# Projekt využití elektronického podpisu v podnikové komunikaci

Project of usage of the elektronic signature in a company comunication

Martin Pilař

Bakalářská práce
2007



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2006/2007

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Martin PILAŘ** |
| Studijní program: | **B 3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Téma práce: | **Projekt využití elektronického podpisu v podnikové komunikaci.** |

Zásady pro vypracování:

**1. Vyhledejte vhodné zdroje řešící problematiku elektronického podpisu a jeho implementace do prostředí organizace.**
**2. Analyzujte současné produkty a technologické možnosti.**
**3. Navrhněte různá implementační řešení a tato vzájemně porovnejte.**
**4. Vyhodnoťte úspěšnost řešení a definujte silná a slabá místa projektu.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:


1. **Zákon 227/2000 sb. o elektronickém podpisu**
2. **www.ica.cz**
3. **Dobda Luboš, Ochrana dat v informačních systémech**
4. **Úřad pro ochranu osobních údajů, www.uoou.cz**
5. **www.mir.cz**
6. **Směrnice Evrovpského parlamentu a rady 1999/93/ES**


Vedoucí bakalářské práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **13. února 2007**

Termín odevzdání bakalářské práce: **29. května 2007**

Ve Zlíně dne 13. února 2007

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.

doc. RNDr. Vojtěch Křesálek, CSc

## ABSTRAKT

V této práci se zabývám využitím elektronického podpisu zejména v podnikové komunikaci. Přibližuji zde problematiku podpisu, jeho právní úpravou v české republice, jeho technickými normami. Dále zde osvětluji využívané kryptografické algoritmy, v další kapitole se věnuji prostředkům bezpečnému uložišti pro elektronický klíč a jejich vlastnostem využívané zejména v podnicích, navazující kapitola popisuje certifikační autority v české republice.


Klíčová slova: Elektronický podpis, Šifrování, Poskytovatel certifikačních služeb, Certifikát, USB Token, eAcoount


## ABSTRACT

I deal with usage of an elektronic signature in company komunication in this work. I explain the problemation of elektronic signature, legal regulations in Czech Republic and technical norms. Next part of the work explain cryptography algorithms which is usage, next chapter explain resources of safety place for elektronic key which is usage in company. Last chapter describes certification authority which acting in Czech Republic.


Keywords: Elektronic signature, Encryption, Provider of certification service, Certificate, USB Token, eAccount

Děkuji svému vedoucímu bakalářské práce doc., Mgr. Romanu Jaškovi Phd., za odborné vedení, rady a věcné připomínky, které mi poskytoval během práce. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi dostávalo během studia.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

# OBSAH

# ÚVOD

Již několik století je institut podpisu používán a ve všech právních systémech akceptován, jako potvrzení souhlasu s dokumentem. Tím, že se pod dokument podepíšeme nepopiratelně stvrzujeme, že jsme se s jeho obsahem obeznámili a že jej akceptujeme. „Klasický“ podpis naprosto dostačoval při komunikaci za použití papíru, nebo jiného fyzického média. V průběhu 80. let se v důsledku značných technologických inovací a poklesu cen informačních technologií začala rozvíjet komunikace elektronická. Nejdříve byla využívána jen pro sporadické posílání zpráv mezi technologickými nadšenci a „vyvolenými,“ kteří si mohli dovolit luxus počítače. V průběhu času se ale rozšířila mezi široké obyvatelstvo, stala se nepostradatelnou pro chod firem i pro orgány veřejné správy. V neposlední řadě začala výhody elektronické komunikace využívat i veřejná správa. Pro zrychlení průběhu různých správních řízení, podávání formulářů a vyřizování žádostí se snaží vlády všech vyspělých zemí zavádět elektronické podatelny, to si zde popíšeme podrobněji. Ty by měly pomoci občanům od dlouhých front na úřadech a úřadům zas od přehlcení v posledních dnech termínů pro odevzdávání např. daňových přiznání. Kompletní elektronická dokumentace by rovněž měla zefektivnit a zprůhlednit průběhy řízení i způsob vykonávání veřejné moci a komunikaci mezi státy evropské unie.

# I. TEORETICKÁ ČÁST

# 1 VYSVĚTLENÍ ZÁKLADNÍCH POJMŮ

## 1.1 Poskytovatel certifikačních služeb ( certifikační autorita)

Poskytovatel certifikačních služeb je autorita, která je důvěryhodná pro uživatele certifikačních služeb, tj. je důvěryhodná jak pro podepisující osoby, kterým vydává certifikáty, tak pro osoby, které se spoléhají na podpisy, s nimž jsou tyto certifikáty spojeny. Certifikační autorita zejména vydává certifikáty, za stanovených podmínek je zneplatňuje a vydává CRL (viz Certificate Revocation List).

Vydané certifikáty a CRL podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci, a je identifikovatelná jako subjekt, který je vydal. Certifikační autorita může některé činnosti zajišťovat prostřednictvím jiných subjektů, např. služby registračních autorit (viz Registrační autorita), vždy však na ní zůstává odpovědnost za poskytované služby. Certifikační autorita může prostřednictvím jiných subjektů zajišťovat i vydávání certifikátů, vždy však data pro vytváření elektronického podpisu (soukromý klíč), kterým jsou tyto certifikáty podepisovány, musí být identifikovatelná jako náležející certifikační autoritě a certifikační autorita je odpovědná za náležité zacházení s nimi.

## 1.2 Certifikát (Kvalifikovaný certifikát)

Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby. Jedná se o datovou zprávu, která je vydána poskytovatelem certifikačních služeb a která spojuje data pro ověřování podpisu s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují.

Vydáním certifikátu poskytovatel stvrzuje, že data pro ověřování elektronického podpisu patřící určité osobě a že ve spojení s daty pro vytváření elektronického podpisu podepisující osoby vykonávají požadované funkce.

Certifikát tedy představuje spojení mezi daty pro ověřování elektronického podpisu a identitou určité osoby. Identitu podepisující osoby podle typu certifikátu může poskytovatel zjišťovat různými způsoby, v některých případech postačí emailová adresa, v jiných je nutné osobně prokázat totožnost příslušnými doklady. Zákon o elektronickém

podpisu neupravuje jiné předávání dat pro ověřování elektronického podpisu než prostřednictvím kvalifikovaných certifikátů.

## 1.3 Časové razítko

Časové razítko je údaj, který lze přidat k elektronicky podepsané datové zprávě a který stvrzuje, že datová zpráva existovala dříve, než k ní bylo toto razítko přidáno. Takové stvrzení musí učinit někdo důvěryhodný a nezávislý na podepisující osobě a příjemci zprávy. Může se jednat o jednu ze služeb, které poskytuje poskytovatel, nebo ji může nabízet jiný subjekt. U datových zpráv, u kterých se předpokládá dlouhodobé uchování, je možné např. díky použití časového razítka prokázat, že datová zpráva byla podepsána v době platnosti příslušného certifikátu.

Proto, aby bylo časové razítko uznáno jako důvěryhodné je třeba, aby jej vydal kvalifikovaný poskytovatel certifikačních služeb. Kvalifikovaným časovým razítkem zákon rozumí datovou zprávu, 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.

Časové razítko vyžaduje opět autoritu, která zaručí, že čas v něm uvedený je správný. Autoritu pro časová razítka (Time Stamp Authority) zastává instituce, která má přístup k zaručenému času a je dostatečně důvěryhodná. PCS tímto získávají příležitost k rozšíření svého oboru činnosti i na vydávání časových razítek.

## 1.4 Podepisující osoba, Digitální podpis

Data pro vytváření elektronického podpisu slouží, jak název napovídá, pro jeho vytvoření. Nestačí však zprávu elektronicky podepsat, je nutné ještě zajistit, aby mohlo být ověřeno, kdo zprávu podepsal. K tomu slouží data pro ověřování elektronického podpisu, která musí být odpovídající datum pro vytváření, tj. obojí data musí být taková, aby ve spojení zajišťovala požadované funkce. Data pro ověřování elektronického podpisu se při použití technologie digitálního podpisu nazývají veřejný klíč a data pro vytváření elektronického podpisu soukromý klíč. Tato data si každý zájemce generuje prostřednictvím aplikace pro generování klíčů. Data pro vytváření podpisu musí podepisující osoba uchovat v tajnosti, data pro ověřování podpisu jsou naopak určena ke zveřejnění. Data pro ověřování podpisu

je nutné bezpečně předávat mezi podepisující osobou a osobou, která se na podpis spoléhá . zpravidla příjemce elektronicky podepsané zprávy. K tomuto bezpečnému předání může sloužit certifikát, což je datová zpráva, která spojuje data pro ověřování podpisu s osobou, které byl vydán (tj. s podepisující osobou) a umožňuje ověřit její totožnost.

Poskytovatelé nabízejí možnost vygenerovat data ve spolupráci s nimi, resp. Umožňují jejich vygenerování. To však zpravidla neznamená, že poskytovatel data sám vygeneruje. V takovém případě by hrozilo nebezpečí, že pokud bude poskytovatel nedůvěryhodný a bude znát data pro vytváření elektronického podpisu osoby, které vydává certifikát, může je zneužít jako kdokoliv jiný. Někteří poskytovatelé, zejména v zahraničí, nabízejí službu generování dat pro vytváření elektronického podpisu.

## 1.5 Elektronická podatelna

Elektronická podatelna je definována v nařízení vlády č. 304/2001 Sb. Jako pracoviště pro příjem a odesílání datových zpráv. Povinnost zřídit jedno či více takových pracovišť je uložena tímto nařízením orgánům veřejné moci, pokud pro ně ze zvláštních předpisů, které jsou v tomto nařízení citovány pod čarou, vyplývá povinnost přijmout podání učiněné v elektronické podobě, podepsané elektronicky, anebo stanoví-li zvláštní právní předpis právo těchto orgánů činit úkony elektronické podobě. Tato povinnost se vztahuje rovněž na územní samosprávné celky provádějící výkon státní správy v rámci přenesené působnosti. Elektronické podatelny musí být vybaveny potřebnými zařízeními připojenými k veřejné datové síti, popřípadě jiným sítím. Tato zařízení musí splňovat požadavky na technické a programové vybavení podle standardů vydaných Úřadem pro veřejné informační systémy.

## 1.6 Digitální podpis, Zaručený elektronický podpis

Elektronický podpis je zpravidla chápán jako číslo, které vytváří podepisující osoba pomocí svých dat pro vytváření elektronického podpisu a pomocí zprávy, kterou podepisuje. Elektronický podpis je jiný pro dvě odlišné zprávy, závisí na podepisované zprávě, nelze jej tedy koupit ani jinak obdobně získat. Přesně vzato by se pod pojem elektronický podpis vešel i podpis, který je napsán z klávesnice PC. Takový podpis příliš velkou důvěru nevzbuzuje - je těžké identifikovat a prokázat, kdo jej skutečně napsal. Elektronickým podpisem je tedy v praxi zpravidla míněn zaručený elektronický podpis.

## 1.7 Kvalifikovaný (elektronický) podpis

Pojem kvalifikovaný podpis, resp. kvalifikovaný elektronický podpis neobsahuje ani zákon o elektronickém podpisu, ani Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy. Poprvé se objevil v dokumentech, které vznikají z iniciativy Evropské komise a na Směrnici navazují.

Kvalifikovaným podpisem je míněn zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí použití prostředku pro bezpečné vytváření elektronického podpisu.

## 1.8 Osoba spoléhající se na podpis

Osobou spoléhající se na podpis může být příjemce elektronicky podepsané zprávy i osoba, která není přímým příjemcem zprávy od podepisující osoby, ale s elektroniky podepsanou zprávou pracuje a potřebuje se na podpis spoléhat (např. správce daně, auditor, soud apod.). Osoba spoléhající se na podpis může využít skutečnosti, že většina běžně užívaných aplikací zasílá certifikát zároveň s elektronicky podepsanou zprávou. Pokud tomu tak není, musí podepisující osoba oznámit, kde je její certifikát dostupný, nebo musí být z použitého systému (nebo protokolu) zřejmé, kde se úložiště takového certifikátu nachází. Zpravidla se jedná o server poskytovatele, který certifikát vydal, nebo webovou stránku podepisující osoby. Nelze počítat s tím, že z certifikátu je možné obecně získat příliš mnoho informací o osobě, které byl vydán, tj. o podepisující osobě. To ostatně není účelem certifikátu. Účelem je důvěryhodným způsobem předat data pro ověřování elektronického podpisu podepisující osoby. Osoba spoléhající se na podpis spoléhá na to, že poskytovatel před vydáním certifikátu ověřil totožnost osoby, které certifikát vydává. Je třeba připomenout, že poskytovatel certifikačních služeb nemůže jiné osobě, tedy ani osobě spoléhající se na podpis, sdělit údaje, které osoba, která žádá o vystavení certifikátu, tomuto poskytovateli sdělila (například poštovní adresa, telefonní číslo) a které nejsou uvedeny v certifikátu. Výjimku představují situace, kdy dotčená osoba vysloví se sdělením těchto údajů souhlas nebo pokud tak stanoví zákon (například v případě soudního řízení apod.).

## 1.9 Ověření platnosti certifikátu

Pro ověření platnosti certifikátu podepisující osoby je nutným předpokladem důvěra v poskytovatele, který jej vydal. Pokud osoba spoléhající se na podpis tuto důvěru má, nainstaluje do svého software certifikát poskytovatele (je nutné odlišit certifikát poskytovatele a certifikát podepisující osoby). Pokud osoba spoléhající se na podpis obdrží elektronicky podepsanou zprávu a zároveň certifikát podepisující osoby (případně získá certifikát jiným způsobem), následně ověří, zda certifikát podepisující osoby vydal poskytovatel uvedený v certifikátu a zda tento certifikát nebyl od okamžiku jeho vydání změněn. Toto ověření zajistí sama aplikace, a to ověřením elektronického podpisu poskytovatele, který je na certifikátu podepisující osoby. Následně se zjišťuje, zda byl certifikát podepisující osoby platný v době, kdy byla zpráva podepsána. Přímo v certifikátu je uveden počátek a konec doby platnosti certifikátu (platnost od - do). V průběhu této doby však mohla být ukončena platnost certifikátu. Zda se tak nestalo, je nutné ověřit u poskytovatele v seznamu certifikátů, které byly zneplatněny (zveřejňován obvykle pod zkratkou CRL - Certification Revocation List ). Vždy je nutné počítat s určitým prodlením, které nastane mezi dobou, kdy držitel certifikátu požádá o ukončení platnosti svého certifikátu, a dobou, kdy je informace o zneplatnění certifikátu zveřejněna v CRL, resp. Je vydán nový, aktualizovaný seznam zneplatněných certifikátů. Z technického i organizačního hlediska je velmi obtížné, aby mezi těmito dvěma akcemi nebyla určitá časová prodleva. Jak dlouhá tato prodleva je, lze zjistit v certifikační politice příslušného poskytovatele. Podle obsahu elektronicky podepsané zprávy je nutné zvážit, zda akceptovat obsah zprávy a poté, kdy uplyne doba, kterou poskytovatel potřebuje ke zveřejnění nového seznamu certifikátů, které byly zneplatněny.

## 1.10 Podepisující osoba

Podepisující osobou ve smyslu zákona č. 227/2000 Sb. může být pouze fyzická osoba. Stejně jako v případě vlastnoručního podpisu není přípustné, aby se elektronicky podepisovala právnická osoba, byť v případě elektronického podpisu by z technického hlediska teoreticky taková možnost byla.

Stejně jako jsou v organizaci (firmě apod.) určeni pracovníci, kteří jsou oprávněni svým podpisem opatřovat listinné dokumenty a jednat tak jménem právnické osoby, je potřeba analogicky postupovat i při elektronickém podepisování. V certifikátu v položce účel lze

konstatovat oprávnění fyzické osoby k podepisování jménem osoby právnické. Fyzická osoba se tak může elektronicky podepisovat jménem právnické osoby a osoba spoléhající se na podpis v certifikátu vidí, že tato osoba je k tomu oprávněna.

Podepisující osoba musí mít prostředek pro vytváření elektronického podpisu a data pro vytváření elektronického podpisu. Bezpečnost elektronického podepisování je do značné míry závislá na chování podepisující osoby, zejména na její schopnosti uchovat v tajnosti svá data pro vytváření elektronického podpisu (soukromý klíč). Pokud hrozí nebezpečí zneužití jejích dat pro vytváření elektronického podpisu, je podepisující osoba o této skutečnosti povinna uvědomit poskytovatele, který jí kvalifikovaný certifikát vydal. Další povinností podepisující osoby je podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu. Ikdyž zákon stanoví uvedené povinnosti pouze v případě, že je vydán certifikát s označením kvalifikovaný a jedná se o kvalifikovaný certifikát podle zákona, je žádoucí, aby se takto podepisující osoba chovala i v případě, že jí byl vydán jakýkoliv certifikát. Fyzická osoba může mít libovolný počet certifikátů. Jiné certifikáty může akceptovat banka, jiné úřad.

## 1.11 Registrační autorita

Vykonává registrační služby, tj. zejména ověřuje totožnost osob, které žádají o vydání certifikátu, případně zjišťuje specifické znaky těchto osob. Tato služba předchází vydání certifikátu. Může zahrnovat rovněž ověření, zda žadatel o vydání certifikátu má data pro vytváření podpisu. Registrační autorita je místem, kde se uzavírá s žadateli smlouva o vydání certifikátu a kde je dostupná certifikační politika a certifikát poskytovatele.

Pro zajišťování činnosti registračních autorit certifikační autority často využívají služeb jiných subjektů, tj. děje se tak na základě smluvních vztahů mezi certifikační autoritou a registrační autoritou. Zákon o elektronickém podpisu neupravuje výslovně činnost registračních autorit, ale povinnosti, které se na činnosti, které zpravidla zajišťují, vztahují, jsou obsaženy v povinnostech poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty.

## 1.12 Šifrování

Šifrování datové zprávy je samostatný úkon, který nevyplývá z funkce elektronického podpisu. Elektronicky podepsaná zpráva může být šifrována, ale toto šifrování nezajišťuje elektronický podpis. Pokud tedy elektronicky podepsaná datová zpráva není šifrována, je předávána v otevřené podobě a osoba, která ji získá, se může seznámit s jejím obsahem. Zákon o elektronickém podpisu šifrování elektronicky podepsaných datových zpráv neupravuje.

# 2 LEGISLATIVA V ČR

Tato část má za úkol přiblížit čtenáři legislativní prostředí České republiky na poli elektronického podpisu. Budu se věnovat zákonu o elektronickém podpisu.

## 2.1 Zákon o elektronickém podpisu

Zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu – dále budeme používat zkratku ZoEP), byl přijat 29.6.2000 jako pokus harmonizovat alespoň částečně naši legislativu s právními nároky Evropské unie. EU vydala směrnici Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy. ZoEP se stal účinným 1.10.2000. Zákon byl 1.7.2002 novelizován zákonem č. 226/2002 Sb., který upravoval elektronické doručování a zákonem č. 517/2002 Sb., což byla novela ZoEP.

Státy Evropské Unie se dohodly na jednotném přístupu k řešení elektronického podpisu. Dva roky byl připravován jeden ze stěžejních dokumentů o elektronickém podpisu v rámci EU. Směrnice EU k elektronickému podpisu byla 13. 12. 1999 schválena Evropskou komisí. Vlády jednotlivých členských zemí EU mají za úkol uvést principy a požadavky této Směrnice do svého zákonodárství nejpozději do 19.7.2001. Směrnice se zabývá elektronickými podpisy především z hlediska speciálního typu tzv. zaručených elektronických podpisů, které mají být právně ekvivalentní klasickým vlastnoručním podpisům. Zaměřuje se na právní platnost elektronického podpisu, který je připojen k elektronickému dokumentu. Směrnice stanoví základní požadavky, které mají být splněny poskytovateli služeb spojených s elektronickými podpisy (certifikační autority) a další požadavky vztahující se k podepisující a ověřující straně. Směrnice byla vypracována tak, aby byly dodrženy tři následující principy:

• technologická neutralita,

• pro poskytovatele certifikačních služeb není definováno žádné schéma pro autorizaci k provádění těchto služeb tak, aby v budoucnu zde existovala principiální možnost technologických inovací,

• upravení zákonné platnosti elektronických podpisů tak, aby nemohlo být odmítnuto jejich použití (např. jako soudní důkaz) na základě toho, že jsou v elektronické podobě a byla zaručena ekvivalence s ručně napsaným podpisem.

Zákon přinesl několik změn. První byla zrovnoprávnění elektronicky podepsaných dokumentů s tištěnými. Toto však není možné tvrdit jednoznačně, jelikož výklad práva se různí. Ale i přes pochybnosti bylo umožněno daleko větší využití elektronické komunikace i pro právní úkony. Další změnou bylo vytvoření odboru elektronického podpisu na Úřadu na ochranu osobních údajů (ÚOOÚ).

ÚOOÚ měl za úkol vypracovat prováděcí vyhlášku, ve které by specifikoval podmínky pro práci poskytovatelů certifikačních služeb. Jeho další funkcí bylo udělování akreditací poskytovatelům certifikačních služeb a vykonávání dozoru nad prací PCS. ÚOOÚ měl i pravomoci vydávat vyhlášky k upřesňování podmínek.

Novela zákona č. 517/2002 Sb. přesunula tyto pravomoci z ÚOOÚ na Ministerstvo informatiky.

### 2.1.1 Obsah zákona o elektronickém podpisu

Zákon vymezuje v první části pojmy, jako jsou:

• elektronický podpis, jeho zaručená verze,

• datová zpráva,

• podepisující osoba,

• poskytovatel certifikačních služeb, dále akreditovaný PCS

• certifikát, jeho kvalifikovaná verze,

• data pro vytváření a ověřování elektronických podpisů (soukromý a veřejný klíč),

• prostředky pro vytváření a ověřování elektronických podpisů a jejich bezpečné varianty,

• nástroj elektronického podpisu.

Dále zákon definuje za jakých podmínek je datová zpráva podepsána, jaké jsou specifické požadavky na podpis. Další část je věnována povinnostem podepisující osoby a poskytovatele certifikačních služeb.

Povinnosti podepisující osoby jsou následující:

• zacházet s prostředky, taktéž i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

• uvědomit okamžitě poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,

• podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

Jak je vidět, výše uvedené povinnosti mají přispět k zajištění bezpečnosti podepisující osoby a umožnit plnění funkcí PCS. Povinnosti poskytovatele certifikačních služeb:

• PCS musí zajistit splnění všech náležitostí certifikátu, uvádění pravdivých informací.

• Dodržování bezpečnostních zásad a používání bezpečných prostředků pro práci s elektronickými podpisy.

• Vedení evidence vydaných kvalifikovaných certifikátu a seznamu zneplatněných certifikátů –CRL.

• PCS musí držet neustále dostatečné množství peněžních prostředků pro plynulý běh systémů při přihlédnutí k riziku.

• Uchovávat veškerou dokumentaci v souvislosti s kvalifikovanými certifikáty po dobu minimálně 10 let.

• Jeho zaměstnanci musí při práci respektovat zákon č. 101/2000 Sb. o ochraně osobních údajů.

Zákon stanoví povinnou písemnou formu smlouvy, na základě které PCS vydává žadateli kvalifikovaný certifikát. Odpovědnost za škodu obou smluvních stran se řídí Občanským zákoníkem.

Zákon dále uvádí, jakým způsobem zažádá poskytovatel certifikačních služeb o udělení akreditace a jak ministerstvo postupuje při jejím udělování.

Zákon řeší, jaké náležitosti má mít kvalifikovaný certifikát a jakým způsobem je možné uznávat zahraniční certifikáty. Dosud platí, že je možné uznat zahraniční certifikát jako

kvalifikovaný pouze za předpokladu splnění všech podmínek uvedených v zákoně a pokud se náš akreditovaný poskytovatel certifikačních služeb zaručí za jejich správnost a platnost. To činí uznávání cizích certifikátů velmi komplikovanou záležitost. Zákon formuluje požadavky na prostředky bezpečného vytváření a ověřování elektronických podpisů takto.

1. Prostředek pro bezpečné vytváření podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že

a) data pro vytváření podpisu se mohou vyskytnout pouze jednou, a že jejich utajení je náležitě zajištěno,

b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření, a že podpis je chráněn proti padělání s využitím existující dostupné technologie,

c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou.

2. Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani

zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

3. Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby

a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě

provádějící ověření,

b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,

c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,

d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,

e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,

f) bylo jasně uvedeno použití pseudonymu,

g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

Zákon tedy klade požadavky na funkce programového vybavení používané při práci se zaručeným podpisem a kvalifikovanými certifikáty. Tyto požadavky by měly zajistit bezpečnost klíče a řádnou funkci institutu elektronického podpisu. Měly by i usnadnit uživateli orientaci při práci s elektronickým podpisem.

Další články zákona se věnují pokutám a postihům za porušení výše daných podmínek. Pokuty smí udělovat ministerstvo, jejich výběr je příjmem státního rozpočtu. Maximální výše pokuty, kterou smí ministerstvo udělit činí 20 000 000 Kč.

Poslední část ZoEP je věnována změnám v některých dalších zákonech. Tím je umožněno kupř. podání trestního oznámení nebo daňového přiznání elektronickou cestou, pokud jsou opatřeny uznávaným elektronickým podpisem.

## 2.2 Vyhláška 366/2001 Sb.

Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb. z Částky 138/2001, o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu, byla přijata s okamžitou účinností 3.10.2001. Dlouhou dobu její neexistence komplikovala naplňování zákona a prakticky znemožňovala používání elektronického podpisu.

### 2.2.1 Obsah vyhlášky 366/2001 Sb.

Vyhláška upravuje jakým způsobem PCS dokazuje, že splnil všechny povinnosti, které mu zákon ukládá. Dokladování probíhá dle následujících pravidel.

1. Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty dokládá splnění

povinností stanovených v § 6 zákona o elektronickém podpisu těmito dokumenty:

a) certifikační politikou,

b) certifikační prováděcí směrnicí,

c) celkovou bezpečnostní politikou,

d) systémovou bezpečnostní politikou,

e) plánem pro zvládání krizových situací a plánem obnovy,

f) odhadem dostatečnosti finančních zdrojů a doklady o tom, že disponuje těmito finančními zdroji.

2. Obsahem certifikační politiky je zejména

a) stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy,

b) popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být vydán kvalifikovaný certifikát; kryptografické algoritmy a jejich parametry, které musí být pro tato data použity, jsou uvedeny v příloze č. 1 této vyhlášky.

3. Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty umožňuje trvalý

dálkový přístup ke své certifikační politice.

4. Obsahem certifikační prováděcí směrnice je zejména stanovení postupů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.

5. Obsahem celkové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

6. Obsahem systémové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění bezpečnosti informačního systému, jehož prostřednictvím poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajišťuje služby spojené s elektronickými podpisy (dále jen „informační systém pro certifikační služby"). Systémová bezpečnostní politika obsahuje zejména

a) způsob uplatnění celkové bezpečnostní politiky ve vztahu k informačnímu systému pro certifikační služby,

b) popis vazeb mezi informačním systémem pro certifikační služby a jinými informačními systémy, které provozuje poskytovatel certifikačních služeb vydávající kvalifikované certifikáty,

c) způsob ochrany dat a jiných prvků informačního systému pro certifikační služby,

d) popis bezpečnostních opatření,

e) vyhodnocení analýzy rizik.

7. Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku Úřad zveřejňuje ve Věstníku Úřadu pro ochranu osobních údajů.

8. Obsahem plánu pro zvládání krizových situací je zejména stanovení postupů, které jsou uplatněny v případě mimořádné události. Mimořádnou událostí se pro účely této vyhlášky rozumí událost, která ohrožuje poskytování služeb spojených s elektronickými podpisy,a která nastává zejména v důsledku selhání informačního systému nebo výskytu faktoru, který není pod kontrolou poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

9. Obsahem plánu obnovy je zejména stanovení postupů pro obnovu řádné funkce informačního systému pro certifikační služby.

10. Při zajišťování služeb spojených s elektronickými podpisy poskytovatel certifikačních

služeb vydávající kvalifikované certifikáty postupuje podle dokumentů uvedených v odstavci 1 písm. a) až f).

11. Dostatečností finančních zdrojů je schopnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty finančně zabezpečit řádné provozování služeb spojených s elektronickými podpisy i s ohledem na riziko odpovědnosti za škody. Tyto požadavky musí splňovat každý PCS, který chce získat akreditaci. Další část vyhlášky se věnuje Ministerstvu informatiky. Ministerstvo informatiky provádí schvalování nástrojů

elektronického podpisu, které PCS používají pro zajištění certifikačních služeb. Bez schválení ministerstvem nesmí PCS nástroje použít.

Dále se vyhláška věnuje podmínkám pro bezpečnost při práci s klíči, CRL, seznamy certifikátů, bezpečnosti informačních systémů a jejímu ověřování. Poslední věcí, kterou vyhláška upravuje, jsou nároky na prostředky pro bezpečné vytváření a ověřování elektronických podpisů.

K vyhlášce jsou jako přílohy dodány seznamy kryptografických algoritmů a jejich parametrů pro data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být vydán kvalifikovaný certifikát. Další přílohou je seznam

kryptografických algoritmů a jejich parametrů pro vytváření párových dat poskytovatele a pro prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu.

## 2.3 Nařízení vlády 304/2001 Sb.

Nařízení vlády č. 304/2001 Sb. z částky 117/2001 Sb. kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), vstoupilo v platnost 25.7.2001 a nabylo účinnosti 1.10.2001. Nařízení vlády upravuje povinnost úřadů orgánů veřejné moci zřídit tzv. Elektronické podatelny, které budou sloužit k přijímání úředních dokumentů v elektronické podobě. Elektronická podatelna musí splňovat požadavky vydané Úřadem pro informační systémy veřejné správy. Ten se nyní sloučil s Ministerstvem informatiky. Podatelna musí mít náležitě proškolené a vybavené zaměstnance, musí mít připojení na internet a přijímat i odesílat poštu nejméně dvakrát denně, vždy na začátku a před koncem pracovní doby. Pro snazší představu jak taková podatelna vypadá, je dobré říci, že je to jedna, nebo více adres pro elektronickou poštu, kterou obsluhují zaměstnanci vyhovující výše uvedeným podmínkám. Takovýto zaměstnanec musí mít vlastní kvalifikovaný certifikát pro zaručený elektronický podpis, kterým jménem státní instituce podepisuje odchozí poštu. Certifikát obsahuje kromě náležitostí, které už jsme si popsali, i označení (název) orgánu veřejné moci, jeho organizačního útvaru a funkce zaměstnance.

# 3 ÚVOD DO HASHOVÁNÍ

Hash vzniká pomocí funkce hashování (hashing), která ze zadaného velkého množství dat vrací mnohem menší objem dat, který však jednoznačně vypovídá o obsahu dokumentu. Při změně jen jednoho bitu zprávy se musí hodnota hashe změnit. Pro potřeby kryptografie musí být funkce hashování jednosměrná. Známe-li hodnotu hashe (a máme-li rovněž původní dokument, ze kterého byl hash vypočítán), mělo by být velmi obtížné vytvořit jiný dokument se stejnou hashovací hodnotou. Silná hashovaní funkce musí tedy vyhovovat následujícím požadavkům:

• musí být jednosměrná, tedy nesmí být možné z hodnoty hashe odvodit původní zprávu,

• musí být nekolizní, nesmí být možné dostat na dvě různé výchozí zprávy tutéž hodnotu hashe.

Poté, co je hash původní zprávy zašifrován, je odeslán příjemci. Ten jej pomocí veřejného klíče dešifruje a z původní zprávy (otevřeného textu), kterou mu odesílatel též pošle, vytvoří stejným způsobem nový hash. Má tak k dispozici dva hashe vytvořené z jedné zprávy. Podle výše uvedených požadavků na hashovací funkci by v případě neporušenosti zprávy byly oba hashe identické. V takovém případě se příjemce může spolehnout na text zaslaného dokumentu.

## 3.1 Úvod do asymetrické kryptografie

Pojem elektronický - resp. digitální podpis se začal objevovat souběžně se vznikem asymetrické kryptografie již v druhé polovině sedmdesátých let dvacátého století. Asymetrická kryptografie používá pro účely zabezpečení dat propojenou dvojici klíčů. První klíč (soukromý) slouží k šifrování dat a vytváří se jím digitální podpis. Druhý (veřejný) klíč slouží k dešifrování podpisu. Důležitou vlastností asymetrické kryptografie je používání jednocestných funkcí. Je to funkce, u níž je snadné pro všechna x vypočítat hodnotu y, ale pro všechna y se nedají vypočítat x.

Kryptografie s veřejným klíčem využívá tuto asymetrii k vytvoření funkcí, u kterých

platí dvě základní pravidla:

• je snadné provést šifrovací operaci - tedy šifrování,

• je však velmi obtížné tuto operaci invertovat (dešifrovat) bez znalosti informací, které k tomu potřebuji (veřejný klíč).

Kryptografie implementuje princip jednocestné funkce použitím dvou odlišných klíčů, které jsou však ve vzájemné vazbě a jsou vytvořeny současně. Jeden klíč lze použít pouze k zašifrování, druhý pouze k dešifrování. Jejich matematický vztah je tedy založen na tom, že se požaduje veřejný klíč k invertování operace se soukromým klíčem. Znamená to, že jedna osoba, která má soukromý klíč, může provést operaci, kterou může každý, kdo vlastní veřejný klíč, invertovat. Jedná se zjevně o způsob použití při digitálním podepisování. ZoEP používá pro pojem soukromý klíč pojem data pro vytváření elektronického podpisu a pro pojem veřejný klíč pojem data pro ověřování elektronického podpisu.

Digitální podpis se používá tehdy, je-li zasílán šifrovaný nebo nešifrovaný (otevřený) text, a odesílatel chce zajistit:

• aby příjemci mohli ověřit, že zpráva přichází skutečně od odesilatele,

• aby příjemci mohli ověřit, zda text nebyl pozměněn poté, co jej odesílatel podepsal.

Samotná zpráva může, ale také nemusí být během přenosu zašifrována. V takovém případě je osvědčený postup podepsat zprávu před jejím šifrováním - odesílatel totiž ví, co podepisuje. V praxi elektronických podpisů se soukromým klíčem nešifruje celá zpráva. Takový postup by vzhledem k rychlosti asymetrické kryptografie zabíral příliš mnoho času. Do procesu podepisování tak vstupuje další matematická operace, která ze zprávy vytvoří kratší otisk neboli hash, který je podepisován (šifrován).

## 3.2 Asymetrická kryptografie a hashování

K tomu, aby byl digitální respektive elektronický podpis universálně použitelný, je nutné, aby prostředky pro jeho tvorbu a ověřování pracovaly na stejných principech. Tyto prostředky musí být té. dostatečně bezpečné a odolné vůči útokům. Tato snaha vedla ke stanovení základních požadavků na asymetrickou kryptografii a našívací funkce, jež jsou (nebo mají být) zachyceny v právních dokumentech jednotlivých států. Vyhláška vyžaduje používání algoritmů RSA, DSA, či DSA založených na eliptických křivkách a při hašování mají být požívány funkce MD5, SHA-1, nebo RIPMED-160

### 3.2.1 RSA

4. dubna 1977 oznámili L. Rivest, A. Shamir a L. Adleman z Massachusetts Institute of Technology objev prvního v praxi použitelného šifrovacího systému s veřejným klíčem. Ten byl posléze pojmenován podle počátečních písmen jejich příjmení RSA Algoritmus RSA je považován za jeden z nejlepších, jedinou jeho nevýhodou je značná časová náročnost. Tu řeší digitální podpis používáním krátkého otisku zprávy. RSA je založena na faktu, že je velice obtížné (pro velká čísla časově nemožné) rozložit čísla, kde každé je součinem dvou velkých prvočísel. Nejprve tedy generujeme náhodně a nepredikovatelně dvě dostatečně velká prvočísla P a Q. Minimální délka těchto čísel, kterou vyžaduje Vyhláška, je 1024 bitů. To odpovídá dekadickému číslu o více než 100 cifrách. Dále spočítáme číslo N=PQ a hodnotu Eulerovi funkce Φ=(P-1)(Q-1). Dále nalezneme číslo E takové, kde 1<E<Φ a NSD(E, Φ)=1. V dalším kroku spočteme číslo D takové, že 1<D<Φ a ED=1 mod Φ. Veřejným klíčem je v našem případě (N,E) a soukromým klíčem je (N,D). Známe-li hodnoty obou klíčů, můžeme přistoupit k vlastnímu šifrování. Předpokládejme, že jsme předali druhé straně (příjemci) náš veřejný klíč (N,E). Svým soukromým klíčem zašifrujeme zprávu M podle vzorce C=MD mod N. C je tedy samotný digitální podpis. Podpis C zašleme příjemci, který vlastní veřejný klíč (N,E). Ten provede CE mod N=M. Získal tedy původní zprávu M.

### 3.2.2 DSA

Tento protokol umožňuje dvěma uživatelům vyměnit si tajný klíč pomocí veřejných medií. Neobsahuje žádnou metodu umožňující podpis zaslané zprávy, ani není možné provést autentizaci, že daný klíč skutečně pochází od daného uživatele. Bezpečnost tohoto algoritmu závisí na obtížnosti řešení úlohy diskrétního logaritmu (obvykle je složitost této úlohy považována za ekvivalentní složitosti úlohy faktorizace). Jádrem jednoho z druhů DSA (Diffie-Hellman) je fakt, že pro velká čísla Z a prvočísla A a P (všechna například 200ciferná), je snadné vypočítat číslo X podle vztahu X=AZ mod P, je na to třeba pouze přibližně 2log2Z násobení, zatímco na výpočet čísla Z (diskrétního logaritmu) ze známého čísla X potřebujeme přibližně odmocninu z P násobení (tedy přibližně 10100). Takový výpočet je opět časově velice náročný. Princip metody, která umožňuje rychle mocnit velká čísla, spočívá v rozkladu exponentu a postupném násobení a mocnění mezivýsledků. Například X=Z49=Z(32+16+1)=(((((Z2)2)2)2)2)*((((Z2)2)2)2)*Z. Tato výpočetní operace

nyní vyžaduje pouze 11 násobení a nikoliv 48. Výměna a tvorba klíčů probíhá v několika krocích.

1. Obě strany vygenerují sejná prvočísla A a P.

2. Strana A nalezne takové ZA, kde 1 <= ZA <= P-2. Strana B nalezne takové ZB,

kde 1 <= ZB <= P-2.

3. Strana A vypočítá zprávu XA = AZA mod P. Strana B vypočítá zprávu XB = AZB

mod P.

4. Obě stany si vymění zprávy XA a XB.

5. Strana A nalezne klíč K=(AZB)ZA mod P; a strana B nalezne stejný klíč K=(AZA)ZB mod P.

Ve Spojených státech byl Diffie-Hellmanův systém pro výměnu klíčů patentován (M. E. Hellman and R. C. Merkle: Public Key Cryptographic Apparatus and Method. US Patent 4,218,582, 1980), ale patent vypršel 29.dubna 1997.

### 3.2.3 Eliptické křivky

Matematická teorie hledá cesty, jak zlepšit vlastnosti systémů s veřejným klíčem. Jestliže v dosažené rychlosti šifrování se zatím žádné význačně změny nerýsují, je tomu jinak z hlediska velikosti použitých klíčů. V tomto směru význačná zlepšení přináší implementace (90 léta) systémů s veřejným klíčem na bázi tzv. eliptických křivek. V roce 1985 přišli nezávisle na sobě Neil Koblitz a Victor Miller k návrhu využívat pro kryptografické účely grupy založené na eliptických křivkách. Primární výhodou kryptosystémů na bázi eliptických křivek je jejich velká kryptografická bezpečnost vzhledem k dané velikosti klíče. Význačně kratší délka klíčů (např. oproti RSA) vede ke kratším certifikátům i menším parametrům systému a tedy i k větší výpočetní efektivnosti algoritmů. Druhá výhoda je v tom, že fakticky všechna již známá použití v systémech na bázi diskrétního logaritmu (kryptografické protokoly, DSA apod.) lze převést do systémů na bázi eliptických křivek. Pro danou množinu parametrů eliptického kryptosystému je dvojice soukromý a veřejný klíč vytvářena následovně. Soukromý klíč S je celé číslo náhodně vygenerované v intervalu 0 << S < r. Veřejný klíč je bod W na eliptické křivce spočtený

jako W = S*G. Číslo r je řád bodu G, pro který musí platit r>2160 a zároveň je dělitelem řádu eliptické křivky E. Bod G=(x,y) je definován kořeny eliptické rovnice E: y2 + xy = x2 + ax2 + b. Pro použití obou klíčů mohou platit výše zmíněná pravidla použití klíčů RSA. Při generování konkrétních eliptických křivek (pro kryptografické účely) je vhodné generovat parametry křivky náhodně. Pomocí tzv. seedu lze zabezpečit dokonce, že strana, která příslušnou křivku generovala, může později prokázat, že daná křivka skutečně náhodně vygenerována byla. Touto cestou ujistí druhou stranu, že v systému nejsou žádná skrytá zadní vrátka, která umožňují první straně získání nějakých výhod (např. vypočtení soukromého klíče druhé strany). Tomu, aby eliptické křivky již dnes plně nahradily RSA a byly více než důstojným nástupcem starších kryptosystémů, již tedy nic nebrání a fakticky se tak již i děje. RSA stále ještě bude používána v řadě existujících systémů a zůstane tak ještě po nějakou dobu dominantním používaným kryptosystémem s veřejným klíčem. Pokud se však jedná o přípravu budoucích systémů, jsou přednosti eliptických kryptosystémů nesporné.

### 3.2.4 MD5

Hašovací funkce, které Vyhláška povoluje, vytvoří z velmi dlouhé zprávy M (soubor dat o délce a. 264 bitů) hašovací kód o délce 128, resp. 160 bitů. Kompresi uvedených hašovacích funkcí zajišťuje tzv. kompresní funkce (f). U zmíněných funkcí je zpráva M před vlastním ha.ováním doplněna a zarovnána na celistvý počet 512 bitových bloků Mi, i=1..n, a dále je definována inicializační hodnota IV (konstanta příslušné hašovací funkce). Proces hašování využívá kompresní funkci MD5 iterativně takto:

H0=IV,

Hi=f(Hi-1,Mi), i=1..n,

H(M)=Hn.

Autorem hašovacích funkcí MD (Message Digest) je R. Rivest, zakladatel RSA Data Security Inc. Jako první z řady MD vznikla MD2 (1989), která je bajtově orientovaná a od svých 32bitových následovníků se odlišuje i zjevnou pomalostí. V roce 1990 byla vytvořena hašovací funkce MD4. Funkce byla rychlejší, avšak byla kolizní. Na podzim roku 1995 tento fakt dokázal pracovník německé informační služby Hans Dobbertin. Verze MD5 byla vydána v roce 1991. Funkce MD5 používá 128bitový kód a je zhruba o 33% pomalejší, než MD4. V neprospěch této funkce přispívá i fakt, že Hans Dobbertin dokázal i

v jejím případě nalézt kolizi (1996), a také je zde obecná námitka proti používání 128bitových kódů. V roce 1994 byl P. Oorschotem a M. Wienerem navržen stroj, který je schopen vygenerovat 264 kódů a tudíž realizuje tzv. narozeninový paradox u 128bitového kódu. V praxi znamená narozeninový paradox možnost nalezení kolize u 2d/2 zpráv s pravděpodobností 50%. Z této skutečnosti vyplývá, že hašovací funkce používající 128bitové kódy jsou se současnou technologií prolomitelné. Vzhledem k těmto skutečnostem se sám autor R. Rivest rozhodl nedoporučit funkci MD5 pro používání v digitálních podpisech. I přes tyto nedostatky, povoluje Vyhláška používání MD5 pro elektronický podpis. Děje se tak proto, že MD5 je široce rozšířena např. v bankovní sféře a její zákaz by znamenal značné komplikace.

### 3.2.5 SHA-1

SHA-1 byla vytvořena americkou tajnou službou NSA americkým úřadem pro normalizaci NIST byla vyhlášena 17. 4. 1995 jako standard v oficiálním dokumentu Federal Information Processing Standards Publication 180-1 (FIPS PUB 180-1). Je určena nejen pro potřeby algoritmu digitálního podpisu (DSA), ale i pro všechny aplikace ve státním sektoru, kde je požadována bezpečná hašovací funkce. SHA-1 tak nahradila svoji předchůdkyni SHA, definovanou v FIPS PUB 180 z 11. 5. 1993. Dokumenty jsou nazvány Secure Hash Standard (SHS), přičemž vlastní algoritmus se nazývá Secure Hash Algorithm (SHA). Rozdíl mezi definicí SHA-1 a SHA je nepatrný: SHA-1 má v příkazovém řádku hlavní smyčky (viz dále) jednu jednobitovou rotaci navíc, ale rozdíl mezi jejich bezpečností je velký. Funkce SHA-1je považována za bezpečnou, zatímco SHA nikoli. SHA-1 byla navržena jako standardní hašovací funkce se vstupem od 0 až do 264-1 bitů a výstupem 160 bitů. Myšlenkově vychází z návrhu algoritmu MD4 od R. Rivesta (1990), ale velmi posiluje jeho vnitřní funkce, tak.e zatímco u MD4 již byly nalezeny kolize, SHA-1 je vůči nim považována za rezistentní. Důležitou úlohu zde hraje také délka kódu. Jestliže jsme uvedli, že současná technologie je schopná v dosažitelném čase najít kolizi hašovací funkce, jejíž kód má délku 128 bitů, pak stejná technologie by našla kolizi u 160bitového kódu až za 216 násobek (princip narozeninového paradoxu) této doby. Podle známého Moorova zákonu bude možné najít kolizi u funkcí se 160bitovým kódem až za zhruba 24 let. Algoritmus SHA-1sestává z několika hlavních kroků, které si v dalším odstavci popíšeme.

Nejprve dojde k doplnění zprávy M na délku, která je celočíselným násobkem 512 bitů. Výpočet hašovací hodnoty se provádí postupným zpracováním bloků M1 až Mn:

1. Každé Mi rozdělíme na 16 slov W(0) až W(15).

2. Provedeme expanzi na slova W(16) až W(79).

3. Proměnné A až E nastavíme na konkrétní hodnoty konstant H0 až H4.

4. V následujících 80 rundách přimícháváme dle vzorce slova W do konstant A až E.

5. Aktualizujeme hodnoty H0 až H4 přičtením závěrečných hodnot A až E.

Po zpracování posledního bloku Mn je hašovací hodnota definována jako 160bitový řetězec tvořený slovy H0 až H4.

### 3.2.6 RIPEMD-160

Funkce RIPEMD byla navržena v rámci projektu RACE Integrity Primitives Evaluation (RIPE) Komise Evropských společenství, který měl pomoci evropské standardizaci kryptografických funkcí. V rámci projektu (zavržen v polovině 90. let) byly hodnoceny a navrženy různé kryptografické nástroje. RIPEMD vychází z MD4, ale je bezpečnostně posílena. Zajímavé je rozdělení kompresní funkce na dvě a kombinace jejich výsledků v závěru zpracování každého bloku. Kolize u ní nebyly nalezeny (jen v její zeslabené variantě), ale nevýhodou je 128bitový kód. Proto v roce 1996 H. Dobbertin a dva Belgičané A. Bosselaers a B. Preenel (již mimo projekt RIPE) navrhli RIPEMD-160 se 160bitovým hašovacím kódem. Zesiluje původní RIPEMD a výsledkem je velice kvalitní návrh hašovací funkce. Navrhli také variantu RIPEMD-128 se 128bitovým kódem jako náhražku RIPEMD tam, kde nelze použít kód 160bitový. Pro ty, kdo vyžadují ještě vyšší bezpečnost, byly vytvořeny dokonce i RIPEMD-256 a RIPEMD-320. Vznikly vytvořením dvou paralelních linií zpracování dat pomocí kompresních funkcí RIPEMD-128 a RIPEMD-160, v nichž jsou navíc vzájemně kombinovány jejich vnitřní stavy. RIPEMD-160 je nejvážnějším dnešním protikandidátem SHA-1 a byla začleněna do mezinárodního standardu ISO/IEC 10118-3, společně s RIPEMD-128 a SHA-1. RIPEMD-128, 160, 256 a 320 jsou zaregistrovány jako funkce společnosti TeleTrustT, ale patří do freewaru a mohou se bezplatně použít i pro komerční účely.

# 4 PROSTŘEDKY PRO ARCHIVACI DAT

## 4.1 Způsoby autentizace

Dvě věci jsou více než jedna a tak je tato možnost autentizace považována za řádově bezpečnější, než pouhé používání hesel.

*Obr. 1: Snímač otisku prstů integrovaný do myši*

*Obr. 2: Autentizační kalkulátor*

*Obr. 3: USB token se snímačem otisku prstu*


*Obr. 4: Čtečka čipových karet ve formě PC Card*

Jsou samozřejmě i jiné řešení autentizace, jako jsou autentizační kalkulátory, zaslání jednorázového kódu ve formě sms na mobil klienta, snímače otisků prstů**,** analyzátory DNA a mnoho dalších. Chtěl bych zde hlavně srovnat čipové karty a USB tokeny, jsou to jedny z mála řešení, která umožňují nejen bezpečnou autentizaci, ale také slouží jako velmi bezpečná úložiště malých (řádově několik kB) dat, která se snažíme před útočníky chránit. Dat, jako jsou hesla, šifrovací klíče, privátní klíče, sdílená tajemství, certifikáty, kódy atd. Čipové karty a USB tokeny jsou tedy velmi univerzální. Celá bezpečnost dat je závislá nikoli na téměř neprůstřelném software a nejlepší šifře, ale na zvoleném hesle. To je velmi dobrý důvod, proč ukládat šifrovací klíče mimo HDD na nějaké bezpečné zařízení. Někam, kam se na něj případný útočník bude dostávat jen velmi těžce. Na nějaké zařízení, které budete pokud možno nosit neustále s sebou, takže budete mít nad přístupem k těm pár vysoce důležitým bitům plnou kontrolu. Na příklad na čipovou kartu, nebo USB token.

## 4.2 Autentizace pomocí jména a hesla

Autentizace je ověření identity uživatele. Autentizace pomocí hesla, by měl být v dnešní době již spíše přežitek. Uživatelé zadávající své username a heslo, jsou noční můrou každého správce sítě, který dbá na bezpečnost.

- Uživatelé volí hesla typu: rodné číslo, jméno partnera/-ky, telefonní číslo, nápisy poblíž počítače, tedy hesla, která může útočník snadno uhádnout
- Obyčejná slova, typu domeček, sluníčko, krteček nejsou o nic lepší. Slovníkový útok se slovníkem o 30 tis. slovech je pořád rychlejší než vyzkoušet všech 78 miliard kombinací u 7 znakového hesla (znaky a-z, 0-9).
- Heslo se dá snadno získat odpozorováním , obzvláště u lidí, kteří nepíší všemi deseti a s využitím moderní techniky. S web kamerami, mobily třetí generace, či digitálními fotoaparáty s možností krátké video sekvence to není až tak veliký problém.
- Pokud odhlédneme od hesel do operačního systému, dají se všechna ostatní hesla (k emailu, informačnímu systému, účetnímu software) odchytit na úrovni klávesnice. Stačí k tomu koupit nějaký software, který to umí. Tento software zaznamenává vše, co uživatel na počítači dělá, včetně všech stisknutých kláves s podrobným výpisem v jaké to bylo aplikaci, webové stránce atd. Nebo si stáhnout nějaký jednodušší freeware na internetu.

## 4.3 Metody autentizace

Nejprve se podíváme na rozdělení metod autentizace. Tedy toho, jakým způsobem můžeme ověřovat uživatelovu identitu.

1. Heslo - Uživatel se prokáže určitou znalostí**,** kterou „by měl“ vědět pouze on, typicky heslo, šifrovací klíč uložený na disku, vstupní PIN.
2. Vlastnictví - Autentizovat se může pouze ten, kdo vlastní nějaký předmět - token. Na příklad: autentizační kalkulátor, čipová karta, USB token.
3. Biometrika - Měří se tzv. biometrické vlastnosti uživatele – otisky prstů, geometrie ruky, oční sítnice, tvar obličeje, rozpoznávání řeči, test DNA.

Dělení:

- Dvoufaktorová autentizace
- Třífaktorová autentizace

Pod pojmem dvoufaktorová autentizace rozumíme současné užití dvou těchto různých metod – faktorů ( např. token a heslo). Třífaktorová autentizace je potom využitím tokenu, znalosti i biometriky dohromady.

*Tab. 1: Srovnání autentizací u Tokenu a čipové karty*

| Možnost | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Heslo | ✓ | | | ✓ | | ✓ | ✓ |
| Token nebo čipová karta | | ✓ | | ✓ | ✓ | | ✓ |
| Biometrika | | | ✓ | | ✓ | ✓ | ✓ |

1. autentizace pomocí hesla – nejméně vhodná varianta, nejsnadnější možnost dešífrování

2. autentizace pomocí USB tokenu nebo čipové karty - patří sem hlavně různé bezkontaktní tokeny a karty s magnetickým proužkem, které nejsou zabezpečeny žádným pinem nebo heslem. Při krádeži může být předmět kýmkoli zneužit. Většinou je navíc možné předmět i poměrně jednoduše duplikovat. Tyto tokeny se využívají spíše pro zabezpečení objektů, v docházkových systémech a pod. Dnes se pro tyto účely poměrně hojně využívá bezkontaktních čipových karet.

3. autentizace pomoci biometrie - je první rozumnou variantou k využití pro autentizaci ve světě počítačů. Levnější snímače otisků prstů, ale nijak zvlášť bezpečné nejsou ( je potřeba použít dražší vybavení, u většího počtu uživatelů se to výrazně prodraží). Existuje však celá řada dalších biometrických metod. Některé z nich se používají například na v prostředí s větší mírou ochrany ( snímač duhovky oka).

4. autentizace pomocí USB token nebo čipovou kartou a heslem – je typicky realizována čipovou kartou, USB tokenem nebo autentizačním kalkulátorem. Uživatel se prokazuje vlastnictvím tokenu a přístup k tokenu je navíc chráněn heslem nebo pinem. Kalkulátor nám bohužel neposlouží jako bezpečné úložiště šifrovacích klíčů, či jiných "tajemství". Jinak má kalkulátor mnoho výhod. Základní idea autentizačního kalkulátoru je ta, že uživatel zadá heslo/PIN a po zadání kalkulátor vygeneruje jednorázové přístupové (po každé jiné) heslo.

5. 6. možnost kdy se uživatel autentizuje vůči tokenu biometrickou veličinou, nejčastěji otiskem prstu ( otiskem prstu, tokenem a heslem). Zvláště použití všech tří faktorů je více finančně náročnější než dvoufaktorová autentizace pomocí tokenu a hesla. Většina čipových karet a USB tokenů, které se dnes nasazují, jsou chráněna heslem nebo pinem. Důvodem, proč se tyto varianty často nenasazují jsou vysoká cena vybavení a hlavně samotná podstata biometriky.

Problém biometriky: Snímač získá otisk prstu a ten se potom porovnává. První problém je to, kde k porovnání dojde. Čipová karta, či USB token nemusí být pro porovnání otisků uzpůsobené. Váš vzorek otisku je pak v lepším případě uložen na kartě, ale porovnání provádí software na Vašem počítači, na který lze zaútočit. V tom horším případě je vzorek uložen na Vašem počítači, nebo dokonce v databázi na nějakém serveru. Druhý problém je ten, že porovnání dvou hesel o 8 znacích je exaktní a bez problému. Porovnání dvou otisků prstů zas tak triviální není. Čím více se nastaví systém tak, aby jste snížili pravděpodobnost přijetí podvrženého otisku, tím více se zvýší pravděpodobnost, že systém odmítne i oprávněného uživatele. A naopak. Čím více se nastaví systém tak, aby k odmítání oprávněných uživatelů nedocházelo, tím více šancí se dá útočníkovi.

## 4.4 Požadavky na zařízení

Zařízení jako jsou USB Tokeny a čip karty jsou mobilní zařízení a musí splňovat určité požadavky, jako jsou mobilita, odolnost proti okolním vlivům ale také musí splňovat vlastnosti pro které byly vytvořeny, jako jsou kapacita kompatibilita atd. Zde si některé představíme.

1. Paměťová kapacita - pokud budeme využívat předmět pro bezpečné ukládání šifrovacích klíčů, hraje úlohu také kapacita paměti. Velikost digitálního klíče pro digitální podpis se pohybuje typicky kolem 3kB (záleží na typu šifry, počtu a obsahu jednotlivých položek certifikátu). Vždy je potřeba počítat ještě s režií pro souborový systém na čipu. Šifrovací klíče zabírají jen pár stovek bitů, takže u nich se o nedostatek místa už vůbec bát nemusíme (na příklad 128 nebo 256 bitů). Standardně se dodávají čipové karty/ USB tokeny o velikostech 8, 16 a 32 kB. Pokud budeme token využívat na příklad pro přihlašování k Windows 2000 serveru, či VPN mělo by být 8KB postačující. Paměťový čip uvnitř není nezničitelný. Většinou je ale garantován minimální počet zápisů okolo 100 000. Při používání digitálních ID, která jsou platná většinou 1 rok je tento počet více než dostačující.

2. Mobilita – první otázka je, zda chceme zařízení používat na více místech (doma , kancelář atd), je nutné brát ohled na to, jaký hardware a software je k tokenu zapotřebí a jak jsou tyto složky „mobilní“, je jasné, že ovladačům a různým utilitám se nvyhneme. Velkou nevýhodou čipových karet potřeba s sebou neustále nosit čtečku. Zatímco USB tokeny čtečku nepotřebují, stačí USB port, který dnes najdete skoro na každém počítači. S bude náskok USB tokenů v této oblasti vůči čipovým kartám stále větší. Již dnes se ve velkém vyrábějí základní desky s portem USB 2.0, který nabízí dostatečnou přenosovou rychlost pro většinu počítačových periférií (teoreticky až 60 MB/s). Do starších PC je možné za několik set korun nainstalovat PCI kartu – řadič USB. To, že se čtečky čipových karet vyrábějí v provedení jako PC Card, se sériovým rozhraním, USB rozhraním, či zabudované do klávesnice již ztrácí význam a USB tokeny jsou i v mobilitě lepší, než čipové karty.

3. Odolnost konektorů ( popř. čtecího zařízení ) – Je dobré zjistit, jaká životnost je výrobcem garantována. Čipové karty, stejně tak čtečky vydrží jen určitý počet zasunutí (čipová karta například: až 10.000 zasunutí/vysunutí čipové karty). Tato hodnota je většinou dostatečně vysoká a proto je dobré se soustředit hlavně na hodnotu vlastní čtečky, než na hodnotu čipové karty. Obzvláště využívá-li počítač (tedy 1 čtečku) více uživatelů. Čtecím zařízením u USB tokenů je vlastní port USB ve Vašem notebooku, či počítači. Při opotřebení by výměna nebyla dvakrát jednoduchá. Řešením je USB prodlužovací kabel, který stojí jen pár korun. Životnost vlastního konektoru na USB tokenu je dána normou USB, ale u některých tokenů výrobci garantují až 50 000 cyklů vysunutí a zasunutí. S tím, že první chyby se začínají objevovat někde okolo 100 000 cyklů.

4. Odolnost zařízení vůči okolním vlivům – zařízení budeme neustále nosit při sobě. Je tedy důležité, aby byl token do určité míry odolný proti nárazům, lidskému potu, statické elektřině, elektromagnetickým polím atd. Důležité jsou i provozní a skladovací teploty, max. vlhkost vzduchu ( pokud necháme čip kartu ležet za sklem auta ), popřípadě zda se k předmětu prodávají nějaké obaly, pouzdra. Příkladem normy, která se tímto zabývá je ISO 7816-1. Norma definuje na příklad fyzické rozměry čipových karet, jejich odolnost proti statické elektřině a fyzickou odolnost při ohýbání karty. V této oblasti mají USB tokeny výhodu, neboť čip je chráněn plastovou skořápkou. Pouzdro u USB tokenu může být i vodotěsné. Zatímco USB tokeny standard ISO 7816-1 nepotřebují, u čipových karet je to nutnost, stejně jako splnění dalších částí této normy. Výrobci většinou uvádějí ISO 7816-1 až 4 (méně známé části jsou 5 až 10).

## 4.5 Bezpečnost

Zde se budeme bavit o čipových kartách a USB tokenech, vůči kterým se autentizujeme znalostí hesla. Heslo (alfanumerické znaky) je vždy bezpečnější než pouhý PIN – Personál Identification Number (jenom číslice).

### 4.5.1 Heslo / PIN

Čtyř místný PIN má 104 = 10 000 kombinací, zatímco čtyřmístné heslo (znaky a-z a číslice) (26+10)4 - 1 680 000 kombinací. U osmi znakového hesla/pinu je pak rozdíl již o

čtyři řády! Heslo je velmi důležité, neboť chrání token a informace v něm uložené při odcizení, či ztrátě.

### 4.5.2 Zablokování při opakovaně chybném zadání hesla

Považuji za nutnost, aby se token při několikanásobném špatném zadání hesla zablokoval. A to, ať je heslo jakkoli dlouhé. Například po 10 špatných pokusech o zadání hesla dojde k zablokování.

Co znamená zablokování:

1. Automatické smazání všech informací uložených uvnitř.
2. Po zablokování lze token pouze ručně smazat pomocí utilit.
3. Pro odblokování se musí zadat další kód, většinou označovaný jako PUK.
    - po zadání kódu PUK má uživatel s heslem/pinem dalších 10 pokusů.
    - po zadání PUK může ten, kdo zná PUK kód nastavit nové heslo/pin.

Možnosti 1 a 2 se tedy týkají hlavně tokenů, ke kterým je pouze jedno přístupové heslo a po x špatných pokusech o zadání takovéhoto hesla dojde (hned, nebo následně) ke smazání obsahu tokenu. Takovéto čipové karty a USB tokeny lze vřele doporučit právě jako uložiště digitálních klíčů, šifrovacích klíčů atd. Tokeny s jedním přístupovým heslem, jsou vždy z bezpečnostního hlediska lepší volbou. Pokud jde o možnost 3, tak je třeba rozlišovat dvě různé situace. Buď zná všechna přístupová hesla tentýž člověk, nebo více lidí.

a) Heslo/PIN a PUK kód vlastní tentýž člověk. Tento systém se používá na příklad u SIM karet v mobilních telefonech (nejde o nic jiného než o smart čip). Problém je v tom, že kód PUK uživatel buď vůbec nepoužije, nebo jen několikrát za celou dobu života řešení. Uživatelé si tedy kód PUK vůbec nepamatují a mají ho někde napsaný.Což není zrovna nejvhodnější varianta, protože potencionální zloděj může PUK najít.

b) PIN zná uživatel, zatímco PUK zná administrátor systému. Zde je velice dobré se zamyslet nad tím, co se stane po zadání kódu PUK. Dvě z nejpoužívanějších variant jsem již naznačil. Tato možnost se dá použít v systémech kde nevadí, že administrátor může nastavit uživatelovi nové heslo (na příklad: přihlašovací heslo do operačního systému).

Dalším problémem je u systémů s více přístupovými kódy fakt, že PIN je sice po několika špatných pokusech zablokován, ale vlastní PUK kód bývá této bezpečnostní pojistky zbaven.

Příklad:

U tokenů řady iKey 1000 (nejlevnější model) se nazývá PUK kód SO PIN (Security Officer). Tento kód není omezen počtem zadání špatných pokusů, uživatelův osobní PIN může administrátor nastavit, odblokovat ve smyslu umožnit několik dalších pokusů o jeho zadaní, ale také ho lze nastavit na novou hodnotu. Slouží tedy pro systémy, kde nevadí, že administrátor může nastavit nové heslo uživateli. Pro systémy, kde toto možné není (digitální podpis, šifrování dokumentů) lze v tokenu vytvořit tzv. PKI oblast. Tato je chráněna heslem PKI**,** které může Security Officer pouze odblokovat, ve smyslu umožnit dalších x pokusů.

U tokenů iKey, řady 2000 je pouze jediné a tedy bezpečnější heslo. Po x špatných pokusech se token zablokuje a pak ho lze pouze inicializovat - smazat vše uvnitř. Inicializaci může ale provést kdokoli, kdo má fyzický přistup k tokenu a nainstalovány utility. Tedy tokeny za vyšší cenu, ale bezpečnější jsou méně pohodlné.

## 4.6 Bezpečnostní certifikace

Jedinou možností je tedy spolehnout se na bezpečnostní certifikaci. V této oblasti existují dvě základní bezpečnostní certifikace: evropský ITSEC a americký FIPS.

1.Americká norma FIPS (vydaná NIST - National Institute of Standards and Technology) může mít úrovně 1 až 4. To, že dva tokeny splňují stejný "level" neznamená, že nabízejí stejnou bezpečnost. Zde se doporučuje prohlédnout certifikát, který řekne, jakých výsledků dosahuje výrobek v jednotlivých kategoriích. Vybraný token s certifikací FIPS 140-1 level 2 totiž musí ve všech kategoriích splňovat úroveň alespoň 2. V některých kategoriích ale může být ještě bezpečnější. U USB tokenů se můžete setkat na příklad s typy, kde je certifikace na čip a firmware, některé mají certifikaci i na plastovou skořápku, která je vyplněna speciálním materiálem, takže při pokusu o rozdělání se skořápka rozlomí na mnoho malých částí a je tak jednoznačně evidentní (tamper evident) pokus o proniknutí.

Pokud token získá certifikaci, většinou je to FIPS 140-1 level 2. Čipové karty, či USB tokeny s certifikací level 3 existují také, jejich zabezpečení je velmi vysoké. Kryptografických tokenů s certifikací FIPS 140-1 level 3 a vyšší využívají například certifikační autority k ukládání privátních klíčů samotné autority. Nejedná se ale o čipové karty, či USB tokeny, nýbrž o jiné speciální zařízení. Tyto zařízení jsou konstruována tak, aby se při fyzickém pokusu o otevření uložené informace zničily (nejčastěji smazaly, v krajním případě se využívá i výbušnina) - tzv. tamper resistant.

2. Evropská norma ITSEC má úrovně E1 Basic až E6 High. Celkem 8 úrovní (úrovně 2 a 3 mají dva stupně). Čipové karty a USB tokeny dosahují většinou úrovně E4 High.

3. Další v Evropě uznávanou certifikací, je norma CC (Common Criteria), nebo jinak: EAL. Tato norma je obecnější, než ITSEC a také novější. Vychází z ITSECu a dalších norem. Celkem má 7 úrovní (1..7), přičemž lze položit rovnítko mezi ITSEC E1 a EAL 2, atd. Čipové karty a USB tokeny s certifikací E4 High jsou tak zjednodušeně řečeno na úrovni EAL 5.

S USB Tokeny a čipovými kartami je to stejné jako s ostatními médii s chráněným zájmem, útoků přibývá a existuje celá řada. Většinu z nich asi jen tak kdokoli provádět nemůže, ale zas tak nedostupné tyto útoky také nejsou. Útočit se dá na:

- Software čipové karty a jeho chyby
- Nějakým způsobem vyvolat chybnou instrukci procesoru na čipu – ozáření vhodným elektromagnetickým zářením, nečekanou změnou hodinového signálu, teploty a čekat, že karta udělá nějakou chybu, které lze využít.
- Ledacos se dá zjistit také z času, který potřebuje procesor na šifrování (timing attack), z proudu, který karta při šifrování odebírá. Těmto útokům se říká útoky postranními kanály.
- Existují i finančně náročné fyzické útoky, jako třeba mikrosondy, elektronový mikroskop.

Bez certifikace si prostě nemůžete být jisti, že software a hardware je navržen správně a že karta odolá většině těchto útoků (hlavně těm „levnějším“). Proto se určitě vyplatí investovat do dražších (certifikovaných) zařízení.

## 4.7 Cena

Posledním důležitým parametrem, ve kterém se čipové karty a USB tokeny liší, je cena. Pokud budeme uvažovat, že chcete začít používat opravdu bezpečný digitální podpis a přihlašování do operačního systému, pak čipová karta bude stát něco kolem 1000,- Kč. Čtečka čipových karet, bez které se neobejdete, zhruba 2000,- Tedy jen za hardware dáte přibližně 3000,- Kč. Za tuto cenu už ale mluvíme o poměrně bezpečném hardware i s FIPS 140-1 level 2 certifikací. Stejný USB token (myšleno se stejným čipem, firmware a se stejnou FIPS certifikací ) se dá koupit o pár korun levněji. Pokud se ale budeme bavit o levnějších tokenech (tedy bez certifikace s méně bezpečnostními funkcemi) může Vás USB token vyjít klidně i o polovinu levněji, než řešení se stejně funkční čipovou kartou. Pokud ale zvolíme levnější model USB tokenu iKey2000 (který nemá FIPS certifikaci a má méně paměti), tak ten u dané firmy vychází na 1890,- Kč. No a za tuhle cenu už se možná dá koupit čtečku čipových karet, ale bez vlastní (tokenu ikey2000 odpovídající) čipové karty. Nemluvě o ještě levnějších modelech USB tokenů řady iKey 1000.

# 5 AKREDITOVANÝ POSKYTOVATEL CERTIFIKAČNÍCH SLUŽEB V ČR

## 5.1 Úvod

Občané mohou komunikovat s orgány státní správy a samosprávy prostřednictvím Internetu. Občané této možnosti však příliš nevyužívají. Chybí totiž aplikace, které jsou nutnou podmínkou pro start takovéto komunikace. Ve svém příspěvku se chci soustředit na skutečnost, že pro tvorbu těchto aplikací nestačí pouhé vydávání certifikátů, ale jsou nutné další služby certifikační autority. Jedná se zejména o časová razítka důvěryhodné archivy.

## 5.2 Akreditovaný poskytovatel certifikačních služeb

Zákonem č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů ze dne 29.června 2000 (ZoEP) byla odstartována éra užívání elektronického podpisu mimo uzavřené systémy. Ne, že by do té doby aplikace založené na technologii elektronického podpisu stagnovaly, spíše naopak.

Přibližně od roku 1997, kdy se u nás objevily první komerční aplikace využívající elektronický podpis v dnešním pojetí, prožívá tato technologie bouřlivý rozvoj. Díky ZoEP však došlo k prolomení bariery, která bránila využití elektronického podpisu ve styku občana se státní správou. ZoEP byl následně podpořen dalšími, podzákonnými normami, zejména Nařízením vlády ze dne 25.7.2001 ,vyhláškou Úřadu pro ochranu osobních údajů č. 366/2001 Sb. a Standardem ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu. Dnem vydání vyhlášky ÚOOÚ byly učiněny veškeré nutné kroky k tomu, aby mohli takzvaní poskytovatelé certifikačních služeb (PCS) nebo, chcete-li, certifikační autority požádat ÚOOÚ o akreditaci ve smyslu výše zmiňovaného zákona. První certifikační autorita, a.s. (I.CA) požádala o akreditaci dne 1.10.2001 a ta jí byla po předložení příslušné dokumentace a jejím prověření udělena. Svět PCS se tak rozdělil na dva tábory, akreditovaní poskytovatelé a ti neakreditovaní. V žádném případě to neznamená dělení na bezpečné či důvěryhodné a ty ostatní. Pouze stát za akreditované poskytovatele jakýmsi způsobem přebírá spoluzodpovědnost ve smyslu „prověření“ jeho činnosti. V neposlední řadě je vhodné zmínit i nutnost použít kvalifikované certifikáty v oblasti veřejné moci. Akreditační proces byl dlouhý a poučný. ZoEP ani žádné směrnice či vyhlášky nemohou být natolik konkrétní a jednoznačné, aby

přesně popsaly požadavky na činnost akreditovaného PCS a dokumentaci jeho systémů. Nicméně k dohodě mezi žadatelem o akreditaci a ÚOOÚ došlo a troufám si říct, že ke vzájemné spokojenosti. Proč trvala akreditace půl roku? Protože je to složitý proces a ani pro organizaci, která vydává certifikáty pět let a má bohaté zkušenosti, to nebylo jednoduché. Na druhé straně se domnívám, že ona složitost a detailní kontrola přispívá k vyšší důvěře v akreditované PCS. Vydávání kvalifikovaných certifikátů zahájila I.CA dne 25.3.2002. Rozsah činností akreditovaného PCS je limitován zákonem a proto I.CA připravila svoji činnost striktně na vydávání certifikátů a ostatní certifikačně správní funkce. Činnost PCS tedy de facto v současné chvíli znamená „pouze“ vydávání a zveřejňování certifikátů, seznamu zneplatněných certifikátů, takzvaného CRL, a s tím spojené příjímání žádostí o tyto služby. Proces vydání kvalifikovaného certifikátu žadateli je z pohledu jednotlivých kroků možné rozdělit do šesti níže uvedených kroků.

## 5.3 Kvalifikovaný certifikát

1. Příprava elektronické žádosti - každý potenciální žadatel o certifikát si nejprve sám vytvoří elektronickou žádost o certifikát (je důležité, aby žadatel tuto operaci provedl na svém PC, protože při této akci vzniká dvojice kryptografických klíčů, která je následně využívána pro realizaci bezpečné komunikace).

2. Příprava identifikačních dat - žadatel o certifikát shromáždí podle požadavků I.CA osobní identifikační materiály nutné pro vydání certifikátu, jako je např. OP a podobně. Zde je možnost definovat různé skupiny uživatelů, od kterých budou následně vyžadovány rozdílné materiály pro identifikaci, např. průkaz zaměstnance, pověření nadřízeného pracovníka. Standardní požadavky na ověření totožnosti žadatele o osobní certifikát je osobní účast a předložení občanského průkazu nebo pasu a dalšího dokladu.

3. Předání elektronické žádosti a identifikačních údajů I.CA - pro zajištění realizace požadavků klientů předpokládáme provoz infrastruktury tzv. registračních autorit (RA), žadatel tedy předá data nutná pro vydání certifikátu spolu s doklady o jejich pravosti na tomto pracovišti. V tomto případě na pracovišti veřejné registrační autority.

4. Ověření informací - pracovníci registrační autority provedou kontrolu předložených podkladů a na příslušných místech si ověří, že je možné vydat žadateli certifikát v souladu s certifikační politikou.

5. Tvorba certifikátu - tvorba certifikátu probíhá přímo v centrálním systému I.CA. Registrační autorita pouze žádost o certifikát zasílá na toto pracoviště. Je vytvořen digitální dokument příslušného formátu, který je zaslán zpět na registrační autoritu.

6. Předání certifikátu - certifikát je žadateli předán na médiu (disketa) a současně zaslán na jeho e-mailovou adresu.

Po získání certifikátu je uživatel dle smlouvy a ZoEP oprávněn s tímto nakládat podle svého uvážení. Mezi práva (a dle ZoEP de facto i povinnosti) patří možnost zneplatnění konkrétního certifikátu. K tomuto kroku mohou uživatele vést různé důvody, počínaje potenciálním či skutečným ohrožením dat pro vytváření zaručeného elektronického podpisu a ukončením své činnosti konče. Podstatné je, jak je možné u I.CA, o zneplatnění certifikátu požádat. Akreditovaný PCS nabízí několik možností. Nejčastěji využívanou cestou je podání žádosti o zneplatnění certifikátu prostřednictvím webových stránek PCS. Ty jsou přístupné 24 hodin denně, sedm dnů v týdnu a žadatel má možnost provést tuto operaci prakticky kdykoliv. Dalšími možnostmi je e-mailová komunikace a osobní žádost prostřednictvím RA. Ve všech případech je vyžadována důvěryhodná identifikace žadatele. V současné době je počet vydaných kvalifikovaných certifikátů v ČR poměrně nízký, pohybuje se kolem 2000 kusů certifikátů. Problém je především v použitelnosti kvalifikovaných certifikátů. V této oblasti se výrazně více namluvilo než udělalo. Mnohé úřady provozují takzvané elektronické podatelny, které mají usnadnit komunikaci občanů s úřadem. Právě s těmito elektronickými podatelnami je podle mého názoru spjat rozvoj elektronické komunikace s využitím zaručeného elektronického podpisu. Mnohé úřady deklarují přijímání elektronicky podepsaných podání. Tady je mimo jiné nutné podotknout, že příliš podpory nemohou úřady hledat ani v legislativě, kde je sice uvedeno, co je úřad povinen zajistit, ale není uvedeno jak. Tato výtka se netýká pouze přijímání elektronických žádostí, ale především dalších, podpůrných činností, jako je například archivace dokumentů podepsaných zaručeným elektronickým podpisem, určením času podání, atd.

## 5.4 Elektronické podatelny

Škála nabídek začíná na úrovni standardního mailového klienta na nezabezpečeném systému, vede přes řešení s využitím čipových karet a končí u skutečně kvalitně zabezpečených systémů za skutečně velké sumy. V oblasti realizace elektronických podatelen dosud u nás neexistuje žádný prakticky použitelný standard. Pokud začneme

zkoumat elektronickou podatelnu, zjistíme, že musí mít dvě rozhraní. Prvním rozhraním je uživatelské rozhraní (rozhraní uživatel/podatelna) a druhým je rozhraní mezi elektronickou podatelnou a organizací provozovaným systémem pro oběh a zpracování dokumentů . Rozhraní uživatel/podatelna je rozhodující z pohledu uživatele. Uživatel bude vyžadovat, aby toto rozhraní bylo pro něj co možná nejpřívětivější. Uživatel si nejčastěji bude přát stahovat formuláře z webového serveru do svého webového prohlížeče. Přitom bude s největší pravděpodobností očekávat formulář, který bude obdobou jemu důvěrně známého papírového formuláře. Formulář vyplní a nyní jej bude chtít elektronicky podepsat a odeslat na server úřadu. Uživatelem vyplněné údaje ve formuláři mohou například být před odesláním z prohlížeče na server převedeny do formátu XML a za využití kryptografické komponenty elektronicky podepsány. Rozhraní uživatel/podatelna tak přijímá elektronicky podepsané zprávy formátu CMS (dříve PKCS#7, Public Key Cryptography Standards, popis formátu pro výměnu dat s použitím kryptografických metod)obsahující data formátovaná v jazyce XML. Pokud je na straně uživatele místo člověka obsluhujícího PC informační systém, který generuje formuláře, pak nic nebrání tomu, aby tento informační systém formátoval data do tvaru XML, výsledek byl elektronicky podepsán a odeslán na stejný webový server. Elektronická podatelna pak verifikuje elektronický podpis přijímaných elektronických dokumentů, čísluje a archivuje dokumenty (včetně jejich elektronického podpisu) a přes rozhraní podatelna - document processing je předává do systému pro oběh dokumentů provozovaným úřadem (resp. firmou). V mnoha případech postačuje dokumenty ve formátu XML jednoduše předat dále do zpracování již bez jejich elektronického podpisu, neboť elektronická podatelna provedla prvotní archivaci dokumentu včetně jeho elektronického podpisu.

Již před několika lety výrobci softwaru mailového klienta vybavili uživatelsky přívětivou podporou tvorby elektronického podpisu. V mailové poště je navíc možné spojit elektronický podpis i s šifrováním přenášených zpráv. Sama elektronická pošta by však nebyla dostatečným motorem rozvoje technologie elektronického podpisu. To musí zajistit komerční aplikace, které dají uživateli jasnou přidanou hodnotu a tím ho de facto donutí k používání popisované technologie nenásilnou formou. Na druhou stranu pro úřady je problematické přijímat elektronicky podepsané dokumenty, které byly vytvořeny běžnými poštovními klienty. Uživatel si totiž může pomocí obecného poštovního klienta vytvořit dokument zcela libovolného formátu, jehož automatické zpracování pak může být obtížné.

Naopak elektronicky podepsanou odpověď úřadu bude uživatel nejspíše očekávat elektronickou poštou.

## 5.5 Komerční aplikace

Nabytí platnosti zákona o elektronickém podpisu jednoznačně nebylo začátkem využívání elektronického podpisu v praxi. Prvními vlaštovkami v nabídce komerčních aplikací byly banky. Mám na mysli Internetbanking, Homebanking a jinak pojmenované aplikace zajišťující bezpečnou komunikaci klienta s bankou zpravidla přes „nebezpečný“ Internet. Je to zcela logické, když si uvědomíme, že jde o peníze, a tak obě strany mají na vysoce bezpečném řešení zájem. Klienti nechtějí trávit čas na pobočkách banky a banky se zase snaží minimalizovat náklady. Z mnoha již v komerční sféře provozovaných aplikací je možné se poučit při realizaci projektů s využitím kvalifikovaných certifikátů a zaručeného elektronického podpisu. Jak se ukazuje, v současné době jsou nejaktuálnějšími problémy ve využívání elektronického podpisu, jak v komerční sféře, tak v oblasti státní správy, především problémy spojené s bezpečnou a důvěryhodnou archivací elektronicky podepsaných dokumentů a určení přesného času transakce. Právě v oblasti řešení těchto bodů vidím možnosti dalšího rozvoje služeb certifikační autority, jedná se o služby autority vydávající časová razítka a o služby důvěryhodného úložiště.

## 5.6 Časová razítka

Časové razítko (nebo též časová značka) je důkazem, že nějaký dokument existoval v konkrétním čase. Takové řešení napomáhající určení času provedené transakce má oporu v evropské legislativě, ale například i ve slovenském zákonu o elektronickém podpisu. Časové razítko je datová struktura podobná certifikátu, která obsahuje kontrolní součet (otisk) dokumentu a čas vydání časového razítka. Časové razítko je elektronicky podepsáno autoritou pro vydávání časových razítek (Time Stamping Authority –TSA). Takže časové razítko svazuje dokument s časem uvedeným v časovém razítku a výsledek je stvrzen nezávislou třetí stranou – TSA. Časové razítko je možné vytvářet z celého dokumentu (např. z celého platebního příkazu), ale zajímavější je časové razítko z elektronického podpisu. Takové časové razítko je pak důkazem o tom, že elektronický podpis existoval před okamžikem vydání časového razítka. Z laického pohledu časové razítko z elektronického podpisu prodlužuje možnost verifikace elektronického podpisu i

po vypršení certifikátu určeného k původní verifikaci podpisu. Norma ETSI TS 101 733 předepisuje přidávání časového razítka z elektronického podpisu k elektronickému podpisu jako tzv. nepodepisovaný atribut. Jelikož se jedná o klientem nepodepisovaný atribut, tak časová razítka z elektronického podpisu mohou například k platebnímu příkazu dodávat i platební brány přijímající v elektronicky podepsané platební příkazy od klientů na straně banky.

## 5.7 Důvěryhodné archivy

Podobně jako klasické papírové dokumenty, tak i elektronické dokumenty je třeba archivovat. Archiv garantuje zejména, že se dokument neztratí, že nebude změněn a že se nedostane do nepravých rukou. Elektronické dokumenty mají navíc výhodu v tom, že je možné snadno kopírovat. Jednotlivé kopie pak mohou být uloženy na geograficky vzdálených pracovištích archivu. Tím se předejde ztrátě dokumentu při živelných pohromách nebo při válečných konfliktech. Nevýhodou elektronických dokumentů je, že jsou uloženy na médiích, která stárnou podstatně rychleji než papírové dokumenty. Elektronické dokumenty se tak musí v archivu pravidelně přehrávat kopírováním na nová média. U elektronicky podepsaných dokumentů nastupuje ještě další aspekt, kterým je efekt „vyprchávání“ elektronického podpisu.

Pokud chceme dlouhodobě archivovat elektronicky podepsaný dokument, pak jej uložíme v důvěryhodném archivu (Trusted Archive Authority - TAA). Základní funkcí TAA pak je, že je to důvěryhodný archiv, tj. že mu důvěřujeme. Pokud tedy dokument z TAA po letech vyzvedneme, tak předpokládáme, že je pravý. Nemusíme se tedy zabývat verifikací elektronického podpisu. Avšak podobně jako u listinných dokumentů se může stát, že se někdo pokusí napadnout platnost archivovaného dokumentu. Pak se nám jako indicie hodí zmíněná časová razítka z elektronického podpisu. Cílem TAA je tedy v případě elektronicky podepsaných dokumentů také zajistit, aby veškeré elektronické podpisy u archivovaných dokumentů byly řádně časově orazítkovány. Před vypršením platnosti samotných časových razítek pak TAA automaticky elektronické podpisy opět „přerazítkuje“ čerstvými tzv. archivními časovými razítky, čímž se udržuje platnost elektronického podpisu až do okamžiku skartace dokumentů.

## 5.8 Poskytovatelé Certifikačních služeb působících v ČR

Kvalifikované systémové certifikáty již vydávají všichni akreditovaní poskytovatelé certifikačních služeb – tj. První certifikační autorita a.s., Česká pošta s.p. a eIdentity a.s. Stejně tak všichni tři akreditovaní poskytovatelé nabízejí služby mobilních registračních autorit. V této práci bych chtěl hlavně vysvětlit principy České pošty.

### 5.8.1 Veřejná certifikační autorita České pošty - PostSignum

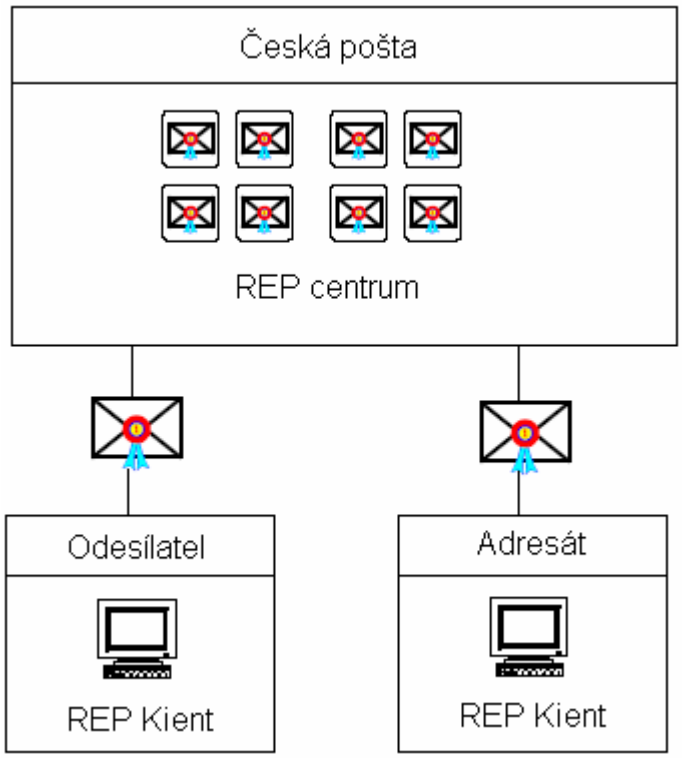
Certifikační služby České pošty jsou zaměřeny především na právnické osoby, které požadují vydávat certifikáty „ve velkém“. Certifikační politiky jsou proto navrženy tak, aby proces vydávání certifikátů byl pro organizace co nejjednodušší. Zákazník uzavře s Českou poštou smlouvu o poskytování certifikačních služeb. Smlouva mimo jiné obsahuje údaje o oprávněných osobách, které smějí jménem zákazníka definovat, komu je dovoleno žádat o certifikáty podle jednotlivých certifikačních politik. Oprávněné osoby pak zasílají certifikační autoritě seznamy žadatelů a rozsah jejich oprávnění ohledně žádostí o certifikáty. Žadatelé mohou následně navštívit kterékoliv ze sedmdesáti kontaktních míst po celé republice. Jejich totožnost a podávaná žádost o certifikát jsou kontrolovány oproti informacím, které certifikační autoritě zaslaly oprávněné osoby. Certifikát je vydán pouze tehdy, pokud jsou žádost o certifikát a totožnost žadatele v souladu s těmito údaji. V případě úspěšného ověření je okamžitě vydán certifikát, což znamená, že k vydání certifikátu stačí jedna návštěva žadatele na kontaktním místě.

Tento model umožňuje přirozeně delegovat pravomoci uvnitř organizace zákazníka a eliminuje požadavek, aby se každou jednotlivou žádostí o certifikát zabýval statutární zástupce organizace či jiná osoba s odpovídajícím podpisovým právem.

Veřejná certifikační autorita České pošty poskytuje služby na vysoké profesionální úrovni, za bezpečnostních a provozních podmínek, které se optimálně blíží podmínkám kladeným na akreditované poskytovatele certifikačních služeb podle zákona č.227/2000 Sb. o elektronickém podpisu. Jádrem certifkační autority je software UniCERT firmy Baltimore Technologies, který byl doplněn podpůrnými aplikacemi vyvinutými společností ICZ.

***Aplikace Registrovaná elektronická pošta***

Česká pošta se počátkem roku 2002 rozhodla obohatit nabídku svých služeb o elektronickou podobu listovní doporučené zásilky s doručenkou. Cílem bylo poskytnout široké veřejnosti elektronický servis zaručující předání elektronických dat mezi odesilatelem a adresátem stejně bezpečně a průkazně, jako je tomu u klasických doporučených zásilek. Řešení je znázorněno na 0br.




*Obr. 5: Registrovaná elektronická pošta*

Každý, kdo chce systém REP použít, musí být registrován jako uživatel této služby a musí být vybaven speciálním klientským programem REP Klient. Jedna instalace programu REP Klient představuje tzv. REP přihrádku. Odesilatel se pomocí programu REP Klient připojí do REP Centra, kde uloží zásilku určenou adresátovi. Adresát je z REP Centra vyrozuměn, že v jeho schránce v centru se nachází zásilka k vyzvednutí. Programem REP Klient se připojí do REP Centra, kde zásilku převezme.

Obdobně jako u listovní doporučené zásilky s doručenkou i v systému REP se elektronicky potvrzuje, že REP Centrum převzalo zásilku od odesilatele, že adresát zásilku vyzvedl nebo nevyzvedl a že ji následně přečetl. Aby byla zajištěna důvěrnost přenášených dat, zásilky jsou chráněny pomocí standardních digitálních obálek, kde data jsou šifrována

pomocí veřejného klíče adresáta. Obsah zásilky je tedy pro REP Centrum nečitelný, podobně jako poštovní úředníci nemohou přečíst klasický dopis vložený v neprůhledné zapečetěné obálce. Integrita zásilek a nepopiratelnost jejich původu je zajištěna pomocí elektronického podpisu. Elektronické záznamy o přepravovaných zásilkách jsou v systému REP uloženy po dobu pěti let, aby bylo možné zpětně dohledat, jak zpracování zásilky probíhalo. Poštovné u klasických zásilek se platí předem, na přepážce, za každou zásilku zvlášť. Zákazník systému REP si službu předplácí na určitý časový interval (v současné době na rok), v rámci kterého může poslat prakticky neomezený počet zásilek. Je ovšem třeba zajistit, aby ke službě měli přístup pouze registrovaní zákazníci. Proto má každá REP přihrádka vlastní certifikát, který se používá pro autentizaci přihrádky.

***Vydávání certifikátů***

Základní službou, kterou nabízí každá certifikační autorita, je vydávání certifikátů. Žadatel o certifikát se dostaví na kontaktní místo, kde předloží elektronickou žádost o certifikát (na disketě) a dokumenty vyžadované certifikační politikou. Po ověření údajů je vydán certifikát, který si žadatel odnáší na disketě, spolu s certifikáty certifikační autority. Certifikační autorita přijímá žádosti o certifikáty ve standardním formátu PKCS#10. Součástí aplikace REP je proto procedura pro generování páru klíčů (soukromého a veřejného) a elektronické žádosti ve formátu PKCS#10. Soukromý klíč zůstává uložen v chráněném úložišti klíčů v aplikaci REP, veřejný se stává součástí žádosti o certifikát. Certifikát vydaný CA PostSignum je importován zpět do aplikace REP, která k tomu má patřičné nástroje.

Aplikace REP využívá tři typy certifikátů:

- osobní certifikáty pro uživatele aplikace REP Klient,
- certifikáty pro jednotlivé technologické komponenty a procesy (REP Klient, REP Centrum),
- šifrovací certifikáty. Ty jsou určeny k vytváření digitálních obálek, které může „otevřít“ více uživatelů.

Jednu REP přihrádku může obsluhovat více uživatelů, z nichž každý musí být schopen přečíst došlou poštu. Proto sdílejí jeden soukromý klíč, kterým lze došlou poštu dešifrovat. Pokud však kterýkoliv uživatel odesílá poštu, připojuje k ní svůj elektronický podpis

vytvořený pomocí vlastního nesdíleného soukromého klíče, aby bylo možné ověřit, který z uživatelů zprávu odeslal.

CA PostSignum vydává všechny tři typy certifikátů. Šifrovací certifikát byl „šit na klíče, jejichž odpovídající soukromé klíče sdílí více osob. míru“ aplikaci REP, protože není obvyklé, aby byly vydávány certifikáty pro veřejné

***Revokace certifikátů***

Certifikát, který je prohlášen za zneplatněný, je zařazen na seznam zneplatněných certifikátů (Certificate Revocation List - CRL). Žádost o zneplatnění (revokaci) lze podat několika způsoby, vždy se však jedná o administrativní proces, který nevyžaduje žádnou přímou podporu v aplikaci REP.

***Předání certifikátů certifikační autority***

Aby mohl kterýkoliv uživatel pracovat s certifikáty vydanými certifikační autoritou, musí této certifikační autoritě důvěřovat. V elektronickém světě svou důvěru vyjádří tak, že certifikát certifikační autority importuje do úložiště certifikátů důvěryhodných certifikačních autorit. V aplikaci REP je možné importovat certifikáty důvěryhodných certifikačních autorit, pokud se však používají pouze certifikáty vydané CA PostSignum, není to zapotřebí, neboť certifikáty CA PostSignum jsou součástí distribuce programu REP Klient.

***Informace o vydaných certifikátech a CRL***

Informace o certifikátech a seznamech zneplatněných certifikátů (CRL) vydaných CA PostSignum lze získat přes webové rozhraní (protokolem http) nebo z LDAP serveru certifikační autority.

REP Centrum udržuje adresář všech REP přihrádek. Ke každé z nich eviduje certifikát, kterým se bude přihrádka autentizovat, a šifrovací certifikát pro přihrádku. V adresáři REPu se udržují pouze odkazy, podle kterých lze tyto certifikáty vyhledat na LDAP serveru CA PostSignum.

Pro ověření platnosti certifikátů je zapotřebí aktuální CRL, který je kvůli dostupnosti uložen na třech místech: na www serveru CA PostSignum, na LDAP serveru CA

PostSignum a také u nezávislého poskytovatele internetového připojení. Odkazy na tato tři místa jsou uvedena v každém certifikátu. Kterákoliv komponent aplikace REP, která ověřuje platnost certifikátu a nemá k dispozici aktuální CRL, zkouší tento seznam získat na některém z uvedených míst (v pořadí, jak jsou v certifikátu uvedena). Pokud by aktuální seznam nebyl na žádném z těchto míst k dispozici, ověřování platnosti certifikátu by selhalo.

***Budování CA PostSignum***

CA PostSignum byla budována podle metodiky KeySteps společnosti Baltimore. V souladu s touto metodikou byla při technické specifikaci řešení navrhována též rozhraní k dalším aplikacím. Nejednalo se pouze o aplikace, které budou využívat certifikáty vydávané CA PostSignum, ale též o interní informační systémy České pošty, jako je SAP, kde se účtují poplatky za vydané certifikáty. Při integračním testování pak byla ověřována spolupráce mezi aplikacemi. Registrovaná elektronická pošta sloužila jako referenční aplikace, pomocí které byly testovány všechny funkce, které budou používat další elektronické služby České pošty.

# II. PRAKTICKÁ ČÁST

# 6 VYUŽITÍ ELEKTRONICKÉHO PODPISU

Kde mohu kvalifikované certifikáty využít?

Elektronický podpis se využívá zejména v komunikaci s úřady státní správy, při komunikaci s ostatními institucemi, které uznávají kvalifikované certifikáty. V této práci se budu zabývat využitím elektronického podpisu při podávání daňových přiznání a další využití zejména v poslední době zaznamenává elektronické žádosti o dotace v Evropské unii, kterou v české republice jako jediná firma poskytoje CzechInvest prostřednictvým internetové aplikace eAccount .

## 6.1 Žádosti o dotace v Evropské unii

V české republice poskytuje elektronické žádosti o dotace v evropské unii firma CzechInvest pomocí aplikace eAccount.

## 6.2 Elektronické žádosti eAccount

Ve snaze snížit administrativní náročnost a zefektivnit proces zpracování žádostí o dotace vytvořila agentura CzechInvest internetovou aplikaci eAccount. Díky ní budou žadatelé vyplňovat formuláře, předkládat žádosti a dodávat potřebné přílohy přímo ze své kanceláře nebo z domova elektronickou formou. Uživatelé zde naleznou veškeré informace, které v souvislosti s podáním projektu a jeho realizací budou potřebovat. Aplikace eAccount jim zároveň umožní průběžně sledovat proces administrace a aktuální stav hodnocení žádosti. eAccount je internetová aplikace vytvořená pro potřeby žadatelů a příjemců dotace v rámci Operačního Programu Podnikání a Inovace. Jejím cílem je zpříjemnit a celkově zjednodušit nejen předkládání žádostí o podporu, ale i veškerých dalších formulářů a dokumentace. EAccount slouží jako prostředek komunikace mezi Žadatelem a příslušnou implementační agenturou programu. Rovněž usnadňuje práci s formuláři (zejména formou nápovědy a instrukcí na obrazovce) a vylepšuje informovanost o aktuální fázi projektu a následných krocích, které je možné (potřeba) v dané chvíli učinit.Osoby oprávněné jednat za danou společnost (organizaci) musejí vlastnit kvalifikovaný elektronický podpis, kterým se podepisuje veškerá dokumentace podávaná elektronicky prostřednictvím této aplikace. Hlavním popudem bylo zdlouhavé vyřizování mnohdy mnohasetstránkový svazků

dokumentů, prodlevy v řádu týdnů či měsíců, nepochopitelná administrace a minimální komunikace s hodnotiteli projektů. Vždyť připomínky k této praxi měla dokonce i Evropská komise.

Některé úřady se naštěstí rozhodli opustit starý systém a vstoupit do dalšího období s novou technoligií. Příkladem může být CzechInvest, který bude žádosti do Operačního programu Podnikání a inovace přijímat prostřednictvím aplikace eAccount. Jako první tak budou firmy podávat projekty do programů Rozvoj a Marketing. Systém přináší řadu výhod. Je snadno ovladatelný a nevyžaduje žádné speciální programové vybavení. Při vyplňování formulářů žadatele upozorní na chyby, takže odpadají problémy s následným opravováním formálních nedostatků. Aplikace zároveň umožní průběžně sledovat proces administrace a aktuální stav hodnocení žádosti.

### 6.2.1 Hlavní myšlenka

eAccount v prvé řadě převádí celé dosud papíry zamořené řízení do elektronické podoby. Hlavní myšlenkou je aby odpadly nekonečné papírování. V minulém období nebyly výjimkou několikasetstránkové projekty, včetně mnoha povinných kopií a pouhá formální kontrola žádosti zabrala jednomu pracovníkovi minimálně půl dne.Teď žadatel v každé chvíli dodá jen to, co je právě potřeba. Například na začátku vyplní do formuláře pouze základní údaje o sobě a o svém projektu. Do dvou týdnů dojde odpověď, jestli je projekt přijatelný a má smysl o dotaci žádat. Pokud ano, sdělíme se mu zároveň termín dodání plné žádosti.

### 6.2.2 Podávání

V praxi má projekt dvě fáze:

- žadatel si na stránkách CzechInvestu založí elektronický účet a v jeho rámci vyplní registrační žádost, jejíž součástí je i finanční výkaz. Odborníci v agentuře následně zhodnotí, zda žadatel a projekt splňují kritéria daná programem, typicky třeba podmínku dobrého finančního zdraví. V případě úspěšného absolvování tohoto prvního kola je na to žadatel upozorněn e-mailem. Zároveň mu v tuto chvíli začínají vznikat takzvané způsobilé výdaje a projekt se může začít realizovat.

- v druhá fáze, v ní musí předkladatel vyplnit Plnou žádost, zahrnující konkrétní informace o samotném projektu, jeho rozpočtu, harmonogramu a dalších závazných ukazatelích, včetně studie proveditelnosti. Následuje proces hodnocení projektu a vůbec další jednotlivé fáze, v zásadě shodné s dosavadní praxí.

Výhody nového dvoufázového systému jsou zřejmé. Pokud agentura zamítne už registrační žádost, podnikatel ušetří čas i peníze, které by musel věnovat do podrobného zpracování „beznadějného" projektu. Hlavně předkladatelů menších projektů se dotkne podstatné zjednodušení formuláře finančního výkazu. U nich se také nejvíce projeví časové úspory díky hodnocení projektů v různých režimech. A zmizí i nutnost běhat při každém nedostatku či chybě do regionální kanceláře, vše se pohodlně vyřeší po internetu. V neposlední řadě jsme navíc úplně odstranili řadu příloh

Elektronická komunikace navíc umožňuje daleko lepší kontrolu nad administrativním vyřizováním projektu. To se projeví například tehdy, když se žadatel při vyplňování formuláře zmýlí nebo něco opomene.

EAccount má nastavený systém hlášení chyb, takže každý může kliknutím na odkaz zjistit, jestli je vše vyplněné správně. U chyb se potom zobrazí červený obdélník, takže je jasné, co je potřeba dát do pořádku. Vycházíme tady ze zkušeností minulého období, kdy zbytečné chyby značně zdržovaly proces hodnocení projektu. Systém navíc nabízí i zabudovanou nápovědu a pro případ obtížnějšího problému i telefonickou linku.

Ideální by samozřejmě bylo, kdyby CzechInvest následovaly i další zodpovědné instituce se svými programy. Zatím totiž systém funguje pouze pro Operační program podnikání a inovace. Zkušenosti z okolních zemí jsou takové, že většinou žadatelé podávají projekty v papírové formě, čestnou výjimkou je Estonsko, kde se vše podává elektronicky.

### 6.2.3 Charakteristika eAccount

- seznam projektů a jejich charakteristika
- registrační žádost – po jejím předložení dojde do deseti dnů k posouzení přijatelnosti projektu a žadatele
- plná žádost – doplnění detailních informací, včetně studie proveditelnosti a finanční realizovatelnost projektu

- formulář žádosti o platbu
- monitoring projektu – žadatel uvádí aktuální údaje k ukazatelům
- změna projektu – slouží k provedení změn u konkrétního projektu v různých fázích projektového cyklu
- nástěnka – na ní agentura komunikuje s žadatelem, upozorňuje ho na chyby, lhůty a podobně; doplňuje ji i komunikace e-maily

### 6.2.4 Obstarání eAccount

- žadatel si na webových stránkách www.czechinvest.cz založí takzvaný master účet; vyplní potřebné identifikační údaje a obdrží heslo * v rámci účtu může přidělit přístupová práva i dalším subjektům, které s ním případně na projektu spolupracují
- k založení a vedení účtu není zapotřebí žádné speciální vybavení, pouze počítač s připojením k internetu a vyřízený elektronický podpis
- prostřednictvím tohoto účtu poté žadatel vede komunikaci s CzechInvestem a překládá jednotlivé žádosti a formuláře

## 6.3 Podání daňového přiznání

Od března 2003 lze podávat některá daňová přiznání pomocí internetu (přiznání k DPH, k dani silniční, k dani z nemovitostí a Oznámení o nezdaněných vyplacených částkách FO). Podání se uskutečňuje odesláním datové zprávy, opatřené zaručeným elektronickým podpisem, České daňové správě. Díky elektronickému podpisu odpadá navštěva instituce, dále má jistotou adresáta i odesílatele (kterou elektronický podpis oběma poskytuje) tu, že během přenosu nebyla zpráva změněna, díky elektronickému podpisu nelze dodatečně popřít, že odesílatel e-mail s příslušným obsahem odeslal. Sám „majitel“ elektronického podpisu má naprostou kontrolu nad svým podpisem, má zaručeno, že se jeho podpis nepokoušel nikdo napodobit - což se u ručního podpisu nedá vyloučit.

Bez el. podpisu je nutné dodat ještě papírovou verzi podání (internet pomůže jen s vyplněním formulářů). Dokument informuje o technických předpokladech a o postupu při podávání daňového přiznání touto formou.

Plně internetové podání se uskutečňuje prostřednictvím datové zprávy opatřené zaručeným elektronickým podpisem, ověřeným certifikační autoritou.

***Dosud je možné, aby daňový subjekt podával elektronickou formou tato přiznání:***

- Přiznání k dani z přidané hodnoty
- Souhrnné hlášení VIES
- Daň z příjmu fyzických osob
- Daň z příjmu právnických osob
- Vyúčtování daně z příjmů fyzických osob ze závislé činnosti a z funkčních požitků včetně všech příloh
- Daňové přiznání k dani silniční
- Daňové přiznání k dani z nemovitostí
- Hlášení platebního zprostředkovatele podle § 38fa zákona 586/1992 Sb.
- Obecné písemnosti

### 6.3.1 Aplikace EPO

Všechna uvedená daňová přiznání lze v elektronické podobě zpracovávat prostřednictvím internetové aplikace EPO (Elektronické podání pro daňovou správu). Aplikace EPO je skutečnou aplikací, která existuje jak v online podobě (v rámci příslušných internetových stránek), tak také v podobě samostatné aplikace pro offline použití. Uživatel tak může data vkládat jak online, tak i do stažených formulářů aplikace v době, kdy není připojen. Teprve následně pak může obsah svého podání odeslat. Stejně tak je možné předat připravené podání v elektronické formě na datovém nosiči (např. na disketě). Služeb EPO tak může využít i ten, kdo má k dispozici pouze pomalé připojení k internetu.

***ONLINE verze aplikace EPO***

Online verze aplikace EPO je provozována pomocí společného technického zařízení správce daně a je i pro takto uskutečněná podání elektronickou podatelnou, kterou naleznete na stránkách ministerstva financí.

Při vyplňování daňového přiznání je program vybaven kontrolou vložených údajů, přičemž po volbě příslušné ikony pro kontrolu program upozorní v Protokolu chyb na případné

chyby, které je třeba opravit pro bezchybné podání. Zpracované nebo načtené daňové přiznání nebo jiné podání lze odeslat prostřednictvím sítě Internet na společné technické zařízení správců daně nebo uložit na disketu. Podání můžete učinit prostřednictvím datové zprávy, opatřené zaručeným elektronickým podpisem, nebo na počítačové sestavě prostřednictvím datové zprávy, neopatřené zaručeným elektronickým podpisem.

V případě zvolení podání prostřednictvím datové zprávy, opatřené zaručeným elektronickým podpisem, je odesílatel vyzván k podpisu datové zprávy, při odeslání prostřednictvím sítě Internet na společné technické zařízení správců daně. Po odeslání prostřednictvím sítě Internet se datová zpráva uloží do souboru označeného v názvu „-potvrzeni.p7s“.

***OFFLINE verze aplikace EPO***

Offline verze aplikace EPO umožňuje i bez stálého připojení k síti Internet vyplnit daňové přiznání nebo napsat daňové podání. Instalace aplikace je dostupná ke stažení a nainstalování na vlastní personální počítač na internetových stránkách České daňové správy.

Offline verze aplikace EPO pracuje podobně jako aplikace přístupná online na internetových stránkách České daňové správy, tj. s potřebnou nápovědou a kontrolou vyplněných údajů.

***Bezpečnost aplikace***

Vlastník aplikace EPO, kterým je Ministerstvo financí (MF), zaručuje, že aplikace neprovede žádnou operaci, která by mohla uživatele poškodit. To stvrzuje pomocí tzv. certifikátu, kterým se ověřuje, že aplikace je opravdu původní, nikým nemodifikovaná. Certifikát je v prohlížeči zobrazen po načtení.

***Odeslání přiznání prostřednictvím zaručeného elektronického podpisu***

Odesílaný soubor (datovou zprávu) se opatří zaručeným elektronickým podpisem podpisem a odešlete se. Po odeslání se datová zpráva uloží do souboru označeného v názvu potvrzeni.p7s. U každého podání je nejprve zkontrolována platnost elektronického podpisu a pak je desláno na cílový finanční úřad.

# ZÁVĚR

Se vstupem do 21.století je více než kdy jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů na státní správu, zavést elektronické peníze a v neposlední řadě zajistit uznání elektronického podpisu, jako jednoho se základních kamenů elektronické společnosti. Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se zařadí mezi moderní, prosperující národy. Při vytváření prostředí legislativního, ekonomického, vědeckého je potřeba respektovat daný stav v Evropské unii. Běžným uživatelům dává možnost bezpečné komunikace na všech úrovních, zejména v komunikaci s úřady veřejné správy, podavání daňových přiznáních a to komunikaci ve firmách a to vše v čase nesrovnatelně rychlejším, než bylo zvykem. Cílem této práce bylo zpracovat praktické využití elektronického podpisu v podniku. Toto využití je velmi specifické, protože podniky mohou s úřady komunikovat na několika úrovních. Tato práce jsem vyzvednul využití elekrtronického podpisu k podávání dáňových přiznání pomocí aplikace EPO, kterou v dnešní době využívá stále více lidí. Opodstatnění je jednoduché, pomocí internetové aplikace mohou podniky a občané podávat daňové přiznání v pohodlí domova, nemusí vypisoat papíry a v podtatě nemusí komunikovat s úřady. Daňové přiznání je opatřeno elektronickým podpisem, kterým se jednoznačně autentizuje odesílatel. Další využití je podávání žádostí o granty v Evropské unii. Tuto službu v české republice jako jediná společnost poskytuje CzechInvest prostřednictvým internetové aplikace eAccount. Využití v dnešní době je obrovské a stále více lidí touto cestou komunikuje. Zabýval jsem se zde zákonem o elektronickém podpisu, protože je velmi důležité znát zákon samý, dále práce vysvětluje kryptografické algoritmy používané v elektronickém podpisu. Velmi důležitou věcí, kterou jsem se zabýval bylo bezpečné uložení elektronického klíče, tento klíč lze uložit na osobním počítači, kde pracuje, ale vystavuje se riziku, že mu případný útočník může klíč odcizit a následně zneužít. Vdalší kapitole jsem se zabýval peskytovateli certifikačních služeb, české republice působí tři poskytovatelé certifikačních služeb. V této práci jsem se zabýval poskytovatelem elektronického podpisu a to Českou poštou. Zde jsem se rozebíral poskytovaní služby touto certifikační autoritou.Práce mi byla velkým přínosem, protože jsem díky ní získal znalosti o elektronickém podpisu a rozšířil si přehled o jeho využití.

# SEZNAM POUŽITÉ LITERATURY

**Monografická literatura:**

[1] KOLEKTIV AUTORŮ *Elektronický podpis.* Olomouc, 2002. ISBN 80-7263-125-X.

[2] DOBDA, Luboš. *Ochrana dat v informačních systémech.* 1. vyd. Praha: Grada Publishing, 1998. 288 s. ISBN 80-7169-479-7.

[3] KLÍMA, Vlastimil. *Hashovací funkce a kódy: výživná hashe. In Chip.* Březen 1999, č. 3

[4] VONDRUŠKA, Pavel. *Kryptologi, šifrování a tajná pésma.* Praha, 2006. ISBN 0-256-07779-X.

**Elektronické zdroje:**

[5] *Wikipedia, Elektronický podpis* [online]. Dostupné z <http://cs.wikipedia.org/wiki/GIS>

[6] Nevosád ,L.: *Jak jsem si pořídil elektronický podpis České pošty* [online]. Dostupné z <http://www.lupa.cz/clanky/jak-jsem-si-poridil-elektronicky-podpis-ceske-posty/>

[7] Vondruška, P.: Přehled standardů pro elektronické podpisy (výběr). In: Crypto-World, 9/2000, dostupné z <http://www.mujweb.cz/veda/gcucmp/>

[8] Úřad pro ochranu osobních údajů. *Odůvodnění.* [online] c2001, Dostupné z <http://www.uoou.cz>.

[9] Kopta, M.:*, Elektronický podpis obcím* [online].

Dostupné z <http://www.lupa.cz/zpravicky/elektronicky-podpis-obcim/>

[10] Kožušník, E.:*, Elektronický podpis a španělská vesnice* [online]. Dostupné z <http://www.lupa.cz/clanky/elektronicky-podpis-a-spanelska-vesnice/>

[11] CzechInvest.: *eAccont* [online].

Dostupné z
<http://www.czechinvest.org/eaccount>

[12] Hajsterová ,H.: *Elektronický podpis k dostání na poštách* [online]. Dostupné z <http://www.chip.cz/novinky/?clanek=8707>

[13] Pinkava ,L.: *Moderní kryptografické algoritmy* [online]. Dostupné z <http://crypto-world.info/pinkava/konference/cack.pdf>

[14] Buy, R.: *Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování* [online]. Dostupné z

<http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=264&clanekID=265>

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| I.CA | První Certifikační Autorita, a.s., jediný akreditovaný PCS v ČR |
| CA | Certifikační autorita, subjekt vydávající certifikáty k veřejným klíčům |
| CRL | Certificate Revocation List, seznam zneplatněných certifikátů |
| DSA | Digital Signature Algorithm, asymetrická šifra pro elektronický podpis |
| DSS | Digital Signature Standard, US standard pro elektronický podpis |
| EP | Elektronický podpis |
| EU | Evropská unie, uskupení evropských států |
| ISVS | Informační systémy veřejné správy |
| MD2 | Message Digest 2, hashovací algoritmus vyvinutý RSA Data Security, Inc. |
| MD5 | Message Digest 5, hashovací algoritmus vyvinutý RSA Data Security, Inc., délka hashe 128 bitů |
| PCS | Poskytovatel certifikačních služeb |
| PIN | Personal Identification Number, osobní identifikační číslo sloužící pro přístup k citlivým informacím |
| PKI | Public Key Infrastructure, systém pro práci s veřejnými klíči |
| RA | Registrační autorita, pobočka CA, která provádí kontakt s klientem, sbírá požadavky o vydání certifikátů a odesílá je CA ke zpracování |
| REP | Registrovaná Elektronická Pošta, služba poskytovaná Českou poštou, |
| RIPEMD-160 | hashovací algoritmus, délka hashe 160 bitů |
| RSA | Rivest – Shamir – Adelman, asymetrická šifra pojmenovaná podle počátečních písmen příjmení autorů |
| SHA-1 | Secure Hash Algorithm, hashovací algoritmus, délka hashe 160 bitů |
| TSA | Time Stamp Authority, Autorita pro časová razítka, instituce přiřazující aktuální čas přijatým datům pomocí časového razítka |
| USA | United States of America, stát v severní Americe |

| | |
|---|---|
| USB | Universal Serial Bus, sériové rozhraní pro připojení periferií, podporuje technologii Plug-and-Play |
| ÚOOÚ | Úřad na ochranu osobních údajů |
| ZoEP | Zákon o elektronickém podpisu, č. 227/2000 Sb. |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK