



Elektronický podpis

Smilovice 4. 4. 2019

Ing. Karel Janeček, MF odbor 70,
Strategické řízení rozvoje ICT resortu a kybernetická bezpečnost



Úvod

Osnova prezentace

- 1. eIDAS**
- 2. Některé pojmy a souvislosti**
- 3. Tvorba elektronických podpisů**
- 4. Jak probíhá ověřování elektronických podpisů**
- 5. Elektronický podpis ŘD PDF EDS/SMVS**

1. eIDAS

Dne 19.9.2016 nabyl účinnosti zákon č. [297/2016](#) Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „Zákon“), který spolu se změnovým zákonem č. [298/2016](#) Sb. zrušil původní zákon č. [227/2000](#) Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů. Český zákonodárce tak reagoval na nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23.7.2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, účinné zčásti ode dne 17.9.2014 a z části ode dne 1.7.2016 (dále jen „eIDAS“).

1. eIDAS

Nejvyšší formou elektronického podpisu **kvalifikovaný elektronický podpis** (§ 5 Zákona). Tuto formu musí používat vyjmenované orgány veřejné moci (dále jen „veřejnoprávní podepisující“) a jiné fyzické či právnické osoby při výkonu působnosti v oblasti veřejné správy, podepisují-li elektronický dokument, kterým právně jednají.

Díky přechodnému ustanovení (§ 19 odst. 1 Zákona) se ustanovení používá až ode dne **19.9.2018**.

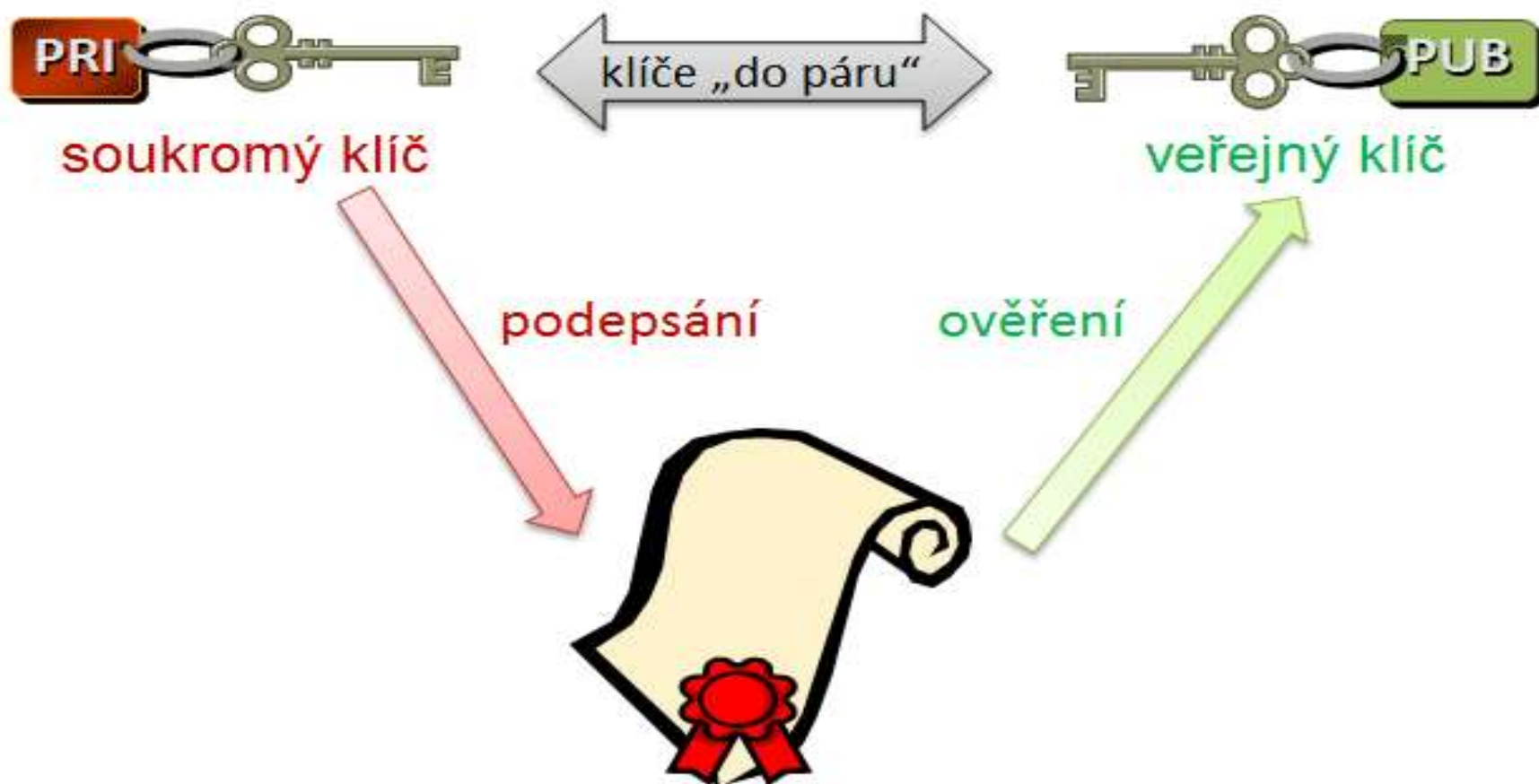


2. Některé pojmy a souvislosti

- Dokument a zpráva, písemná, listinná, elektronická
- Podpis, elektronický a digitální podpis (4-5)
- Uznávaný a kvalifikovaný el. podpis
- Integrita, identifikace, nepopiratelnost
- Důvěrnost, autorizace, autenticita
- Kvalifikovaná elektronická pečeť a časové razítko

2. Některé pojmy a souvislosti

- Klíče a asymetrická kryptografie



2. Některé pojmy a souvislosti

- Certifikáty a certifikační authority, struktura



- Biometrie

2. Některé pojmy a souvislosti

- osobní certifikát

Certifikát

Obecné Podrobnosti Cesta k certifikátu

 **Informace o certifikátu**

Tento certifikát je určen k následujícímu účelu:

- 2.23.134.1.4.1.7.110
- Všechny zásady použití

* Podrobnosti naleznete v prohlášení certifikační autority.

Vystaveno pro: 

Vystavitel: PostSignum Qualified CA

Platnost od 15. 1. 2010 **do** 15. 1. 2011

 Máte privátní klíč, jenž odpovídá tomuto certifikátu.

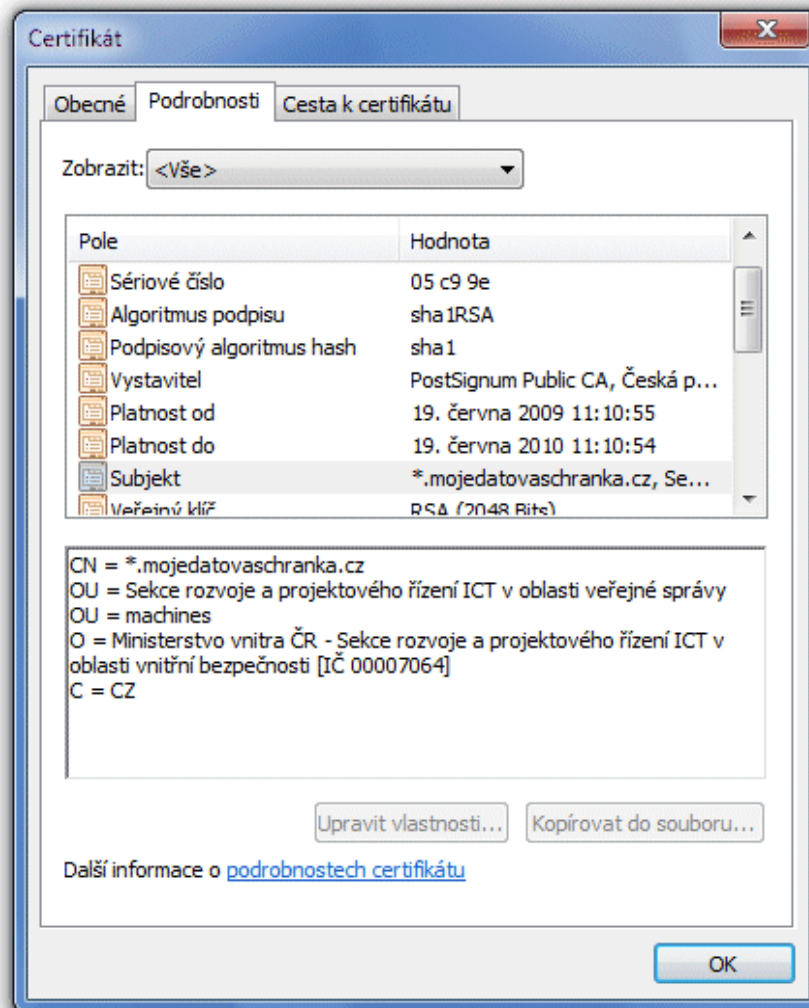
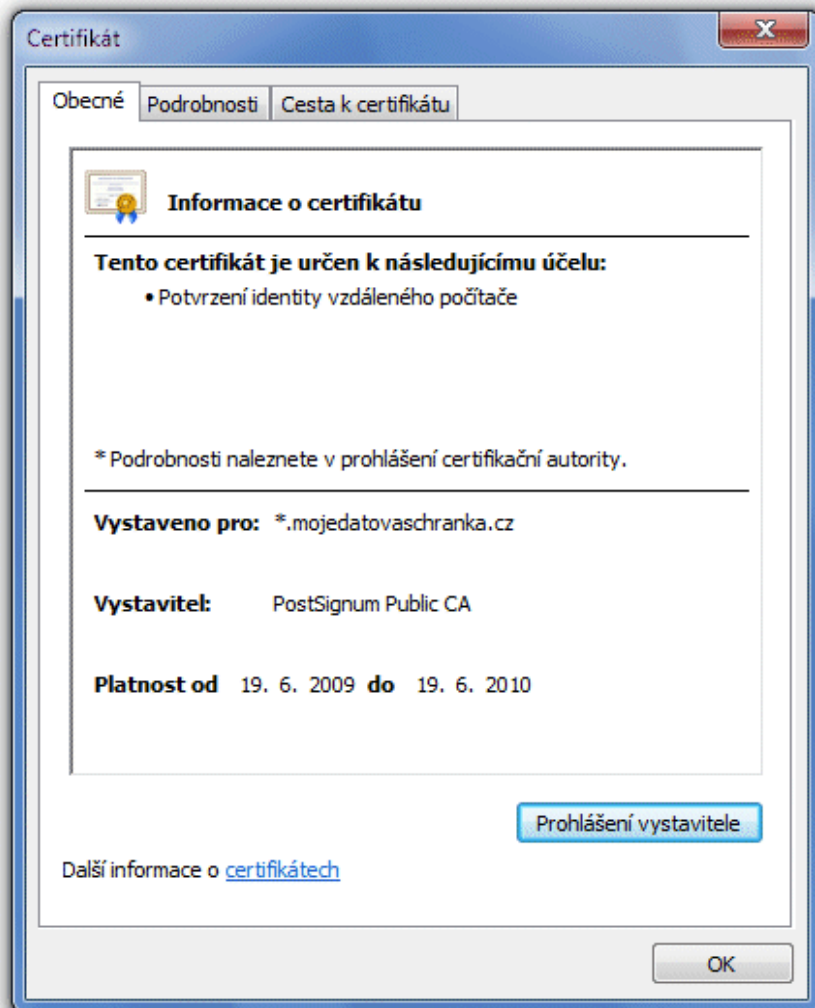
[Prohlášení vystavitele](#)

Další informace o [certifikátech](#)

OK

2. Některé pojmy a souvislosti

- systémový certifikát





2. Některé pojmy a souvislosti

• komerční a kvalifikovaný certifikát



Certifikát

Obecné Podrobnosti Cesta k certifikátu



Informace o certifikátu

Tento certifikát je určen k následujícímu účelu:

- Ochrana e-mailů
- 1.3.6.1.4.1.23624.10.1.30.1.1
- 0.4.0.194112.1.2

* Podrobnosti naleznete v prohlášení certifikační autority.

Vystaveno pro:

Vystavitel:

I.CA Qualified 2 CA/RSA 02/2016

Platnost od 18.09.2018 do 18.09.2019

Nainstalovat certifikát...

Prohlášení vystavitele

Zřeknutí se práv

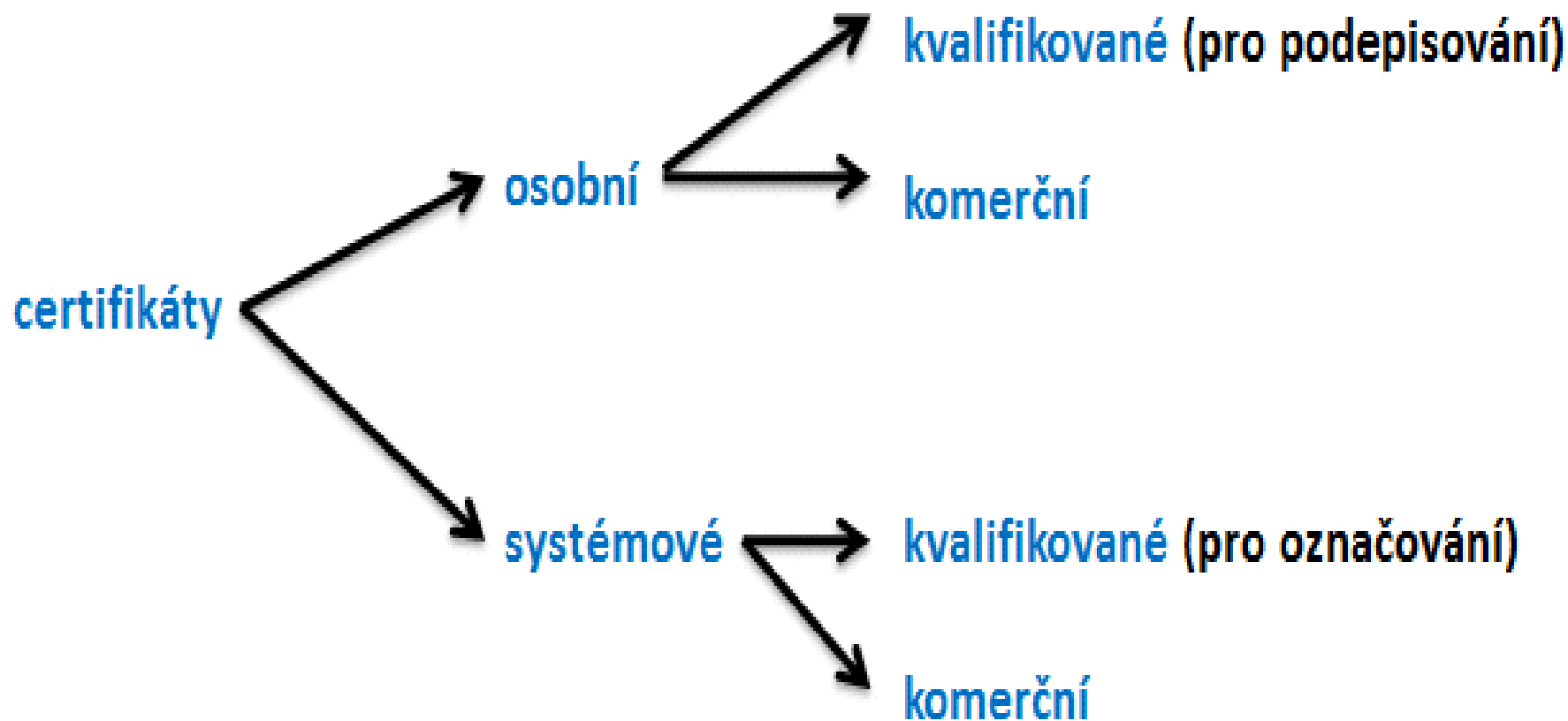
Tento kvalifikovaný certifikát pro elektronický podpis byl vydán v souladu s nařízením EU č. 910/2014. This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.

Zavřít

Další informace

2. Některé pojmy a souvislosti

- shrnutí certifikátů





2. Některé pojmy a souvislosti

- certifikační authority – akreditace MV ČR

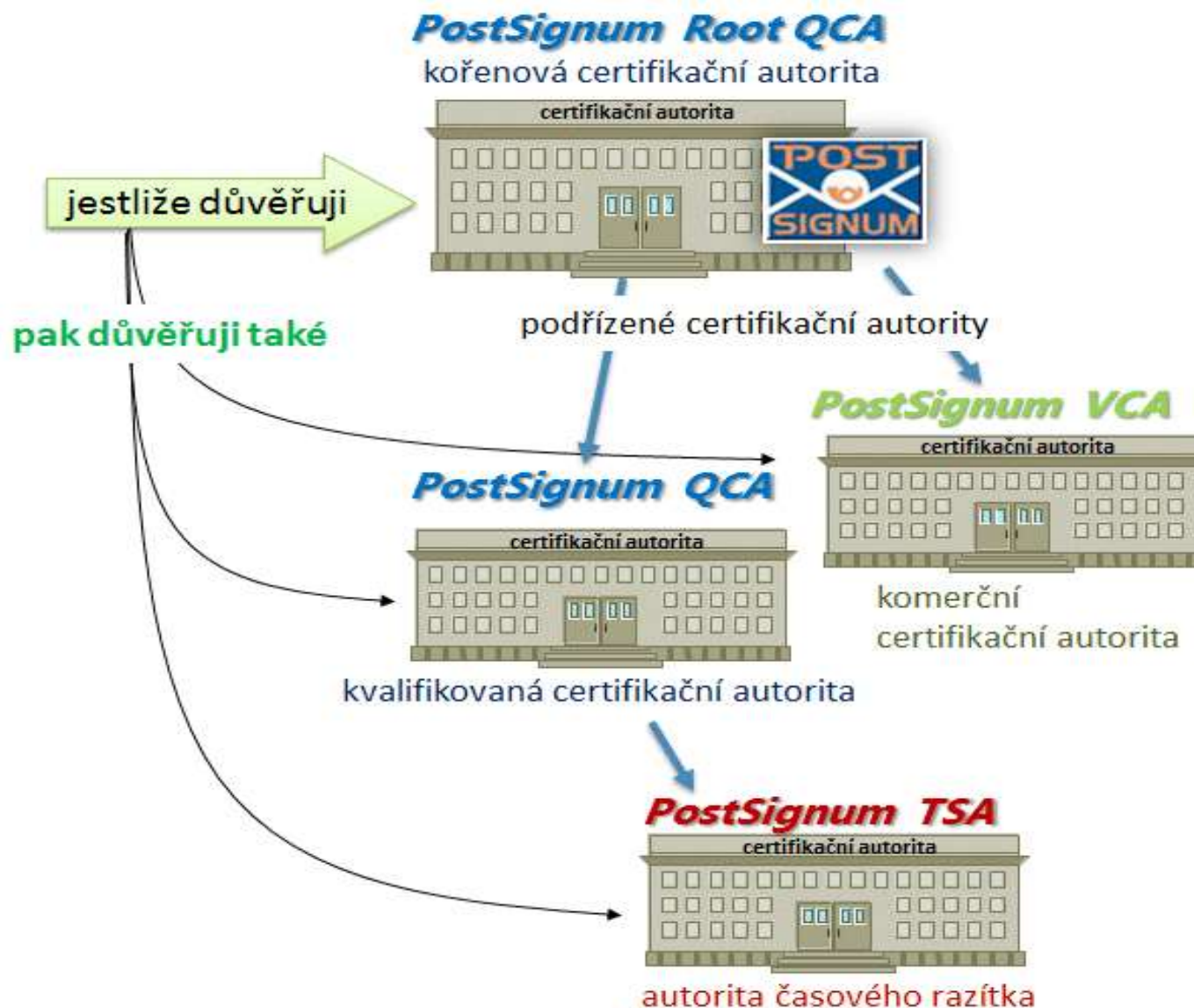
1. První certifikační autorita, a. s.,
identifikační číslo 26 43 93 95,
Podvinný mlýn 2178/6,
PSČ 190 00 Praha 9

2. Česká pošta, s. p.
identifikační číslo 47 11 49 83,
Olšanská 38/9,
PSČ 225 99 Praha 3

3. elidentity a. s.,
identifikační číslo 27 11 24 89,
Vinohradská 184/2396,
PSČ 130 00 Praha 3

2. Některé pojmy a souvislosti

- CA PS
strom
důvěry



2. Některé pojmy a souvislosti

- Elektronický podpis – číslo resp. řetězec

IQB1AwUBMVSIA5QYCuMfgNYjAQFAKgL/ZkBfbeNEsbthba4BlrcnjaqbcKgNv+a5kr4537y8RCd+RHm75yYh5xxA1o
jELwNhhb7cltrp2V7LlOnAelws4S87UX80cLBtBcN6AACf11qymC2h+Rb2j5SU+rmXWru+=QFMx



2. Některé pojmy a souvislosti

- kód je nesrozumitelný; v praxi pracuje člověk s el. podpisem jinak, ale programy s ním pracují v původní formě čísla
- programy el. podpis ověřují a výsledek zobrazí pro nás v příjemnější formě.

2. Některé pojmy a souvislosti

- Elektronický podpis – příklad výsledku ověření v programu Acrobat Readeru

Přehled

Podrobnosti

Odvolání

Důvěryhodnost

Zásady

Právní upozornění



Ing. Karel Janeček <Karel.Janecek@mfcz.cz>

MFCR

Vydal(a): Ministerstvo financí - CA Urad 2013-01

MFCR

Platný od: 2019/02/25 11:45:00 +01'00'

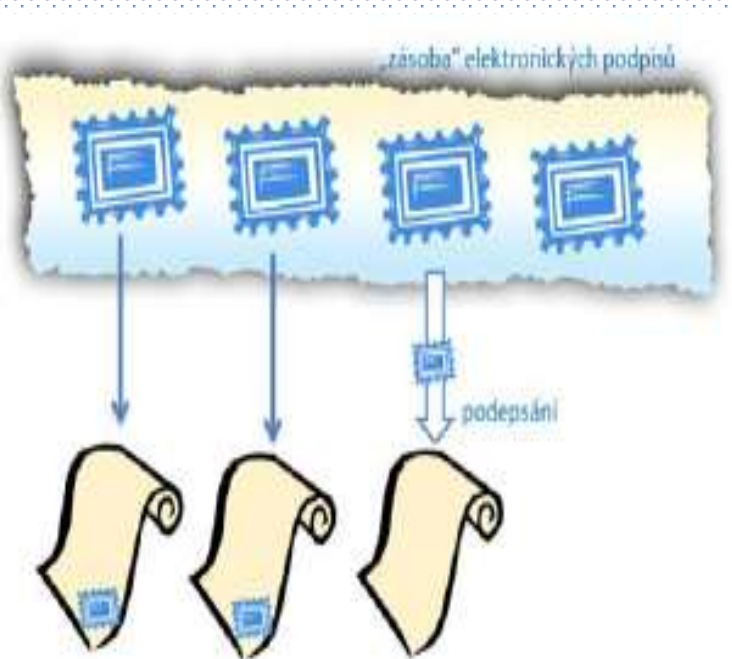
Platný do: 2021/02/24 11:45:00 +01'00'

Zamýšlené použití:

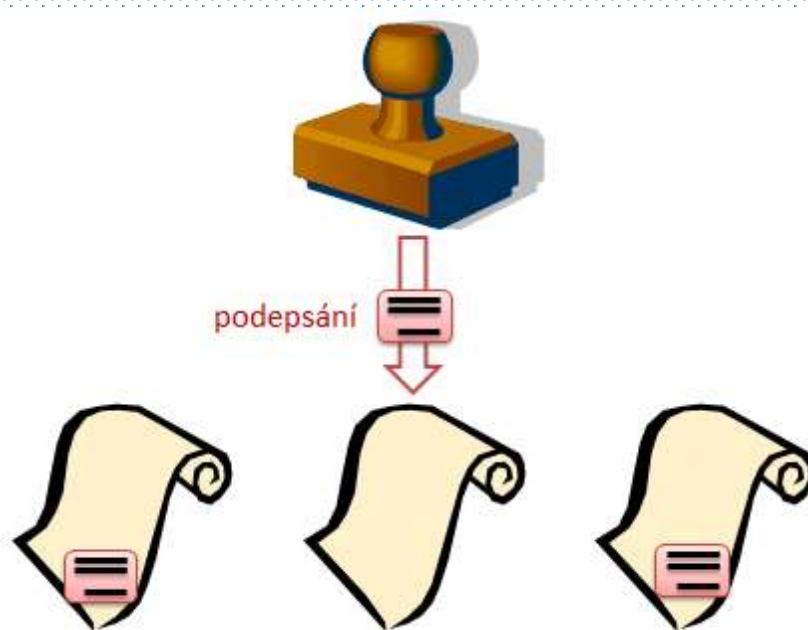
Digitální podpis, Neodvolatelnost, Ochrana e-mailu

3. Vytváření elektronických podpisů

známka

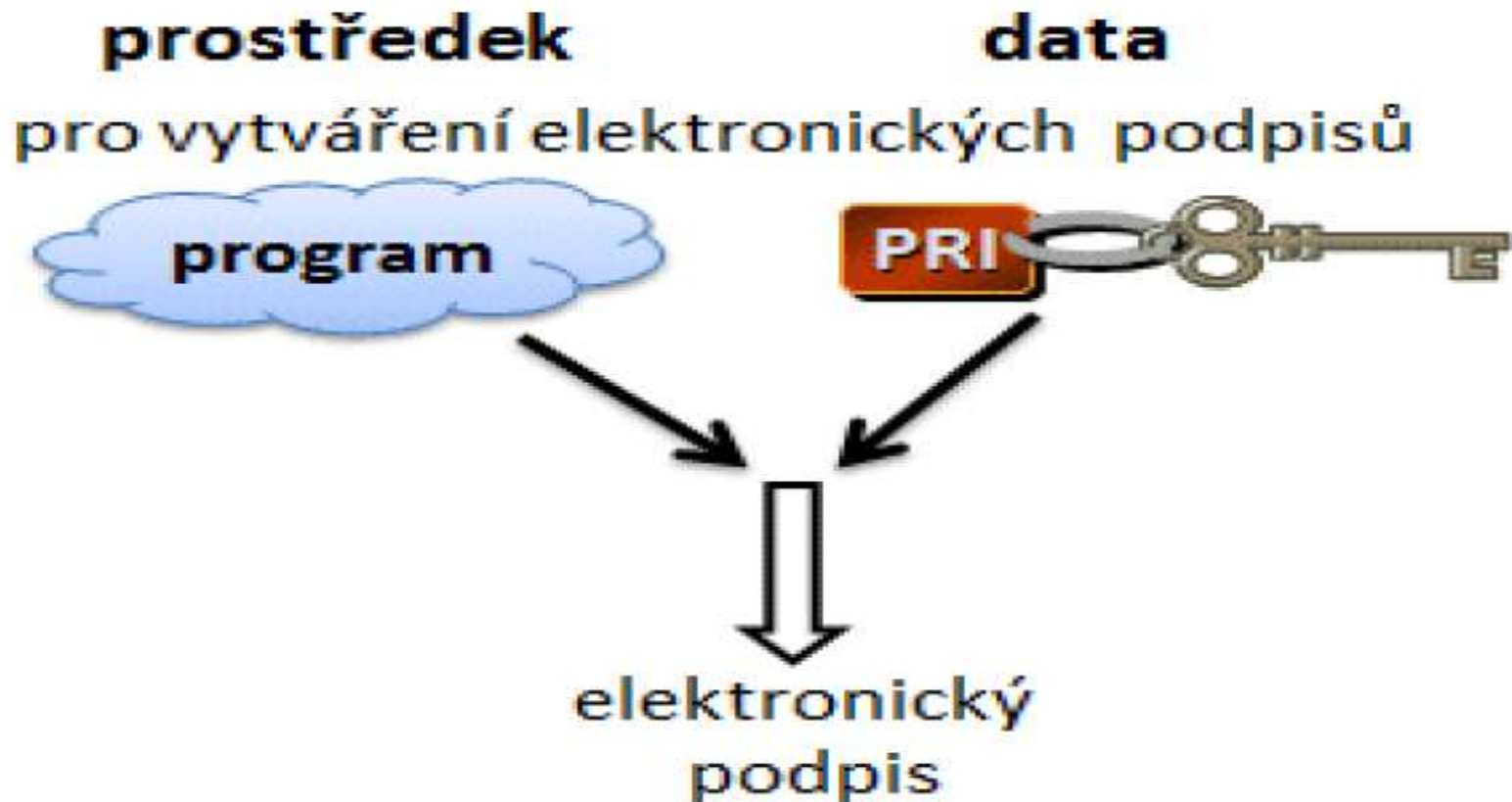


kulaté razítko



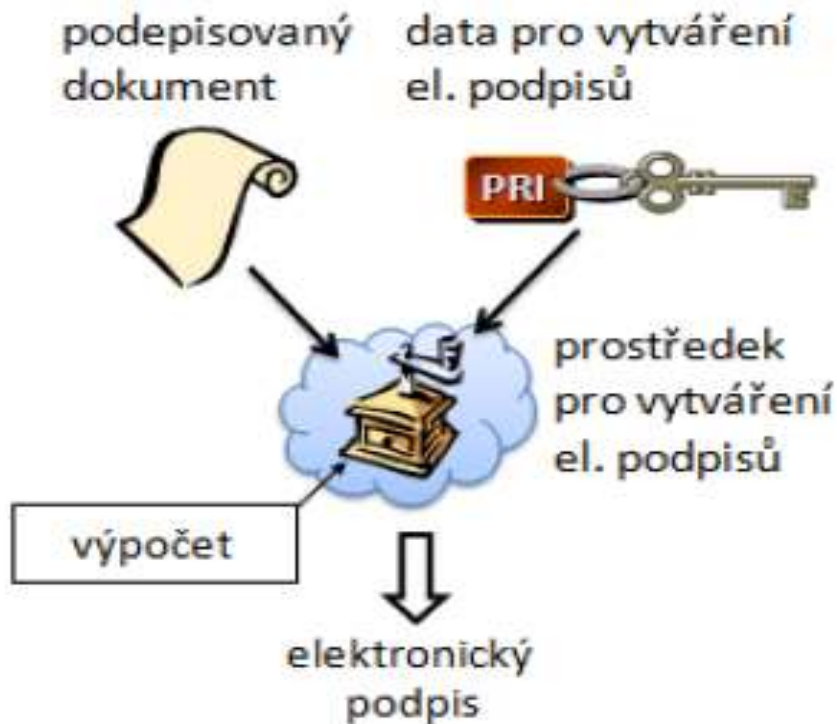
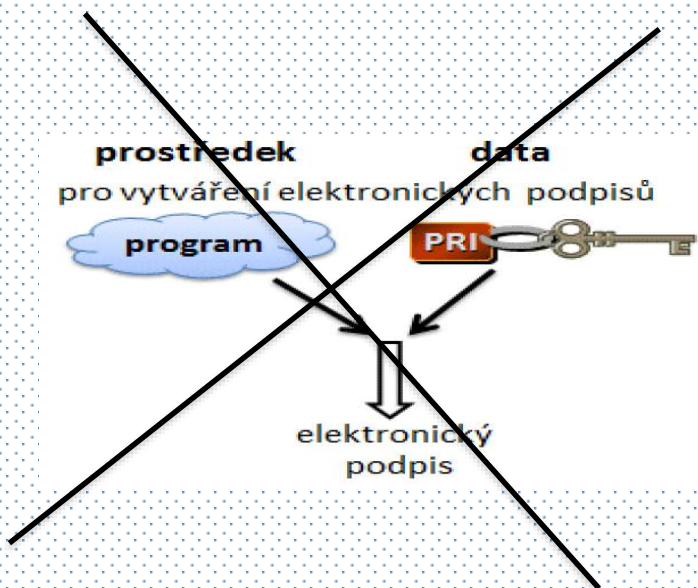
3. Vytváření elektronických podpisů

- soukromý a veřejný klíč



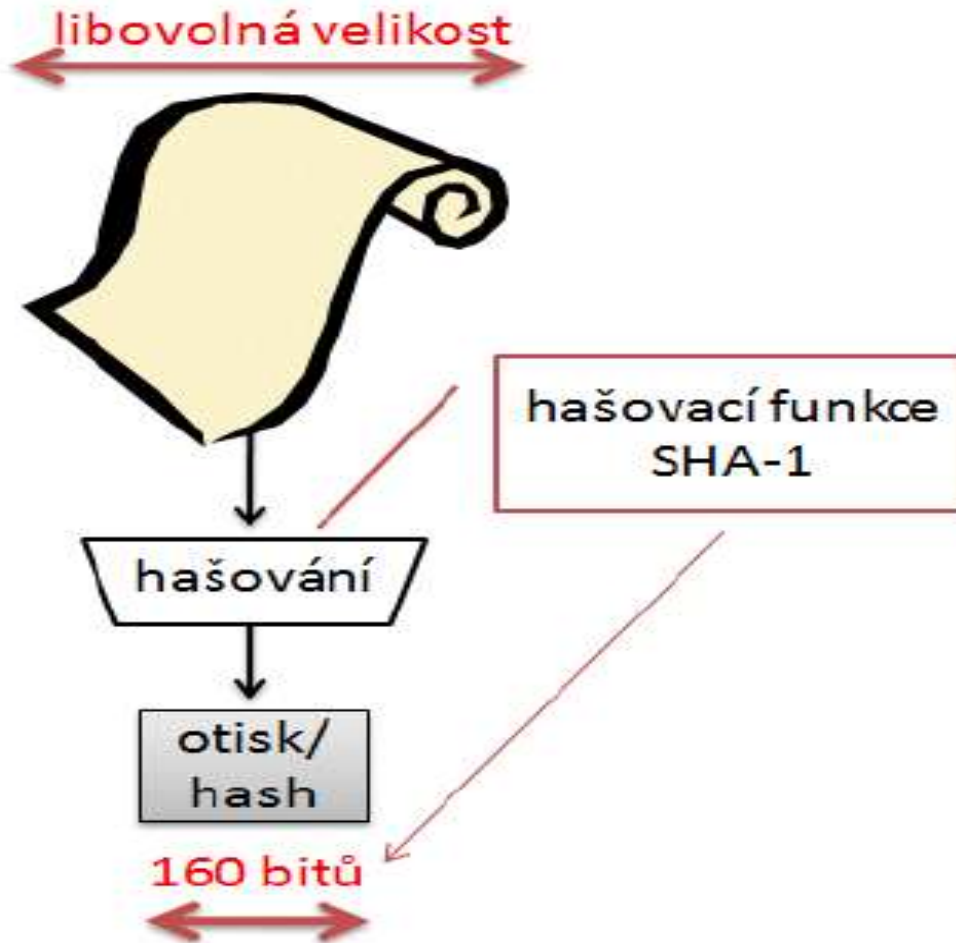
3. Vytváření elektronických podpisů

- Závislost el. podpisu na podepisovaném dokumentu



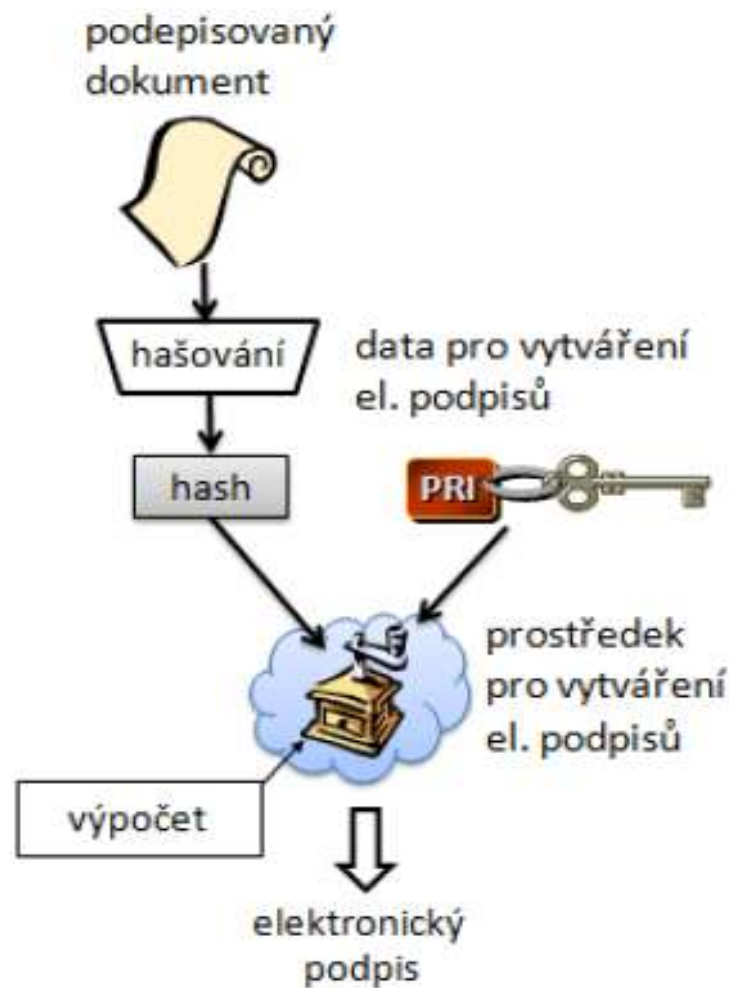
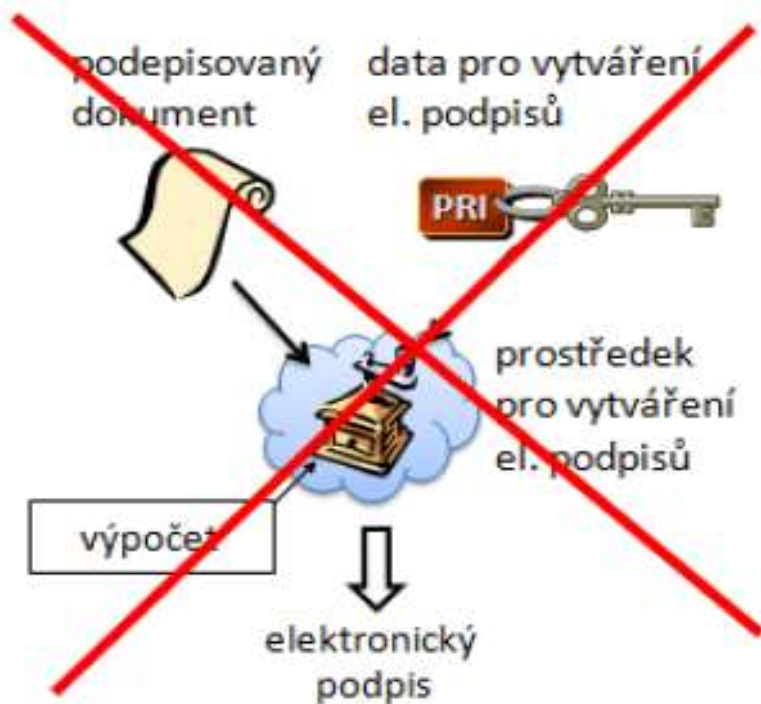
3. Vytváření elektronických podpisů

- Hashing
hašování



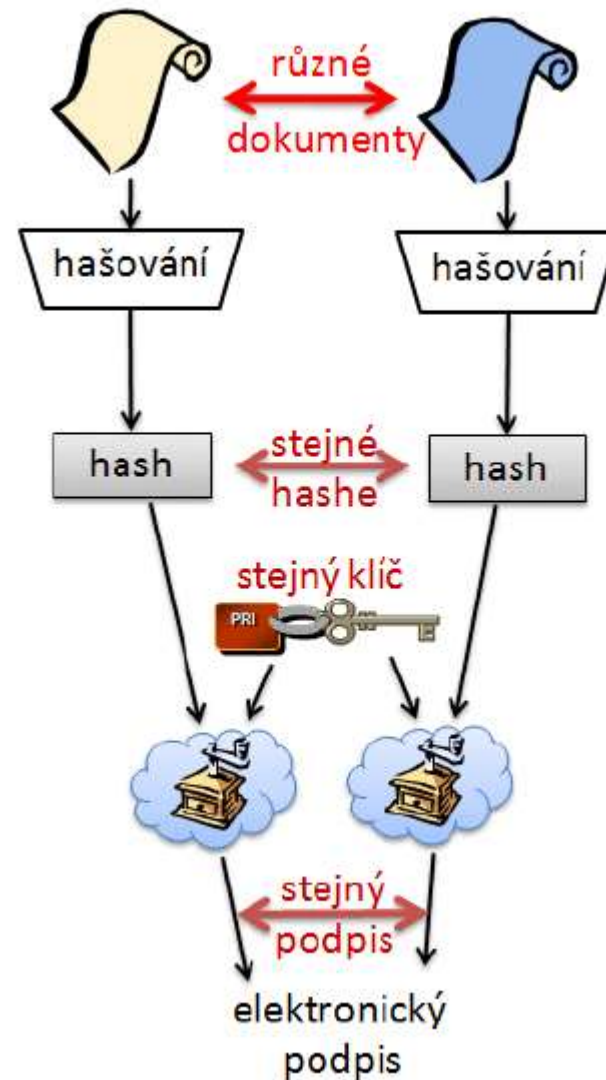
3. Vytváření elektronických podpisů

- zapojení HASH při vytváření el.podpisu



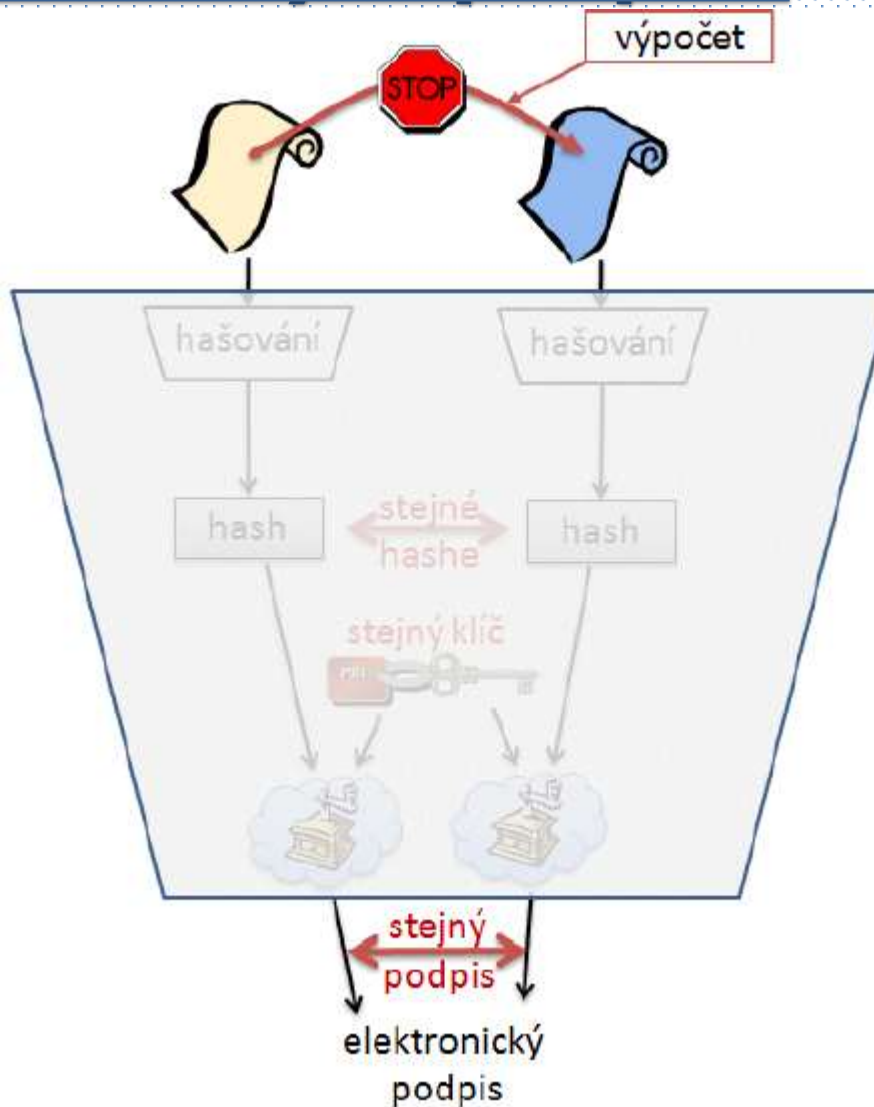
3. Vytváření elektronických podpisů

- kolizní dokumenty



3. Vytváření elektronických podpisů

- nemožnost výpočtu kolizního dokumentu

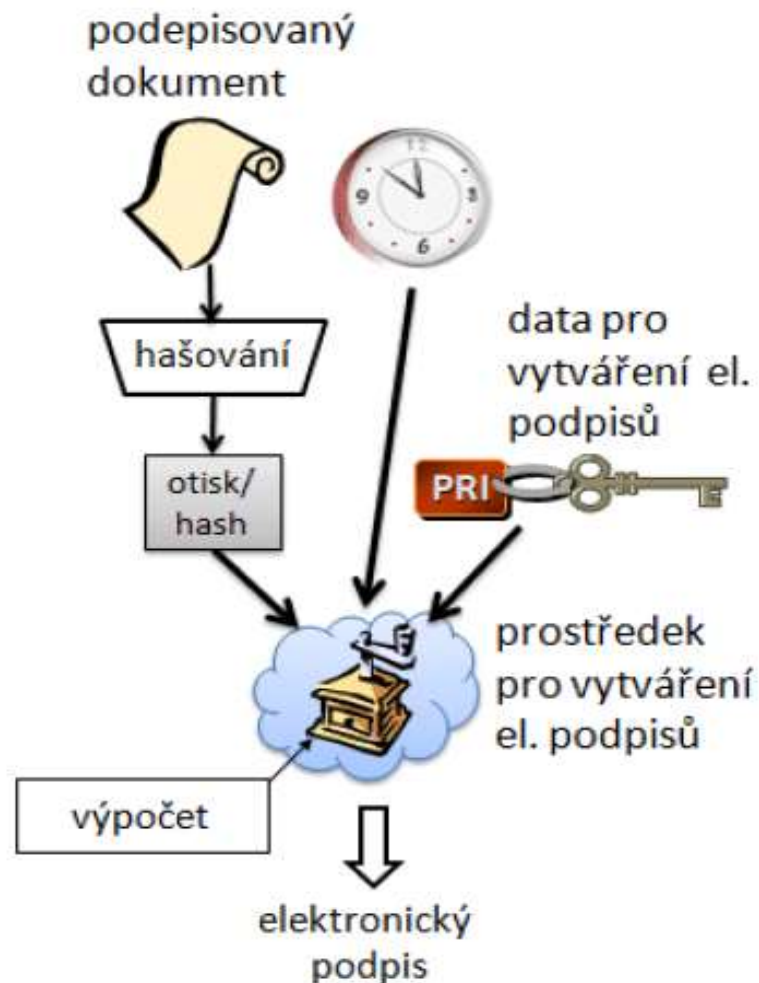
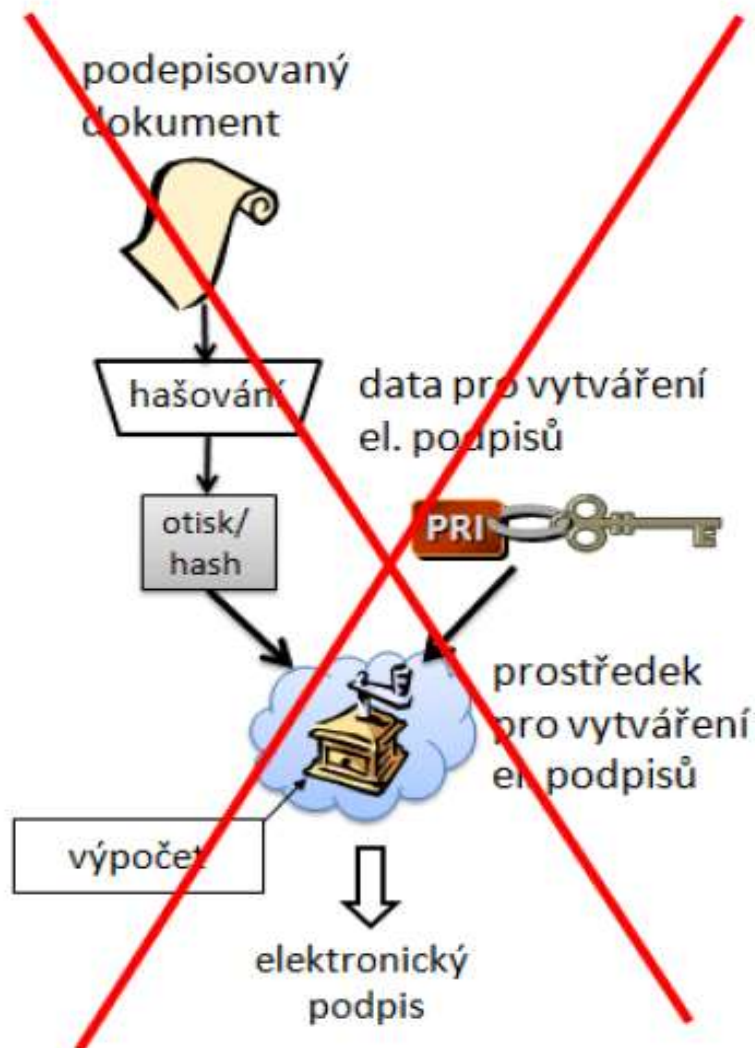




3. Vytváření elektronických podpisů

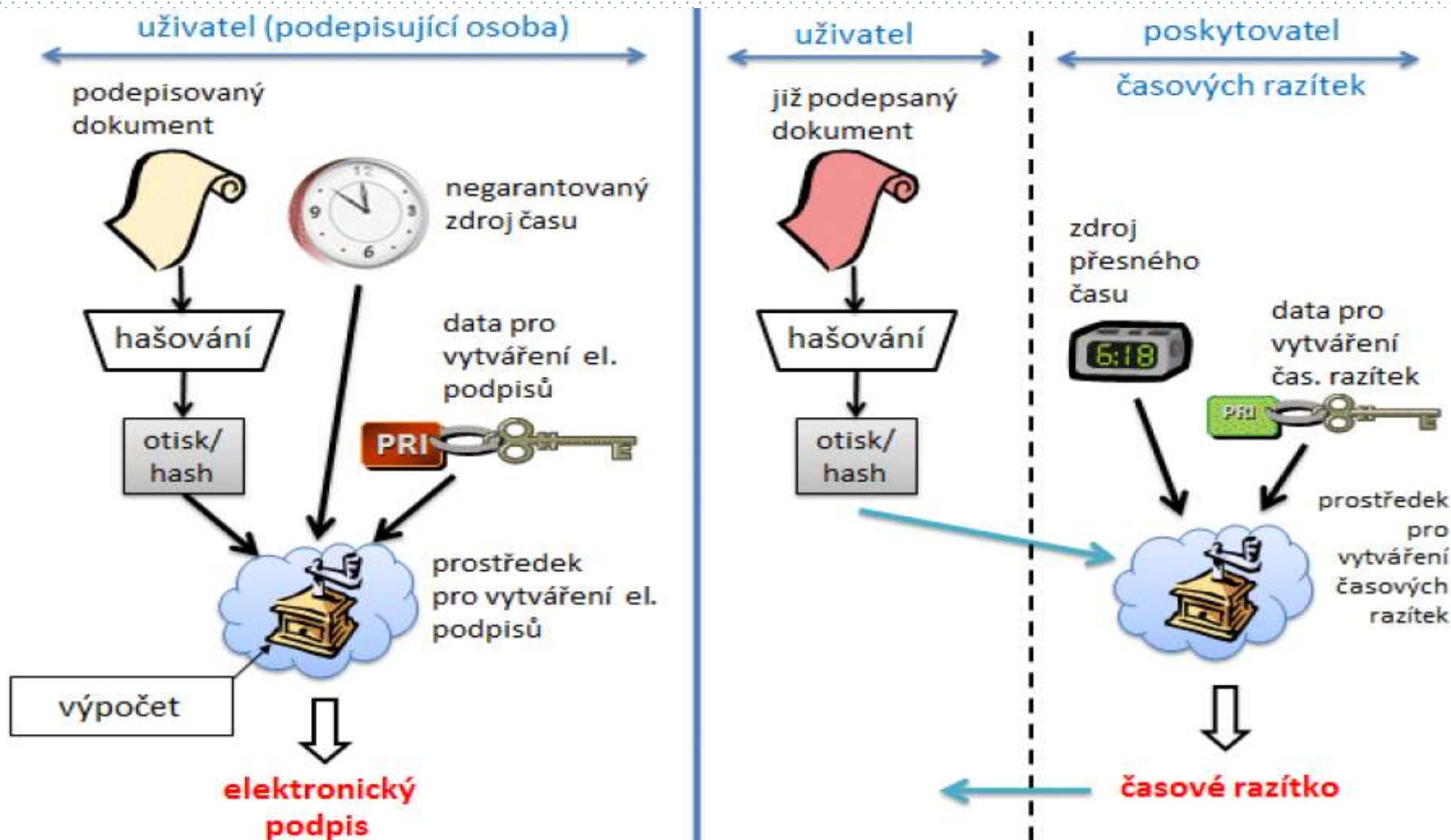
- časové omezení el. podpisu
- doba vzniku el. podpisu

3. Vytváření elektronických podpisů



3. Vytváření elektronických podpisů

- časové razítko



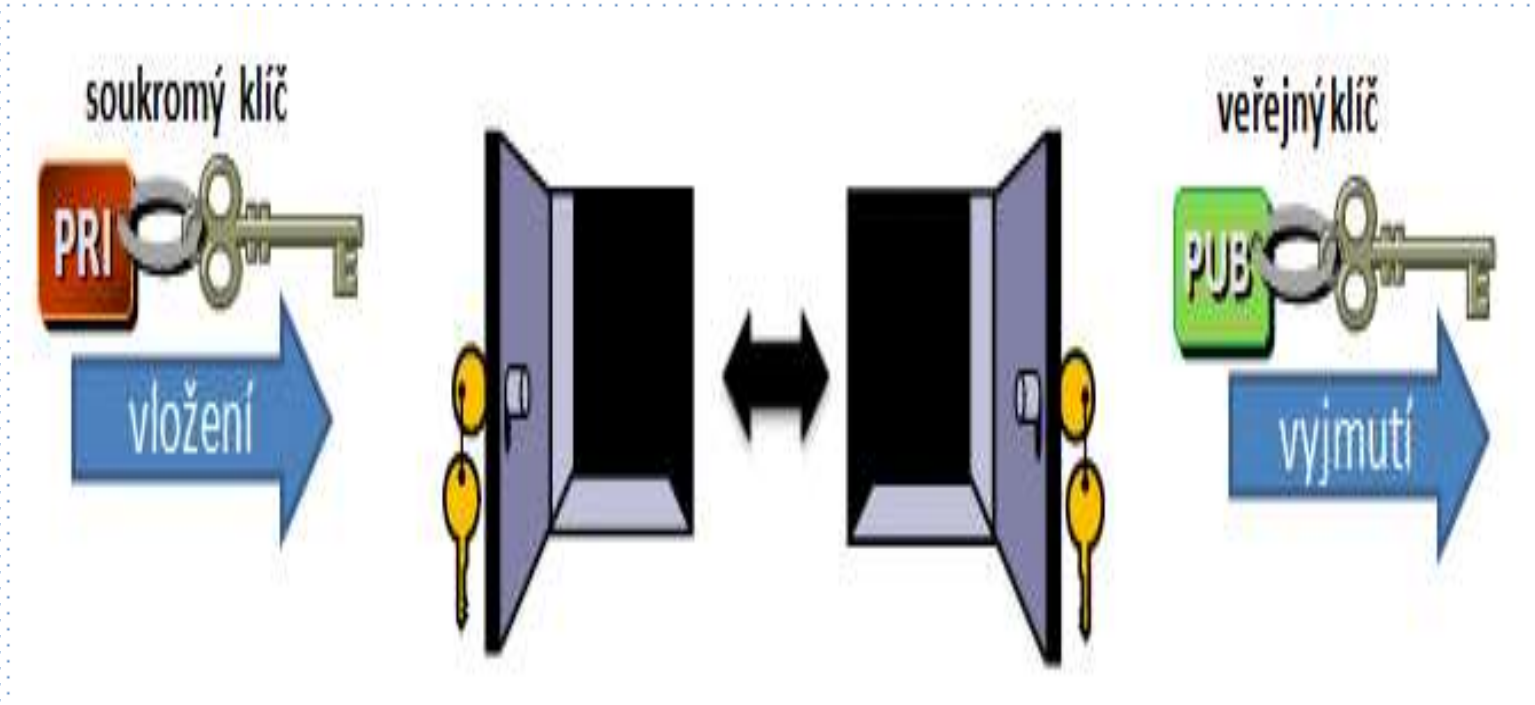
4. Ověřování elektronických podpisů

Výsledek ověření platnosti el.podpisu:

1. zjištěním, že elektronický podpis je **platný**:
jsme schopni ověřit a prokázat platnost podpisu.
2. zjištěním, že elektronický podpis je **neplatný**:
jsme schopni ověřit a prokázat neplatnost podpisu.
3. zjištěním, že „**nevíme**“ (že platnost podpisu nedokážeme posoudit, že nejsme schopni ověřit, zda podpis je či není platný).

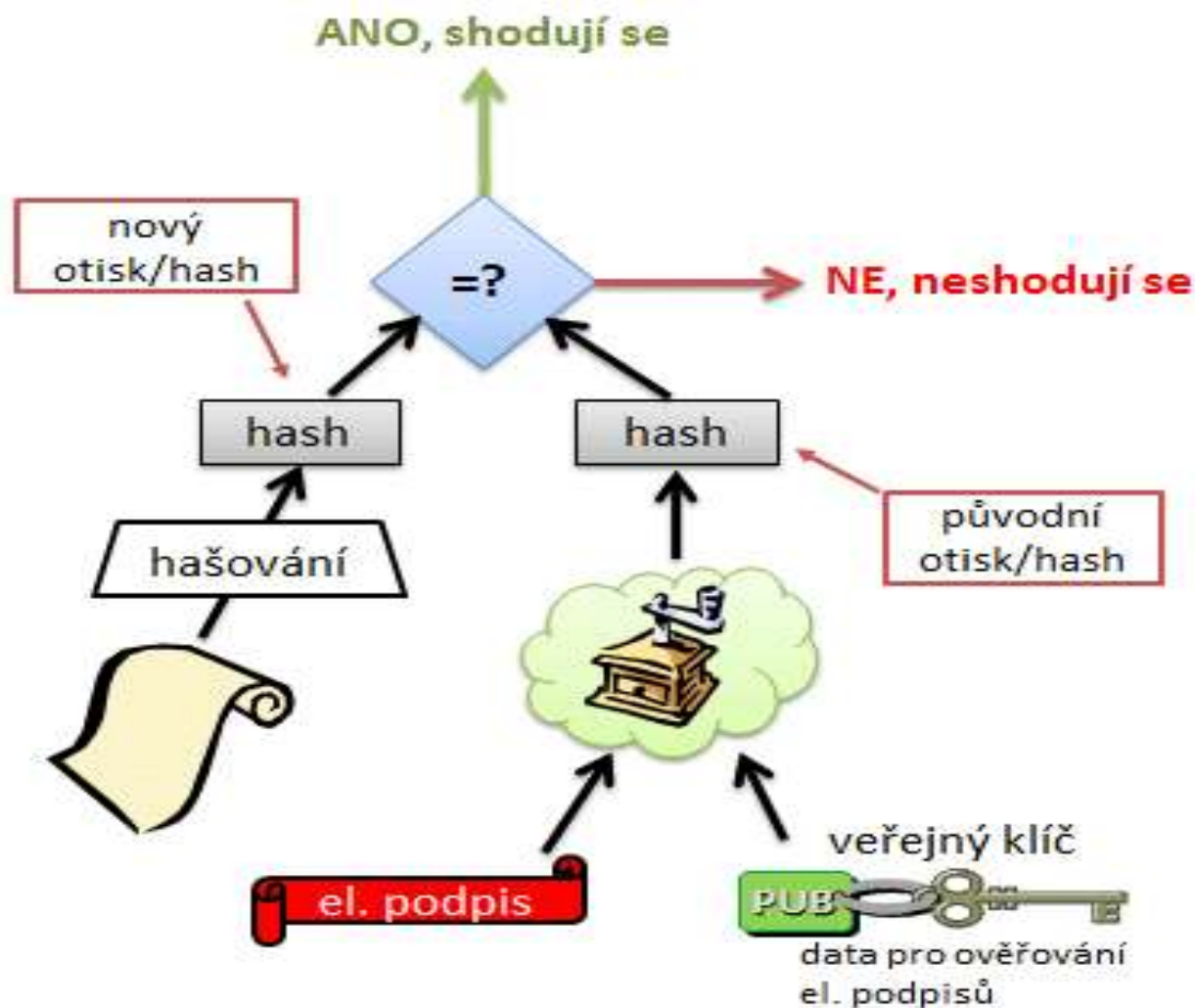
4. Ověřování elektronických podpisů

- **skříňka**



4. Ověřování elektronických podpisů

- hašování



4. Ověřování elektronických podpisů

- **posuzovaný okamžik**
 - posuzovat platnost podpisu k okamžiku jeho vzniku, ale takovému okamžiku nelze věřit (čas z PC)
 - posuzovat k jinému okamžiku – díky časovému razítku, resp. po něm, kdy víme, že podpis někdy platný byl (před čas.razítkem)
 - pozdější ověření má riziko z plynoucího času

5. Elektronický podpis ŘD EDS/SMVS

- **EDS/SMVS je agentovým systémem**
- **není však prostředkem pro vedení samostatné evidence spisů, nepřiděluje, nespravuje čj.**
- **po vyplnění formuláře přidáváme čj. ze spisové služby**
- **vytvoříme PDF**
- **vložíme do spisové služby, např. do podpisové knihy a zajistíme, aby podepisující osoba připojila kvalifikovaný el. podpis – jedná se o právní úkon**
- **čj. je odesláno adresátovi spisovou sl.**



Přeji vám příjemný zbytek dne

Ing. Karel Janeček, MF odbor 70,
Strategické řízení rozvoje ICT resortu a kybernetická bezpečnost
zdroje: internet, kniha Báječný svět elektronického podpisu (Jiří Peterka)