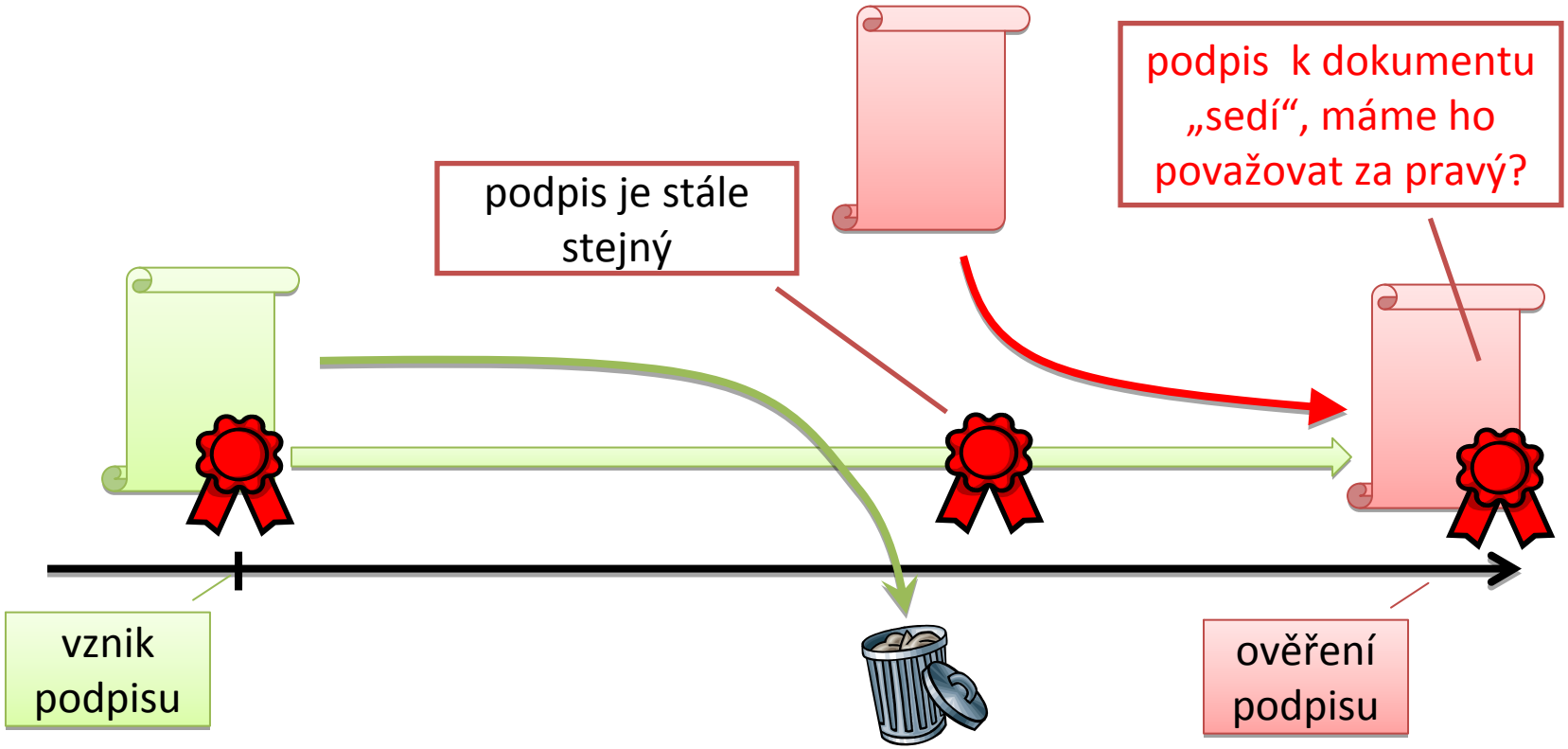
jakou to má logiku?

- přirovnání:
  - je to jako s objektivní realitou – i když ji přestanu vidět (vnímat), ona nepřestává existovat
- argumenty na podporu (neomezené platnosti el. podpisu):
  - platnost podpisu můžeme prokázat jinak (např. svědecky)
  - smluvní vztah, stvrzený elektronickým podpisem, by s koncem platnosti podpisu také končil
  - možnosti ověření můžeme uměle prodlužovat, nezávisle na samotném podpisu
    - například úkony, které provádí třetí strana (přerazítkovávání apod.). Má ona rozhodovat o tom, jak dlouho platí náš podpis, a tím i námi uzavřený smluvní vztah?



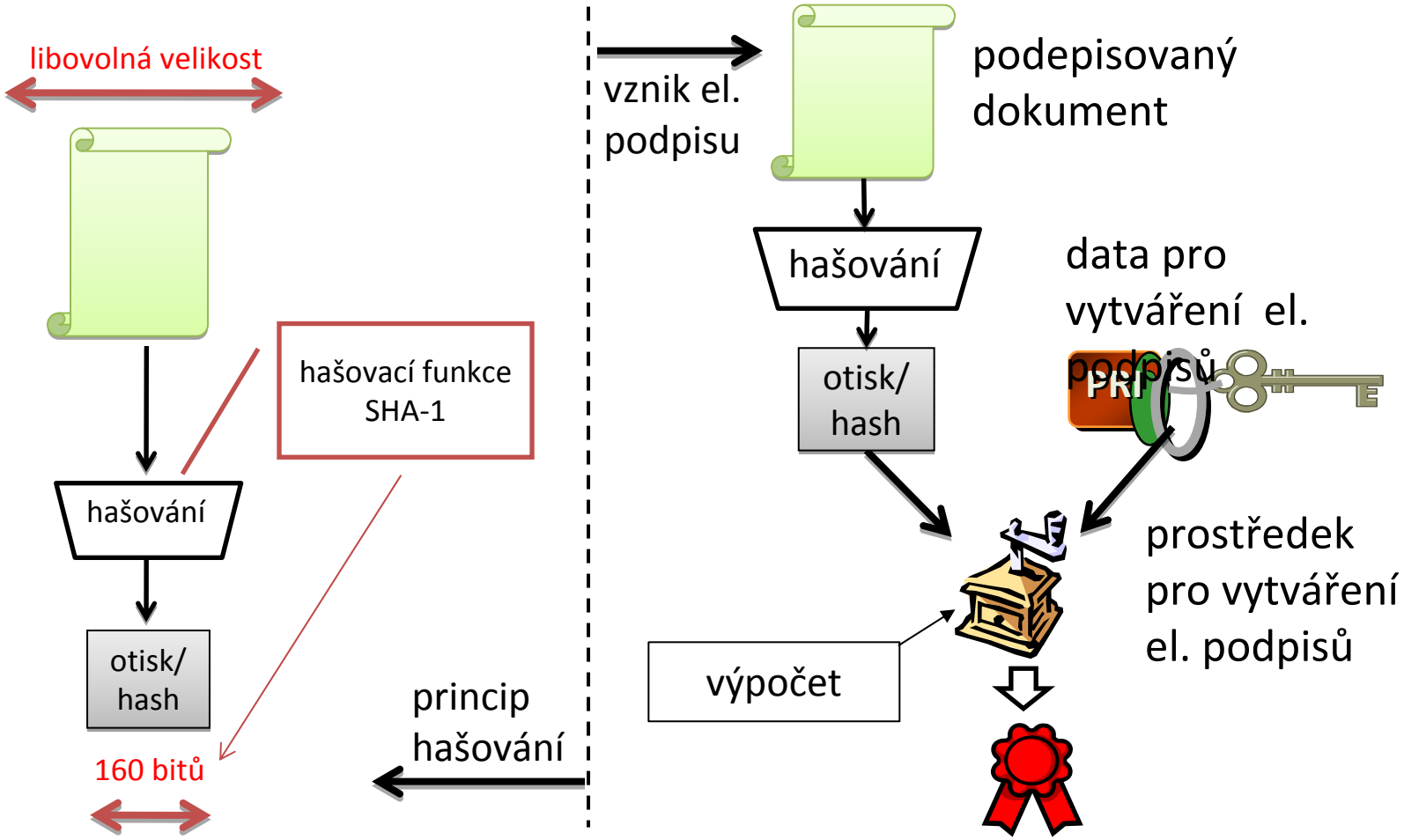
základní otázka

- možnost ověřit (a prokázat) platnost podpisu (elektronicky, cestou výpočtu) je časově omezována zcela záměrně a programově !!!!!
  - otázka: **proč?**
  - odpověď: **kvůli hrozbě tzv. kolizních dokumentů!**

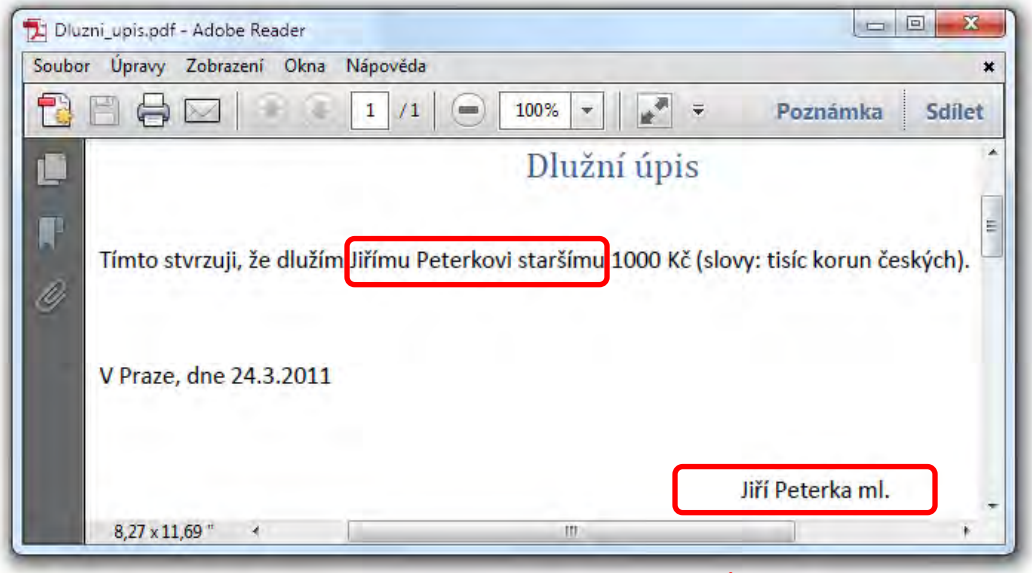


kde se berou kolizní dokumenty?

- jsou důsledkem toho, jak vzniká el. podpis
  - nepodepisují se samotné dokumenty (které mají různou velikost), ale pouze jejich otisky/hashe (které jsou vždy stejně velké)

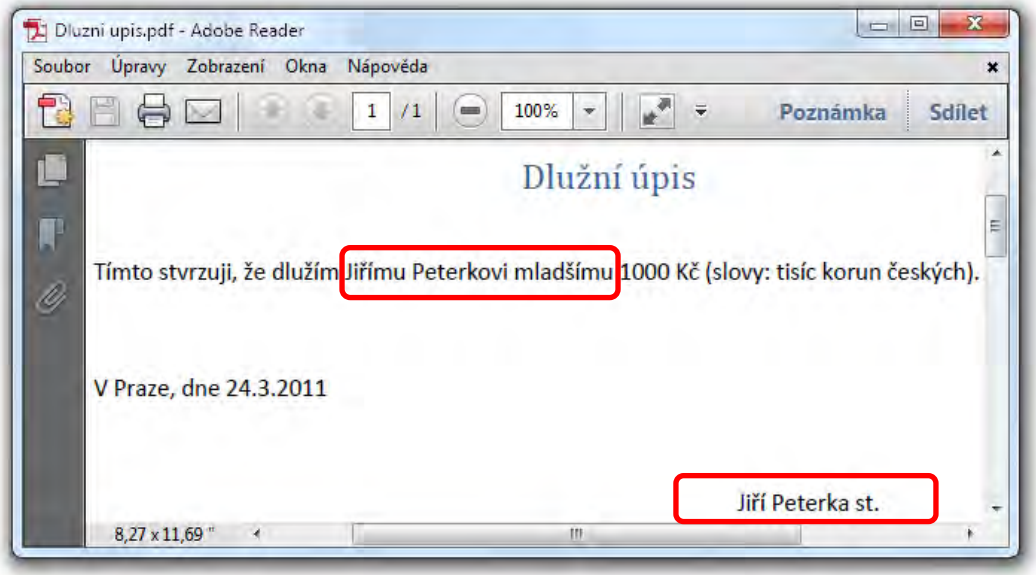


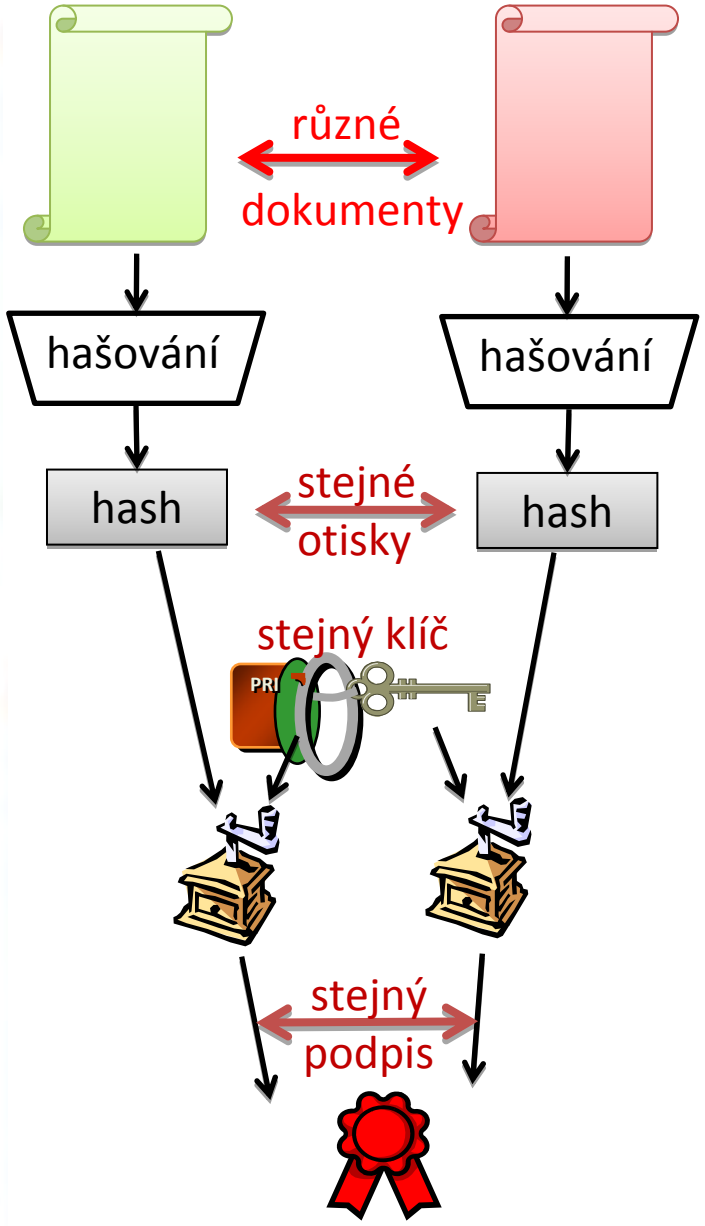
příklad kolizních dokumentů
(lze je stáhnout z http://bajecnysvet.cz)



(zabalené v obálce) mají stejný otisk/hash

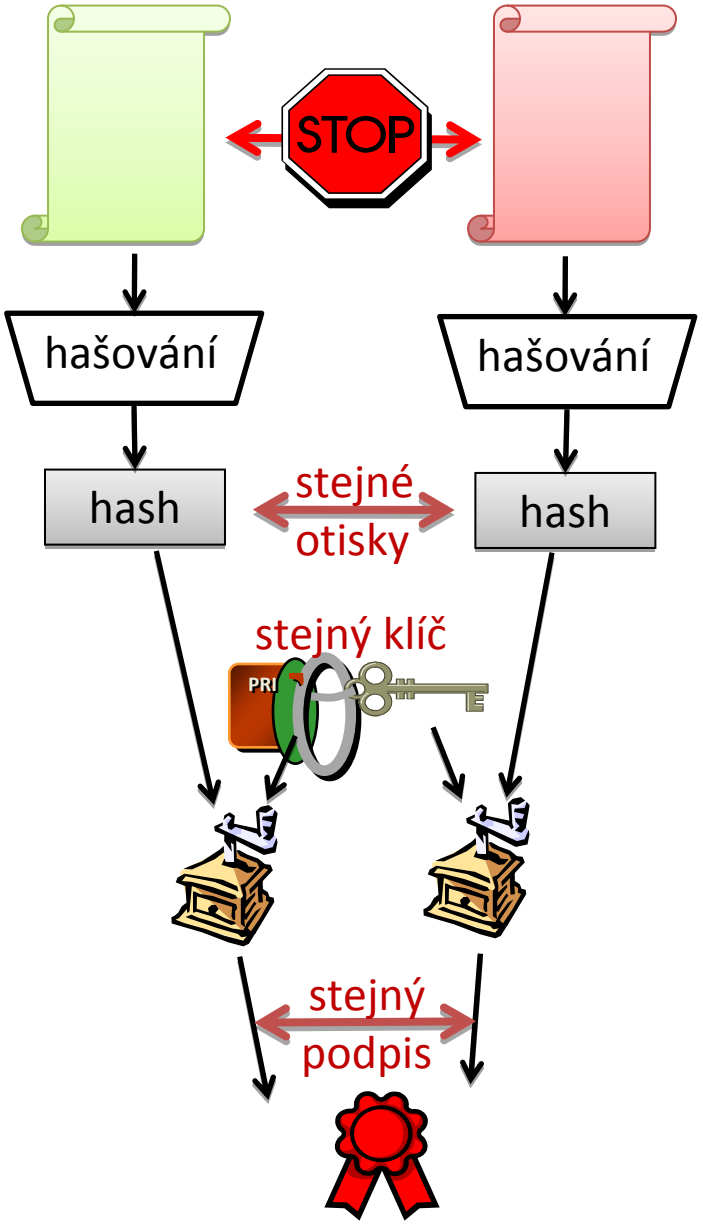
MD5: 4F15BCE86956225FA125269779583CC5





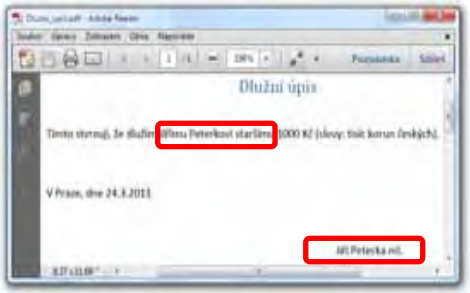
kdy může elektronický podpis „fungovat“?

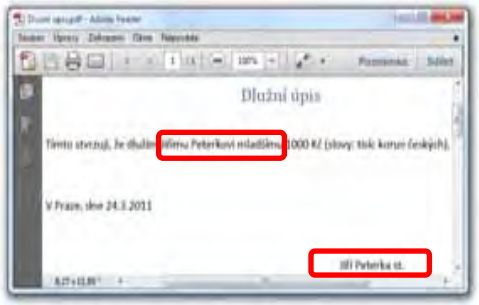
- pouze tehdy, pokud bude hledání (výpočet) kolizních dokumentů neúnosně dlouhé
  - nebude kratší, než „*nějaké miliony let*“
    - a podvodníkovi se nevyplatí je hledat
- ale:
  - výpočetní „síla“ našich počítačů rychle roste !!!!
- proto:
  - je nutné neustále zvyšovat složitost výpočtu (hledání kolizních dokumentů)
- jak?
  - používání „silnějších“ hašovacích funkcí
  - používáním delších klíčů
  - .....



3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6

vývoj hašovacích funkcí





4F15BCE86956225F
A125269779583CC5

=

4F15BCE86956225F
A125269779583CC5

5B991F4015BA79826380
4173566BD2C6B3DB8D09

≠

B73ED4198FBF69C4A874
FB5D7E2DD54373058338

77508B752C17273CD2467
2145C4868BFB22D311F376
780D366B5299CDCF1DA53

≠

CAD7C9CB5B9146DD6673E
35C4E1572C17AC4367AFC
10F084367351B898A63A21

nalezení kolizních dokumentů dnes trvá jen několik sekund

MD5
128 bitů

MD4
128 bitů

MD2
128 bitů

nepoužívat!!!!

SHA1
160 bitů

raději už také nepoužívat!!!!

SHA2
256 bitů

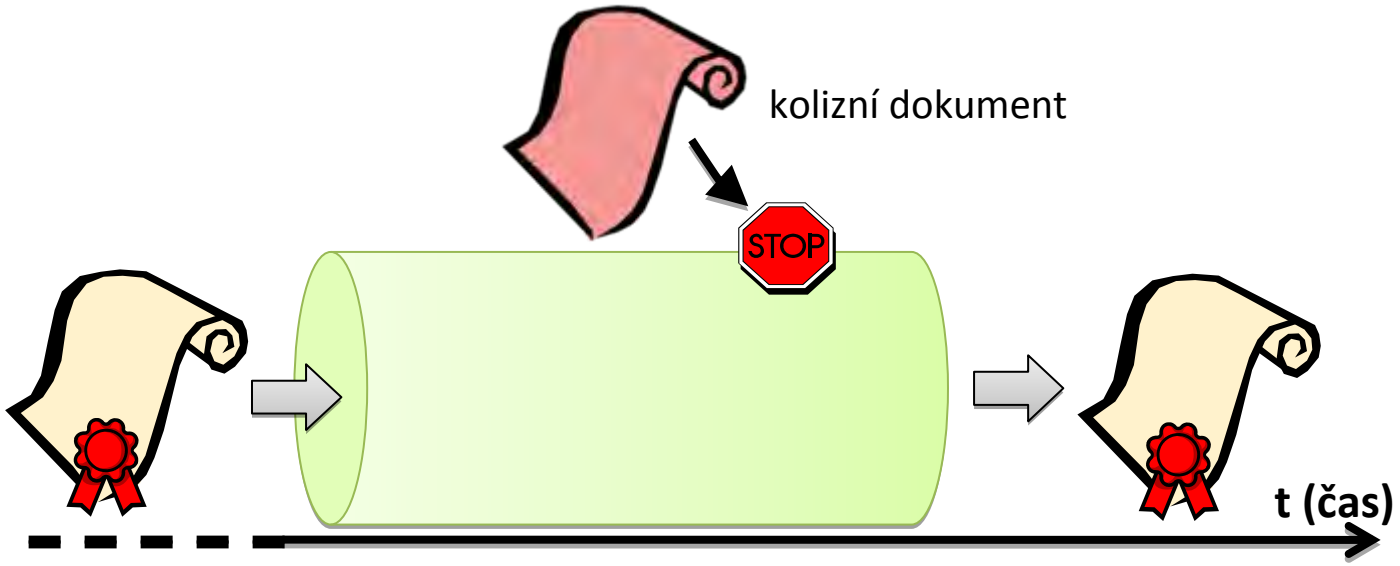
dnes doporučeno

čas

3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6

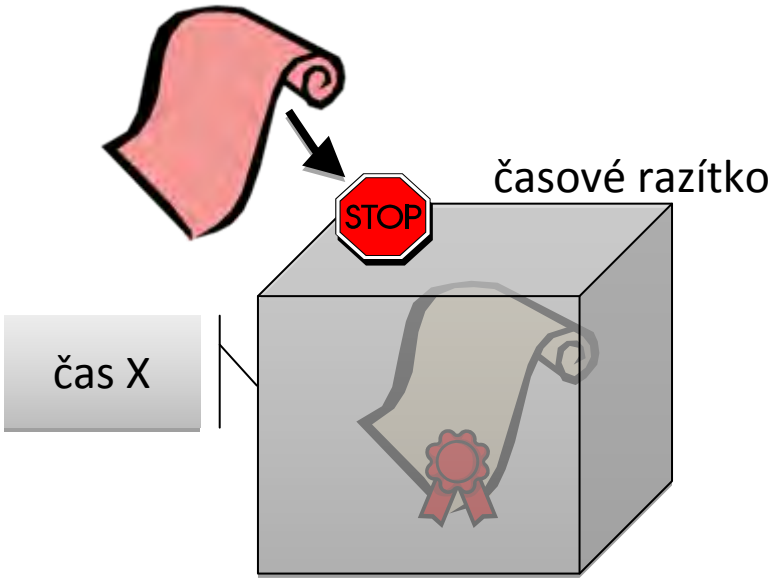
jak čelit nebezpečí kolizních dokumentů?

- technické řešení:
  - princip: zabráníme tomu, aby původní dokument mohl být nahrazen kolizním dokumentem
    - ve skutečnosti: zajistíme, abychom případnou záměnu kolizním dokumentem spolehlivě poznali
- jak?
  - postupným ~~přepodepisováním~~ přerazítkováváním .....



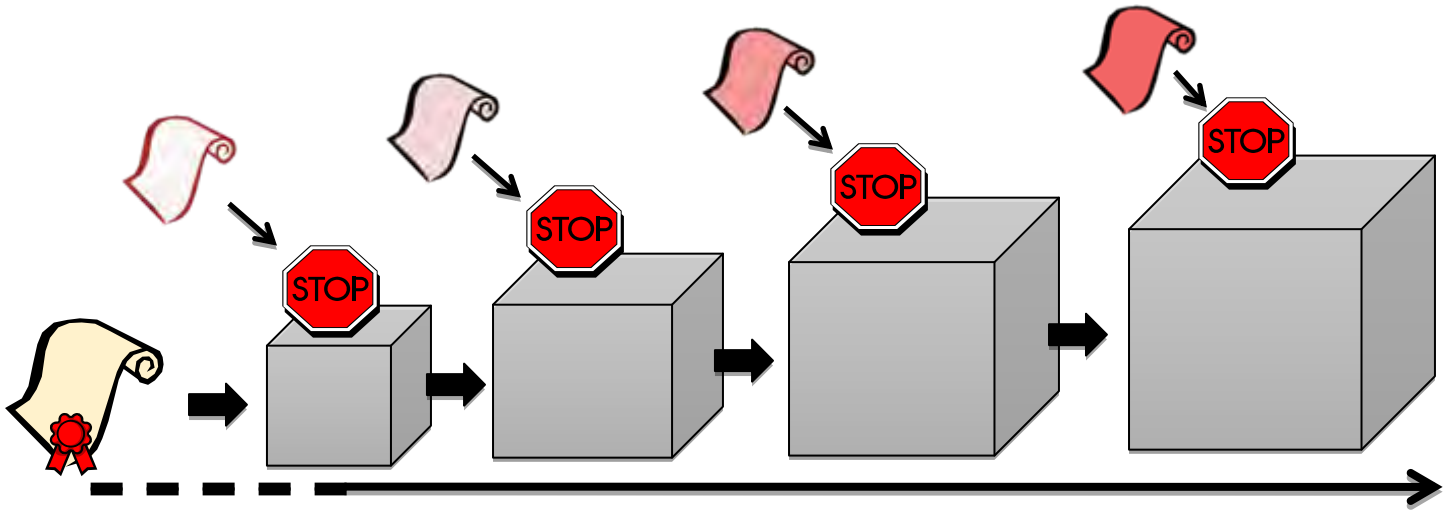
časové razítko místo el. podpisů

- proč ne postupné „přepodepisování“?
  - protože podpis vyjadřuje určité stanovisko k obsahu dokumentu (souhlas)
    - pokud zajišťuje třetí strana, neměla by žádné stanovisko zaujímat
  - časové razítko nevyjadřuje žádné stanovisko k obsahu
    - pouze ho fixuje „v čase“
      - stvrzuje jeho existenci v určitém časovém okamžiku
- představa:
  - časové razítko „vloží“ dokument (i s jeho podpisem) do bezpečnostní schránky
    - která chrání před nebezpečím záměny kolizním dokumentem
  - a ještě přidá (důvěryhodný) údaj o čase



postupné „přerazítkovávání“

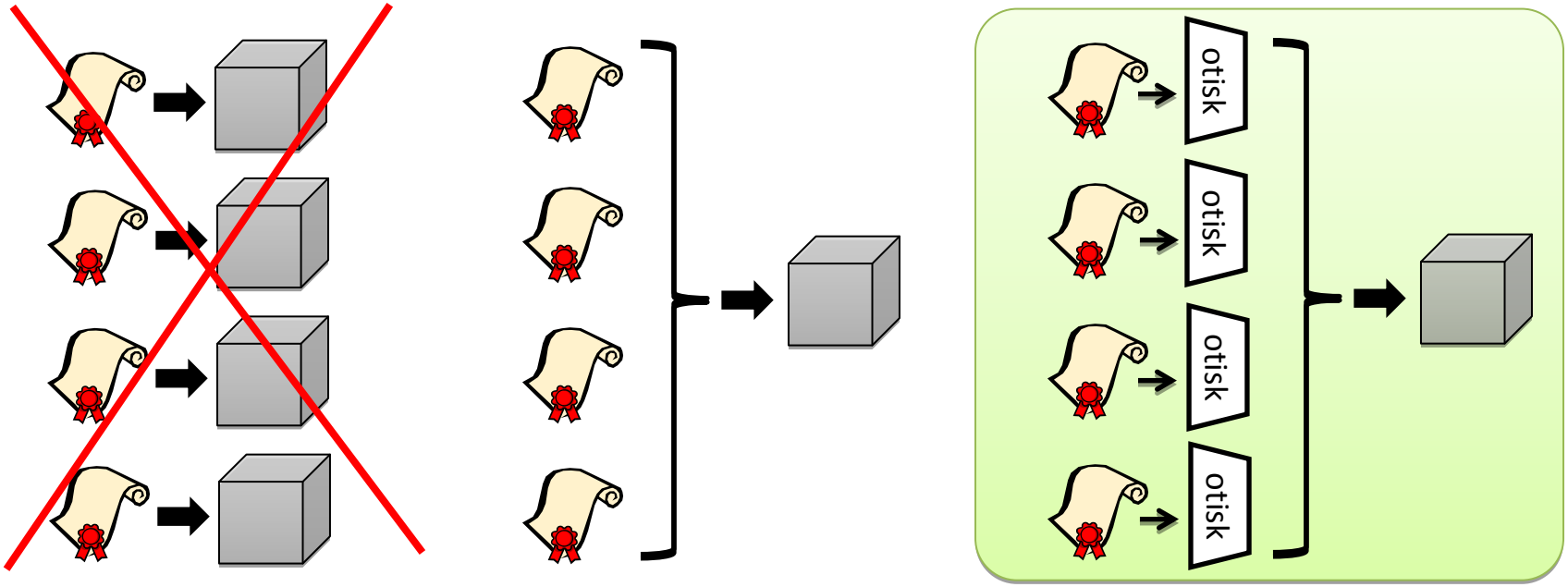
- i časová razítka mají omezenou „trvanlivost“
  - možnost jejich ověření (nikoli platnost) je záměrně omezena v čase
    - skrze časově omezenou platnost certifikátů, na kterých je časové razítko založeno
  - fakticky: je to nutné kvůli hrozbě kolizních dokumentů
    - i časová razítka musí postupně „přitvrzovat“
      - používat silnější hašovací funkce atd.
- důsledek:
  - nové (další) časové razítko je třeba přidat ještě dříve, než skončí možnost ověření platnosti předchozího časového razítka



3A2E 5665 6E6F 7661 6E69 2E3A 0D0 A 5475 746F 206B 6E69 6875 2076 656E 756A 6920 7376 6520 7A65 6E65 2049 7265 6E65 2C20 7379 6E6F 7669 204A 6972 696D 7520 6120 6463 6572 6920 4576 652E 0D0 A562 0507 2617 A652 C204 C503 2303 1302 04A6 9726 9205 0657 4657 26B6 1

jak přerazítkovávat?

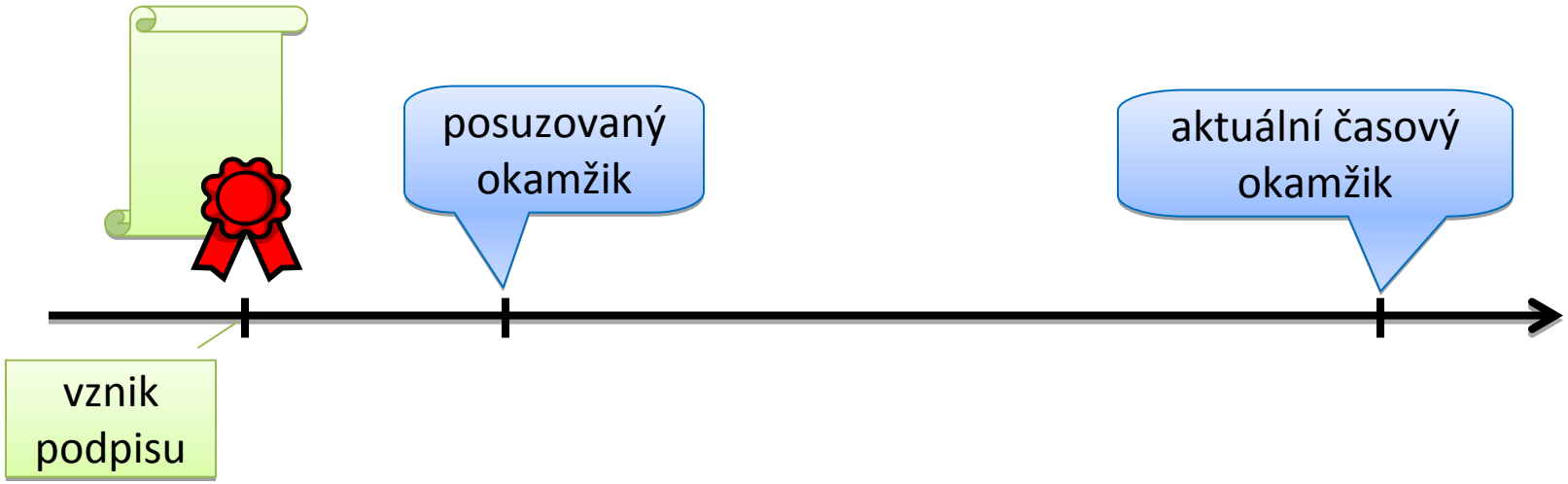
- přerazítkovávat každý dokument samostatně by bylo drahé
  - a není to nutné
  - lze přerazítkovávat více dokumentů současně
    - 1 razítko na N dokumentů
    - ale: problém s ověřováním, k tomu je nutných všech N dokumentů
  - výhodnější:
    - přerazítkovávat otisky více dokumentů
    - 1 razítko na N otisků (od N dokumentů)
      - k ověření pak stačí jen otisky dokumentů, nejsou nutné samotné dokumenty



3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

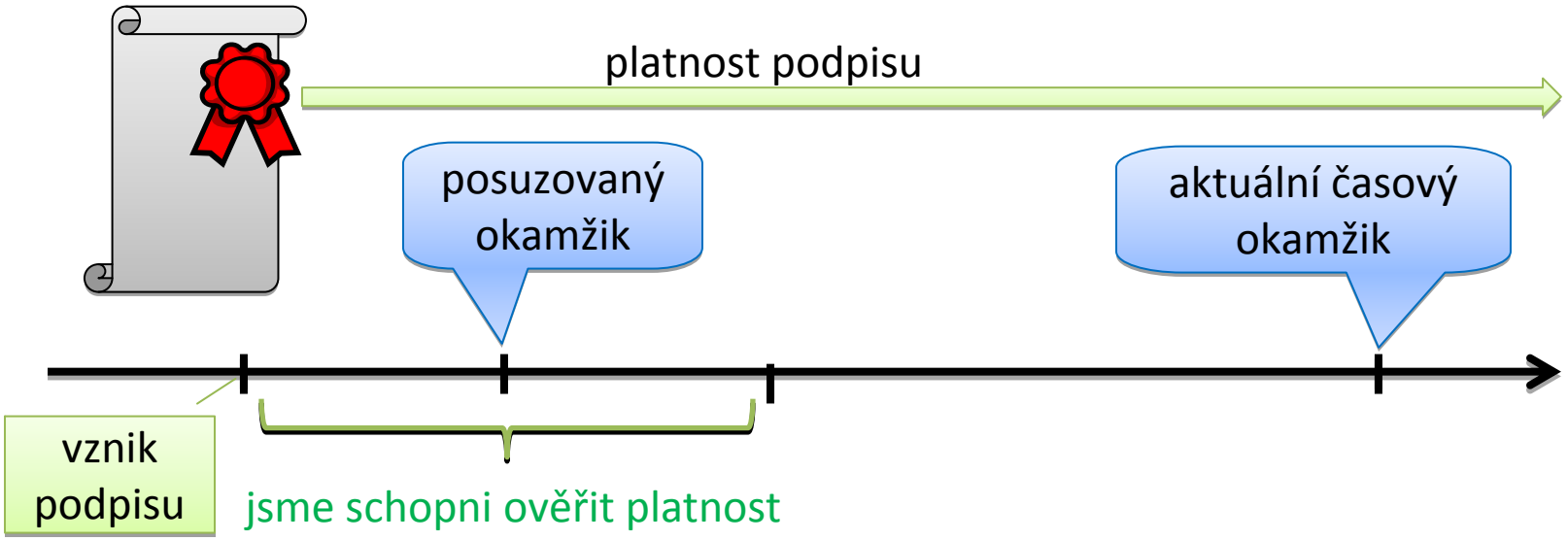
faktor času při ověřování

- je třeba rozlišovat:
  - **kdy ověření provádíme** (vždy: v aktuálním časovém okamžiku)
  - **k jakému okamžiku ověření provádíme** (tzv. posuzovaný okamžik)
    - optimálně: měl by to být okamžik vzniku podpisu
    - v praxi: tento okamžik neznáme !!!!
      - pokud je časové razítko, pak **posuzovaný okamžik = čas razítka**
      - jinak musí být **posuzovaný okamžik = aktuální okamžik**



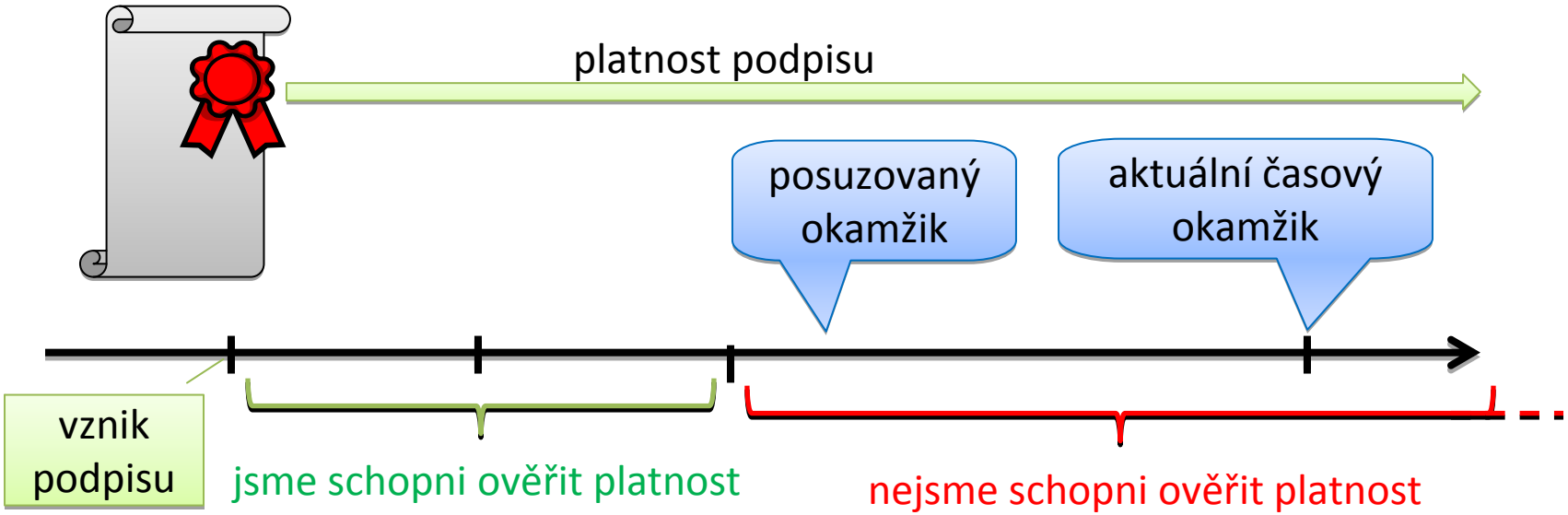
faktor času při ověřování

- zjistíme-li, že podpis byl platný k posuzovanému okamžiku
  - pak byl platný i v době svého vzniku
  - pak je platný i v aktuálním časovém okamžiku
    - a bude platný i v budoucnu (viz: jeho platnost nekončí)



faktor času při ověřování

- pozor: opačně to neplatí
  - pokud k posuzovanému okamžiku nejsme schopni ověřit platnost podpisu, neznamená to, že musí být neplatný
    - může být platný
      - a pouze námi použitý posuzovaný okamžik již „leží“ mimo dobu, po kterou je možné platnost ověřit



3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

jak může ověření dopadnout?

- konstatováním, že podpis je platný
  - pokud jsou splněny všechny podmínky pro platnost podpisu
    - vyhodnocování provádíme v aktuálním časovém okamžiku
    - platnost hodnotíme k posuzovanému okamžiku
- konstatováním, že podpis je neplatný
  - jen pokud pro to existuje explicitní důvod
    - například porušená integrita dokumentu
    - například: některý z certifikátů byl k posuzovanému okamžiku revokovaný
    - .....
- konstatováním, že „nevíme“
  - ve všech ostatních případech, například:
    - nemáme k dispozici všechny potřebné podklady
    - nevíme, zda se můžeme na všechny podklady spoléhat, například:
      - některému z certifikátů k posuzovanému okamžiku již skončila jeho řádná platnost
      - nevíme, zda certifikát je důvěryhodný
      - .....

co potřebujeme pro ověření

- všechny „podklady“ potřebujeme mít k dispozici v aktuálním časovém okamžiku
  - ale logicky musí být vztaženy k posuzovanému okamžiku !!!
- musíme zajistit:
  - aby všechny „podklady“ byly skutečně k dispozici
  - aby všechny „podklady“ byly autentické a důvěryhodné
    - abychom se na ně mohli spoléhat
      - včetně toho, že k otisku ještě neexistují kolizní dokumenty

3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

příklad: expirovaný certifikát

- dokument je opatřen elektronickým podpisem, ale nikoli časovým razítkem
  - proto nutně: posuzovaný okamžik = aktuální okamžik
- konkrétně:
  - podpis o sobě tvrdí, že vnikl 1.7.2009
    - ale to mu nemůžeme věřit (jde o údaj, který lze libovolně nastavit)
  - řádná platnost certifikátu skončila 1.3.2010
  - podpis ověřujeme k aktuálnímu okamžiku (5.4.2011)
- výsledek: **„nevíme“**
- důsledek: musíme se chovat stejně, jako kdyby podpis byl neplatný
  - nemůžeme se spoléhat na to, co je podepsáno

3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

příklad: časové razítko

- PDF dokument je opatřen elektronickým podpisem a také časovým razítkem
  - proto: posuzovaný okamžik = **okamžik dle razítka**
- konkrétně:
  - časový údaj na časovém razítku: 1.7.2009
    - časové razítko stále dokážeme vyhodnotit jako platné, příslušný certifikát je ještě platný (PostSignum do června 2012)
  - řádná platnost certifikátu skončila 1.3.2010
  - podpis ověřujeme k aktuálnímu okamžiku (5.4.2011)
- problém:
  - informace o revokaci již nejsou dostupné tam, kde by měly být (dle URL v certifikátu)
- výsledek: Adobe Acrobat/Reader: **„nevíme“**
- CzechPoint: „podpis je platný“
  - dokáže si najít/získat „historické“ údaje o revokaci

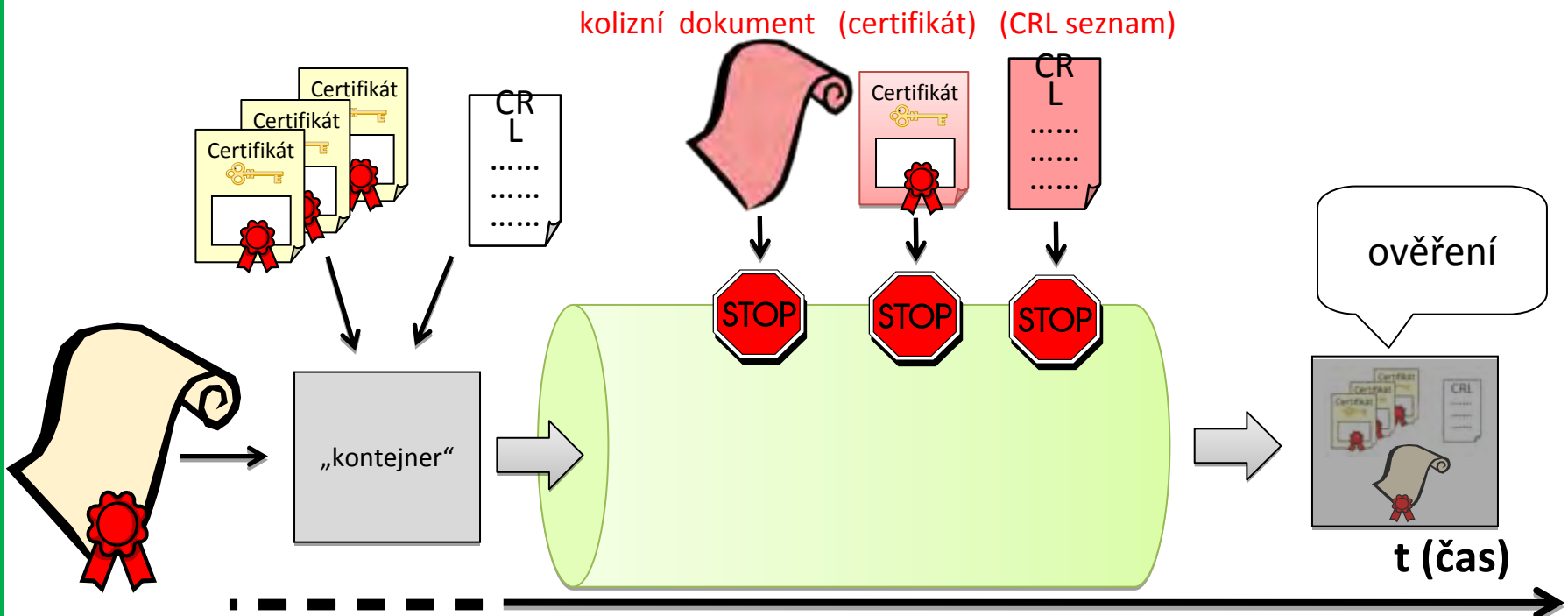
3A2E 5665 6E6F 7661 6E69 2E3A 0D0 A 5475 746F 206B 6E69 6875 2076 656E 756A 6920 7376 6520 7A65 6E65 2049 7265 6E65 2C20 7379 6E6F 7669 204A 6972 696D 7520 6120 6463 6572 6920 4576 652E 0D0 A562 0507 2617 A652 C204 C503 2303 1302 04A6 9726 9205 0657 4657 26B6 1

co potřebujeme pro ověření

- otisk (hash) dokumentu
  - nesmějí k němu (zatím) existovat kolizní dokumenty
- elektronický podpis (značku, razítko)
- certifikát, na kterém je podpis založen
  - obsahuje veřejný klíč, nutný k ověření podpisu
  - musí být platný k posuzovanému okamžiku
    1. k posuzovanému okamžiku nesměla skončit jeho řádná platnost
    2. k posuzovanému okamžiku nesměl být revokovaný
- všechny nadřazené certifikáty
  - všechny musí být platné k posuzovanému okamžiku (1.+2.)
- revokační informace
  - vše, co potřebuji ke spolehlivému zjištění případné revokace všech certifikátů (tyto informace nejsou a nemohou být součástí samotných certifikátů)

koncept LTV

- LTV (Long Term Validation) – elektronické podpisy s možností dlouhodobého ověření
  - jejich platnost lze ověřit i po delší (hodně dlouhé) době
- základní princip:
  - všechno to, co je potřeba k pozdějšímu ověření, se připojí k samotnému dokumentu a jeho podpisu
    - a uchovává tak, aby nehrozila záměna s kolizním dokumentem (ale i dalšími údaji)



jiný způsob zajištění „dlouhověkosti“

- elektronická obdoba notářské úschovy
- princip:
  - někdo bude oprávněn přijmout el. dokument do úschovy, uchovávat ho (delší dobu), a pak jej vydat s dobrozdáním, že je to „ten pravý“ dokument
    - například sám podepíše svým podpisem
- nutný předpoklad:
  - „ukotvení“ v zákoně, aby dobrozdání (podpis) el. notáře dával dokumentu potřebný statut

3A2E 5665 6E6F 7661 6E69 2E3A 0D0 A 5475 746F 206B 6E69 6875 2076 656E 756A 6920 7376 6520 7A65 6E65 2049 7265 6E65 2C20 7379 6E6F 7669 204A 6972 696D 7520 6120 6463 6572 6920 4576 652E 0D0 A562 0507 2617 A652 C204 C503 2303 1302 04A6 9726 9205 0657 4657 26B6 1

alternativní názorový proud

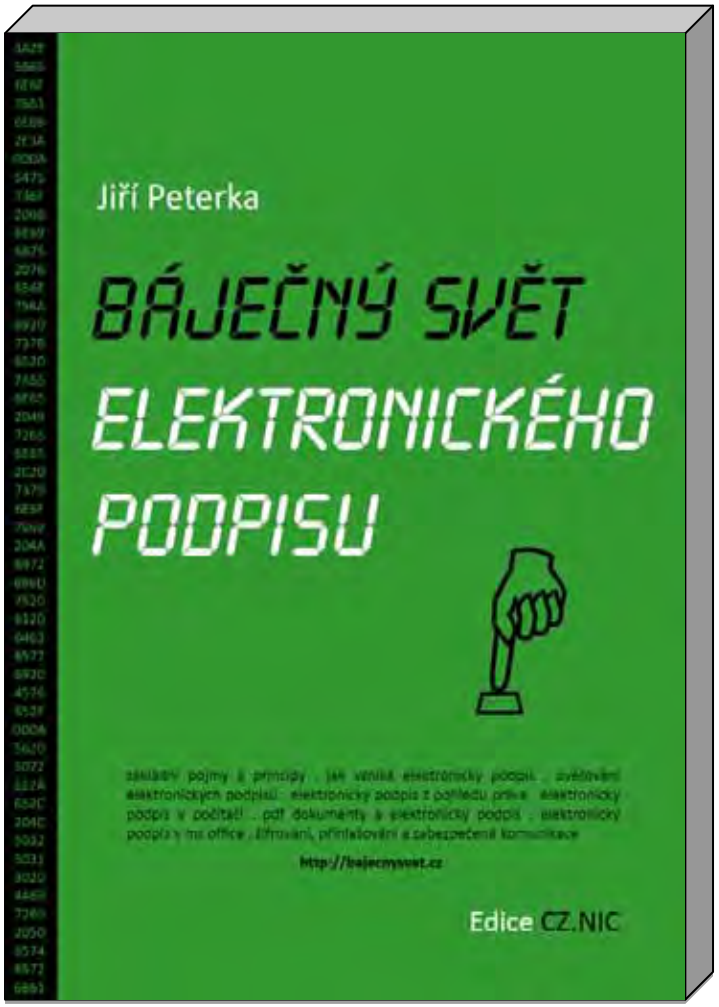
- teze: přerazítkovávání je zbytečné
  - nebo dokonce nesprávné ……
- obvykle zdůvodnění: tzv. **vyvratitelná domněnka pravosti**
  - *„Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem …… a opatřen kvalifikovaným časovým razítkem“.*
- ale:
  - jsme-li (stále ještě) schopni prokázat, že dokument byl platně podepsán, pak nepotřebujeme žádnou domněnku – protože máme jistotu
    - tím méně nepotřebujeme zpochybnění („dokud se neprokáže opak“)
  - nejsme-li již schopni prokázat platnost podpisu, pak domněnku nemůžeme aplikovat
    - nejsou splněny její předpoklady)

3A2E
5665
6E6F
7661
6E69
2E3A
0D0
A
5475
746F
206B
6E69
6875
2076
656E
756A
6920
7376
6520
7A65
6E65
2049
7265
6E65
2C20
7379
6E6F
7669
204A
6972
696D
7520
6120
6463
6572
6920
4576
652E
0D0
A562
0507
2617
A652
C204
C503
2303
1302
04A6
9726
9205
0657
4657
26B6
1

jaký je smysl domněnky?

- názor:
  - pokud by (elektronický) podpis ztrácel platnost v čase, pak by domněnka dávala smysl (
    - „budeme věřit v pravost dokumentu, pokud – někdy dříve – podpis byl platný, ale teď už jeho platnost skončila„
- ale:
  - jelikož platnost podpisu v čase nekončí, je domněnka nejen zbytečná, ale dokonce nebezpečná:
    - svádí k tomu, aby se lidé nestarali (aktivně) o své elektronické dokumenty a nechávali je „jen tak“ ležet
    - nechrání před kolizními dokumenty
      - jakoby říkala: věřme kolizním dokumentům, že jsou pravé – dokud se neprokáže opak. Ten se ale prokázat prakticky nedá …..

děkuji za pozornost



právě vychází v Edici CZ.NIC
volně ke stažení na http://knihy.nic.cz
on-line podpora na http://bajecnysvet.cz

Jiří Peterka

jiri@peterka.cz
http://jiri.peterka.cz
http://earchiv.cz
http://bajecnysvet.cz

tuto přednášku najdete v mém archivu (earchiv.cz)