

# Elektronický obchod

Jan Doubek, MBA

Prezentaci připravili: Ing. Petr Budiš, Ph.D. a Jan Doubek, MBA

# Důležité termíny

- Písemná a ústní zkouška z předmětu  
Elektronické obchodování

1. termín - 16. prosince 2013    16:30 písemný test  
17:00 a dále ústní zkouška - 12 studentů

2. termín - 17. prosince 2013    8:30 písemný test  
9.00 a dále ústní zkouška - 12 studentů  
12:30 písemný test  
13:00 a dále ústní zkouška - 12 studentů

3. termín bude určen dodatečně - leden 2014

# Co bychom měli vědět až dnes skončíme?

- Právní rámec elektronického obchodování
  - Jaká je problematika šíření obchodních sdělení
  - Co je to smlouva uzavíraná na dálku, distanční smlouva a právní rámec ochrany spotřebitele,
- Základní pojmy spojené s používáním elektronického podpisu v elektronickém obchodu a elektronickém bankovníctví,
  - kryptografické principy e-podpisu
  - certifikáty veřejného klíče a typy e-podpisu
  - životní cyklus certifikátu
  - legislativní základ e-podpisu

# Co bychom měli vědět až dnes skončíme?

- Symetrická a asymetrická kryptografie, principy, použití, výhody
  - schéma využití kryptografických funkcí pro zajištění důvěrnosti, integrity a autenticity elektronických dokumentů,
- Časové razítko, účel a principy
  - co je časové razítko, k čemu slouží
  - časové razítko v legislativě
  - využití časového razítka v e-obchodu a e-bankovníctví





# Právní rámec oblasti elektronického obchodování

# Právní úprava elektronického obchodu

- V některých případech lze stávající právní úpravu bez dalšího aplikovat na e-obchod (např. ochrana autorského práva).
- Jiné stávající právní normy dostaly aplikací na právní vztahy vznikající v rámci e-obchodu zcela nový rozměr (např. určení rozhodného práva).
- V neposlední řadě si e-obchod vynutil přijetí i zcela nových právních norem (např. právní úprava elektronického podpisu).

# Základní právní normy spojené s elektronickým obchodem

- zákon č. 480/2004 Sb., o některých službách informační společnosti
- zákon č. 227/2000 Sb., o elektronickém podpisu
- Občanský zákoník (úpravou spotřebitelských smluv prostřednictvím elektronických prostředků)
- Občanský soudní řád (úpravou elektronického podání, doručování a elektronického platebního rozkazu)
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který upravuje elektronické úkony státních orgánů, orgánů územních samosprávných celků, Pozemkového fondu České republiky a jiných státních fondů, zdravotních pojišťoven, Českého rozhlasu, České televize, samosprávných komor zřízených zákonem, notářů a soudních exekutorů (orgán veřejné moci) vůči fyzickým osobám a právnickým osobám, elektronické úkony fyzických osob a právnických osob vůči orgánům veřejné moci a elektronické úkony mezi orgány veřejné moci navzájem prostřednictvím datových schránek.

# Zákon o některých službách informační společnosti

- **Službou informační společnosti** se rozumí jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu;  
služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat.
- **Elektronickou poštou** je textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.
- **Elektronickými prostředky** jsou zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová telekomunikační zařízení a elektronická pošta.



# Zákon o některých službách informační společnosti

- **Poskytovatelem služby** je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti.
- **Uživatel** je každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací.
- **Obchodním sdělením** jsou všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama.

**Za obchodní sdělení se nepovažují** údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle.

- je

# Odpovědnost poskytovatelů zprostředkovatelských služeb

- Do účinnosti zákona č. 480/2004 Sb., byla oblast odpovědnosti poskytovatele pouze otázkou dohody mezi poskytovatelem služeb a jejich uživatelem.
- ***Zákon o některých službách informační společnosti stanovil podmínky***, za kterých je poskytovatel služby odpovědný za obsah jím přenesených či uložených informací a za šíření obchodních sdělení elektronickými prostředky.
- Poskytovatelé služeb však ***nejsou povinni***
  - dohlížet na obsah jimi přenášených nebo ukládaných informací,
  - aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.

## Odpovědnost poskytovatele služby za obsah přenášených informací

- Zákon o některých službách informační společnosti stanovuje případy, kdy jsou poskytovatelé služeb za to, že umožní uživatelům připojit se k síti odpovědni za obsah jimi přenášených informací.
- Uživatelé v některých případech na síti činí některé protiprávní kroky, jako jsou např. propagace nacismu, šíření dětské pornografie nebo šíření nelegálního software. Poskytovatelé pouze přenášejí informace, a zásadně není proto možné požadovat, aby sledovali obsah a navíc za něj ještě nesli zodpovědnost.
- Poskytovatel služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí odpovídá za obsah přenášených informací, jen pokud:
  - přenos sám iniciuje,
  - zvolí uživatele přenášené informace, nebo
  - zvolí nebo změní obsah přenášené informace.

# Odpovědnost poskytovatele služby za ukládání obsahu

- Poskytovatelé služeb umožňují svým uživatelům, aby uložili svá data na servery poskytovatele. Poskytují jim k tomu prostor na základě smlouvy o uložení informací či dat.
- Není rozumné požadovat od poskytovatelů, aby při vysokém počtu uživatelů a vysokém objemu uložených dat zjišťovali a posuzovali legálnost či nelegálnost veškerého obsahu uložených informací. Je věcí a odpovědností samotných uživatelů, jaký obsah ukládají na poskytnutém serverovém prostoru.
- Poskytovatelé nemají povinnost aktivně monitorovat materiály, které jsou na jejich serverech uloženy.

# Odpovědnost poskytovatele služby za ukládání obsahu

- ***Pokud se však poskytovatel dozví o protiprávní povaze obsahu, a neučiní veškeré možné kroky*** vedoucí k odstranění či znepřístupnění takového obsahu, které po něm lze požadovat, stává se odpovědným za obsah uložených informací.
- Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen
  - mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo
  - dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.



# Šíření obchodních sdělení

- Zákon stanovuje pravidla pro šíření obchodních sdělení zejména pro případy šíření nevyžádaných obchodních sdělení.
- **Zakazuje se šíření nevyžádaných obchodních sdělení za použití elektronických prostředků.** Tímto se umožňuje šíření obchodních sdělení pouze tzv. systémem opt-in, tedy šíření vyžádaných obchodních sdělení.
- Dále se stanovuje povinnost subjektů získávajících od svých zákazníků kontakty pro elektronickou poštu získat souhlas pro šíření obchodních sdělení a povinnost umožnit zákazníkům zdarma odmítnout souhlas s využitím této adresy k zasílání obchodních sdělení kdykoliv při zasílání zprávy.
- Zároveň je zakázáno šířit obchodní sdělení elektronickou poštou, pokud není zřetelně a jasně označena jako obchodní sdělení, skrývá nebo utajuje totožnost odesílatele, nebo je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat žádost na vyřazení z příslušného opt-in seznamu.

# Šíření obchodních sdělení

- Ochrany požívají jak osoby fyzické, tak i osoby právnické. (Nelze tedy zasílat nevyžádaná obchodní sdělení ani na emailové adresy, jež nejsou přiřazeny konkrétní fyzické osobě a představují třeba obecný kontakt na osobu právnickou.)
- Pokud fyzická nebo právnická osoba získá od svého zákazníka podrobnosti jeho elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů, může tato osoba využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jejích **vlastních obdobných výrobků nebo služeb** za předpokladu, že zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.

# Šíření obchodních sdělení

- Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud
  - tato není zřetelně a jasně **označena jako obchodní sdělení**,
  - skrývá nebo **utahuje totožnost odesílatele**, jehož jménem se komunikace uskutečňuje, nebo
  - **je zaslána bez platné adresy**, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.

# Vazba služeb informační společnosti na vnitřní trh EU

- Základním předpokladem pro dobré fungování vnitřního trhu v oblasti elektronického obchodu je jasné stanovení působnosti zákonodárství jednotlivých členských států, respektive stanovení zásady jednoho aplikovatelného práva, aby bylo možno předejít možným konfliktům v právních úpravách jednotlivých členských států.
- Na poskytovatele služby, který poskytuje služby prostřednictvím podniku nebo organizační složky umístěné na území České republiky, se použijí ustanovení zákona č. 480/2004 Sb., o některých službách informační společnosti a zvláštních právních předpisů upravujících podmínky zahájení a výkonu činnosti, která je předmětem poskytované služby, zejména právních předpisů upravujících vznik podnikatelského oprávnění, požadavky na odbornou způsobilost, požadavky na obsah a kvalitu poskytované služby a odpovědnost poskytovatele služby za porušení těchto povinností.
- Na poskytovatele služby, který je usazen v jiném členském státě Evropské unie a poskytujícího tuto službu na území České republiky, se zákon č. 480/2004 Sb., o některých službách informační společnosti a další uvedené právní předpisy **nevztahují**.

## Smlouvy uzavírané na dálku distanční smlouvy a ochrana spotřebitele

- Smlouva uzavíraná na dálku v elektronickém obchodě je smlouva, jejíž sjednání, uzavření anebo plnění se děje za použití elektronických přenosových nebo sdělovacích prostředků. Jde o tzv. **distanční smlouvy**.
- Na uzavření e-smluv se použije obecná úprava **občanského zákoníku**, která předpokládá návrh smlouvy a její přijetí.
- Zda konkrétní e-obchodní sdělení má právní povahu návrhu smlouvy je třeba **posuzovat podle formy a obsahu takového sdělení**.
- Zvláštní úpravu uzavírání distančních smluv obsahuje občanský zákoník pro tzv. spotřebitelské smlouvy (B2C). Jde-li však o spotřebitelskou smlouvu, mohou být prostředky komunikace na dálku umožňující individuální jednání použity jen tehdy, jestliže **spotřebitel jejich použití neodmítá**.



## Smlouvy uzavírané na dálku distanční smlouvy a ochrana spotřebitele

- Automatické rozesílání elektronické pošty může být použito pouze s předchozím ***výslovným souhlasem spotřebitele***.
- Použitím těchto prostředků komunikace na dálku ***nesmí spotřebiteli vzniknout žádné náklady***.

# Spotřebitelské smlouvy v elektronickém obchodu

- Spotřebitelské smlouvy (**B2C**) jsou nejrozšířenějším typem smluv v rámci elektronického obchodu.
- Jde o **soukromoprávní smlouvy**, ve kterých mají smluvní strany zásadně rovné postavení. Ve skutečnosti je však postavení stran často nerovné.  
Potřeba chránit slabší smluvní stranu – spotřebitele – vedla k vytvoření zvláštní právní úpravy tohoto typu smluv.
- Spotřebitelskými smlouvami jsou **smlouvy kupní, smlouvy o dílo, případně jiné smlouvy**, pokud smluvními stranami jsou na jedné straně spotřebitel a na druhé straně dodavatel.  
**Dodavatelem** je osoba, která při uzavírání a plnění smlouvy jedná v rámci své obchodní nebo jiné podnikatelské činnosti.  
**Spotřebitelem** je osoba, která při uzavírání a plnění smlouvy nejedná v rámci své obchodní nebo jiné podnikatelské činnosti.

# Spotřebitelské smlouvy v elektronickém obchodu

- Uzavírání elektronických spotřebitelských smluv má samostatnou úpravu v občanském zákoníku, přičemž nedodržování pravidel **ochrany spotřebitele** může vést k **veřejnoprávnímu postihu** prostřednictvím orgánů správního dozoru, ale může mít i **následky soukromoprávní**, zejména odpovědnost za škodu nebo neplatnost smlouvy.
- Při použití elektronických prostředků musí být obsahem návrhu informace nutné k uzavření smlouvy ve smyslu obecných náležitostí smlouvy a podstatných náležitostí smlouvy upravených v občanském zákoníku.

Tyto informace musí být poskytnuty určitým a **srozumitelným způsobem** s přihlédnutím k zásadám **dobré víry a k ochraně osob**, zejména nezletilých nebo spotřebitelů.

# Spotřebitelské smlouvy v elektronickém obchodu

- *Dále musí být součástí rovněž informace:*
  - zda je smlouva po svém uzavření dodavatelem archivována a zda je přístupná,
  - informace o jednotlivých technických krocích vedoucích k uzavření smlouvy,
  - informace o jazycích, v nichž lze smlouvu uzavřít,
  - informace o možnosti zjištění a opravování chyb vzniklých při zadávání dat před podáním objednávky,
  - informace o kodexech chování, které jsou pro dodavatele závazné nebo které dobrovolně dodržuje, a jejich přístupnosti při použití elektronických prostředků.

# Spotřebitelské smlouvy v elektronickém obchodu

- ***Před podáním objednávky*** musí být při použití elektronických prostředků spotřebiteli umožněno zkontrolovat a měnit vstupní údaje v ní obsažené, které do objednávky vložil; (to neplatí při jednání výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací).
- Smlouva a všeobecné obchodní podmínky musí být spotřebiteli poskytnuty ve formě, která ***umožňuje archivaci a reprodukci***.
- Byla-li smlouva uzavřena při použití elektronických prostředků komunikace na dálku, má spotřebitel právo od smlouvy odstoupit bez uvedení důvodu a ***bez jakékoliv sankce do 14 dnů*** od převzetí plnění. V případě, že dodavatel ***nepředal spotřebiteli informace***, které je povinen předat, činí tato lhůta pro odstoupení 3 měsíce od převzetí plnění.





# Elektronický podpis Časové razítko

- **Obecné informace**  
(úvod do problematiky elektronického podpisu)
- **Základní atributy bezpečnosti**  
(popis požadavků na bezpečnost dat)
- **Úvod do kryptografie**  
(vysvětlení základních pojmů a kryptografických principů)
- **Vysvětlení klíčových pojmů**  
(definice pojmů, aneb, aby bylo jasno)
- **Legislativa**  
(evropská a česká legislativa spojená s elektronickým podpisem)
- **Certifikát**
- **Časové razítko** (co je a k čemu se užívá)
- **Poskytovatel certifikačních služeb, využití v praxi**  
(jak fungují a k čemu se využívají certifikační authority)
- **PKI**  
(popis technik spojených s využíváním infrastruktury veřejného klíče)

# Bezpečná komunikace

- Specifický pohled na řešení bezpečnosti  
(problém propojení a přímé komunikace interních a externích zdrojů)
- Kdo je můj komunikační partner?
- Je důvěryhodný?
- Je naše komunikace důvěrná?
- Bezpečná vstupní brána nebo “end to end” řešení?
- Jakým způsobem je vhodné řešit bezpečnost elektronické komunikace?

# Cíle komunikační bezpečnosti

Zajistit, aby procesy, založené na elektronické komunikaci byly minimálně stejně důvěryhodné a bezpečné, jako standardní procesy spojené s “papírovou” agendou.



# Cíle komunikační bezpečnosti

- **Dostupnost**
- **Důvěrnost informací**
  - neautorizované subjekty nemají možnost přístupu k důvěrným informacím
- **Integrita dat**
  - zabezpečení proti neautorizované modifikaci dat
- **Autentičnost**
  - možnost jednoznačně identifikovat odesílatele zprávy
- **Neodmítnutelnost odpovědnosti**
  - důkaz o přímé odpovědnosti subjektu za odeslanou zprávu



# Co je to KRYPTOGRAFIE ?

- Kryptografie je disciplína, která ztělesňuje zásady, prostředky a metody pro ochranu určených skutečností za účelem jejich:
  - skrytí před neoprávněnou stranou,
  - zajištění jejich autentičnosti,
  - zabránění jejich nedetekované modifikaci,
  - zabránění jejich odmítnutí (popření),  
nebo
  - zabránění jejich neoprávněnému použití.

# Co je to PKI

- **PKI - public key infrastructure** je soustavou technických a především organizačních opatření spojených s
  - vydáváním,
  - správou,
  - používáníma
- odvoláváním platnosti kryptografických klíčů a certifikátů.

# Úvod do problematiky

- Elektronický podpis <===> Podpis
- Zaručený elektr. podpis <===> Vlastnoruční podpis
- Certifikát <===> Průkaz totožnosti
- Kvalifikovaný certifikát <===> Občanský průkaz
- Certifikační autorita <===> Vydavatel průkazů totožnosti
- Akreditovaná CA <===> Vydavatel Občanských průkazů
- Uznávaný elektronický podpis .....

# Šifrování a dešifrování

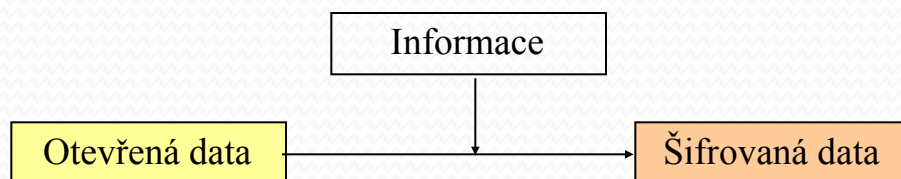
## Otevřená data:

data, která nejsou chráněna proti přístupu neoprávněných subjektů.

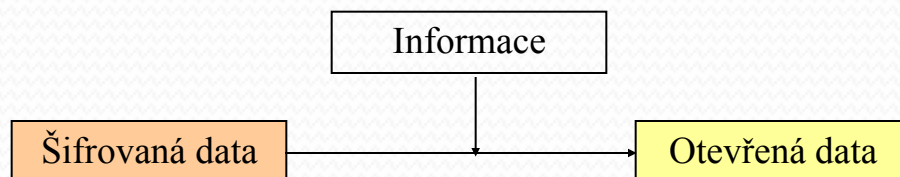
## Šifrovaná data:

data chráněna proti přístupu neoprávněných subjektů.

**Šifrování:** vytvoření šifrovaných dat z dat otevřených



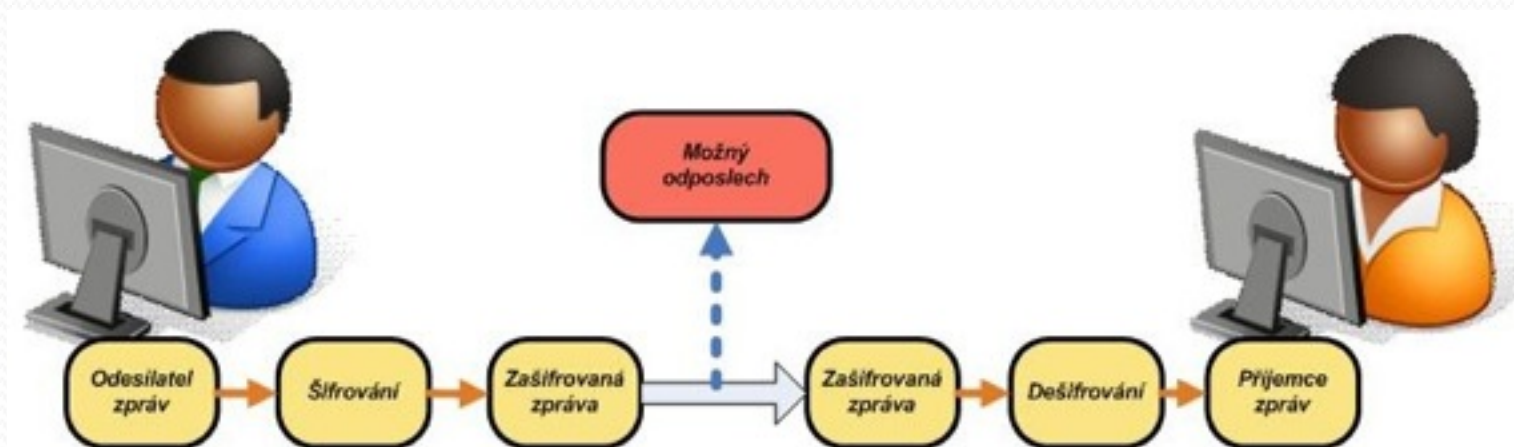
**Dešifrování:** získání otevřených dat z dat šifrovaných



Informaci používané při šifrování a dešifrování dat budeme říkat **klíč**.

# Symetrická kryptografie

Pojem “**symetrická**” vyjadřuje fakt, že tyto metody používají tutéž informaci - tzv. **tajný klíč (secret key)** - jak k šifrování, tak dešifrování dat.



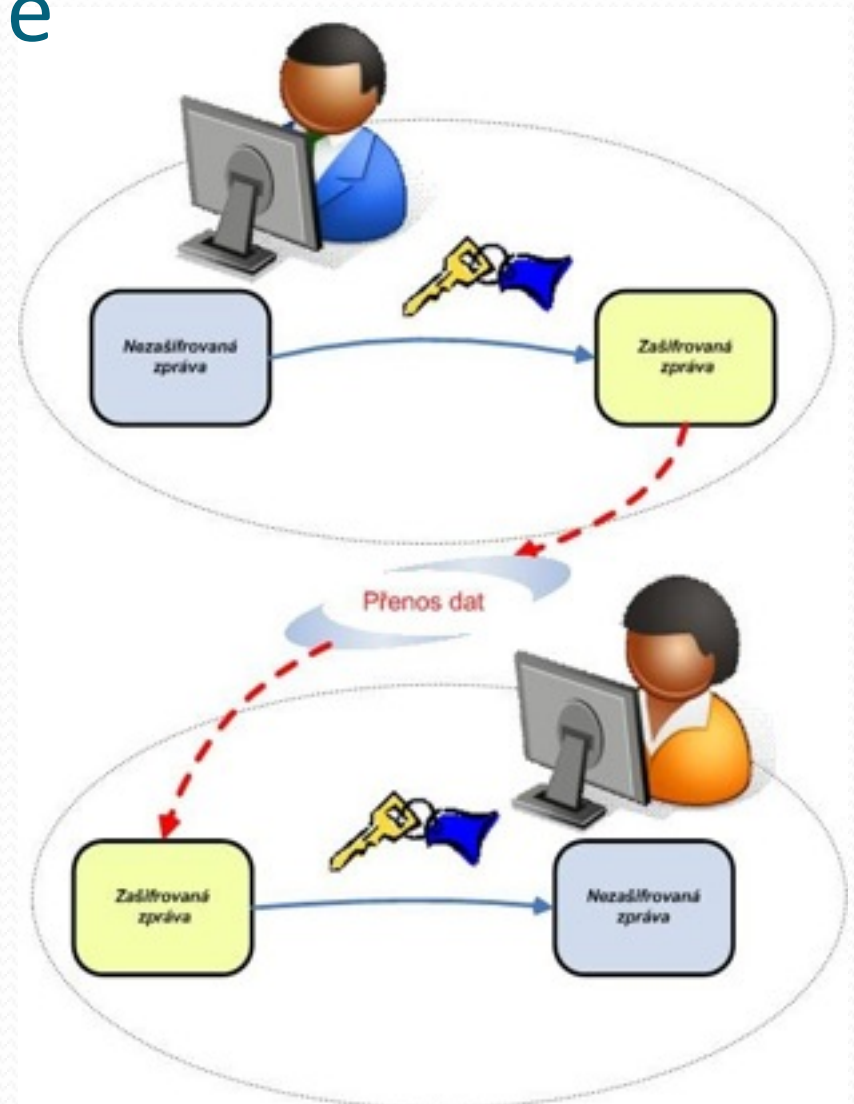
Dnes se používají především:

**DES(56b), DES<sub>3</sub>(112b), DES-EDE<sub>3</sub>-CBC(112b), RC2(40,64,128b), RC4(40,64,128).** K modernějším pak patří **IDEA(128b), CAST(128b)** a **BlowFish(128b)**. Za dostatečně bezpečné se dnes považují šifry alespoň na úrovni DES<sub>3</sub>, obecně se pak hovoří o “**128-bitové symetrické kryptografii**”.



# Symetrická kryptografie

šifrování dat symetrickou šifrou

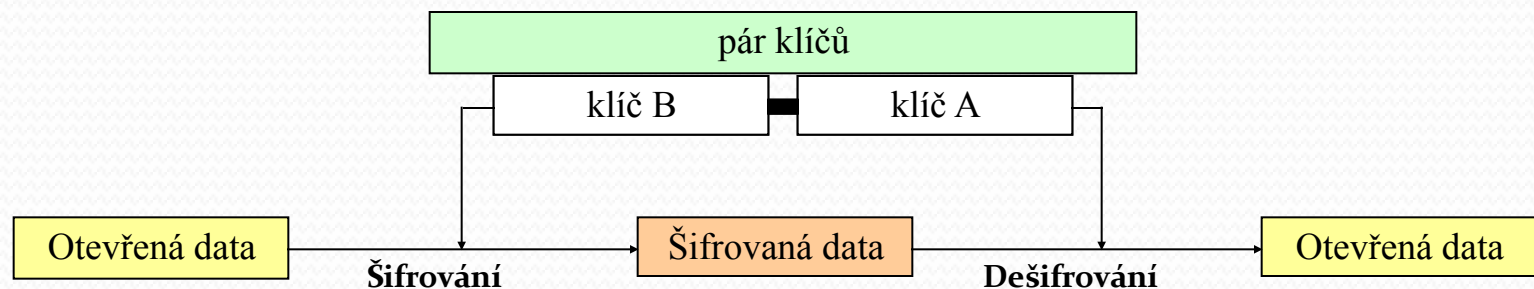


# Asymetrická kryptografie

Pojem **asymetrie** vyjadřuje fakt, že tyto metody používají dvojici klíčů A,B (pár klíčů), které mají tuto vlastnost:

- data šifrovaná klíčem A lze dešifrovat jen a pouze klíčem B.
- data šifrovaná klíčem B lze dešifrovat jen a pouze klíčem A.

Asymetrické metody jsou výpočetně náročné a podstatně pomalejší (a to řádově) než metody symetrické.



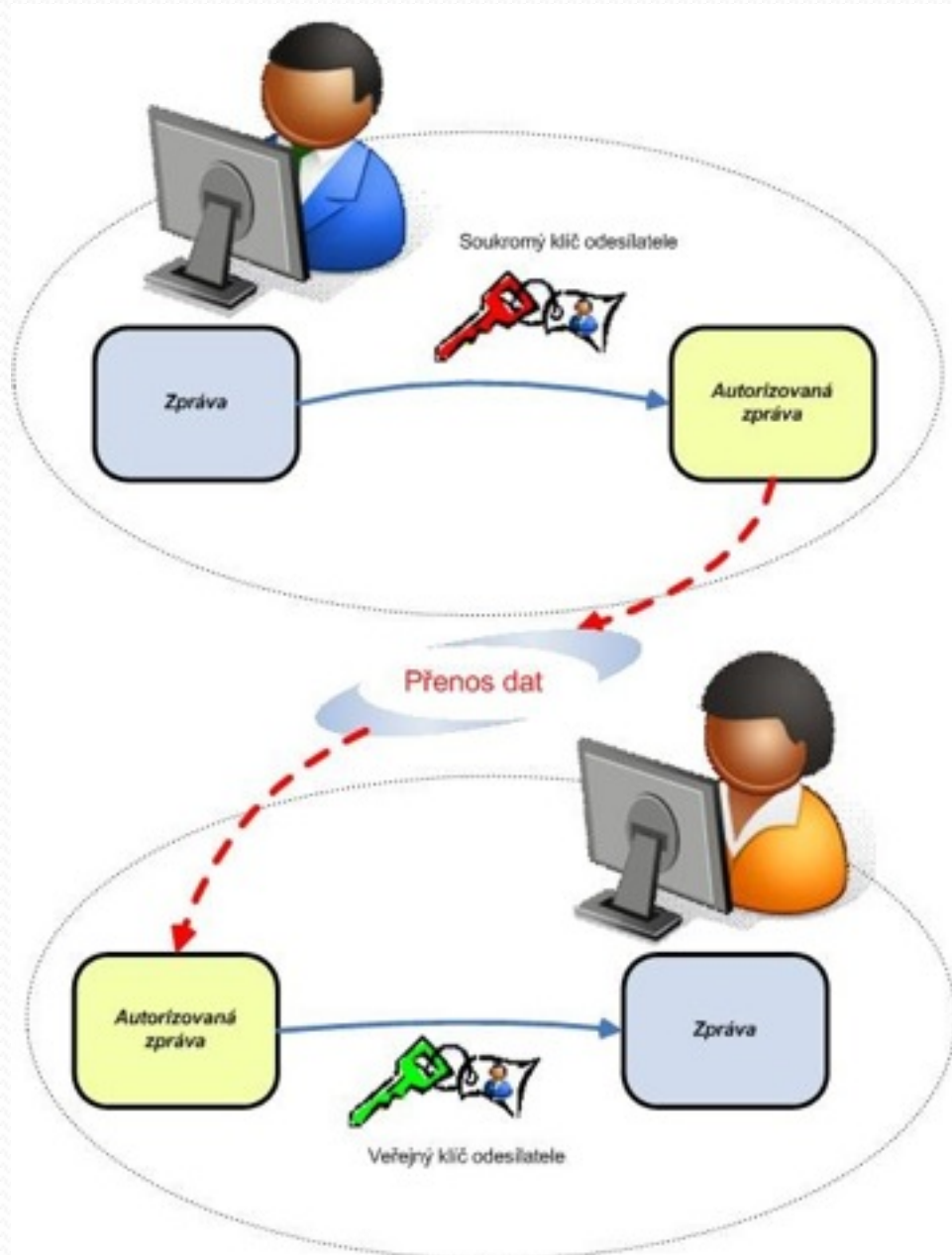
Dnes se používají především:

**RSA(1024b)**, k novějším pak patří **eliptické křivky - ECC(160b)**.  
Obecně se pak hovoří o “**1024-bitové asymetrické kryptografii**”.  
**Dnes již není bezpečné použití slabší kryptografie!!!**

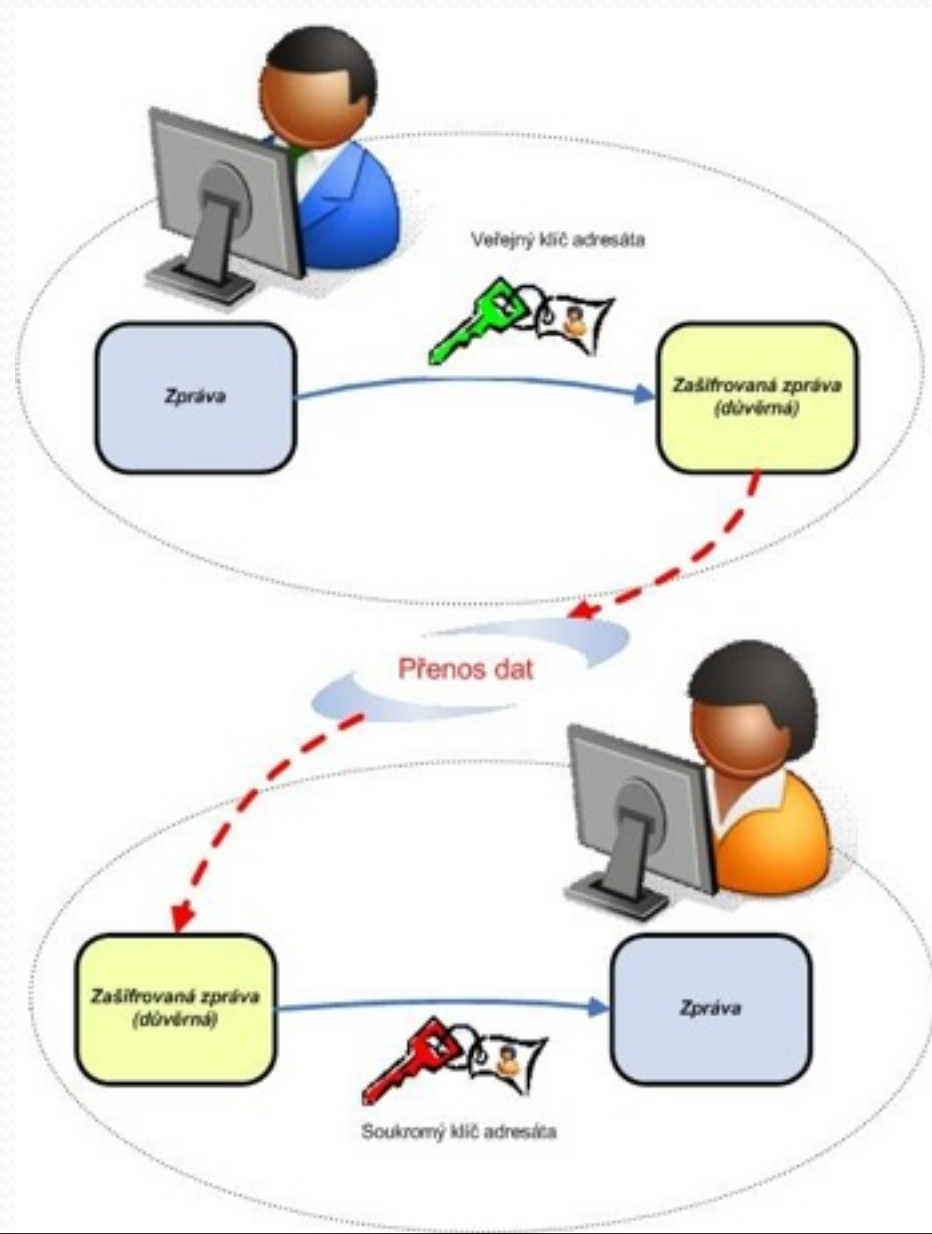
# Kryptografie s veřejným klíčem (PKI)

- Je založena na asymetrické kryptografii.
- První klíč (A) z páru klíčů nazýváme **soukromý klíč** (private key), druhý klíč (B) nazýváme **veřejný klíč** (public key).
- Soukromý klíč je znám pouze vlastníkov. Před ostatními je vlastníkem utajován a chráněn.
- Veřejný klíč je naopak vlastníkem zveřejněn - je k dispozici všem (zveřejněný – certifikát)
- Umožňuje :
  - **Bezpečné zasílání dat příjemci** (důvěrnost)
  - **Podepisování dat odesilatelem** (integrita, autentičnost, neodmítnutelnost odpovědnosti)

Přenos NEadresované,  
NEzašifrované (veřejné),  
ale autorizované zprávy

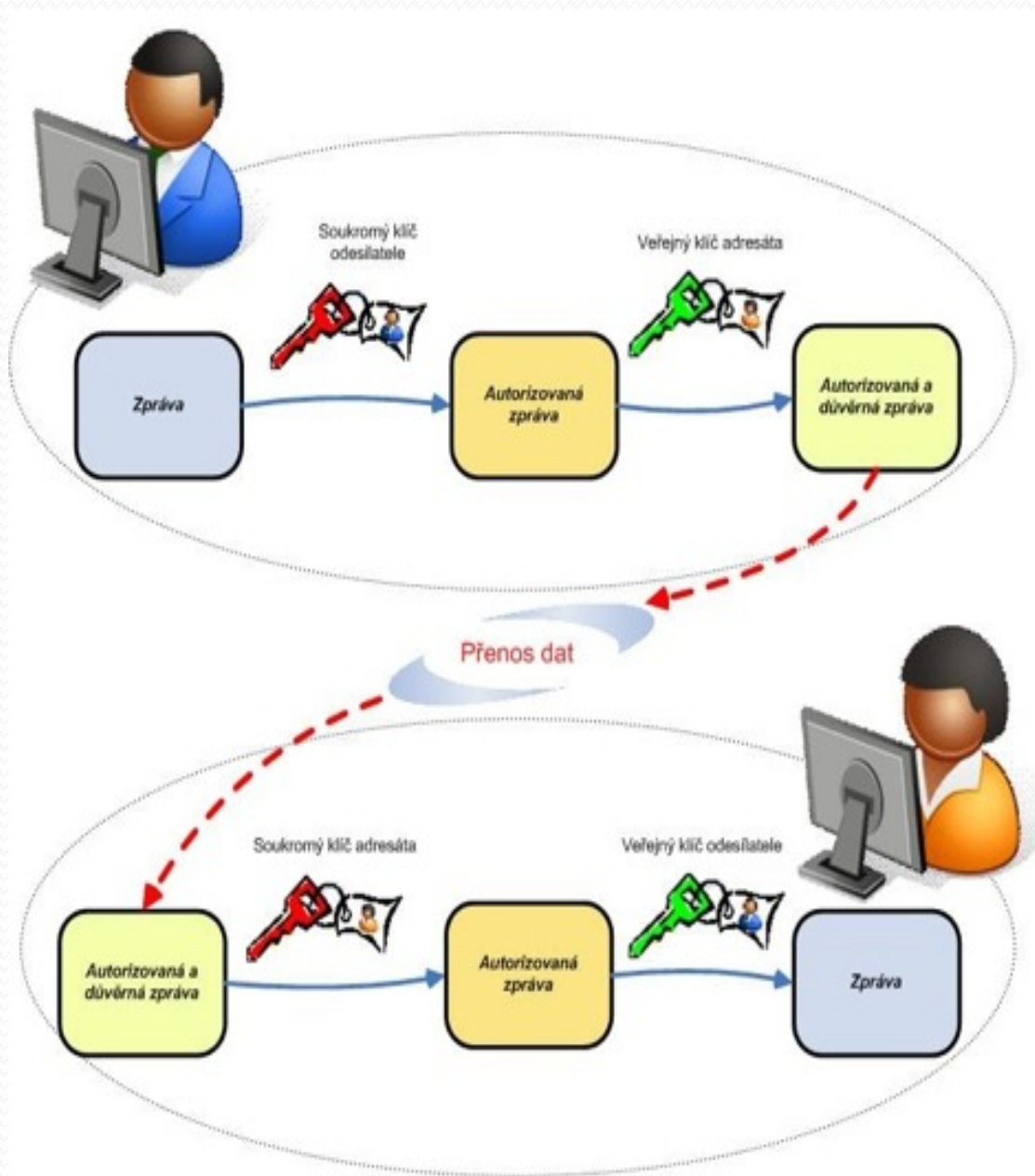


Přenos adresované,  
zašifrované (důvěrné),  
ale NEautorizované zprávy





Přenos adresované,  
zašifrované (důvěrné)  
a autorizované zprávy





# Hashovací funkce

- Jednosměrné funkce **mapující data (různé velikosti) na sekvenci bitů s danou délkou** (typicky 256 nebo 512 bitů).
- Nejde o prosté mapování - existují data, která jsou vzájemně různá, ale jejich hash (výsledek hashovací funkce) je shodný (hash-ekvivalentní data).
- Pro kvalitní hashovací funkce je úloha najít data se stejným hash kódem výpočetně velmi náročná.

Minimálně stejně náročný je problém nalezení dat, jejichž hashováním kód vznikl, neboť se jedná o získání a prohledání skupiny hash-ekvivalentních dat, přičemž správná data nemohou být nalezena jen na základě hash kódu, ale i dalších informací o hledaných datech, které nemají s hashováním žádnou souvislost.

# Hashovací funkce

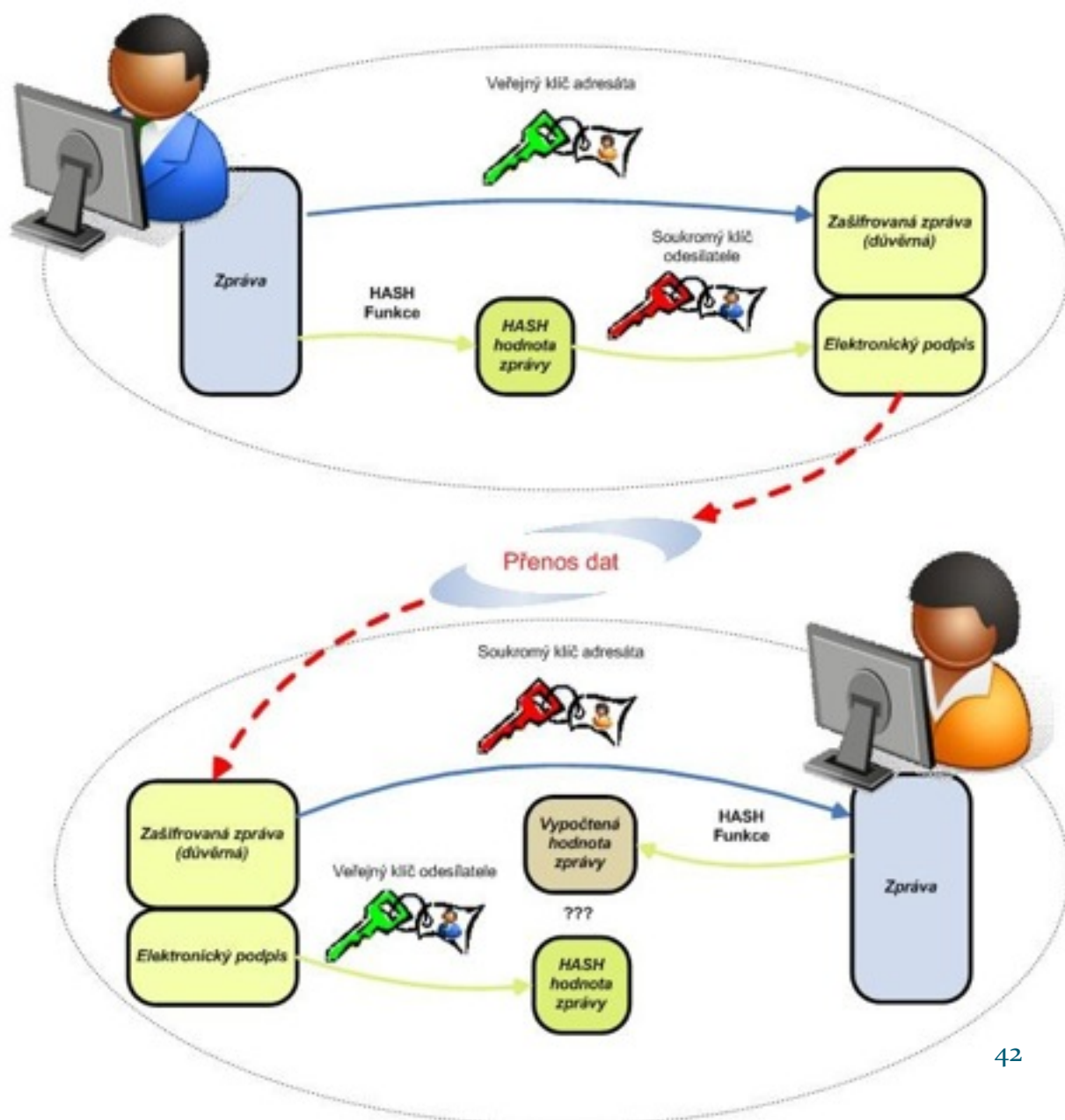
- Hashovací algoritmy nejsou v žádném případě šifrovací (už vzhledem k nejednoznačnosti – obecně neexistuje inverzní funkce), ale používají se v roli kvalitního “otisku prstu dat” - **fingerprintu** dat.
- Hashovací funkce jsou konstruovány na výpočetních operacích nízké úrovně (především bitové operace a posuny) a jsou tedy výpočetně velmi rychlé a efektivní.
- Dnes se používají především algoritmy (**SHA-1**), **SHA-2** a **MD5**. Dále pak např. moderní **RIPEMD-160**.

Jana Nováková, Dlouhá 36/83, Novosedly

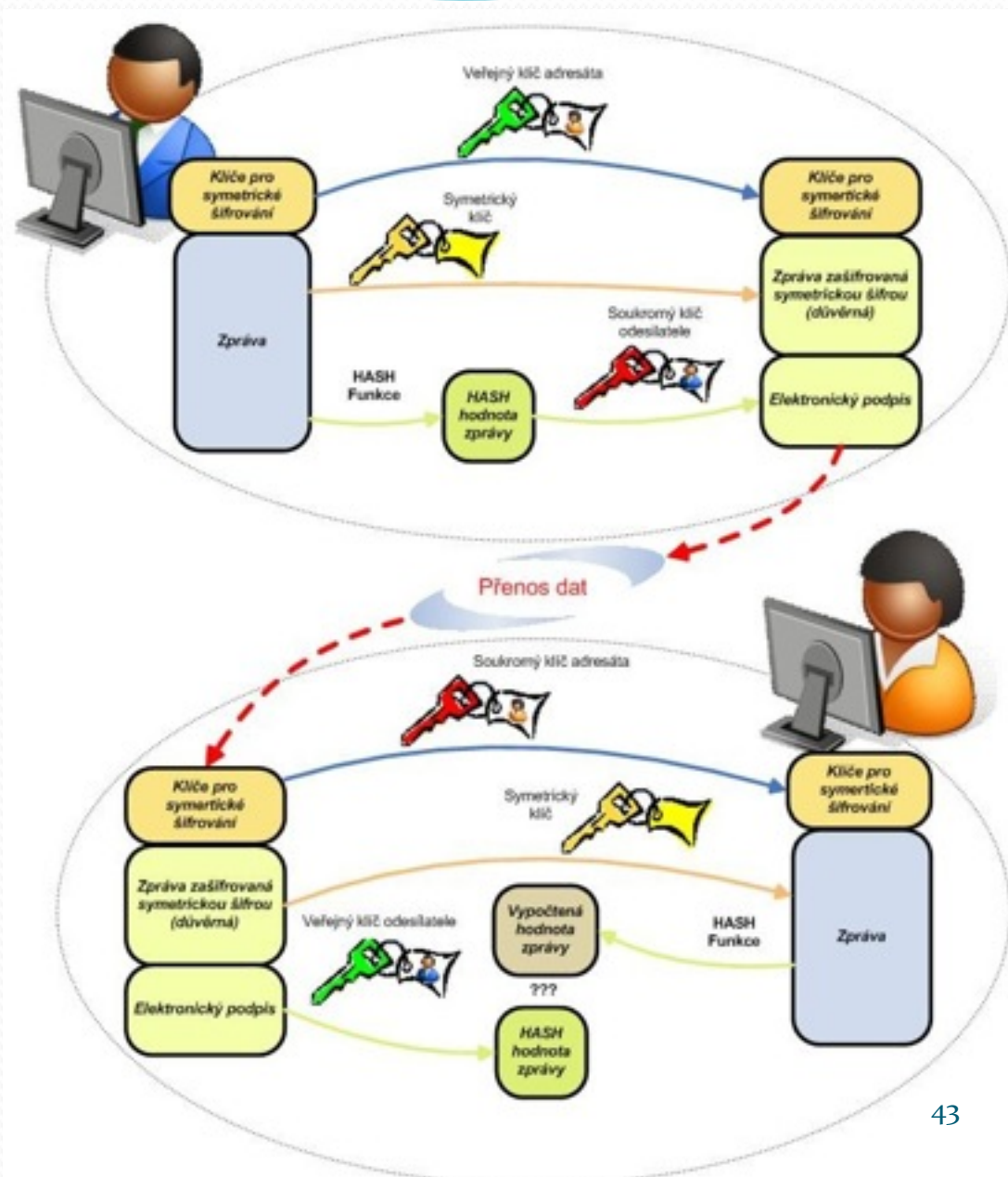
**MD5 hash:** 3cde28f6f67d813ae7dbc5db0587e55c

**SHA1 hash:** 6dbe4b53d924641b40e797bb2b6018cc436a5dc0

# Bezpečná komunikace s využitím elektronického podpisu

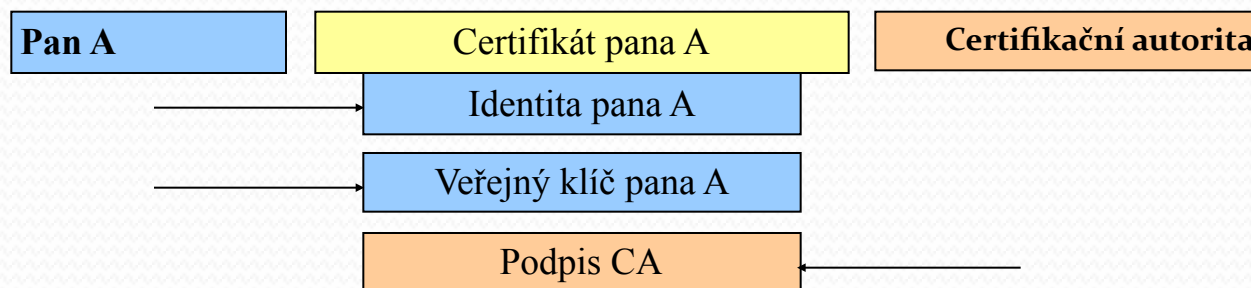


# Bezpečná komunikace s využitím elektronického podpisu a šifrováním zprávy symetrickou šifrou



# Princip certifikátu

- ***Certifikát*** obsahuje identifikaci vlastníka a veřejný klíč vlastníka.
- ***Certifikát*** je podepsán vystavitelem certifikátu (certifikační autoritou).



- ***Certifikát*** svazuje identitu vlastníka (pana A) a veřejný klíč vlastníka (veřejný klíč pana A).
- ***Certifikát*** umožňuje publikovat veřejný klíč vlastníka (pana A) certifikátu spolu s jeho identitou.
- Integrita (neporušenost certifikátu) je chráněna podpisem certifikační authority.



# Certifikát





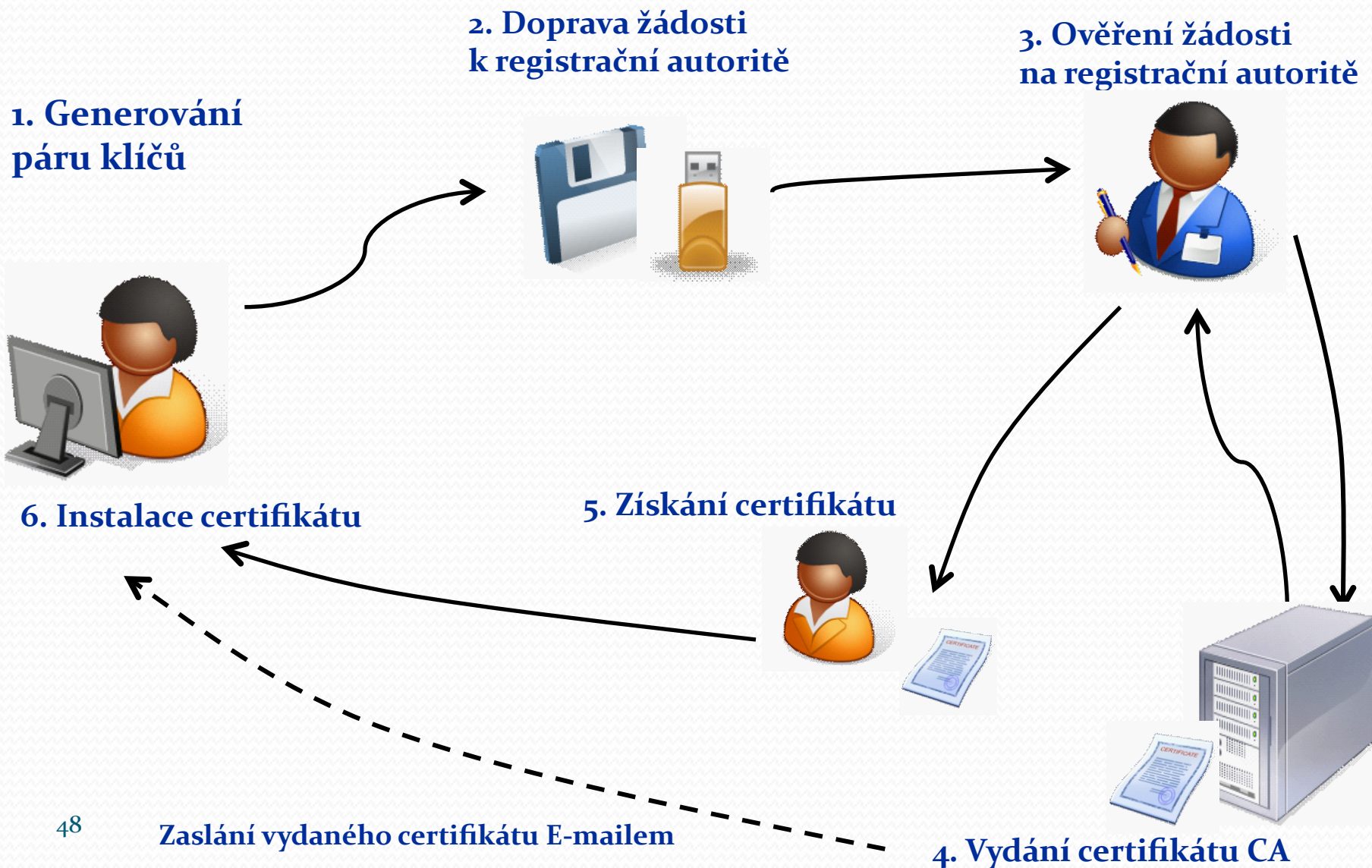
# Akreditovaní poskytovatelé certifikačních služeb v ČR

- Společnostem, které požádají o akreditaci a které současně splní požadované podmínky, vydá tuto Ministerstvo Vnitra ČR (dále jen MVČR, dříve MI ČR, ÚOOÚ)
- Získání akreditace předchází poměrně dlouhodobý proces konkrétních řešení uvnitř těchto společností, na jehož konci – pokud je tento proces úspěšný - dojde k získání akreditace – přehled akreditací podle MVČR:
  1. První certifikační autorita, a.s.
  2. Česká pošta, s.p. - Post Signum
  3. eIdentity a.s.

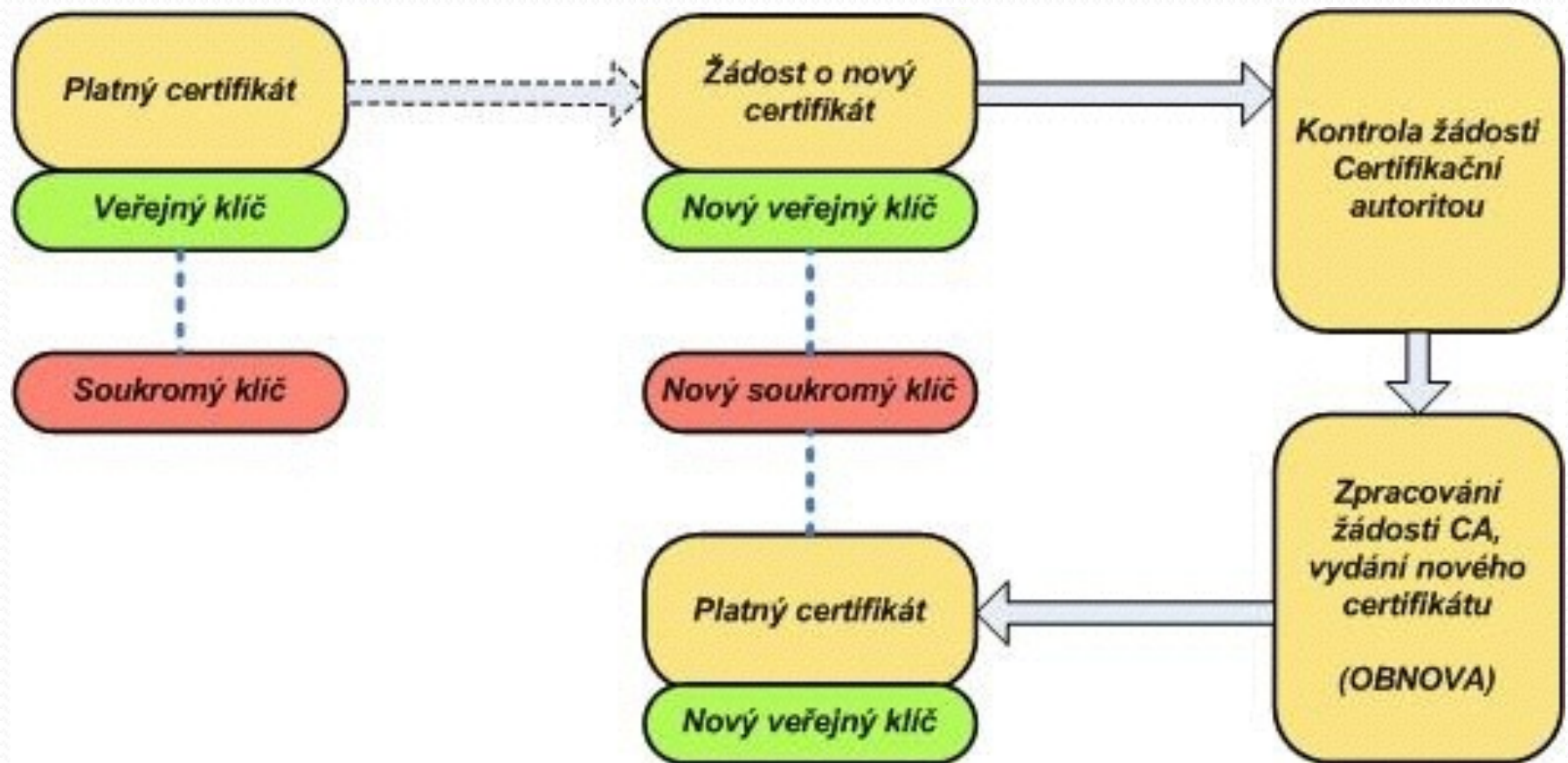
# Certifikační autorita – certifikační služby

- Vydává certifikáty  
(má odpovědnost za ověření totožnosti žadatele o certifikát)
- Vydává seznam zneplatněných certifikátů - CRL
- Vydává seznam veřejných certifikátů
- Zajišťuje uložení a distribuci identifikačních informací

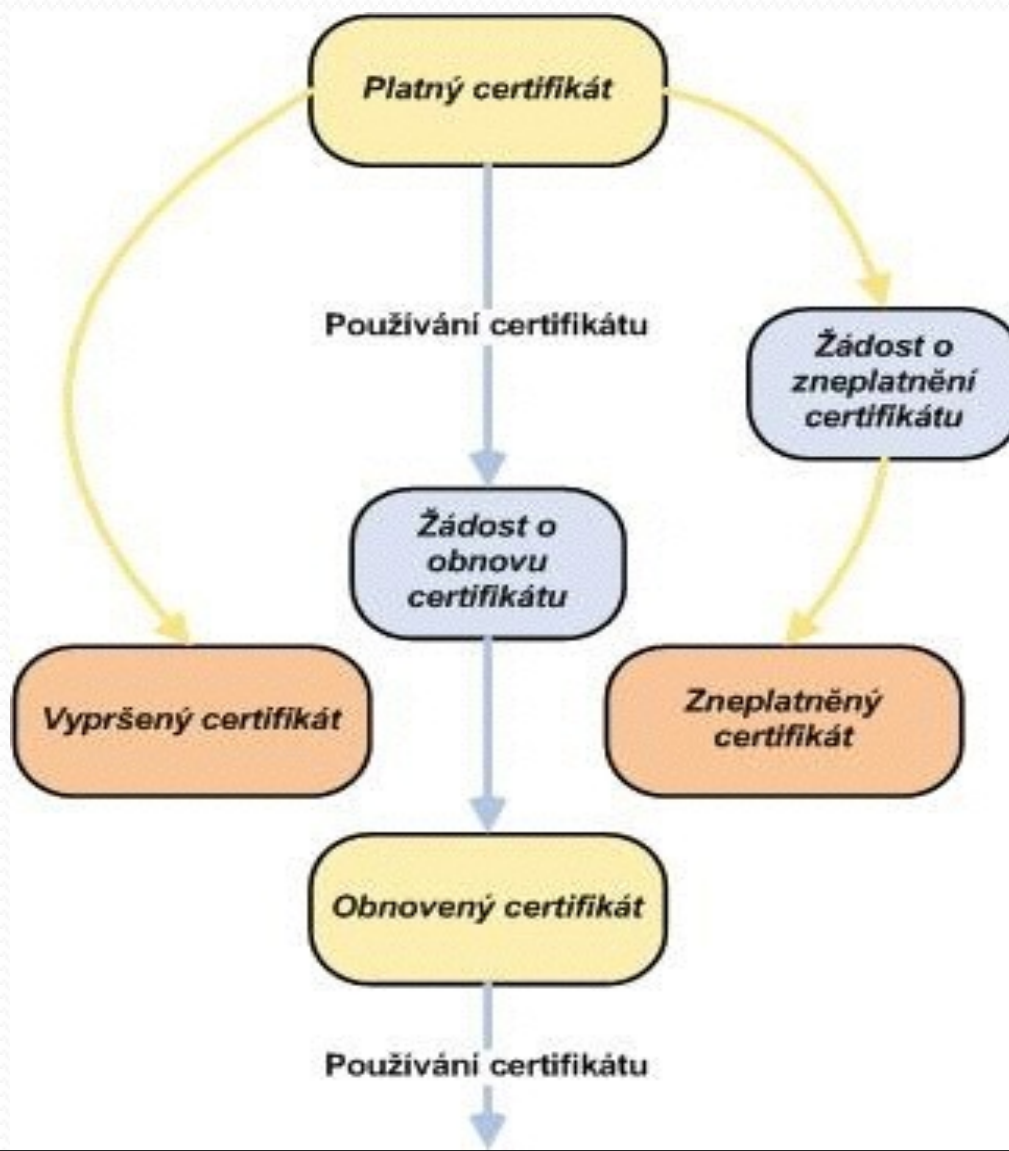
# Proces vydání certifikátu



# Proces obnovy certifikátu



# Životní cyklus certifikátu





# Legislativa k elektronickému podpisu

- Směrnice Evropského parlamentu a Rady 1999/93/ES
- Zákon 227/2000 Sb. o elektronickém podpisu v platném znění
- Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č.227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- Vyhláška č.496/2004 Sb. k elektronickým podatelnám
- Vyhláška z 19.7.2006 č.378/2006

Kvalifikovaný certifikát – podpis

Komerční certifikát – autentizace a šifrování

- Certifikační politiku I.CA - najdete na <http://sy.pe/LiVyc>
- Certifikační politiku Post Signum pak na <http://sy.pe/dHj5b>
- Zákon o e-Governmentu <http://sy.pe/okWud>



# Legislativa k elektronickému podpisu

- Směrnice Evropského parlamentu a Rady 1999/93/ES <http://sy.pe/WL6r>
- Zákon 227/2000 Sb. o elektronickém podpisu v platném znění <http://sy.pe/XGLEb>

# Klíčové pojmy v legislativě (1)

- ***elektronický podpis*** - *údaje v elektronické podobě*, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako *metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*
- ***zaručený elektronický podpis*** - elektronický podpis, který splňuje následující:
  1. je jednoznačně spojen s podepisující osobou,
  2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
  3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- 1. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

## Klíčové pojmy v legislativě (2)

- **elektronická značka** - údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky
  1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu
  2. byly vytvořeny a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
    1. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat
- **kvalifikované časové razítko** - datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb (CA) a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

# Legislativně nedořešené oblasti

- Archivace elektronických dokumentů
- Průkaznost provedené operace
- Standardizovaná garantovaná pošta
- Mezinárodní uznatelnost elektronického podpisu

# Je zaručený elektronický podpis bezpečný?

- Má oporu v evropské legislativě, jasně vymezená práva a povinnosti (výrazně lépe než vlastnoruční podpis),
- Je založen na moderních kryptografických metodách,
- Má jasně definované a popsané procesy tvorby a ověření podpisu,
- Zaručený elektronický podpis ***je neporovnatelně bezpečnější a důvěryhodnější než podpis vlastnoruční !!!***

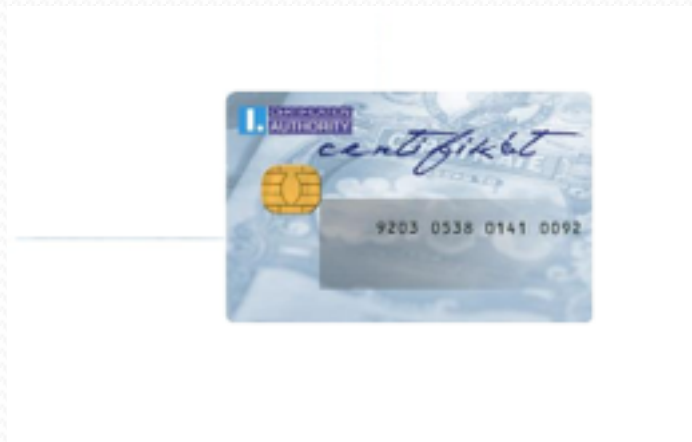
# Certifikační služby

- ❑ Vydávání komerčních certifikátů
- ❑ Vydávání kvalifikovaných certifikátů
- ❑ Vydávání kvalifikovaných systémových certifikátů
- ❑ Zřizování registračních autorit
- ❑ Vydávání časových razítek
- ❑ Nabídka čipových karet a čteček
- ❑ Spolupráce s klienty při implementaci služeb
- ❑ Další služby související s činností CA (archivace, ...)



# Úložiště dat pro vytváření elektronického podpisu

- Osobní počítač
- Čipová karta + čtečka
- USB token



V některých zemích čipová karta  
s certifikátem již nahrazuje OP



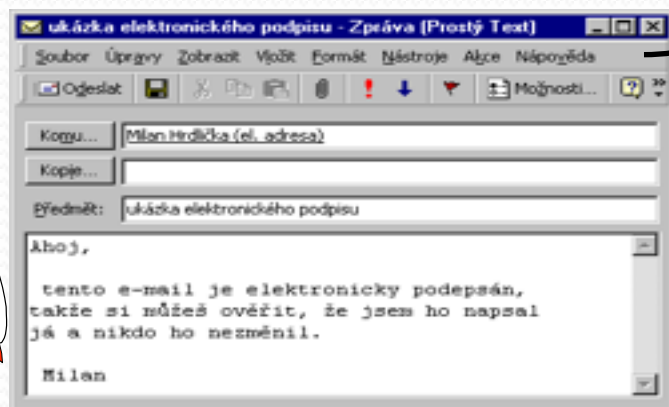
# V některých zemích čipová karta s certifikátem již nahrazuje OP a v ČR ?

jde “jen” o občanský průkaz s čipem a tedy nosičem certifikátu  
pro elektronické podepisování a je o něj malý zájem  
- cena OP bez čipu 100,- Kč s čipem 500,- Kč

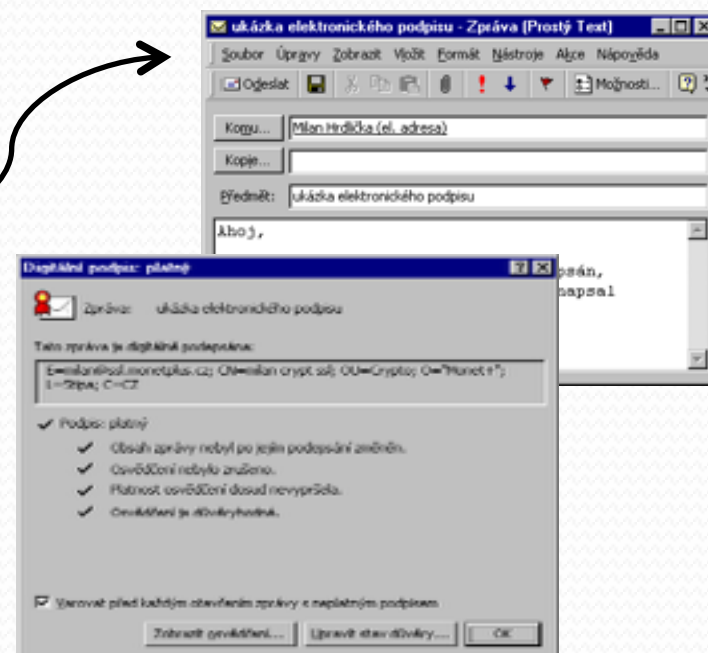


# Podepsaná komunikace e-mailem

## 1. Napíšeš a odešleš e-mail s elektronickým podpisem



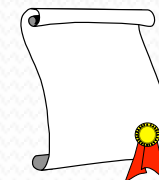
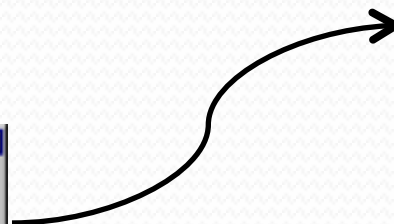
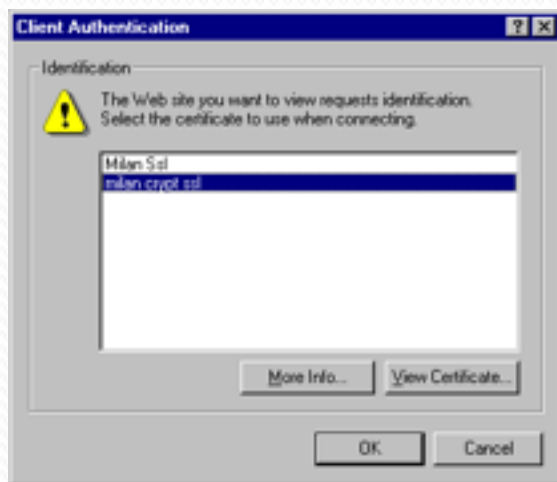
## 2. Příjemce obdrží e-mail



## 3. Příjemce zkontroluje elektronický podpis

# Komunikace s web serverem

## 1. Výběr certifikátu pro přístup



## 2. Přístup na web server

# Využití certifikátů

- **Oblast orgánů veřejné moci**
  - realizace projektů v souladu se státní informační politikou (eGovernment)
- **Finanční a bankovní sektor**
  - řešení bezpečné komunikace mezi subjekty
  - portálové aplikace
  - specializované aplikace využívající certifikáty jako formu zabezpečení
  - přenos důvěrných dat
- **Sféra středních a větších firem**
  - bezpečná komunikace managementu firmy
  - bezpečný přístup na firemní www server k důvěrným informacím
- **Internetová veřejnost**
  - komunikace se státní správou a samosprávou ve smyslu Zákona o elektronickém podpisu



# Využití certifikátů

- podání Přehledu o příjmech a výdajích OSVČ za rok
- podání Evidenčních listů důchodového pojištění
- podání Přihlášek a odhlášek k nemocenskému pojištění
- podání Přiznání daně z příjmů
- měsíční podání Přiznání daně z přidané hodnoty
- žádosti o sociální dávky a rodičovské příspěvky
- žádosti o porodné
- komunikace se zdravotními pojišťovnami
- žádosti o zaslání Přehledu vykázané zdravotní péče na pojištěnce za uplynulý kalendářní rok a případně také při reklamaci
- komunikace s krajskými, městskými či obecními úřady
- .....

# Využití komerčních i kvalifikovaných certifikátů v praxi

## ■ Bankovníctví a pojišťovnictví:

- **Československá obchodní banka, a.s.**
  - ČSOB Internatbanking 24 a ČSOB Bussinesbanking 24,
  - Max Homebanking Poštovní spořitelny
- **Českomoravská hypoteční banka, a.s.**
  - mezipobočková výměna elektronické dokumentace
- **PORTÁL zdravotních pojišťoven**
  - společné řešení 6 zdravotních pojišťoven v ČR
  - ČNZP, OZP, RBP, ZP MA, ZPŠ, Vojenská ZP
- **Všeobecná zdravotní pojišťovna ČR**
- **Česká spořitelna a.s.**

# Využití komerčních i kvalifikovaných certifikátů v praxi

## ■ Komerční sféra (příklady)

### • Obchodní řetězce

- GLOBUS

### • Energetika

- Českomoravská komoditní burza Kladno
- ČEPS, a.s. (systém DAMAS)
- ČEZ, a.s., SME, JČE, PRE, VČE, ZČE, JME, .....

### • CK Vítkovice Tours

- objednávkový dealerský systém


### • Středisko cenných papírů ČR


- dnes již přes 2.000 společností ke komunikaci využívá certifikáty I.CA

# PKI - Klasický certifikát veřejného klíče

<b>Certifikát</b>
<b>Předmět:</b> Pepa Novák
-----
<b>Vydal:</b> Certifikační autorita Sériové číslo: 1234567 Platnost:
-----
<b>Veřejný klíč:</b> FAABBE45BB2FDA...
-----
El. podpis: 

<b>Časové razítko</b>
<b>Vydal:</b> TSA Sériové číslo: 1234 Čas:
-----
<b>Hash z dokumentu:</b> SHA-1,FE3445BB2FDA...
-----
El. podpis: 

<b>Atributový certifikát</b>
<b>Držitel:</b> Pepa Novák
-----
<b>Vydal:</b> Atributová autorita Sériové číslo: 9876543 Platnost:
-----
<b>Atributy:</b> blabla..
-----
El. podpis: 

<b>DV-certifikát</b>
<b>Držitel:</b> Pepa Novák
-----
<b>Vydal:</b> DVCS Sériové číslo: 9876543 Platnost:
-----
<b>Hash z dokumentu:</b> SHA-1,FE3445BB2FDA...
-----
El. podpis: 

**Datová** struktura, která spojuje identifikaci žadatele s jeho veřejným klíčem. Tato vazba je stvrzena **elektronickým podpisem certifikační autority**.


Obsahuje jedinečné číslo certifikátu, jméno vydavatele certifikátu, jméno držitele certifikátu (předmět certifikátu), platnost certifikátu a veřejný klíč držitele certifikátu.

Autentizace na základě certifikátu se provádí **prokazatelným** vlastnictvím soukromého klíče náležejícímu k veřejnému klíči uvedenému v certifikátu.

# PKI – časové razítko

<b>Certifikát</b>
<b>Předmět:</b> Pepa Novák
<b>Vydal:</b> Certifikační autorita Sériové číslo: 1234567 Platnost:
<b>Veřejný klíč:</b> FAABBE45BB2FDA...
<b>El. podpis:</b> 

<b>Časové razítko</b>
<b>Vydal:</b> TSA Sériové číslo: 1234 Čas:
<b>Hash z dokumentu:</b> SHA-1,FE3445BB2FDA...
<b>El. podpis:</b> 

<b>Atributový certifikát</b>
<b>Držitel:</b> Pepa Novák
<b>Vydal:</b> Atributová autorita Sériové číslo: 9876543 Platnost:
<b>Atributy:</b> blabla..
<b>El. podpis:</b> 

<b>DV-certifikát</b>
<b>Držitel:</b> Pepa Novák
<b>Vydal:</b> DVCS Sériové číslo: 9876543 Platnost:
<b>Hash z dokumentu:</b> SHA-1,FE3445BB2FDA...
<b>El. podpis:</b> 

Časové razítko slouží jako důkaz o tom, že daný dokument existoval před časem uvedeným v časovém razítku.

Struktura obdobná certifikátu, která svazuje hash z dokumentu s časem.

Je elektronicky podepsáno (vydáváno) **autoritou pro vydávání časových razítek** (Time Stamping Authority TSA)

# Definice

**kvalifikovaným časovým razítkem** je datová zpráva, kterou vydal **kvalifikovaný** poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem “orazítkování” dat.





# Co je časové razítko

- Časové razítko je datová zpráva, která **potvrzuje existenci dokumentu v čase**,
- Slouží jako důkaz, že datový objekt, ke kterému je připojeno, **existoval bezprostředně před časovým údajem**, uloženým v tomto časovém razítku,
- Zajišťuje **přiřazení aktuálního časového údaje** k existujícím datům, informacím, souborům nebo událostem,
- Spojení **nezpochybnitelného časového údaje** a konkrétních dat je nezbytné zejména pro účely jejich zpětného ověřování,
- Časové razítko obsahuje:
  - **datum a čas vydání**,
  - **číslo časového razítka**,
  - **identifikaci třetí strany**, která časové razítko vydala (poskytovatele certifikačních služeb),
  - a **otisk dat (hash)**, ke kterým je razítko vydáno.

# Kvalifikované časové razítko

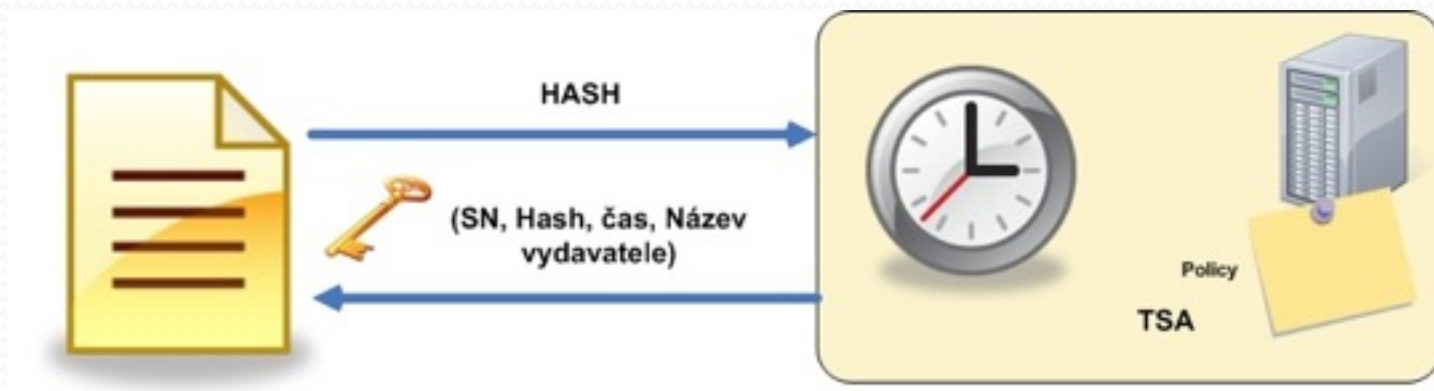
**Vydané kvalifikované časové razítko obsahuje minimálně :**

- unikátní číslo kvalifikovaného časového razítka
- označení pravidel, podle kterých bylo kvalifikované časové razítko vydáno
- časový údaj, jehož odchylka nepřesáhne **1 sekundu od UTC** (UTC = Coordinated Universal Time, je založen na atomových, tzn. je na rotaci Země nezávislý (pominou-li se vlivy dilatace času))
- data v elektronické podobě - otisk (hash) dat, pro která bylo kvalifikované časové razítko vydáno
- elektronickou značku serveru, který kvalifikované časové razítko vydal (TSU = Time stamping unit)

# K čemu časové razítko slouží a k čemu ne

- **Ano** - **Existence** dokumentu v daném čase
  - Potvrzení o uzavření obchodu s konkrétními podmínkami (zafixování kurzu zahraničních měn)
  - Předání dokumentace (on-line obchodování, soudní dokazování, výběrové řízení)
  - Časové razítkování logových záznamů
  - Elektronická podatelna
- **Ne** - **Vlastnictví** dokumentu v daném čase
  - Ochrana autorských práv
  - Elektronický podací lístek

# Vydání časového razítka

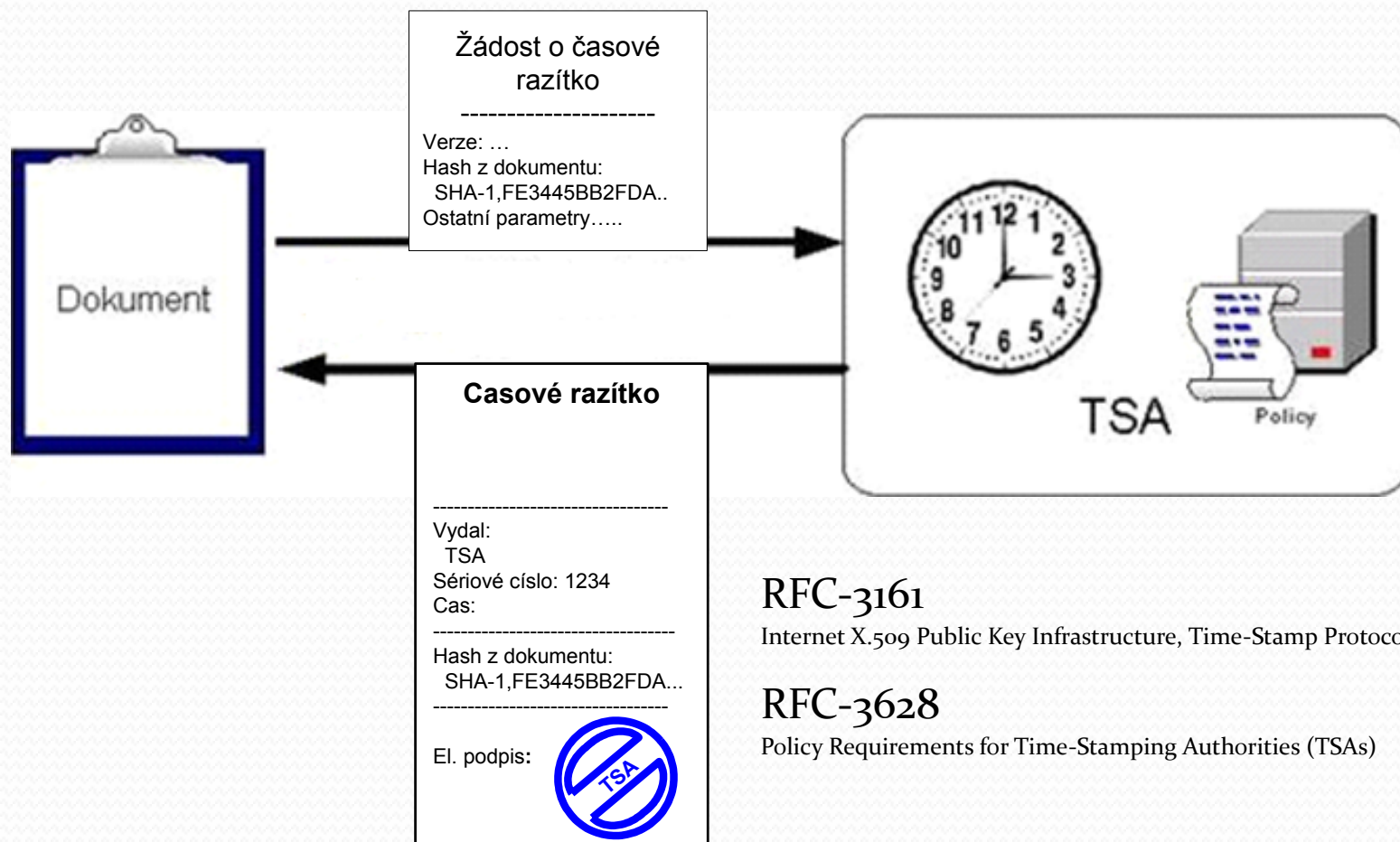


Časová razítka vydává poskytovatel certifikačních služeb, který nabízí služby časové autority (*TSA – Time Stamp Authority*).

Postup získání časového razítka:

- Tvorba žádosti o vydání časového razítka
- Odeslání žádosti o vydání časového razítka na server časové autority
- Zpracování žádosti o časové razítko
- Přijetí odpovědi od serveru časové autority
- Kontrola odpovědi na žádost o vydání časového razítka

# Časové razítko



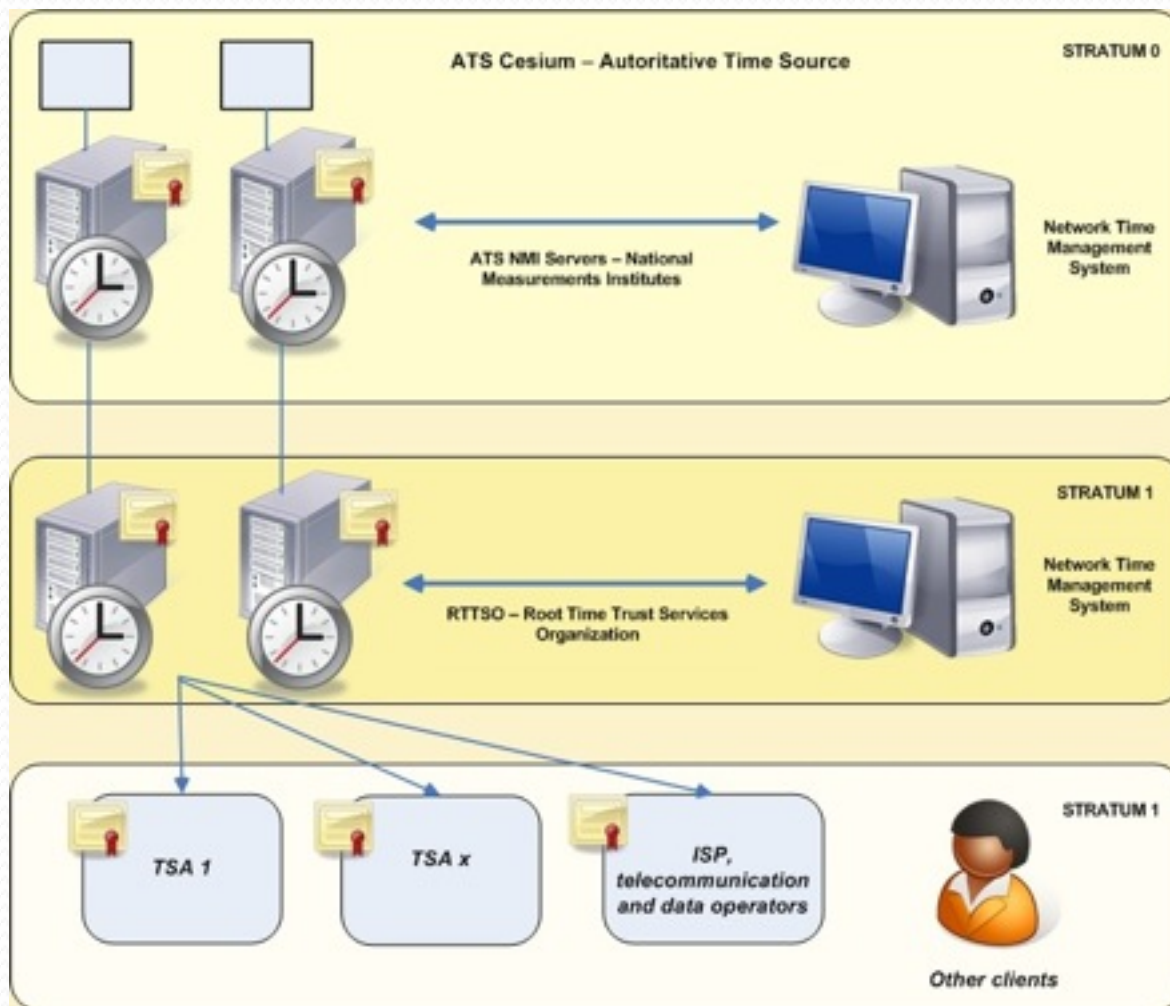
**RFC-3161**

Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)

**RFC-3628**

Policy Requirements for Time-Stamping Authorities (TSAs)

# Získání důvěryhodného času





# Příklady použití časového razítka

- Elektronické podatelny
- Elektronický podpis
- registry
- dlouhodobý důvěryhodný archiv
- mailové servery a mailová komunikace
- kanály elektronického bankovníctví
- notářské systémy
- databáze a archivační programy
- auditní záznamy
- certifikační authority
- programy a aplikace se zvýšenými nároky na bezpečnost

# Certifikát X časové razítko

## Certifikát

**Předmět:**

Pepa Novák

---

**Vydal:**

Certifikační autorita

Sériové číslo: 1234567

Platnost:

---

**Veřejný klíč:**

FAABBE45BB2FDA...

---

El. podpis:



## Časové razítko

**Vydal:**

TSA

Sériové číslo: 1234

Čas:

---

**Hash z dokumentu:**




SHA-1,FE3445BB2FDA...

---

El. podpis:



# PKI – Atributový certifikát

Certifikát	Časové razítko	Atributový certifikát	DV-certifikát
<b>Předmět:</b> Pepa Novák		<b>Držitel:</b> Pepa Novák	<b>Držitel:</b> Pepa Novák
<b>Vydal:</b> Certifikační autorita Sériové číslo: 1234567 Platnost:	<b>Vydal:</b> TSA Sériové číslo: 1234 Čas:	<b>Vydal:</b> Atributová autorita Sériové číslo: 9876543 Platnost:	<b>Vydal:</b> DVCS Sériové číslo: 9876543 Platnost:
<b>Veřejný klíč:</b> FAABBE45BB2FDA...	<b>Hash z dokumentu:</b> SHA-1, FE3445BB2FDA...	<b>Atributy:</b> blabla..	<b>Hash z dokumentu:</b> SHA-1, FE3445BB2FDA...
El. podpis: 	El. podpis: 	El. podpis: 	El. podpis: 

Atributový certifikát zobecňuje mechanismus certifikátu veřejného klíče.

Místo veřejného klíče jsou v něm jiné údaje o držiteli certifikátu (mluvíme o tzv. **atributech**).

Atributovým certifikátem aplikaci sdělujeme svá přístupová práva.





AC vydává **atributová autorita (AA)**.

Samotným **atributovým certifikátem nelze prokázat totožnost držitele** a vystavují se na kratší dobu.

O atributových certifikátech pojednává **RFC 3281**.

RFC-3281. An Internet Attribute Certificate Profile for Authorization. The Internet Society (2002)

# PKI – DV certifikát resp. DV časové razítko

Certifikát	Časové razítko	Atributový certifikát	DV-certifikát
<b>Předmět:</b> Pepa Novák		<b>Držitel:</b> Pepa Novák	<b>Držitel:</b> Pepa Novák
<b>Vydal:</b> Certifikační autorita Sériové číslo: 1234567 Platnost:	<b>Vydal:</b> TSA Sériové číslo: 1234 Čas:	<b>Vydal:</b> Atributová autorita Sériové číslo: 9876543 Platnost:	<b>Vydal:</b> DVCS Sériové číslo: 9876543 Platnost:
<b>Veřejný klíč:</b> FAABBE45BB2FDA...	<b>Hash z dokumentu:</b> SHA-1,FE3445BB2FDA...	<b>Atributy:</b> blabla..	<b>Hash z dokumentu:</b> SHA-1,FE3445BB2FDA...
El. podpis: 	El. podpis: 	El. podpis: 	El. podpis: 

**DV-certifikát (DV = data validation) slouží jako důkaz o držení dokumentu bezprostředně před časem uvedeným v DV-certifikátu.**

Tento typ certifikátu se také někdy označuje jako **DV-časové razítko**, kromě toho mohou DV-certifikáty jiných typů sloužit k:

- důkazu pravosti elektronických podpisů
- důkazu pravosti celého dokumentu
- důkazu pravosti certifikátu

DV-certifikáty vydává **DVCS (Data Validation Certificate Server)**