

BAKALÁŘSKÁ PRÁCE

Teorie a praxe elektronického podpisu

Tomáš Stegura

2004

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra systémové analýzy

Student : **Tomáš Stegura**
Vedoucí bakalářské práce : **Doc. Ing. Prokop Toman, CSc.**
Recenzent bakalářské práce : **Ing. Vojtěch Kment**

TÉMA BAKALÁŘSKÉ PRÁCE

Teorie a praxe elektronického podpisu

ROK : 2004

Prohlášení

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze kterých jsem čerpal.

V Praze dne 1.9.2004

.....
podpis

Předmluva

V textu jsem záměrně používal názvosloví uváděné v připravované novele zákona o elektronickém podpisu. To má čtenáři usnadnit orientaci v současných dokumentech týkajících se problematiky. V částech, které se věnují předchozím zněním zákona, jsou ponechány historické názvy.

Poděkování

Rád bych tímto poděkoval panu Doc. Ing. Prokopu Tomanovi, CSc. za to, že mi pomohl zaměřit úsilí tím správným směrem a umožnil překonat chvíle nejistoty svým trpělivým vedením. Dále bych chtěl vyjádřit svůj dík panu Ing. Vojtěchu Kmentovi, který mi umožnil hlubší náhled do problematiky elektronického podpisu a poskytl mi cenné studijní materiály. Mé poslední díky směřují k panu Ondřejovi Zaoralovi, který mi pomohl otestovat elektronický podpis v praxi při využití v elektronické poště a byl mi cennou morální podporou.

Obsah

Abstrakt	6
Abstract.....	7
Úvod	8
1 Geneze elektronického podpisu	9
2 Vysvětlení pojmů	11
2.1 Elektronický podpis	11
2.1.1 Identifikace (Identification).....	12
2.1.2 Autentizace (Authentication).....	12
2.1.3 Integrita (Integrity).....	12
2.1.4 Nepopíratelnost (Non-repudiation).....	12
2.2 Certifikát.....	13
2.3 Poskytovatel certifikačních služeb.....	13
3 Asymetrické kryptování a elektronický podpis	14
3.1 Kryptosystém RSA.....	16
3.2 Kryptosystém DSA.....	17
3.3 Hashovací funkce	17
4 Podepisování a ověřování.....	18
5 Důvěra	20
5.1 Systém PGP	20
5.2 Standard X.509.....	21
6 Certificate Revocation List	23
7 Prostředky pro vytváření elektronického podpisu	24
8 Legislativa v ČR.....	26
8.1 Zákon o elektronickém podpisu.....	26
8.1.1 Rozbor zákona o elektronickém podpisu	27
8.2 Vyhláška 366/2001 Sb.	29
8.2.1 Rozbor vyhlášky 366/2001 Sb.....	29
8.3 Nařízení vlády 304/2001 Sb.	31
8.4 Novela zákona o elektronickém podpisu.....	32
8.4.1 Nové pojmy	32
Časové razítko.....	32
Elektronická značka	33
8.4.2 Rozbor novely zákona o elektronickém podpisu	34
9 Elektronický podpis v praxi.....	38
9.1 Stav na českém trhu.....	38
9.2 Model získávání kvalifikovaného certifikátu.....	39
9.3 Vlastní zkušenosti se získáváním kvalifikovaného certifikátu	39
9.4 Možnosti využití elektronického podpisu v ČR.....	41
9.4.1 Komunikace s veřejnou správou.....	42
Ministerstvo financí.....	42
Ministerstvo práce a sociálních věcí.....	42
9.4.2 Zdravotní pojišťovny	43
9.4.3 Česká pošta	43
9.4.4 Bezpečná a ověřitelná e-mailová komunikace	44
9.4.5 Shrnutí možností využití elektronického podpisu	44

10	Podpisování e-mailu v prostředí MS Outlook	45
11	Využívání elektronického podpisu v ČR	49
12	Vyhlídky do budoucna	51
	Závěr	52
	Seznam použitých zkratk.....	53
	Seznam obrázků	55
	Seznam literatury	56
	Příloha	I - XI

Abstrakt

Tato práce se věnuje problematice elektronického podpisu. Zabývá se analýzou faktorů, které umožnily jeho vznik, rozebírá princip elektronického podepisování a přibližuje technickou i legislativní stránku věci se zaměřením na novelu zákona o elektronickém podpisu. Práce přináší náhled na postup při získávání všech náležitostí k elektronickému podpisu a na možnosti praktického využití. V závěru je naznačen uživatelský pohled na elektronický podpis při práci s elektronickou poštou.

Elektronický podpis je téměř plnohodnotnou, zákonem uznávanou alternativou k fyzickému podpisu, určenou pro využití v elektronickém prostředí. Princip využívá asymetrických šifer a hashovacích algoritmů. V současnosti se ve většině států s uzákoněným elektronickým podpisem využívá podpisu ve spojení se standardem X.509, který definuje formát certifikátů, organizaci a jednání certifikačních autorit. Certifikační autorita zajišťuje důvěryhodné spojení osoby a veřejného klíče k využití pro elektronický podpis.

Novela zavádí nově pojmy elektronická značka a časové razítko. První slouží k automatickému označování dokumentů a druhý zajišťuje jednoznačné spojení času a dokumentu. Novela upravuje i uznávání zahraničních certifikátů.

Získávání certifikátu pro elektronický podpis je modelově snadná cesta avšak podle mých zkušeností s určitými odlišnostmi v praxi. V textu je zhodnocena ekonomická stránka elektronického podpisu. Práce dává možnost seznámit se s nedávným průzkumem o povědomí obyvatelstva o elektronickém podpisu. Závěrečné zhodnocení i výhled do budoucnosti doplňují ucelený přehled o tématu. Příloha zachycuje tvorbu žádosti o kvalifikovaný certifikát při použití čipové karty jako úložiště klíčů.

Abstract

My thesis is focused on e-signing. It contains the analysis of factors that enabled development of the e-signing and discusses principles of the e-signing. The thesis outlines technical and legislative background with focus on the novel of the e-signing law in Czech Republic. It brings insight into the process of acquiring all necessities for using the e-signing and into the possibilities of its consequential usage. In the end of thesis the user's view of the e-signing in the e-mail communication is foreshadowed.

The e-signature is legally acknowledged substitute for "normal" signature meant for usage in the electronic environment. The e-signature is based on the asymmetric cryptography and hash functions. In the present times majority of states, in which the e-signing is legalized, uses the e-signature based on the X.509 norm. The X.509 determines hierarchical structure of the certification authorities. The certification authority, known as the trusted third party, provides reliable bond between the signing person and its public key.

The novel of the e-signing law brings new terms. These are the time stamp and the electronic mark. The former is used for the explicit assignment of time to the document. The latter is meant for the automatic signature-like marking of documents without direct presence of the human factor. The novel also alters approving of the foreign certificates.

Acquiring the certificate is basically a simple task in the theory, but according to my experience, the reality is little different. My thesis also evaluates the economic part of the e-signature usage. The reader may as well get acquainted with the recent survey of the awareness of the e-signature in Czech Republic. Final evaluation and the indication of estimated future should conclude the overview. The appendix serves as a guide to the process of requesting a qualified certificate.

Úvod

Elektronický podpis je fenoménem, který se v posledních letech dostává stále více do povědomí obyvatelstva a stoupá i zájem odborníků. Vzali jej na vědomí i zákonodárci a v těchto dnech jsme svědky dokončení legislativního procesu u novely zákona o elektronickém podpisu. Úkolem této práce bude vysvětlit pojem elektronický podpis, analyzovat principy elektronického podepisování, technické i zákonné normy, které se k němu vztahují a zhodnotit jeho využitelnost v současné praxi. V práci přiblížím i postup získávání kvalifikovaného certifikátu v modelovém podání konfrontovaném s realitou.

Téma jsem si zvolil pro jeho široké uplatnění v mnoha oborech lidské činnosti. Spojení informatiky, kryptografie a práva, které má za cíl usnadnit společnosti život, je jistě téma hodné bližšího zájmu. Můj přínos spatřuji v přidání praktických zkušeností s elektronickým podpisem a možnosti nezaujatě zhodnotit současný stav.

Práci jsem se snažil zpracovat stylem, který by umožňoval komunikativně s elementárními znalostmi z IT pochopit principy, na kterých elektronický podpis stojí a utvořit si vlastní názor na současný stav i vývojové tendence.

1 Geneze elektronického podpisu

Podpis. Již několik století je institut podpisu používán a ve všech právních systémech akceptován, jako potvrzení souhlasu s dokumentem. Tím, že se pod dokument podepíšeme nepopíratelně 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. Avšak pokrok přináší změny. Jak se tedy dostaneme od klasického podpisu na papíře k jeho digitální reprezentaci v podobě několika kilobajtů připojených ke zprávě? Za vznik elektronického podpisu může několik skutečností, o kterých pojednáme dále.

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. Dnes si již těžko dokáže každý druhý Evropan představit svůj den bez zkontrolování e-mailové schránky. Elektronická pošta objemem předstihuje poštu papírovou, jelikož je rychlejší, snadnější a i levnější.

Rozvoj elektronické komunikace nepřinesl jen možnost elektronické pošty. Možnost, téměř ihned vyměňovat na dálku větší množství informací, otevřela nové příležitosti. Je v lidské přirozenosti se pokusit za všech okolností vydělat, stejně tak je lidská lenost a touha po minimální námaze při maximální efektivitě. Tyto faktory jen podpořily vznik elektronického obchodu. Elektronický obchod rozeznává několik typů vztahů. Nejvýznamnější z nich B2B (business to business) a B2C (business to consumer) si přiblížíme více.

B2B je vztah mezi dvěma subjekty, při kterém nakupující nakupuje, nejčastěji zboží, za účelem dalšího podnikatelského využití. Tento typ obchodu zdaleka převyšuje svým objemem vztah druhý. Vznikají velká internetová tržiště, kde podniky mohou koupit rozsáhlý sortiment statků, kancelářskými sponkami počínaje, parními turbínami konče. Použití internetového obchodování je výhodné pro obě strany. Z toho důvodu můžeme očekávat jeho další rozvoj.

B2C je označením pro vztah, při kterém nakupující subjekt zamýšlí nakupované zboží či službu využít ke spotřebě. Je využíván firmami z důvodů rozšíření odbytiště za hranice sídelního státu, nižších nákladů na skladování, nájmy apod. Orientuje se na běžného občana, kterému jsou prezentovány výhody pohodlného a rychlého nákupu z domova, za menší ceny a za jinak téměř nezměněných podmínek.

Co by to bylo za obchod, kdyby se za něj neplatilo? Jelikož barter již není hlavním způsobem obchodu, je třeba nakoupené statky zaplatit. A jak jinak, než elektronicky? Na rozvoj elektronického obchodu bryskně zareagoval bankovní sektor a přinesl svým klientům možnost spravovat své finance na dálku, pomocí telefonu nebo internetu. Umožnil jim i zadávat příkazy k platbám i jiným bankovním operacím po 24 hodin denně a účinně tak podpořil další růst elektronického obchodu.

Není možné uzavírat obchody s někým, koho neznáte, nemáte o něm dostatečné informace, natož takovému subjektu platit. Proto je nutné nejprve subjekt identifikovat a následně ověřit, zda-li je tím, za koho se vydává. To potřebují všichni v internetovém prostředí. Banka si musí být jistá, že příkazy vydává opravdu její klient. Klient si musí být jistý, že komunikuje se svojí bankou a nikoliv s hackerem, který se za ni pouze vydává, aby získal přístupová hesla. To samé platí u obou stran při uzavírání obchodů.

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. 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. Aby byla elektronická komunikace důvěryhodná a bezpečná, bylo třeba najít mechanismy, kterými to zaručit. Proto existuje kryptografie, obor matematiky, podporovaný hlavně vojenskou a vládní sférou, který se zabývá šifrováním a tyto mechanismy zkoumá.

Možnost realizace elektronického podpisu přinesl až objev asymetrické kryptografie. Ten přišel v roce 1976 a začala tak nová éra kryptografie. Autory byli Whitfield Diffie, Martin Hellman a Ralph Merkle. V dřívějších dobách bylo nutné, aby dva subjekty, které si chtěly vyměňovat tajnou informaci, sdílely jedno tajemství – šifrovací klíč. Ten sloužil pro šifrování i dešifrování zprávy. Asymetrická kryptografie učinila průlom. Používá totiž klíče dva – jeden pro šifrování a druhý pro dešifrování. Veřejný klíč je určen pro šifrování, může být volně dostupný (a je dobré pokud je) a umožní tak komukoliv odeslat šifrovanou zprávu. Soukromý klíč, ten si každý drží v tajnosti, je určen k dešifrování a je schopen dešifrovat ty zprávy, které byly zašifrovány příslušným veřejným klíčem. Inverzní využití dvojice klíčů slouží pro elektronický podpis. Více si ukážeme ve 3. kapitole práce.

2 Vysvětlení pojmů

Všechny dříve zmíněné faktory přispěly ke vzniku elektronického podpisu. O tom, k čemu takový elektronický podpis je, jakou má formu a jaké je v současnosti jeho možné využití, si povíme dále. Nejprve se zaměříme na vysvětlení pojmů, které se budou v práci dále objevovat.

2.1 Elektronický podpis

Musíme začít tím, že si vysvětlíme, co to vlastně elektronický podpis je. Litera zákona nám říká toto:

„Pro účely tohoto zákona se rozumí elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.“ [1]

Je tedy důležité upozornit čtenáře na běžnou chybu, a to, že elektronický podpis nepředstavuje vlastnoruční podpis převedený do elektronické podoby. Elektronický podpis je představován speciálně vygenerovanými daty, která jsou pro každý dokument unikátní a k datové zprávě se připojí.

„Datovou zprávou zákon rozumí elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou.“[2]

Jak probíhá proces elektronického podepisování si popíšeme ve 4. kapitole práce.

V naší legislativě platný **zaručený elektronický podpis** musí splňovat následující kritéria:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.[2]

Podmínkou, aby byl podpis chápán jako zaručený, je schopnost podepisující osoby udržet prostředky pro vytváření elektronického podpisu pod svou výhradní kontrolou. Těmito prostředky rozumíme technické či programové vybavení, které slouží k vytváření elektronického podpisu. O prostředcích pro vytváření elektronického podpisu si povíme více v sedmé kapitole práce.

Elektronický podpis by měl plnit určité funkce. Tyto funkce rozeznáváme čtyři. Jsou jimi:

- Identifikace
- Autentizace
- Integrita
- Nepopiratelnost

2.1.1 Identifikace (Identification)

Identifikaci rozumíme rozpoznání osoby, která učinila právní úkon. Při použití elektronického podpisu musí být druhé straně jasné, kdo dokument podepsal. To znamená, že musí být patrné jméno a příjmení podepisující osoby, nebo jasně označený pseudonym, pokud je certifikát vydán na pseudonym.

2.1.2 Autentizace (Authentication)

Autentizace představuje ověření, že osoba uvedená v certifikátu elektronického podpisu je skutečně osobou, která dokument podepsala. Jinými slovy, ověření proklamované identity. To zaručuje certifikační autorita.

2.1.3 Integrita (Integrity)

Po obdržení dokumentu, který byl elektronicky podepsán musí být zřejmé, zda-li se jeho obsah nezměnil od doby jeho podepsání. Mechanismus elektronického podpisu toto ověření umožňuje.

2.1.4 Nepopiratelnost (Non-repudiation)

Stejně jako u vlastnoručního podpisu je nemožné popřít souhlas s podepsaným dokumentem. Zákon uvádí toto:

„Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.“ [3]

Poslední podmínkou pro uznání elektronického podpisu našimi úřady, kromě dříve zmíněných, je založení zaručeného elektronického podpisu na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb.

2.2 Certifikát

Certifikát je datová zpráva, kterou vydává poskytovatel certifikačních služeb (CA), spojující data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit identitu podepisující osoby.

Certifikát je uznáván jako kvalifikovaný pokud jej vydal kvalifikovaný poskytovatel certifikačních služeb a splňuje následující podmínky.

- Je označen jako kvalifikovaný.
- Uvádí v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen nebo v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen. Čili jednoznačně identifikuje CA.
- Uvádí jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym. Dále uvádí zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu. To společně se sériovým číslem umožňuje jednoznačnou identifikaci podepisující osoby.
- Obsahuje číslo kvalifikovaného certifikátu, unikátní u daného poskytovatele certifikačních služeb.
- Má uveden počátek a konec platnosti kvalifikovaného certifikátu.
- Obsahuje data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby. Jinými slovy, jeho součástí je veřejný klíč podepisující osoby.
- Zmiňuje případná omezení pro nakládání s certifikátem.

Parafráze [4]

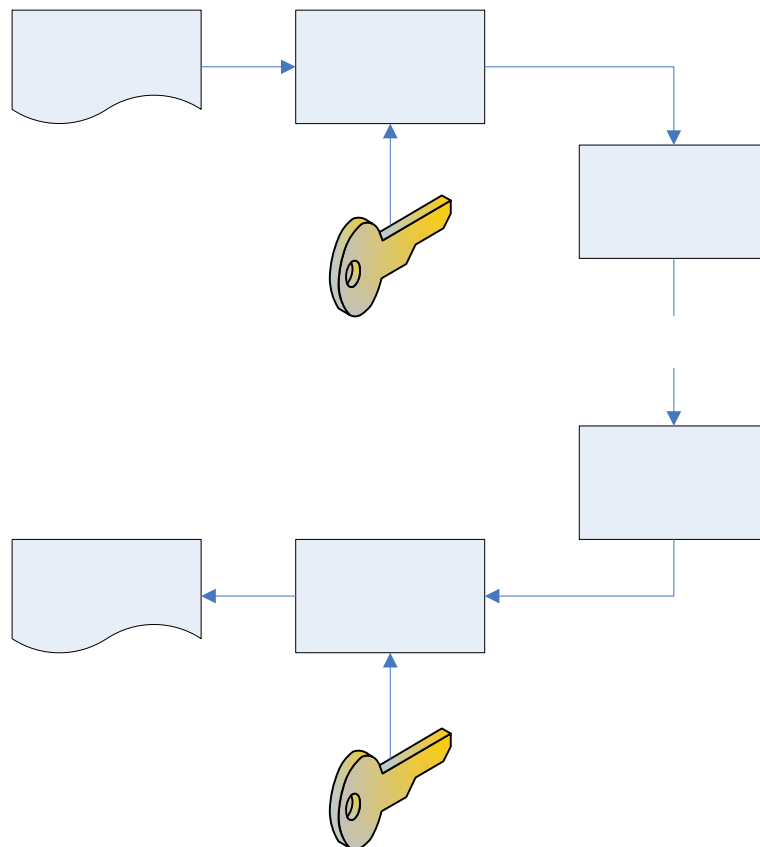
2.3 Poskytovatel certifikačních služeb

Instituce, často označovaná jako certifikační autorita (CA), která se zabývá vydáváním certifikátů k elektronickým podpisům a někdy i vydáváním prostředků pro vytváření elektronických podpisů. Plní funkci důvěryhodné třetí strany (trusted third party). Jejím hlavním cílem je zaručit spojení mezi veřejným klíčem a podepisující osobou, což následně zaručí pravost elektronického podpisu. Jako ověření tohoto spojení vydává certifikáty. Pokud CA splní požadavky dané zákonem a zažádá Ministerstvo informatiky o udělení akreditace, stává se po jejím udělení akreditovaným poskytovatelem certifikačních služeb. O důvěře a roli CA se dozvíme více v 5. části práce.

3 Asymetrické kryptování a elektronický podpis

Předem bych rád upozornil, že pokud není uvedeno jinak, je výklad v práci koncipován na využití kryptosystému RSA, který je u nás nejčastěji užíván. Podepisování dle algoritmu DSA pracuje odlišně. Bližší informace o jednotlivých kryptosystémech jsou uvedeny v další podkapitole.

Jak již jsme si řekli v úvodu, asymetrické kryptování se od symetrického liší používáním dvojice klíčů. To mu nejen umožňuje výměnu klíčů v nezabezpečeném prostředí, ale i využít ho pro objekt našeho zájmu – elektronický podpis. Pokud si dříve chtěli lidé vyměňovat šifrované zprávy, museli se buď sejít, nebo jiným způsobem si doručit společný klíč pro symetrickou šifru. Při použití asymetrického kryptování žádná schůzka není nutná. Každý má svůj veřejný klíč, který může druhé straně poslat kupříkladu elektronickou poštou bez obav, z jeho zneužití. Proč? Protože z jednoho klíče není možné v „rozumném“ čase odvodit klíč druhý a zprávu zašifrovanou veřejným klíčem je schopen dešifrovat pouze majitel správného soukromého klíče. Takže strany si vymění veřejné klíče a může začít šifrovaná komunikace. Viz Obr. 1



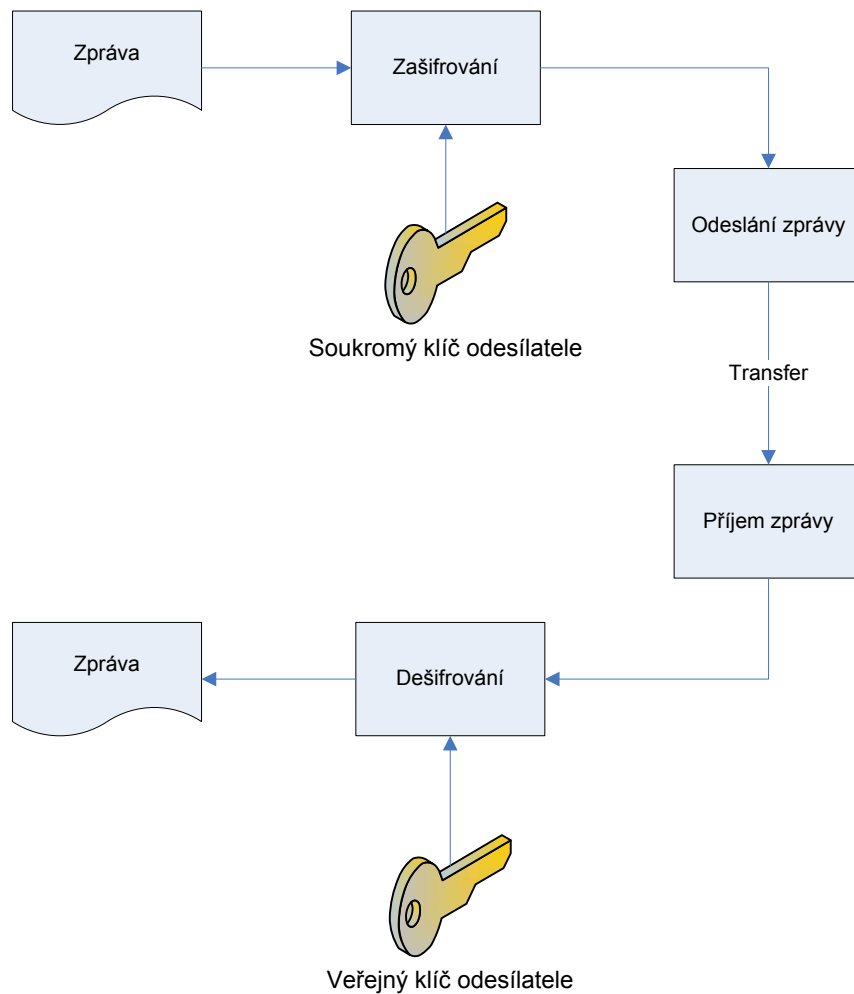
Obr. 1 - Asymetrické šifrování

Zpráva

Jenže to není způsob, který by byl využíván pro elektronický podpis. Ten totiž pracuje na opačném principu. Co je naším cílem při obdržení elektronicky podepsaného dokumentu? Zjistit, zda-li jej podepsal skutečně člověk, uvedený jako odesílatel. I k tomuto můžeme využít asymetrické

Zašifrova

kryptování. Jak? Obrátíme postup. Pokud někdo zašifruje dokument svým soukromým klíčem, jsou jej schopni dešifrovat naprosto všichni. To je naprosto nepřijatelné pro šifrovanou komunikaci, ale nám plně vyhovující. Položme si nyní otázku, kdo mohl zašifrovat zprávu, kterou jsme obdrželi a dešifrovali pomocí veřejného klíče? Nikdo jiný, než majitel soukromého klíče. A pokud je držen soukromý klíč v tajnosti, je to jediná osoba. Tím jsme se dostali k principu elektronického podpisu. Názorně viz Obr. 2

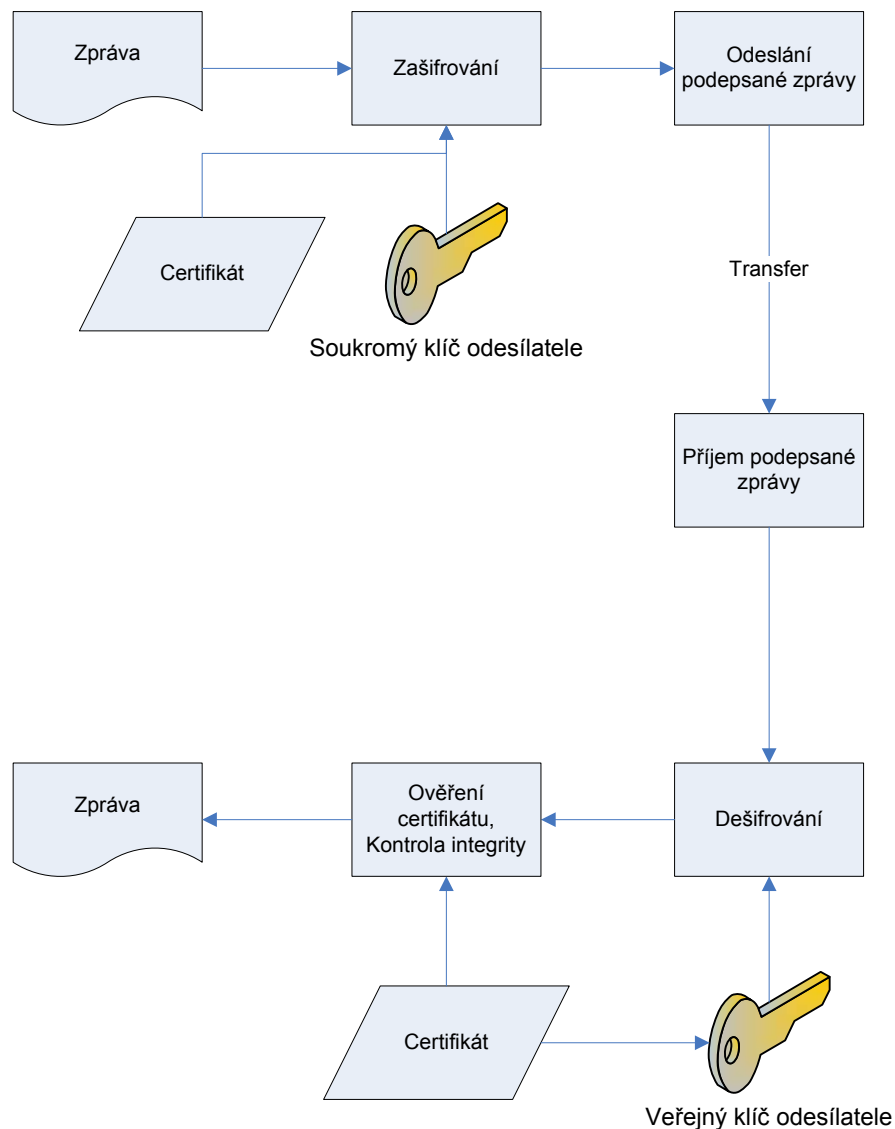


Obr. 2 - Využití asymetrického šifrování pro elektronický podpis

Princip sice ještě není kompletní, ale základy již máme. Chybí nám jistota, že klíč vlastní opravdu ten jedinec, který je uveden jako odesílatel a ne jen někdo, kdo se za něj vydává.

Pro zajištění této jistoty se využívají dva přístupy. Oba si uvedeme a rozebereme, ale jelikož se práce zabývá elektronickým podpisem v ČR budeme nyní postupovat v souladu se zákonem. Využijeme služeb důvěryhodné třetí strany, neboli certifikační autority. Ta za nás ověří identitu podepisující osoby, zkontroluje její veřejný klíč a proces zakončí vydáním certifikátu, který stvrzuje vazbu mezi osobou a klíčem. Po obdržení podepsané zprávy, ověříme platnost certifikátu a můžeme si

být jisti, že nám píše skutečně osoba v certifikátu uvedená. Již daleko kompletnější schéma si můžete prohlédnout na Obr. 3. Certifikát není vstupem pro šifrovací proces. Nejčastěji je pouze přílohou.



Obr. 3 - Elektronický podpis s využitím certifikátu od CA

Základní princip již známe a proto je čas, abychom si pověděli o využívaných šifrovacích algoritmech.

3.1 Kryptosystém RSA

Jako první uvedeme RSA, pojmenované podle počátečních písmen příjmení svých autorů. Těmi byli Ronald Rivest, Adi Shamir a Leonard Adelman, kteří princip RSA vynalezli již v roce 1977. Není možné říci, že to byli právě oni, kteří RSA algoritmus vytvořili, protože kryptografie a její úspěchy podléhají přísnému utajení, ale historie je jako autory rozeznává. Popisovat matematický

základ tohoto algoritmu je mimo rámec této práce. Nám bude stačit si říci, že princip pracuje s velkými prvočísly, jejich součiny a jejich obtížnou faktorizací.

Délka klíče se pohybuje od 512 bitů pro běžné komerční využití, přes 1024 bitů pro zaručený elektronický podpis, až po daleko větší klíče používané při práci s tajnými materiály. Snad by bylo dobré říci, že RSA s délkou klíče 512 bitů bylo prolomeno v srpnu roku 1999 a tedy není již kompletně bezpečné. Rozlomit klíč s 1024 bitovou délkou je však 7-milionkrát výpočetně náročnější. Proto se neočekává prolomení klíče po dobu nejméně 15 let. Více o RSA se dočtete v publikaci [5].

3.2 Kryptosystém DSA

Druhým algoritmem, který je využíván v oblasti elektronického podpisu je DSA (Digital Signature Algorithm) specifikovaný v DSS (Digital Signature Standard). Byl vyvinut organizacemi NIST a NSA jako alternativa k RSA, který byl tou dobou chráněn patentem. Je využíván jako standard pro elektronický podpis například v USA. Bezpečnost algoritmu DSA spočívá v obtížnosti výpočtu diskrétního logaritmu v multiplikativní grupě prvočíselného tělesa F_p . Doporučená délka klíče u DSA je rovněž 1024 bitů. DSA nelze využít pro šifrování. Více o DSA je k nalezení v publikaci [6].

3.3 Hashovací funkce

Nevýhodou asymetrického kryptování je jeho malá rychlost. Jeho použití je značně pomalejší, než u symetrických šifer. Při podepisování větších datových zpráv by tak uživatel strávil mnoho času čekáním na dokončení šifrování. Proto se u elektronického podpisu používá ještě jeden mezikrok. Tím je využití hashovací funkce (hash function).

Hashovací funkce je speciální jednocestná matematická operace. Jako vstup slouží libovolný dokument, soubor, text, i jiná data. Jejím výstupem je soubor dat o přesně dané velikosti, tzv. hash (můžeme se setkat i s výrazem počeštěným – haš nebo otisk), který jasně odpovídá hashovanému dokumentu. Na hashovací funkci jsou kladeny následující požadavky.

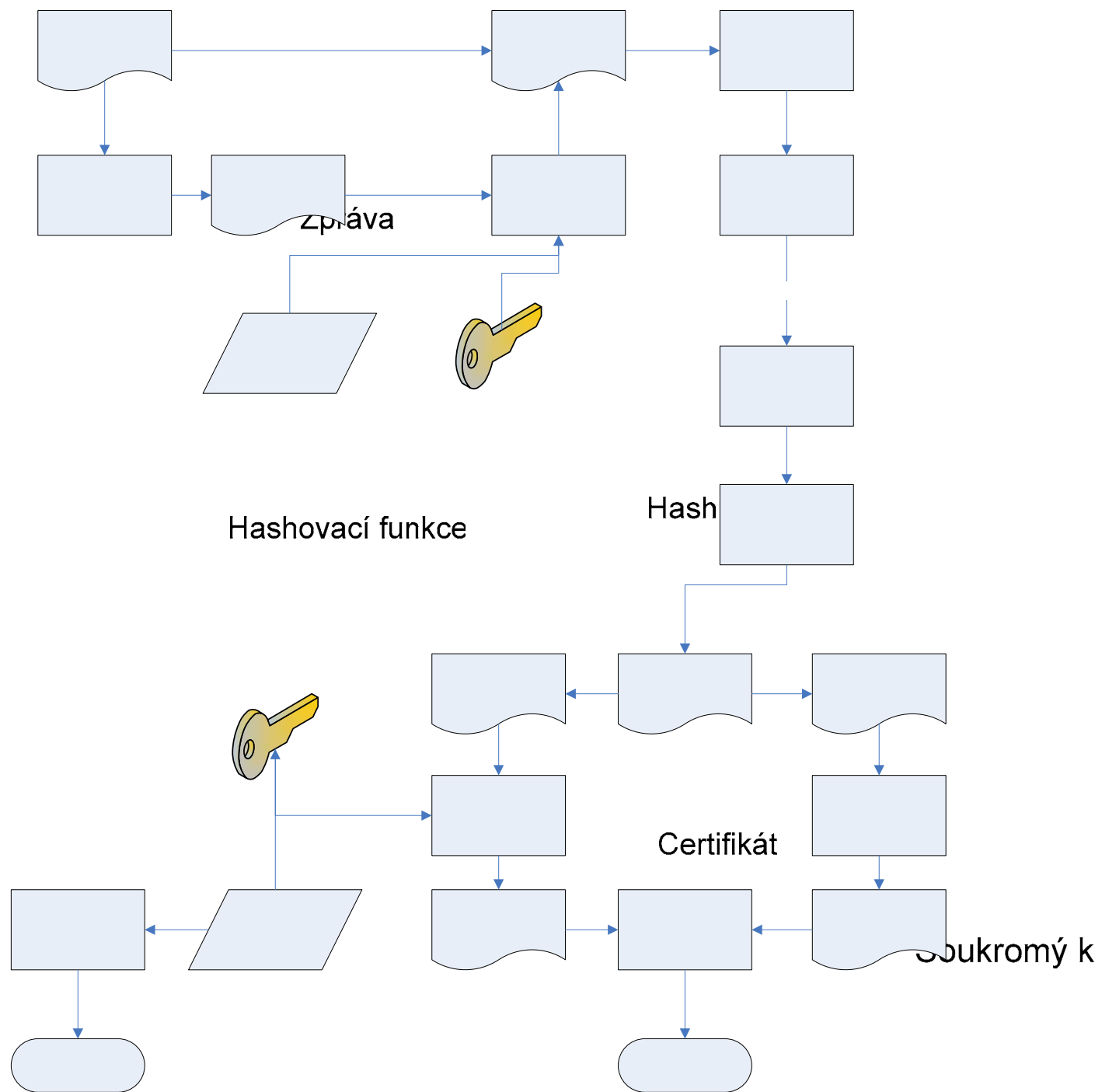
- Výstup má jednoznačně danou pevnou délku.
- Pro rozdílné vstupy nesmí být stejný výstup.
- Při znalosti výstupu nesmí být možné zpětně dopočítat vstup.

Pro potřeby elektronického podpisu se využívá v současnosti dvou funkcí. Jsou jimi MD5 (Message Digest) a SHA-1 (Secure Hash Algorithm). Funkce MD5 má výstup o délce 128 bitů. U funkce SHA-1 je výstup dlouhý 160 bitů. V tuzemských certifikátech se setkáme s oběma.

4 Podepisování a ověřování

Nyní můžeme dokončit postup podepisování i ověřování podpisu v praxi. Nejprve máme datovou zprávu, kterou chceme podepsat. Tu, protože její podepisování by trvalo dlouho, necháme projít hashovací funkcí a získáme tak její krátký otisk. Otisk podepíšeme (zašifrujeme soukromým klíčem) a připojíme k datové zprávě. Datovou zprávu s podepsaným hashem odešleme příjemci.

Příjemce obdrží zprávu, z certifikátu pozná, kdo mu zprávu posílá a použije příslušný veřejný klíč. Měl by ještě zkontrolovat, zda-li je certifikát odesílatele platný u CA, ale tomu se budeme věnovat později. Tím, že hash rozšifruje veřejným klíčem, který je uveden v certifikátu, ověří, že mu zprávu odeslal opravdu držitel certifikátu. Následně spočítá z datové zprávy svůj hash. (Na obrázku je označen jako hash 2.) Porovná svůj hash s dešifrovaným hashem od odesílatele. Pokud jsou si hashe rovny, nebyl změněn obsah datové zprávy od doby jejího podepsání. Tím si ověřil integritu obsahu. Pokud by si chtěly dva subjekty vyměňovat podepsané a ještě i šifrované zprávy, použijí i symetrickou šifru pro zašifrování obsahu. Podepsaná zpráva není totiž šifrovaná a může si ji tedy kdokoliv přečíst! Schéma výše uvedeného postupu najdete na obrázku: Obr. 4



Obr. 4 - Kompletní schéma elektronického podpisu

5 Důvěra

Řekli jsme si, že důvěra je klíčovým prvkem při elektronické komunikaci. Jelikož není v našich silách rychle a snadno ověřit identitu druhé strany, musíme se spolehnout, že to udělá za nás subjekt, který k tomu má prostředky. Existuje několik způsobů, jak tohoto docílit. My si povíme o dvou.

Prvním z nich je systém PGP, který se pro elektronický podpis používá na úrovni komunikace mezi jedinci pomocí elektronické pošty. Není akceptován úřady, protože postrádá centrální autoritu, kterou by bylo možné dozorovat.

Druhým je systém certifikátů podle normy X.509, který se opírá o hierarchickou strukturu certifikačních autorit. Tento systém se používá i v České republice pro certifikaci elektronického podpisu.

5.1 Systém PGP

PGP, z anglického Pretty Good Privacy, byl vyvinut primárně pro ověřitelnou e-mailovou komunikaci s bezpečným obsahem. PGP poprvé prezentoval Philip Zimmermann v roce 1991. PGP používá asymetrickou kryptografii pro podepisování a ověřování odesílaných zpráv. Podpis je nezávislý na zprávě, aby umožnil podepsání ostatními uživateli. Pro zachování bezpečnosti zprávy, může být šifrována za pomoci symetrického klíče, který je náhodně generován pro každou odesílanou zprávu. Následně je zpráva i klíč zašifrována veřejným klíčem příjemce. Elektronické podepisování je totožné se schématem, které jsme si popsali dříve. Jako hashovací funkce používá PGP (v současném standardu OpenPGP) MD5, MD2 (dřívější verze), SHA-1 a RIPEMD-160. Pro transport speciálních znaků využívá PGP Radix-64 konverzi. Ta umožňuje převod zprávy v libovolném kódování, např. UTF-8, do ASCII a její přenos i přes starší typy kanálů. Příjemce po doručení odstraní konverzi a získá zprávu v originálním znění.

Specifikem systému PGP je nepřítomnost centrální certifikační autority. V decentralizovaném modelu PGP každý uživatel vystupuje jako certifikační autorita. Svým podpisem pod certifikát někoho jiného mu vyjadřuje důvěru a činí jej tak důvěryhodnějším pro ostatní. Toto je reálné, pokud se alespoň někteří z uživatelů osobně znají. V případě velkých vzdáleností mezi uživateli důvěryhodnost značně klesá.

Certifikát PGP má typicky následující strukturu.

Verze PGP	Označuje použitou verzi PGP.
Informace o držiteli klíče	Identifikační údaje – jméno, e-mail...
Certifikovaný klíč	Veřejný klíč držitele certifikátu.
Podpis držitele klíče	Ten je vytvořen soukromým klíčem držitele, který odpovídá certifikovanému klíči, tzv. self-signature.
Preferované šifrovací algoritmy	Seznam šifrovacích algoritmů, které preferuje držitel.

Doba platnosti	Časový údaj vytvoření klíče, doba jeho platnosti.
Podpisy	Podpisy ostatních uživatelů, kteří držiteli věří. Mohou být přidávány i dodatečně po vytvoření certifikátu.

V březnu roku 2001 se objevila zpráva, že bylo PGP prolomeno. Ukázalo se, že nešlo o prolomení šifrovacího algoritmu, ale o objevení bezpečnostní chyby při ukládání klíčů. Ta umožňovala úpravu souborů, které PGP program používá a následnou extrakci soukromého klíče s možností jeho zneužití pro falzifikaci podpisu.

Další informace o PGP lze nalézt v [7],[8].

5.2 Standard X.509

Standard ITU-T X.509 je mezinárodně platné doporučení, které popisuje formu využití PKI (Public Key Infrastructure). PKI je soubor hardware, software, lidí a metod a politik, který slouží k jednoznačnému přiřazení veřejného klíče konkrétní entitě při využití elektronického podpisu. V současnosti se používá její třetí verze. [9] Na rozdíl od PGP je systém X.509 centralizován. Používá tzv. stromu důvěry. Na jeho vrcholu je hlavní certifikační autorita. Tu nazýváme kořenová certifikační autorita (Root CA) a ta je chápána jako důvěryhodná. Stará se o to zákon, u nás pak Ministerstvo informatiky (dříve Úřad pro ochranu osobních údajů). Kořenová certifikační autorita musí splňovat nejpřísnější podmínky. Funkcí kořenové CA je hlavně plnit funkci CA pro jiné poskytovatele certifikačních služeb. Tím, že kořenová CA certifikuje jinou certifikační autoritu, umožní té nižší, aby požívala důvěru téměř stejnou, jako kořenová CA. Ty mohou pak certifikovat další. Tím se vytvoří strom, ve kterém se může uživatel dopracovat až k autoritě, kterou považuje za důvěryhodnou. Cesta od koncového certifikátu až k důvěryhodnému místu je nazývána certifikační cestou (certification path). Čím je cesta kratší, tím lépe systém v praxi pracuje.

Každá certifikační autorita vydává svou certifikační politiku. To je dokument, ve kterém CA specifikuje postup ověřování identity žadatele o certifikát, jaké nároky na něj klade a za jakých podmínek vydává certifikáty a jakým způsobem se stará o bezpečnost. Doporučenou strukturu tohoto dokumentu lze najít v [8]. Dále by CA měla mít vypracovanou bezpečnostní politiku, plán pro zvládnutí krizových situací a plán obnovy. Tyto dokumenty značně ovlivňuje místní legislativa.

Součástí standardu je i požadavek na pravidelné zpracovávání a uveřejňování CRL. Jeho vedení je rovněž jednou z funkcí CA. Nemusí ji však vykonávat sama, ale může ji delegovat na jinou instituci.

Certifikát podle X.509 má následující strukturu.

Držitel certifikátu	Identifikační údaje o osobě, které je certifikát vydáván. Ta je vlastníkem certifikovaného veřejného klíče .
Doba platnosti	Na sekundu určená platnost Od – Do, mimo tento interval je certifikát neplatný.
Název vystavitele	Identifikace CA, která vytvořila a podepsala certifikát.
Verze	Číslo, které charakterizuje použitou verzi. 0 pro v1, 1 pro v2 a 2 pro v3.
Sériové číslo	Unikátní číslo certifikátu přidělené certifikační autoritou.
Identifikace algoritmu	Určení, jaký algoritmus a s jakými parametry byl použit pro vytváření podpisu certifikátu.
Veřejný klíč	Veřejný klíč držitele certifikátu, určení pro jaké algoritmy je možné jej využít.
Další rozšíření	Například umístění CRL, certifikační politiky, prohlášení, aj.

Ukázku části certifikátu vytvořeného podle standardu X.509 můžete najít na Obr. 5. Více o X.509 je možné najít přímo v normě ITU-T, nebo v [10].

Předmět	Jméno/název [CN]= Tomáš Stegura Stát [C]= CZ Obec [L]= Praha 3, Laubova 1689/4 Email [E]= waylander@tiscali.cz Příjmení [E]= Stegura Křestní jméno [G]= Tomáš Jméno [N]= Tomáš Stegura
Platnost od	04.05.2004 07:35:03
Platnost do	04.05.2005 07:35:03
Vystavitel	Jméno/název [CN]= I.CA - Qualified root certificate (kvalifikovaný certifikát poskytovatele) - PSEUDONYM Stát [C]= CZ Obec [L]= Podvinný mlýn 2178/6, 190 00 Praha 9 Útvar ve firmě [OU]= Akreditovaný poskytovatel certifikačních služeb Firma [O]= První certifikační autorita a.s.
Verze	v3
Sériové číslo	98A956
Veřejný klíč	3081 8902 8181 00E9 DFD3 5398 191F DD1A 8883 6635 D8A0 397B 3E41 6B7D 528C 458F 166C 24C2 728B CC37 F813 34AB 6ECD 7E2A 6CD0 29DC 4120 4E21 DC47 2133 BD0E E55D EBBE DA2F BC30 94B7 77A0 9161 FE3D E5C4 CBC2 C8A0 3620 B288 5BAB 0F16 6639 4C2C 3D67 5A52 DC21 6DD3 3145 D135 352B 26D6 6037 6B58 4CAD FEB3 C1B4 6E1A 3B01 F4E3 674F FFF8 97FF 0D02 0301 0001

Obr. 5 - Ukázka části certifikátu dle normy X.509

6 Certificate Revocation List

CRL je zkratka z anglického Certificate Revocation List, což znamená seznam revokovaných certifikátů. (V češtině se používá i výrazu zneplatněných.) Pokud z jakéhokoliv důvodu je nutné certifikát zneplatnit, pošle držitel žádost na CA, která zneplatnění provede umístěním certifikátu na CRL. CRL seznam je následně podepsán CA a uveřejněn. Pokud není smluvně dohodnuto jinak, tak je povinností každého, kdo obdrží dokument podepsaný podpisem s certifikátem dle X.509, ověřit na CRL vystavitele certifikátu, zda-li certifikát nebyl zneplatněn. Každý CRL má své zaměření. To může být ovlivněno subjektem, nebo důvodem zneplatnění. Např. všechny certifikáty vydané pro firmu XY, nebo všechny certifikáty zneplatněné z určitého důvodu. V CRL je tedy možné uvádět důvody zneplatnění certifikátu. Obsahuje sériové číslo certifikátu, přesnou dobu jeho zneplatnění a většinou i jeho důvod. Nejčastěji jimi jsou:

- prozrazení klíče (key compromise),
- porušení bezpečnosti CA (CA compromise),
- vydání nového certifikátu, kvůli změnám údajů v něm uvedených (update),
- pozastavení platnosti certifikátu (certificate hold).

CRL rozeznáváme dvojího typu: kompletní a dílčí. Kompletní CRL obsahuje všechny zneplatněné certifikáty v daném zaměření. Dílčí CRL (Delta CRL) zachycuje změny, které se staly od vydání posledního kompletního CRL. Je tedy možné, za předpokladu dostupnosti posledního kompletního a posledního Delta CRL stejného poskytovatele certifikačních služeb, získat jejich složením aktuální kompletní CRL. Je na volbě CA, zda-li bude používat Delta certifikáty, ale pokud se rozhodne, že ano, musí k nim rovněž uvést cestu.

Ke kvalifikovaným certifikátům I.CA je CRL vydáván každých 12 hodin.

7 Prostředky pro vytváření elektronického podpisu

Již je nám jasné, že pro elektronický podpis potřebujeme dvojici spojených klíčů pro asymetrickou šifru. Kde je ale získáme? Jakým způsobem podpis vytvoříme? O tom by měla být následující část.

Pro generování klíčů jsou používány generátory náhodných čísel, které následně otestují prvočíselnost vygenerovaného čísla. Pravděpodobnost, že je číslo číslem složeným, by měla být nejvýše 2^{-60} . Postup spočívá v generování fyzikálního šumu – chaosu a jeho následnou kryptografickou a statistickou úpravou. Více o této komplikované problematice viz [11].

Tyto informace se vztahují k akreditovanému PCS. Generování dvojice čísel je většinou součástí žádosti o vydání certifikátu. Podle naší legislativy je možné, aby certifikační autorita poskytovala službu generování dvojice klíčů, avšak nesmí generovaná data uchovávat. Proto nejčastěji generování dat pro tvorbu elektronického podpisu probíhá v počítači žadatele o certifikát.

Vygenerovaný veřejný klíč se přiloží k žádosti o certifikát. Soukromý klíč, neboli data pro vytváření elektronického podpisu, si uživatel uloží na disk, nebo jiné médium. Současná doba má pro média jisté limity. Z důvodu bezpečnosti je vhodné, aby soukromý klíč zůstal opravdu soukromým, a tedy byl uložen zašifrován s přístupem zabezpečeným heslem.

Ukládat certifikát na pevný disk je proto krajně nevhodné, nemluvě o ukládání na disk sdílený v lokální síti. Diskety jsou méně vhodné kvůli relativně velké možnosti jejich selhání a následné ztrátě klíče. Ta ale není fatální, jelikož lze vygenerovat novou dvojici klíčů a pokračovat ve využívání podpisu. Jako lepší varianta se nabízí USB token. Malá tyčinka velikosti klíčenky je vybavena flash pamětí, která dokáže udržet data i bez přísunu energie a nehrozí jejich náhlá ztráta jako u disket. Existují i aktivní USB tokeny, které jsou speciálně vytvořeny pouze pro elektronický podpis. Obsahují mikročip, který obstarává kryptografické operace a dovolí použití klíčů pouze po zadání hesla. Tato varianta představuje mnohem bezpečnější způsob uchování klíče.

V poslední řadě je zde i možnost využití čipové karty. Čipová karta je standardní velikosti platební karty a z jedné strany má kontaktní plochy pro komunikační rozhraní čtečky. (Viz Obr. 6.) Dnešní čipové karty jsou rovněž aktivní a umožňují provádění kryptografických operací přímo na kartě. Karta pro svou práci také vyžaduje zadání PINu (Personal Identification Number – osobní identifikační číslo). Klíč proto nemusí opustit kartu a zůstává v ní bezpečně uložen. Drobnou nevýhodou oproti USB je fakt, že čtečkou čipových karet, na rozdíl od USB, současná PC vybavena nejsou. Samotnou operaci podepisování vyvolá používaný program, kupříkladu MS Outlook při práci s poštou.



Obr. 6 - Čipová karta vydávaná I.CA

8 Legislativa v ČR

Tato část má za úkol přiblížit čtenáři legislativní prostředí České republiky na poli elektronického podpisu. Budeme se věnovat zákonu o elektronickém podpisu, doplňující vyhlášce Úřadu pro ochranu osobních údajů, nařízením vlády a zakončíme analýzou novely zákona o elektronickém podpisu.

8.1 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. Ta vydala směrnici Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy. Jejím rozbořem se zde nebudeme zabývat. Bude nám stačit její přiblížení v následujícím odstavci. 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.

Citace z literatury [12].

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.

8.1.1 Rozbor zákona o elektronickém podpisu

Zákon v první části vymezuje pojmy, jako jsou:

- elektronický podpis, jeho zaručená verze,
- datová zpráva,
- podepisující osoba,
- poskytovatel certifikačních služeb, dále akreditovaný PCS (běžně označování jako CA),
- 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.

Všechny výše uvedené pojmy jsme si již vysvětlili, nebo nepotřebují vysvětlení, a proto se k nim nebudeme vracet. Dále zákon definuje za jakých podmínek je datová zpráva podepsána, jaké jsou požadavky na podpis.

Další část je věnována povinnostem podepisující osoby a poskytovatele certifikačních služeb. Povinnosti podepisující osoby jsou následující:

- zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu,
- podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.[13]

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

Povinnosti poskytovatele certifikačních služeb si shrneme následovně.

- 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 certifikátů 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 PCS 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 PCS zaručí za jejich správnost a platnost. To činí uznávání cizích certifikátů velmi komplikovanou záležitostí a letošní novela tuto problematiku řeší, viz dále.

Zákon formuluje požadavky na prostředky bezpečného vytváření a ověřování elektronických podpisů následovně.

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. [14]

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.

8.2 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.

8.2.1 Rozbor 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 (dále jen „Věstník Úřadu“).
 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. [15]

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.

8.3 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.

8.4 Novela zákona o elektronickém podpisu

Novela zákona o elektronickém podpisu přináší několik úplně nových prvků do našeho zákonodárství. Upravuje problematiku elektronických značek, časových razítek, přepracovává uznávání zahraničních certifikátů, řeší správní delikty a přestupky. Novela byla v době psaní tohoto textu po schválení sněmovnou i senátem, čekala pouze na podpis prezidenta. Je tedy vysoká šance, že brzy vstoupí v platnost. Proto se jí budeme věnovat více a upozorníme na změny i nové prvky.

8.4.1 Nové pojmy

Novými pojmy v novele zákona o elektronickém podpisu jsou

- Časové razítko
- Označující osoba
- Elektronická značka
- Systémový certifikát

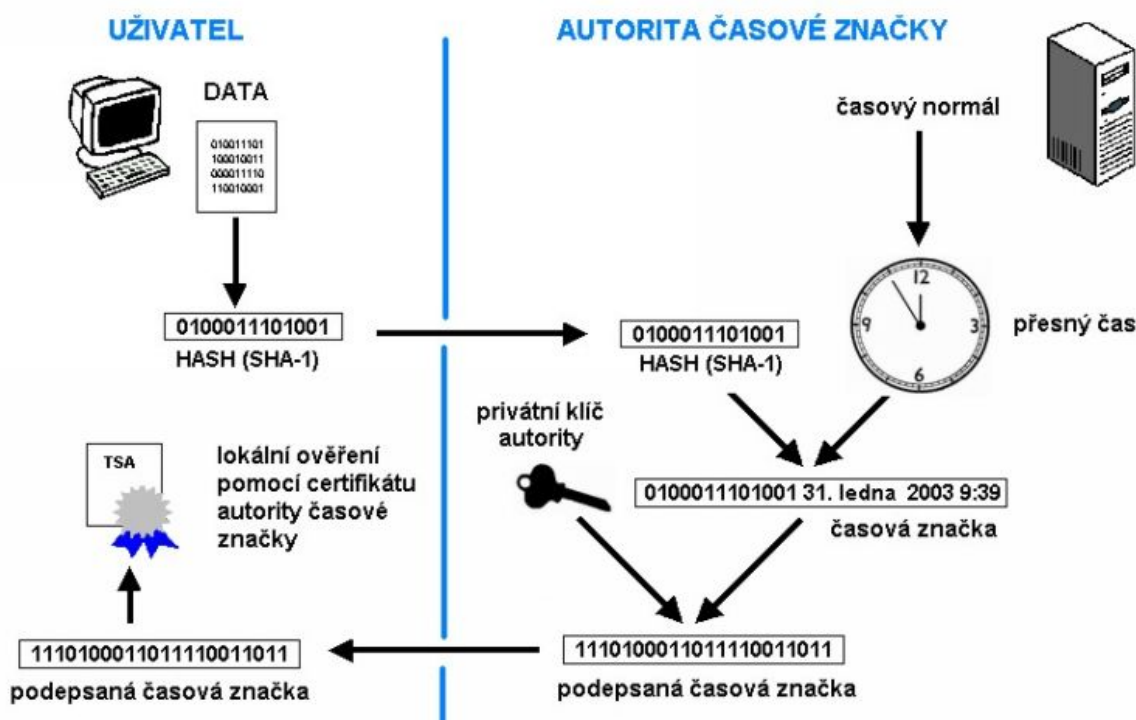
Časové razítko

Proto, aby bylo časové razítko uznáno jako relevantní 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.[16]

Časové razítko se, podobně jako elektronický podpis, spojuje s datovou zprávou a spolehlivě dokazuje dobu existence datové zprávy. To elektronický podpis nedokazuje. Využití časového razítka spočívá v prokázání existence dat před určitým okamžikem. Časové razítko znemožňuje, aby podepisující zneplatnil po podpisu svůj certifikát a tvrdil, že podpis vznikl až po zneplatnění. Další možnost využití najdeme například v dokládání vývoje autorského díla v elektronické podobě při případném sporu o autorství.

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.



Obr. 7 - Časové razítko

Obrázek převzat z www stránek certifikační autority TrustPort (www.trustport.cz)

Schéma na Obr. 7 ilustruje získání časového razítka. Princip využívá elektronického podpisu. Nejprve je vypočítán hash datové zprávy a doplní se dalšími údaji do formy žádosti o vydání časové značky (razítka), která je následně odeslána TSA. Tam je žádost zpracována tak, že k dodanému hashi je přidán přesný časový údaj a celý tento „balíček“ je elektronicky podepsán soukromým klíčem TSA. Tím je zajištěna důvěryhodnost časového údaje. Takto vytvořené časové razítko je doručeno žadateli. Jakékoliv změny v dokumentu pozmění výslednou hodnotu hashe, a tak je zaručeno, že data s časovým razítkem jsou v nezměněné podobě.

Elektronická značka

Do přijetí novely byl elektronický podpis spjat s fyzickou osobou. V certifikátu mohlo být uvedeno, že osoba je zastupitelem určité právnické osoby, ale právnická osoba nemohla získat elektronický podpis jako taková. To nyní již není zcela pravda. Přichází institut elektronické značky, aby umožnil automatické označování dokumentů bez vázání na konkrétního jedince. Nyní je možné automatizovaně označovat dokumenty. Elektronická značka však není plně ekvivalentní elektronickému podpisu.

Zákon rozeznává elektronickou značku jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.[16]

Je tedy patrné, že elektronická značka plní funkce elektronického podpisu. Zákon říká: „Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli.“[15] Neboli, je možné popřít uvědomění si obsahu. Elektronická značka najde uplatnění při zaslání automatických potvrzení přijetí dokumentů a při výpisech z veřejných rejstříků a seznamů. Postup při označování využívá stejných principů jako elektronický podpis.

8.4.2 Rozbor novely zákona o elektronickém podpisu

Novela, jak již bylo řečeno, zavádí několik nových prvků, dále upravuje drobně názvosloví, aby lépe odpovídalo evropským poměrům. Novela ZoEP nově definuje požadavky kladené na označující osobu.

1. Označující osoba je povinna
 - a. zacházet s prostředkem jakož i s daty pro vytváření elektronických značek s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
 - b. uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný systémový certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření elektronických značek.
2. Označující osoba je povinna zajistit, aby prostředek pro vytváření elektronických značek, který používá, splňoval požadavky stanovené tímto zákonem.
3. Za škodu způsobenou porušením povinnosti podle odstavce 1 odpovídá označující osoba, i když škodu nezavinila, podle zvláštních právních předpisů, odpovědnost za vady podle zvláštních předpisů tím není dotčena. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn.[16]

Zvláštním právním předpisem je rozuměn Občanský zákoník v aktuálním znění. (zákon č. 40/1964 Sb.) Povinnost podávat přesné a pravdivé informace ve vztahu k certifikátu je nyní stejná pro označující i podepisující osobu nezávisle na druhu certifikátu. Jde opět o zajištění důvěryhodnosti a spolehlivosti údajů uvedených v certifikátu.

Další nároky, které nový zákon specifikuje se vztahují ke kvalifikovanému časovému razítku. Novela je uvádí takto.

1. Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, je povinen
 - a. zajistit, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené tímto zákonem,
 - b. zajistit, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,
 - c. zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,
 - d. přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek,
 - e. poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.
2. Kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.[16]

Takto nastavené právní „mantinely“ by měly umožnit dostatečnou volnost pro poskytovatele služeb časových razítek a přitom zajistit, aby bylo časové razítko důvěryhodným a spolehlivým nástrojem. Druhý bod je kritický pro samotný smysl využívání časových razítek.

Je nutné, aby novela specifikovala náležitosti časového razítka a proto tak novela činí.

Kvalifikované časové razítko musí obsahovat

- a. číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,
- b. označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,
- c. v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,
- d. hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,
- e. data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno,

- f. elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.[16]

Na dozoru ani na udělování akreditací se nemění nic, jen je přidána ministerstvu povinnost vést evidenci kvalifikovaných systémových certifikátů akreditovaných PCS. Novela definuje, námi dříve již používaný, pojem „**uznávaný podpis**.“ Ten zákon chápe jako zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Pouze takovýto podpis je možné využít pro úřední komunikaci s orgány veřejné správy. Dále novela ustavuje, že elektronické dokumenty, vydané orgánem veřejné moci označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem, mají stejné právní účinky jako veřejné listiny vydané těmito orgány. Jelikož se předpokládá extenzivní využití elektronických značek ve veřejné správě, hlavně v oblasti podatelů, je nutné, aby byly specifikovány požadavky na nástroje pro tvorbu elektronických značek. Novela je určuje takto.

1. Prostředek pro vytváření elektronických značek musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
 - a. data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,
 - b. označující osoba je informována, že zahajuje používání tohoto prostředku.
2. Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí.
3. Prostředek pro vytváření elektronických značek musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.[16]

Formulace je sice obecná, ale to je nezbytné z důvodu technologické nezávislosti, možnosti inovací a jiných způsobů řešení.

Abychom měli analýzu kompletní, uvedeme si podmínky kladené na kvalifikovaný systémový certifikát, který jednoznačně spojuje označující osobu s příslušnou elektronickou značkou.

Kvalifikovaný systémový certifikát musí obsahovat:

- a. označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona,
- b. v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,
- c. jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek,

- d. data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby,
- e. elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává,
- f. číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,
- g. počátek a konec platnosti kvalifikovaného systémového certifikátu,
- h. omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.[16]

Jak jsme si řekli v úvodu této části, novela nově upravuje problematiku uznávání zahraničních certifikátů. Dříve bylo nutné, aby se za zahraniční certifikát, který kompletně naplňoval požadavky kladené našim zákonem, zaručil náš akreditovaný PCS. Novela nyní považuje kvalifikované certifikáty vydané PCS usazeným na území Evropské Unie za ekvivalentní kvalifikovaným certifikátům dle naší legislativy. Certifikáty vydané v jiných zemích se uznávají stejným způsobem, jako před novelou s tím rozdílem, že se zaručit může kterýkoliv PCS vydávající kvalifikované certifikáty na území EU.

Ministerstvo informatiky je v novele zmocněno vydávat nové prováděcí vyhlášky k zákonu o elektronickém podpisu.

Novela upravuje nově i přestupky a správní delikty. Maximální výše pokuty, kterou je možné udělit za porušení pravidel stanovených novým ZoEP činí 10 000 000 Kč. Společná ustanovení upravují odpovědnost právnických osob a klauzule o účinnosti uvádí, že se novela stává účinnou první den třetího měsíce od dne vyhlášení.

Tímto jsme ukončili rozbor novely zákona, která snad přinese pokrok na poli elektronického podepisování. Novela přináší větší možnost automatizace a to by mohlo přispět k dalšímu rozvoji elektronického obchodu. Jen zmíníme, že o konkrétní úpravu pro úřady se starají standardy ISVS vydávané úřadem pro ISVS. Ten je nyní součástí Ministerstva informatiky. Legislativní část tímto ukončíme a budeme se věnovat části praktické.

9 Elektronický podpis v praxi

V následujícím textu vám nastíním postup při získávání kvalifikovaného certifikátu, stav na našem trhu a své osobní zkušenosti s elektronickým podpisem nabyté jeho používáním. Praktickou část zakončíme shrnutím nynějších možností využití elektronického podpisu běžným občanem České republiky.

9.1 Stav na českém trhu

Na našem trhu působí v oblasti elektronického podepisování několik firem. Jsou mezi nimi české podniky i pobočky velikých mezinárodních firem. Protože nás zajímá uznávaný podpis, zaměříme se na akreditované poskytovatele certifikačních služeb.

V tomto segmentu trhu je situace naprosto odlišná. Od 18. března 2002 na něm působí zatím jediný subjekt a tím je I. Certifikační Autorita, a.s. I.CA, jak budeme I. Certifikační Autoritu označovat, je součástí firmy PVT, a.s., která působí v oblasti obecného ICT trhu. V ČR má přes 300 poboček, působících jako tzv. registrační autority (RA), které sbírají data od klientů a vyřizují žádosti o certifikáty. Jejich úkolem je ověřovat na základě předložených dokladů údaje uvedené v žádosti o certifikát. Tyto RA můžeme najít na pobočkách PVT, a.s. nebo na pobočkách ČSOB, a.s. Více informací o I.CA můžeme najít v [17].

I.CA nabízí kvalifikované certifikáty ve dvou verzích, verze STANDARD a verze COMFORT. Tato provedení se liší v úložišti certifikátu. Certifikát ve verzi STANDARD je uložen na PC uživatele, ve verzi COMFORT je uživateli vydána čipová karta, na kterou si uživatel certifikát uloží. Samozřejmostí je i odlišná cena. Ceny se jsou v současnosti 752 Kč na rok platný kvalifikovaný certifikát STANDARD a 1728 Kč nebo 1663 Kč za kvalifikovaný certifikát COMFORT. Nižší cena je při odběru deseti a více certifikátů. Obě ceny zahrnují čipovou kartu.[18]

Do certifikátu vydaného I.CA bývá přidáván i identifikátor Ministerstva práce a sociálních věcí. Tento speciální bezvýznamový identifikátor má v budoucnu nahradit rodné číslo. Pro zabezpečení jednodušší a jednoznačné identifikace osoby je zapotřebí nějakého identifikátoru, nejlépe čísla. K tomuto účelu např. v USA slouží číslo sociálního pojištění. U nás dosud takto slouží rodné číslo. Jelikož v evidenci rodných čísel existuje mnoho duplicít a z rodného čísla lze odvodit datum narození i pohlaví osoby, směřuje vývoj k novému identifikátoru. Identifikátor MPSV je náhodně generované číslo, které nebude mít jiný, než identifikační význam. Identifikátor je desetiferné číslo v rozsahu 1 100 100 100 až 4 294 967 295. Měl by přinést větší bezpečnost osobních údajů a zabránit duplicitám. Je však diskutabilní, zda-li tento cíl naplní. Jeho uvádění ve veřejném certifikátu je při nejmenším podivné, jelikož by měl nahradit rodné číslo, které je před veřejností utajováno.

Certifikáty vydávané I.CA jsou vydávány na základě normy X.509 ve verzi 3. Používané algoritmy jsou MD5 a SHA-1 pro hashování. Na vytváření elektronického podpisu je využíván algoritmus RSA o délce klíče 512 bitů pro komerční certifikáty a 1024 bitů pro kvalifikované

certifikáty. Musím přiznat, že mě poněkud zarazí komerční využívání klíčů o délce 512 bitů. RSA klíč o délce 512 bitů byl úspěšně faktorizován, tedy prolomen a již není bezpečný.

9.2 Model získávání kvalifikovaného certifikátu

Žadatel nejprve zvolí poskytovatele certifikačních služeb, kterému dostatečně věří a je certifikován Ministerstvem informatiky. Na jeho www stránkách se seznámí s certifikační politikou a rozhodne se, zda-li mu politika vyhovuje. Přes www rozhraní zažádá ze svého PCS o vydání kvalifikovaného certifikátu. Při tom vygeneruje dvojici klíčů a veřejný klíč přiloží k žádosti. Po zpracování uloží žádost na disketu a vydá se na RA, aby tam ověřili jeho totožnost. Po ověření totožnosti a sepsání smlouvy je mu na disketu nahrán jeho nový certifikát. Ten si uživatel spolu s certifikátem CA nainstaluje do svého operačního systému a může jej začít využívat.

Chybu tohoto modelu bych viděl v několika bodech.

1. U nás na trhu není žádný další akreditovaný poskytovatel certifikačních služeb. Uživatel si může maximálně vybrat, chce-li mít možnost využívat elektronického podpisu, nebo ne. To se může změnit s novelizací ZoEP, který umožní vstup zahraničních akreditovaných PCS na náš trh. Mohlo by to přinést zlepšení konkurenčního prostředí a zkvalitnění poskytovaných služeb. Rovněž by našemu trhu prospělo snížení cen. Za stávajících cenových podmínek bude masové rozšíření elektronického podepisování silně komplikované.
2. Druhým problematickým místem je disketa. Je to jediné registračními autoritami akceptované médium. Pokud uživatel plánuje elektronicky podepisovat zprávy ze svého nového notebooku, který není vybaven disketovou mechanikou, vyvstanou mu značné problémy. RA není vybavena na přijímání generovaných žádostí na CD, Flash paměťových tokenech ani na jiných médiích. Přijde mi to poněkud omezující a zpátečnické. Jediné štěstí je, že RA nepožadují žádost na disketách velikosti 5¼“.

9.3 Vlastní zkušenosti se získáváním kvalifikovaného certifikátu

Předem bych rád podotknul, že text je založen na mých zkušenostech a reprezentuje tedy subjektivní názor. Zda-li se jedná o objektivní skutečnosti by vyžadovalo důkladnější zkoumání a statistické vyhodnocení.

První věc, které jsem se musel věnovat bylo získávání informací. Webové stránky I.CA, kterou jsem si vybral přesně dle modelu, poskytovaly vcelku přehledný návod, jak o certifikát zažádat. Prvním bodem bylo získání čtečky čipových karet, jelikož jsem čipovou kartu zvolil jako optimální médium pro uložení certifikátu. Po e-mailovém dotazu na helpdesk I.CA mi bylo sděleno, že čtečku mohu zakoupit libovolnou, ale že mi mohou nabídnout osvědčený model USB čtečky od firmy Gemplus za cenu okolo 2100 Kč včetně DPH. Jako nedůvěřivý člověk jsem se podíval na www stránky firmy Gemplus a zjistil, že „osvědčený model“ se již nevyrábí a byl nahrazen novou

výrobovkovou řadou. Dalším dotazem jsem zjistil, že je možné přes mou banku zakoupit nový model čtečky za poloviční koncovou cenu než stál nabízený „osvědčený model.“ Rád bych jen podotknul, že cena nebyla bankou dotována, pouze působili jako zprostředkovatelé. Můj první kontakt s I.CA nedopadl nejlépe.

Věděl jsem, že dále potřebuji získat čipovou kartu. Je nutné přiznat, že jsem přehlédl na stránkách I.CA odkaz, který odkazoval na způsob žádání o kartu. Vzhledem k faktu, že jsem netušil, jak o kartu zažádat, vydal jsem se na pracoviště RA s nadějí, že mi poradí. První místo, které jsem navštívil byla pobočka ČSOB, a.s. na Vinohradské třídě na Praze 3. Tam jsem zjistil, že paní, která se jako jediná zabývá elektronickým podpisem, je na školení, ale řekli mi ať přijdu odpoledne. Pán z ČSOB si na mě vzal kontakt, aby mne mohl informovat v případě změn. Dobře, že to udělal, poněvadž po poledni mi volal, že jeho kolegyně dnes do práce už nepříjde a poprosil mě, abych navštívil jinou pobočku. Vyhověl jsem mu a zavítal do pobočky ČSOB, a.s. poblíž náměstí I.P.Pavlova. Mile mne poprosili ať se posadím a chvíli vyčkám, že se mi hned bude jejich člověk věnovat. Po půl hodině se tak vskutku stalo a já mohl přednést svou prosbu o radu. Pracovník banky si mne pozorně vyslechl a pak mi sdělil, že žádná z poboček ČSOB není vybavena pro práci s čipovými kartami a pokud chci certifikát na čipové kartě, necht' se obrátím na libovolnou pobočku PVT, a.s. Ochotně mi na mapě vyhledal nejbližší pobočku a já se mohl opět vydat na cestu.

Pobočka PVT, a.s. se nacházela na Pankráci na pobočce SCP a RM-Systému. Paní přede mnou, podle konverzace lékařka, si již potřetí šla žádat o certifikát, ale i tentokrát neúspěšně, z důvodu chybně vyplněné žádosti. Když se na mě dostala řada, já přednesl svůj problém bylo mi pracovníci řečeno, že oni s čipovými kartami nic neudělají, ať se obrátím na centrálu PVT, která je poblíž stanice metra B, Českomoravská. Dále mi sdělila, že toho moc nevědí, že jim čas od času podnik zařídí nějaké školení, ale že se podmínky mění natolik rychle, že jsou z toho i samotní pracovníci RA zmateni. Vzhledem k pozdní hodině jsem odložil návštěvu centrály na další den.

Cesta na Českomoravskou proběhla hladce a já dospěl k centrále PVT, a.s. Po několika dotazech a telefonátech z vrátnice jsem se dovolal paní Dvořákové, která s panem Čermákem má na starost elektronický podpis. Ta mi poradila, ať se vrátím domů, prostuduji www stránky a řekla mi o mnou přehlédnutém odkazu. Pln nadšení jsem se vrátil domů k počítači a na stránkách I.CA našel požadovanou informaci. Musel jsem zaslat písemnou objednávku karty na centrálu PVT, a.s.! Velice mne zaráží, že se nedá vyřídit nic osobně. Na centrále jsem byl, ale stejně mi nezbylo nic jiného, než jim psát „obyčejný“ dopis. Rovněž si myslím, že jsem se mohl o své chybě dozvědět daleko dříve. Sepsal jsem tedy žádost a odeslal ji. I.CA uvádí, že požadavek na kartu je vyřízen do 14-ti dnů.

Po třech týdnech dorazil doporučený dopis obsahující kartu. Na kartě se nacházel pouze systémový certifikát I.CA. Nyní zbývalo jen vygenerovat pomocí karty žádost o vydání certifikátu. WWW aplikace, která k tomu má sloužit, mi bez udání důvodu chyby sloužit odmítla a odmítala se mnou další komunikaci. Poslední záchranou mi byl ke kartě dodávaný ovládací program ComfortChip,

kteřý umožňoval žádost vygenerovat. Uložil jsem ji na disketu, přesně jak si model žádá a vydal se na pobočku PVT.

Paní za přepážkou, teď již jiná, se mnou sepsala smlouvu o poskytování certifikačních služeb a nechala dálkově zpracovat mou žádost. Výpočetní středisko se nachází údajně na východní Moravě. Veškerá interakce, která proběhla na pobočce s mou kartou, byla o opsání čísla karty do počítače. Mylně jsem se domníval, že mi na kartu bude nahrán certifikát. Dostal jsem jej na disketu, ať si ho tam nainstaluji sám. To jsem doma učinil. Dále jsem obdržel mail s certifikační politikou a kopií svého certifikátu. Má cesta ze elektronickým podpisem byla zakončena fakturou na 1771 Kč, která přišla zanedlouho poštou.

Nezastírám, že i já jsem chyboval při získávání certifikátu, ale myslím, že bylo možné mou chybu odhalit daleko dříve. Postačila by k tomu větší informovanost zaměstnanců zabývajících se problematikou. Rovněž si myslím, že jediný možný způsob žádání o certifikát věci škodí. Pokud nelze věc vyřídit osobně, je rozhodně někde chyba.

Literatura [19] uvádí, že přes 20 % žadatelů o certifikát uspěje až na druhý či další pokus, což je připisováno na vrub i nedostatečné technické podpoře ze strany I.CA.

Osobně si myslím, že celý problém je způsoben monopolním postavením I.CA, která tak nemá důvod snižovat ceny a zvyšovat kvalitu služeb. Jako porovnání bych rád nastínil podobnou operaci v bankovním sektoru.

Jelikož jsem nyní vybaven čtečkou čipových karet, rozhodl jsem se, že si klíč pro internetové bankovníctví nechám rovněž nahrát na čipovou kartu. Přišel jsem do pobočky a slečně za přepážkou vysvětlil svůj požadavek. Vypadala překvapeně, poprosila mě o chvíli strpení a šla o radu k nadřízenému. Trvalo to opravdu jen chvíli, následně mi předali novou čipovou kartu, zapečetěnou obálkou s přístupovými kódy, na jejich počítači mne nechali vytvořit elektronickou žádost a následně ji ihned potvrdili. Operace zabrala 15 minut a byla zdarma.

Je vidět že konkurenční prostředí nutí firmy ke zkvalitnění služeb. Proto se již nyní těším na schválení novely ZoEP, která by snad monopolní postavení I.CA mohla změnit alespoň o zahraniční CA. Na druhou stranu není možné použít kvalifikovaný certifikát ke komunikaci s bankou. Pro autorizaci e-bankingových operací klient potřebuje certifikát vydaný jeho bankou.

9.4 Možnosti využití elektronického podpisu v ČR

V následujícím textu si ukážeme k čemu může obyčejný občan využít zaručený podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Pokud si myslíte, že opatřením elektronického podpisu se dramaticky změní váš život, jsem nucen vás zklamat. Možnosti využití elektronického podpisu v současné době nejsou zdaleka tak rozsáhlé, jak by se mohlo zdát.

9.4.1 Komunikace s veřejnou správou

Dle nařízení vlády by měly mít všechny důležité úřady zřízenou elektronickou podatelnu, ve tvaru posta@domena_uradu.cz. Podmiňovací způsob je namístě, jelikož úřady podatelnu často nemají v požadovaném tvaru a nesplňují podmínky, které jim standardy ISVS ukládají. Kupříkladu chybí potvrzení o přijetí pošty, nejsou specifikovány typy příloh, které podatelna přijímá, atd. Ministerstvo informatiky se snaží podpořit tvorbu elektronických podatel a elektronické komunikace s úřady tím, že obcím zdarma nabídl kvalifikovaný certifikát pro jednoho jejich pracovníka. Ten by pak mohl spravovat podatelnu. Samo ministerstvo však neočekává velký úspěch akce, jelikož by považovalo 50% odezvu za výtečnou.

Ministerstvo financí

Ministerstvo umožňuje občanovi, který disponuje uznávaným elektronickým podpisem podat přiznání k některým daním elektronickou formou. Jsou jimi:

- přiznání k dani z nemovitostí,
- přiznání k silniční dani,
- přiznání k DPH.

Dále ministerstvo dovoluje podat elektronickou cestou oznámení o nezdaněných vyplacených částkách fyzickým osobám a podat obecnou písemnost. Možnost podat přiznání k dani z příjmu zatím chybí, ale ministerstvo ji v dlouhodobém horizontu plánuje vyřešit. O počtech elektronicky podaných přiznání informuje následující tabulka.

Podání	Rok 2003		Rok 2004	
	Se zar. el. podpisem	Bez zar. el. podpisu	Se zar. el. podpisem	Bez zar. el. podpisu
Přiznání k DPH	3353	1173	1564	547
dani z nemovitostí	460	325	135	296
dani silniční	14	789	852	835
Hlášení o vypl. Částkách	0	71	4	13
Obecné podání	233	–	281	–
Celkem	4060	2958	2836	1691

Tabulka 1 - Počty elektronických podání k 26.2.2004

Zdroj: [20]

Ministerstvo práce a sociálních věcí

Občan vybavený uznávaným elektronickým podpisem, který je doplněn o identifikátor MPSV, může podat elektronicky žádost o příspěvek státu. Je možné elektronicky zažádat o:

- sociální příplatek,
- příspěvek na dopravu,
- příspěvek na bydlení,

- pohřebné,
- porodné,
- příspěvek na dítě,
- dávku péstounské péče,
- rodičovský příspěvek,
- zaopatřovací příspěvek pro nezaopatřené děti vojáka nebo o zaopatřovací příspěvek pro manželku vojáka.

Nevýhodou je nutnost doručit příslušná potvrzení a přílohy na úřad ve fyzické podobě a to poštou, nebo osobně. Tím se celý efekt rapidně snižuje. Ministerstvo připravuje elektronické podávání potvrzení o studiu, potvrzení o zdravotním stavu, potvrzení o době trvání služby a některá další. Rovněž je možné hlásit změny v údajích.

Musím se pozastavit nad koncepcí ministerstva. Jelikož jsou přídavky určené sociálně slabším vrstvám, nedá se předpokládat, že by měli příslušníci těchto vrstev dostatečné prostředky pro zakoupení počítače. Rovněž pochybuji, že by alokovali část takto získaných peněz na placení poplatků za vystavení certifikátu. Občané, kteří si mohou dovolit vlastnictví počítače i certifikátu většinou přídavek od státu nepožívají.

9.4.2 Zdravotní pojišťovny

Instituce velikosti zdravotních pojišťoven si mohou dovolit zřídit elektronickou podatelnu nebo portál pro komunikaci se svými smluvními partnery – zdravotnickými zařízeními a případně klienty – pojištěnci. Této možnosti využilo zatím sedm našich pojišťoven. Využití systému klienty umožnila zatím pouze Hutnická zaměstnanecká pojišťovna.

Všeobecná zdravotní pojišťovna, naše největší, má přístup povolen pouze pro zdravotnická zařízení a zaměstnavatele. Česká národní zdravotní pojišťovna, Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví, Revírní bratrská pokladna, Zaměstnanecká pojišťovna Škoda a Zdravotní pojišťovna Metal-Aliance provozují systém, který je rovněž určen jen zdravotnickým zařízením a zaměstnavatelům. Mezi běžnou funkcionalitu těchto systémů patří možnost elektronického vyúčtování zdravotní péče, které využívají zdravotnická zařízení a hromadné oznámení zaměstnavatele společně s zasláním přehledu o platbě pojistného, které slouží zaměstnavatelům.

9.4.3 Česká pošta

Česká pošta nabízí službu REP (Registrovaná elektronická pošta). Jedná se o elektronickou obdobu doporučeného dopisu s doručenkou. Obě komunikující strany si musí nainstalovat REP klienta

a pomocí této aplikace komunikují přes REP server České pošty. REP server informuje podavatele o stavu zásilky, zasílá potvrzení o podání zásilky, potvrzení o doručení a otevření zásilky (doručenka).

Nevýhodou je, že obě strany musí být uživateli REP, mít s Českou poštou uzavřenou smlouvu a samozřejmě za užívání služby platit. Certifikát vydaný I.CA nevyužijete, jelikož má Česká pošta vlastní (neakreditovanou) certifikační autoritu, která vydává certifikáty pro uživatele poštovních aplikací.

9.4.4 Bezpečná a ověřitelná e-mailová komunikace

Hlavní funkci elektronického podpisu nesmíme v našem seznamu opomenout. Pokud oba komunikující subjekty jsou držiteli certifikátu, mohou použít své veřejné klíče k zašifrování zprávy. Šifruje se veřejným klíčem příjemce. Není vhodné používat stejný klíč pro více účelů, jelikož to usnadňuje případný útok. Podepsání zaručí druhé straně jistotu odesilatele. Problematiku jsme však probrali již dříve (viz. 3) a není nutné se jí zde více věnovat. Poslední možností mnou uvedenou jak zatím využít elektronický podpis, je podepisování dokumentů. Takto je možné podepisovat hlavně dokumenty ve formátu .pdf, dokumenty vytvořené v prostředí MS Office a přílohy k elektronické poště.

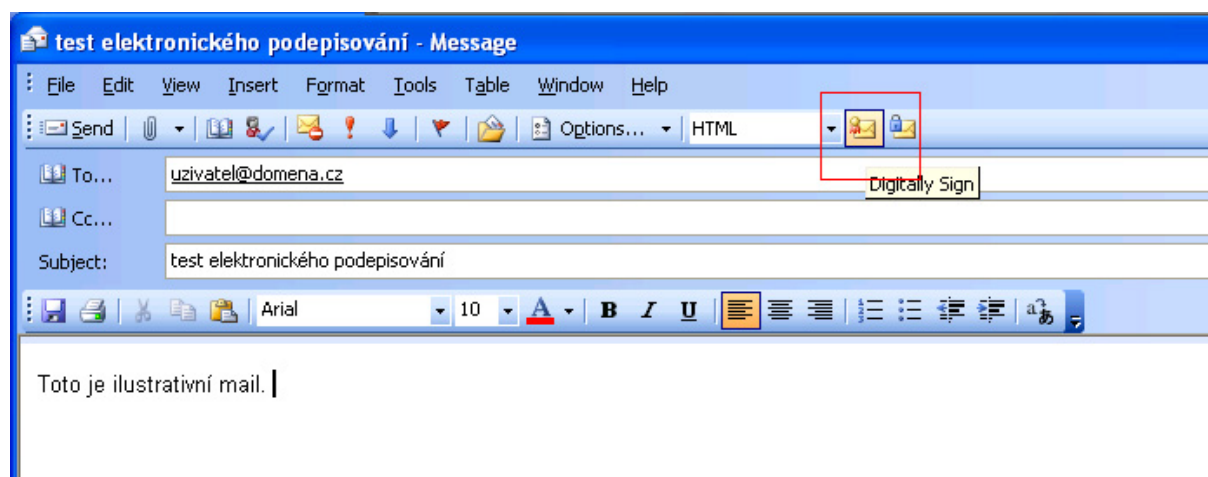
9.4.5 Shrnutí možností využití elektronického podpisu

Pokud se podíváme na výše uvedený seznam, je vidět, že největší uplatnění najde elektronický podpis ve firemní oblasti a zvláště ve zdravotnictví. Za předpokladu, že se subjekt dostává často do kontaktu s úřady, rovněž se mu vyplatí pořízení uznávaného podpisu.

Vezmeme-li v úvahu běžného občana, který je zaměstnancem nějaké firmy, kontaktu s úřady se vyhýbá jak může a e-mailovou komunikaci využívá pouze občasně, pak musím říci, že při současných cenových podmínkách se mu elektronický podpis rozhodně nevyplatí. Jediné využití, které mu zbývá je zabezpečená a ověřitelná e-mailová komunikace, a ta zdaleka nevyváží pořizovací náklady. My si přesto ukážeme, jak vypadá podepisování v aplikaci pro elektronickou poštu, abychom ilustrovali jediné možné použití pro nepodnikatele nekomunikujícího často s úřady.

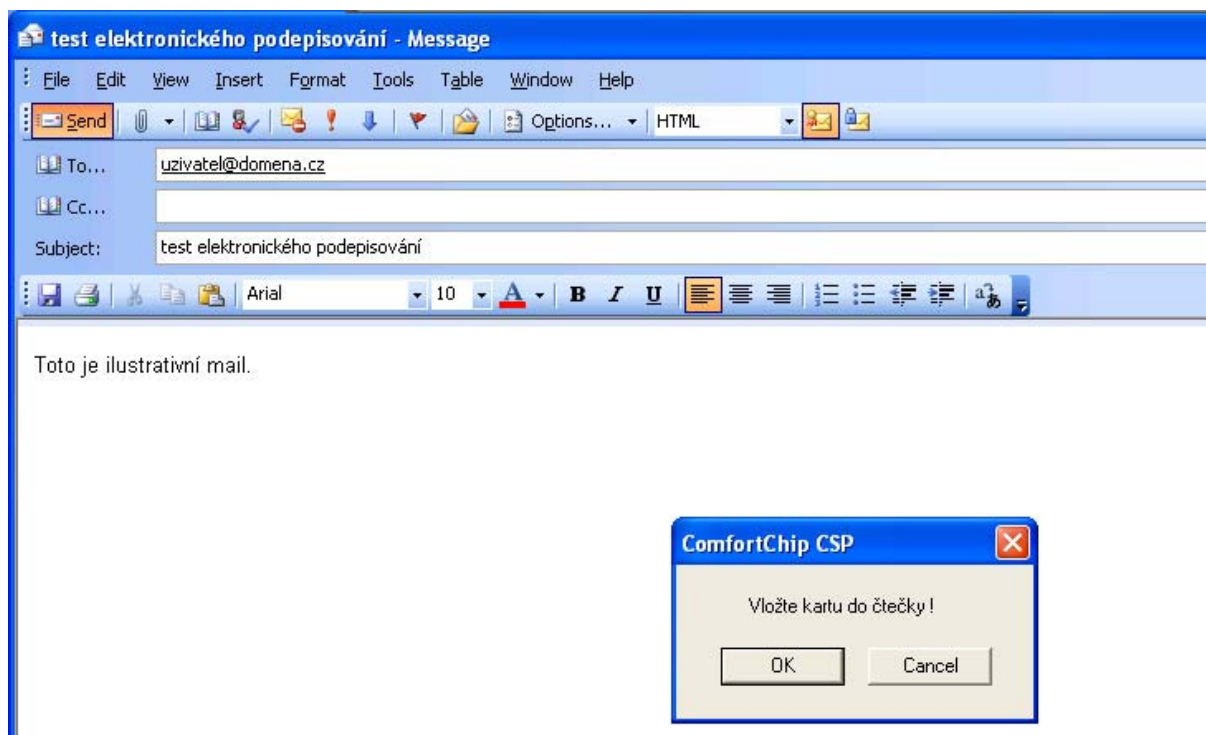
10 Podepisování e-mailu v prostředí MS Outlook

Práce s elektronickým podpisem je v prostředí MS Outlook velmi jednoduchá. Po snadné konfiguraci cesty ke klíči se můžeme směle pustit do tvorby e-mailu. Je nutné zmínit, že je nevhodné používat jeden klíč k více účelům. Avšak MS Outlook vyžaduje, aby měl klíč nastaveny parametry, které využití pro více účelů povolují. Přístupy vyžadované Microsoftem tak opět ovlivnily celý trh. Po vytvoření požadovaného e-mailu zvolíme možnost podepsat. To ukazuje červeně zvýrazněná část obrázku Obr. 8.

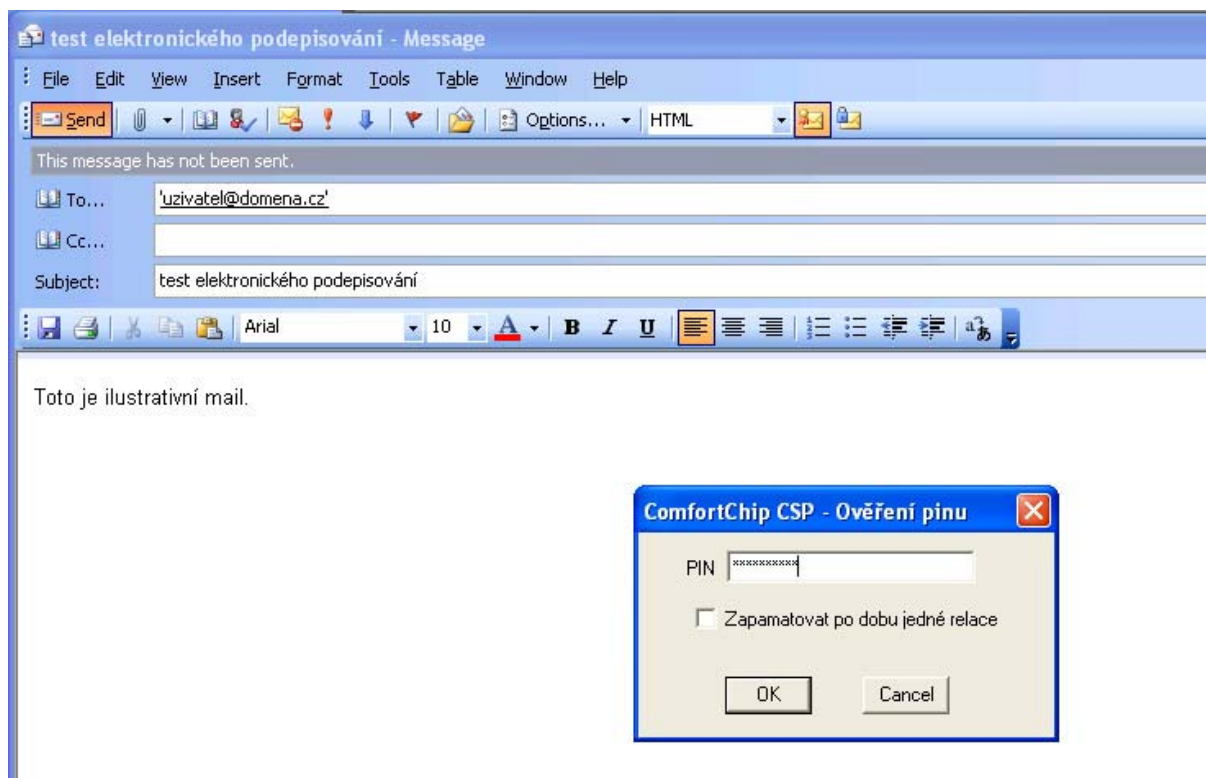


Obr. 8 - Podepsání e-mailu

Pokud máme prostředek pro vytváření podpisu na čipové kartě, tak po zvolení možnosti odeslat, budeme vyzváni k jejímu vložení a následnému zadání PINu. To nám ukazují obrázky Obr. 9 a Obr.10. Na kartě proběhnou kryptografické operace, které zajistí použití soukromého klíče na hash e-mailu a připojení výsledných dat k e-mailu. Po dokončení kryptografických operací máme podepsaný e-mail připravený k odeslání.

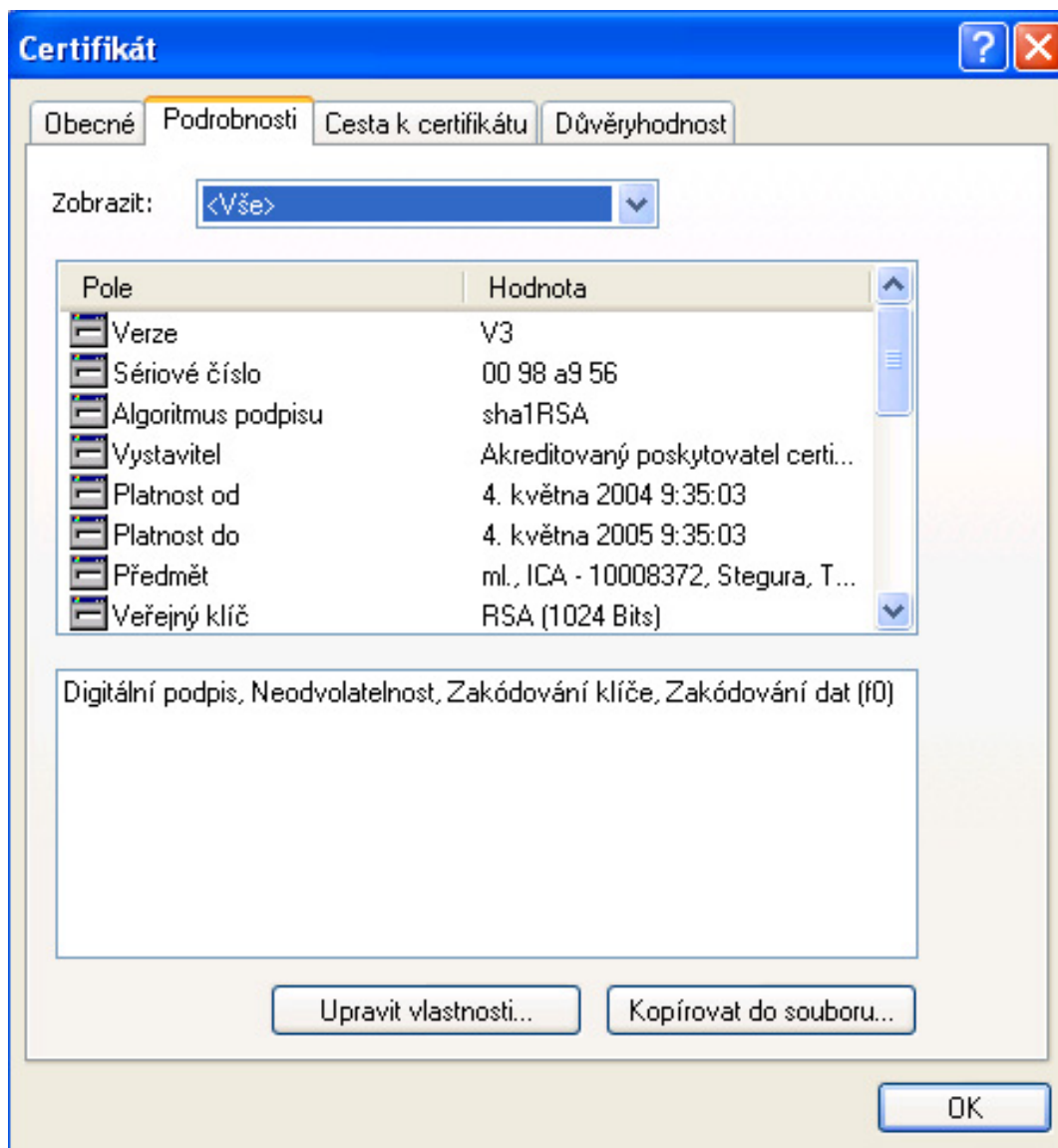


Obr. 9 - Zahájení procedury podepisování



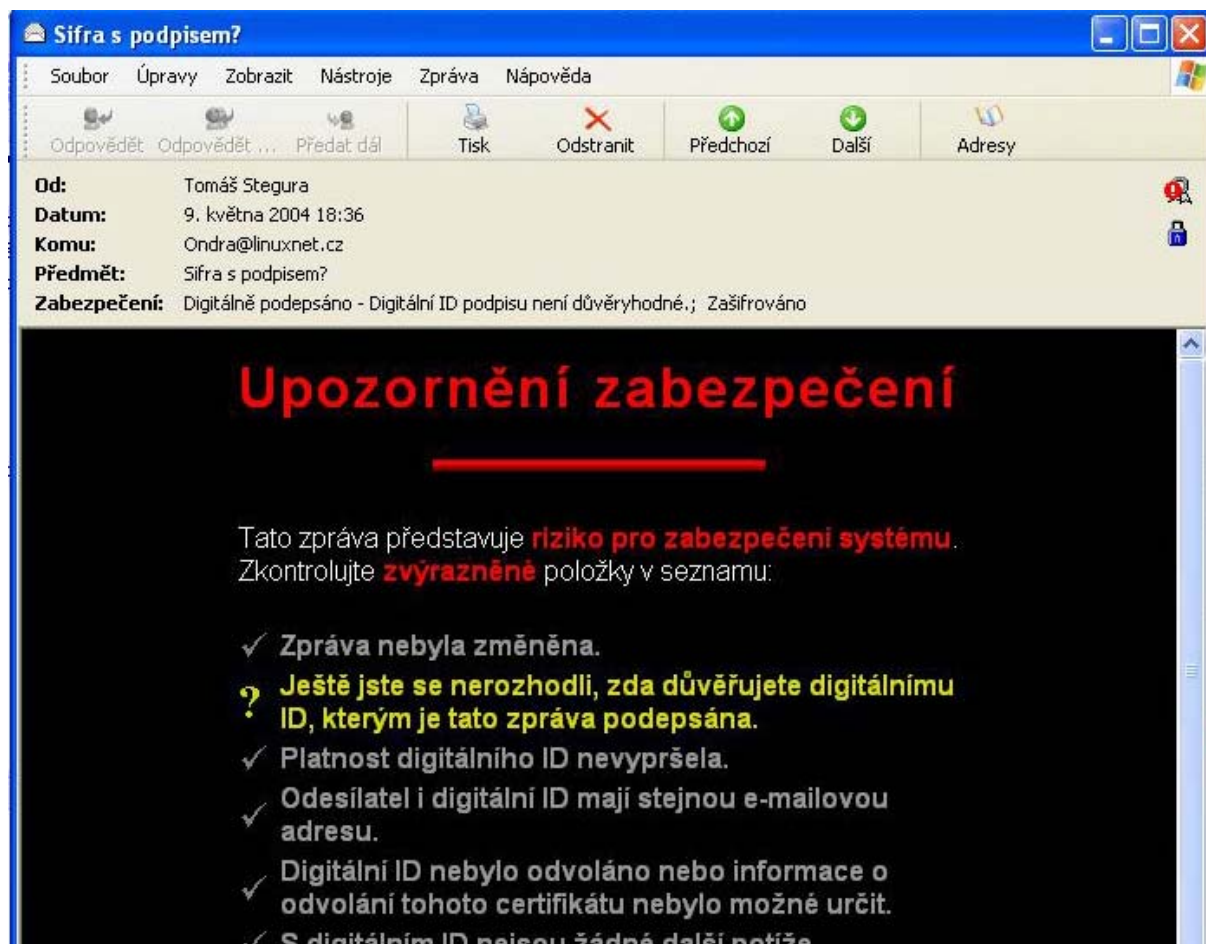
Obr. 10 - Autorizace uživatele karty

Další věcí, kterou si ukážeme je, jak operační systém Windows zobrazuje certifikáty. Můžeme se přesvědčit, že certifikát je vydán podle verze 3 normy X.509 a plní všechny námi jmenované funkce. Certifikát ukazuje obrázek Obr. 11.



Obr. 11 - Certifikát elektronického podpisu v prostředí Windows

Abychom dokončili ilustraci uživatelského pohledu na elektronický podpis, ukážeme si podepsaný příchozí e-mail. Můžeme vidět, že kompletní ověření elektronického podpisu za uživatele vykoná program. To dokládá obrázek Obr. 12.



Obr. 12 - Ověření elektronického podpisu programem MS Outlook

11 Využívání elektronického podpisu v ČR

V této části se podíváme jak je u nás EP využíván, jaké jsou faktory, které jeho využití ovlivňují a kterým směrem se ubírá vývoj.

Oblast komunikace občanů s úřady, kterou by stát rád rozvíjel, je ovlivněna těmito faktory:

- ochota občanů komunikovat s úřady,
- přístup občanů k prostředkům elektronické komunikace,
- počítačová gramotnost, neboli schopnost tyto prostředky ovládat,
- schopnost úřadů přijímat elektronickou komunikaci,
- vytvoření podmínek pro tuto komunikaci a zajištění právního rámce.

První bod v posledních letech značně stagnuje. Stále více lidí se snaží jakémukoliv kontaktu s úřady vyhnout a nezajímají se o informace úřady poskytované. Procento lidí, kteří spadají do této kategorie se od roku 2000 zvedlo z 38 % na 48 % v roce 2003, jak dokládá výzkum[21].

Druhý bod byl pravděpodobně naplněn. Podle výše zmíněného průzkumu dosáhla penetrace internetem u nás 41% populace. Což znamená, že dotazovaní deklarovali možnost přístupu k internetu. Největší možnosti má věková skupina 15 – 17 let, která deklarovala přístup k internetu v 84 % dotázaných. Nejnižší počet kladných odpovědí byl, dle očekávání, u kategorie 60 let a více, kde činil 15%. Je vidět, že k elektronické komunikaci lidé přístup mají.

Počítačová gramotnost je již závažnějším faktorem. Neschopnost ovládat počítač je patrná zvláště u starších generací. V kategorii 45 – 59 let počítačovou ngramotnost proklamovalo 66 % dotázaných a v kategorii 60 let a více počítačově ngramotní činili 80 % dotázaných. Zapojení těchto kategorií do využívání prostředků elektronické komunikace je téměř nereálné.

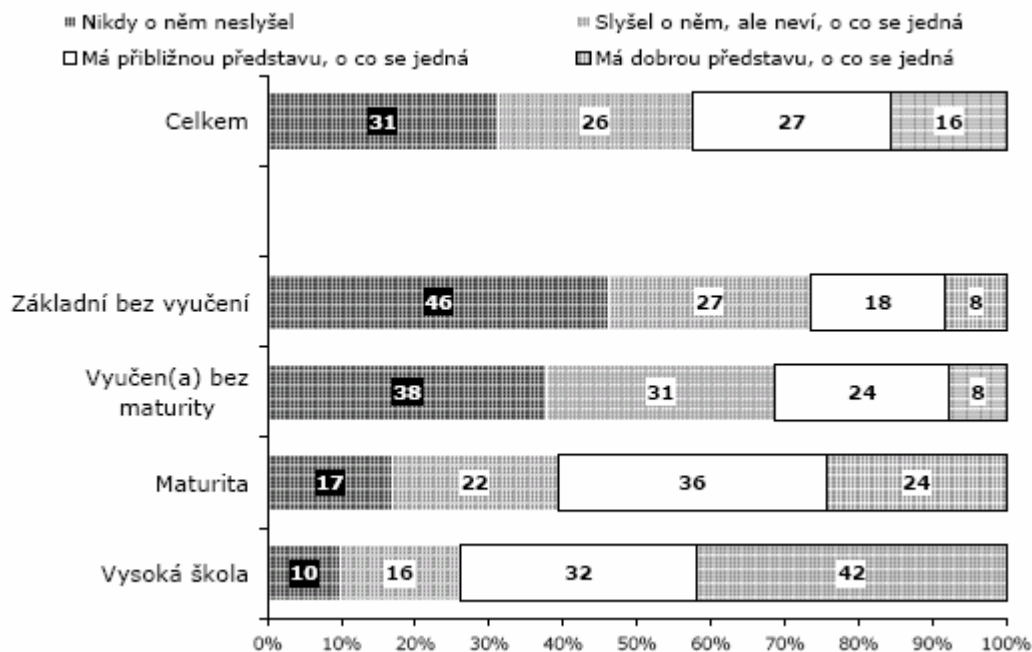
Úřady jsou se standardy ISVS většinou seznámeny. Jejich naplňování není zdaleka na úrovni, která by byla dostačující. Z velké většiny požadavky stanovené standardy splňuje pouze 27 % úřadů.

Podmínky pro využívání elektronické komunikace vytvořeny byly. Legislativa je dostačující.

Z výše uvedených faktů vyplývá, že lidí, kteří by využili elektronický podpis pro komunikaci s úřady, není mnoho. Navíc s elektronickým podpisem není ani obyvatelstvo dostatečně seznámeno. Pouze 43 % obyvatel má alespoň hrubou představu, co to je elektronický podpis. Viz Obr. 13. Po odečtení té části populace, která není schopna zacházet s počítačem, nám zůstávají lidé, kteří si zdaleka nepřejí využívat institutu elektronického podpisu. Zájem využít elektronický podpis pro komunikaci s úřady projevilo zhruba 20 % lidí. Oproti tomu zájem využít elektronického podpisu při komunikaci s bankovním sektorem vyjádřilo 28 % dotazovaných.

Dalším faktorem, který brání širšímu využití elektronického podpisu je cena certifikátu. Podle výzkumu [21] jsou naši občané ochotni platit za certifikát částku 400 Kč ročně. Nejlevnější certifikát splňující podmínky dané legislativou však stojí téměř dvakrát tolik. V ceně certifikátu vidím výraznou brzdou rozšíření elektronického podpisu.

Elektronický podpis je u nás využíván převážně státním sektorem, bankami a pojišťovny. Pouze 5 % lidí využívajících elektronický podpis jsou „obyčejní“ občané. [22] Toto číslo se bude jistě postupem času zvyšovat, ale pokud budou stávající podmínky zachovány, tak zajisté velmi pomalu.



Obr. 13 - Znalost elektronického podpisu, rozložení podle vzdělání
Obrázek převzat ze zdroje [21]

Abychom shrnuli výše uvedené závěry, uvedeme, že elektronický podpis se v našich zemích teprve rozvíjí. Zákony nastavily podmínky v takové míře, že je možné elektronický podpis reálně využívat. Avšak i přes podporu zákonů se o něm musí občané dozvědět, pochopit jeho princip a získat motivaci pro jeho užívání. Ta musí být natolik vysoká, aby potlačila negativum v podobě vysoké ceny certifikátu.

12 Vyhlídky do budoucna

Elektronický podpis, za předpokladu, že se rozšíří, může přinést zvýšení bezpečnosti, usnadnit komunikaci s orgány veřejné moci a umožnit plný rozvoj elektronického obchodu. Proto se však musí naplnit několik podmínek. Elektronický podpis musí být využíván daleko více v komerční sféře, nikoliv jen ve sféře soukromé a ve veřejné správě. Zákonem uznaný podpis by měl být akceptován všemi subjekty, bez nutnosti mít několik podpisů pro různé příležitosti.

Elektronický podpis by se mohl stát součástí elektronického dokladu budoucnosti, který by za kombinace biometrie a kryptografie přinesl bezpečný univerzální doklad totožnosti kombinovaný s průkazem pojištěnce, elektronickou peněženkou i klubovými kartami. Ale to již příliš zabíháme do budoucnosti.

V nejbližší době se pravděpodobně staneme svědky rozsáhlejšího využití časových razítek v kombinaci s elektronickým podpisem. Tato kombinace zajistí elektronickou formu notářských služeb. Rozvoj elektronických značek zpřístupní vyšší míru automatizace při vyřizování žádostí bez nutnosti práce lidského faktoru. S elektronickým podpisem by, jako s každým správným vynálezem, měl být náš život opět o něco snazší.

Závěr

Nyní nastal čas, abych shrnul své poznatky jak z teoretické části, tak i z praxe. Poznal jsem princip elektronického podepisování, asymetrického kryptování i zákony. Všechny tyto prvky umožňují využití elektronického podpisu v praxi. Model získávání certifikátu za ostatními sice trochu pokulhává, ale stále nebrání většímu rozmachu elektronického podepisování.

Co na to říká praxe? Jak jsem mohl vyzkoušet, praxe není příliš rozšířená. Je smutným faktem, že elektronický podpis není v ČR ani natolik známý, aby mohl být masově používán. Většina lidí má neustále představu o tom, že se podepíše do počítače. Ti, kteří vědí, jak se věci mají ve skutečnosti, ale narážejí na několik překážek.

První z nich je nízká využitelnost pro nepodnikatelský subjekt. Do doby, než bude jeden kvalifikovaný zákonem uznávaný certifikát akceptován téměř všude, zůstane tato překážka nepřekonatelná. Pokud dojde ke sjednocení a bankovní sektor začne přijímat takovéto certifikáty pro vstup do svých e-bankingových systémů, může to výrazně přispět k rozšíření používání elektronického podpisu.

Druhou překážkou je vysoká cena za vydání certifikátu. Při současné využitelnosti se většině lidí naprosto nevyplatí zaručený elektronický podpis používat. Podnikatelé mohou mít pro elektronický podpis větší uplatnění, ale běžný občan nikoliv. Několik dotazů na úřad, případně podání k soudu nemůže ospravedlnit výdaj na certifikát. Původ této překážky bych viděl v jediném akreditovaném poskytovateli certifikačních služeb.

Překážku počítačové gramotnosti pouze zmíním, ale s vědomím, že jí nepřekoná téměř polovina národa. Musím ale také zmínit, že je tendence tento stav změnit. Stát se snaží obyvatelstvu pomoci při používání počítače. Existují kurzy, například ECDL, které mají za úkol posluchače naučit základům práce s počítačem. Jejich dotování státem má pomoci změnit nepříznivý stav počítačové gramotnosti. Věřím, že počítačová gramotnost časem přestane být problémem.

Do překonání těchto překážek se rozšířeného využití elektronického podpisu nedočkáme. Zůstane nástrojem několika vyvolených, kteří jej získají od zaměstnavatele, nebo nadšenců pro moderní technologie, kteří jej musí mít. Je to osud každé moderní technologie. Každou čeká test, zda-li přináší takové výhody, aby se začlenila do běžného života. Já doufám, že elektronický podpis v tomto testu obstojí.

Přínos mé práce spočívá v praktických zkušenostech s elektronickým podpisem a zhodnocení současného stavu s analýzou možných příčin, jejichž odstranění by mohlo mít za následek jeho další rozvoj.

Seznam použitých zkratk

I.CA	První Certifikační Autorita, a.s., jediný akreditovaný PCS v ČR
ASCII	American Standard Code for Information Interchange, znaková sada
B2B	Business to Business, elektronický obchod mezi podnikatelskými subjekty
B2C	Business to Consumer, elektronický obchod mezi podnikatelským subjektem a spotřebitelem
CA	Certifikační autorita, subjekt vydávající certifikáty k veřejným klíčům
CD	Compact Disc, médium pracující na optickém principu, běžná kapacita 800 MB
CRL	Certificate Revocation List, seznam zneplatněných certifikátů
ČR	Česká republika, stát ve střední Evropě
DPH	Daň z přidané hodnoty, nepřímá spotřební daň
DSA	Digital Signature Algorithm, asymetrická šifra pro elektronický podpis
DSS	Digital Signature Standard, US standard pro elektronický podpis
EP	Elektronický podpis
ES	Evropské společenství, předchůdce EU
EU	Evropská unie, uskupení evropských států
ISVS	Informační systémy veřejné správy
ITU-T	International Telecommunication Union, sekce Telecommunication Standardization Sector, instituce vydávající standardy k telekomunikacím
MB	Mega Byte, jednotka velikosti informace
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
MS	Microsoft, softwarový gigant
PCS	Poskytovatel certifikačních služeb
PGP	Pretty Good Privacy, systém bezpečné a podepsané elektronické pošty vytvořený Philipem Zimmermannem
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, elektronický doporučený dopis
rfc	Request for query, standardizační dokumenty pro prostředí internetu
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
UTF-8	Unicode Transmission format, kódování znakové sady Unicode
ÚOOÚ	Úřad na ochranu osobních údajů
WWW	World Wide Web, technologie internetového prezentování informací
ZoEP	Zákon o elektronickém podpisu, č. 227/2000 Sb.

Seznam obrázků

OBR. 1 - ASYMETRICKÉ ŠIFROVÁNÍ	14
OBR. 2 - VYUŽITÍ ASYMETRICKÉHO ŠIFROVÁNÍ PRO ELEKTRONICKÝ PODPIS	15
OBR. 3 - ELEKTRONICKÝ PODPIS S VYUŽITÍM CERTIFIKÁTU OD CA	16
OBR. 4 - KOMPLETNÍ SCHÉMA ELEKTRONICKÉHO PODPISU	19
OBR. 5 - UKÁZKA ČÁSTI CERTIFIKÁTU DLE NORMY X.509	22
OBR. 6 - ČIPOVÁ KARTA VYDÁVANÁ I.CA	25
OBR. 7 - ČASOVÉ RAZÍTKO	33
TABULKA 1 - POČTY ELEKTRONICKÝCH PODÁNÍ K 26.2.2004	42
OBR. 8 - PODEPSÁNÍ E-MAILU	45
OBR. 9 - ZAHÁJENÍ PROCEDURY PODEPISOVÁNÍ	46
OBR. 10 - AUTORIZACE UŽIVATELE KARTY	46
OBR. 11 - CERTIFIKÁT ELEKTRONICKÉHO PODPISU V PROSTŘEDÍ WINDOWS	47
OBR. 12 - OVĚŘENÍ ELEKTRONICKÉHO PODPISU PROGRAMEM MS OUTLOOK	48
OBR. 13 - ZNALOST ELEKTRONICKÉHO PODPISU, ROZLOŽENÍ PODLE VZDĚLÁNÍ	50

Seznam literatury

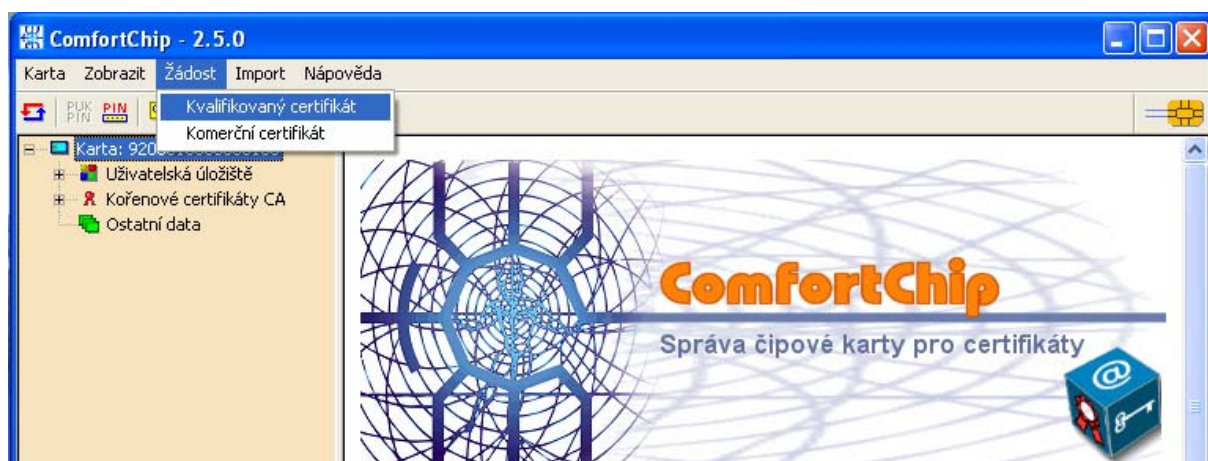
- [1] Zákon 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu, dále označovaný jako ZoEP, § 2
- [2] ZoEP, § 2
- [3] ZoEP, § 3a
- [4] ZoEP, § 12
- [5] RSA Laboratories, PKCS #1 v2.0: RSA Cryptography Standard, October 1998.
- [6] National Institute of Standards and Technology, .NIST: FIPS Publication 186-2: Digital Signature Standard (DSS), January 2000.
- [7] rfc 1991 – PGP Message Exchange Formats, Network Working Group, August 1996
- [8] rfc 2440 – OpenPGP Message Format, Network Working Group, November 1998
- [9] rfc 2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, March 1999
- [10] rfc 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group, April 2002
- [11] National Institute of Standards and Technology, .NIST: FIPS Publication 140-1: Security requirements for cryptographic modules, January 1994.
- [12] Vondruška, P.: Přehled standardů pro elektronické podpisy (výběr).
In: Crypto-World, 9/2000, <http://www.muweb.cz/veda/gcucmp/>
- [13] ZoEP, § 12
- [14] ZoEP, § 17
- [15] Vyhláška č. 366/2001 Sb., kterou se provádí zákon o elektronickém podpisu
- [16] Novela zákona o elektronickém podpisu – znění se senátními pozměňovacími návrhy k 24.6.2004.
Zdroj: Vojtěch Kment Consulting
- [17] www.ica.cz
- [18] Ceník I.CA, <http://www.ica.cz/cenik.html>
- [19] Kment, V.: Elektronický podpis pomalu ale jistě.
In: ComputerWorld, 43/2002
- [20] Faltýnek, M.: Podávání daňových přiznání v elektronické podobě se zaručeným elektronickým podpisem.
In: ISSS 2004, Hradec Králové, 2004, www.issc.cz
- [21] Výzkum agentury STEM/MARK 15.12.-22.12.2003, 2599 respondentů dotazováno face-to-face metodou.
Zdroj: materiály konference ISSS 2004 konané v březnu 2004

- [22] Rees, B., Tichá L.: E-podpisy zdarma k mání
In: ebiz, 7-8/2004
- [23] Smejkal, V.: Informační systémy veřejné správy ČR.
Skripta, VŠE, 2003
- [24] Smejkal, V.: Internet a §§§.
druhé aktualizované a rozšířené vydání, Grada, Praha, 2001
- [25] Materiály ke konferenci ISSS z let 2004, 2003, 2002
- [26] Studijní text o ASN.1, zdroj: Vojtěch Kment Consulting, 2004
- [27] Články z informačního serveru Lupa, www.lupa.cz
- [28] Malina, P.: Důvěřuj, ale prověřuj.
In: PC World, 3/2004 a 4/2004
- [29] Články z periodik Hospodářské noviny, Business World, PC World, Computer World, Crypto-World
- [30] Elektronické dokumenty publikované Ministerstvem Informatiky, www.micr.cz
- [31] První Certifikační Autorita, a.s.: Certifikační politika pro vydávání osobních kvalifikovaných certifikátů.
verze 1.03, 2004, www.ica.cz
- [32] Magazín Egovernment, vybraná čísla z ročníků 2001, 2002, 2003

Generování žádosti o kvalifikovaný certifikát

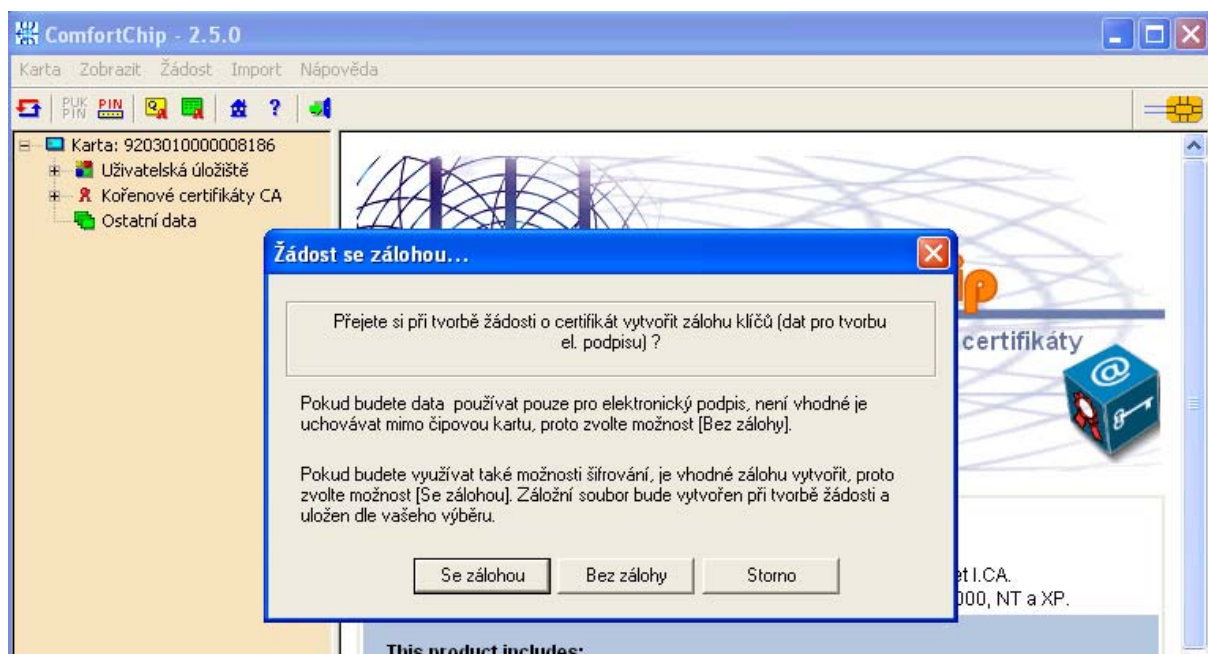
V příloze vám popíši jakým způsobem zažádat o kvalifikovaný certifikát. Pro přehlednost výkladu jej doplním screenshoty (ukázky obrazovek) z využitého programu.

Generování žádosti o kvalifikovaný certifikát provedeme za pomoci programu ComfortChip. Ten je k dispozici na www stránkách I.CA ke stažení. Program slouží ke správě dat na čipové kartě. Prvním krokem bude spuštění programu ComfortChip a vložení karty do čtečky. Následně z menu vybereme položku „Žádost“ a zvolíme „Kvalifikovaný certifikát“. To ukazuje screenshot na Obr. 1.



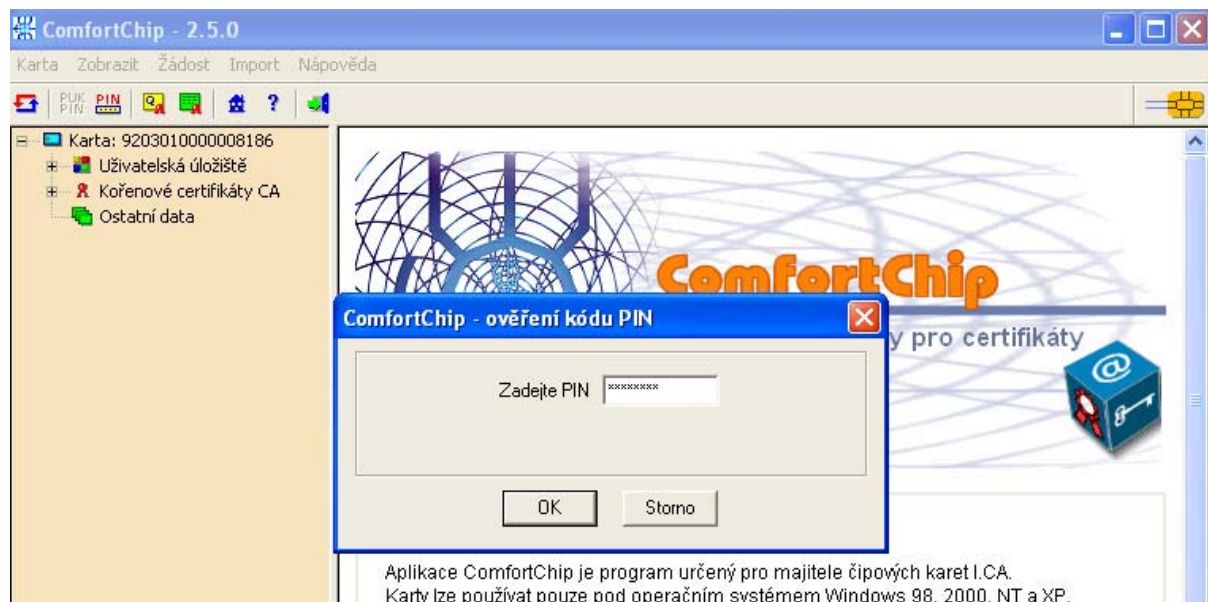
Obr. 1 - Volba z menu

Dále vybereme, pro jistotu, možnost se zálohou klíčů. Vždy ji můžeme smazat, ale musíme se ujistit, že se nedostane do nepovolaných rukou. To ukazuje Obr. 2



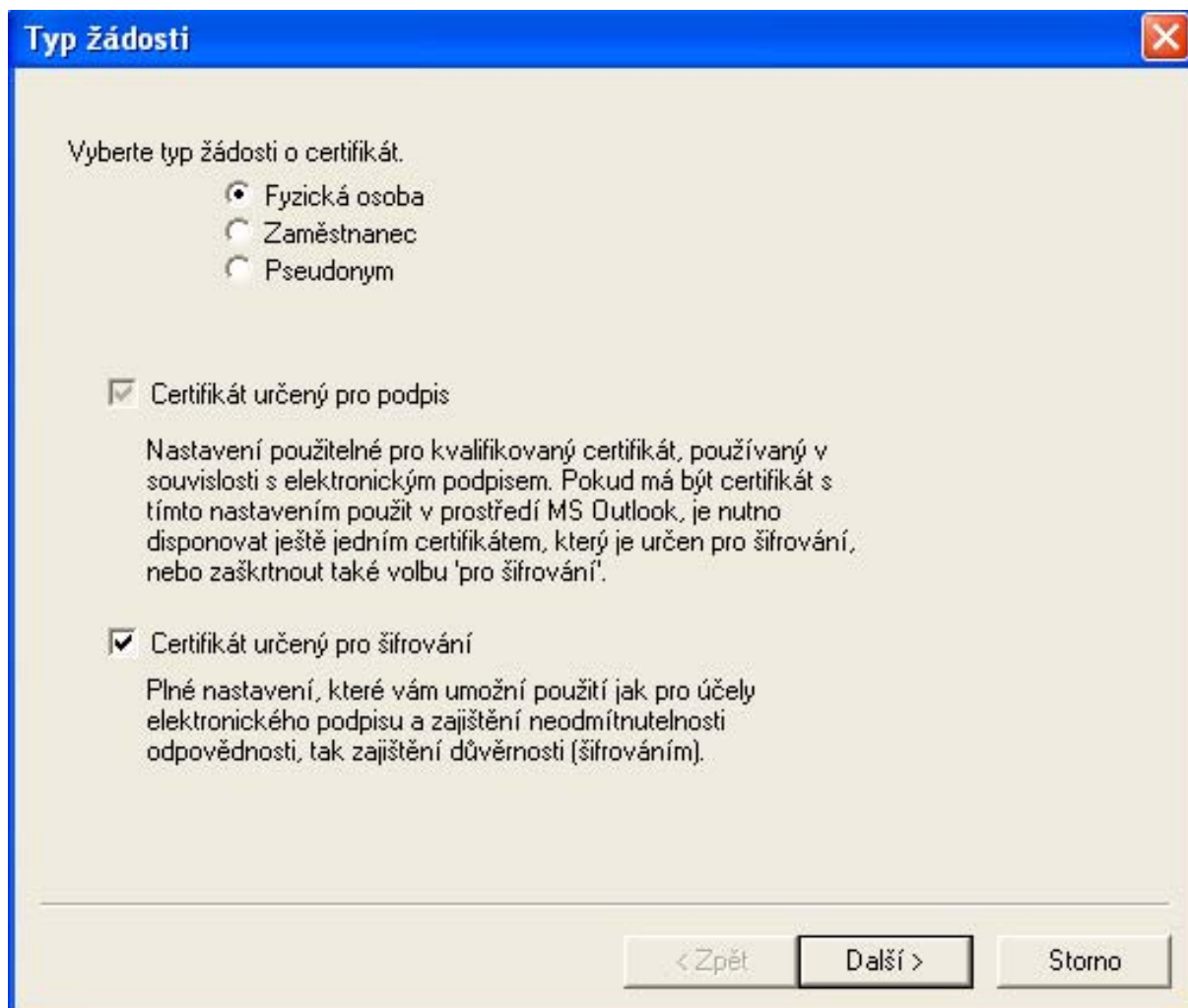
Obr. 2 - Volba zálohy klíčů

Budeme vyzváni k zadání PINu karty. Ten jsme obdrželi společně s kartou, nebo jej nastavili dříve. To ukazuje Obr. 3.



Obr. 3 - Zadání PIN

Na následující obrazovce zvolíme, o jaký typ certifikátu budeme žádat. Jelikož proces žádání o kvalifikovaný certifikát řešíme pro fyzickou osobou, zvolíme tuto možnost. Protože chceme, aby nám certifikát bez problémů pracoval v prostředí MS Outlook, zvolíme, že chceme certifikát používat i pro šifrování. Neznamená to ale, že jej tak skutečně budeme používat, protože teorie šifrování nedoporučuje využití klíče k více účelům. To, jak tyto možnosti zvolíme, je vidět na Obr. 4.



The screenshot shows a dialog box with a blue title bar containing the text 'Typ žádosti' and a close button. The main area is light gray and contains the following text and controls:

Vyberte typ žádosti o certifikát.

- Fyzická osoba
- Zaměstnanec
- Pseudonym

Certifikát určený pro podpis

Nastavení použitelné pro kvalifikovaný certifikát, používaný v souvislosti s elektronickým podpisem. Pokud má být certifikát s tímto nastavením použit v prostředí MS Outlook, je nutno disponovat ještě jedním certifikátem, který je určen pro šifrování, nebo zaškrtnout také volbu 'pro šifrování'.

Certifikát určený pro šifrování

Plné nastavení, které vám umožní použití jak pro účely elektronického podpisu a zajištění neodmítnutelnosti odpovědnosti, tak zajištění důvěrnosti (šifrováním).

At the bottom, there are three buttons: '< Zpět', 'Další >', and 'Storno'.

Obr. 4 - Volba typu žádosti

Na následující obrazovce zadáme jméno a příjmení osoby, která žádá o certifikát. Doplníme tituly a uvedeme rodné číslo. Jelikož rodné číslo nebude přepravováno nezabezpečeným prostředím, můžeme jej bez obav zadat. To ukazuje Obr. 5.

Na další obrazovce zadáme kompletní adresu trvalého bydliště, přesně jak můžeme vidět na Obr. 6.

Osobní údaje ✖

Vyplňte prosím Vaše údaje.
Údaje budou použity pro vytvoření položek žádosti o certifikát.
Všechny vyplněné údaje budou na Registrační autoritě ověřeny podle průkazu totožnosti.

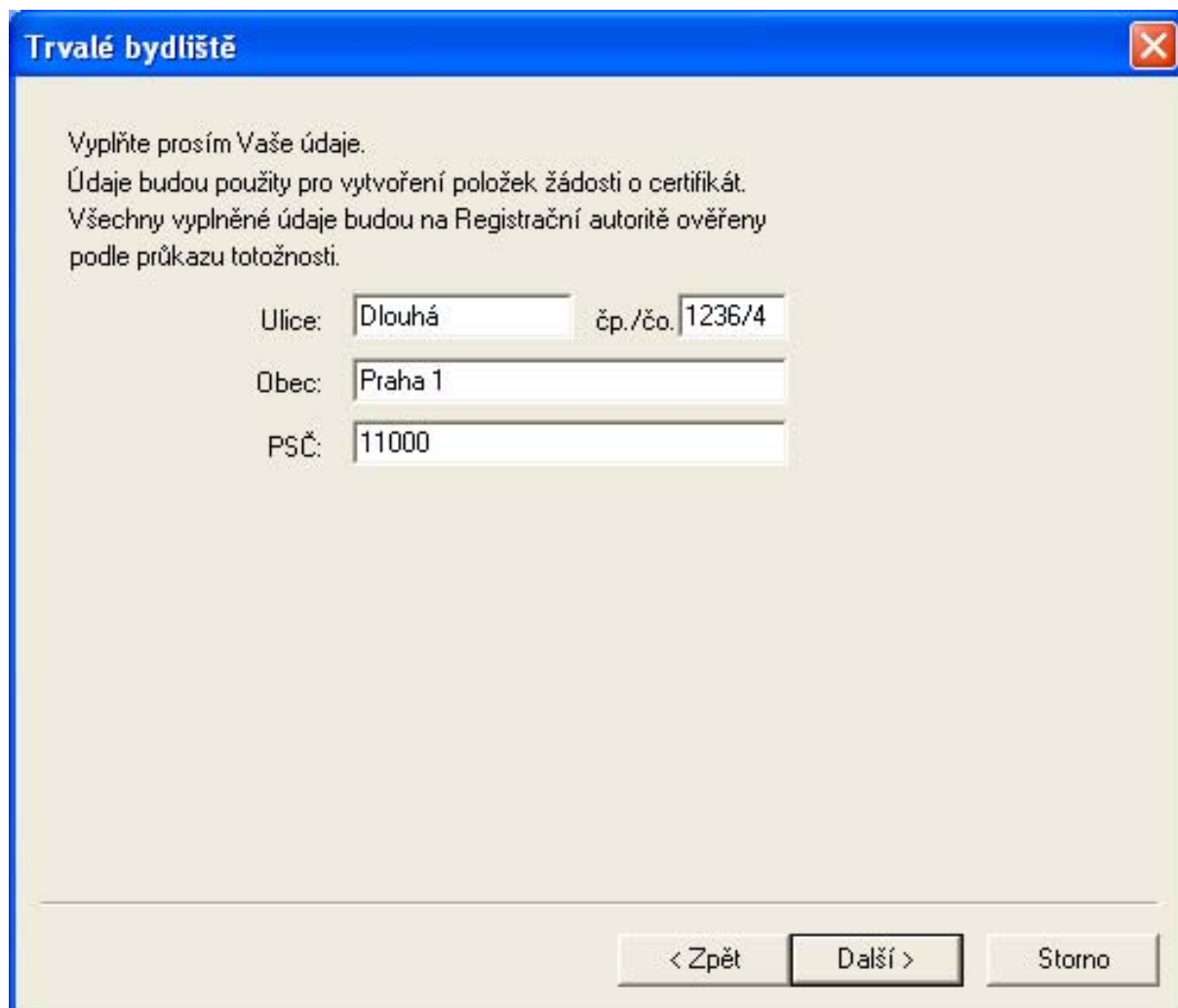
Jméno:

Příjmení:

Titul:

Rodné číslo:

Obr. 5 - Vyplnění osobních údajů



Trvalé bydliště

Vyplňte prosím Vaše údaje.
Údaje budou použity pro vytvoření položek žádosti o certifikát.
Všechny vyplněné údaje budou na Registrační autoritě ověřeny podle průkazu totožnosti.

Ulice: čp./č.o.

Obec:

PSČ:

< Zpět

Obr. 6 - Zadání adresy trvalého bydliště

Pokud by náhodou došlo k prozrazení soukromého klíče, je nezbytné zadat heslo pro zneplatnění certifikátu. Jen pro připomenutí uvedu, že heslo by mělo mít nejméně 8 znaků a mělo by obsahovat malá i velká písmena v kombinaci s číslicemi a speciálními znaky jako jsou #, @, %, &, * a jiné. Kam zadat heslo ukáže Obr. 7.

Heslo pro zneplatnění

Vyplňte položku heslo pro zneplatnění.
Toto heslo se používá v případě ztráty nebo krádeže soukromého klíče pro zrušení platnosti dosud platného certifikátu. Heslo nikdy nevolte stejné jako kterékoliv Vaše tajné heslo.

Heslo pro zneplatnění:

Ověření hesla:

< Zpět Další > Storno

Obr. 7 - Zadání hesla pro zneplatnění

Na následující obrazovce zkontrolujeme všechny uvedené údaje a případně doplníme ty, které bychom chtěli mít uvedené v certifikátu. Obrazovku ukazuje Obr. 8. Nezapomeneme zadat e-mailovou adresu, kterou plánujeme používat pro zaručenou poštu.

Položky certifikátu

Zkontrolujte a doplňte všechny položky certifikátu. Pro využití pro bezpečnou poštu musí být korektně vyplněna položka Email. Položky musí obsahovat diakritiku.

Celé jméno:	Jan Novák
Křestní jméno:	Jan
Příjmení:	Novák
Iniciály:	JN
Generační kvalifikátor:	
Titul:	
Stát:	CZ
Místo trvalého bydliště (Město, ulice čp./č.o.):	Praha 1, Dlouhá 1236/4
Oblast (např. Kraj):	Praha
Elektronická poštovní adresa:	elektronická@adresa.cz

Pro odborníky

< Zpět Další > Storno

Obr. 8 - Kontrola a doplnění údajů

V okně, které se nám odhalí po kliknutí na tlačítko „Pro odborníky“, zkontrolujeme, že jsou zatrženy atributy keyEncipherment a dataEncipherment, abychom se vyhnuli potížím s Outlookem, viz Obr. 9.

Položky pro odborníky

Použití klíče:

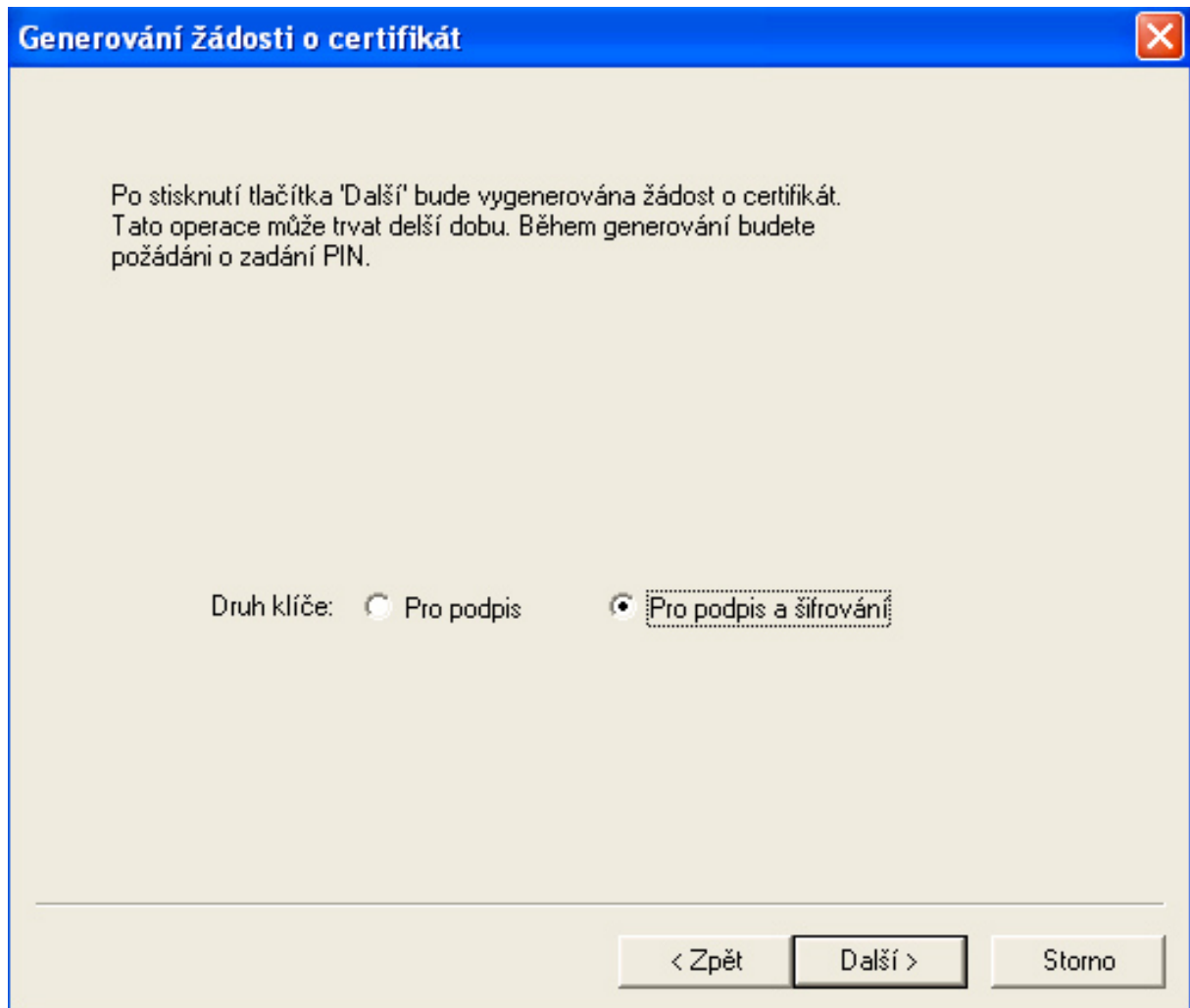
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment

OK Storno

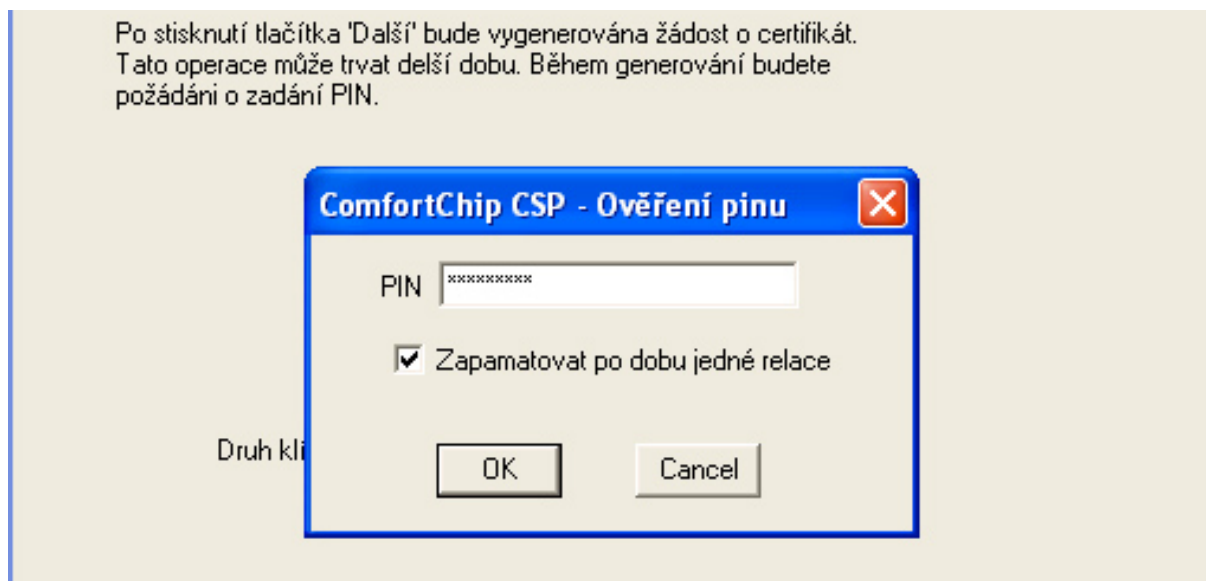
Pro odborníky

Obr. 9 - Okno volby Pro odborníky

Na další obrazovce zvolíme klíč pro podpis a šifrování, pro což máme pořád stejný důvod. To dokládá Obr. 10. Program nás opět požádá o PIN. Pro usnadnění zatrhneme možnost zapamatování PINu po dobu jedné relace. To nám ukazuje Obr. 11.

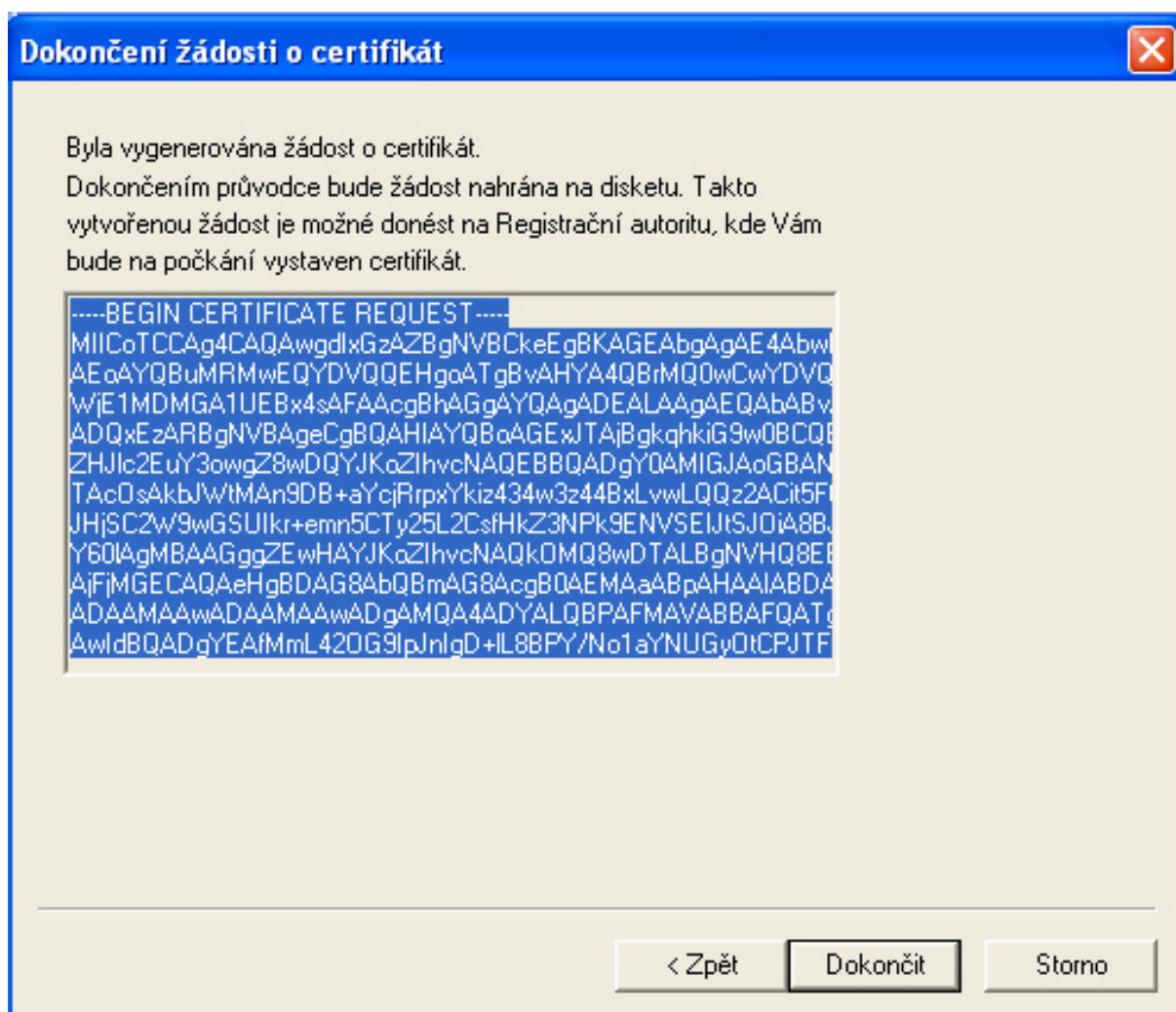


Obr. 10 - Volba využití klíče

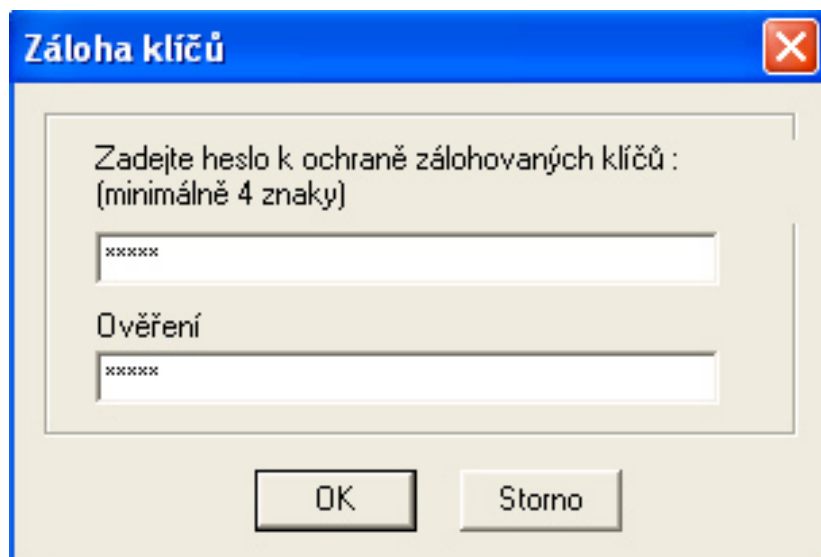


Obr. 11 - Zadání PIN

Na následující obrazovce (viz Obr. 12) si můžeme prohlédnout naši žádost o certifikát. Tím jsme skoro dospěli na konec procesu a zbývá nám jen uložit žádost na disketu. Zálohované klíče musíme ochránit heslem (viz Obr. 13).

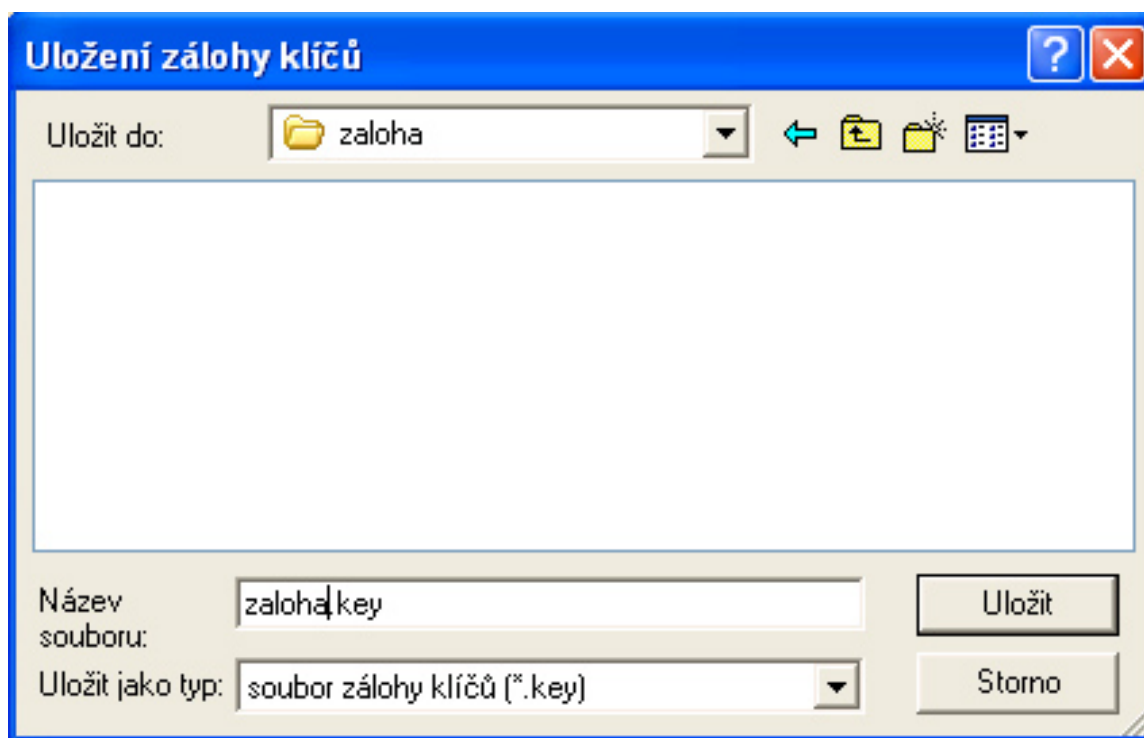


Obr. 12 - Dokončená žádost

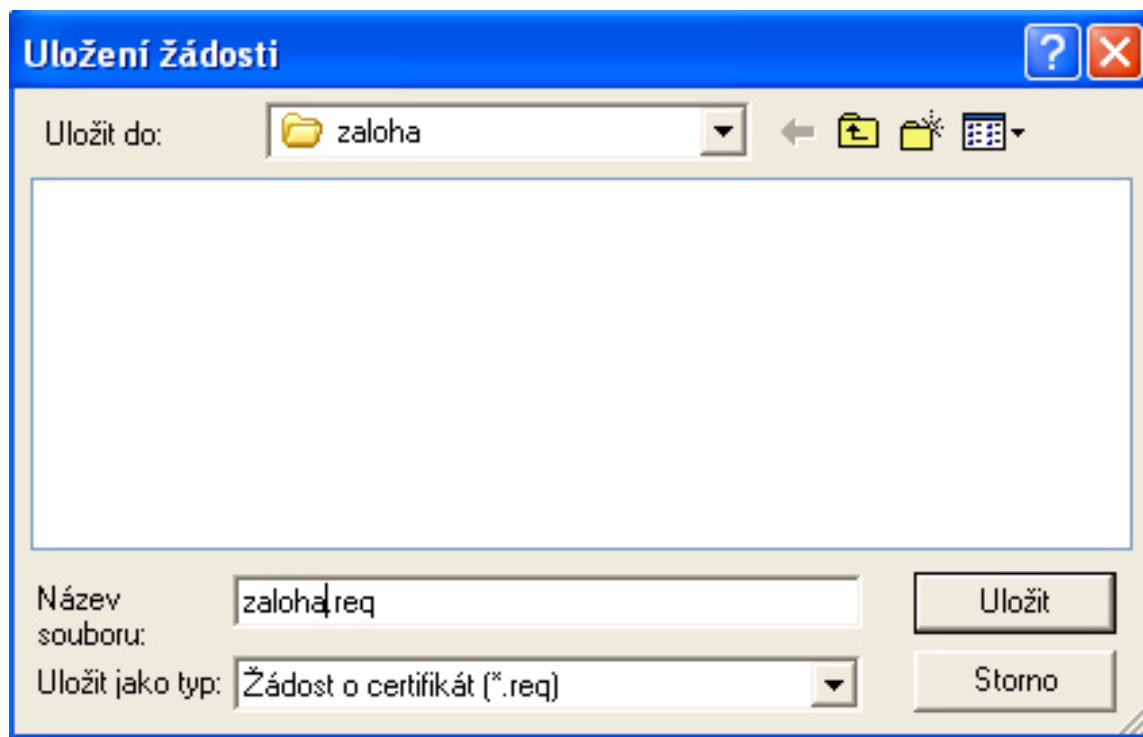


Obr. 13 - Zadání hesla pro zálohu klíčů

Vybereme umístění pro uložení záložních klíčů (viz Obr. 14) a pro uložení žádosti zvolíme disketu (Viz Obr. 15).

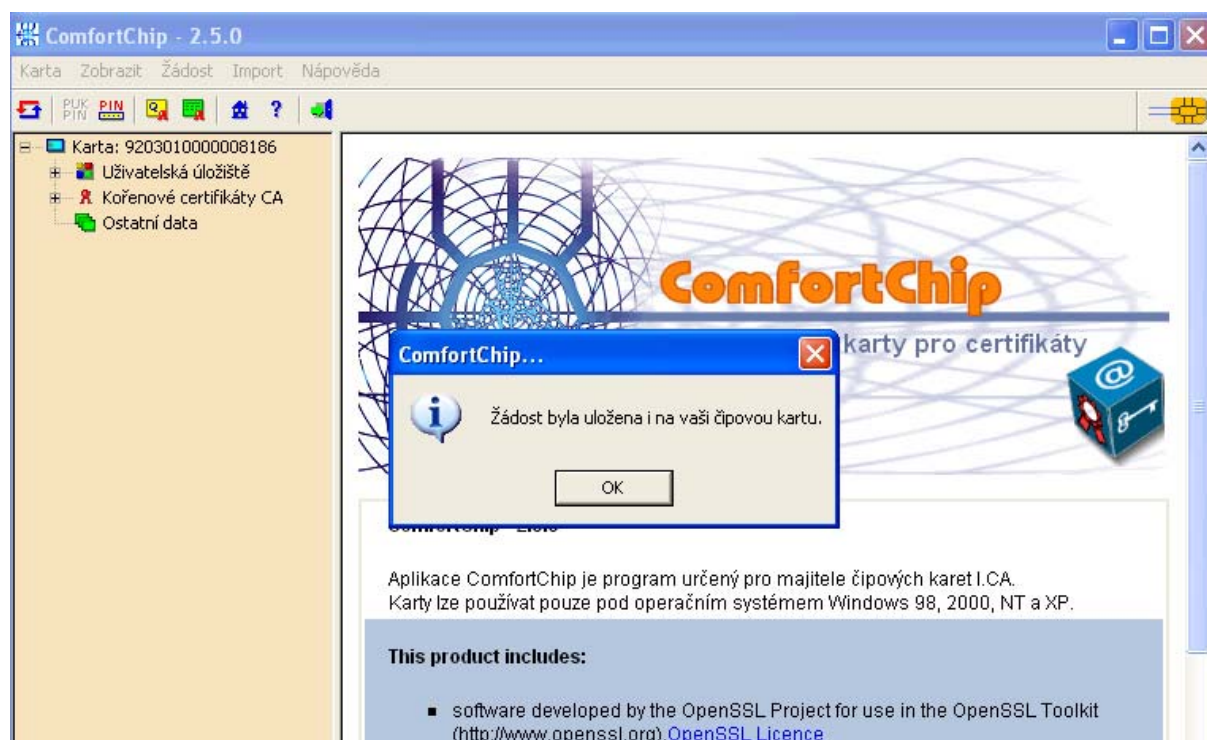


Obr. 14 - Uložení záložních klíčů



Obr. 15 - Uložení žádosti

Tím jsme úspěšně zakončili tvorbu žádosti o certifikát (viz Obr. 16). Žádost o certifikát máme uloženu na disketě i na čipové kartě. S disketou a dvěma doklady se musíme vypravit na pobočku CA, kde ověří naši identitu a sepiší s námi smlouvu o poskytování certifikačních služeb. Po zpracování žádosti CA obdržíme certifikát, který importujeme na kartu. Zvolíme z menu volbu „Import“ a postupujeme podle průvodce.



Obr. 16 - Dokončení