ELEKTRONICKÝ PODPIS A JEHO POUŽITÍ V PRAXI

Elektronic signature and his usage practically

Bc. Jan Prygl

Diplomová práce
2007

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav automatizace a řídicí techniky
akademický rok: 2006/2007

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan PRYGL**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Automatické řízení a informatika**
Téma práce:	**ELEKTRONICKÝ PODPIS A JEHO POUŽITÍ V PRAXI**

Zásady pro vypracování:

1.Vysvětlete pojem "elektronický podpis", jeho využití, potřebné nástroje, popř. používané technologie. Popište jaké algoritmy se využívají k šifrování el. podpisu, jaké existují typy el. podpisu.
2.Prezentujte v ucelené podobě maximum zákonů, vyhlášek a nařízení vlády tákající se el. podpisu.
3.Zpracujte téma "certifikační autorita" (obsah, akceptování jednotlivých certifikátů, autorita časové značky).
4.Porovnejte jednotlivé certifikační autority v tabulkové formě (dle ceny, délky klíče,způsobu ověření totožnosti, doby platnosti, způsobu podání žádosti o certifikát, atd.). Zhodnoťte certifikační autority dle výše uvedené tabulky.
5.Vyzkoušejte využití certifikátu v aplikaci Outlok Express.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. Bosáková,D;Vondružka,P; : Elektronický podpis
2. Vyhláška č.366/2001 Sb.: Vyhláška ÚOOÚ ze dne 3. října 2001 o upřesnění podmínek stanovených v Ô 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.
3. Vyhláška č.496/2004 Sb.: Vyhláška o elektronických podatelnách.
4. Zákon č.486/2004 Sb. (227/2000 Sb.): Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn.
5. Webové stránky certifikačních autorit,zdravotních pojišťoven,veřejné zprávy.

Vedoucí diplomové práce: **Ing. Tomáš Sysala, Ph.D.**
Ústav automatizace a řídicí techniky

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

Termín odevzdání diplomové práce: **24. května 2007**

Ve Zlíně dne 13. února 2007

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.
①

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá problematikou elektronického podpisu. Analyzuje faktory, které umožnily jeho vznik, rozebírá princip elektronického podepisování a přibližuje technickou i legislativní stránku věci se zaměřením na novelu zákona o elektronickém podpisu. Nastiňuje použití elektronického podpisu v komunikaci se státní správou, zdravotními pojišťovnami a porovnává poskytovatele certifikačních služeb především z hlediska pro-duktů, služeb, jejich cen, informací, které poskytují a mnoha dalších aspektů, které jsou vždy uvedeny v přehledové tabulce. Závěrečná kapitola popisuje způsob získání kvalifikovaného certifikátu od certifikační autority I.CA a první kroky při jeho využití. Je zde také naznačen uživatelský pohled na elektronický podpis při práci s elektronickou poštou. Závěrečné zhodnocení a výhled do budoucnosti doplňují ucelený přehled o tématu.

Klíčová slova: elektronický podpis , zákon o elektronickém podpisu, certifikát, certifikační autorita, šifrování, šifrovací algoritmy;

Abstrac

This thesis deals with the issue of electronic signature. It analyses factors which enabled its rise, construes principle of electronic signature and comes near to a technical and legislative side with a view to a law novel about electronic signature. It outlines using the electronic signature in communication with offices, health insurance company a. compare providers of certification services especially their products, services, prices and information that they offer and also many other aspects always mentioned in overview table. The final chapter describes the way how to obtain qualified certificate from certification authorities I.CA and first steps for its usage. There is also suggested a user's view of electronic signature during work with an electronic post. Final evaluation and a view into the future support comprehensive survey about the topic.

Key words: electronic signature, the law about digital signature, certificate, certification authority, coding and coding algorithms;

PODĚKOVÁNÍ

Dovoluji si tímto poděkovat panu Ing. Tomáši Sýsalovi, Ph.D., vedoucímu diplomové práce, za pomoc při sestavování mé diplomové práce, za usměrnění mé činnosti při plnění zadání diplomové práce a za všechny zodpovězené dotazy týkající se dané problematiky. Závěrem chci vyjádřit poděkování mé manželce Jitce Pryglové, dceři Magdalence, rodině a přátelům za jejich duševní podporu a trpělivost.

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

Ve Zlíně, dne 21. května 2007

…….

Bc.Jan Prygl

OBSAH

ÚVOD

V posledních letech se stále více dostává do povědomí jak laické tak odborné veřejnosti a medií pojem Elektronický podpis. Toto téma oslovilo i mne a tak jsem se začal o tuto problematiku zajímat blíže . Postupně jsem zjišťoval co to vlastně elektronický podpis je a na jakém principu funguje. Problematika elektronického podepisování mne zaujala tak, že jsem se rozhodl si téma elektronického podpisu vybrat jako téma diplomové práce.

Cílem této práce bude uceleně a přehledně vysvětlit pojem elektronický podpis, analyzovat principy elektronického podepisování po technické stránce, vytvořit přehled legislativních norem zabývajících se problematikou elektronického podpisu, jeho využití v současné praxi a to zvláště při komunikaci s orgány veřejné zprávy, zdravotními pojišťovnami nebo bankami.

V praktické části dojde k porovnání akreditovaných certifikačních autorit, přiblížím postup získání kvalifikovaného certifikátu , který je nutný pro používání elektronického podpisu a dále využití elektronického podpisu v aplikaci Outlook Express.

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

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÝ PODPIS

1.1 Seznámení s elektronickým podpisem

Naše planeta je protkána jednou velkou komunikační sítí, které se obecně říká Internet. Díky internetu a dalším moderním a komunikačním technologiím je možné navázat kontakt s opačnou polokoulí již za několik sekund. Elektronická pošta se tak rozmáhá čím dál víc. Mnoho lidí však chápe svět internetu jako svět bez pravidel, svět, ve kterém si každý může dělat co chce, vydávat se za koho chce a v případě nouze popřít své činy s vědomím, že mu je nebude nikdo sto prokázat.

Každý člověk má svoji identitu , kterou můžeme zjistit několika způsoby (např. občanský průkaz, otisk prstu atd.). Jedním z velmi používaných způsobů identifikace člověka je jeho vlastnoruční podpis. Ten má za úkol vyjádřit a současně stvrdit identitu autora i jeho vztah k napsanému textu.

Lidé již měli také dost času na to, aby si ujasnili, kdy, v jaké situaci a pro jaké účely stačí "obyčejný" vlastnoruční podpis, a kdy jsou zapotřebí jeho "silnější" formy (notářsky ověřený podpis, podpis před svědky apod.). Takto odstupňované požadavky jsou přitom pevně zakotveny v zákonech. Stejně tak je již dostatečně "zažité", kdo, kdy a jak ověřuje pravost podpisu - každý sám za sebe si kdykoli může udělat jakési letmé porovnání podpisu s podpisovým vzorem, má-li jej k dispozici. Důkladnější porovnání s podpisovým vzorem dělají například v bance když svým podpisem stvrzujete svůj požadavek na bankovní transakci. Ovšem skutečně věrohodné posouzení pravosti vlastnoručního podpisu musí dělat až soud, resp. soudní znalci (grafologové). Ani jejich verdikt však nemusí být vždy jednoznačný, v případě umně vyhotoveného falsifikátu. [2]

V případě elektronické komunikace je to jiné. Není už tak jednoduché zajistit pravost podpisu, původu zprávy, která nám přišla elektronickou poštou nebo pouze obsahu nějaké internetové stránky, to všechno mohl napsat kdokoliv a pouze se za danou osobu vydávat. U informačních a telekomunikačních technologií je typické i to, že zpráva či cokoliv jiného je rozesíláno či zveřejněno hromadně a má tedy mnoho příjemců. Jak mohou mít ale tyto osoby jistotu, že to, co si právě přečetly, pochází opravdu od podepsaného autora. Co když se pouze někdo snaží autora zdiskreditovat, ať už z jakéhokoliv důvodu a tím čehokoliv dosáhnout. Technologie, které nám zaručí pravost podpisu, původu zprávy, které nám přišla elektronickou poštou nebo autora obsahu nějaké internetové stránky již existují.

Tyto technologie jsou založeny na poměrně složitých algoritmech a principech. Na tyto se podíváme v další části této práce. Je důležité, že tuto, ať už jakkoliv složitou proceduru, je možné zredukovat na tlačítko „podepsat“ což je pro obyčejného uživatele, který by chtěl tuto technologii využít podstatné. Co se děje dál už není z hlediska obyčejného uživatele tak podstatné. K tomu, abychom mohli podepsat papírový dokument, potřebujeme kromě pera také schopnost vytvořit svůj právoplatný (vlastnoruční) podpis. Tato pro každého člověka jedinečná schopnost umožňuje pořídit náš, sice ne vždy zcela shodný, ale jednoznačně určující, charakteristický podpis na jakýkoliv dokument a za jakýchkoliv okolností. Tato schopnost je složitě zakódována v našem mozku. Je to jen naše soukromá charakteristika, která je (nebo by alespoň měla být) pro jiné osoby nedostupnou (tajnou) informací. Podobně pro elektronický podpis budeme používat také nějakou soukromou (tajnou) informaci, kterou vlastníme jenom my a nikdo jiný, a tato informace (číslo) bude reprezentovat naši schopnost vytvořit elektronický podpis. Toto číslo proto budeme dále nazývat „(tajné) podepisovací číslo“ nebo také „(tajný) podepisovací klíč“.

Nyní si představme, že podepisujeme papírový dokument. Vezmeme pero a na papír napíšeme svůj podpis. Tím, že na papír naneseme inkoust určitým způsobem, který je jedinečný jen pro nás, spojíme hmotné věci, tedy papír a inkoust, s věcí zcela nehmotnou - se svou jedinečnou schopností se podepsat a s konkrétním projevem této schopnosti (vyjádřené konkrétním jedinečným podpisem). U elektronického podpisu to probíhá velmi podobně. Místo papírového dokumentu zde máme číslo reprezentující digitální dokument a místo podpisové schopnosti máme teď tajné podepisovací číslo. Určitým matematickým spojením těchto dvou čísel vzniká číslo nové, a tím je právě elektronický podpis. Všechno probíhá stejně přirozeně jako u podpisu ručního. Proces spojení inkoustu s papírem při ručním podpisu je v případě elektronického podpisu nahrazen procesem spojení dvou čísel (digitálního dokumentu a tajného podepisovacího klíče) složitými matematickými operacemi. Toto spojení je schopen provést, jak jsme již uvedli, pouze počítač, protože je to velmi složitý výpočet.

Číslo reprezentující elektronický podpis daného digitálního dokumentu má mnoho zajímavých a výhodných vlastností:

- identifikuje původce podpisu (to znamená, že příjemce zprávy bezpečně ví, kdo je autorem nebo odesilatelem elektronické zprávy),

- zaručuje nepopiratelnost (osoba nemůže popřít, že danou zprávu s daným obsahem vytvořila),
- zaručuje integritu zpráv (příjemce má jistotu, že zpráva nebyla změněna) podpis je vytvořen pomocí prostředků, které podepisující osoba může mít pod svou výhradní kontrolou.

Elektronický podpis je také možné uložit nebo elektronicky přenášet mimo vlastní dokument. Ale hlavně: elektronický podpis je nepřenosný na jiný digitální dokument! Je totiž závislý na každém bitu digitálního dokumentu, k němuž náleží. Pokud podepisujeme (byť v jediném bitu) odlišné digitální dokumenty, jejich elektronické podpisy budou naprosto odlišné (nikoliv jen v jediném bitu). Tuto vlastnost zaručují právě výše uvedené matematické operace provádějící spojení tajného čísla s digitálním dokumentem. Jinými slovy, elektronický podpis má lepší vlastnosti než ručně psaný podpis – ten je totiž pokaždé stejný (a tedy snadno zfalšovatelný), zatímco elektronický podpis je na každém dokumentu jiný.

Když se podíváme-li na možnosti uplatnění elektronického podpisu, to první, co nás asi napadne, bude využití při komunikaci pomocí elektronické pošty (e-mailu). Dnes je poměrně jednoduché zfalšovat odesílatele elektronické zprávy, tak aby se tvářila, jako že ji poslal někdo úplně jiný. U zprávy opatřené elektronickým podpisem tato situace nikdy nastat nemůže. Dalším příkladem může být např. podepisování WWW stránek. Na internetu je možné najít opravdu mnoho článků a je fakt, že publikovat článek pod cizím jménem je ještě jednodušší, než zfalšovat onoho odesílatele u elektronické pošty. Proto, abychom mohli mít jistotu, že informace jsou podložené či že pochází od důvěryhodného autora, stačí opět elektronický podpis. V tisku hodně diskutovaná je komunikace se státní správou. Možností komunikace se státní správou je celá řada např. možnost podat daňové přiznání pomocí elektronické pošty a tak se vyhnout čekání ve frontách na finančním úřadě. Samotná komunikace pak probíhá přes tzv. elektronické podatelny (E - podatelny), o kterých se zmíním později. Posledním příkladem je bankovní sféra. Služby internetového bankovnictví umožňují získávat informace o účtech a provádět bankovní operace z domova či kanceláře, a to v kteroukoliv denní či noční hodinu.

Jistou zvláštností elektronického podpisu je to, že k tomu, aby se mohlo ověřit, zda daná elektronicky podepsaná zpráva pochází od onoho odesílatele není zapotřebí nějakého

znalce či specialistu v oblasti grafologie, o ověření se totiž postará technologie v podobě poměrně jednoduchého programu, který je už často připraven např. v emailových klientech. Co je však potřeba důsledně kontrolovat a dokonce ošetřit zákonem, je vydávání tzv. „podpisového vzoru“.

„Tento řeší tzv. certifikáty, které si lze představit jako spojení podpisového vzoru s identitou konkrétní fyzické osoby, neboli jako doklad o tom, že konkrétní podpisový vzor patří konkrétní fyzické osobě.“ [2]

Tyto certifikáty nemůže vydávat kdokoliv. Musí existovat zvláštní subjekty, které mají dostatečnou důvěru a prostředky na to, aby mohly zajistit vydávání takových podpisových vzorů , které budou pevně spojené s identitou konkrétních osob, tedy certifikátů. Takovýto subjekt se nazývá certifikační autorita.

Pořídit si certifikát je tedy záležitostí toho, kdo chce podepisovat. Tato osoba by pak ve svém vlastním zájmu měla poskytnout svůj certifikát co možná nejširšímu publiku (nejlépe zveřejnit na internetu). Pak svůj podpis může přikládat ke všemu, co uzná za vhodné a každý, kdo bude mít zájem, si může identitu této osoby jednoduše ověřit na základě zveřejněného certifikátu.

1.2 Pojmy a definice vztahující se k elektronickému podpisu

V této podkapitole se zaměřím na vysvětlení definic pojmů souvisejících s elektronickým podpisem, jež se budou objevovat v této diplomové práci. K tomuto účelu využiji literaturu [1], [3] a [7]

Elektronický podpis

Elektronický podpis je pro účely zákona o elektronickém podpisu chápán jako data v elektronické podobě, která jsou připojena k datové zprávě nebo jsou s ní logicky spojena a která umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Je jiný pro dvě odlišné zprávy, závisí na podepisované zprávě, nelze jej tedy koupit ani jinak obdobně získat. Elektronickým podpisem je v praxi zpravidla míněn zaručený elektronický podpis. Ten umožňuje vytvářet technologie digitálních podpisů.

Symetrická kryptografie

Typ kryptografických mechanismů založený na existenci jednoho šifrovacího klíče. Znamená to, že stejný klíč, který byl užit k zašifrování zprávy na straně odesilatele bude použit i na straně příjemce pro dešifrování zprávy. Z toho vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (konkrétní typ algoritmu) druhé straně. Problémem tohoto řešení je, že nelze zajistit tzv. neodmítnutelnost odpovědnosti (nelze jednoznačně určit autora zprávy, neboť oba komunikující partneři mají totožný šifrovací klíč).

Asymetrická kryptografie

Typ kryptografických mechanismů založený na dvojici klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných SW produktů (např. SSL) a stává se tak jejich jediným majitelem. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, takzvaný privátní klíč, je s maximální bezpečností ukrýván majitelem (čipová karty, USB token...), zatímco druhý klíč je zveřejněn – veřejný klíč. Veřejný klíč je následně využíván pro ověřován elektronického podpisu.

Soukromý klíč

Data pro vytváření elektronického podpisu. Zákon je definuje jako jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu. Tato data si každý zájemce generuje prostřednictvím aplikace pro generování klíčů. Data pro vytváření podpisu musí podepisující osoba uchovat v tajnosti. Mohou být uložena na pevném disku počítače, na disketě, na čipové kartě nebo v přenosném bezpečnostním modulu "tokeny".

Veřejný klíč

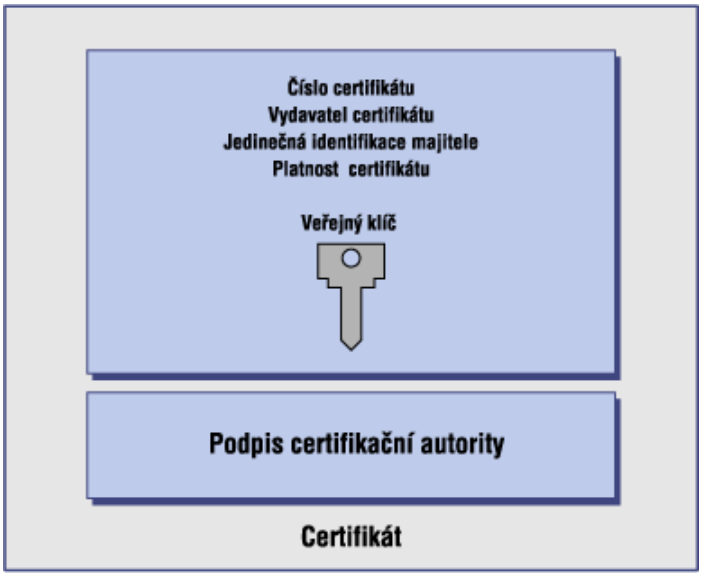
Data pro ověřování elektronického podpisu. Tato data si opět každý zájemce generuje prostřednictvím aplikace pro generování klíčů současně s daty pro vytváření elektronického podpisu. Data pro ověřování podpisu jsou na rozdíl od soukromého klíče určena ke zveřejnění. Je nutné je bezpečně předávat mezi podepisující osobou a osobou, která se na podpis spoléhá - zpravidla příjemce elektronicky podepsané zprávy. K tomuto bezpečnému předání může sloužit certifikát.

Hashovací funkce

Obecně matematická funkce, jejímž vstupem je libovolně velký datový blok a výstupem je datový řetězec pevné délky. V oblasti digitálních podpisů se hashovací funkce obvykle používají k výpočtu tzv. otisku podepisované zprávy. Namísto původní zprávy, tak podepisujeme její podstatně "kratší"otisk (délky např. 128 nebo160 bitů). Vlastnosti takových hashovacích funkcí navíc zaručují, že je prakticky nemožné vytvořit k libovolné zprávě jinou zprávu, která by měla stejný otisk. Když tedy ve zprávě změníme byť i jediné písmeno, otisk na výstupu bude zcela odlišný.

Certifikát

Certifikát je datová zpráva, která je vydávána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou nebo subjektem a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu. Certifikáty obsahují ve své nejjednodušší formě veřejný klíč, jméno a další údaje zajišťující nezaměnitelnost subjektů. Běžně používané certifikáty též obsahují datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu. To je zajištěno legislativními a technickými pravidly provozu instituce Certifikační autority.



Obr. č. 1 - Certifikát

Kvalifikovaný certifikát

Kvalifikovaný certifikát je certifikát, který byl vydán kvalifikovaným poskytovatelem certifikačních služeb. Tento certifikát obsahuje jednoznačnou identifikaci označující osoby, případně prostředku, pro vytváření elektronických značek, data pro ověřování elektronických značek.

Poskytovatel certifikačních služeb, certifikační autorita

Instituce, 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.

Certifikační politika

Podle § 2 odst. 2 vyhlášky č. 366/2001 Sb. Obsahem certifikační politiky je zejména:

- stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.
- 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 nim 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. [6],

Certificate revocation list (CRL)

Anglický výraz se překládá jako seznam zneplatněných (odvolaných) certifikátů. CRL vydává poskytovatel v pravidelných, předem stanovených intervalech. Každý zneplatněný certifikát je v CRL identifikován svým unikátním číslem, které je certifikátu přiděleno při jeho vydání a které je jedinečné u daného poskytovatele. Každý vydaný CRL obsahuje přesný časový údaj svého vydání a je podepsán elektronickým podpisem poskytovatele. Je veřejně přístupný, zpravidla na webových stránkách poskytovatele.

Časové razítko

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

Datová zpráva

Podle § 2 zákona o elektronickém podpisu :

„Datovou zprávou se rozumí elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou.“ [4]

Podepisující osoba

Fyzická osoba, která má prostředek pro vytváření elektronického podpisu a data pro vytváření elektronického podpisu a která jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby.

Osoba spoléhající na podpis

Zpravidla to bývá příjemce elektronicky podepsané zprávy. Může se však jednat i o osobu, která není přímým příjemcem zprávy, ale s elektronicky podepsanou zprávou pracuje a potřebuje se na podpis spoléhat (např. správce daně, auditor, soud apod.). Osoba spoléhající na podpis může využít skutečnosti, že většina běžně užívaných aplikací zasílá certifikát zároveň s elektronicky podepsanou zprávou. Pokud tomu tak není, musí podepisující osoba oznámit, kde je její certifikát dostupný, nebo musí být z použitého systému (nebo protokolu) zřejmé, kde se úložiště takovéhoto certifikátu nachází. Účelem je důvěryhodným způsobem předat data pro ověřování elektronického podpisu podepisující osoby a identifikovat ji.

2 TECHNOLOGICKÉ ASPEKTY ELEKTRONICKÉHO PODPISU

Jestliže,chceme správně pochopit princip elektronického podpisu resp. digitálního podpisu, rozdíl vysvětlen dále) je nezbytné seznámit se ze základy technologií šifrování , kterými se zabývá kryptografie.

2.1 Kryptografie

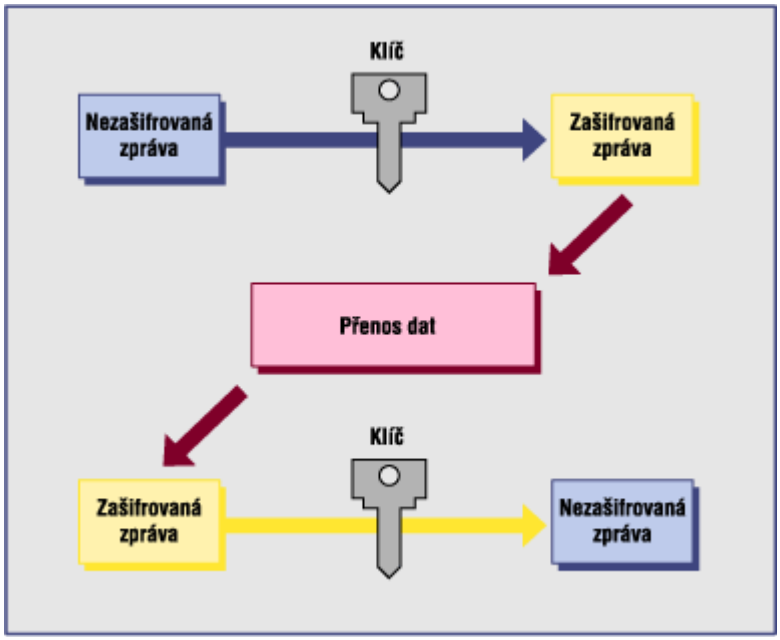
Kryptografie zahrnuje utajení zpráv a autentizaci. Základním prostředkem utajení zpráv je jejich šifrování. Šifrování spočívá v převedení zprávy (otevřeného textu) do jedné z astronomického počtu reprezentací (šifrového textu). Cílem šifrování je skrýt obsah zprávy před každým komu tato zpráva není určena. Konkrétní šifrový text je určen klíčem. Původní vysílanou zprávu nazýváme otevřeným textem. Tato zpráva je následně šifrována pomocí kryptografického algoritmu.Zašifrované zprávě říkáme šifrový text. Dešifrování je opačný postup vzhledem k šifrování, je to převedení šifrového textu zpět do podoby otevřeného textu. Všechny moderní algoritmy používají klíč, který kontroluje proces šifrování a dešifrování. Zprávu lze dešifrovat pouze tehdy, jestliže klíč použitý při dešifrování odpovídá klíči použitému při šifrování. Klíč použitý pro šifrování a klíč použitý pro dešifrování se nemusí přitom shodovat.

Moderní kryptografie však zahrnuje podstatně více než jen metody vedoucí ke skrytí obsahu zpráv. Autentizace je velmi potřebnou součástí dnešního života. Potřebujeme potvrdit, že druhým účastníkem komunikace, transakce jsme právě my a nikdo jiný. Účinné prostředky v tomto směru jsou vytvářeny právě na bázi kryptografických mechanizmů a digitální podpis je jednou z nejznámějších takových technik.

2.2 Metody šifrování

2.2.1 Symetrické šifrování

Pro zašifrování i pro dešifrování dat se používá jeden šifrovací klíč. Znamená to, že stejný klíč, který byl užit k zašifrování zprávy na straně odesilatele bude užit i na straně příjemce pro dešifrování zprávy. Z toho vyplývá nutnost před začátkem komunikace předat důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (konkrétní typ algoritmu) druhé straně.



Obr. č. 2 - Šifrování zpráv symetrickou šifrou.

Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy (např. DES, 3DES, IDEA, BlowFish a CAST.) téměř v reálnem čase. Na druhé straně i nejmodernější výpočetní technika je schopna dešifrovat data bez znalosti příslušných klíčů jen za relativně dlouhé časové období a s velkými finančními náklady. Při použití klíče s délkou 40 bitů je možné zdolat šifru za pomocí paralelního algoritmu s použitím 1200 propojených počítačů za necelé 4 hodiny. Doba rozkódování z délkou klíče roste velmi rychle (128 bitů – 1000 počítačů a 3.10 exp 22 let). USA, které jsou na špičce v šifrovacích technologiích většinu algoritmů a technologií patentovala, a tím omezují vývoz. Nakolik je doba nutná ke zdolání šifry dostačující je dáno individuálními podmínkami uživatele.

Použití symetrických algoritmů představuje způsob, jak zabezpečit důvěrnost transakcí definovaným způsobem s možností přesného stanovení hrozeb, kterým toto zabezpečení odolává.Tyto algoritmy však neřeší důležitý požadavek neodmítnutelnosti odpovědnosti. Nelze totiž určit, která strana zprávu odeslala a která přijala. [8]

Výhody a nevýhody symetrické kryptografie

Výhodou symetrických metod je jejich rychlost. Dají se velmi dobře využít pro šifrování dat, která se nikam neposílají (zašifrují se dokumenty na počítači, aby je nikdo nemohl číst). Největší nevýhodou je, že pokud chceme s někým tajně komunikovat, musíme si předem bezpečným kanálem předat klíč. To někdy muže být ona slabina tohoto šifrování.

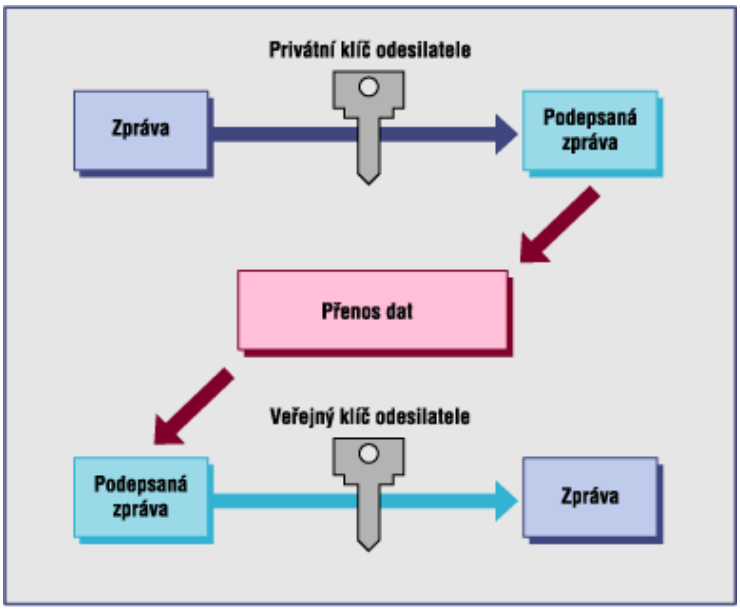
Druhá nevýhoda je počet klíčů. Chceme-li zajistit, aby spolu mohly tajně komunikovat dvě osoby, je zapotřebí jednoho klíče. Pro tři osoby jsou to již tři klíče, pro čtyři osoby šest klíčů, obecně pak:

$$\text{počet klíčů} = n*(n-1)/2 ,$$

kde n je počet osob [9]. Při vyšším poctu osob tak začíná být správa klíčů problémem.

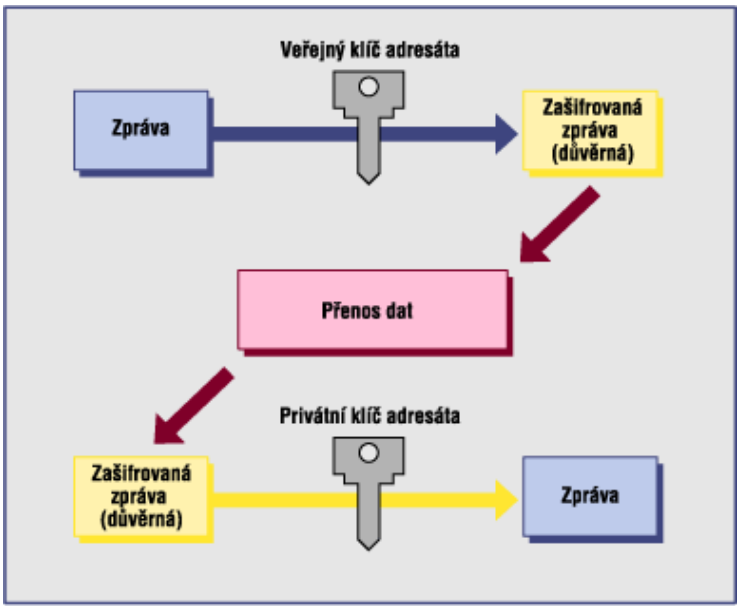
2.2.2 Asymetrické šifrování

Oproti symetrické kryptografii se zde užívá dvojice klíčů. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných SW produktů (např. SSL) a stává se tak jejich jediným majitelem. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Jeden z nich, takzvaný privátní klíč je s maximální bezpečností ukrýván majitelem (čipové karty, disketa v trezoru, ...), zatímco druhý klíč je zveřejněn. Známe-li tedy vlastníka veřejného klíče, kterým jsme zprávu dešifrovali, známe odesilatele. Protože je veřejný klíč obecně znám všem, nelze zprávu zašifrovanou podle výše popsaného postupu považovat za zašifrovanou v plném smyslu slova (důvěrnou), ale pouze za podepsanou. [8]



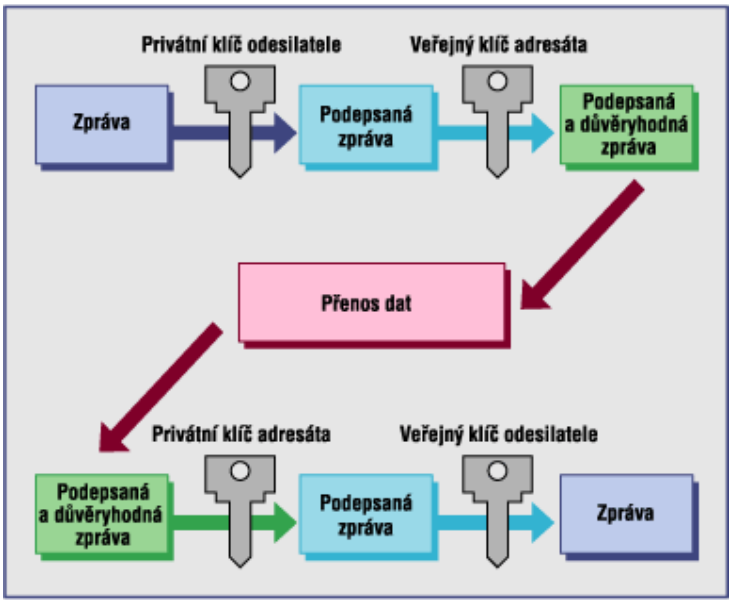
Obr. č. 3 - Přenos neadresované, nezašifrované (veřejné), ale podepsané (autorizované) zprávy

Tímto způsobem lze za pomocí asymetrické kryptografie řešit integritu dat a neodmítnutelnost odpovědnosti na straně odesilatele. Jestliže příjemce pošle podepsané potvrzení o přijetí zprávy, je zajištěna neodmítnutelnost odpovědnosti i ze strany příjemce. Není tak ovšem vyřešena otázka důvěryhodnosti zpráv, tedy nečitelnosti pro neautorizované subjekty. K tomu lze využít šifrování zpráv pomocí veřejného klíče adresáta. Při zašifrování zprávy tímto klíčem máme jistotu, že ji přečte pouze adresát se svým privátním klíčem. Situace je znázorněna na obrázku č.4.



Obr. č. 4 - Přenos adresované, zašifrované (důvěrné), ale nepodepsané (neautorizované) zprávy

Celý systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie pracuje tedy následujícím způsobem. Zpráva je obvykle na straně odesilatele nejprve podepsána, podepsán je čitelný text zprávy, a potom šifrována. Na straně příjemce je zpráva nejprve dešifrována privátním klíčem příjemce, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče ověřena identifikace odesilatele. Situaci zobrazuje obrázek č. 5



Obr. č. 5 - Přenos adresované, zašifrované (důvěrné) a podepsané (autorizované) zprávy.

Výhody a nevýhody asymetrické kryptografie

Hlavní výhodou je to, že není třeba nikam posílat soukromý klíč a tak nemůže dojít k jeho vyzrazení. Naproti tomu veřejný klíč je možné dát k dispozici všem. Je třeba méně klíčů než u symetrických metod – pro komunikaci třeba i několika osob postačí pro každou osobu jen jeden pár klíčů. Nevýhodou asymetrických metod je však rychlost. Tyto metody jsou až 1000 x pomalejší než metody symetrické. Další nevýhodou je nutnost ověření pravosti klíče, tj. stoprocentní identifikace majitele veřejného klíče. Pro tyto účely existují již zmiňované certifikační autority, které zjednodušeně řečeno udržují databázi osob s ověřenou totožností a jejich veřejných klíčů. [9].

2.2.3 Šifrovací algoritmy

Asymetrický algoritmus pro podpis je společně s daty pro vytváření elektronického podpisu (soukromý klíč) aplikován na otisk dokumentu, který má být podepsán, čímž se vytvoří podpis dokumentu. Společně s daty pro ověřování elektronického podpisu (veřejný klíč) je pak algoritmus použit pro ověření podpisu.

Vyhláška [5] schvaluje použití následujících asymetrických algoritmů:

- RSA
- DSA

RSA

Patří mezi nejznámější algoritmy pro výměnu klíčů a tvorbu elektronického podpisu . Jedná se o patentovanou (US Patent 4,405,829, 20.9.1983 vlastníkem je Public Key Partners (PKP),of Sunnyvale, California; patent vypršel v roce 2000. Na základě využívání RSA vznikla i známá americká společnost RSA Data Security Inc. Bezpečnost RSA je založena na skutečnosti, že je obtížné rozložit velká čísla (z nichž každé je součinem dvou velkých prvočísel), závisí tedy na možnostech řešit úlohu faktorizace. [10]

Popíšeme stručně vlastní algoritmus:

Celý algoritmus je tedy založen na obtížnosti faktorizace velkých čísel. Oba klíče se odvozují jako součin dvou velkých (100-200 místných) prvočísel.

$n = p.q$

Poté se zvolí šifrovací klíč e tak, aby čísla e a $(p-1).(q-1)$ byla čísla nesoudělná. A pomocí Eulerova rozšířeného algoritmu vypočteme dešifrovací klíč d, pro který platí.

$e.d = 1(mod(p-1)(q-1))$

V tuto chvíli již čísla p a q pro další postup nepotřebujeme. Přesto je nikdy nesmíme prozradit,neb tím bychom oslabili bezpečnost algoritmu. V tuto chvíli musíme rozdělit zprávu na bloky, které budou kratší než-li n (pokud p a q jsou 100 místná čísla, n bude 200 místné, měly by části zprávy být kratší než-li 200. A teď můžeme za pomoci tohoto algoritmu šifrovat a dešifrovat.

Šifrování: $c = m^e.mod\ n$

Dešifrování: $m = c^d.mod\ n$ [11]

Tím máme celý algoritmus popsán. Algoritmus RSA lze snadnou využít pro digitální podepisování. Princip jeho použití je pak opačný, než-li při šifrování. Účastník přidá ke zprávě identifikační číslo, které vytvořil „dešifrováním“ hashe své zprávy pomocí svého

soukromého klíče. Pro ověření pak stačí pouze znovu zašifrovat daný identifikátor pomocí veřejného klíče a výsledky porovnat. Pokud vyjde stejná hodnota, dokument byl opravdu podepsán dotyčným. RSA v současnosti představuje celosvětovou normu, kterou formuluje i ISO 9796.

DSA

DSS značí Digital Signature Standard, který specifikuje Digital Signature Algorithm (DSA). Byl vybrán NIST (ve spolupráci s NSA) jako vládní norma pro digitální autentizaci. Tato norma (FIPS – 186) původně obsahovala jediný algoritmus, který je založen na problému diskrétního logaritmu a je odvozen ze systému, který původně navrhli Schnorr a ElGamal. [10]

Jak algoritmus funguje:

Mějme čísla P, Q, G, X, Y, K, M, R, S, M', R', S' která splňují:

- P je prvočíslo, Q dělí (P-1) a je také prvočíslo, - G=H^((P-1)/Q) mod P, kde H je libovolné celé číslo, pro které platí (1<H<P-1) a H^((P-1)/Q) mod P > 1, - X je náhodné vygenerované a platí, že (0<X<Q), X=G^X mód P, - K je náhodně vygenerované a platí, že (0<K<Q)).

Pak veřejným klíčem je sada čísel [P, Q, G, Y] , přičemž P, Q a G mohou být sdíleny skupinou uživatelů, soukromým klíčem číslo [X]. Původní zprávou je číslo M, digitálním podpisem dvojice (R, S), ověřovanou zprávou číslo M' a ověřovaným digitálním podpisem dvojice (R', S').

Digitální podpis (R, S) vytvoříme pomocí vzorců R=(G^K mód P) mod Q, S=((Sha(M)+X*R)/K) mod Q, přičemž Sha() je funkce, která vrací výsledek algoritmu SHA-1 (což je 160ti bitový řetězec) převedený na celé číslo. Pokud se při výpočtu stane, že R nebo S bude rovno nule, vygenerujeme nové číslo K a celý postup opakujeme.

Ověření digitálního podpisu provedeme následovně. Nejdříve zjistíme zda platí dvě podmínky: (0<R'<Q) a (0<S'<Q). Pokud neplatí, podpis není platný. Pokud ano, pokračujeme dále. Dejme W=(1/S') mod Q, U1=(Sha(M')*W) mod Q, U2=(R'*W) mod Q a V=((G^U1*Y^U2) mod P) mod Q.

Jestliže pak platí, že R' = V, pak je možné prohlásit podpis i zprávu za autentické. [9]

2.2.4. Hashovací funkce

Vzorkovací, neboli hashovací, funkce jsou velmi důležité pro kryptografii a tvorbu digitálních podpisů. 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 Je to 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.

K zaručení bezpečnosti elektronického podpisu musí být použita bezkolizní hashovací funkce, tzn. musí být prakticky nemožné najít dva různé dokumenty se stejným otiskem. Vyhláška [5] v současné době schvaluje použití těchto hashovacích funkcí:

- MD5
- SHA-1
- RIPEMD-160

MD5: Algoritmus MD5 vyvinula společnost RSA Data Security Inc. Lze ho použít k vytvoření hashe v délce 128 bitů ze zprávy libovolné délky. Je považován za dostatečně bezpečný algoritmus a je široce používán.

SHA-1: SHA-1 (Secure hash algoritnm) je hashovaní funkce odpovídající normě FIPS PUB 180-1.Vytvoří 160 bitů dlouhý kontrolní hash. Algoritmus byl vyvinut NIST jako součást SHS (Secure Hash Standard). Algoritmus je zhruba o 2ᵭ pomalejší než MD5 (je však svým způsobem bezpečnější, poskytuje delší hodnotu hashe – 160.

RIPEMD-160: Vytváří hash v délce 160 bitů. Byl vyvinut v rámci evropského projektu RIPE. Byl navržen s cílem nahradit MD5. [10]

3 LEGISLATIVNÍ RÁMEC ELEKTRONICKÉHO PODPISU

3.1 Legislativa v EU

Evropský parlament a Rada Evropské unie schválily 13.12.1999 Směrnici 1999/93/EC pro elektronické podpisy v rámci společenství s cílem usnadnit používání elektronických podpisů a přispět k jejich právnímu uznání v prostředí členských států EU. Na jejím základě byl ustanoven Výbor pro elektronický podpis, který byl pověřen vypracováním podrobných technických požadavků na prostředky pro vytváření elektronických podpisů, kvalifikované certifikáty poskytovatele certifikačních služeb. Koordinací přípravy standardů se zabývá iniciativa EESSI (European Electronic Signature Standardization Initiative), která rozdělila úkoly mezi dvanáct pracovních skupin. Vlastní vydávání technických standardů pak zajišťují normalizační instituce ETSI (Electronic Signatures and Infrastructures) a CEN/ISSS [13].

3.2 Legislativa v ČR

Zákon o elektronickém podpisu vstoupil v platnost 1. října roku 2000 pod názvem Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Tímto zákonem mělo dojít k zrovnoprávnění dokumentů v elektronické podobě s dosavadními klasickými dokumenty v listinné podobě.

Následovalo vydání nařízení vlády č. 304/2001 ze dne 25.7.2001, kterým se zmiňovaný zákon provádí. To stanovilo povinnost orgánů veřejné moci zřídit elektronické podatelny a zajistit jejich provoz. Těmito opatřeními by měla být zabezpečena činnost elektronických podatelen v rámci orgánů veřejné moci tak, aby bylo zajištěno přijímání podání v elektronické podobě při využití kvalifikovaných certifikátů dle zákona o elektronickém podpisu.

Zákon o elektronickém podpisu předpokládal, že Úřad pro ochranu osobních údajů (ÚOOU) vydá potřebnou prováděcí vyhlášku, ale tvůrci zákona pozapomněli na skutečnost, že ÚOOU nebyl zmocněn pro vydávání prováděcích právních předpisů. Proto byla iniciována novela zákona o ochraně osobních údajů, jejíž součástí bylo ustanovení, které obsahuje zmocnění pro ÚOOU vydat vyhlášku k provedení zákona o elektronickém podpisu. Toto ustanovení však nabylo účinnosti až dnem 31. května 2001, kdy teprve mohl Úřad pro ochranu osobních údajů oficiálně předložit návrh vyhlášky, jejímž

cílem bylo upřesnit podmínky stanovené v § 6 a 17 zákona o elektronickém podpisu. Po rozsáhlém připomínkovém řízení byla 10. října 2001 vyhláška publikována ve Sbírce zákonů pod č. 366/2001 Sb. jako vyhláška o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu. Je určena především poskytovatelům certifikačních služeb a upřesňuje požadavky na ty poskytovatele, kteří hodlají vydávat kvalifikované certifikáty, upřesňuje postup akreditace těch poskytovatelů certifikačních služeb, kteří zažádali ÚOOÚ o akreditaci a dále upřesňuje požadavky na nástroje elektronického podpisu.

9.5 května 2002 proběhla malá novelizace zákona o elektronického podpisu zákon č.226/2002 Sb. Změna § 11 zákona o elektronického podpisu upřesňující podmínky používání elektronického podpisu a certifikátů v oblasti orgánů veřejné moci.

14. listopadu 2002 byla zákonem č.517/2002 provedena úprava zákona o elektronického podpisu na základě provedení některých opatření v soustavě ústředních orgánů státní správy, nahrazení slova "Úřad pro ochranu osobních údajů" a "Úřad" slovem "Ministerstvo informatiky".

24. června 2004 schválila Poslanecká sněmovna Parlamentu ČR zatím jednoznačně nejrozsáhlejší novelu zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů pod označením Zákon č.486/2004 Sb. (227/2000 Sb.), Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn.

25.srpna 2004 vydáno nařízení vlády č. 495/2004 Sb., které stanovuje povinnost orgánů veřejné moci zřídit elektronické podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu), vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací. Toto nařízení nabylo účinnosti k 1. lednu 2005.

1. ledna 2005 vstoupila v platnost vyhláška č. 496/2004 Sb. o elektronických podatelnách, která upravuje postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny. Tato vyhláška navazuje na nařízení vlády č. 495/2004 Sb., k elektronickým podatelnám, které nařizuje orgánům veřejné moci elektronickou podatelnu zřídit a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády.

3.2.1 Zákon č. 227/2000 Sb. o elektronickém podpisu

Zákon v § 2 definuje některé pojmy. 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 umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě,
- zaručeným elektronickým podpisem elektronický podpis,který splňuje následující požadavky: 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,
- datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích používaných při zpracování a přenosu dat elektronickou formou,
- certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její identitu.
- kvalifikovaným certifikátem certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty,
- poskytovatelem certifikačních služeb subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. [14]

Zákon dále definuje práva a povinnosti všech subjektů, účastnících se v nějaké roli systému elektronického podepisování.

V § 5 jsou definovány povinnosti podepisující osoby. V lit.[14] se uvádí „ Podepisující osoba je povinna zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití, dále neprodleně uvědomit poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu a podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.“

§ 6 tohoto zákona jsou definuje povinnosti poskytovatele certifikačních služeb a akreditovaného poskytovatele certifikačních služeb – jedná se o poskytovatele certifikačních služeb, jemuž byla udělena akreditace podle § 10 ZoEP, jenž jej opravňuje k poskytování služeb v oblasti orgánů veřejné moci. V soukromoprávní oblasti, například při komunikaci komerčních bank s jejich klienty, dvou firem apod., Je na komunikujících subjektech, zda budou vyžadovat používání kvalifikovaných certifikátů ve smyslu zákona. Toto rozhodnutí je zcela na jejich smluvním ujednání. Zákon akreditovanému poskytovateli ukládá mnoho povinností, protože tento subjekt je klíčovým v systému elektronického podepisování a jeho selhání by mělo dalekosáhlé důsledky včetně likvidace celého systému. § 6 dále podrobně upravuje Vyhláška ÚOOU č. 366/2001 Sb.

K zaručení vysoké důvěryhodnosti v oblasti elektronické komunikace je do zákona začleněn § 11, který říká, že v oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

V § 17 jsou specifikovány prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů. Prostředek pro bezpečné vytváření podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že

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

- 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,
- data pro vytváření podpisu mohou být podepisující osobou spolehlivě
- chráněna proti zneužití třetí osobou.

Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících Technických a programových prostředků a postupů minimálně zajistit, aby data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,

- podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,
- ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,
- pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,
- výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,
- bylo jasně uvedeno použití pseudonymu,
- bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§ 17 je stejně jako § 6 podrobně upraven Vyhláškou ÚOOU č. 366/2001 Sb.

3.2.2 Nařízení vlády č. 304/2001, kterým se provádí zákon č. 227/2000 Sb.

Podle nařízení vlády, vydaného k provedení zákona o elektronickém podpisu, musí orgány veřejné moci zřídit jednu nebo více elektronických podatelen. Jejich úkolem je především přijímání a potvrzování přijetí podání a příprava na jejich následné zpracování. Podatelny, které zpracovávají podání podle zákona o správě daní a poplatků, musí též zajišťovat doručování písemností na e-mailovou adresu žadatele. Pro snazší představu jak taková podatelna vypadá, je dobré říci, že je to jedna, nebo více adres pro elektronickou poštu, kterou obsluhují zaměstnanci určité instituce. Takovýto zaměstnanec musí mít vlastní kvalifikovaný certifikát pro zaručený elektronický podpis, kterým jménem státní instituce podepisuje odchozí poštu. Certifikát obsahuje mimo jiné, i označení (název) orgánu veřejné moci, jeho organizačního útvaru a funkce zaměstnance.

Součástí činností podatelny musí být především kontrola čitelnosti podání (tj. zda je zpráva v některém z akceptovatelných formátů - povinně .txt nebo .htm a volitelně další jako.rtf, .pdf, .doc apod. a zda neobsahuje viry, červy, trojské koně apod.). Dále zda kvalifikovaný certifikát žadatele je platný a zda jej vydal akreditovaný poskytovatel. Pokud podání nebude mít tyto náležitosti, musí orgán veřejné moci postupovat podle předpisů upravujících odstraňování vad podání.

Elektronická adresa podatelny musí být ve formátu posta@<doména orgánu>.cz podle standardu ISVS č. 002/01.03. Příjem a odesílání elektronických zpráv musí podporovat minimálně protokoly SMTP a POP3 a kódování zpráv ve formátu MIME a S/MIME. Ostatní technické a programové vybavení musí odpovídat standardům ISVS vydaným ve Věstníku ÚVIS.

Pro zavádění a provoz podatelny je nutné zpracovat bezpečnostní projekt podle standardu ISVS 005/01.01. Jeho součástí je definování požadavků na personální a fyzickou bezpečnost, režimové zabezpečení a bezpečnost IS. Technické vybavení podatelny musí mít atest na shodu s technickými požadavky Standardu ISVS 016/01.01.

[15], [16]

3.2.3 Vyhláška ÚOOU č.366/2001 Sb.

Požadavky uvedené v § 6 a 17 zákona č. 227/2000 Sb. jsou příliš obecné, a proto je upřesňuje tato prováděcí vyhláška.Jsou zde konkretizovány alespoň některé z požadavků na prostředky pro bezpečné vytváření a ověřování elektronického podpisu, např. je vyžadováno, aby podepisující osoba byla informována o tom, že používá tento prostředek a musela před jeho použitím zadat přístupové heslo nebo použít jiný obdobný autentizační mechanismus. Upřesněny jsou i požadavky na kryptografické algoritmy a jejich parametry. V příloze č. 2 této vyhlášky a zároveň v příloze P2 této diplomové práce jsou 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 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. 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 bez-pečné vytváření a ověřování elektronických podpisů.

Nástroj elektronického podpisu je prostředek pro vytváření elektronického podpisu, který lze používat k podepisování kvalifikovaných certifikátů a seznamu certifikátů, které byly zneplatněny. Poskytovatelé certifikačních služeb, kteří vydávají kvalifikované certifikáty, musí takovýto nástroj používat.

V § 3 této vyhlášky je uvedeno, že poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje svým zaručeným elektronickým podpisem kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Nástroj elektronického podpisu používaný pro toto podepisování nelze z důvodů vyšší bezpečnosti použít pro jiné než tyto účely.

Úřad pro ochranu osobních údajů vyhodnocuje na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

Pokud nástroj elektronického podpisu splnil požadavky stanovené zákonem o elektronickém podpisu a úřad vyslovil shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, zveřejňuje úřad ve Věstníku a na svých webových stránkách. [5]

3.2.4 Zákon č.486/2004 Sb. (227/2000 Sb.)

Zákon č. 227/2000 Sb. reaguje na výtky, které byly odbornou veřejností sdělovány již od samého počátku existence zákona o elektronickém podpisu. I vláda si všimla určitých problémů a proto v dokumentu „Bílá kniha elektronického obchodu“ identifikovala následující problémové okruhy:

- absenci kompatibility zákona s právem ES,
- absenci tzv. časových razítek v zákoně,

- možnost používání zahraničních certifikátů v režimu našeho zákona (stávající zákon obsahuje totiž stále požadavek, aby byl kvalifikovaný certifikát vydán v ČR),
- problematiku elektronického „podepisování“ zpráv, tj. bez přímé účasti člověka.

Právě tyto problémy by měla novela vyřešit. Došlo i k drobným kosmetickým úpravám, takže„zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb“ je od této chvíle nazýván zkráceně „uznávaný elektronický podpis“.„Poskytoval certifikačních služeb vydávající kvalifikované certifikáty" je nazýván „kvalifikovaný poskytoval certifikačních služeb".

Novela zákona o elektronickém podpisu přináší několik úplně nových prvků .

Časová razítka

V lit. [4] § 2 písm.r) je definuje takto: „kvalifikovaným časovým razítkem je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.“

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.

Elektronická značka a systémový certifikát

Zatímco e-podpis je určen pro fyzickou osobu, která přímo osobně podepisuje daný dokument,elektronickou značku může používat fyzická i právnická osoba a také organizační složka státu (například ministerstvo) pro automatické bezpečné hromadné označování

dokumentů. V praxi lze předpokládat řadu využití, například pro automatické (bezpečné) odpovědi podatelny, podepisování elektronických výpisů a další - tedy všude tam, kde se hodí mít jednoznačně prokazatelnou autenticitu zdroje, ovšem vzhledem k objemům podpisů to nebylo možné delegovat na fyzické pracovníky. [17]

Elektronickou značkou se tedy, zjednodušeně řečeno, rozumí elektronický podpis provedený automatem. Systémový certifikát pak je analogicky certifikát dokládající identitu „označující osoby", která automat ovládá. Orgány veřejné moci mohou použít pouze kvalifikované systémové certifikáty (se zákonem určeným obsahem) od akreditované (pro stát důvěryhodné) CA. Systémový certifikát by se neměl zaměňovat s tzv. serverovým certifikátem, užívaným a známým z běžných webových serverů pro relaci SSL. Systémový certifikát totiž dosvědčuje identitu označujícího pro formu e-označení (tj. e-podpisu), zatímco serverový certifikát se používá pro šifrování obsahu popř. šifrovanou výměnu klíčů

Elektronické podatelny

Tento pojem, který se poprvé objevil i v samotném zákoně o elektronickém podpisu, stanoví, že přes elektronickou podatelnu musí orgány veřejné moci posílat veškeré své zprávy podepsané uznávaným podpisem.

Toto je blíže upraveno vyhláškou č. 496/2004 Sb. o elektronických podatelnách.

Zahraniční certifikáty

Novela plní zadání vlády i v oblasti "rozšíření" elektronického podpisu přes národní hranice, a to

- směrem "ven", odstraněním požadavku, aby kvalifikovaný certifikát byl vydán v České republice,
- směrem "dovnitř", konstatováním, že "certifikát vydaný v jiném členském státu EU jako kvalifikovaný je kvalifikovaným certifikátem ve smyslu navrhovaného zákona", a dále zavedením možnosti získat akreditaci poskytovatele certifikačních služeb i pro poskytovatelské subjekty, které nemají sídlo v ČR. [18],[4]

3.2.5 Vyhláška č. 496/2004 Sb. o elektronických podatelnách

Tato vyhláška stanovuje postupy orgánů veřejné moci, uplatňované při přijímání pro-střednictví elektronické podatelny a odesílání datových zpráv prostřednictvím a strukturu údajů kvalifikovaného certifikátu, na základě, kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat.

Především upravuje případy, kdy je zpráva přijata, kam se ukládá a jakým způsobem se eviduje, jak se potvrzuje doručení datové zprávy. Dále definuje povinnosti při odesílání datových zpráv (místo úložiště, antivirová kontrola). Údaj, na jehož základě je možné osobu jednoznačně identifikovat, se uvádí ve struktuře desetimístného čísla v desítkové soustavě v rozsahu 1 100 100 100 až 4 294 967 295 a je spravován ústředním orgánem státní správy. Jeho hodnota není zaměnitelná s rodným číslem a nesmí být osobním údajem podle zvláštního právního předpisu [19]

3.2.6 Nařízení vlády č. 495/2004, kterým se provádí zákon č.227/200 Sb.

Provozování elektronické podatelny se považuje za splněné rovněž v případě, kdy orgán veřejné moci dohodne s jiným orgánem veřejné moci, že bude přijímat a odesílat datové zprávy prostřednictvím jím provozované elektronické podatelny. Dále je nutné, aby provozovatel vybavil zaměstnance, kteří jsou oprávněni činit právní úkony v oblasti orgánů veřejné moci, kvalifikovanými certifikáty vydanými akreditovanými poskytovateli certifikačních služeb. Orgán veřejné moci musí zveřejnit na své úřední desce, pokud ji má zřízenu, a též způsobem umožňujícím dálkový přístup, informace potřebné k doručování datových zpráv orgánu veřejné moci. Těmito informacemi jsou alespoň:

- elektronická adresa elektronické podatelny a údaj o tom, zda je určena pro příjem všech datových zpráv nebo pouze datových zpráv určitého, předem stanoveného obsahu,
- kontaktní údaje pro přijímání datových zpráv na technických nosičích,
- pravidla potvrzování doručení datových zpráv podle zvláštního právního předpisu včetně vzoru datové zprávy, kterou se doručení potvrzuje,

- technické parametry datových zpráv, pro jejichž přijetí má elektronická podatelna technické a programové vybavení,
- postup orgánu veřejné moci v případě, že u přijaté datové zprávy je zjištěn výskyt počítačového viru
- způsob vyřizování dotazů týkajících se provozu elektronické podatelny,
- aktuální seznam zaměstnanců s uvedením příjmení, jména.

3.2.7 Zákon 81/2006 sb. kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Novela zákona o informačních systémech veřejné zprávy doplňuje pravidla pro elektronickou komunikaci s veřejnou správou, ukládá povinnosti veřejné zprávě ve vztahu k tělesně postiženým a rozšiřuje okruh míst, která jsou oprávněná k vydávání ověřených výpisů z úředních rejstříků a databází. Rozšiřuje povinné atestování informačních systémů používaných veřejnou zprávou.

Z pohledu této práce je podstatná část novely, která označuje Portál veřejné zprávy za elektronickou podatelnu státu, jedno přístupové místo, přes které je možné komunikovat s celou veřejnou správou. Novela umožňuje, aby elektronické podání , zpráva podepsaná zaručeným elektronickým podpisem, odeslané na adresu www.portal.gov. cz mohlo být považováno za úřadům doručené.

Tato zněna v zákoně je prostředkem k rozvoji rychlé a pro firmy a úřady méně nákladné komunikace se státem.

4 TYPY ELEKTRONICKÝCH PODPISŮ

Velmi často se stává, že lidé používají termíny elektronický nebo digitální podpis, kvalifikovaný podpis atd., přičemž si nepřesně uvědomují jejich pravý význam, v čem spočívají jejich odlišnosti a specifika. S využitím lit. [01] v této kapitole popíši jednotlivé typy a odlišnosti mezi nimi. Rozdíly mezi jednotlivými typy budou velmi zřejmé z tabulek, které doprovázejí jejich charakteristiku a které jsou sestaveny podle níže specifikovaných kritérií.

Typů elektronických podpisů je celá řada, přičemž jednotlivé druhy podpisu se v zásadě liší mírou, v níž naplňují požadavky na elektronický podpis kladené a kritéria, jimiž je elektronický podpis charakterizován. K porovnání jednotlivých typů je možno použít následující kategorie:

- politika kvalifikovaného certifikátu (zpravidla uvedena v certifikační politice),
- formát elektronického podpisu,
- formát kvalifikovaného certifikátu,
- časové razítko,
- požadavek na bezpečný systém,
- požadavek na prostředek pro bezpečné vytváření elektronického podpisu (PBVP).

Podle konkrétních požadavků na tyto kategorie pak můžeme definovat následující typy elektronických podpisů:

- elektronický podpis,
- zaručený elektronický podpis,
- zaručený elektronický podpis založený na kvalifikovaném certifikátu,
- kvalifikovaný podpis,
- vylepšený elektronický podpis,
- kvalifikovaný podpis určený pro archivaci dat.

Definicemi elektronického podpisu a požadavky na elektronický podpis kladených se zabývá celá řada dokumentů a institucí. Ze strany Evropské unie (s jejíž legislativou je legislativa České republiky uváděna v soulad) se jedná o Směrnici o elektronických

podpisech (1999/93/EC), s níž je Zákon o elektronickém podpisu (zákon č. 486/2004 Sb. (227/2000Sb.)) v souladu.

Dále se problematikou elektronického podpisu zabývá řada standardizačních organizací – např. ETSI (European Telecommunication Standards Institute), CEN/ISSS (European Committee for Standardization/Information Society Standardization SystEm). Jisté zmínky obsahuje i dokument Komise OSN UNCITRAL o elektronickém obchodu, který je však problematice poněkud méně relevantní. Podívejme se nyní na definice typů elektronického podpisu podrobněji.

4.1 Elektronický podpis

Pro definici tohoto typu vyjděme ze zákona o elektronickém podpisu § 2 [4]. Ten rozumí takovýmto podpisem „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě".

Pavel Vondruška v lit.[1] říká: „Takovýto „podpis“ nemá pro příjemce příliš velkou vypovídací hodnotu. Důvěra v takto vytvořený podpis by měla být osobou spoléhající se na podpis zcela minimální. Slouží spíše pouze pro informaci příjemce.“ Jako příklad si můžeme uvést klasický podpis pod e-mailovou zprávu nebo identifikace autora v záhlaví článku.

Požadavky na námi definované a sledované kategorie jsou tedy zcela minimální. Nepožaduje se časové razítko, není definován žádný konkrétní formát nebo standard, který by popisoval tvar vytvořených nebo předávaných dat. Není použit certifikát nebo jiný způsob zveřejnění pomocných dat (např. dat pro ověřování podpisu, osobních dat podepisující osoby, informace o systému použitém při podpisu apod.) ani tato data nejsou definována. Nejsou kladeny žádné specifické požadavky na použitý podpisový systém nebo na prostředek pro vytváření, případně pro ověřování elektronického podpisu.

Vlastnosti, které jsme si vytyčili jako požadavek na námi hledaný vhodný typ elektronického podpisu, zajišťuje teprve podpis definovaný ve stejném zákoně v § 2, písmeno b). Tento podpis se nazývá zaručený elektronický podpis.

ESSI Standard	Volba standardu		
Politika kvalifikovaného certifikátu	**Nezveřejnění nebo přímé poskytování politiky**	Zveřejnění politiky	Zveřejnění užívání PBVP
Formát elektronického podpisu	Elektronický podpis	Elektronický podpis + testování dat	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	Profil kvalifikovaného certifikátu		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	**Nižší úroveň**	Kvalifikovaná úroveň	
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Tab. č. 1 - Elektronický podpis

4.2 Zaručený elektronický podpis

Zaručeným elektronickým podpisem je elektronický podpis, který splňuje následující požadavky:

- 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.

Požadavky na tuto kategorii se vzhledem k předchozí definici mění. Stále se nevyžaduje časové razítko, nevyžaduje se použití certifikátu ke zveřejnění dat pro ověření

podpisu (veřejného klíče). Zavádí se přesné formáty pro vytváření a přenos elektronických podpisů. Základním dokumentem v této oblasti je dokument Electronic Signature Formats (ETSI TS 101 733 V1.2.2, 2000-12). Nově se zavádí požadavek na důvěryhodnost operačního systému, ve kterém se dokument podepisuje. Nejsou kladeny žádné specifické požadavky na podpisový prostředek nebo ověřovací prostředek. Bezpečnost těchto prostředků (použití, zabezpečení, ochrana) se zcela nechává na podepisující osobě (případně na osobě, která se spoléhá na podpis). [1]

EESSI Standard	Volba standardu		
Politika kvalifikovaného certifikátu	**Nezveřejnění nebo přímé poskytování politiky**	Zveřejnění politiky	Zveřejnění užívání PBVP
Formát elektronického podpisu	**Elektronický podpis**	Elektronický podpis + testování dat	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	Profil kvalifikovaného certifikátu		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň	**Kvalifikovaná úroveň**	
Požadavek na prostředek pro bezpečné vytváření	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Tab. č. 2 - Zaručený elektronický podpis

Takovýto podpis má pro příjemce vyšší vypovídací hodnotu - důvěra v takto vytvořený podpis je tedy podstatně vyšší než v případě elektronického podpisu. Slouží pro styk příjemce a odesílatele, kteří se na takovéto komunikaci předem dohodnou. Příjemce musí od podepisující se osoby získat důvěryhodným způsobem její data sloužící k ověření zaručeného elektronického podpisu (její veřejný klíč). Ani tento typ podpisu neslouží k „anonymnímu“ styku, tedy ke styku odesílatele a univerzálního příjemce (např. nákup zboží na internetu). Příkladem komunikace, ke které může být tento druh podpisu

využit, může být komunikace klient – banka či obchodník – zákazník. Umožnění této komunikace se řídí podle uzavřené smlouvy podle obchodního nebo občanského zákoníku.

4.3 Zaručený elektronický podpis založený na kvalifikovaném certifikátu

U tohoto typu elektronického podpisu se zavádějí pojmy certifikát, kvalifikovaný certifikát a pojem poskytovatel certifikačních služeb. Poskytovatelé certifikačních služeb se dělí na poskytovatele, kteří vydávají certifikáty a na poskytovatele, kteří vydávají kvalifikované certifikáty a na akreditované poskytovatele certifikačních služeb.

Definice jednotlivých pojmů jsou uvedeny v zákoně o elektronickém podpisu [03] .

Pro účely tohoto zákona se rozumí:

Certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu.

Kvalifikovaným certifikátem certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb.

Poskytovatelem certifikačních služeb fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.

Akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona, [03]

Povinnosti poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, jsou obsaženy v § 6 zákona o elektronickém podpisu a jsou dále upřesněny v prováděcí vyhlášce č.366/2001 Sb.

Požadavky na tento podpis se podle zvolených kritérií vzhledem k předchozím typům rozšiřují, ale stále ještě není vyžadováno časové razítko. V lit. [1] je uvedeno: Zpřísňují se požadavky na přesné formáty pro vytváření a přenos elektronických podpisů. Používání formátů se rozšiřuje o stanovení požadavků na formáty kvalifikovaných certifikátů a o další související formáty (např. žádost o vydání certifikátu apod.).

Požadavek na důvěryhodnost operačního systému, ve kterém se datová zpráva podepisuje, je stejný jako u předchozího typu.

EESSI Standard	Volba standardu		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	**Zveřejnění politiky**	Zveřejnění užívání PBVP
Formát elektronického podpisu	Elektronický podpis	**Elektronický podpis + testování dat**	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň	**Kvalifikovaná úroveň**	
Požadavek na prostředek pro bezpečné vytváření	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Tab. č. 3 - Zaručený elektronický podpis založený na kvalifikovaném certifikátu

Tento typ podpisu je základním typem elektronického podpisu, kterým se zákon o elektronickém podpisu zabývá. Tento podpis má pro příjemce vysokou vypovídací hodnotu. Důvěra v takto vytvořený podpis je vysoká. Důvěra je podpořena právními aspekty, které vyplývají z použití takovéhoto podpisu, a které plynou ze zákona o elektronickém podpisu. Slouží pro styk příjemce a nějakého jiného subjektu, který vlastní kvalifikovaný certifikát. Příjemce podepsanou osobu nemusí osobně znát, data pro ověření získá příjemce z kvalifikovaného certifikátu. Právní jistota v souvislosti s tímto způsobem komunikace vyplívá ze o elektronickém podpisu, nemusí tedy na rozdíl od předchozího případu uzavírat speciální smlouvy pro právní podporu této komunikace. Důvěra v obsah

certifikátu je podmíněna důvěrou v poskytovatele certifikačních služeb, který certifikát vydal. Tato důvěra vyplívá ze skutečnosti, že zákon o elektronickém podpisu stanoví poskytovatelům vydávajícím kvalifikované certifikáty celou řadu povinností. Tento typ podpisu může být použit i k „anonymnímu“ styku (místo jména podepisující osoby může být uveden pseudonym). V případě právního sporu je„anonymní“držitel certifikátu dohledán prostřednictvím údajů, které má k dispozici poskytovatel certifikačních služeb. Lze použít všude tam, kde se v českém zákoně o elektronickém podpisu umožňuje nahradit podpis elektronickým podpisem. [1]

Obecně se považuje tento typ za vhodný pro přímou komunikaci mezi subjekty. Není vhodný k archivaci dat a tam, kde je nutné zpětně prokazovat, kdy přesně byl dokument podepsán.

Novela zákona o elektronickém podpisu nezavádí pojem elektronické značky . Z techno - logického hlediska je elektronická značka stejná jako zaručený elektronický podpis, tj. jedná se o digitální podpis. Pro vlastní vytváření elektronických značek nebo pro přijímání datových zpráv jimi označených není tedy potřeba pořizovat jiný software.

Odlišnost elektronické značky a zaručeného elektronického podpisu má především právní charakter. Elektronický podpis vytváří fyzická osoba (stejně jako vlastnoruční), elektronickou značkou může datové zprávy označovat i právnická osoba nebo organizační složka státu. Lze ji přirovnat k otisku úředního razítka. Například orgány státu mohou vydávat některé listiny v elektronické podobě a označovat je elektronickou značkou.

4.4 Kvalifikovaný podpis

Požadavky na tento podpis se podle zvolených kritérií vzhledem k předchozím typům rozšiřují, ale stále ještě není vyžadováno časové razítko. V lit. [1] je uvedeno: Zpřísňují se požadavky na přesné formáty pro vytváření a přenos elektronických podpisů. Používání formátů se rozšiřuje o stanovení požadavků na formáty kvalifikovaných certifikátů a o další související formáty (např. žádost o vydání certifikátu atd.). Požadavek na důvěryhodnost operačního systému, ve kterém se datová zpráva podepisuje, je stejný jako u předchozího typu. Právě pojem bezpečného podpisového a ověřovacího prostředku (tedy SW vybavení tvořícího a ověřujícího data pro elektronický podpis) je jeden z nejproblematičtějších pojmů celého systému elektronického podepisování. Obecně lze říci, že se tyto požadavky dají rozdělit na tři oblasti : požadavky technicko -

kryptografické, požadavky na začlenění tohoto prostředku do informačního systému a legislativně právní požadavky. Nejsou uzavřeny ani otázky související s hodnocením bezpečnosti takovéhoto prostředku.

EESSI Standard	Volba standardu		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	Zveřejnění politiky	**Zveřejnění užívání PBVP**
Formát elektronického podpisu	Elektronický podpis	**Elektronický podpis + testování dat**	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň	**Kvalifikovaná úroveň**	
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	Nižší úroveň	**Kvalifikovaná úroveň**	Vyšší úroveň

Tab. č. 4 - Kvalifikovaný podpis

Kvalifikovaný podpis se považuje z hlediska důvěry za nejvhodnější. Tento typ podpisu má pro příjemce nejvyšší vypovídací hodnotu. V dokumentech EU se uvažuje, že by mohl být používán v situaci, kde se v písemné podobě vyžaduje vlastnoruční podpis [1].

4.5 „Vylepšený “ elektronický podpis

Vylepšený elektronický podpis se od předchozích typů elektronického podpisu liší přidáním některého z dalších požadavků na podpis, který není součástí zaručeného elektronického podpisu a ani nemá žádnou souvislost s předchozími typy (např. časová značka, rozšířené požadavky na verifikaci, rozšířené požadavky na podpisový prostředek, apod.).

4.6 Kvalifikovaný podpis určený pro archivaci dat

Nejdůležitějším typem, který vznikl jako vylepšený elektronický podpis z kvalifikovaného podpisu, je kvalifikovaný podpis určený pro archivaci dat.

<table>
<tr><td>EESSI Standard</td><td colspan="3">Volba standardu</td></tr>
<tr><td>Politika kvalifikovaného certifikátu</td><td>Nezveřejnění nebo přímé poskytování politiky</td><td>Zveřejnění politiky</td><td>Zveřejnění užívání PBVP</td></tr>
<tr><td>Formát elektronického podpisu</td><td>Elektronický podpis</td><td>Elektronický podpis + testování dat</td><td>Elektronický podpis + testování dat + časová razítka</td></tr>
<tr><td>Formát kvalifikovaného certifikátu</td><td colspan="3">Profil kvalifikovaného certifikátu</td></tr>
<tr><td>Časové razítko</td><td colspan="3">Použití protokolu pro časová razítka</td></tr>
<tr><td>Požadavek na bezpečný systém</td><td colspan="2">Nižší úroveň</td><td>Kvalifikovaná úroveň</td></tr>
<tr><td>Požadavek na prostředek pro bezpečné vytváření elektronického podpisu</td><td>Nižší úroveň</td><td>Kvalifikovaná úroveň</td><td>Vyšší úroveň</td></tr>
</table>

Tab. č. 5 - Kvalifikovaný podpis určený pro archivaci dat

Využití tohoto typu elektronického podpisu vzhledem k jeho specifickým požadavkům je - dlouhodobá archivace elektronicky podepsaných dokumentů v elektronické formě. Pokud tuto službu zajišťuje poskytovatel certifikačních služeb, Měl by zajistit i uchování příslušného software, který umožní otevření a zobrazení podepsaných dat i v době, kdy tento software již není běžně používán.

II. PRAKTICKÁ ČÁST

5 VYUŽITÍ ELEKRONICKÉHO PODPISU V PRAXI

Způsoby využití elektronického podpisu vyplývají z jeho vlastností: kdykoli máme nějaký text či cokoli jiného v elektronické podobě a potřebujeme to někomu poslat, předat, přenést či jinou formou zpřístupnit, můžeme to opatřit elektronickým podpisem. Příjemce pak bude mít jistotu, že to co dostal skutečně pochází od vás, že to po cestě nebylo změněno, a také to, že nebudete moci popřít, že to pochází od vás.

Elektronický podpis by měl dále umožnit bezpečnou elektronickou komunikaci například v těchto případech: komunikace uvnitř firmy, komunikace se zákazníkem, komunikaci s dalšími firmami (dodavatelé, banky atd.) a komunikaci se státními institucemi (finanční úřady, správa sociálního zabezpečení, obchodní rejstřík atd.). Až do druhé poloviny roku 2001 se ovšem elektronický podpis ve styku s úřady používat nemohl. To se stalo až po stanovení závazných pravidel prováděcím předpisem. Ani poté se ovšem nezdvihla masivní vlna používání. Klasickým příkladem využití elektronického podpisu, které je velmi často citováno v médiích, je podávání daňového přiznání v elektronické formě.

Používání elektronických dokladů by mělo přinést značné úspory nákladů na provoz a zvýšení kvality informačních systému podniků, přispět k rozvoji elektronického obchodu a zvýšit bezpečnost takovéto komunikace.

V následujícím textu jsou shrnuty některé možnosti jak využívat elektronický podpis ve státní a soukromé sféře. Pouze zopakuji, že při komunikaci s orgány veřejné správy je vyžadován zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb. Informace zde obsažené jsem převážně čerpal z webových stránek ministerstev, jednotlivých zdravotních pojišťoven a poskytovatelů certifikačních služeb.

5.1 Využití ve státní správě

5.1.1 Ministerstvo práce a sociálních věcí

Jedná se o projekt podávání žádostí o dávky sociální podpory elektronickou cestou. Žádosti je možné podat podepsané elektronicky s využitím kvalifikovaného certifikátu, který musí kromě základních vlastností obsahovat MPSV Identifikátor klienta MPSV.

Bez významový identifikátor osoby akceptovaný Ministerstvem práce a sociálních věcí). Certifikáty tohoto typu vydává v současné době akreditovaná certifikační autorita 1.CA a akreditovaná certifikační autorita PostSignum QCA České pošty, s.p. Certifikáty, které nesplňují výše uvedené požadavky nelze použít pro elektronické podepsání formuláře v této aplikaci.

Výhodou řešení pro žadatele je skutečnost, že při jakékoli elektronické komunikaci se systémem státní sociální podpory bude vždy identifikován a nebude v tomto případě nutná jeho fyzická návštěva na úřadu. Na straně úředníka státní sociální podpory je systém připraven na přijetí a ověření elektronicky podané žádosti a automatické přenesení dat z formuláře do aplikačního vybavení systému SSP.

Pomocí webových stránek ministerstva lze podat následující typy žádostí:

- žádost o přídavek na dítě,
- žádost o sociální příplatek,
- žádost o příspěvek na bydlení,
- žádost o dávku pěstounské péče – příspěvek na úhradu potřeb dítěte,
- žádost o dávku pěstounské péče – odměnu pěstouna,
- žádost o dávku pěstounské péče – příspěvek při převzetí dítěte,
- žádost o dávku pěstounské péče – příspěvek na zakoupení motorového vozidla,
- žádost o rodičovský příspěvek,
- žádost o příspěvek na školní pomůcky,
- žádost o porodné,
- žádost o pohřebné,
- hlášení změn

Nevýhodou , znepříjemňující využití elektronického podpisu je fakt, že téměř ke všem žádostem je potřeba podložit určitá potvrzení. Ty na stránkách nalezneme , ale je možné si je pouze vytisknout a osobně nebo jinou než elektronickou formou doručit. [21], [22]

5.1.2 Ministerstvo financí

Ministerstvo financí – ÚFDŘ provozuje aplikaci s názvem EPO, která v současné době umožňuje podávat na disketě nebo po Internetu níže uvedené písemnosti, jako elektronická podání pro finanční úřady:

- Daňové přiznání k dani z přidané hodnoty,
- Daňové přiznání k dani z příjmu fyzických osob,
- Daňové přiznání k dani z příjmu právnických osob,
- Daňové přiznání k dani z nemovitostí,
- Daňové přiznání k silniční dani,
- Daňové oznámení podle §34 zákona č.337/1992 Sb.- oznámení o nezdaněných vyplacených částkách fyzickým osobám,
- Daňové podání obecné písemnosti.

Program je umístěn na adrese <http://adis.mfcr.cz/adis/jepo/> a je na něj přímý odkaz z hlavní internetové stránky Ministerstva financí a České daňové správy. Program umožňuje shora uvedené písemnosti vyplnit, včetně kontroly úplnosti a věcné správnosti, případně jej načíst jako soubor XML, vytvořený v tomto nebo v jiném programu a odeslat jej. Po odeslání datové zprávy na společné technické zařízení správce daně je automatizovaně vystaveno potvrzení o přijetí podání. Uživatel má možnost ověřit si prostřednictvím aplikace stav zpracování podání.

Pro opatření podání zaručeným elektronickým podpisem lze použít kvalifikovaný certifikát, který musí obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Proto při žádosti o vystavení certifikátu je nezbytné požádat, o uvedení bezvýznamového identifikátoru vytvářeného Ministerstvem práce a sociálních věcí, který je První certifikační autoritou (I. CA) a akreditovanou certifikační autoritou PostSignum QCA České pošty, s.p na požádání při vydávání certifikátu přidělen zdarma.

Zároveň program umožňuje podávat uvedené písemnosti prostřednictvím datové zprávy neopatřené zaručeným elektronickým podpisem. Součástí takového podání datové zprávy je e-tiskopis vytisknutý na PC uživatele, který daňový subjekt podepíše a do tří dnů po

odeslání elektronického podání doručí správci daně. Výhoda tohoto postupu spočívá v tom, že bez kvalifikovaného certifikátu lze využívat všech výhod programu (zejména automatické kontroly na správnost vyplnění a nápovědy). Údaje lze rovněž vytisknout na standardní tiskopis daňového přiznání nebo vytisknout úplný opis.

Podání lze učinit všemi typy internetových prohlížečů. Server daňové správy umožňuje přijmout podepsaný XML soubor ve stanovené struktuře, vytvořený jinou aplikací z libovolného OS a prohlížeče (např.z účetních SW) prostřednictvím programového vybavení, využívajícího aplikační rozhraní pro třetí strany. [23]

5.1.3 Rejstřík trestů Praha

Novela zákona č. 126/2003 Sb., kterou se mění zákon č. 269/1994 Sb., o Rejstříku trestů, umožnila od počátku roku 2004 kromě jiného fyzickým osobám požádat o vydání výpisu z rejstříku trestů (dále jen výpis) a o nahlédnutí do opisu z rejstříku trestů (dále jen opisu) také i elektronicky. Výpis i opis podle citovaného zákona je veřejnou listinou. Oba dva zmiňované úkony lze provést na žádost fyzické osoby za podmínek připojení zaručeného elektronického podpisu a úhradě stanoveného správního poplatku na zvláštní účet Rejstříku trestů.

Za tímto účelem Rejstřík trestů počátkem roku 2004 zřídil elektronickou podatelnu, která je připravena přijímat žádosti fyzických osob o výpis a o nahlédnutí do opisu v elektronické podobě. Z důvodu chybějící právní úpravy ohledně jednoznačné identifikace osoby dle údajů uvedených v certifikátu, nebylo možné od počátku roku 2004 žádnou žádost fyzické osoby řádně přijmout a vyřídit.

Rejstřík trestů je v současné době jediný subjekt státní správy, který má zákonnou povinnost vydávat dokumenty, které obsahují citlivé osobní údaje a mají charakter veřejné listiny, a to na základě elektronicky podané žádosti. Ministerstvo práce a sociálních věcí (MPSV) a Ministerstvo financí sice využívá pro jednotnou identifikaci občanů při elektronických podáních tzv. „identifikátor klienta MPSV“. Stávající právní úprava (vyhláška č. 496/2004 Sb.) ale tento identifikátor neupravuje (přestože v návrhu vyhlášky při projednávání sněmovního tisku 507 byl identifikátor klienta MPSV uveden), služby, které uvedené resorty poskytují v elektronické podobě, nemají charakter veřejné listiny a jsou fakultativní.

Elektronická podání lze provést pouze na základě použití kvalifikovaného certifikátu. Pro elektronické podání je tedy nutno mít platný kvalifikovaný certifikát, který vystaví akreditovaný poskytovatel certifikačních služeb. Dále je nutno mít emailovou adresu, na kterou budou zaslány informace o výsledku ověření údajů žádosti a způsobu úhrady poplatku, a případně i výsledný dokument.

Elektronické podání žádostí o výpis/opis se rozlišuje v základním členění dle subjektu, který podává žádost, a to na:

- ORG - orgány veřejné moci
- OS – osoba

Každý z těchto subjektů může žádat o výpis/opis za účelem definovaným příslušným zákonem, jehož citace je zpravidla na žádosti uvedena. V důsledku toho nelze použít žádost vygenerovanou pro elektronické podání pro podání v papírové podobě. A naopak žádost pro podání v papírové podobě nelze použít pro elektronické podání.

Druhy žádostí osob :

- Výpis z RT - jedná se o výpis z rejstříku trestů
- Nahlédnutí do opisu z RT - jedná se poskytnutí opisu RT, tak jak jej dostávají orgány státní správy.
- Informace o poskytnutí výpisu/opisu z RT elektronickou cestou - poskytuje informace o tom, kdy a komu byly vydány výpisy a opisy, tuto žádost může podat fyzická osoba pouze sama na sebe.

Druhy žádostí orgánů veřejné moci :

- Výpis z RT - výpis z rejstříku trestů
- Opis z RT - opis z rejstříku trestů

[24]

5.1.4 Česká správa sociálního zabezpečení

Česká správa sociálního zabezpečení využívá portál veřejné správy. Na tomto portálu tři agendy, které převedla do elektronické podoby :

- Evidenční listy důchodového pojištění (ELDP)

- Přihlášky a odhlášky zaměstnanců k nemocenskému pojištění (PRIHL)
- Přehled o příjmech a výdajích OSVČ za rok 2006 - platné od 1. 1. 2007

Vlastní zasílání formulářů evidenčních listů důchodového pojištění (eELDP) bylo zahájeno v lednu 2005 a k 1.7.2005 byla zahájena služba přihlášek a odhlášek zaměstnanců k nemocenskému pojištění. Ke konci června 2006 prošlo transakční částí Portálu veřejné správy více než 11 mil. těchto formulářů [25].

ČSSZ preferuje podpis kvalifikovaným certifikátem. Údaje jednoznačně identifikující certifikát vystavený akreditovanou certifikační autoritou, musí být nahlášeny příslušné správě sociálního zabezpečení. Tzn. je nutno je předložit při osobní návštěvě příslušné správy sociálního zabezpečení na disketě.

Těmito údaji jsou:„sériové číslo“ a „vystavitel certifikátu“. Jedná se o řetězce znaků, které musí být poskytnuty ČSSZ naprosto nepozměněné. Rozhodující jsou i zdánlivě bezvýznamné znaky jako je např. mezera. Veřejná část certifikátu se ukládá ve formátu cer.

[25] ,[26]

5.2 Zdravotní pojišťovny

Instituce velikosti zdravotních pojišťoven si mohou dovolit zřídit elektronickou podatelnu nebo portál pro komunikaci svými smluvními partnery – zdravotnickými zařízeními a případně klienty – pojištěnci. Této možnosti využilo zatím sedm našich pojišťoven**.**

5.2.1 Všeobecná zdravotní pojišťovna

Všeobecná zdravotní pojišťovna České republiky nabízí svým pojištěncům, smluvním partnerům, zaměstnavatelům i státním institucím, vlastnícím příslušné certifikáty, zdarma přístup na svůj Portál. Jeho velkou výhodou je zjednodušení administrativy, zrychlení komunikace klientů s pojišťovnou a v neposlední míře i značná úspora času.

Portál VZP obsahuje aplikace vytvořené pro potřeby různých skupin klientů. V současné době jsou dostupné aplikace pro pojištěnce, osoby samostatně výdělečně činné (OSVČ), zaměstnavatele, smluvní zdravotnická zařízení (lékaře) a státní instituce.

Služby nabízené prostřednictvím elektronické komunikace:

Aplikace pro smluvní zdravotnická zařízení (lékaře) :

- ověření aktuální registrace pojištěnce u zdravotní pojišťovny
- ověření platnosti smlouvy s VZP ČR
- vyhledání zdravotnického zařízení ve smluvním vztahu k VZP ČR
- vyhledání informace o registraci pojištěnce u jeho ošetřujícího lékaře
- zasílání faktur za poskytnutou zdravotní péči
- předávání souborů vyúčtování zdravotní péče poskytnuté pojištěncům VZP ČR

Aplikace pro zaměstnavatele:

- zpracování hlášení a kontrolu identifikačních údajů zaměstnavatele
- zpracování a zaslání hlášení hromadného oznámení zaměstnavatele
- zaslání přehledu o platbě pojistného na zdravotní pojištění zaměstnavatele
- informování zaměstnavatele o jeho platbách pojistného
- podávat Oznámení o změnách v evidenci zaměstnavatele

Aplikace pro osoby samostatně výdělečně činným:

- zasílat Přehled o příjmech a výdajích za příslušný rok
- zasílat Vyúčtování plateb pojistného a Přehled o platbách pojistného a penále

Aplikace pro pojištěnce:

- podávat Oznámení pojištěnce
- požádat o zaslání Přehledu vykázané zdravotní péče na pojištěnce
- reklamovat Přehled vykázané zdravotní péče na pojištěnce

Aplikace pro Státním instituce:

- Hromadná oznámení instituce
- Obecné podání

Pro práci s Portálem VZP ČR je možné využít dva druhy certifikátů:

- komerční, který se k ověření totožnosti uživatele při přihlašování k Portálu a šifrování jeho spojení s Portálem (protokolem SSL) - zkráceně přístup k Portálu. Tento certifikát lze využít i pro elektronický podpis zasílaných dat (je součástí minimální konfigurace).
- kvalifikovaný, slouží pouze pro elektronický podpis podání zasílaných přes Portál VZP ČR
- zkráceně podepisování. Tento certifikát lze smluvně nahradit komerčním certifikátem.

Obecně Pojišťovna pro potřeby Portálu VZP ČR akceptuje certifikáty vydávané akreditovanými veřejnými a komerčními certifikačními autoritami (dále jen CA) ve smyslu zákona č. 227/2000 Sb. O elektronickém podpisu a certifikáty dalších certifikačních autorit, které na základě smluvních vztahů uznává jako důvěryhodné.

Konkrétně jsou v současné době akceptovány certifikáty od akreditovaných CA:

První certifikační autorita, a.s. (I.CA, komerční i kvalifikovaný)

Česká pošta, s.p. (PostSignum, komerční i kvalifikovaný)

eIdentity, a.s. (ACAeID, komerční i kvalifikovaný)

Navíc jsou akceptovány certifikáty vydávané bankovními ústavy k systémům elektronického bankovnictví:

Komerční banka, a.s. (DCS CA KB, komerční)

Česká spořitelna, a.s. (I.CA, komerční)

Československá obchodní banka, a.s. (I.CA, komerční) [27] ,[28]

5.2.2 Hutnická zaměstnanecká pojišťovna

Tato pojišťovna provozuje službu 24 online servis. Nabízí moderní služby a nástroje e-komunikace, které zajistí úsporu času, jednoduché vyřízení běžných formalit, pohodlnou komunikaci 24 hodin denně, možnost práce z pohodlí domova a vysokou bezpečnost zajištěnou využitím elektronického podpisu. Součástí balíčku služeb 24 online servis je možnost získání kvalifikovaného certifikátu za výhodnou cenu, nebo komerčního certifikátu zcela zdarma.

V rámci této služby nabízí svým klientům:

- E-přepážku - nástroj pro elektronickou komunikaci klientů s HZP
- E-podatelnu - možnost podání dokumentů elektronicky
- Získání elektronického certifikátu
- Technickou podporu uživatelů

E-přepážka

E-přepážku HZP mohou využívat všichni klienti HZP zcela zdarma. Nástroj umí vyřídit většinu běžných požadavků a administrativních úkonů bez nutnosti návštěvy přepážky HZP. Pro přístup do E-přepážku potřebuje mít elektronický certifikát (elektronický podpis). Druhou podmínkou je jednoduchá elektronická registrace a podepsání příslušné smlouvy.

E-podatelna:

Elektronická podatelna umožňuje doručování dokumentů v elektronické podobě, automatické zaknihování a zaslání informací klientům o přijetí zásilky, jednacím čísle s časem přijetí. Odesílané zprávy můžete například šifrovat nebo podepisovat kvalifikovaným certifikátem. Odešleme zprávu nebo dokument a můžeme zcela jednoduše sledovat, v jakém stavu se váš požadavek právě nachází.

Technická podpora:

Pro plátce a zdravotnická zařízení nabízí možnost vystavení kvalifikovaného nebo komerčního certifikátu přímo u klienta. Po předchozí domluvě jsou schopni prostřednictvím mobilní kanceláře vystavit certifikát, poradit s instalací certifikátu, zařídit přístup do Elektronické přepážky HZP a poradit s jejím používáním. [29]

5.2.3 Portál zdravotních pojišťoven

Portál ZP je internetovou aplikací vytvořenou pro zlepšení a zrychlení komunikace mezi pojišťovnami provozujícími tento Portál. To jsou Česká národní zdravotní pojišťovna, Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví, Revírní bratrská pokladna, zdravotní pojišťovna, Zaměstnanecká pojišťovna Škoda, Zdravotní pojišťovna Metal-Aliance a poskytovateli zdravotní péče, plátci pojistného i samotnými pojištěnci.

Portál ZP umožňuje automatizovaný přístup při výměně dat typu:

- Předávání dávek a faktur
- Hromadné oznámení zaměstnavatele
- Přehled plateb zaměstnavatele
- Elektronická podatelna.

Zásadní výhody komunikace prostřednictvím Portálu ZP spočívají v:

- Snadné, pohodlné, rychlé výměně standardních dokladů jako jsou faktury a výsledné zúčtovací zprávy
- Odstranění manipulace s disketami
- Možnost rychlé reakce na urgentní požadavky
- Snížení nákladů
- Okamžitá kontrola formální správnosti předaných dat
- Bezpečné doručení a přijetí
- Zvýšení produktivity na základě předávání dat v zabezpečené elektronické podobě.
- Offline pořízení některých standardizovaných souborů

Pokud již používám certifikát Komerční banky nebo certifikát I.CA, mohu se jeho prostřednictvím přihlásit k Portálu ZP. Pokud dosud nevlastním požadovaný certifikát, stačí opatřit si jej dle návodu uvedeného podrobně na již uvedených webových stránkách.

Pojišťovny sdružené v Portálu ZP nabízejí zdarma svým klientům a partnerům, kteří vlastní klientský certifikát služby SERVIS 24 České spořitelny přístup na svůj Portál ZP.

Společné služby Portálu ZP :

Pro zdravotnická zařízení a lékaře nabízí služby jako vyúčtování zdravotní péče, přehled odeslaných faktur, protokoly o zpracování, chybové protokoly, prohlížení plateb, čtvrtletní vyúčtování, registrace pojištěnce EU, výpis registrovaných pacientů , verifikace pojištěnce/ ověření EHIC

Pro plátce pojistného je to hromadné oznámení zaměstnavatele, přehled plateb pojistného zaměstnavatele, prohlížení evidovaných plateb, verifikace pojištěnce/ ověření EHIC, elektronická podatelna , osobní schránka

Pro pojištěnce nabízí přehled OSVČ (podání, prohlížení, opravný přehled), přehled evidovaných plateb od OBZP , verifikace pojištěnce / ověření EHIC, elektronická podatelna, osobní schránka.

Pro externí instituce to jsou žádost o součinnost (FO) ,žádost o součinnost (PO). [30]

5.3 Další příklady použití

5.3.1 Bankovní sféra

V bankovní sféře je obvyklé, že bankovní domy vydávají vlastní certifikáty, platné jen pro použití při komunikaci s touto bankou a vystupují tak jako certifikační autority. Tvůrci jiných aplikací je většinou nemohou použít proto, že veřejné klíče vydaných certifikátů ani CRL (seznam zneplatněných certifikátů) nejsou veřejně dostupné. ČSOB používá komerční certifikát I.CA , ale i o ten musíme nejdříve požádat ČSOB a až poté jej můžeme používat jako jakýkoli jiný komerční certifikát. Služby internetového bankovnictví umožňují získávat informace o účtech a provádět bankovní operace z domova či kanceláře, a to v kteroukoli denní či noční dobu nezávisle na otevírací době pobočky.

5.3.2 RM-systém

RM – Systém nabízí od roku 1999 klientům možnost obchodovat na trhu RM - S přes síť Internet v reálném čase. Této služby mohou využít zákazníci z řad fyzických i právnických osob. Podle Tržního řádu RM- S, který definuje dvě základní skupiny zákazníků, se I-Zákazník řadí mezi zákazníky zvláštní. I-Zákazník aktivací této služby získává možnosti srovnatelné s přístupem přes rychlou podatelnu na obchodním místě RM

-S z tím rozdílem, že pokyny k obchodování podává doma či ve své kanceláři. Využít lze komerční certifikát První certifikační autority. [31]

5.3.3 Elektronická komunikace

V možnostech využití EP nemůžeme vynechat i téměř implicitní funkci, a to zabezpečenou e-mailovou komunikaci. V případě, že si potřebujete s jinou osobou nebo subjektem vyměňovat tajná data a obě strany vlastní certifikát,můžete e-maily zašifrovat.Tato ochrana je zcela jistě silnější než pouhé zaheslování zasílaného souboru.. [32]

5.3.4 Šifrování

Odesílatelův osobní certifikát může také využít adresát. Použitím veřejného klíče odesílatele zašifruje zprávu či dokument, který bude moci být rozšifrován pouze za pomoci soukromého klíče původního odesílatele. Je tak zajištěno, že zaslaná zpráva bude k přečtení pouze určené osobě.

5.4 Zhodnocení využití elektronického podpisu

Aplikací využívající elektronický podpis stále přibývá. Možností využití elektronického podpisu je veliké množství a aplikací využívající elektronický podpis stále přibývá Jako hlavního tahouna bych vyděl stát. Zde v sektoru státní správy asi běžný občan využije elektronický podpis nejvíc. Zdravotnictví je natolik zmítáno vážnějšími problémy, že nelze očekávat zásadní pokrok směrem k čipovým kartám se zdravotnickou dokumentací, kterou by zřejmě používaly nejen velké nemocnice, ale i soukromí lékaři. Co se týká soukromo-právních vztahů a elektronického podpisu, zde nejsem moc optimistický. Banky, které by mohly jako jediné masově používat elektronický podpis podle zákona, daly přednost internet-bankingu a home-bankingu. Domnívám se , že do budoucna bude asi jen stát, tím největším hybatelem, který dá impuls k masovému zavádění elektronického podpisu. Ten uvažuje o čipových kartách, pro zaměstnance státní správy, které by měly sdružovat osobní průkazy, přístupové karty a prostředky pro elektronické podepisování.

6 CERTIFIKAČNÍ AUTORITY

Zákon o elektronickém podpisu [03] rozumí certifikační autoritou poskytovatele certifikačních služeb, kterým může být fyzická osoba, právnická osoba nebo organizační složka státu a který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. Kvalifikovaným poskytovatelem certifikačních služeb naproti tomu může být pouze poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty, kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů.

V ZoEP jsou definovány následující tři typy certifikačních autorit:

- poskytovatel certifikačních služeb
- poskytovatel certifikačních služeb vydávající kvalifikované certifikáty
- akreditovaný poskytovatel certifikačních služeb

V České republice působí několik poskytovatelů a je pouze na nich, zda se rozhodnou požádat ÚOOU o udělení akreditace.

Kdybychom chtěli k něčemu přirovnat činnost certifikační autority, asi nejlépe by její funkci vystihovalo přirovnání k činnosti notáře při ověřování klasického podpisu. Postup při ověřování je v obou případech podobný. Notář i CA ověří totožnost žadatele, ověří, že se osoba podepsala resp. v případě CA, že má vytvořenu dvojici klíčů k vytváření elektronického podpisu, provede záznam do knihy, resp. do databáze. Poté vydá ověření – notář razítko, kde vyplní potřebné údaje a CA vydá certifikát podepsaný soukromým klíčem CA. Odlišnost mezi notářem a CA spočívá především v tom, že zatímco notář musí ověřit každý jednotlivý podpis, CA ověřuje pouze data pro vytváření elektronického podpisu, díky kterým můžeme vytvořit libovolné množství podpisů. Z tohoto rozdílu plyne i další odlišnost. Zatímco návštěva notáře je jednorázový akt, tak mezi držitelem certifikátu a CA vzniká smluvní vztah, který je podepřen uzavřením smlouvy, která vychází především z Certifikační politiky. Na základě této smlouvy vznikají stranám práva a povinnosti, některé z nich ukládá přímo ZoEP.

Na základě takové smlouvy jsou potom poskytovány další služby jako zneplatňování certifikátů a zveřejňování jejich seznamu, vydávání následných certifikátů apod. Certifikát

tedy spojuje data pro ověřování podpisu s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují.

Povinnosti kvalifikovaných poskytovatelů certifikačních služeb vyplívají z § 6 ZoEP. Jedná se např. o:

- povinnosti zajistit, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu,
- používat bezpečné systémy a bezpečné nástroje elektronického podpisu,
- používat bezpečné systémy pro uchovávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů nebo kvalifikovaných časových razítek v ověřitelné podobě.

Kvalifikovaný poskytovatel je povinen zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem, dále zajistit, aby údaje uvedené v těchto certifikátech byly přesné, pravdivé a úplné a zjistit, zda v okamžiku podání žádosti o vydání certifikátu jako kvalifikovaného měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů. Další povinnost se týká vydávání seznamu zneplatněných certifikátů – musí zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem. Co se týče autority časové značky, tak je povinna zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydán nebo zneplatněn, mohly být přesně určeny.

6.1 Certifikační politika

Obsahem certifikační politiky je podle vyhlášky č.366/2001 Sb. stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy a popis vlastností dat pro vytváření elektronického podpisu. Jsou zde uvedeny veškeré informace, které by měli žadatele o certifikát zajímat. Nalezneme zde údaje o CA, informace o vydávaných typech certifikátů, povinnosti jednotlivých subjektů, podmínky pro vydání certifikátu, informace o způsobech zneplatnění certifikátu a s tím spojený CRL, odpovědnost za škody atd. Jelikož

zákon nestanovuje přesnou struktura, jak by měla politika vypadat, stanovil ÚOOU doporučenou osnovu. Předpokládá se, že obsahem certifikační politiky musí být zejména:

- kontakty na registrační autority,
- kontakty na poskytovatele certifikačních služeb,
- povinnosti jednotlivých subjektů (registrační autority, poskytovatele certifikačních služeb, žadatele),
- odpovědnost za škodu,
- poplatky za služby spojené se správou certifikátů,
- přístup ke zveřejňovaným informacím (seznam všech vydaných kvalifikovaných certifikátů, seznam kvalifikovaných certifikátů, které byly zneplatněny),
- zásady ochrany informací,
- informace o auditu,
- způsob ověření vazby mezi daty na vytváření a ověření elektronického podpisu žadatele,
- způsob prokázání identity fyzické osoby žadatele,
- vzor žádosti o vydání kvalifikovaného certifikátu,
- podmínky pro vydání a převzetí kvalifikovaného certifikátu,
- vzor žádosti o ukončení platnosti kvalifikovaného certifikátu,
- obecné bezpečnostní mechanizmy pro oblasti fyzické, procedurální a personální bezpečnosti,
- způsob distribuce kvalifikovaného certifikátu poskytovatele klientům,
- seznam položek v kvalifikovaném certifikátu (povinné, doporučené, možné),
- způsob dokládání informací zapsaných v kvalifikovaném certifikátu atd.

K Certifikační politice musí poskytovatel umožnit trvalý dálkový přístup (např. pomocí webových stránek).

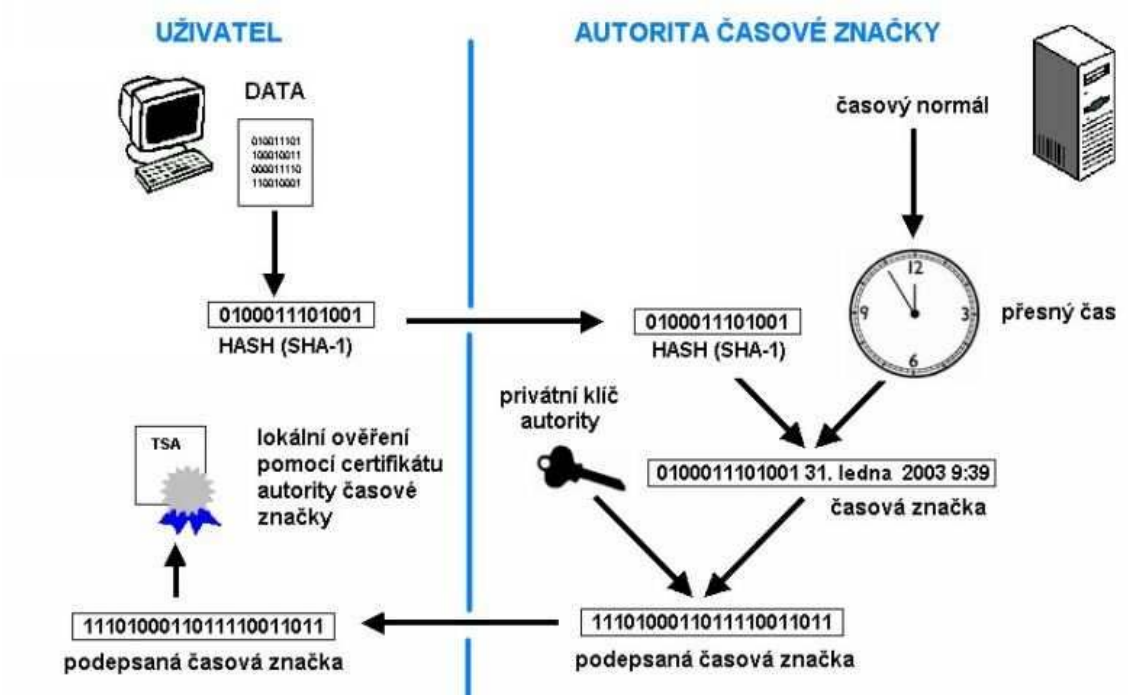
6.2 Autorita časové značky

Autorita časové značky slouží k vydávání tzv. časových razítek, s jejichž pomocí lze pro elektronické transakce, formuláře, archivovaná data, elektronický podpis apod. zajistit

jejich přesné určení v čase. Časové razítko vydané AČZ potvrzuje, že označená data existovala před uvedeným časovým okamžikem. Je tedy vhodným nástrojem pro určování, zda elektronický dokument a elektronický podpis byly vytvořeny v okamžiku platnosti certifikátu. Cílem této služby je tedy zajistit nepopiratelnost dokumentu vzhledem k určitému času.

Problémy spojené s důvěryhodným určením času je možné uspokojivě vyřešit dvěma způsoby. Jedním z nich je používání časových značek. Jedná se o auditovatelné záznamy uchovávané v bezpečném prostředí třetí důvěryhodnou stranou, která spojuje zasílaná data s hodnotou času při jejich přijetí do archivu. Druhý způsob představuje časové razítko resp. časový token. Jedná se o request/response komunikaci žadatele a poskytovatele služby časových razítek, který k zaslaným datům přidává časové razítko a vrací žadateli podepsaný časový token. [15]

Princip celého procesu vydání časové značky je patrný z následujícího obrázku.



Obr. č. 6 - Princip procesu vydávání časové značky

Vše probíhá tak, že speciální klientský software vypočítá hash určených dat a doplní jej dalšími údaji do formy žádosti o vydání časové značky, která je následně odeslána autoritě časové značky. Tam je žádost zpracována tak, že k dodanému hashi je přidán přesný

časový údaj a celý tento „balíček“ je elektronicky podepsán privátním klíčem autority časové značky.Tím je zajištěna důvěryhodnost časového údaje. Takto vytvořené časové razítko je doručeno žadateli.

Časové razítko nemusí být využíváno pouze v souvislosti s elektronickým podpisem. Uvedeme-li v žádosti o časové razítko jako vstupní údaj přímo celý text dokumentu, pak získaným časovým razítkem potvrdíme nezávislým způsobem datum a čas existence dokumentu. Časové razítko může být užitečné i pro netextové dokumenty, například pro dokumenty představované binárními soubory.

Situace ve kterých může být potřeba ověřit čas jsou následující:

- v průběhu doby platnosti certifikátu podepisující osoby mohlo dojít ke kompromitaci jejího soukromého klíče a ta jej z tohoto důvodu zneplatnila. V takovém případě je nutné zjistit, zda byl elektronický podpis vytvořen před okamžikem zneplatnění certifikátu,
- certifikát podepisující osoby je omezen dobou své platnosti, která je vymezena v položkách certifikátu. Po jejím vypršení je certifikát již neplatný a není možné se na takový certifikát spolehnout,
- právní předpisy mohou vyžadovat jako náležitost některých právních úkonů určení okamžiku, kdy byly učiněny. Pokud se takové právní úkony činí elektronicky je vhodné za účelem důvěryhodného určení času použít adekvátní elektronický nástroj.[15]

Příklady využití časových razítek a značek:

- v mailových serverech a při komunikaci,
- v auditních záznamech,
- ve zdravotnických záznamech,
- v databázích,
- v aplikacích se zvýšenými nároky na bezpečnost,
- v archivech elektronické dokumentace,
- v elektronickém bankovnictví,
- v elektronických podatelnách,
- u notářských systémů.

6.3 Akceptování jednotlivých typů certifikátů

Jak už jsem se zmínil, tak §11 ZoEP upravuje používání certifikátů při komunikaci s veřejnou správou takto: „V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen "uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná…“

Problém by mohl vzniknout s výkladem pojmu „orgán veřejné moci“. Někteří právníci zastávají názor, že komunikace soukromých subjektů s orgánem veřejné moci není výkonem ani oblastí výkonu této moci a že tedy soukromá osoba podávající podání směrem k orgánu veřejné moci se nemusí (ale může) podepisovat způsobem uvedeným v § 11. Výrazem „V oblasti orgánů veřejné moci…“ se tedy podle usnesení Ústavního soudu ČR rozumí taková situace, kdy je veřejná moc vykonávána, zejména tedy, pokud bude takový orgán vystupovat ve vztazích navenek vůči adresátům, mocensky rozhodovat o právech, povinnostech a právem chráněných zájmech fyzických a právnických osob. Může ovšem jít i o další vztahy, jako např. ty, které vznikají při rozhodování o právech a povinnostech zaměstnanců ve služebním poměru nebo i vztahy mezi dvěma orgány veřejné moci, pokud se tak činí při jejím výkonu (např. předávání vyjádření, stanovisek při přípravě právních předpisů a samozřejmě vydávání rozhodnutí). V této souvislosti je třeba zdůraznit, že pro posouzení toho, zda se jedná o orgán veřejné moci, není důležitá skutečnost, zda takový orgán je organizační složkou státu či má-li právní subjektivitu. Půjde-li však o činnost těchto orgánů ve vnitřních vztazích, není třeba používat zaručený elektronický podpis. Totéž pak platí i pro případ, kde takový orgán vystupuje v soukromoprávních vztazích (např. majetkových nebo pracovněprávních). [33].

Pokud jde o oblast komunikace, která se netýká veřejné správy, tak v této oblasti se elektronický podpis běžně používal ještě před přijetím zákona o elektronickém podpisu. Jde například o komunikaci obchodník - občan, která je nazývána zkratkou B2C (Business-to-Customer). Jde např. o nákup zboží na internetu pomocí webových obchodních domů. Ale zdaleka největším objem elektronické komunikace probíhá v

režimu B2B (Business-to- Business), který představuje až 90%. V tomto případě se jedná především o nákupní systémy velkých podniků. Existuje celá řada možností, jakým způsobem spolu mohou jednotlivé subjekty komunikovat, některé z nich budou uvedeny v tabulce. Komunikace B2A (Business-to-Administration) představuje nabídku služeb a zboží pro státní správu, C2B obsahuje např. sledování cen za účelem snížení ceny, C2C zahrnují klasickou e-mailovou komunikaci nebo různé aukční systémy, C2A slouží ke komunikaci občanů se státní správou, podávání daňových přiznání atd., při A2B dochází např. k zadávání veřejných zakázek nebo vypisování grantových projektů, A2C poskytuje informace občanům o chodu veřejné správy a A2A koordinuje činnosti orgánů veřejné moci.

„Možnost využívat zaručených elektronických podpisů a kvalifikovaných certifikátů podle zákona o elektronickém podpisu zvýší důvěru v takovouto komunikaci, obecně pak zajišťuje právní akceptovatelnost takovéto komunikace. Hlavní výhodou tedy je, že subjekty spolu mohou komunikovat na základě tohoto zákona a nemusí navzájem uzavírat speciální smlouvy nebo dohody akceptovatelnosti elektronického podpisu v této komunikaci.“ [33]

V tabulce jsou shrnuty základní formy komunikace mezi subjekty obchodník, spotřebitel a státní instituce.Tabulka obsahuje informace o nutnosti používání jednotlivých typů certifikátů.

Pro úplnost dodejme, že by neměla být porušena zásada, že takováto komunikace musí být pro konkrétní agendu v souladu s ostatními platnými zákony a musí být dodržena zásada, že subjekt, který se spoléhá na podpis, si může vyhlásit dodatečná pravidla pro tuto komunikaci, přičemž tato pravidla uvádí, kdy je takováto komunikace akceptovatelná.

<table>
<tr><th rowspan="2">Původce informace</th><th colspan="3">Adresát</th></tr>
<tr><th>Obchodník B=Business</th><th>Spotřebitel C=Consumer (Costumer)</th><th>Státní instituce A=Administration</th></tr>
<tr><td rowspan="2">Obchodník B=Business</td><td rowspan="2">B2B
C,QC,QC-APCS</td><td>B2C
C,QC,QC-APCS</td><td rowspan="2">B2A (B2G)
C,QC,QC-APCS
3. QC,QC-APCS</td></tr>
<tr><td>Bank2C
C,QC,QC-APCS</td></tr>
<tr><td>Spotřebitel C=Consumer (Costumer)</td><td>C2B
C,QC,QC-APCS</td><td>C2C
C,QC,QC-APCS</td><td>C2A (C2G)
C,QC,QC-APCS
3. QC,QC-APCS</td></tr>
<tr><td>Státní instituce A=Administration (G=Government)</td><td>A2B (G2B)
1. C,QC,QC-APCS
2. QC-APCS</td><td>A2C
1. C,QC,QC-APCS
2. QC-APCS</td><td>A2A (G2G)
1. C,QC,QC-APCS</td></tr>
</table>

Tab. č. 6 - Akceptování jednotlivých typů certifikátů

Legenda:

C - certifikát od libovolného poskytovatele certifikačních služeb

QC - kvalifikovaný certifikát

QC-APCS- kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb

1. - běžná komunikace

2. - výkon veřejné moci

3. - podání (ve smyslu NV č. 304/20001Sb.)

7 POROVNÁNÍ VÝZNAMNÝCH ČESKÝCH CERTIFIKAČNÍCH AUTORIT

7.1 První certifikační autorita, a.s (I.CA)

Certifikační autorita I.CA zahájila poskytování svých služeb v roce 1996 jako součást produktového portfolia společnosti PVT, a.s. Postupně I.CA přerostla hranice projektu a tak byla počátkem roku 2001 založena dceřiná společnost PVT, a.s. s názvem První certifikační autorita, a.s. Tato společnost převzala od mateřské společnosti veškeré činnosti, které bezprostředně souvisí s poskytováním certifikačních služeb. V současnosti je společnost vlastněna několika významnými společnostmi, a to: Česká spořitelna, a.s. Československá obchodní banka, a.s. Telefónica O2 Czech Republic, a.s. PVT, a.s. Státní tiskárna cenin s.p.

I.CA je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice. Svoje služby poskytuje také na Slovensku. Pro zajištění realizace požadavků svých klientů provozuje infrastrukturu tzv. registračních autorit a v současnosti jich spravuje více než 300 po celém území ČR a SR. Tato kontaktní pracoviště umožňují optimální dostupnost nabízených služeb. Počty vydaných certifikátů jsou dnes evidovány řádově ve statisících.

Úřad pro ochranu osobních údajů udělil První certifikační autoritě, a.s. I.CA akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 18. 3. 2002. I.CA takto úspěšně ukončila akreditační proces a je oprávněna zahájit poskytování služeb v oblasti kvalifikovaných certifikátů.

Vydávání kvalifikovaných certifikátů určených zejména pro komunikaci v oblasti orgánů veřejné moci I.CA zahájila dne 25.3. 2002 plně v intencích výše uvedeného zákona.

Ministerstvo informatiky ČR udělilo společnosti První certifikační autorita, a.s. rozšířenou akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 01. 02. 2006. Od tohoto data je I.CA oprávněna poskytovat kvalifikované certifikační služby nejen v oblasti kvalifikovaných certifikátů, ale i v oblastech kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek.

7.1.1 Druhy nabízených certifikátů a služeb

Hlavní činností poskytovatele certifikačních služeb je vydávání certifikátů. Každá certifikační autorita vydává zpravidla certifikáty několika druhů. Každý druh se pak odlišuje technickými parametry, způsobem jak je provedeno ověření totožnosti žadatele či možnostmi svého využití Aby uživateli bylo zřejmé, jaké tyto rozdíly jsou, existuje pro každý druh certifikátů dokument nazývaný Certifikační politika .

Příslušná Certifikační politika pak definuje především způsob vydání certifikátu, další správu, použití, akceptaci, ukončení platnosti, zneplatnění a všechny další činnosti související s nakládáním s párovými daty.

Kvalifikované certifikáty jsou vydávány fyzickým osobám. Délka platnosti těchto certifikátu je vždy 1 rok.

Kvalifikované certifikáty, vydané poskytovatelem certifikačních služeb (I.CA) v souladu se zákonem 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů v platném znění, lze používat pro následující účely:

- ověřování elektronických podpisů
- bezpečné ověřování elektronických podpisů
- zajištění neodmítnutelnosti odpovědnosti
- pokud klient při tvorbě žádosti nastaví odpovídající kritický atribut Key Usage, může využívat kvalifikované certifikáty i pro následující účely :
    - NonRepudation (povinný) - klíč bude používán pro vytváření elektronického podpisu
    - DigitalSignature (nepovinný) - soukromý klíč bude obecně používán pro vytváření elektronického podpisu (např.v rámci bezpečné elektronické pošty)
    - KeyEncipherment (nepovinný) – veřejný klíč obsažený v tomto kvalifikovaném certifikátu bude používán pro účely šifrování v rámci bezpečné elektronické pošty. DataEncipherment (nepovinný) " veřejný klíč obsažený v tomto kvalifikovaném certifikátu bude používán pro šifrování obecných dat, např. dokumentů
- v případě, že je zaručený elektronický podpis založený na kvalifikovaném certifikátu používaný pro autentizaci, musí být podepisující osoba provozovatelem

příslušné aplikace informována, zda má nebo nemá možnost se seznámit s daty, které podepisuje.

Kvalifikované certifikáty jsou rozděleny na :

- certifikáty standard
- certifikáty comfort

Osobní kvalifikovaný certifikáty standard mají data pro tvorbu elektronického podpisu uložena přímo ve našem počítači. Vytváření elektronického podpisu je tak umožněno pouze z tohoto konkrétního počítače ve kterém je uložen.

Osobní kvalifikované certifikáty Comfort představují certifikáty, jejichž hlavní odlišností od osobních certifikátů standard je čipová karta, která je součástí této služby. Slouží jako médium k bezpečnému uložení dat pro tvorbu elektronického podpisu a k bezpečnému vytváření elektronického podpisu. Přímo na kartě probíhá jednak vlastní generace dat pro tvorbu elektronického podpisu, následně také tvorba elektronického podpisu vlastníka těchto dat. Prakticky se tedy důvěrná data uživatele nikdy nedostanou mimo kartu. Na kartě je zároveň uložen také osobní certifikát majitele karty). Tato čipová karta je určena výhradně pro použití s certifikátem vydaným I.CA. Platnost dat pro tvorbu elektronického podpisu, která jsou uložena na kartě, je stanovena na 1 rok, přičemž na tuto čipovou kartu lze uložit celkem tři po sobě následující data pro tvorbu elektronického podpisu. Čipová karta je tedy určena a uzpůsobena k používání po dobu tří let.

I.CA vydává tři typy kvalifikovaných certifikátů.

- kvalifikovaný certifikát pro fyzickou osobu (je určen pro žadatele, kteří žádají o certifikát pro osobní účely)
- zaměstnanecký kvalifikovaný certifikát (je ověřována kromě totožnosti také vazba fyzické osoby na jejího zaměstnavatele)
- kvalifikovaný certifikát pro PSEUDONYM (umožňuje žadateli, získat certifikát, který neobsahuje jeho vlastní identifikaci. Pseudonym pak může obsahovat jakoukoliv sekvenci znaků. Nejsou povoleny výrazy vulgární, propagující fašismus, rasovou a třídní nenávist)

Komerční certifikáty

- certifikát standard
- certifikát comfort
- certifikát pro server

Komerční certifikáty jsou osobní certifikáty, určené především pro použití v uzavřených systémech, kde je mezi účastníky bezpečné komunikace uzavřena smlouva, zahrnující rovněž podmínky komunikace. Tedy hlavně pro firemní účely. Tyto certifikáty jsou spolu s příslušnými daty pro vytváření elektronického podpisu vhodné a použitelné pro elektronický podpis, šifrování, autentizaci a případně pro další operace na obdobných základech. Jsou vydávány fyzickým nebo právnickým osobám .

Rozdíl mezi certifikáty Standard a Comfort opět spočívá, jak jsem již uvedl výše, v čipové kartě, která je součástí služby Comfort.

Certifikáty pro servery jsou určené pro bezpečnou komunikaci serverů. Jsou vydávány pro fyzické nebo právnické osoby.

Kvalifikované systémové certifikáty

Tyto certifikáty jsou obdobou klasických kvalifikovaných certifikátů s tím rozdílem, že slouží k ověřování automaticky vytvořených elektronických značek, tzn. že osoba vlastnící certifikát nemusí být fyzicky přítomna. Využívá se především tam, kde není možné, vzhledem k objemům podpisů, delegovat fyzické pracovníky.

Testovací certifikáty

Jedná se o certifikáty sloužící k ověření funkčnosti technologie použité pro realizaci tvorby digitálního podpisu. K jejich vydání dochází prakticky okamžitě po odeslání řádně vyplněné žádosti do centrálního systému První certifikační autority. Fyzické ověření totožnosti žadatele o testovací certifikát není v tomto případě požadováno.

Platnost testovacího certifikátu je stanovena na 14 dní. Po uplynutí této lhůty je automaticky ukončena jeho platnost. Tyto certifikáty jsou neveřejné a jsou vydávány vždy zdarma. Zdarma je možné zažádat a otestovat standardní či serverový certifikát.

Kvalifikovaná časová razítka

Časové razítko/kvalifikované časové razítko je nástrojem, který hodnověrným způsobem zajišťuje přiřazení aktuálního časového údaje k existujícím datům, informacím, souborům atd. - je tedy elektronickým důkazem o existenci určitého dokumentu daném čase. Spojení nezpochybnitelného časového údaje a konkrétních dat je nezbytné zejména pro účely jejich zpětného ověřování v budoucnosti.Kvalifikovaná časová razítka jsou službou určenou jak pro jednotlivce z řad veřejnosti, tak pro firemní účely a jsou vydávána jakémukoliv žadateli, který má k dispozici komerční certifikát vydaný naší společností. Mezi nejčastější způsoby využití patří:

- práce s dokumenty – jednoznačné doložení času, ve kterém dokument v daném tvaru existoval
- ochrana logových záznamů v auditních souborech – časové razítko jednoznačně definuje čas, ve kterém v dané podobě soubor existoval (zpětná úprava vede k porušení)
- elektronické podatelny
- notářské služby
- uzavírání elektronických smluv
- on-line obchody
- aplikace, kde je nutné stanovit časový rámec

7.1.2 Ceny certifikátů I.CA

Druh služby	Poznámky	Cena s DPH
Kvalifikovaný certifikát typ Standart	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče	752,- Kč
Kvalifikovaný certifikát typ Comfort	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče. čipová karta, ovládací SW I.CA	1758,- Kč obnovený 752,- Kč

Tab. č. 7 - Přehled cen certifikátů I.CA

Druh služby	Poznámky	Cena s DPH
Kvalifikovaný systémový certifikát typ Standart	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče	780 Kč
Kvalifikovaný systémový certifikát typ Comfort	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče. čipová karta, ovládací SW I.CA	1756,- Kč obnovený 780,- Kč
Podpisový certifikát ke kvalifikovanému systémovému certifikátu - kvalifikovaný	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče	390,- Kč
Komerční certifikát typ Standart	Platnost certifikátu: 6 měsíců. Použití 512 bitového klíče	322,- Kč
Komerční certifikát typ Standart	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče	580,- Kč
Komerční certifikát typ Comfort	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče. čipová karta, ovládací SW I.CA	1556,- Kč obnovený 580,- Kč
Certifikát pro server	Platnost certifikátu: 6 měsíců. Použití 512 bitového klíče	1073,- Kč
Certifikát pro server	Platnost certifikátu: 12 měsíců. Použití 1024 bitového klíče	1931,- Kč
Kvalifikovaná časová razítka	Ceny jsou individuální podle počtu razítek.	

Tab. č. 8 - Přehled cen certifikátů I.CA

[34].

7.2 Certifikační autorita PostSignum České pošty, s.p.

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb dne 3.8.2005 na základě akreditace udělené Ministerstvem informatiky ČR. Tímto aktem se z českého trhu akreditovaných certifikačních autorit záhy stalo konkurenční prostředí. Česká pošta se do tohoto souboje vrhla s velmi dobrými zbraněmi: velmi příznivé ceny a snadná dostupnost široké veřejnosti.

7.2.1 Druhy nabízených certifikátů a služeb

Certifikační autorita PostSignum se dělí na dvě části, podle druhu samotných certifikátů: VCA a QCA.

PostSignum VCA, nebo-li Veřejná certifikační autorita je zaměřena na vydávání komerčních certifikátů, které jsou určeny především pro zajištění šifrované komunikace, ověření elektronických podpisů či autentizace uživatelů. Komerční certifikáty mohou být vydávány osobám i technologickým komponentám (aplikace, zařízení, servery).

V této práci se zaměřím spíše na QCA.

Certifikačni autorita PostSignum QCA rozšiřuje obchodní aktivity České pošty, s. p. o služby vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů. Na základě novel příslušného zákona o elektronickém podpisu nabízí dále PostSignum elektronické značky, neboli systémové certifikáty. Zatímco e-podpis je určen pro fyzickou osobu, která přímo osobně podepisuje daný dokument, elektronickou značku může používat fyzická i právnická osoba a také organizační složka státu (například ministerstvo) pro automatické bezpečné hromadné označování dokumentů. V praxi tak lze předpokládat řadu využití, například pro automatické (bezpečné) odpovědi podatelny, podepisování elektronických výpisů a další - tedy všude tam, kde se hodí mít jednoznačně prokazatelnou autenticitu zdroje, ovšem vzhledem k objemům podpisů to nebylo možné delegovat na fyzické pracovníky. Cena certifikátu pro elektronickou značku je 2856 korun vč. DPH.

kvalifikované certifikáty

- Certifikát pro ověření elektronického podpisu zaměstnance: Certifikáty vydané podle této politiky jsou určeny pro podepisující osoby, které jsou v určitém vztahu k zákazníkovi, jenž uzavřel s Českou poštou smlouvu o poskytování certifikačních

služeb. Tyto certifikáty mohou být použity pouze pro ověření elektronického podpisu podepisující osoby v souladu se ZoEP.

- Certifikát organizace pro ověření elektronické značky: Certifikáty vydané podle této politiky jsou určeny pro zákazníky (označující osoby), kteří s Českou poštou uzavřeli smlouvu o poskytování certifikačních služeb. Certifikáty vydané podle této politiky mohou být použity pouze pro ověření elektronické značky označující osoby v souladu se ZoEP.
- Certifikát pro ověření elektronické značky fyzické osoby: Certifikáty vydané podle této politiky jsou určeny pro fyzické podepisující osoby, které s Českou poštou uzavřely smlouvu o poskytování certifikačních služeb. Tyto certifikáty mohou být použity pouze pro ověření elektronického podpisu fyzické podepisující osoby v souladu se ZoEP.

Kvalifikované certifikáty a kvalifikované systémové certifikáty tedy nejsou (dle příslušné CP) určené pro komunikaci nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod., nebo v souvislosti s bezpečností a obranyschopností státu.

Vydávání certifikátů zákazníkům se standardně provádí na kontaktních místech České pošty. Máte však také možnost objednat si službu Mobilní registrační autority (MRA), která provede vydání certifikátu(ů) na dohodnutém místě (např. vaše bydliště).

MRA může také vyřídit ostatní služby kontaktního místa:

- uzavření smlouvy se zákazníkem
- zavedení zákazníka do systému PostSignum QCA
- zneplatnění certifikátu(ů)

Objednání mobilní registrační autority se provádí tak, že si stáhneme objednávku služeb MRA a vyplníte údaje o odběrateli. Vyplněnou objednávku zašlete e-mailem kontaktní osobě České pošty. Kontaktní adresy pro jednotlivé regiony jsou uvedeny v objednávce.

Objednávku je potřeba zaslat nejméně týden před požadovaným termínem odběru služby! Termín výjezdu MRA je zákazníkovi potvrzen e-mailem nebo telefonicky.

7.2.2 Ceny certifikátů CA PostSignum

Druh služby	Poznámky	Cena s DPH
Certifikáty pro ověření elektronického podpisu fyzické osoby	Platnost certifikátu: 1 rok Použití 1024 nebo 2048 bitového klíče	190,- Kč
Certifikáty pro ověření elektronického podpisu podnikající osoby, zaměstnance	Platnost certifikátu: 1 rok Použití 1024 nebo 2048 bitového klíče	190,- Kč
Certifikáty pro ověření elektronické značky fyzické osoby	Platnost certifikátu: 1 rok Použití 1024 nebo 2048 bitového klíče	2856,- Kč
Certifikáty organizace pro ověření elektronické značky	Platnost certifikátu: 1 rok Použití 1024 nebo 2048 bitového klíče	2856,- Kč
Certifikáty pro technologické komponenty fyzických osob nebo organizace	Platnost certifikátu: 1 rok Použití 1024 nebo 2048 bitového klíče	800,- Kč
Šifrovací certifikáty pro skupiny osob	Platnost certifikátu: 1 rok Použití 1024 nebo 2048 bitového klíče	800,- Kč
Zneplatnění certifikátu		zdarma

Tab. č. 9 - Ceny certifikátů PostSignum

V současnosti má Česká pošta kolem 80 poboček po celé ČR, které jsou zplnomocněné vydávat kvalifikované certifikáty. [34].

7.3 Certifikační autorita eIdentity

společnost vznikla počátkem roku 2004 s jasnou orientací na komplexní služby v oblasti správy elektronické identity. Je tedy, co se týče vzniku i udělené akreditace, na našem trhu nejmladší a své postavení na trhu si musí ještě vydobýt. eIdentity má zatím pouze jedno kontaktní místo, což je oproti konkurenci opravdu velký rozdíl.

7.3.1 Druhy nabízených certifikátů a služeb

Společnosti eIdentity byla Ministerstvem informatiky v září 2005 udělena zatím poslední akreditace a to v těchto oblastech:

- vydávání kvalifikovaných certifikátů,
- vydávání kvalifikovaných systémových certifikátů.

eIdentity dále nabízí řadu komerčních certifikátů. Do budoucna by měla přibýt v nabídce také časová razítka. Počítá se prý i s vydáváním e-mailových certifikátů (tj. certifikátů garantujících právě a pouze e-mailovou adresu). Naopak s vydáváním testovacích certifikátů prý identity nepočítá. [38]

Kvalifikované certifikáty

Akreditovaná certifikační autorita eIdentity a.s. (ACAeID) je tvořena kořenovou certifikační autoritou **(RCA)** a autoritou vydávající kvalifikované a kvalifikované systémové certifikáty pro podepisující a označující osoby **(QCA)**. RCA vydává kvalifikované systémové certifikáty pouze podřízeným certifikačním autoritám (tedy i QCA a CCA). QCA vydává kvalifikované certifikáty a kvalifikované systémové certifikáty jednotlivým žadatelům.

Jednána se o poskytování těchto základních kvalifikovaných certifikačních služeb:

- Vydání kvalifikovaného certifikátu
- Vydání kvalifikovaného certifikátu s vyznačením identifikátoru ministerstva práce a sociálních věcí (MPSV)
- Vydání kvalifikovaného certifikátu s vyznačením pracovní pozice v organizaci
- Vydání kvalifikovaného systémového certifikátu

Mezi další služby ACAeID patří pravidelné vydávání seznamu zneplatněných certifikátů (CRL) či seznamu vydaných certifikátů.

Komerční certifikáty

Pro účely šifrování, identifikace, ale také pro vytváření a ověřování elektronických podpisů v oblasti běžné komerční komunikace lze využít elektronických certifikátů, vydaných Komerční certifikační autoritou (CCA). Tato certifikační autorita vydává také elektronické certifikáty pro technologické komponenty informačních systémů (např. pro webové servery či servery elektronické pošty, zabezpečeně komunikující pomocí SSL/TLS).

Jedná se o poskytování těchto základních komerčních certifikačních služeb:

- Vydání komerčního certifikátu pro elektronický podpis
- Vydání komerčního certifikátu pro šifrování zpráv
- Vydání komerčního certifikátu pro identifikaci
- Vydání komerčního serverového certifikátu pro SSL/TLS

Společnost eIdentity a.s. poskytuje také hosting či outsourcing komerčním certifikačním autoritám třetích stran. Mezi další služby ACAeID patří také pravidelné vydávání seznamu zneplatněných certifikátů (CRL) či seznamu vydaných certifikátů. [35].

7.3.2 Ceny certifikátů a služeb CA eIdentity

Druh služby	Poznámky	Cena s DPH
Kvalifikovaný certifikát	Platnost certifikátu: 12 měsíců.	702,- Kč
Kvalifikovaný systémový certifikát	Platnost certifikátu: 12 měsíců.	3451,- Kč
Komerční certifikát (k již vydanému kvalifikovanému systémovému certifikátu)	Platnost certifikátu: 12 měsíců.	238,- Kč
Komerční serverový certifikát (k již vydanému kvalifikovanému systémovému certifikátu)	Platnost certifikátu: 12 měsíců.	752,- Kč
Komerční certifikát	max. 12 měsíců, n let (n>1)	583,- Kč n krát 500,- Kč
Komerční serverový certifikát	max. 12 měsíců, n let (n>1)	1845,- Kč n krát 1566,- Kč
Zneplatnění certifikátu	trvale	zdarma
Podání žádosti o zjištění IKMPSV	trvale	zdarma

Tab. č. 10 - Ceny certifikátů identity

7.4 Certifikační autorita Czechia

Certifikační autorita Czechia, s.r.o. zahájila svou činnost již v roce 1999, tehdy však pod jménem Altimo, s.r.o. Společnost se orientovala na poskytování standardních internetových služeb. Úspěšný a dynamický rozvoj vyústil v akvizici společností ZONER software, s.r.o. Počátkem roku 2000 začala pro ZONER software připravovat projekt Certifikační autority Czechia. V roce 2002 pak plně přebrala od mateřské společnosti ZONER software veškeré činnosti a služby přímo související s poskytováním certifikačních služeb. Na podzim roku 2002 došlo k přejmenování společnosti na Certifikační autorita Czechia, s.r.o.

7.4.1 Druhy nabízených certifikátů a služeb

- Vydání osobního certifikátu
- Vydání firemního certifikátu
- Vydání testovacího certifikátu
- Vydání komerčního serverového certifikátu pro SSL/TLS

CA Czechia nevydává kvalifikované certifikáty. To znamená, že její certifikáty nelze použít v oblasti orgánů státní moci, kde je možné používat pouze kvalifikované certifikáty od akreditované certifikační autorit, kterou CA Czechia není. Přesto vychází důsledně ze zákona o elektronickém podpisu. Žádosti o certifikát jsou podrobně kontrolovány a je vyžadováno notářské ověření totožnosti žadatele na smlouvě.

Firemní certifikáty lze použít i jako "systémové certifikáty" dle novely zákona o EP.V rámci služeb pro klienty je nabízeno bezpečné uložení klíče formou USB Tokenu. Největší konkurenční výhodou této CA jsou ceny certifikátů. [36].

7.4.2 Ceny certifikátů s služeb CA Czechia

Druh služby	Poznámky	Cena s DPH
Osobní certifikát	Platnost certifikátu: 12 měsíců.	159,- Kč
Firemní certifikát	Platnost certifikátu: 12 měsíců.	390,- Kč
serverový certifikát	Platnost certifikátu: 12 měsíců.	1000,- Kč
Testovací certifikát	Platnost certifikátu: 1 měsíc.	zdarma

Tab. č. 11 - Ceny certifikátů Czechia

7.5 Porovnání významných českých certifikačních autorit

Abychom mohli certifikační autority porovnat, je třeba si určit kritéria, podle kterých je budeme hodnotit. Asi nejvýznamnějším kritériem, podle kterého se bude případný zájemce o certifikát rozhodovat bude důvěryhodnost.Tento požadavek je zcela zásadní. Informace o certifikační agentuře je možno získat např. z její webové stránky, z referencí ostatních uživatelů, z praktických zkušeností, ale především je to Certifikační politika, která obsahuje pro nás ty nejpodstatnější informace. Velmi důležitým faktorem při výběru certifikační autority je její akceptace druhou stranou.

Jedním z možných rozhodovacích kritérií může být počet kontaktních míst, tzv. registračních autorit. Pokud certifikační autorita vyžaduje při ověřování totožnosti osobní návštěvu kontaktního místa, bylo by nepříjemné, abychom museli dojíždět velmi

daleko. Je proto důležité zjistit si, kolika registračními autoritami a kde jednotlivé certifikační autority disponují.

Dalším důležitým kritériem jsou typy vydávaných certifikátů. Existuje velké množství certifikátů, ale každá certifikační autorita poskytuje pouze určité typy. Opět je pro náš výběr důležité, s kým budeme v budoucnosti komunikovat. Např. banky ve většině případů vyžadují pouze jimi vydané certifikáty. Opět zopakuji, že pokud bychom chtěli komunikovat s orgány veřejné správy, je podle zákona nutné používat pouze kvalifikovaný certifikát vydávaný akreditovaným poskytovatelem certifikačních služeb, tedy tzv. "uznávaný elektronický podpis".

Cena certifikátu může být pro někoho velmi důležitá, ale je třeba si uvědomit, že nemůže být hlavním kritériem. Cena bude opět záležet na případném použití certifikátu, typu certifikátu, dále na délce klíče, době platnosti atd. Cenu může ovlivnit, pokud využijeme bezpečné hardwarové uložení klíče. Standardně se jako úložiště používají čipové karty nebo USB Tokeny (viz obrázek).

Obr. č. 7 - Čipová karta

Obr. č. 8 - USB token

Samozřejmě dále existuje celá řada kritérií, podle kterých bychom mohli jednotlivé certifikační autority hodnotit. Rozdíly mezi jednotlivými autoritami budou velmi patrné z přehledných tabulek, které obsahují hodnotící kritéria.

Rozhodl jsem se pro následující hodnotící kritéria:

- počet registračních autorit,
- typy vydávaných certifikátů,
- akceptace certifikátu ve státní správě,
- délka klíče,
- doba platnosti certifikátu,
- časová razítka,
- bezpečné uložení klíče,
- způsob ověření totožnosti žadatele o certifikát,
- způsob podání žádosti o certifikát,
- způsob vydání certifikátu,
- způsob zneplatnění certifikátu,
- interval vydávání CRL.
- cena certifikátů,

Pro hodnocení jsem vybral čtyři významné certifikačních autorit působících na území České republiky:

- První Certifikační autorita,
- CA PostSignum,
- CA eIdentity,
- CA Czechia,

Poskytovatel	První certifikační autorita, a.s.	PostSignum
Počet registračních autorit	300	80
Typy vydávaných certifikátů	testovací, komerční certifikáty pro fyzické i právnické osoby, kvalifikované certifikáty, serverové certifikáty,	certifikát zaměstnanců, certifikát technologických komponent, šifrovací certifikát skupiny osob
akceptace certifikátu ve státní správě	je akceptován	je akceptován
Délka klíče	512 - 1024 bitů	1024 - 2048 bitů
Doba platnosti certifikátu	6-12 měsíců, testovací 14 dní	12 měsíců
Časová razítka	jsou součástí nabídky pro klienty I.CA	nejsou v nabídce
Bezpečné uložení klíče	čipová karta u varianty komfort, token iKey 3000	není v nabídce
Způsob ověření totožnosti	2 osobní doklady, osobní návštěva registrační autority	1 osobní doklad, osobní návštěva
Způsob podání žádosti o certifikát	on-line na webu nebo s pomocí off-line aplikace NewCert stažené z www stránek	on-line www stránkách, osobní návštěva registrační autority
Způsob vydání certifikátu	osobně předáním na médiu, případně zasláním v předepsaných formátech na adresu uvedenou v žádosti	osobně předáním na médiu
Způsob zneplatnění certifikátu	osobně, elektronickou poštou s heslem pro zneplatnění, formulářem na www stránkách, listovní zásilkou, pomocí SMS, telefonicky	osobní návštěva (heslo pro zneplatnění, 1 osobní doklad), telefonicky nebo písemně (heslo pro zneplatnění); zneplatněn do 12 hodin
Interval vydávání CRL	12 hodin v případě kvalifikovaných certifikátů a 24 hodin u komerčních certifikátů	12 hodin

Tab. č. 12 - Porovnání certifikačních autorit

Poskytovatel	CA eIdentity a. s.	CA Czechia
Počet registračních autorit	1	3
Typy vydávaných certifikátů	testovací, klientské, serverové certifikáty pro fyzické i právnické osoby	testovací, osobní a firemní, serverové certifikáty
akceptace certifikátu ve státní správě	je akceptován	není akceptován
Délka klíče	neuvádí, předpokládá se 1024 bitů	512 - 1024 bitů
Doba platnosti certifikátu	neuvádí, předpokládá se 1024 bitů	12 měsíců12 měsíců, testovací 1 měsíc
Časová razítka	nejsou v nabídce	nejsou v nabídce nejsou součástí nabídky
Bezpečné uložení klíče	není v nabídce	token iKey 2032
Způsob ověření totožnosti	žadatel notářsky ověří žádost,(kterou odevzdal a která je mu zaslána zpět) a zašle ji poštou certifikační autoritě	občanský průkaz, ověření může proběhnout osobní návštěvou, nebo úředním ověřením podpisu smlouvy žadatele s CA
Způsob podání žádosti o certifikát	on-line na www stránkách	pomocí aplikace na www stránkách,
Způsob vydání certifikátu	zaslání poštou na digitálním nosiči	po ověření je uvolněn ke stažení na uživatelském účtu na www stránkách
Způsob zneplatnění certifikátu	on-line na webových stránkách	pomocí webového rozhraní (do 24 hodin)
Interval vydávání CRL	24 hodin	1x týdně

Tab. č. 13 - Porovnání certifikačních autorit

	Typ certifikátu					
Poskytovatel	**Kvalifikovaný certifikáty**	**Kvalifikované systémové certifikáty**	**Komerční certifikáty**	**Certifikát pro server**	**Osobní certifikát**	**Testovací certifikát**
První certifikační autorita, a.s. **typ Standard** **typ Comfort**	 752,- Kč 1728,- Kč	 780,- Kč 1756,- Kč	 322,- Kč 580,- Kč 1556,- Kč	1073,-Kč 1931,-Kč	---------	zdarma
CA České pošty PostSignum	190,- Kč	2856,- Kč	800,- Kč	1000,-Kč	--------	zdarma
CA eIdentity	702,- Kč	3451,- Kč	583,- Kč	1845,-Kč	--------	zdarma
CA Czechia	--------	---------	322,- Kč	1000,-Kč	159,- Kč	zdarma

Tab. č. 14 - Porovnání cen za certifikáty

7.5.1 Zhodnocení porovnání certifikačních autorit

V této části práce provedu slovní zhodnocení certifikačních autorit, podle jednotlivých kritérií, které jsme porovnávali v tabulkách.

Akceptace certifikátu ve státní správě – je velmi důležitým kritériem při výběru certifikační autority. Pokud budeme chtít komunikovat s orgány veřejné správy, musíme mít kvalifikovaný certifikát od akreditované certifikační autority. Z toho vyplívá, že pro tento účel musíme vlastnit certifikát od První certifikační autority, CA PostSignum nebo CA identity .

Počet registračních autorit - podle tohoto kritéria je jednoznačná volba. Je to CA I.CA. Má 300 registračním autorit. V tomto případě jí nemůže žádná z ostatních CA konkurovat.

Typy vydávaných certifikátů – u tohoto kritéria jsou si nabídky jednotlivých CA podobné. Jen I. CA, jako jediná, nabízí možnost časových razítek.

Délka klíče - u většiny CA podobná, pouze PostSignum nabízí až 4096 bitů, které zajistí nadprůměrné zabezpečení.

Doba platnosti - v době platnosti certifikátů jsem mezi jednotlivými poskytovateli nezjistil výraznější odchylky, nabízí platnost v délce 12 měsíců, to je podle mého názoru, celkem málo a dovedu si představit platnost nejméně v délce 24 měsíců

Časová razítka – toto možnost nabízí jen I.CA

Bezpečné uložení klíče- u I.CA je to řešeno pomocí čipové karty (u varianty komfort) a USB token iKey 3000, CA Czechia nabízí bezpečné uložení klíče na USB token iKey 2032 ostatní bezpečné uložení klíče nenabízí.

Způsob ověření totožnosti - způsob ověření totožnosti spočívá u většiny CA v osobní návštěvě a předložení minimálně jednoho osobního dokladu. CA Czechia a eIdentity nabízejí možnost zaslat úředně ověřenou žádost, což může být v případě vzdáleného umístění registrační autority velká výhoda.

Způsob podání žádosti certifikátu je řešen on-line způsobem na webových stránkách.

Způsob vydání certifikátu - Způsob vydání certifikátu je řešen různě, převládá možnost předání na datovém médiu a to buď osobně nebo zasláním, případně stažení z webových stránek u Ca Czechia.

Zneplatnění certifikátu - Zneplatnění certifikátu je prováděno u všech poskytovatelů standardně pomocí webového rozhraní a některé umožňují i jiné formy, jako např. pomocí SMS, telefonicky, listovní zásilkou, osobní návštěvou atd. V tomto ohledu jsem u tohoto kritéria nezjistil významnější rozdíly.

Interval vydávání CRL – podle mého názoru velmi důležité kritérium.V případě prozrazení našeho soukromého klíče je velmi důležité zanést co nejdříve tuto skutečnost do seznamu zneplatněných certifikátů. Tento interval se pohybuje od 12 hodin až po poměrně dlouhou dobu jednoho týdne u CA Czechia.

Cena certifikátů – u tohoto kritéria jsou na tom nejlépe CA Czechia (159 Kč) a CA PostSignum (190 Kč). Cena za kvalifikovaný certifikát v této výši, jak ji uvádějí tyto certifikačníc autority, je podle mého názoru již pro většinu obyvatel přijatelná .,

Konečné rozhodnutí bude pravděpodobně záležet na preferencích každého jednotlivce.

Někdo bude preferovat autoritu časových razítek, jiný bezpečné uložení klíče pomocí USB Tokenu nebo cenu certifikátu. Volba je na každém z nás. Já osobně bych vsadil na jistotu a doporučil První certifikační autoritu a. s. jak pro komunikaci se státní správou tak i mimo ni. První certifikační autoritu a. s. Tato CA byla na trhu první a její certifikáty jsou akceptovány všemi subjekty. Její portfolio služeb je ze všech porovnávaných CA nejširší. Rozsáhlá síť kontaktních míst je velmi dobrá, jediné co zaostává, je vyšší cena služeb. Delší kryptografický klíč a tím i vyšší bezpečnost je u ní zpoplatněna. Využití kratšího klíče má za následek zkrácení doby platnosti certifikátu.

Jako, jako druhou alternativu bych volil CA PostSignum, která má velmi přijatelnou cenu certifikátu 190 Kč. Což je podlé mého názoru velmi přijatelná cena pro většinu obyvatel. Nabízí také využití kryptografického klíče o délce až 2048 bitů. Toto žádná jiná CA zatím nenabízí a navíc to nabízí bez rozdílu ceně. (větší délka znamená vyšší bezpečnost a tak by si mohla nárokovat vyšší cenu.) Menší nevýhodou může být menší počet registračních míst oproti I.CA.Což se do budoucna vzhledem tomu, že je poskytovatelem Česká pošta , může rychle změnit. A to z toho důvodu, že má pobočky ve všech větších městech.

Společnost eIdentity. Ta vlastní pouze jednu registrační autoritu a ceny certifikátů nejsou zrovna nejlevnější. Od svých konkurentů se eIdentity odlišuje procesem vystavování certifikátů (i následné "údržby", jako je třeba vystavování následných certifikátů). Placení se odehrává bezhotovostně a předem. Teprve po zaplacení má zákazník možnost vygenerovat si nezbytný pár klíčů, potřebný k žádosti o vystavení certifikátů, a vydat se k vystaviteli (jeho registrační autoritě) pro ověření své identity. To má mít i bezpečnostní aspekt -

zkrátí se tím doba, po kterou budou mít lidé ("někde" na svém počítači) vygenerované klíče bez zpracované a přijaté žádosti a vydaného certifikátu.

Poslední, CA Czechia bych nedoporučoval .V některých porovnávaných parametrech sice dopadla dobře (např.cena). ale její velkou nevýhodou je to, že nemá akreditaci a tudíž nelze použít její certifikáty pro komunikaci se státní zprávou. Interval vydávání CRL je u této CA 1týden. Což je poměrně dlouhá doba.

Na závěr bych ještě chtěl zhodnotit webové stránky jednotlivých poskytovatelů, Ty se hodně lišily, jak co do obsahu a poskytování informací, tak co do přehlednosti a intuitivnosti v navigaci. V tomto ohledu se mi jako nejkvalitnější jevily stránky První certifikační autority a CA Czechia. I.CA na svých velmi přehledných stránkách, kromě základních informací o svých produktech, certifikační politiky a ostatních službách shrnuje základní teorie a principy elektronického podpisu, nabízí seznam legislativních norem a předpisů upravujících využívání certifikátů nebose zabývá problematikou využívání čipových karet.

Taky CA Czechia pojala své stránky jako jakýsi portál, jsou zde soustředěny informace týkající se elektronického podpisu, různé články o EP, souhrn legislativy, principy fungování a možnosti využití.

Každá z těchto CA je něčím výjimečná a společně vytváří poměrně bohatou nabídku služeb a produktů, takže budoucí uživatelé elektronického podpisu mají z čeho vybírat.

8 POSTUP ZÍSKÁNÍ KVALIFIKOVANÉHO CERTIFIKÁTU U I.CA, INSTALACE , POUŽITÍ V OUTLOOK EXPRES A VLASTNÍ ZKUŠENOSTI

Jelikož mne zaujala nabídka I.CA, rozhodl jsem se pořídit si kvalifikovaný certifikát a otestovat tak elektronické podepisování v praxi. V této kapitole si popíšeme především postup získání samotného certifikátu, jeho instalaci a další vlastní zkušenosti s tímto postupem.

8.1 Podrobný popis získání certifikátu a instalace v Outlook Expres

Pro získání osobního kvalifikovaného certifikátu standard je třeba postupovat podle následujících kroků :

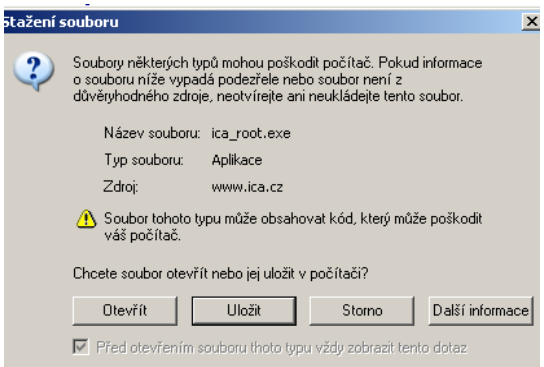
- Instalace kořenového certifikátu I.CA - pro oblast kvalifikovaných certifikátů
- Vytvoření žádosti o kvalifikovaný certifikát standard.
- Návštěva kontaktního pracoviště I.CA (Registrační autorita)
- Instalace kvalifikovaného certifikátu do vašeho systému.

a) Instalace kořenového certifikátu I.CA - pro oblast kvalifikovaných certifikátů

Nejprve si otevřeme webové stránky I.CA, zde nalezneme v nabídce „ žádost o certifikát“.

V této části si zvolíme správný, námi požadovaný typ certifikátu. Já, jsem jsi zvolil *Kvalifikovaný certifikát pro fyzickou osobu(typ standard).*

Ještě než začneme proces generování žádosti a následného užívání certifikátu, je nutné provést instalaci certifikátů certifikační autority I.CA " tzv. kořenových certifikátů.“

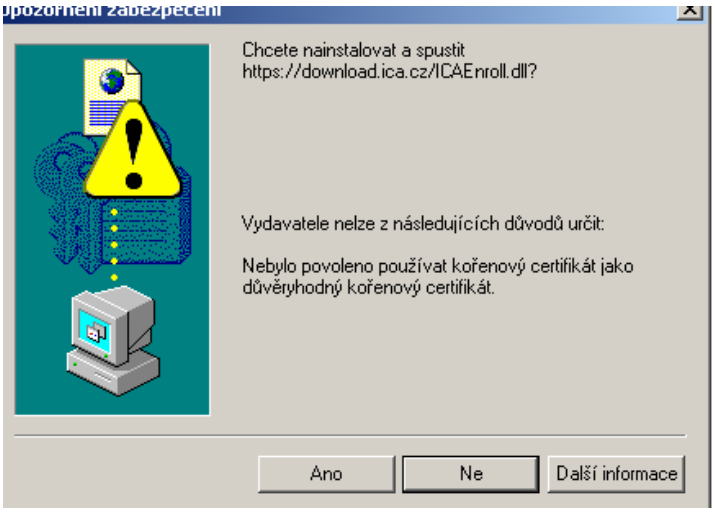


Obr. č. 9 - Kořenový certifikát - instalace

b) Vytvoření žádosti o kvalifikovaný certifikát standard.

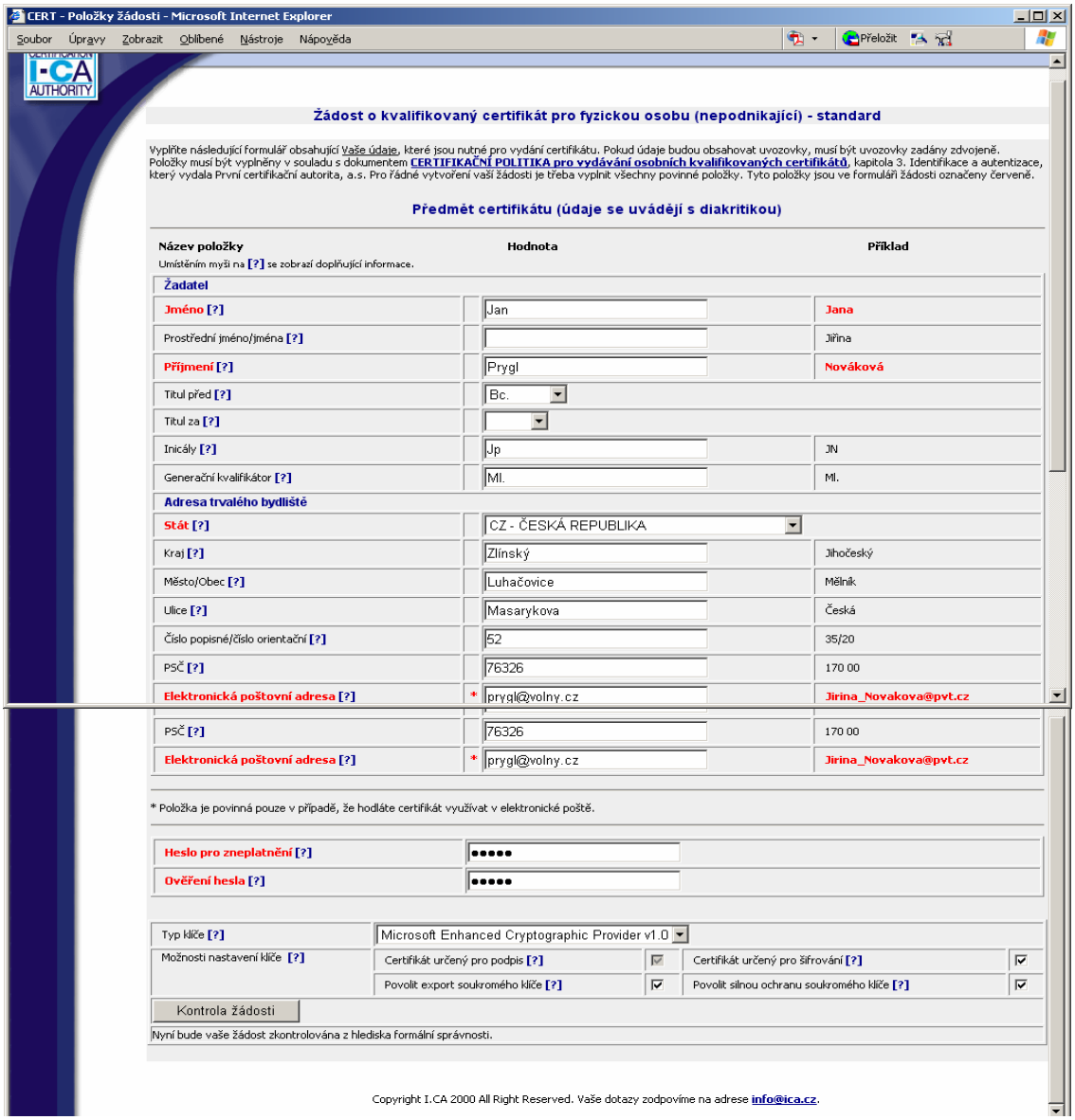
Před zahájením tvorby žádosti o certifikát musíme pamatovat na následující:

- Na PC, na kterém budete tvořit žádost o certifikát musíme také následně provést instalaci našeho certifikátu. Pouze takto zajistíme správné fungování našich dat pro tvorbu elektronického podpisu. Instalace na jiném PC nelze provést.
- Před zahájením tvorby žádosti o certifikát provedeme kontrolu svého přihlášení k PC (jaký uživatelský účet používáme, zda máte v rámci tohoto účtu dostatečná oprávnění) .
- Pro řádné vytvoření naší žádosti je třeba vyplnit všechny povinné položky. Ve formuláři jsou označeny hvězdičkami. Žádost vyplňujte podle platného občanského průkazu. Veškeré údaje, které v žádosti uvedeme budou na kontaktním pracovišti I.CA na základě jeho předložení kontrolovány. Chybně vyplněná žádost nebude kontaktním pracovištěm I.CA přijata ke zpracování.
- Pro správnou tvorbu žádosti o certifikát je nutné, nainstalovat aplikaci" I.CA Enroll ", která nám zajistí správné vytvoření žádosti.



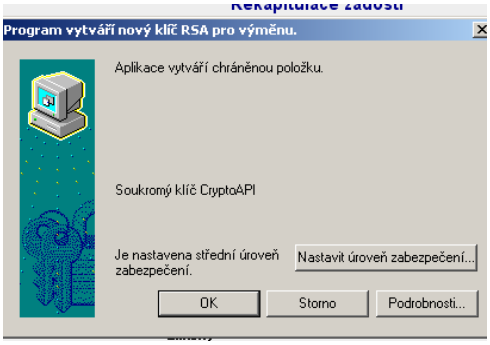
Obr. č. 10 - Aplikace I.CA Enrol

Pokud jsme na toto pamatovali, přistoupíme na vyplnění on-line formuláře.



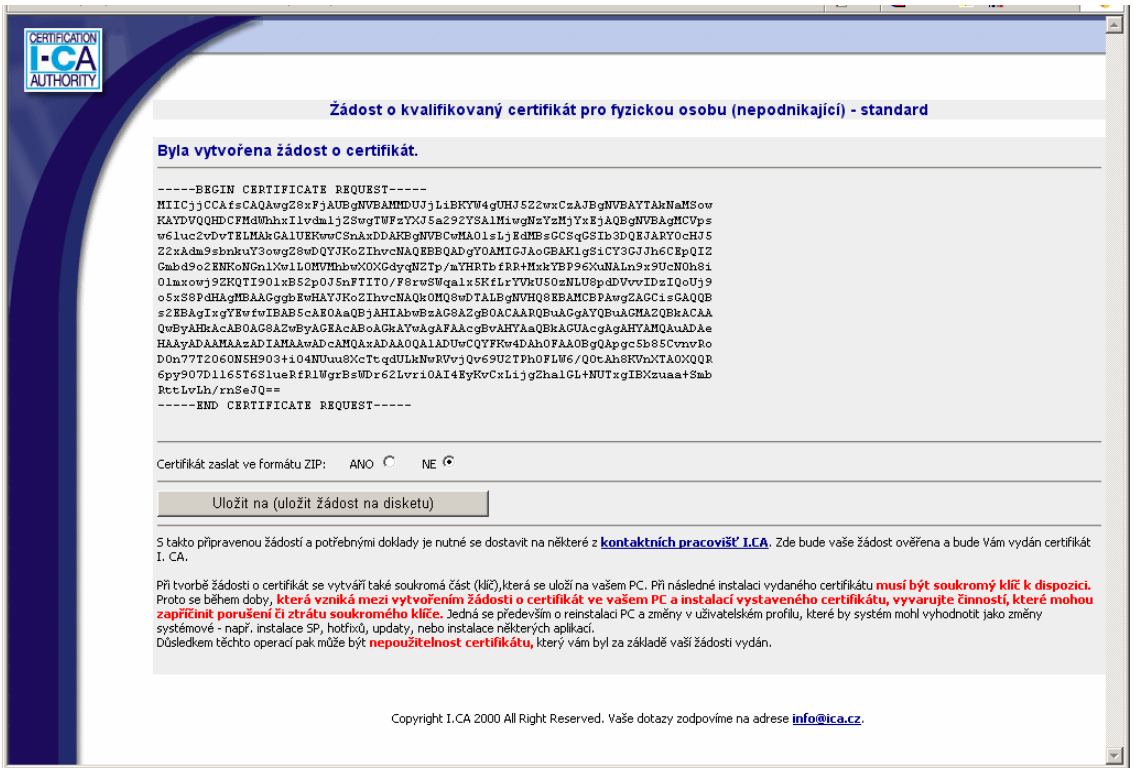
Obr. č. 11 - Žádost o certifikát

Po vyplnění žádosti se proklikáme okny, která nás informují o vytváření klíče RSA a zvolíte si úroveň zabezpečení pro budoucí certifikát .



Obr. č. 12 - Úroveň zabezpečení

Pokud je žádost formálně v pořádku vytvoří se konečná podoba elektronické žádosti, kterou je nutné si nahrát na disketu a poté sní navštívit sní pracoviště registrační autority.



Obr. č. 13 - Konečná podoba žádosti o certifikát

c)Návštěva kontaktního pracoviště I.CA (Registrační autorita)

S disketou s vygenerovanou žádostí o certifikát se navštíví nejbližší kontaktní místo I.CA. Kontaktní místa I.CA jsou umístěna na pobočkách Československé obchodní banky, a.s. Tam se prokáže identita za pomoci dvou osobních dokladů (v mém případě to byl občanský a řidičský průkaz). Abychom mohli komunikovat s institucemi, jako např. MPSV, ČSSZ a ÚP je nutné požádat o „Identifikátor MPSV“, který označuje jedinečnou identifikaci klienta vůči MPSV, ČSSZ a ÚP. Požádat je třeba přímo na pracovišti registrační autority před podáním žádosti o certifikát. Když je vše v pořádku, obě strany podepíší smlouvy, žádost o vydání certifikátu a na závěr protokol o vydání certifikátu a po zaplacení (cena kvalifikovaného certifikátu je 752,- Kč) nám je vydána disketa s vygenerovaným certifikátem. Kompletní odbavení, které proběhlo na kontaktním místě ve Zlíně, v pobočce ČSOB na ulici Dlouhé, trvalo asi 25 minut.

d) Instalace kvalifikovaného certifikátu do našeho systému.

Po návštěvě kontaktního místa obdržíme na disketě následující soubory:

9A910D.der - certifikát č. 9A910D ve formátu X509 a kódování DER

9A910D.pem - certifikát č. 9A910D ve formátu X509 a kódování PEM

9A910D.p7c - certifikát č. 9A910D ve formátu PKCS#7 a kódování DER

9A910D.pk7 - certifikát č. 9A910D ve formátu PKCS#7 a kódování PEM

9A910D.txt - textový výpis certifikátu č. 9A910D

cert_ca.der - kořenový certifikát I.CA ve formátu X509 a kódování DER ve formátu X509 a kódování DER

cert_ca.pem - kořenový certifikát I.CA ve formátu X509 a kódování PEM

cert_ca.txt - textový výpis kořenového certifikátu I.CA

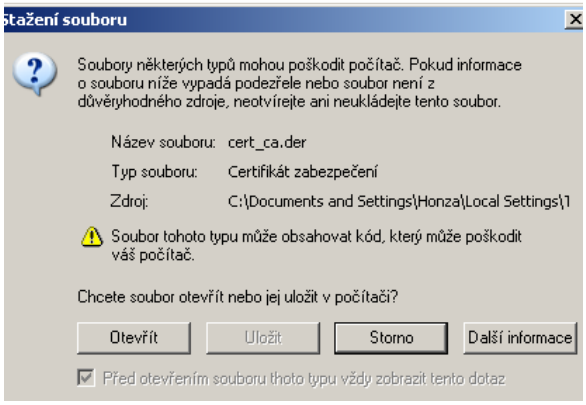
9A910D.htm - HTML stránka pro instalaci certifikátu do MS Windows

cp_qc.pdf - certifikační politika I.CA pro kvalifikovaný certifikáty ve formátu PDF

popis.txt - tento soubor

Tyto soubory také obdržíme e-mailovou zprávou pod názvem "Osobní Certifikát" dále ještě k tomu "Certifikát Certifikační autority I.CA" a "CRL" (Seznam zneplatněných certifikátů).

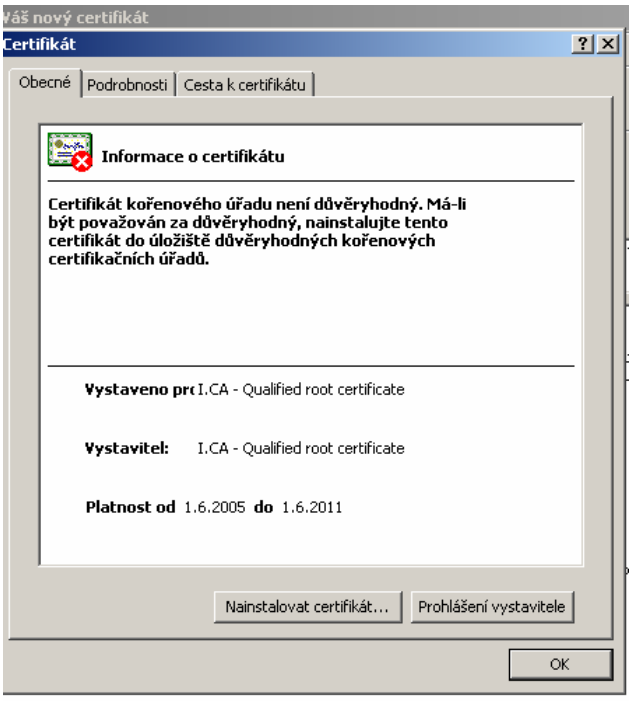
Instalaci certifikátu je nutné provádět na stejném počítači, na kterém došlo k vygenerování klíčů a žádosti certifikát.Před zahájením samotné instalace kvalifikovaného certifikátu je nutné pro jeho správné fungování nainstalovat příslušný certifikát pro poskytování kvalifikovaných služeb I.CA. Instalace proběhne spuštěním přiloženého souboru cert_ca.der, a zvolením možnosti "Otevřít".



Obr. č. 14 - Certifikát zabezpečení

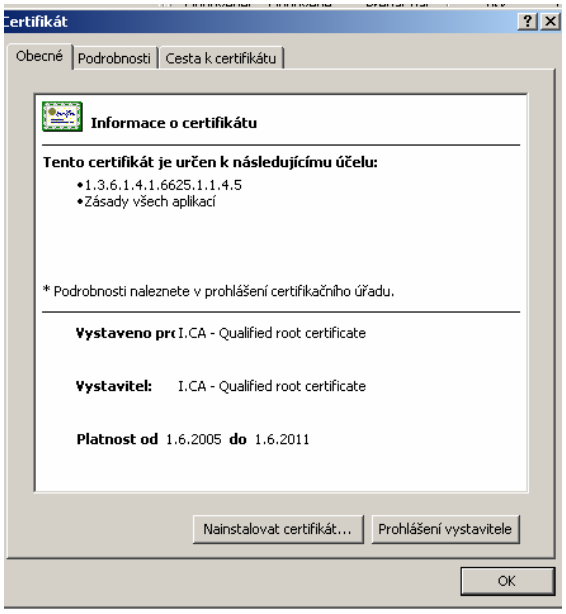
Pokud jsme tento krok učinili, můžete zahájit instalaci kvalifikovaného certifikátu dle následujícího popisu. Pro instalaci osobního certifikátu do www prohlížeče nebo e-mailového klienta klikneme na přiložený soubor 10129677.htm. a zvolíme možnost "Otevřít". Pokud import proběhl v pořádku, došlo ke spojení certifikátu a soukromého klíče, který byl vytvořen při generování žádosti o certifikát. To zjistíme jednoduše tak, že se zobrazí nainstalovaný certifikát a v dolní části okna se bude nacházet text „Máte soukromý klíč...“

Proto, aby se náš certifikát jevil jako důvěryhodný, musí se ještě nainstalovat příslušné certifikáty samotné CA, protože právě ona je podepsána pod naším certifikátem.



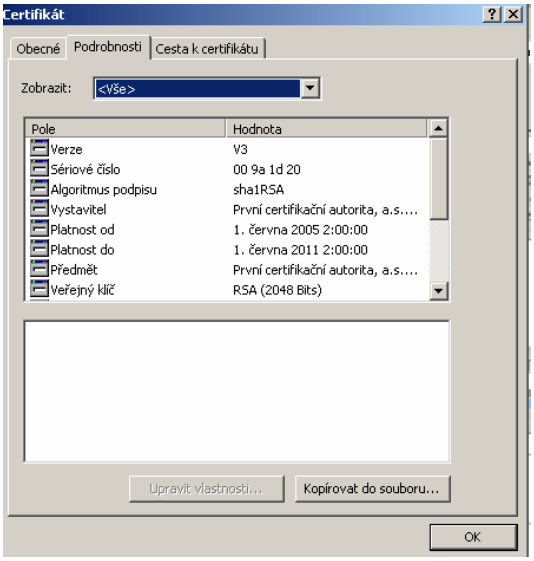
Obr. č. 15 - Informace o certifikátu

Po provedení instalace těchto certifikátů bude náš kompletní osobní certifikát vypadat takto:



Obr. č. 16 - Úspěšně nainstalovaný certifikát

Pokud si zobrazíme podrobnosti certifikátu, dočteme se zde několik důležitých informací o tomto certifikátu, jako např. kdo ho vystavitel, algoritmus podpisu, veřejný klíč a jeho délku, platnost od – do, komu byl certifikát vystaven, použití klíče, otisk veřejného klíče atd.



Obr. č. 17 - Certifikát - podrobnosti

Na závěr po provedení instalace certifikátu, ještě provedeme za zálohování certifikátu a dat pro tvorbu digitálního podpisu.

Součástí každého certifikátu je nenahraditelný soukromý klíč, který je uložen v počítači. Dojde-li k jeho ztrátě, nebudeme pomocí certifikátu nadále moci odesílat podepsanou poštu nebo číst zašifrované zprávy, proto je užitečné vytvořit si záložní kopii certifikátu pro případ, že dojde k poškození nebo ztrátě souboru, jež obsahuje zmíněný prostředek. Chceme-li vytvořit záložní kopii certifikátu, spustíme aplikaci Internet Explorer, klepneme na nabídku **Zobrazit** a pak zvolíme příkaz **Možnosti sítě Internet**. Klepneme na kartu **Obsah** a pak na tlačítko **Osobní.** Tlačítka **Importovat** a **Exportova**t na této stránce nám umožňují spravovat certifikáty.

8.2 Podepisování e-mailu v prostředí Outlook Expres

S certifikátem I.CA můžeme odesílat zabezpečenou elektronickou poštu. Tato funkce aplikace Outlook Express zabezpečuje ochranu naší komunikace v síti Internet dvěma způsoby : pomocí digitálních podpisů a šifrování.

Pomocí digitálních podpisů můžete podepisovat zprávy elektronické pošty certifikátem, které zaručuje příjemci zprávy, že jejím odesílatelem jste skutečně vy a že zpráva nebyla během přenosu poškozena.

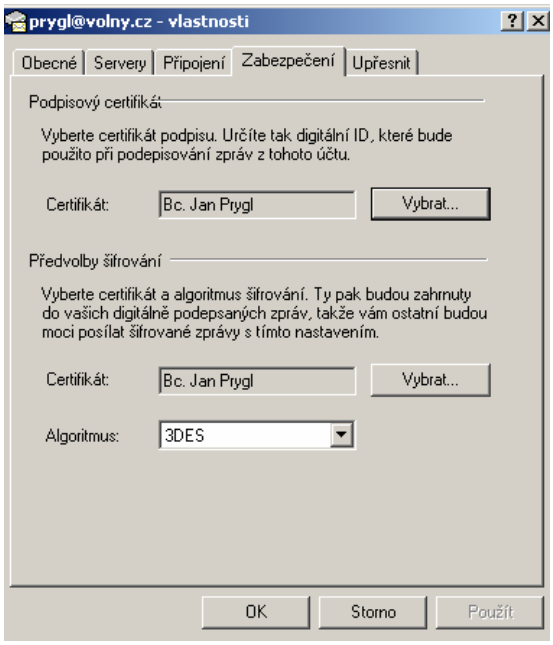
Šifrování odesílané elektronické pošty zajišťuje, že obsah zprávy nemůže během přenosu přečíst žádný jiný uživatel než její příjemce.

Aplikace Outlook Express používá normu S/MIME a ostatní uživatelé mohou číst vámi napsanou elektronickou poštu pomocí programů, které podporují tuto technologii. My můžeme naopak číst zprávy dalších uživatelů, pokud byly vytvořeny pomocí programů podporujících technologii S/MIME. Aplikace Outlook Express má vestavěnou zabezpečenou poštu a nabízí jednoduché uživatelské prostředí.

Než začnete odesílat podepsanou poštu, musíte svůj certifikát přidružit k poštovnímu účtu, se kterým jej chcete používat. V Outlooku ve volbě **Nástroje** si zvolíme příkaz **Účty**. Vyberte účet, se kterým chcete používat certifikát, klepneme na tlačítko **Vlastnost**i a dále na **Zabezpečení**. Zvolíme certifikát, který chceme přidružit k tomuto účtu. (Zobrazí se pouze ty certifikáty, které mají stejné elektronické adresy, jako je elektronická adresa

účtu.) Tuto volbu provedeme jak pro **podpis** (tj.vyberete digitální certifikát, který bude použit pro podepisování zpráv z tohoto účtu), tak i pro **šifrován**í. Zde si můžeme vybrat i algoritmus, pomocí kterého budou naše zprávy šifrovány (doporučuje se 3 DES).

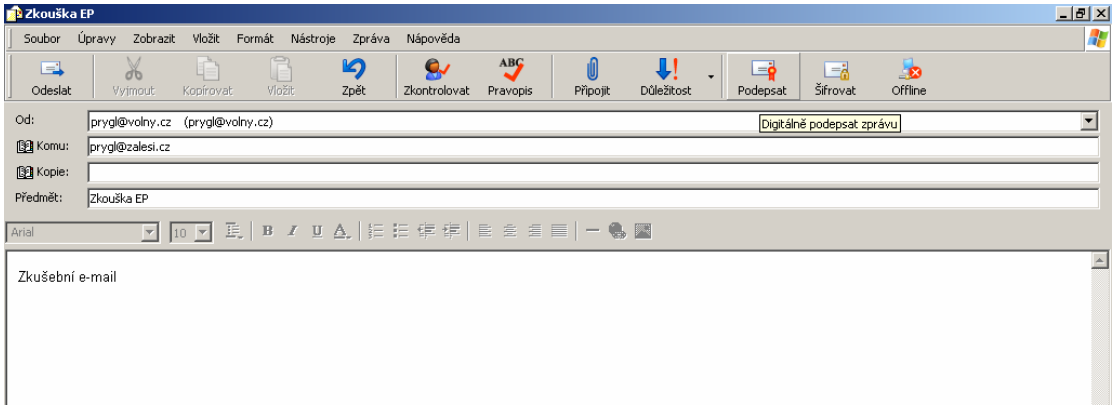
V programech Microsoftu se digitálním certifikátům říká **digitální ID.**



Obr. č. 18 - Vlastnosti účtu

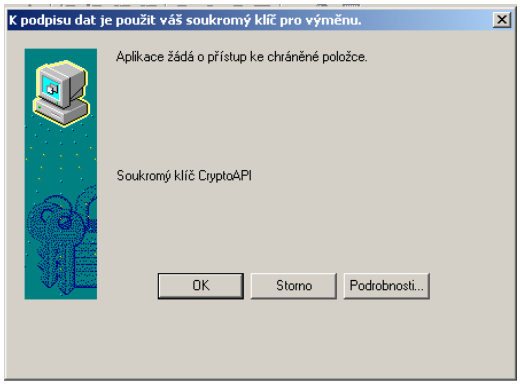
8.3 Odesílaní digitálně podepsané zprávy

Jakmile máme certifikát přidružen k poštovnímu účtu, tak nic nebrání tomu, abychom mohli podepisovat e-maily. Práce s elektronickým podpisem je v prostředí Outlook Express jednoduchá. Po vytvoření požadovaného e-mailu zvolíme možnost podepsat, jak ukazuje obrázek. Digitálně podepsaná zpráva není zprávou zašifrovanou. Digitálně podepsaná zpráva umožňuje příjemci ověřit naši totožnost, ale jde "otevřená". Jestliže zprávu navíc zašifrujete, znemožníme tím ostatním uživatelům, aby si ji během přenosu přečetli.



Obr. č. 19 - Podepisování e-mailu v Outlook Express

Vždy při podepisování se objeví dialogové okno obr. č. 20, když dáme OK proběhnou kryptografické operace, které zajistí použití soukromého klíče na hash e-mailu a připojení výsledných dat k emailu.Po dokončení kryptografických operací je podepsaný e-mail odeslán.

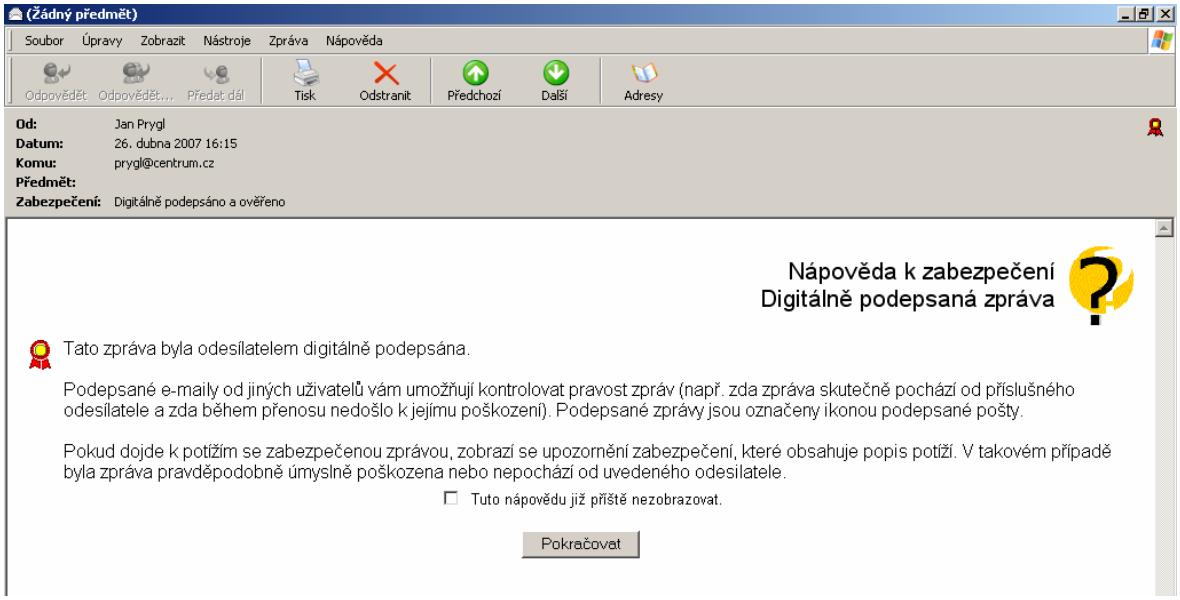


Obr. č. 20 - Upozornění na použití soukromého klíče

8.4 Příjem podepsané pošty

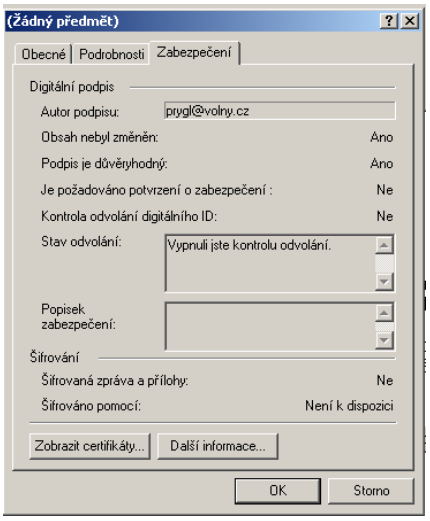
Podepsaná elektronická pošta od jiných uživatelů nám umožňuje kontrolovat věrohodnost zprávy (např. zda zprávu skutečně odeslal uvedený odesílatel či zda nebyla poškozena během přenosu). Podepsané elektronické zprávy jsou označeny speciální ikonou. Problémy s přijatou podepsanou elektronickou poštou mohou znamenat, že zpráva byla poškozena

nebo nepochází od uvedeného odesílatele. Na obrázku můžeme vidět podepsaný příchozí e-mail.



Obr. č. 21 - Přijatá podepsaná e-mailová pošta

Po otevření zprávy a kliknutí v pravém horním rohu na ikonku pečeti se zobrazí informace o platném certifikátu. To však pouze v případě, že mám nainstalované všechny příslušné certifikáty (jak certifikáty dané CA, tak certifikát odesílatele). Pokud tyto certifikáty nejsou nainstalované, jeví se podepsaný email jako nedůvěryhodný, a méně zkušený příjemce si může myslet, že email je nějak poškozen či byl zkompromitován. Některé poštovní aplikace dokonce nepovolí email otevřít, dokud se nenastaví důvěryhodnost odesílatele či nenainstalují dané certifikáty. Proto je potřeba své okolí alespoň okrajově seznámit s touto problematikou a popsat postup nainstalování si potřebných certifikátů. Jak můžeme vidět, kompletní ověření elektronického podpisu za uživatele vykoná program.



Obr. č. 22 - Informace o podpisu

8.5 Odesílání zašifrované pošty

Šifrování elektronické pošty zabraňuje dalším uživatelům číst zprávy během přenosu. Pokud chcete šifrovat elektronickou poštu, musíte mít k dispozici certifikát uživatele, kterému zprávu odesíláme. Necháme si tedy poslat od osoby, s kterou budeme komunikovat digitálně podepsanou zprávu. Tuto zprávu otevřeme, stiskneme pravé tlačítko myši, zvolíme položku **Přidat do Adresáře** a dále potvrdíme tlačítkem OK.

Kdykoli, potom budeme chtít nějakému příjemci něco zašifrovat, vybereme adresu z kontaktů, kam jsme si ji takto uložili (i s jeho veřejným klíčem) a v horní liště zvolíme ikonu **Šifrovat**.

8.6 Příjem zašifrované pošty

Aplikace Outlook provádí automatické dešifrování elektronických zpráv za předpokladu, že máme v počítači nainstalován správný certifikát. Pokud chceme, aby nám ostatní uživatelé mohli posílat zašifrovanou poštu, musejí mít k dispozici náš certifikát. Pokud jej chceme poslat, jednoduše odešleme digitálně podepsanou poštu a aplikace Outlook automaticky zahrne náš certifikát.

8.7 Změna statutu důvěryhodnosti digitálního certifikátu

Přidáme-li do Adresáře certifikát dalšího uživatele, bude mu přidělen statut, který označuje, zda důvěřujeme jednotlivci, skupině, či společnosti, jíž byl certifikát vydán. Pokud nás vlastník příslušného certifikátu upozorní, že má podezření, že soukromý klíč certifikátu byl narušen, bude zřejmě nezbytné změnit jeho statut na Výslovně nedůvěřovat. Další informace nalezneme v rejstříku nápovědy aplikace Outlook pod heslem Statut důvěryhodnosti certifikátu.

ZÁVĚR

Cílem diplomové práce bylo podat ucelený přehled o problematice a využití elektronického podpisu a zmapovat současný stav na trhu poskytovatelů certifikačních služeb v České republice. Komplexnost diplomové práce spočívá v podání teoretických základů, kterým se věnují kapitoly jedna až čtyři, tedy technologické aspekty, legislativní rámec a typy ele-ktronických podpisů, doplněných o analytickou část, kterou representují kapitoly pět až osm, tedy využití elektronického podpisu v praxi, srovnání certifikačních autorit, popis vlastních zkušeností s pořizováním Certifikátu u I.CA, jeho instalací a používáním v aplikaci Outlook Expres.

V části, která se zabývá technologickými aspekty elektronického podpisu jsem popsal několik nejužívanějších šifrovacích metod a algoritmů, jejich aplikaci a především základní princip bezpečné komunikace. Podle mého názoru zabezpečení a délka v současné době používaných klíčů je dostačující (kombinace šifrovacího algoritmu RSA a hashování funkce SHA-1). Ale tím, že se kryptografie stále vyvíjí a zlepšuje, zlepšují se také možnosti na prolomení šifer. To by do budoucna mohlo být určité nebezpečí.

Ve třetí kapitole jsem svoji pozornost obrátil na legislativu týkající se elektronického podpisu. Prošel jsem všechny zákony, vyhlášky a nařízení, které se k elektronickému podpisu vztahují. Legislativa zabývající se elektronickém podpisu prošla do této doby řadou novelizací. Osobně si myslím, že v současné době je situace okolo legislativní stránky elektronického podpisu stabilní. Žádná další novela zákona o elektronickém podpisu se nepřipravuje a tento zákon již reguluje všechno co regulovat má.

Čtvrtá kapitola popisuje jednotlivé typy elektronických podpisů a odlišnosti mezi nimi. Rozdíly mezi jednotlivými typy jsou zřejmé z tabulek, v kterých jsou uvedeny parametry jednotlivých podpisů. Tato kapitola by měla přispět k správnému pochopení termínu elektronický podpis.

V analytické části nejdříve popisuji využití elektronického podpisu v praxi a analyzuji trh v České republice. Zde jsem se ve větší míře zaměřil na komunikaci se státní správou a zdravotními pojišťovnami což jsou dle mého názoru oblasti, (když opomenu elektronické bankovnictví, kde každá banka využívá své vlastní aplikace) ve kterých, běžný občan může elektronický podpis využít nejvíce. Tím, že se cena kvalifikovaného certifikátu, diky CA PostSignum , snížila na 190 Kč se elektronický podpis stává dosažitelný pro širší

okruh veřejnosti a tím mže dojít i k jeho většímu rozšíření. K většímu rozšíření by určitě přispělo i to kdyby se např. velké bankovní domy rozhodly pro akceptaci zákonem uznávaného elektronickému podpisu.

Analytická část pokračuje kapitolou věnovanou poskytovatelům certifikačních služeb. Tady se zaměřuji na principy jejich fungování, certifikační politiku, autoritu časové značky a akceptování jednotlivých typů certifikátů. Zásadní částí této kapitoly je srovnání jednotlivých certifikačních autorit podle kritérií, která jsem si určil jako relevantní pro jejich hodnocení. Podle těchto kritérií jsem sestavil tabulky, ve kterých jsou jasně a přehledně formulovány parametry jednotlivých certifikačních autorit. Při hodnocení jsem vycházel především z certifikačních politik a webových stránek společností. Podle vybraných parametrů jsem určil jako vítěze První certifikační autoritu a. s., která byla akreditována v ČR jako první a má nejširší nabídku svých služeb i když jistou nevýhodou může být cena certifikátu, která je vyšší. V těsném závěsu za ní je CA PostSignum České pošty o, které si myslím, že by mohl být časem takovou štikou trhu, s přijatelnou cenou a velkým pokrytím. Díky velké síti svých poboček, ale za předpokladu, že se ji podaří rozšířit své služby.

Osmá kapitola popsuje mé vlastní zkušenosti s pořizováním, instalací a podepisováním pošty certifikátu u I.CA certfikační agentury, jeho instalací a podepisováním elektronické pošty v Outlook Express. Tento postup může sloužit jako návod všem, kteří v budoucnu budou chtít zažádat o podobný certifikát nebo pouze pro seznámení se všemi formalitami při pořizování certifikátu.

Přínos mé práce spočívá v praktických zkušenostech s elektronickým podpisem, v podání uceleného přehledu o elektronickém podpisu a především v analytické části , ve které se zaměřuji na zhodnocení současných možností využití elektronického podpisu v praxi a analyzuji možné příčiny, jejichž odstranění by mohlo směřovat k jeho dalšímu rozvoji.

Conclusion

The aim of my diploma work was to give a comprehensive survey about the issue, usage of electronic signature and giving a present situation in the marketplace of provider's certification services in the Czech Republic. There is also the roundness of my diploma because it consists presenting theoretical principles in chapters one to four, e.g. technological aspects, legislative frame and types of electronic signatures, supplemented with analytical part in chapters five to eight, then practical usage of electronic signature, comparing certification authorities, description of personal experience with obtaining the I.CA certificate, its installation and using in Outlook Express application.

In the part that deals with technological aspects of electronic signature I described the most common coding methods and algorithms, their application and especially the essential principles of safe communication. In my opinion security and longitude of used keys are sufficient nowadays (combination of coding algorithm RSA and hash function SHA- 1). But because the coding is developing and innovating all the time, the possibilities of coding breakthrough are innovating too. It could be a danger in the future.

The third chapter is about legislature of electronic signature. I studied all laws, public notices and orders that are about the electronic signature. Legislature about electronic signature was revised many times. Personally I think the situation about legislative side of electronic signature is fixed nowadays. No other amendment of act about electronic signature is preparing and this law already regulates all that it should regulate.

The fourth chapter describes all types of electronic signatures and their differences. Differences are evident from tables, where characteristics of single signatures are mentioned. This chapter should help to understand the idea of electronic signature.

In analytical part I describe the usage of electronic signature practically and analyze the market in the Czech Republic. I aimed my survey to the communication with offices and health insurance companies. In my opinion these are the areas (when I leave out an electronic banking, where every bank benefits from his personal application) in which common citizen is able to use electronic signature the most. Thanks to CA Post Signum the price of qualified certificate was lowered to 190 Kc per electronic signature. This makes it available for a wider group of public and it is possible to make it even larger. A

bigger enlargement would certainly help if e.g .big banking - houses decided to accept law electronic signature.

The analytical part continues with chapter about the providers of certification services. There is a survey about principles of their behaviour, certification policy, authority of time brands and accepting the single types certificates. The most important in this chapter is comparing each single certification authorities according to factors which I used for their evaluation. According to these factors I drew up the tables, in which characteristics of single certification authorities are set up brightly. During evaluation I used certification characteristics and web pages about companies. According to choice of parameters I established the winner, the First certification authority a.s., which was the first an accredited representative in CR and has the widest offer in its services. The certain disadvantage is higher price of certificate. In tight hangings behind there is CA PostSignum. I think it could be with acceptable price and big coverage, big deal in the future, thanks to their wide spread branches. They should also extend their services

The Eighth chapter describes my own experience with using, installation and signing the post with I.CA certificate agency, its installation and signing electronic post in Outlook Express. This progress could be used as an instruction to all, who would like to apply for similar certificate or only for familiarization with all formalities for certificate in future.

The benefit of my work is in practical experiences with electronic signature, presented as an comprehensive survey about electronic signature. And especially in an analytical part there is an evaluation of contemporary possibilities and usage of electronic signature practically, analyzing possible cause and their taking out, which could help in their further development.

SEZNAM POUŽITÉ LITERATURY

[1] Bosáková, D.; Kučerová, A.; Peca, J.; Vondruška, P.; *Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů;* Nakladatelství ANAG, Olomouc 2002, 141 s., ISBN 80-7263-125-X

[2] Peterka, J.: Co je elektronický podpis, [on-line]. [cit. 2007-03-11]. Dostupný z WWW: < http://www.earchiv.cz/b00/b0405001.php3?print=1 >

. [3] Zákon č.486/2004 Sb. (227/2000 Sb.): Úplné znění zákona č. 227/2000 Sb.,o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn [online]. Dostupný z: <http://www.crypto-world.info/pravo/podpis/pravo/486_04.htm >

[4] Zákon č.486/2004 Sb. (227/2000 Sb.): Úplné znění zákona č. 227/2000 Sb.,o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn. § 2 [online]. [cit. 2007-03-20].

Dostupný z:http://www.crypto-world.info/pravo/podpis/pravo/486_04.htm

[5] Vyhláška č.366/2001 Sb.: Vyhláška ÚOOÚ ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu Dostupný z: http://www.crypto-world.info/pravo/podpis/pravo/v_366_2001.pdf

[6] Vyhláška č.366/2001 Sb**.:** Vyhláška ÚOOÚ ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu § 2 [online]. [cit. 2007-03-20]. Dostupný z: http://www.crypto-world.info/pravo/podpis/pravo/v_366_2001.pdf

[7] ica.cz–slovník pojmů [on-line].

Dostupný z www : <http://www.ica.cz/home_cs/?acc=slovnik_pojmu >

[8] I.CA.cz – Teorie symetrické a asymetrické kryptografie [online]. Dostupný z: <http://www.ica.cz/home_cs/?acc=teorie_symetricke_a_asymetricke_kryptografie

[9] Louženský, L. Kryptografie [online]. [cit. 2007-04-01].

Dostupný z: < http://biosoup.wz.cz/prg/krypto.htm>

[10] Pinkava, J.: Moderní kryptografické algoritmy pro elektronický podpis [online]. Dostupný z WWW: < http://crypto-world.info/pinkava/konference/cack.pdf >

[11] Šifrovací algoritmus RSA [online]. [cit. 2007-04-01].Dostupný z WWW:

< http://www.specialista.info/view.php?cisloclanku=2006032201 >

[12] Pinkava, J.: Úvod do kryptologie [online].

Dostupný z WWW: < http://crypto-world.info/pinkava/uvod/uvod98.pdf>

[13] Pinkava, J.: EU a E-podpis, legislativa a normy [online]. [cit. 2007-04-05]. Dostupný z WWW: < http://crypto-world.info/pinkava/konference/tatry.pdf >

[14] Zákon č.227/2000 Sb. Sbírka zákonů České republiky ,částka 68, Zákon č.227 ze dne 29.června 2000 o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), [online]. [cit.2007-03-20] Dostupný z:

<http://www.mvcr.cz/sbirka/2000/sb068-00.pdf>

[15] Hobza, J.: Elektronický podpis. Crypto world č.10, 2002, [online]. [cit. 2007-04-01]. Dostupný z: < http://crypto-world.info/casop4/crypto10_02.pdf>

[16] Nařízení vlády č. 304/2001, kterým se provádí zákon č. 227/2000 Sb. Sbírka zákonů České republiky, částka 117,[online]. Dostupný z: <http://www.mvcr.cz/sbirka/2001/sb117-01.pdf>

[17] Lér, M.: E-podpisy České pošty [online]. [cit. 2007-04-04]. Dostupný z WWW: < http://www.lupa.cz/clanky/e-podpisy-ceske-posty-lek-pro-cesky-e-goverment/ >

[18] Peterka, J.: Elektronický podpis, verze 2.0 [online]. [cit. 2007-04-12]. Dostupný z WWW: http://www.earchiv.cz/b03/b0822001.php3

[19] Vyhláška č. 496 /2004 Sb. o elektronických podatelnách, Sbírka zákonů České Republiky, částka 171/2004 Sb. [online]. Dostupný z :

<http://www.crypto-world.info/pravo/podpis/pravo/496_04.htm>

[20] Nařízení vlády č. 495/2004, kterým se provádí zákon č. 227/2000 Sb.,o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. Sbírka předpisů České republiky, částka 171/2004 Sb. Dostupný z WWW :

<http://www.crypto-world.info/pravo/podpis/pravo/495_04.htm>

[21] Webové stránky Ministerstva práce a sociálních věcí [online]. Dostupný z WWW: <http://portal.mpsv.cz/forms>,

[22] Webové stránky Ministerstva práce a sociálních věcí, formuláře státní sociální podpory, elektronický podpis [online]. Dostupný z WWW: <http://forms.mpsv.cz/sspforms/Zabezpeceni.jsp?L=cs>

[23] Webové stránky Ministerstva financí [online]. Dostupný z WWW: <http://adis.mfcr.cz/adis/jepo/>,

[24] Webové stránky Rejstřík trestů Praha [online]. Dostupný z WWW: <http://portal.justice.cz/soud/soud.aspx?o=203&j=213&k=2027>,

[25] Statistika elektronických podání pro ČSSZ [online]. Dostupný z WWW: <http://www.micr.cz/images/dokumenty/E-podani_20060715.pdf>

[26] Webové stránky Česká správa sociálního zabezpečení, Elektronický podpis, [online]. Dostupný z WWW: <http://www.cssz.cz/osvc/prehled/elektronicky_podpis.asp>,

[27] Portál VZP ČR, Všeobecné informace [online]. Dostupný z WWW:

< http://www.vzp.cz/cms/internet/cz/Vseobecne/Portal/ >

[28] Portál VZP ČR, Podporované certifikáty [online]. Dostupný z WWW:

< http://www.vzp.cz/cms/internet/cz/Vseobecne/Portal/Certifikaty/ >

[29] Webové stránky HZP, Elektronická přepážka, [online]. Dostupný z WWW:

< http://www.hzp.cz/prepazka/>

[30] Webové stránky portál zdravotních pojišťoven [online]. Dostupný z WWW:

< http://www.portalzp.cz/>

[31] Webové stránky I.CA [online]. Dostupný z WWW:

< http://www.ica.cz/home_cs/>

[32] Hrabalová, M.: Použití elektronického podpisu v praxi, [online]. [cit. 2007-04-20]. Dostupný z WWW:
<http://archiv.cw.cz/cwarchiv.nsf/clanky/3A549C2A534D78EDC1256EBC0035F0F8?OpenDocument>

[33] Vondruška, P.; Elektronický podpis. Elektronický podpis, 41 stran, Informace a komunikace, Řízení místních orgánů, březen 2002 , RAABE.

[34] Webové stránky CA PostSignum [online]. Dostupné z WWW:

< http://www.postsignum.cz//>

[35] Webové stránky CA identity a.s [online]. Dostupné z WWW:

< https://www.eidentity.cz/app/>

[36] Webové stránky Czechia s.r.o [online]. Dostupné z WWW:

< http://www.ca-czechia.cz/>

[37] Peterka, J.: eIdentity, podpis a věda mimo zákon, článek z eArchívu J. Peterky [online]. [cit. 2007-04-06]. Dostupný z WWW:

< http://www.earchiv.cz/b05/b1017001.php3>

[38] Webové stránky Ministerstva informatiky [online]. Dostupný z WWW: http://e-
<trziste.micr.cz/images/statistiky/epodpis.pdf>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

I.CA	První Certifikační Autorita, a.s.
A2A	Administration-to-Administration
A2B	Administration-to-Business
A2C	Administration-to-Customer
AČZ	Autorita časové značky
B2A	Business-to-Administration
B2B	Business to Business
B2C	Business to Consumer
C2A	Customer-to-Administration
C2B	Customer-to-Business
C2C	Customer-to-Customer
CA	Certifikační autorita
CRL	Seznam zneplatněných certifikátů
ČR	Česká republika
DPH	Daň z přidané hodnoty
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EESSI	European Electronic Signature Standardization Initiative
EP	Elektronický podpis
ES	Evropské společenství
ETSI	Electronic Signatures and Infrastructures
EU	Evropská unie
MD5	Message Digest 5
MPSV	Ministerstvo práce a sociálních věcí

MRA	Mobilní registrační autorita
POP3	Post Office Protocol version 3
QCA	Vydávající certifikační autorita
QSC	Kvalifikovaný systémový certifikát
RA	Registrační autorita
RCA	Kořenová certifikační autorita
RIPEMD-160	Hashovací algoritmus, délka hashe 160 bitů
RQS	Kořenový kvalifikovaný systémový certifikát
RSA	Rivest – Shamir – Adelman,
SHA-1	Secure Hash Algorithm
SMTP	Simple Mail Tranfer Protocol
SSL	Secure Sockets Layer
USB	Universal Serial Bus
ÚOOÚ	Úřad na ochranu osobních údajů
VCA	Veřejná certifikační autorita
WWW	World Wibe Web
ZoEP	Zákon o elektronickém podpisu č. 486/2004 Sb

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘÍLOHA Č.1 K VYHLÁŠCE Č. 366/2001 SB.

Kryptografické algoritmy a jejich parametry 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.

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Metoda určená pro padding	Hašovací funkce
1	RS	MinModLen=1020	emsa-pkcs #1-v1.5	SHA
2	RS	MinModLen=1020	emsa-pss	SHA
3	RS	MinModLen=1020	emsa-pkcs #1-v1.5	RIPEMD160
4	RS	MinModLen=1020	emsa-pss	RIPEMD160
5	DSA	pMinLen=1024 qMinLen=160	-	SHA 1
6	ECDSA-Fp	qMinLen=160 r0Min=10^4 MinClass=200	-	SHA 1
7	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	-	SHA 1
8	RS	MinModLen=1020	emsa-pkcs #1-v1.5	MD
9	RS	MinModLen=1020	emsa-pss	MD

Tab. č. 15 - Podpisová schémata

Na přílohu č. 1 se odkazuje v §2 odst. 2 písm. b) vyhlášky. Příloha obsahuje údaje, které určují požadavky na vlastnosti 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 poskytovatelem vydán kvalifikovaný certifikát. Příloha obsahuje konkrétní kryptografické algoritmy a jejich parametry, které musí být pro tato data použity. Ve všech případech se jedná se o standardní asymetrické algoritmy RSA, DSA a ECDSA. Z důvodu bezpečnosti se stanoví minimální parametry pro klíče (modul) těchto funkcí. K dosažení kvality těchto parametrů je nutné nainstalovat podporu pro tzv.silnou kryptografii. Jako hašovací funkce se povolují SHA-1, RIPEMD-160 a MD 5. [1]

PŘÍLOHA P II : PŘÍLOHA Č.2 K VYHLÁŠCE Č. 366/2001 SB.

Kryptografické algoritmy a jejich parametry pro vytváření párových dat poskytovatele a pro prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu.

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus pro generování klíčů	Metoda určená pro padding	Hašovací funkce
1	RSA	MinModLen=1020	rsagen1	emsa-pkcs#l-vl.5	SHA1
2	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
3	RSA	MinModLen=1020	rsagen1	emsa-pkcs#l-vl.5	RIPEMD160
4	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
5	DSA	pMinLen=1024	dsagen1	-	SHA1
6	ECDSA-Fp	qMinLen=160 r0Min=10^4	ecgen1	-	SHA1
7	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4	ecgen1	-	SHA1

Tab. č. 16 - Podpisová schémata

Označení generátoru klíčů	Používané označení	Asymetrický algoritmus	Metoda generování náhodných čísel	Parametry náhodného generátoru
4.I	rsagen1	RSA	trueran	EntropyBits>128
4.II	dsagen1	DSA	trueran nebo pseuran (FIPS 186-2)	EntropyBits>128 nebo SeedLen>128
4.III	ecgen1	ECDSA-F_p nebo ECDSA-F2"[1]	trueran nebo pseuran	EntropyBits>128 nebo SeedLen>128

Tab. č. 17 - Algoritmy pro generování klíčů

Označení náhodného generátoru	Používané označení	Parametry náhodného generátoru
5.I	trueran	EntropyBits
5.I I	pseura n	SeedLen
5.I II	FIPS 186-2- 31	SeedLen
5.I V	FIPS 186-2- 32	SeedLen

Tab. č. 18 - Metody generování náhodných čísel

Na přílohu č. 2 vyhláška odkazuje na dvou místech textu. Poprvé je na ni odkazováno v§5 odst. 2 vyhlášky v souvislosti s vytvářením párových dat poskytovatele a podruhé v §7 odst. 2 vyhlášky v souvislosti s kryptografickými algoritmy prostředku pro bezpečné vytváření elektronického podpisu. Tato příloha byla vytvořena na základě publikovaného doporučení EESSI. Toto doporučení – dokument Algorithms and Parameters for Secure Electronic Signatures - v době přípravy vyhlášky existovalo pouze v návrhu (draft V 1.44, ze 4.5.2001). V říjnu 2001 byl tento dokument nahrazen verzí 2.1. Oproti verzi 1.44 došlo jen k nepatrným změnám. Byly doplněny algoritmy pro speciální verzi asymetrických šifer-německou verzi ECDSA nazývanou ECGDSA (Elliptic Curve German Digital Signatuře Algorithm). Byl rovněž upraven požadavek na generátor klíčů pro RSA. Kromě používání „trueran" generátoru (fyzikální generátor) bylo povoleno používat i „pseuran" (pseudonáhodný generátor). Zatímco první změna je z hlediska právní úpravy přijaté v České republice nepodstatná, druhá změna znamená, že posuzování generátorů se v České republice uskutečňuje podle „přísnějších" požadavků, než je tomu v členských státech Evropské unie. Lze předpokládat, že v případě novelizace vyhlášky budou požadavky pro posuzování generátorů odpovídat požadavkům, podle nichž se při hodnocení postupuje v členských státech Evropské unie. V případě nejasnosti ve výkladu některých ve vyhlášce uvedených pojmů se doporučuje prostudovat dokument Algorithms and Parameters for Secure Electronic Signatures, kde jsou jednotlivé pojmy přesně a vysvětleny.[1]

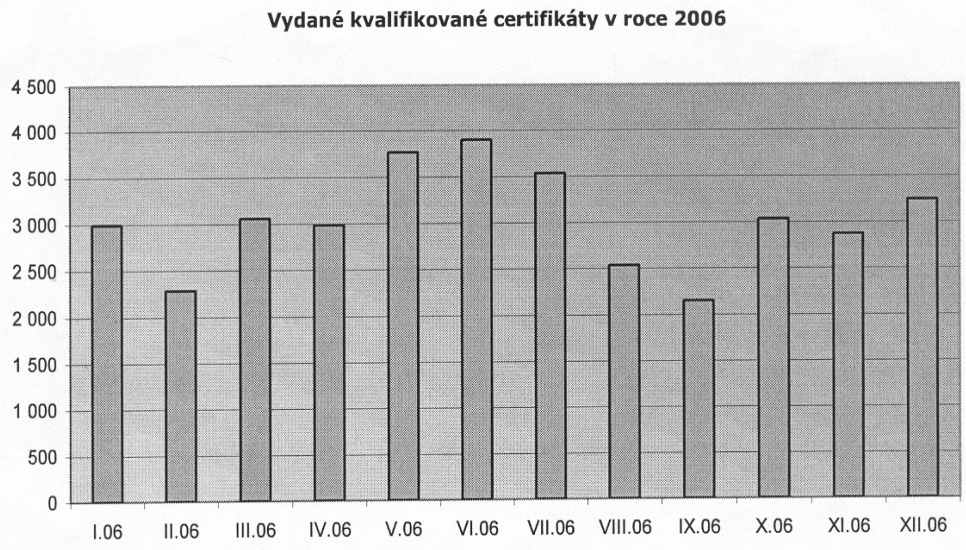
PŘÍLOHA P III : VYDANÉ KVALIFIKOVANÉ CERTIFIKÁTY V ROCE 2006

V současné době jsou v ČR tři subjekty, které působí jako akreditovaný poskytovatel certifikačních služeb po splnění všech podmínek daných zákonem č. 227/2000 Sb., o elektronickém podpisu, a to První certifikační autorita, a.s., Česká pošta, s.p.– PostSignumQCA a eIdentity, a.s. První certifikační autorita a.s. pak jako jediná společnost vydává od března 2006 i kvalifikovaná časová razítka.

Za rok 2006 bylo těmito subjekty vydáno celkem 36 356 kvalifikovaných certifikátů a 3 420 614 kvalifikovaných časových razítek. K 31. prosinci 2006 je registrováno v ČR celkem 35 050 platných kvalifikovaných certifikátů.

Následující grafy ukazují souhrnný počet vydaných a aktivních kvalifikovaných certifikátů a počet vydaných časových razítek v roce 2006.

Graf 1: Vydané kvalifikované certifikáty v roce 2006 - podle měsíců



Obr. č. 23 - Vydané kvalifikované certifikáty v roce 2006

[38]