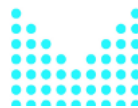




## Zaručený elektronický podpis (eGON)



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

**PODPORUJEME  
VAŠI BUDOUCNOST**  
[www.esfcr.cz](http://www.esfcr.cz)

## Rozsah:

8 hodin

## Anotace:

Tento eLearningový kurz je určen k seznámení se základní problematikou elektronického podpisu (typy, principy) a využití elektronického podpisu v praxi.

## Průvodce kurzem:

eLearningový kurz Zaručený elektronický podpis obsahuje základní problematiku digitálních podpisů, jejich typy, principy a použití. Dále nás seznámí s certifikačními autoritami působících v České republice a ověřování platnosti elektronických podpisů.

## Seznam modulů:

- Zaručený elektronický podpis

## Přílohy ke kurzu:

- žádné

## Obsah modulu Zaručený elektronický podpis

1	Úvod do kurzu.....	5
2	Co je elektronický podpis .....	5
3	Právní úprava.....	8
4	Certifikát veřejného klíče .....	8
5	Poskytovatel certifikačních služeb neboli certifikační autorita .....	10
6	Proces získání certifikátu .....	11
7	Podepisování a ověření podpisu.....	13
8	Jak funguje elektronický podpis .....	15
9	Ochrana certifikátu před zneužitím .....	19
10	Další nástroje využívající technologii elektronického podpisu.....	21
11	Informační zdroje.....	22
12	Souhrn .....	22

# **MODUL: Zaručený elektronický podpis**

## **I. Úvod do problematiky zaručeného elektronického podpisu**

- Vysvětlení základních pojmů zaručeného elektronického podpisu
- Elektronická značka
- Právní úprava elektronického podpisu v ČR
- Typy elektronických podpisů
- Principy digitálního podpisu

## **II. Využití zaručeného elektronického podpisu v praxi**

- Vydávání a správa certifikátů
- Certifikační autority
- Ověřování platnosti certifikátu a digitálního podpisu
- Technologická řešení elektronického podpisu
- Čipové karty
- Časová razítka
- Digitálně zabezpečené poštovní zprávy
- Praktická ukázka úkolu k vytvoření a ověření platnosti elektronického podpisu.

Cílem kurzu je seznámit vedoucí úřadů, vedoucí úředníky a úředníky územně samosprávných celků s platnou právní úpravou související se zaručeným elektronickým podpisem a jeho využitím v praxi.

# 1 Úvod do kurzu



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

PODPORUJEME  
VAŠI BUDOUCNOST  
[www.esfcr.cz](http://www.esfcr.cz)

Projekt je spolufinancován z ESF z OP LZZ Vzdělávání úředníků a zaměstnanců veřejné správy, metodiků a školitelů a politiků v oblasti zavádění eGovernmentu do veřejné správy,

reg. č. CZ.1.04/4.1.00/38.00001

Připravili jsme pro vás kurz o zaručeném elektronickém podpisu. Budeme se zabývat tím, co je elektronický podpis, jak si ho můžeme zřídit a jak ho budeme používat. Vysvětlíme si princip fungování elektronického podpisu a v té souvislosti se zmíníme o kryptografii. Budeme se věnovat i otázce ochrany certifikátu před zneužitím.

Na konci kurzu si můžete zkusit odpovědět na několik kontrolních otázek, abyste se přesvědčili, jak jste problematice zaručeného elektronického podpisu porozuměli.

## 2 Co je elektronický podpis

Elektronický podpis jsou data, která jsou připojena k dokumentu a která nahrazují vlastnoruční podpis. Vzniknul z potřeby vytvořit nástroj, který by v elektronických dokumentech plnil obdobnou funkci, jakou zajišťuje v listinných dokumentech podpis vlastnoruční.

Tento nástroj musí zajistit:

- **Autentičnost zprávy**, tedy jistotu, že zprávu podepsala osoba uvedená v certifikátu.
- **Integritu zprávy**, nebo-li to, že je možné snadno zjistit jakoukoliv následnou změnu zprávy.
- **Nepopíratelnost odpovědnosti podepsané osoby** - osoba, která zprávu podepsala, nemůže svou činnost popřít.

### PŘÍKLAD

Pokud mi přijde zpráva, která je elektronicky podepsána paní Marií Vomáčkovou, mohu se spolehnout na to, že zprávu podepsala skutečně paní Vomáčková, že od okamžiku podpisu zprávu nikdo nezměnil a také na to, že se paní Vomáčková, před tím než zprávu podepsala, seznámila s jejím obsahem.

Pro zajištění těchto požadavků se v ČR využívá tzv. „**zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb**“, který je definován zákonem č. 227/2000 Sb. o elektronickém podpisu. Tento podpis je v zákoně o elektronickém podpisu označován též jako „uznávaný elektronický podpis“.

**Pokud nebude výslovně uvedeno jinak, tak v dalším textu budeme pod pojmem elektronický podpis vždy rozumět tento uznávaný elektronický podpis.**



*Definice elektronického podpisu podle § 2 zákona č. 227/2000 Sb., o elektronickém podpisu: Elektronickým podpisem se rozumí 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.*

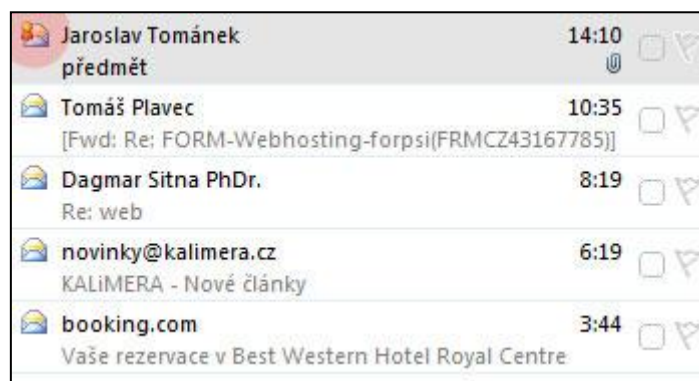
## 2.1 Jak vypadá elektronický podpis

### Jak vypadá elektronický podpis

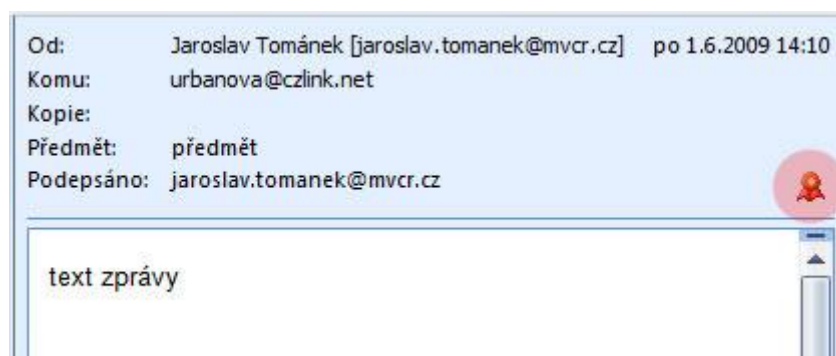
Elektronický podpis jako takový nemusí mít žádnou vizuální prezentaci, takže ve vlastním dokumentu nemusí být vůbec vidět. V různých aplikacích je elektronický podpis zpracováván různě. Některé aplikace sice vkládají do dokumentu viditelnou informaci o podpisu, ale takových aplikací je menšina. Často se elektronický podpis projeví například pouze zobrazením informační ikonky, pomocí které lze zobrazit podrobnosti o podpisu.

#### Ukázky:

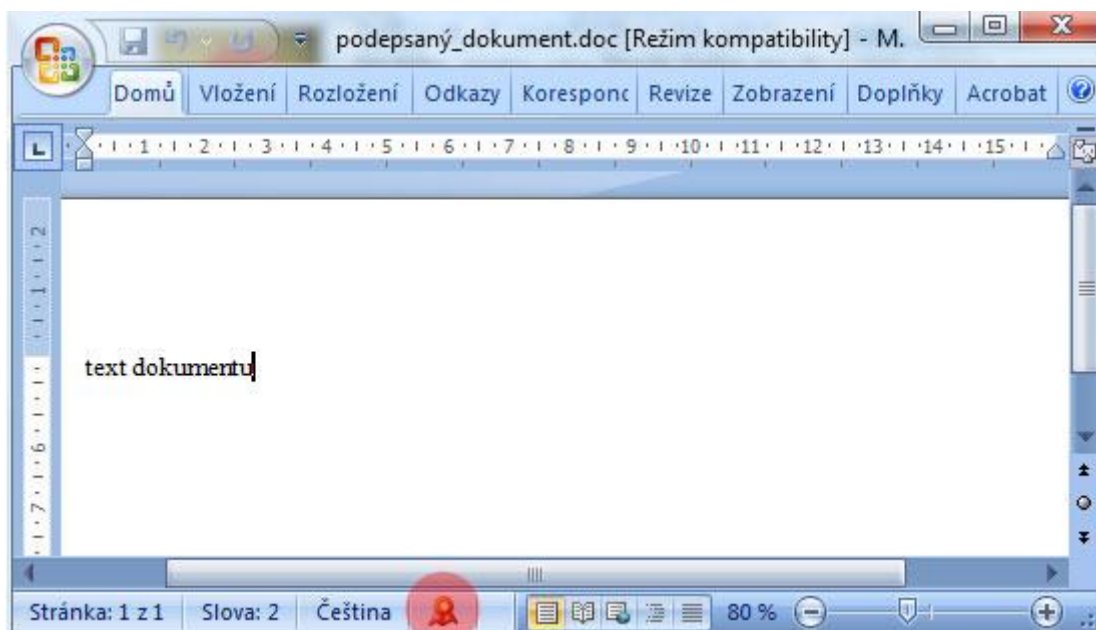
*Ikona označující el. podepsanou zprávu v přehledu zpráv aplikace MS Outlook 2007*



*Ikona označující, že zpráva je el. podepsána (MS Outlook 2007)*



Ikona označující el. podepsaný dokument (MS Word 2007)



Ukázka naskenovaného podpisu na faktuře – **toto není elektronický podpis ve smyslu zákona o elektronickém podpisu!!!**



## 2.2 Jak mohu elektronicky podepsat zprávu

### Jak mohu elektronicky podepsat zprávu

Pro to, aby se někdo mohl elektronicky podepisovat, musí nejprve získat tzv. certifikát. Poté je třeba tento certifikát nainstalovat do počítače. Vlastníme-li nainstalovaný certifikát, můžeme elektronicky podepisovat v programech, které podporují používání elektronického podpisu – např. MS Outlook, MS Word nebo Adobe Acrobat. Podepsání dokumentu je většinou realizováno kliknutím na příslušnou ikonu, nebo vybráním příslušné volby v menu aplikace a zadáním PINu nebo hesla k certifikátu. Jednotlivé pojmy jsou podrobně popsány v následujících kapitolách.

### 3 Právní úprava

Oblast elektronického podpisu je v rámci Evropské unie upravena Směrnicí 1999/93/EC Evropského parlamentu a Rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

Tato směrnice je do českého právního řádu transponována zákonem č. 227/2000 Sb., o elektronickém podpisu. Ten je základním právním předpisem upravující používání elektronického podpisu v ČR.

K tomuto zákonu existuje prováděcí vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, kterou se v rámci tohoto kurzu nebudeme zabývat, neboť její předmět úpravy se nevztahuje přímo na uživatele elektronického podpisu.

S elektronickým podpisem úzce souvisí problematika elektronických podatelů, která je upravena nařízením vlády č. 495/2004 Sb. k elektronickým podatelům a vyhláškou č. 496/2004 Sb. o elektronických podatelích.

Všechny tyto dokumenty jsou volně přístupné mimo jiné na webu Ministerstva vnitra, konkrétně na stránce <http://www.mvcr.cz/e-podpis-legislativa.aspx>

### 4 Certifikát veřejného klíče

V této kapitole se seznámíme

- s druhy certifikátů
- s úložišti certifikátů

Pro elektronické podepisování je nutné vlastnit tzv. certifikát. Certifikát je datový soubor, který obsahuje informace o osobě, které je vydán a tzv. veřejný klíč, což jsou data potřebná k ověření elektronického podpisu.

#### 4.1 Druhy certifikátů

Existuje několik druhů certifikátů. Z hlediska elektronického podpisu nás zajímá především dělení na kvalifikované a nekvalifikované certifikáty.

#### Kvalifikované certifikáty

Kvalifikovaný certifikát je certifikát, který byl vydán podle zákona o elektronickém podpisu a který se používá výhradně pro účely elektronického podepisování. Pokud tedy chceme používat elektronický podpis, musíme si pořídit právě tento certifikát.



## Nekvalifikované certifikáty

Kromě kvalifikovaných certifikátů existuje řada dalších certifikátů, které se používají například pro autentizaci, šifrování a další procesy. Tyto certifikáty se často nazývají také komerční. Po technické stránce jsou velmi podobné kvalifikovaným certifikátům, ale liší se způsobem používání a právními účinky. Vydávání těchto certifikátů není upraveno žádným zákonem.

## 4.2 Úložiště certifikátů

Po zvolení druhu certifikátu, je dalším krokem vybrání tzv. úložiště certifikátu, tedy umístění, kde chceme mít certifikát uložen. Úložiště může být buď v počítači, na kterém se budeme chtít elektronicky podepisovat a nebo nějaký externí prostředek – nejčastěji čipová karta, nebo USB token.

### Softwarový certifikát

Pokud zvolíme variantu uložení certifikátu přímo v počítači, nazývá se takový certifikát také softwarový certifikát. Certifikát a především s ním svázané soukromé klíče (data pro vytváření elektronického podpisu) jsou uloženy do tzv. bezpečného úložiště operačního systému. Data uložená v tomto úložišti není možné zkopírovat jinam, takže ani v případě, kdy se k počítači dostane nepovolaná osoba, nehrozí nebezpečí, že by si mohla zkopírovat soukromé klíče k certifikátu a použít je k podepisování.

*Výhody:*

- nízká cena – neplatíme za prostředek pro uložení

*Nevýhody:*

- přes určitou úroveň zabezpečení je tento způsob uložení považován za nejméně bezpečný
- nepřenositelnost – certifikát můžeme používat pouze v počítači, na kterém jsme si generovali žádost o vydání certifikátu (viz. další kapitola)
- pokud dojde k poškození počítače, nebo nutnosti přinstalovat operační systém, dojde ke ztrátě soukromých klíčů

### Čipová karta

Čipová karta je plastická karta formátu kreditní karty se zabudovaným kontaktním čipem, na kterém se vytváří a uchovávají soukromé klíče. Běžně používané čipové karty jsou navrženy tak, aby soukromé klíče nikdy neopustily čipovou kartu a čipová karta je tak, velmi bezpečným úložištěm.

*Výhody:*

- bezpečnost
- přenositelnost – karta není vázána na jeden počítač, lze ji použít na jakémkoliv počítači vybaveném čtečkou čipových karet

- čipová karta lze snáze udržet pod výhradní kontrolou uživatele, než například počítač v kanceláři

*Nevýhody:*

- cena – je nutné zakoupit kartu a vybavit se čtečkou

## **USB token**

USB token je zařízení podobné USB flash disku. Jak název napovídá, k počítači se připojuje prostřednictvím USB portu, kterým jsou dnes již vybaveny víceméně všechny počítače.

*Výhody:*

- bezpečnost
- přenositelnost – token není vázán na jeden počítač
- lze snáze udržet pod výhradní kontrolou uživatele, než například počítač v kanceláři

*Nevýhody:*

- cena za token

## **5 Poskytovatel certifikačních služeb neboli certifikační autorita**

Kvalifikované certifikáty vydává takzvaný poskytovatel certifikačních služeb. Často se můžeme setkat i s pojmem certifikační autorita. Poskytovatel certifikačních služeb je subjekt, který je důvěryhodný pro uživatele certifikačních služeb, tj. pro podepisující osoby, kterým vydává certifikáty, a pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny.

Certifikační autorita zejména vydává certifikáty a zajišťuje jejich správu, včetně jejich zneplatňování. Vydané certifikáty podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci a je identifikovatelná jako subjekt, který je vydal.

V oblasti orgánů veřejné moci je možné používat pouze kvalifikované certifikáty vydané akreditovaným poskytovatelem certifikačních služeb. V současné době jsou v ČR akreditováni tři poskytovatelé:

- Česká pošta, s.p. – <http://qca.postsignum.cz>
- První certifikační autorita, a.s. – <http://www.ica.cz>
- eIdentity, a.s. – <http://www.ie.cz>

Aktuální přehled udělených akreditací je zveřejněn na webu Ministerstva vnitra v sekci Elektronický podpis na stránce <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

Každý z uvedených poskytovatelů má síť "poboček", na kterých vydává certifikáty. Těmto "pobočkám" se říká registrační autority.

## 5.1 Kořenové certifikáty poskytovatele certifikačních služeb

Každý poskytovatel certifikačních služeb má kvalifikované certifikáty, které používá k podepisování certifikátů, které vydává. Těmto certifikátům se říká **kořenové certifikáty**.

Tyto certifikáty má vystavené na svých webových stránkách a jsou dostupné i na dalších místech, která jsou popsána v certifikační politice. Všechny kořenové certifikáty ověřuje také Ministerstvo vnitra a publikuje je na svých stránkách. <http://www.mvcr.cz/clanek/vysledky-overeni-platnych-kvalifikovanych-systemovych-certifikatu-akreditovanych-poskytovatelu-certifikacnich-sluzeb.aspx>

Pokud jsou v počítači nainstalovány kořenové certifikáty certifikační autority, aplikace důvěřují certifikátům vydaným touto certifikační autoritou.

## 6 Proces získání certifikátu

V této kapitole se seznámíme s tím, co potřebujeme udělat, abychom získali certifikát.

Řekneme si něco o:

- Výběru poskytovatele certifikačních služeb
- Generování žádosti o certifikát
- Návštěvě registrační autority
- Instalaci certifikátů

### 6.1 Výběr poskytovatele certifikačních služeb

Hlavní kritéria, kterými by se měl žadatel o vydání certifikátu řídit při výběru certifikační autority, jsou následující:

- **Nabídka služeb** - Různí poskytovatelé certifikačních služeb mají různou nabídku typů certifikátů a úložišť. Je tedy třeba v první řadě zohlednit, zda certifikační autorita nabízí požadovaný typ certifikátu a požadovaný druh úložiště. Některé certifikační autority poskytují i zvýhodněné balíčky služeb (např. kvalifikovaný certifikát pro podepisování společně s komerčním certifikátem pro autentizaci a tokenem, nebo čipovou kartou a čtečkou), které mohou zákazníkovi ušetřit dost peněz.
- **Dostupnost registrační autority** - I když je certifikát datový soubor a technicky by bylo možné předání elektronicky, v praxi je nutná osobní návštěva osoby, pro kterou je certifikát vystavován, na registrační autoritě. Poskytovatel certifikačních služeb má totiž povinnost ověřit totožnost majitele certifikátu a všechny další údaje, které jsou v certifikátu uvedeny.

Proto je dobré zvolit poskytovatele, který má registrační autoritu v místě, které je pro majitele certifikátu dobře dostupné.

- **Certifikační politika** - Certifikační politika je veřejný dokument, ve kterém poskytovatel certifikačních služeb popisuje pravidla vydávání a používání certifikátů, kterými se musí řídit jak on sám, tak majitel certifikátu. Certifikační politiky jsou vystaveny na webech poskytovatelů certifikačních služeb.
- **Cena** - Cena se liší nejen u různých druhů certifikátů a úložišť, ale i u různých poskytovatelů certifikačních služeb. Ti mají na svých webových stránkách zveřejněny ceny, takže je možné ceny jednotlivých služeb snadno porovnat. Nutno však upozornit, že různí poskytovatelé nabízejí ke svým certifikátům různé služby, a tak může být pouhé porovnání cen někdy zavádějící.

## 6.2 Generování žádosti o certifikát

Po výběru poskytovatele certifikačních služeb můžeme přistoupit ke generování žádosti o certifikát. Pokud se rozhodneme pro jiné úložiště než úložiště v operačním systému, musíme mít už nyní toto úložiště k dispozici a generovat klíče přímo na něm.

### PŘÍKLAD

Pokud chci mít soukromé klíče ke svému certifikátu uložené na čipové kartě, musím si nejprve zakoupit tuto kartu (nejlépe přímo od certifikační autority, která mi bude vydávat certifikát). Po zakoupení a nainstalování karty mohu teprve generovat žádost o certifikát. Při generování žádosti se totiž soukromý klíč k certifikátu vytvoří přímo na kartě a nikdy ji neopustí.

Ke generování žádosti o certifikát slouží aplikace poskytnutá certifikační autoritou. Může to být aplikace umístěná přímo na webových stránkách poskytovatele, nebo aplikace, která se nainstaluje do počítače.

V této aplikaci se vyplní formulář obsahující údaje, které budou uloženy v certifikátu. Při vyplňování je potřeba dávat pozor na překlepy a vše vyplňovat přesně tak, jak je uvedeno na dokumentech, kterými budeme tyto údaje na registrační autoritě dokládat. Pokud by totiž při návštěvě registrační autority objevil pracovník registrační autority nějaký nesoulad, nesmí certifikát vydat.

Po vyplnění formuláře vygeneruje aplikace soukromé a veřejné klíče a žádost o certifikát. Žádost si uložíme a vezmeme s sebou na registrační autoritu.

## 6.3 Návštěva registrační autority

Po vygenerování žádosti je dalším krokem návštěva registrační autority. Na některých autoritách je nutné mít předem smlouvenou schůzku, na některé je možné přijít kdykoliv v otevírací době. Jak je již zmíněno v předchozím odstavci, na registrační autoritu si s sebou vezmeme vygenerovanou žádost a dokumenty dokládající údaje, které jsme uváděli do žádosti o certifikát. Je dobré si předem zjistit, jaké dokumenty daná autorita akceptuje – buď na webu, v certifikační politice, nebo dotazem na certifikační autoritu.

Pokud je při návštěvě registrační autority vše v pořádku, vydá nám operátor certifikát. Společně s ním můžeme obdržet další instrukce či aplikace a také tzv. kořenové certifikáty dané certifikační autority.

## 6.4 Instalace certifikátů

Obdržený certifikát si nainstalujeme do svého počítače. Pokud již nemáme nainstalované kořenové certifikáty certifikační autority, nainstalujeme i kořenové certifikáty. V prostředí MS Windows se certifikát nainstaluje dvuklikem na soubor s certifikátem (nejčastěji přípona .crt nebo .der). To spustí průvodce instalací certifikátu. Dále postupujeme podle pokynů na obrazovce.

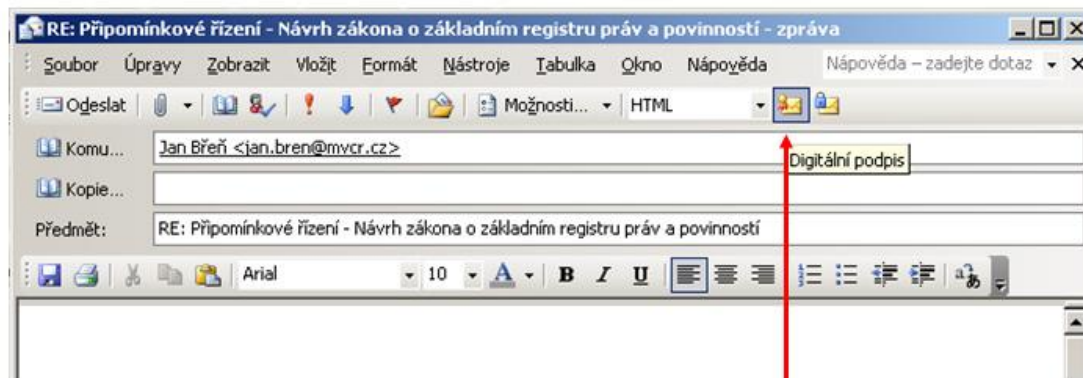
## 7 Podepisování a ověření podpisu

### Podepisování

K podepisování potřebujeme aplikaci, která podporuje práci s elektronickým podpisem. Nejvíce rozšířené u nás jsou např. aplikace sady Microsoft Office (např. poštovní klient Microsoft Outlook, nebo textový editor MS Word) a Adobe Acrobat.

V každé aplikaci se podepisuje poněkud odlišně, většinou je však podepsání dokumentu otázkou kliknutí na ikonku, nebo zvolením položky v menu a vyplněním hesla k certifikátu, nebo PINu k čipové kartě, na které je certifikát uložen.

Certifikáty musí být vždy používány v souladu s certifikační politikou, kterou majitel certifikátu obdrží od poskytovatele certifikačních služeb, případně získá z jeho webových stránek.



Podepsání zprávy v MS Outlook - kliknutí na ikonu a zadání PINu, kterým je chráněn certifikát.

### Ověření podpisu

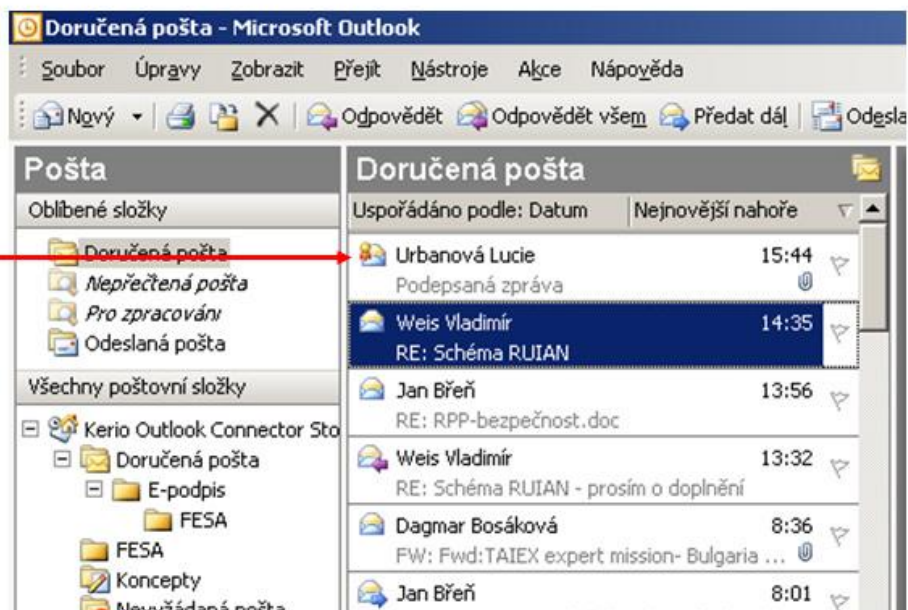
Při ověřování podpisu se ověřuje následující:

- Integrita dokumentu – dokument nebyl od okamžiku podpisu změněn (ověřuje aplikace)
- Vydavatel certifikátu – certifikát, na kterém je založen podpis vydala certifikační autorita, které důvěřujeme (tj. máme nainstalovány její kořenové certifikáty v systémovém úložišti kořenových certifikátů důvěryhodných certifikačních autorit)
- Platnost kořenového certifikátu certifikační autority – ověřuje se interval platnosti a to, že certifikát nebyl zneplatněn, pokud je více nadřizovaných certifikátů, ověřují se takto všechny nadřizované certifikáty
- Platnost certifikátu, na kterém je založen podpis – ověřuje se interval platnosti a to, že certifikát nebyl zneplatněn
- Komu byl certifikát vydán (vždy ověřuje uživatel, nikdy aplikace)

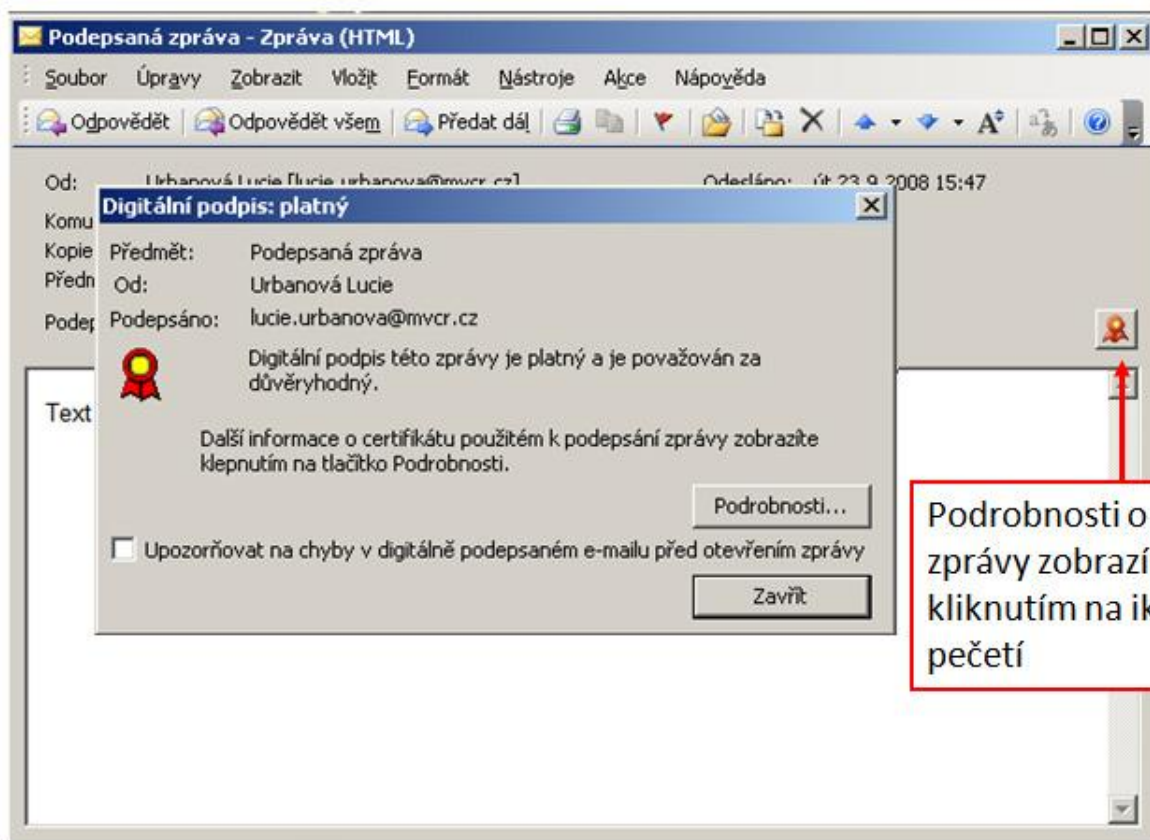
Pakliže máme nainstalovány příslušné kořenové certifikáty, dokáže většinu těchto úkonů automatizovaně zajistit aplikace.

## Ověření podpisu v Outlooku

V MS Outlook je zpráva označena ikonkou s pečetí. Obdobně v dalších aplikacích.



## Podrobnosti podpisu



Podrobnosti o podpisu zprávy zobrazím kliknutím na ikonku s pečetí

## 8 Jak funguje elektronický podpis

Abychom si mohli popsat, jak funguje elektronický podpis, musíme si nejprve alespoň zhruba vysvětlit dvě výpočetní operace, které jsou v elektronickém podpisu využívány. Těmito operacemi je tzv. vytvoření otisku zprávy a asymetrická kryptografie (šifrování).

## 8.1 Vytvoření otisku zprávy

Protože při vytváření elektronického podpisu jsou používány velmi složité matematické algoritmy (asymetrické šifrování), bylo by výpočetně velmi náročné provádět tyto matematické operace s celou dlouhou zprávou. Proto se využívá tzv. otisk neboli hash zprávy. Otisk (hash) se vytváří tzv. hashovací funkcí neboli hashovacím algoritmem.

### Hashovací algoritmus má několik zajímavých vlastností:

- Jeho pomocí lze z libovolně dlouhého souboru vypočítat řetězec o stejné délce. Tomuto řetězci se říká otisk zprávy, neboli hash.
- I nepatrná změna vstupních dat způsobí velkou změnu otisku.
- Funkce je jednosměrná. To znamená, že ze zprávy dokážeme spočítat otisk, ale naopak z otisku zprávu spočítat nedokážeme.

### Ukažme si to na praktickém příkladě:

	Vstupní text	Otisk vytvořený algoritmem SHA-1
<b>A</b>	Dohodnutá kupní cena je 10 000 Kč.	93c038d1a6ca429ba9077bdb90e9b413309109ab
<b>B</b>	Dohodnutá kupní cena je 100 000 Kč.	720b1abbe5e55a1049870d806dc6d7bc1e14b042
<b>C</b>	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque faucibus imperdiet eros, a ultricies quam varius in. Maecenas accumsan, diam sit amet blandit sagittis, velit sapien luctus tortor, ut rutrum nisi orci nec nisl. Sed vel tempus erat. Phasellus luctus eleifend leo, vel lobortis ligula ultricies et.	d30a78918564e3a37f02ecb6c0b08d4c27f7f6e2

### Komentář k tabulce:

Z ukázky je vidět, že ačkoliv vstupní řetězce jsou různě dlouhé, otisk má vždy stejnou délku. Nyní se podívejme na text A a na text B. Oba tyto texty jsou velmi podobné, do textu B byla pouze dopsána jedna nula navíc. Podíváme-li se na otisky těchto textů, vidíme, že jsou naprosto odlišné.

### 8.1.1 Konkrétní hashovací algoritmy

Hashovacích algoritmů existuje několik a všechny mají společné výše uvedené vlastnosti. V současné době se v elektronickém podpisu využívá pro vytvoření otisku podepisované zprávy algoritmus SHA-1. SHA je zkratka pro Secure Hash Algorithm, tedy bezpečný hashovací algoritmus. Funkce SHA-1 vytváří otisky o délce 128 bitů. V současné době je algoritmus SHA-1 stále dostatečně bezpečný avšak se zvyšující se výkonností počítačů není možné spoléhat na to, že algoritmus SHA-1 bude odolávat útokům neustále.

Proto už byla vyvinuta nová rodina hashovacích funkcí, která se označuje SHA-2. Součástí rodiny SHA-2 jsou čtyři funkce a to SHA-224, SHA-256, SHA-384 a SHA-512. Číslo v označení funkce udává,



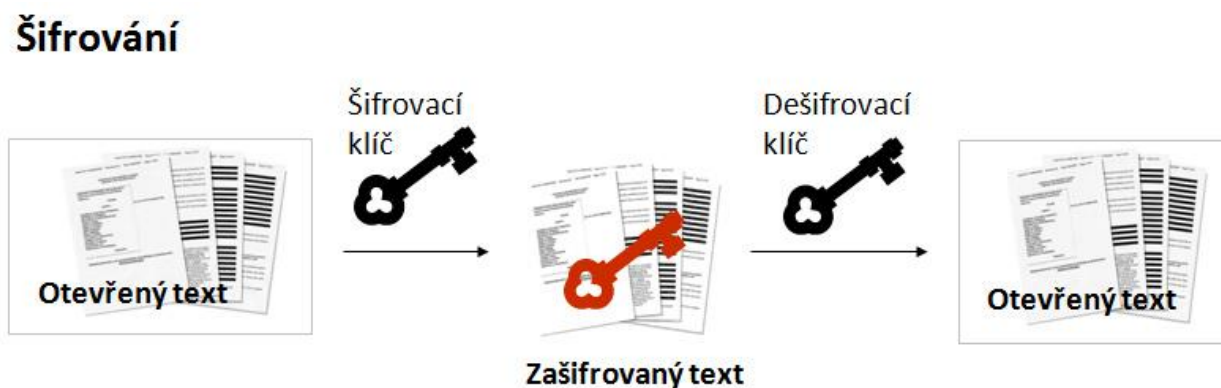
jak dlouhý otisk funkce vytváří. U SHA-256 je to tedy např. 256 bitů. Na přelomu roku 2009 a 2010 bude i Česká republika přecházet na bezpečnější algoritmy a po Novém roce tak již budou všechny nové kvalifikované certifikáty vytvářeny pouze s využitím funkcí rodiny SHA-2.

Více informací: [http://cs.wikipedia.org/wiki/Kryptografická\\_hashovací\\_funkce](http://cs.wikipedia.org/wiki/Kryptografická_hashovací_funkce)

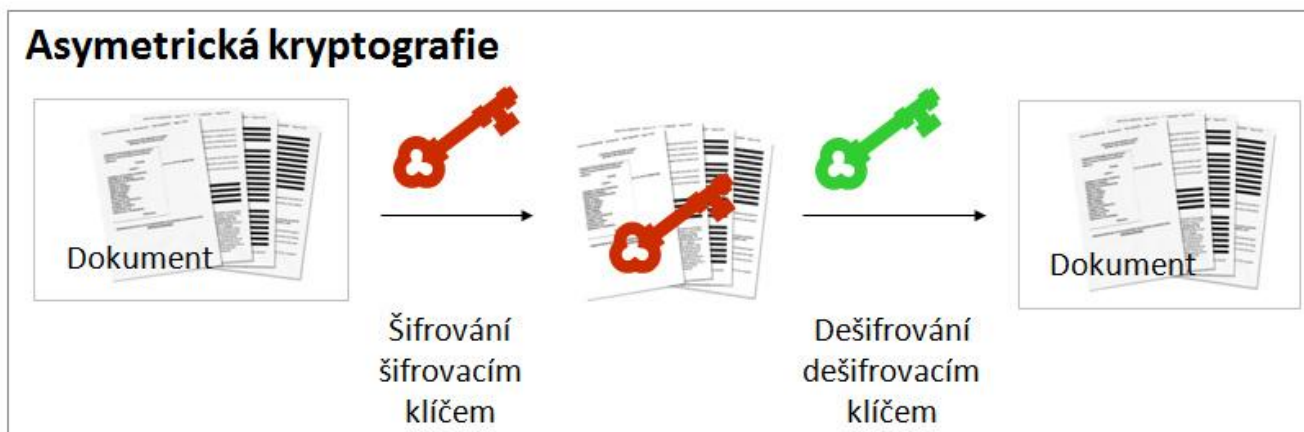
## 8.2 Asymetrická kryptografie

Další operací využívanou při elektronickém podepisování je šifrování, neboli kryptografie. A konkrétně asymetrická kryptografie. Co to konkrétně znamená? Jak jsme si již pověděli, kryptografie je šifrování. Princip šifrování je takový, že pokud chce někdo poslat zašifrovanou zprávu, musí mít k dispozici text zprávy (nezašifrovanému textu se říká také otevřený text) a šifrovací klíč. Tento text zašifruje šifrovacím klíčem a odešle příjemci. Příjemce přijme zašifrovanou zprávu a pokud má správný dešifrovací klíč, může zprávu dešifrovat a získat zpět otevřený text.

*Šifrování*



To je tedy šifrování. Co se týká rozdílu mezi symetrickým a asymetrickým šifrováním, ten spočívá v tom, že při symetrickém šifrování se používá pro šifrování a dešifrování stejný klíč, zatímco u asymetrického šifrování se šifruje jiným klíčem než dešifruje. A právě dvojice různých klíčů se s výhodou užívá při elektronickém podepisování.



Pro vytváření elektronického podpisu se používá šifrovací algoritmus RSA (podle autorů - Rivest, Shamir, Adleman). Více informací o tomto algoritmu se dá v češtině nalézt např. na stránce <http://cs.wikipedia.org/wiki/RSA>

### 8.3 Jak to celé funguje

Ted' už tedy víme, co to je otisk zprávy i asymetrické šifrování a tak si konečně můžeme vysvětlit, jak probíhá celý proces podepisování. Elektronický podpis totiž není nic jiného než zašifrovaný otisk zprávy.

#### Podepisování

Princip elektronického podepisování (ověření elektronického podpisu) je znázorněn na následující animaci. Kliknutím na animaci se vždy přesunete na další krok procesu. Vysvětlení jednotlivých kroků najdete v textu pod animací.

1. Na začátku všeho je dokument, který chceme podepsat. Z tohoto dokumentu se spočte otisk. Podepisuje se pouze tento otisk a nikoliv celá zpráva, neboť šifrování dlouhých dokumentů by bylo nesmírně výpočetně náročné.
2. Poté je tento otisk zašifrován šifrovacím klíčem. Šifrovací klíč, který se používá k vytváření podpisu, podepisující osoba s nikým nesdílí a drží ho stále pod svou kontrolou (na čipové kartě, tokenu, v počítači). Proto se tomuto klíči říká také soukromý neboli privátní. Tento zašifrovaný otisk je vlastní elektronický podpis.

3. Tento elektronický podpis se připojí k dokumentu.
4. Dále je k dokumentu připojen kvalifikovaný certifikát podepisující osoby, pomocí kterého příjemce zprávy může ověřit podpis. Certifikát obsahuje údaje o podepisující osobě a tzv. veřejný klíč. O tom více v popisu další animace věnující se ověření podpisu.

## Ověření podpisu

Ověřující osoba přijala dokument, ke kterému je připojen elektronický podpis a kvalifikovaný certifikát. Ověření probíhá ve třech krocích:

1. Spočítá se otisk z dokumentu.
2. Podpis (který je, jak už jsme si řekli, vlastně zašifrovaným otiskem zprávy) se dešifruje dešifrovacím klíčem, který je součástí kvalifikovaného certifikátu (protože tento klíč se vždy předává společně s podpisem, aby si příjemce mohl podpis ověřit, říká se mu veřejný klíč). Výsledkem je dešifrovaný otisk původní zprávy.
3. Nakonec jsou tyto dva otisky porovnány. Pokud otisky souhlasí, znamená to, že:
  - Zpráva nebyla od okamžiku podepsání změněna. Pokud by byla změněna, pak by se její otisk od původního velmi lišil.
  - Zprávu podepsala osoba, která vlastní soukromý klíč k veřejnému klíči, který je součástí přiloženého certifikátu, tedy osoba uvedená v certifikátu.

Pokud vám text této kapitoly přišel složitý a nesrozumitelný, nezoufejte. Oba tyto procesy, jak podepisování, tak ověřování, jsou v aplikacích pracujících s elektronickým podpisem automatizovány a k prostému používání elektronického podpisu je tedy nezbytně znát nepotřebujete.

## 9 Ochrana certifikátu před zneužitím

Stejně jako u většiny jiných elektronických služeb i u elektronického podpisu panují u některých lidí obavy z jeho zneužití. Podívejme se tedy na to, jak je certifikát chráněn.

Povíme si o

- Fyzické ochraně
- Heslu či PINu
- Zneplatnění certifikátu

### 9.1 Fyzická ochrana

Majitel certifikátu je povinen udržet data pro vytváření elektronického podpisu pod svou výhradní kontrolou. To je velmi dobře realizovatelné zejména při použití externích úložišť (čipová karta, token), které je možné nosit u sebe, nebo uložit na bezpečné místo. Pokud používáme softwarový certifikát, který máme uložený na počítači, ke kterému mají přístup i další osoby, měli bychom se snažit dodatečně chránit přístup k tomuto počítači, např. dostatečně silným heslem, které nebudeme s nikým sdílet ani uchovávat v blízkosti tohoto počítače.



§ 5 zákona č. 227/2000 Sb., o elektronickém podpisu, odst. 1, písm. a) stanoví: *Podpisující osoba je povinna zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití.*

## 9.2 Heslo či PIN

Druhým stupněm ochrany je ochrana heslem nebo PINem. V případě, že by se někdo zmocnil našeho certifikátu, neznamená to automaticky, že ho může využít k podepisování dokumentů naším jménem. Většina certifikátů je totiž chráněna ještě heslem, nebo PINem. Na zadání správného hesla či PINu může být omezený počet pokusů. Záleží na konkrétním druhu certifikátu. Pokud se tedy potenciální útočník nezmocní zároveň hesla či PINu, je majitel certifikátu chráněn touto cestou. Na tomto místě je dobré znovu varovat před zapisováním PINů či hesel. Pokud si tyto údaje musíme zapisovat, je nutné je uchovávat na bezpečném místě odděleně od certifikátu.

## 9.3 Zneplatnění certifikátu

Posledním stupněm ochrany je tzv. zneplatnění certifikátu. Zneplatnění certifikátu je úkon, který můžeme přirovnat k zablokování platební karty a přistupujeme k němu tehdy, když máme podezření, že by mohlo dojít ke zneužití certifikátu (například když ztratíme token nebo čipovou kartu). V tom případě zákon ukládá povinnost tuto skutečnost oznámit poskytovateli certifikačních služeb, který certifikát zneplatní.



§ 5 zákona č. 227/2000 Sb., o elektronickém podpisu, odst. 1, písm. b) stanoví: *Podpisující osoba je povinna uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu.*

### Jak probíhá zneplatnění certifikátu

Po oznámení podezření na možnost kompromitace certifikátu a tzv. hesla pro zneplatnění (toto heslo si majitel volí při žádosti o vydání certifikátu) poskytovateli certifikačních služeb, vloží poskytovatel certifikačních služeb údaje o zneplatnění certifikátu (zejména sériové číslo zneplatněného certifikátu) na tzv. seznam zneplatněných certifikátů, neboli CRL (certificate revocation list). Tento CRL vydává každý poskytovatel certifikačních služeb několikrát denně a publikuje ho na internetu, takže aplikace, které ověřují platnost certifikátu mají k tomuto seznamu přístup a mohou tak u každého ověřovaného certifikátu zjistit, zda nebyl zneplatněn. Na CRL zůstávají zneplatněné certifikáty minimálně do konce jejich původní platnosti.

### PŘÍKLAD

Certifikát je vydán s platností od 1.2.2010 15:54:26 do 1.2.2011 15:54:26. Pokud 15. 2. 2010 ztratím čipovou kartu s certifikátem a jsem nucena certifikát zneplatnit, vloží certifikační autorita údaje o zneplatnění tohoto certifikátu na nejbližší vydaný CRL a na každý další vydávaný CRL minimálně do 1.2.2011 15:54:26.

Zabezpečení certifikátu je tedy srovnatelné se zabezpečením platebních karet. Technické zabezpečení

však musí vždy jít ruku v ruce s určitou zodpovědností osoby, které byl certifikát vydán. Pokud si tedy někdo například nechává ve čtečce kartu s kvalifikovaným certifikátem a poblíž má poznamenaný PIN, tak kompromitaci certifikátu nezabrání ani sebedokonalejší technologie.

## 10 Další nástroje využívající technologii elektronického podpisu

### Elektronická značka

Pokud elektronický podpis přirovnáme k vlastnoručnímu podpisu, tak elektronickou značku si můžeme představit jako obdobu otisku razítka. Technologicky jsou elektronický podpis a elektronická značka velmi podobné, hlavní rozdíl je v legislativní stránce.

Nejlépe si elektronickou značku představíme, srovnáme-li ji s elektronickým podpisem a ukážeme-li si, v čem se od sebe liší.

### Certifikát

Elektronický podpis je založen na kvalifikovaném certifikátu, elektronická značka na kvalifikovaném systémovém certifikátu. Technicky jsou oba tyto druhy certifikátu velmi podobné, liší se zejména označením přímo v certifikátu a každý z těchto certifikátů je vydáván podle jiné certifikační politiky.

### Automatizace

Zatímco u elektronického podpisu se má za to, že se podepisující osoba před podpisem s dokumentem seznámila, označování elektronickou značkou může probíhat automatizovaně. Například informační systém elektronické podatelny může automatizovaně označovat doručky doručených zpráv.

### Osoba, které je certifikát vydáván


Kvalifikovaný certifikát, na kterém je založen elektronický podpis, je vždy vydáván fyzické osobě, kdežto kvalifikovaný systémový certifikát, na němž je založena elektronická značka, může být vydán jak fyzické, tak právnické osobě.

### Časové razítko

Kvalifikované časové razítko je důkaz o tom, že dokument existoval před časovým okamžikem uvedeným v časovém razítku. Na rozdíl od elektronického podpisu, které po opatření příslušného certifikátu vytváří přímo "uživatel", kvalifikovaná časová razítka vydává vždy pouze poskytovatel certifikačních služeb, který disponuje příslušným vybavením, zejména velmi přesným měřidlem času, které je navázáno na koordinovaný světový čas.

Časová razítka nejsou nabízena jednotlivě, ale jako služba. Odběratel nejprve podepíše smlouvu s poskytovatelem certifikačních služeb a po té je mezi nimi vytvořen komunikační kanál, kterým

odběratel posílá tzv. otisky dokumentů (viz. níže), ke kterým poskytovatel certifikačních služeb vydává časová razítka. Podle počtu vydaných razítek pak odběrateli fakturuje služby.

 § 2 zákona č. 227/2000 Sb., o elektronickém podpisu, písm. r): kvalifikovaným časovým razítkem se rozumí 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.

Kvalifikované časové razítko umožňuje ověření elektronického podpisu i po uplynutí doby platnosti certifikátu, na kterém je podpis založen.

## 11 Informační zdroje

<http://www.postsignum.cz>

## 12 Souhrn

V tomto kurzu jsme se věnovali problematice zaručeného elektronického podpisu.

Seznámili jsme se s tím, **co je elektronický podpis** a jaké má náležitosti.

Zmínili jsme se o **legislativní úpravě**.

Popsali jsme si proces **získávání** certifikátu a dále jeho **použití**.

Zabývali jsme se i **ochranou** certifikátu **před zneužitím**.