

3A2E
5665
6E6F
7661
6E69
2E3A
0D0A
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
0D0A
5620
5072
617A
652C
204C
5032
3031
3020
4A69
7269
2050
6574
6572
6B61

Co dnes s elektronickými cáry papíru?

Jiří Peterka
2011



základní otázka

- proč se z elektronicky podepsaných (elektronických) dokumentů časem stávají bezcenné cary (elektronického) papíru?
 - na jejichž obsah se nemůžeme spoléhat
 - které nejdou autorizovaně konvertovat
 - které nám příjemce nemusí přijmout (když nechce)
 -
- možné odpovědi:
 - a) protože s časem končí platnost elektronického podpisu na elektronickém dokumentu
 - b) protože s časem končí naše schopnost ověřit platnost elektronického podpisu na elektronickém dokumentu
 - c) protože je časem již nedokážeme přečíst

základní otázka

- proč se z elektronicky podepsaných (elektronických) dokumentů časem stávají bezcenné cary (elektronického) papíru?
 - na jejichž obsah se nemůžeme spoléhat
 - které nejdou autorizovaně konvertovat
 - které nám příjemce nemusí přijmout (když nechce)
 -
- možné odpovědi:
 - ~~a) protože s časem končí platnost elektronického podpisu na elektronickém dokumentu~~
 - b) protože s časem končí naše schopnost ověřit platnost elektronického podpisu na elektronickém dokumentu
 - c) protože je časem již nedokážeme přečíst

kdy se ověřuje platnost podpisu?

- praxe u listinných dokumentů:
 - platnost se (obvykle) ověřuje, až když někdo napadne pravost dokumentu
 - formálně:
 - u veřejných listin platí presumpce pravosti a správnosti
 - u soukromoprávních dokumentů musí předkladatel prokázat jejich pravost a správnost
- u elektronických dokumentů tuto otázku řeší zákon (o elektronickém podpisu, č. 227/2000 Sb, §5/2):
 - za škodu odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zproští, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.
 - aneb: **pokud příjemce akceptuje elektronický dokument, u kterého nejde ověřit platnost jeho podpisu, ponese případné následky on !!!!**

elektronické podpisy jsou věčné !!!!

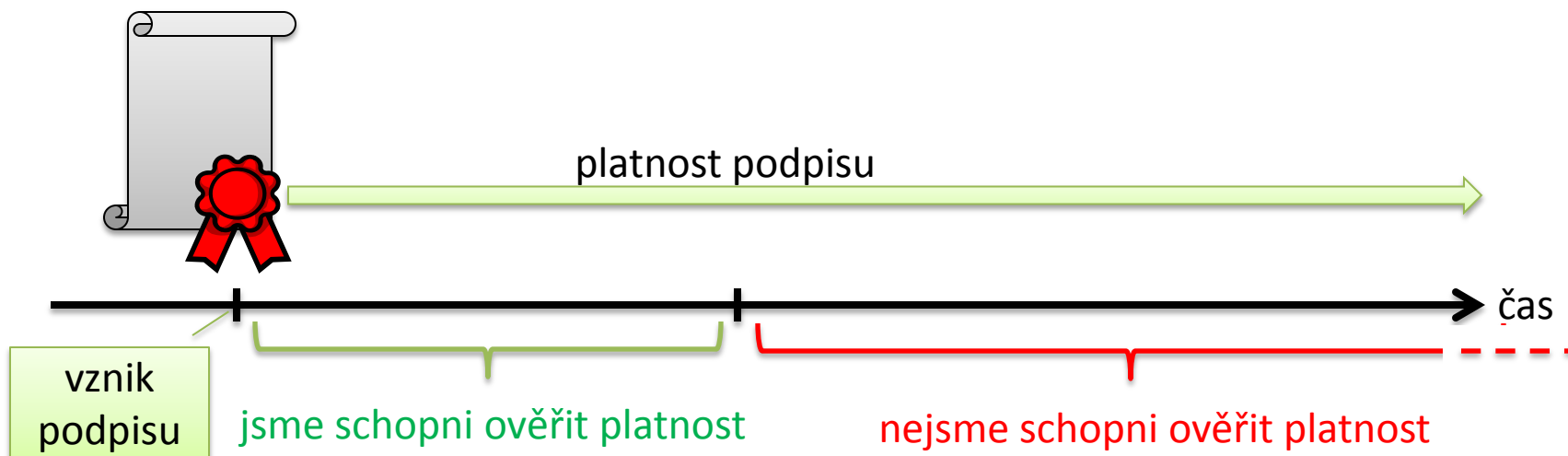
- stejně jako všechny (ostatní) druhy podpisů
 - i vlastnoruční podpisy na listinných dokumentech
- důvod?
 - právní řád nezná „podpis na dobu určitou“, resp. „podpis s omezenou platností v čase“
 - vůbec nepočítá s tím, že by platnost podpisu byla omezena v čase
 - ve smyslu: tento podpis pozbývá platnosti 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

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 ...)

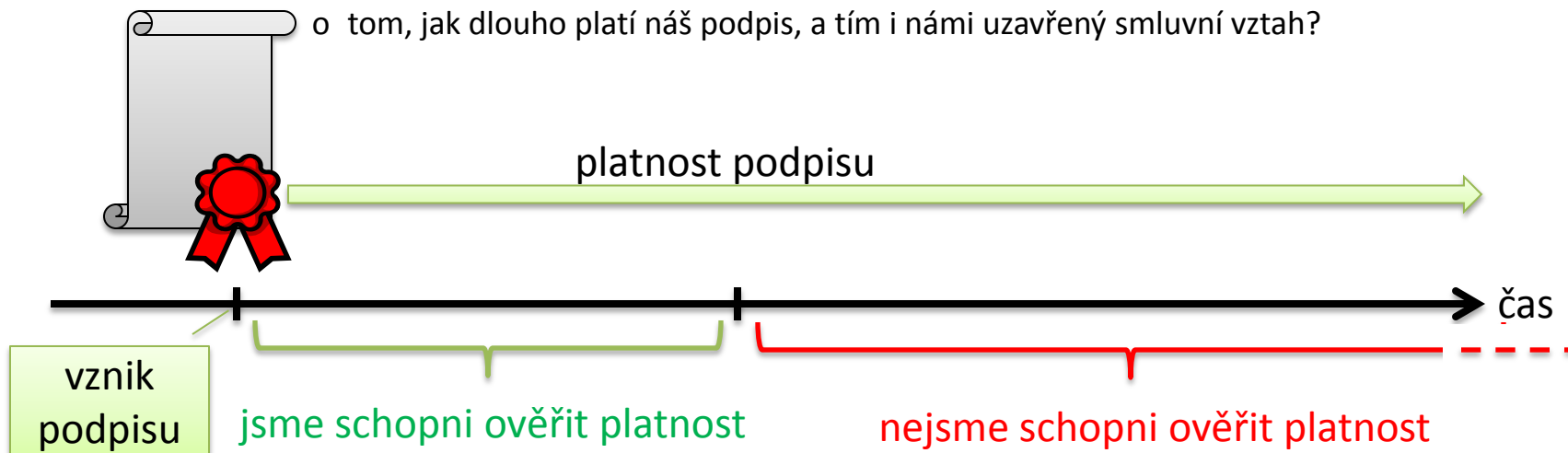
přesvědčit
sami sebe

přesvědčit
někoho jiného



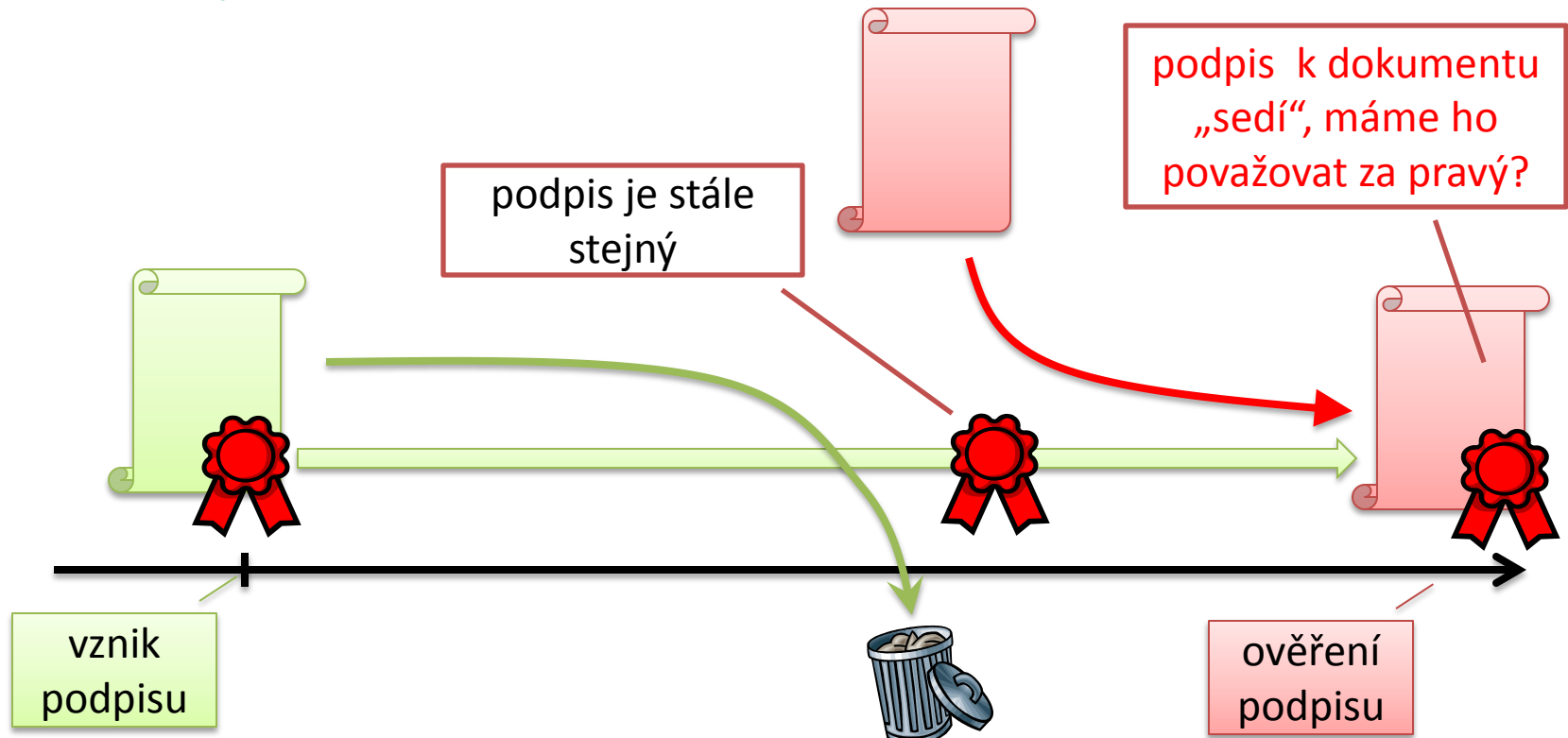
jakou to má logiku?

- 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?



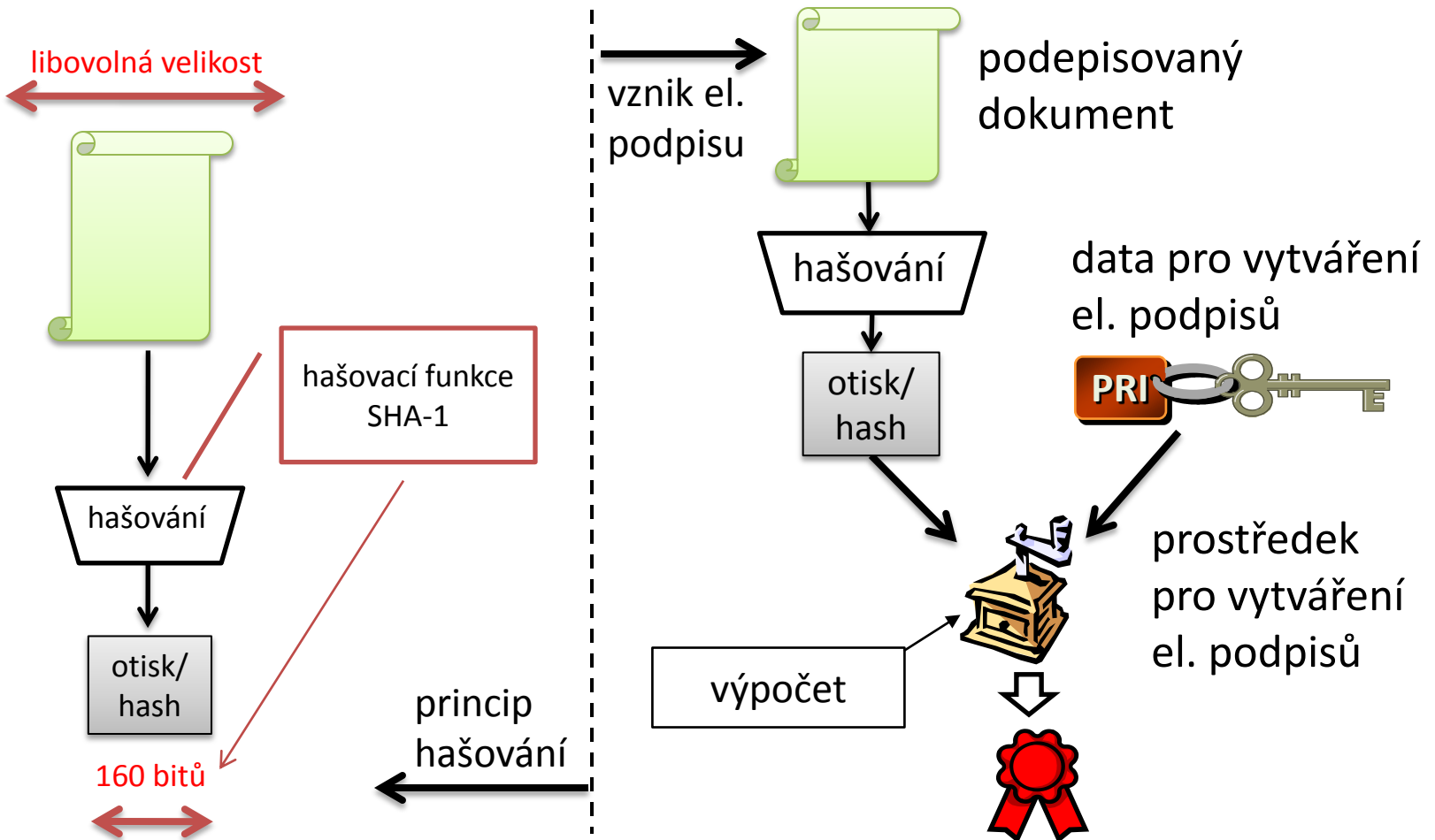
základní otázka

- 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?

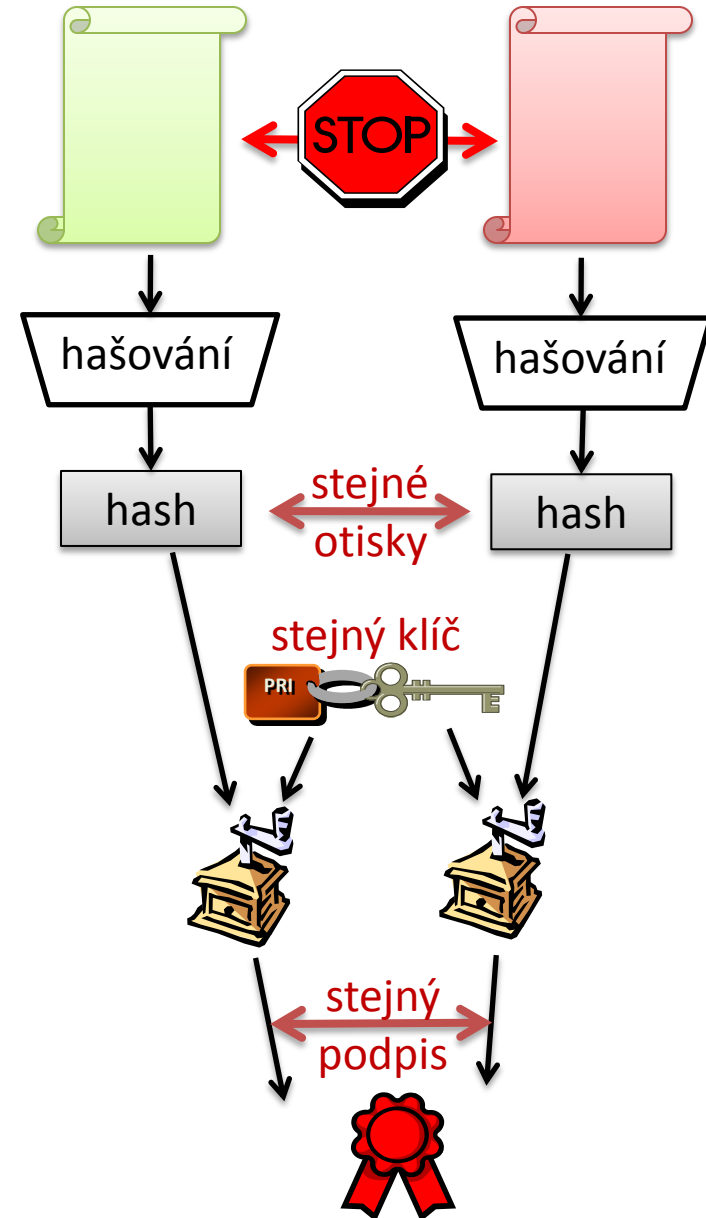
- jsou důsledkem toho, jak vzniká el. podpis
 - nepodepisují se samotné dokumenty (které mají různou velikost), ale pouze jejich otisky/hashe (které jsou vždy stejně velké)



3A2E
5665
6E6F
7661
6E69
2E3A
0D0A
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
0D0A
5620
5072
617A
652C
204C
5032
3031
3020
4A69
7269
2050
6574
6572
6B61
9

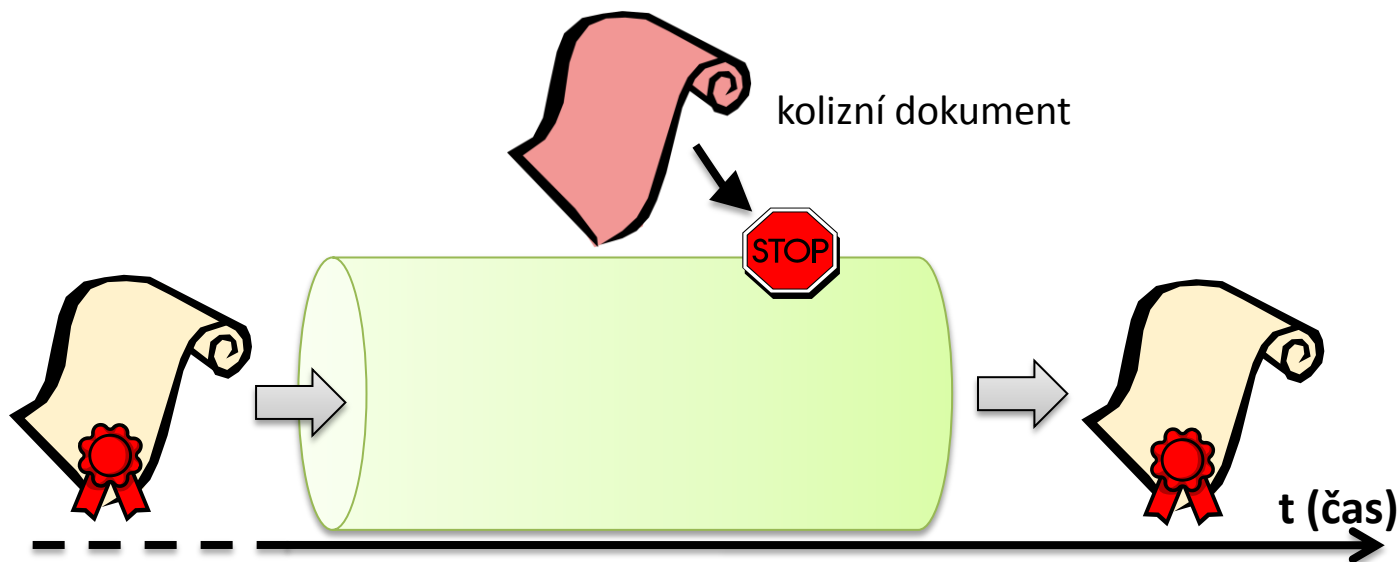
kdy může elektronický podpis „fungovat“?

- 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
 -



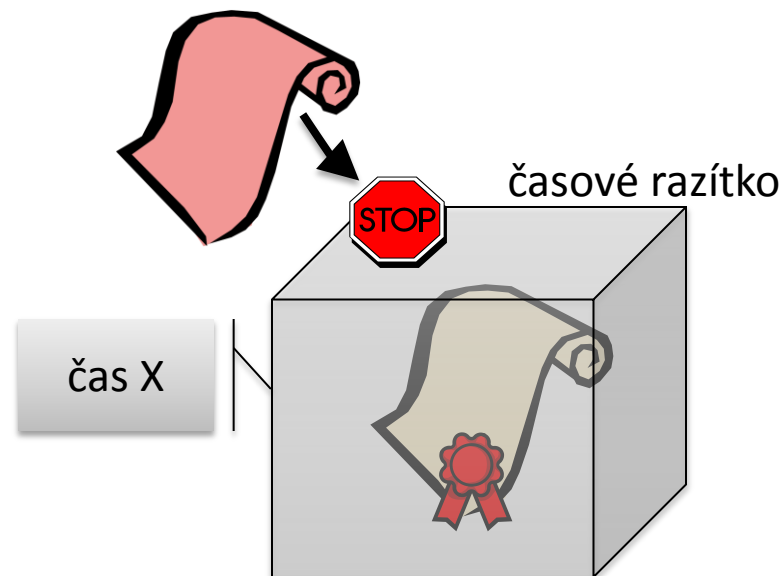
jak čelit nebezpečí kolizních dokumentů?

- 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 přepodpisováním přerazítkováním~~



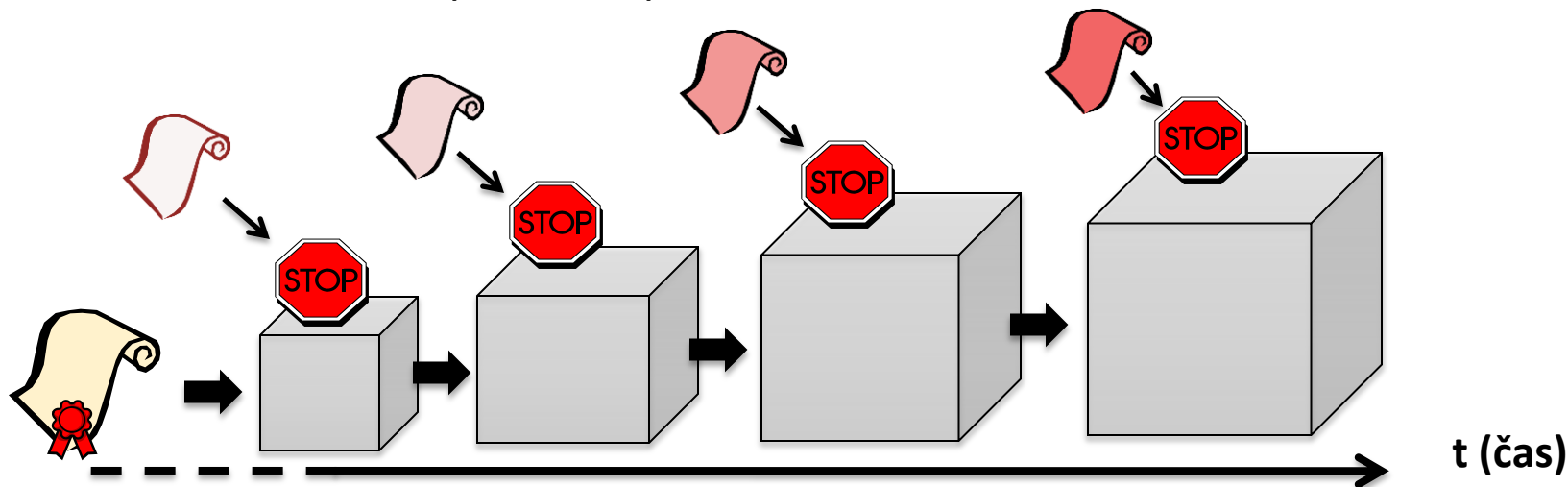
časové razítko místo el. podpisů

- 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



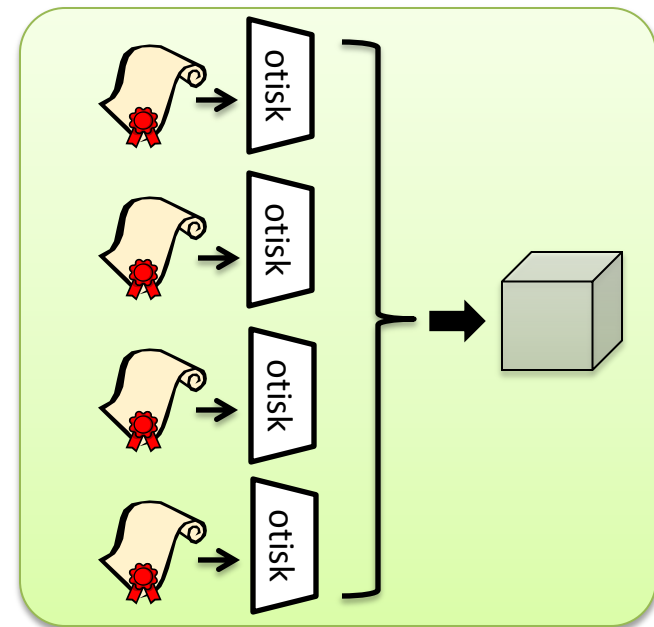
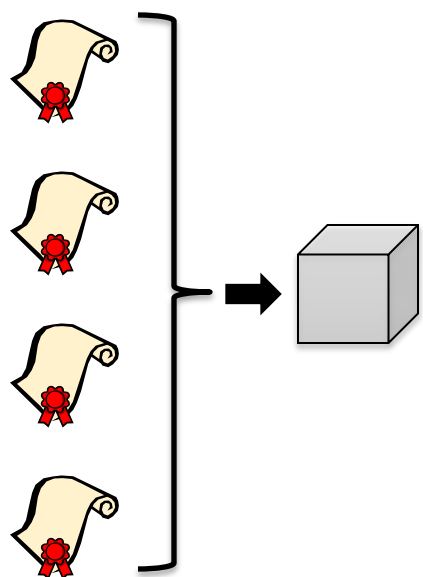
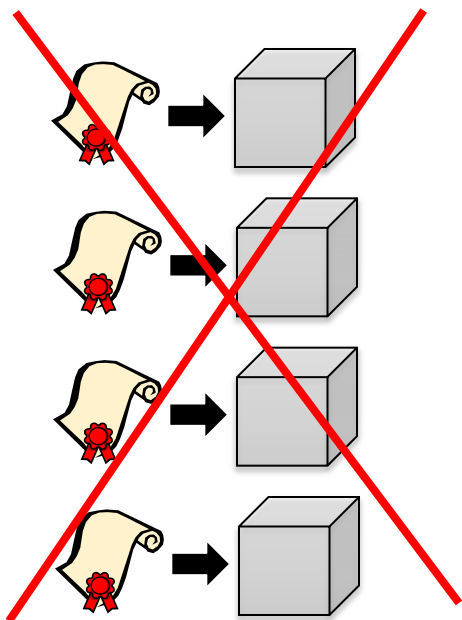
postupné „přerazítkování“

- 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



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
0D0A
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
0D0A
5620
5072
617A
652C
204C
5032
3031
3020
4A69
7269
2050
6574
6572
6B61
14

problém s autorizovanou konverzí

- přerazítkovávání musí podporovat mechanismy autorizované konverze
 - dnešní Czechpointy to nedělají !!!!!
 - proto: ani přerazítkovávání (dnes, v běžné praxi) nepomůže !!!!!
 - CzechPointy neberou v úvahu / nedokáží pracovat s:
 - externími časovými razítky
 - archivními razítky na PDF dokumentech
 - časovými razítky na „kontejnerech“ PDF dokumentů
 - včetně časových razítek na datových zprávách

platnost lze
ověřit ještě
do června
2012

MV ČR radí: uchovávejte si celé datové zprávy a místo dokumentů předkládejte celé datové zprávy

CzechPointy se podle této rady nechovají: když přijdete s dokumentem uvnitř datové zprávy, nebude vám to nic platné !!!!
(při ověřování podpisu na dokumentu CzechPoint nebude brát v úvahu časové razítko na datové zprávě)

jiný způsob zajištění „dlohověkosti“

- 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 dávalo dokumentu potřebný statut



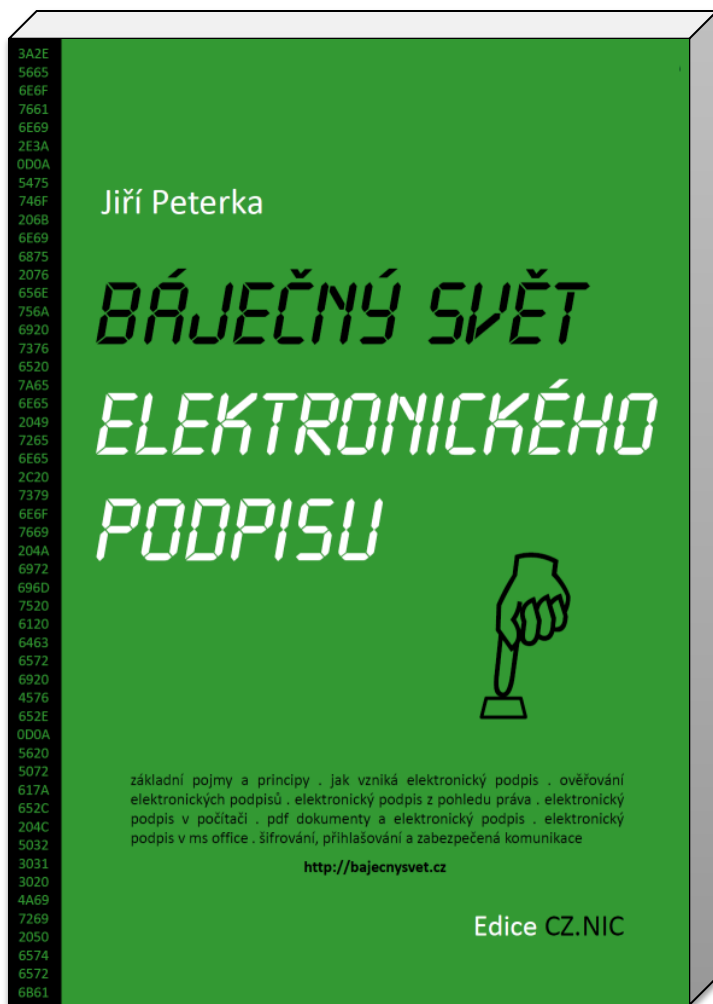
alternativní názorový proud

- 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 potřebujeme zpochybnění („dokud se neprokáže opak“)
 - nejsme-li již schopni prokázat platnost podpisu, pak domněnku nemůžeme aplikovat
 - nejsou splněny její předpoklady

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



Jiří Peterka

jiri@peterka.cz

<http://jiri.peterka.cz>

<http://earchiv.cz>

<http://bajecnysvet.cz>

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

tuto přednášku najdete v mém archivu
(earchiv.cz)