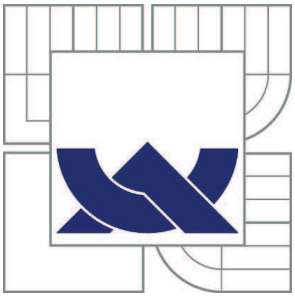


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF MANAGEMENT

BEZPEČNOST ELEKTRONICKÉHO OBCHODU

SAFETY OF E-COMMERCE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MARTIN JONÁŠ
AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. JIŘÍ DVOŘÁK, DrSc.
SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/2010
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jonáš Martin, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Bezpečnost elektronického obchodu

v anglickém jazyce:

Safety of E-commerce

Pokyny pro vypracování:

Úvod
Systémové vymezení problému
Cíl práce
Přehled informačních zdrojů světa
Použité metody řešení problému
Současný stav řešené problematiky
Analýza problému
Návrh řešení
Zhodnocení návrhu řešení
Závěr
Seznam použitých informačních zdrojů
Přílohy

Seznam odborné literatury:

LANCE,James. Phishing bez záhad. Praha : Computer Press, 2007. 281 s. ISBN 978-80-247-1766-1.
MLNEK, Jaroslav. Zabezpečení obchodních informací. 1.vyd. Praha : Grada 2007. 154 s. ISBN 978-80-251-1511-4.
PIPER, Frederic. Kryptografie. 2.vyd. Praha : Grada 2006. 157 s. ISBN 80-7363-074-5.
SEDLEK,J. E-komerce, internet a mobil marketing od A do Z.1.vyd. Praha : Grada 2006. 351 s. ISBN 80-7300-195-0.
VADLENKA,Libor. Elektronické obchodování. Praha : Computer Press, 2007. 163 s. ISBN 978-80-86530-40-6.

Vedoucí diplomové práce: prof. Ing. Jiří Dvořák, DrSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2009/2010.

L.S.

PhDr. Martina Rašticová, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA

V Brně, dne 24.05.2010

Abstrakt

Diplomová práce vyjadřuje bezpečnostní funkce informačního systému, popis elektronických podpisů a certifikačních autorit. Dále je zaměřená na získání, zprovoznění a použití elektronického podpisu.

Abstract

Master´s thesis is supposed to formulation safety of information system functions, description of elktronic signature and certificion authority. Next is oriented at conversion, launching and application of elektronic signature.

Klíčová slova

bezpečnost, elektronický podpis, důvěrnost, autentizace, soukromí

Keywords

safeness, electronic signature, intimacy, autentization, privacy

JONÁŠ, M. *Bezpečnost elektronického obchodu.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 62 s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně.Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 27. května 2010

Poděkování

Rád bych poděkoval svému vedoucímu diplomové práce, panu prof. Ing. Jiřímu Dvořákovi, DrSc. za odborné vedení a cenné rady, které mi pomohly ke zdárnému vytvoření této práce.

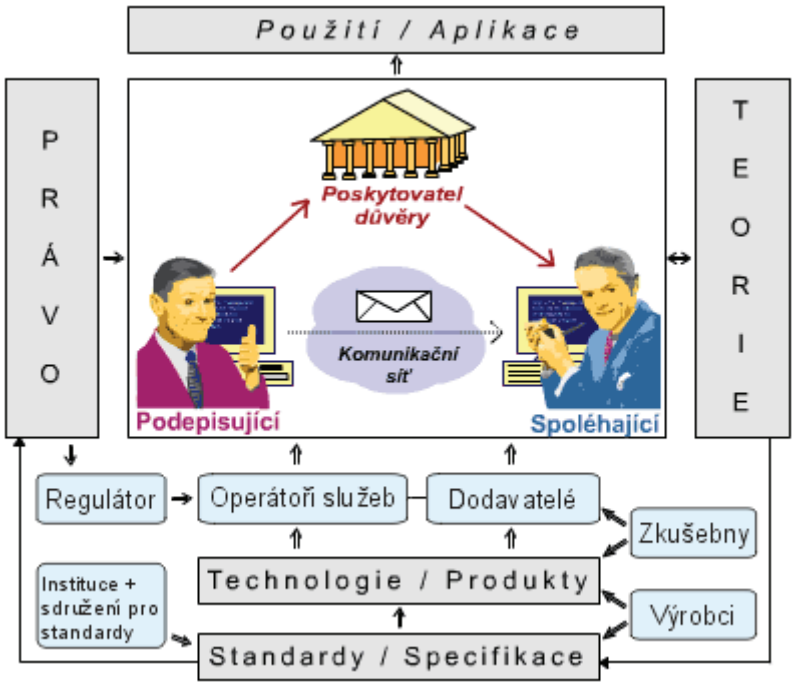
Obsah

Úvod

Diplomovou práci mám zaměřenou na stále aktuálnější téma a to je elektronický obchod a s tím související elektronický podpis. V poslední době stále narůstá požadavek o zřízení elektronického podpisu a člověk by se měl zorientovat, jaký je pro konkrétní osobu nebo firmu nejvhodnější, k čemu mu bude sloužit a jaká důvěra v něj bude vkládána. Dále se musí také brát v potaz cena pořízení elektronického podpisu, nároky na hardware a software a složitost jeho instalace.

1. Systémové vymezení problému

Bezpečnost elektronického obchodu a elektronického podpisu popisuje následující obrázek, na celou problematiku působí technické a i teoretické aspekty.



Obrázek 1: Systémové vyjádření problému

Zdroj: (2)

Jedná se o podepisujícího a spoléhajícího, mezi kterými probíhá elektronická komunikace po komunikační síti. Vychází se z teoretických východisek a musí se dodržovat platné právní normy a standardy . Standardy / Specifikace vydávají instituce a sdružení pro standardy.

Výrobci za použití vyvinutých technologií vyrobí produkty pro koncového uživatele. Předtím, než se daný výrobek dostane na trh projde zkušebnami a potom je teprve předán dodavatelům. Dodavatelé a operátoři služeb poskytují tento výrobek zákazníkovi.

Každý kdo si pořídí elektronický podpis je zapsán u poskytovatele důvěry. Podepisující odesílá svou elektronicky podepsanou zprávu příjemci a ten po obdržení si podpis u tohoto poskytovatele ověří, zda je podpis platný.

2. Cíl práce

Cílem této diplomové práce je zhodnocení složitosti pořízení a zprovoznění elektronického podpisu. Dále se zaměřím na srovnání ceny elektronického podpisu s možnostmi jeho využití.

3. Přehled informačních zdrojů

3.1 Přednášky

K mému tématu diplomové práce bezpečnost internetového obchodu se mi hodily přednášky od doc. Ing. Daniel Cvrček, Ph.D., s kterým jsme měli ve druhém ročníku předmět Kryptografie a informační bezpečnost. Využil jsem především poznámek z přednášek. Dále mi byly přínosem přednášky z předmětu Elektronický obchod, které vedl prof. Ing. Jiří Dvořák, DrSc.

3.2 Skripta

K bezpečnosti elektronického obchodu jsem čerpal ze skript v které jsou vystaveny na www.buslab.org v elektronické podobě. Jsou to studijní materiály z předmětů vyučovaných na Fakultě informatiky a Přírodovědecké fakultě MU v Brně, dále také na Fakultě informačních technologií a Podnikatelské fakultě VUT v Brně. Čerpal jsem převážně z předmětů Bezpečnost informačních systémů, Bezpečnost a kryptografie, Kryptografie a informační bezpečnost, Ochrana dat a informačního soukromí, Kryptografie.

3.3 Internet

Převážně z internetu jsem čerpal informace k elektronickým podpisům. Vyhledal jsem zde i ceny jednotlivých druhů elektronických podpisů, co je třeba k zprovoznění elektronického podpisu a v jakém sledu mám postupovat k úspěšnému pořízení elektronického podpisu.

3.4 Knihy

Mým hlavním tištěným zdrojem je kniha od KLANDER, Lars. *Hacker Proof : váš počítač, vaše síť a vaše připojení na Internet - Je to opravdu bezpečné?* a dále pak od ŠILHÁNEK, Radim: *Bezpečnostní aspekty elektronického obchodu*.

4. Použité metody řešení problému a současný stav řešené problematiky

Souhrn elektronických podpisů na trhu v České republice od nejjednoduššího až po nejsložitější.

Tabulka 1: Analýza současného stavu

Elektronický podpis – General Electronic Signature	Takovýto "podpis" nemá pro příjemce příliš velkou vypovídací hodnotu. Důvěra v takto vytvořený podpis je minimální
Zaručený elektronický podpis – Advanced Electronic Signature	Zaručený elektronický podpis musí podle zákona o elektronickém podpisu. 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.
Zaručený elektronický podpis založený na kvalifikovaném certifikátu - Electronic Signature Using Qualified Certificate	Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu. Identifikuje odesílající osobu.
Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb	Je v zásadě obdobou zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Jediný rozdíl spočívá v tom, že certifikát je vydán akreditovaným poskytovatelem certifikačních služeb. Vyšší úroveň důvěry v něj.
Kvalifikovaný podpis -	Je zde požadavek na použití prostředku pro

Qualified Electronic Signature	bezpečné vytváření podpisu. Je z hlediska důvěry nejdokonalejší
Vylepšený elektronický podpis – Enhanced Electronic Signature	Od předchozího typu liší přidáním některého z požadavků (např. časová značka)
Kvalifikovaný podpis určený pro archivaci dat - Qualified Electronic Signature with Long-term Validity	Je zde požadavek na časové razítko. Je zde vznesen požadavek zvýšené bezpečnosti.
Časové razítko – time stamp	Lze přidat k elektronicky podepsané datové zprávě a stvrzuje, že datová zpráva existovala dříve, než k ní bylo toto razítko přidáno
Digitální podpis	Obvykle je to zaručený elektronický podpis založený na kvalifikovaném certifikátu.

Zdroj: vlastní

5. Analýza problému

5.1 Bezpečnostní funkce informačního systému

Bezpečnostními funkcemi informačního systému organizace rozumíme takové funkce, které naplňují požadavky udržení důvěrnosti, integrity, dostupnosti, autenticity, nepopiratelnosti a konečně spolehlivosti informací a služeb tímto systémem poskytovaných (tedy zejména datové báze), a to na předem nadefinované úrovni. Jednotlivé bezpečnostní funkce jsou zajišťovány dílčími bezpečnostními technikami a technologiemi

Tabulka 2: Definice

Bezpečnostní funkce	Definice
Důvěrnost (confidentiality)	Důvěrností rozumíme utajení některých skutečností (resp. dat) před neautorizovanými třetími osobami. Narušení této funkce je jednou ze základních hrozeb pro informační systém podniku. Zajištění této funkce potom znamená zajištění přístupu pouze pro autorizované subjekty.
Integrita (Integrity)	Integritou rozumíme skutečnost, že data mohou být modifikována pouze autorizovanými subjekty. Ztrátou integrity potom rozumíme modifikaci dat subjektem neautorizovaným.
Autentizace (Autentization)	Autentizací rozumíme ověřitelnost totožnosti subjektu, který vystupuje v jisté transakci.
Nepopiratelnost, neodmítnutelnost (Non-repudiation)	Nepopiratelnost souvisí se zajištěním požadavku, aby subjekt nemohl v budoucnu popřít jím realizované kroky a snažit se tím zbavit svých vlastních závazků.
Dostupnost (Availability)	Tato bezpečnostní funkce znamená, že aktiva jsou autorizovaným subjektům k dispozici pouze s minimálním zpožděním.
Vedení evidence (Auditing)	Monitoring činnosti systému umožňuje odhalit útoky na systém dodatečně, pokud nebyl dostupný mechanismus jejich odhalení v okamžiku útoku.

Spolehlivost (Reliability)	Spolehlivostí systému rozumíme konzistenci zamýšleného a skutečného stavu celého systému.
Soukromí (Privacy)	Neodmyslitelnou součástí bezpečnosti každého informačního systému je zajištění soukromí jeho uživatelů, což je do jisté míry v rozporu s naplňováním jednotlivých bezpečnostních funkcí. Proto je vždy nutno při řešení jednotlivých bezpečnostních funkcí nadefinovat, do jaké míry bude poškozeno lidské soukromí.

Zdroj: vlastní

5.1.1 Důvěrnost

Při přenosech dat je základním prostředkem pro zajištění důvěrnosti dat šifrování. K ochraně dat uložených v počítačových systémech se vhodně kombinují metody fyzického a logického zabezpečení. Především se jedná o řízení přístupu uživatelů k datům včetně fyzické bezpečnosti a šifrování uložených dat. Vzhledem k výkonovým vlastnostem šifrovacích algoritmů jsou používány především šifry symetrického typu (DES, RC2, RC4, RC6, Blowfish, Skipjack apod.). Celá řada kryptosystémů je dostupná i formou freewaru na webových stránkách různých vývojářských firem.

5.1.2 Integrita

Podobně jako v případě důvěrnosti může být zajištění integrity rozděleno na zajištění jejich integrity při přenosu a při jejich uložení. V případě uložení dat se využívá zejména řízení přístupu uživatelů pomocí hesel, v případě přenosu dat se využívá právě *elektronického podpisu* (tedy kombinace tzv. hashovací jednocestné funkce - MD5, SHA-1 - a asymetrického šifrovacího algoritmu, jako např. RSA, Diffie-Hellman apod.).

5.1.3 Autentizace

Obecně existují tři způsoby realizace autentizace – uživatel buď něco ví (heslo nebo tajný klíč), něco vlastní (magnetická či čipová karta) nebo něčím je (biometrické metody – otisky prstů, sítnice). Pro zajištění bezpečnosti a především v neinteraktivních systémech se využívá opět zejména technologie elektronických podpisů a digitálních certifikátů.

5.1.4 Nepopiratelnost

K zajištění nepopiratelnosti se používají *elektronické podpisy*. Samotný elektronický podpis však ke splnění požadavku nepopiratelnosti nestačí. Aby byla tato vlastnost zajištěna, pak musí mít strana, která ji vyžaduje, k dispozici průkazní materiál (NRI – Non Repudiation Information). NRI se vztahuje k subjektu i ke zprávě, proto je její součástí digitální podpis, který autentizuje jednoznačně původce zprávy i příslušnou zprávu. Vedle struktury se také digitální podpis a NRI liší v době vzniku a době obvyklého použití. Samotný digitální podpis je obvykle kontrolován okamžitě, zatímco u NRI je důležitá možnost kontroly i za několik let. Podstatná je v tomto případě nepopiratelnost původu (původce dat poskytuje NRI spolu s daty a pokud příjemce obdrží data bez NRI, pak musí tato data považovat za nedůvěryhodná a jako taková je odmítnout) a nepopiratelnost přijetí/doručení (zde se vyskytuje problém v případě, že se komunikace účastní pouze dva subjekty – příjemce potom může informaci přijmout, ale může odmítnout zaslat NRI. Bez existence třetí strany je pak možné pouze nevynucené poskytnutí NRI příjemcem zprávy).

5.1.5 Dostupnost

Dostupnost služeb a dat souvisí bezprostředně s volbou spolehlivého systému, který navíc umožňuje spolehlivé zálohování jak dat, tak i funkčních částí systému. Pro zajištění této bezpečnostní funkce se používají různé zálohovací utility a zálohovací zařízení.

5.1.6 Vedení evidence

Některé systémy (například systémy elektronického obchodu) by měly být schopny uchovávat jisté informace. Otázka doby uložení těchto informací by pak měla vyplývat hlavně ze zákonných norem – například ze zákona o elektronickém podpisu. Tuto bezpečnostní funkci naplňují svou existencí různé protokolovací a archivační nástroje.

5.1.7 Spolehlivost dat

Základem pro zajištění spolehlivosti dat je existence důvěryhodných třetích stran (tzv. trusted third party, TTP), které poskytují certifikát, v němž potvrzují platnost a správnost příslušných informací. Otázka však vzniká v případě, jaký druh informací může TTP potvrdit

z hlediska správnosti. Bezproblémová je zejména certifikace faktografických údajů, například v rámci certifikátu X.509, kdy certifikát potvrzuje, že vlastníkem daného veřejného klíče je jistá konkrétní osoba.

5.1.8 Soukromí a anonymita

Základem pro zajištění anonymity subjektu je použití pseudonymů při vzájemné interakci. Častost používání jistého pseudonymu však musí být regulována, aby nebylo možno rozpoznat identitu uživatele podle naakumulovaných dat. Použití pseudonymů však musí být podpořeno užitím technologií které jejich užití umožňují. Typickým příkladem je systém elektronických plateb DIgiCash e-cash. (7)

5.2 Elektronický podpis a certifikační autorita

Druhů 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. Liší se i technologií, na níž jsou založeny – kryptografické, biometrické aj.

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 číslo 227/2000 Sb., účinnost k 1.10.2000) v souladu. Dále se problematikou elektronického podpisu zabývá řada standardizačních organizací – např. ETSI, CEN, EESSI a NIST.

5.2.1 Elektronický podpis – General Electronic Signature

Elektronickým podpisem rozumíme 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.

Takovýto “podpis” nemá pro příjemce příliš velkou vypovídací hodnotu. Důvěra v takto vytvořený podpis je minimální – tato úroveň podpisu slouží spíše pro informaci

příjemce. Příkladem může být na klávesnici napsaný “podpis” vložený pod klasický e-mail, ale i např. jméno autora uvedené v záhlaví článku vytvořeného pomocí některého ze známých textových editorů (např. MS Word). Lze však dovodit, že "elektronický podpis" výše uvedeného typu může být i např. jméno autora e-mailu, pokud je uvedeno v e-mail adrese. Ačkoli by tedy autor dokumentu (či obecně nějaké datové zprávy) mohl tvrdit, že dokument nepodepsal, mohl by jeho příjemce na základě výše uvedeného výkladu tvrdit pravý opak.

Požadavky na tuto kategorii elektronického podpisu jsou minimální. Nepožaduje se časové razítko, není definován žádný formát nebo standard, který by popisoval tvar vytvořených nebo předávaných dat. Není použit certifikát nebo jiný způsob zveřejnění pomocných dat (dat pro ověření podpisu – tedy veřejného klíče osoby, zveřejnění dat pro určení identity) ani nejsou tato data definována. Nejsou kladeny žádné specifické požadavky na použitý systém nebo podpisový prostředek (prostředek pro ověření podpisu se nedefinuje).

5.2.2 Zaručený elektronický podpis – Advanced Electronic Signature

Zaručený elektronický podpis musí podle zákona o elektronickém podpisu (jež je, v souladu s evropskými normami) musí splňovat 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). Nově se zavádí přesné formáty pro vytváření a přenos elektronických podpisů. Toto je nutné především z hlediska kompatibility a interoperability. 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 podpisuje. Nejsou kladeny žádné specifické požadavky na podpisový prostředek nebo ověřovací prostředek. Bezpečnost těchto prostředků (použití, zabezpečení, ochrana) se zcela nechává na podepisující se o sobě (případně na osobě, která se spoléhá na 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 předem na takovéto komunikaci dohodnou. Příjemce musí od podepisující se osoby získat důvěryhodným způsobem její data sloužící k ověření zaručeného elektronického podpisu (její veřejný klíč). Ani tento druh podpisu však neslouží k „anonymnímu“ styku, tedy ke styku odesilatele a univerzálního příjemce. Příkladem komunikace, ke které může být tento druh podpisu využit, může být komunikace klient – banka či obchodník – zákazník. Patří sem i využívání celosvětově známého programu PGP (který však je schopen i implementace elektronického podpisu založeného na kvalifikovaném certifikátu).

Na příkladě zaručeného elektronického podpisu je již možné vysvětlit obecný princip elektronického podpisu, který budeme v dalším textu v souvislosti s výkladem dalších druhů elektronického podpisu rozšiřovat o požadavky kladené na ostatní (pokročilejší) druhy elektronického podpisu. Procedura je tedy následující:

Na straně podepisující osoby se z napsané zprávy pomocí vzorkovací (hash) funkce vytvoří tzv. otisk zprávy (message digest). Označme jej pro další výklad jako HASH 1. Na vstupu hashovací funkce může být libovolná a libovolně dlouhá datová zpráva, na jejím výstupu je otisk, který má pevnou délku 128 nebo 160 bitů (první údaj platí pro hashovací funkci MD5, druhý pro SHA-1).

Máme tedy vytvořen otisk napsané zprávy. Ten se šifruje pomocí námi zvoleného asymetrického algoritmu soukromým klíčem odesilatele. Získaný výsledek je zaručeným elektronickým podpisem, který je ke zprávě připojen. Zpráva samotná může být v případě potřeby též šifrována (veřejným klíčem příjemce).

Na straně příjemce zprávy se k otevřenému textu vypočte hash, který označme jako HASH 2. Z digitálního podpisu se pomocí veřejného klíče osoby, která zprávu podepsala, získá hodnota HASH 1, která by se měla rovnat hodnotě HASH 2. Pokud jsou hodnoty HASH

1 a HASH 2 shodné, máme jistotu, že zpráva nebyla cestou změněna a že zprávu podepsala osoba, které přísluší data pro vytváření elektronického podpisu, neboť jen ta mohla z HASH 1 vytvořit digitální podpis.

Zaručené elektronické podpisy jsou založeny na matematických a kryptografických metodách (postupech), jejichž znalost není na straně uživatele předpokladem běžného používání těchto technologií. Předpokládá se, že v budoucnu bude elektronický podpis založen i na dalších metodách, například biometrických charakteristikách člověka - otisku prstu, obrazu oční sítnice, zvuku hlasu, biometrické charakteristice podpisu aj.

Zaručené elektronické podpisy jsou elektronickým protějškem ručně psaných podpisů. Jsou to dlouhá a složitě generovaná čísla, která vypočítává buď procesor nebo čipová karta. K výpočtu těchto podpisů je zapotřebí výše zmíněná dvojice klíčů. Privátním klíčem, ke kterému nemá přístup nikdo kromě vlastníka (neboť bývá uložen na čipové kartě nebo v počítači a je chráněn heslem), lze zprávu podepsat. Důležité je, že vygenerovaný digitální podpis (jako zmíněné číslo) závisí na každém bitu podepisované zprávy. Protože by však při aplikaci na zprávu jako takovou byl zaručený elektronický podpis neúměrně dlouhý, využívají se vzorkovací funkce (viz předchozí odstavec). Po vytvoření vzorku je pak podepsán vzorek a nikoli celá zpráva.

Soukromý a veřejný klíč i certifikát může mít uživatel zaznamenán na libovolném nosiči - disketě, čipové kartě, speciálním konektoru obsahujícím elektronické obvody apod. Rovněž je možné, aby tyto údaje potřebné pro elektronické podepisování byly na čipové kartě používané jako osobní doklad nebo na SIM-kartě nové generace v mobilním telefonu.

5.2.3 Zaručený elektronický podpis založený na kvalifikovaném certifikátu

K použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu se zavádí pojem certifikátu, kvalifikovaného certifikátu a pojem poskytovatele certifikačních služeb. Poskytovatelé certifikačních služeb se dělí na poskytovatele, kteří vydávají certifikáty, na poskytovatele, kteří vydávají kvalifikované certifikáty a na akreditované poskytovatele certifikačních služeb.

Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu. Jedná se o datovou zprávu, která spojuje data pro ověřování podpisů (tedy veřejný klíč podepisující osoby) s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují. Jinak řečeno, identifikuje odesílající osobu. Kvalifikovaným certifikátem se zpravidla rozumí certifikát, který má náležitosti stanovené příslušným zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty.

Poskytovatelem certifikačních služeb se rozumí subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.

Akreditovaným poskytovatelem certifikačních služeb je poskytovatel certifikačních služeb, jemuž zpravidla byla udělena akreditace podle příslušného zákona. Akreditovaný poskytovatel certifikačních služeb by měl být chápán jako důvěryhodný poskytovatel těchto služeb.
Procedura podepisování zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vypadá asi následovně. První tři kroky se nijak neliší od procedury podepisování zaručeným elektronickým podpisem

Na straně podepisující osoby se z napsané zprávy pomocí vzorkovací (hash) funkce vytvoří tzv. otisk zprávy (message digest). Označme jej pro další výklad jako HASH 1. Na vstupu hashovací funkce může být libovolná a libovolně dlouhá datová zpráva, na jejím výstupu je otisk, který má pevnou délku 128 nebo 160 bitů (první údaj platí pro hashovací funkci MD5, druhý pro SHA-1).

Máme tedy vytvořen otisk napsané zprávy. Ten se šifruje pomocí námi zvoleného asymetrického algoritmu soukromým klíčem odesilatele. Získaný výsledek je zaručeným elektronickým podpisem, který je ke zprávě připojen.

Na straně příjemce zprávy se k otevřenému textu vypočte hash, který označme jako HASH 2. Z digitálního podpisu se pomocí veřejného klíče osoby, která zprávu podepsala, získá hodnota HASH 1, která by se měla rovnat hodnotě HASH 2. Pokud jsou hodnoty HASH 1 a HASH 2 shodné, máme jistotu, že zpráva nebyla cestou změněna a že zprávu podepsala

osoba, které přísluší data pro vytváření elektronického podpisu, neboť jen ta mohla z HASH 1 vytvořit digitální podpis. Poznamenejme, že veřejný klíč odesílatele získáme z jeho digitálního certifikátu, který máme uložen v příslušném adresáři, ke kterému má poštovní klient přístup.

Naproti tomu je procedura rozšířena o další krok, který se vřadí do výše zmíněné posloupnosti mezi kroky 2 a 3:

Schází však ještě ujištění o tom, že máme správnou informaci o fyzické osobě, ke které se veřejný klíč (neboli tzv. data pro ověřování elektronického podpisu) a tedy i soukromý klíč (neboli tzv. data pro vytváření elektronického podpisu) vztahují, tedy informaci o tom, kdo se elektronicky podepsal. K tomu potřebujeme, aby někdo dostatečně důvěryhodný byl schopen potvrdit - tato data pro ověřování elektronického podpisu patří osobě X.Y. a jsou "do páru" s daty pro vytváření elektronického podpisu, která tato osoba X.Y. vlastní. Takové tvrzení v praxi představuje právě certifikát vydaný poskytovatelem certifikačních služeb, který se k zaručenému elektronickému podpisu připojí a zašle spolu s ním.

Ne vždy však procedura podepisování vypadá tak, jak jsme ji právě popsali. Většina běžně užívaných aplikací sice zasílá certifikát zároveň s elektronicky podepsanou zprávou, ale pokud tomu tak není, musí podepisující osoba oznámit, kde je její certifikát dostupný. Zpravidla se jedná o server poskytovatele, který certifikát vydal, nebo webovou stránku podepisující osoby.

K ověření platnosti certifikátu podepisující osoby je nutným předpokladem důvěra v poskytovatele, který jej vydal. Máme-li důvěru v poskytovatele, pak nainstalujeme do svého software jeho certifikát (odlišujme certifikát poskytovatele a certifikát podepisující osoby), čímž vyjádříme danému poskytovateli (a tím i podepisující osobě) důvěru .

Pokud jsme obdrželi elektronicky podepsanou zprávu a zároveň certifikát podepisující osoby (případně jsme certifikát získali jiným způsobem), ověříme, zda certifikát podepisující osoby vydal poskytovatel uvedený v certifikátu a zda tento certifikát nebyl od okamžiku jeho vydání změněn. Toto ověření zajistí sama aplikace, a to ověřením elektronického podpisu poskytovatele, který je na certifikátu podepisující osoby.

Následně zjišťujeme, zda byl certifikát podepisující osoby platný v době, kdy byla zpráva podepsána. Přímo v certifikátu je uveden počátek a konec doby platnosti certifikátu (platnost od … do…). V průběhu této doby však mohla být ukončena platnost certifikátu. Zda se tak nestalo, je nutné ověřit u poskytovatele v seznamu zneplatněných certifikátů.

Vždy je třeba počítat s určitým prodlením, které nastane mezi dobou, kdy držitel certifikátu požádá o ukončení platnosti svého certifikátu, a dobou, kdy je informace o zneplatnění certifikátu zveřejněna v CRL, resp. je vydán nový, aktualizovaný seznam zneplatněných certifikátů. Z technického hlediska je velmi obtížné, aby mezi těmito dvěma akcemi nebyla určitá časová prodleva. Proto je třeba se u poskytovatele informovat, jak dlouhá tato prodleva u něj je. Podle obsahu elektronicky podepsané zprávy je pak třeba zvážit, zda tento obsah budeme akceptovat až poté, kdy uplyne doba, kterou poskytovatel potřebuje ke zveřejnění nového seznamu zneplatněných certifikátů. Například pokud obdržíme zprávu se závažným obsahem a víme, že poskytovatel vydává nový seznam zneplatněných certifikátů každých 24 hodin, vyčkáme s platbou oněch 24 hodin, než si ověříme, že certifikát je stále platný.

U zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu se požadavky na tuto kategorii podpisu vzhledem k předchozímu typu dále rozšiřují. Stále se ještě nevyžaduje časové razítko. 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 (žádost o vydání certifikátu apod.). Požadavek na důvěryhodnost operačního systému, ve kterém se dokument podpisuje, je stejný jako u předchozího typu.

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.

5.2.4 Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb

Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb je v zásadě obdobou zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu. Jediný rozdíl spočívá v tom, že certifikát je vydán akreditovaným poskytovatelem certifikačních služeb. Akreditovaný poskytovatel certifikačních služeb zakládá možnost širšího užití elektronického podpisu a v neposlední řadě i vyšší úroveň důvěry v něj.

5.2.5 Kvalifikovaný podpis - Qualified Electronic Signature

Kvalifikovaný podpis se od předchozího typu liší požadavkem na použití prostředku pro bezpečné vytváření podpisu. 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.

Kvalifikovaný podpis se považuje z hlediska důvěry za nejdokonalejší. 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.

5.2.6 Vylepšený elektronický podpis – Enhanced Electronic Signature

Vylepšený elektronický podpis se od předchozího typu liší přidáním některého z požadavků (např. časová značka, rozšířené požadavky na verifikaci, rozšířené požadavky na podpisový prostředek, rozšířená ochrana proti jedné konkrétní hrozbě apod).

5.2.7 Kvalifikovaný podpis určený pro archivaci dat

Nejdůležitějším typem, který vznikl jako vylepšený elektronický podpis z kvalifikovaného podpisu, je **kvalifikovaný podpis určený pro archivaci dat**. Novým základním požadavkem je pojem časového razítka. Vzhledem k tomu, že musí být zajištěna odolnost proti útokům po celou dobu archivace, je v kategorii bezpečný podpisový prostředek vznesen požadavek zvýšené bezpečnosti.

Vzhledem ke specifickým požadavkům je využití zřejmé - dlouhodobá archivace podepsaných elektronických dokumentů. V této souvislosti se připomíná, že 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.

5.2.8 Časové razítko – time stamp

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

5.2.9 Digitální podpis

Vedle pojmu elektronický podpis se v řadě dokumentů objevuje i pojem digitální podpis. Digitálním podpisem se obvykle rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu, tedy elektronický podpis založený na kryptografické technologii. Zaručeným elektronickým podpisem v širším slova smyslu se však rozumí i podpis založený na jiné technologii (například na biometrii částí lidského těla). Pojem digitální podpis je tedy užší než pojem zaručený elektronický podpis. (8)

5.3 Technologická stránka el. podpisu

5.3.1 Symetrické šifrování

Symetrické (neboli konvenční) šifrování je založeno na principu jednoho klíče, kterým lze zprávu jak zašifrovat, tak i odšifrovat. Typickým příkladem symetrické šifry je **DES** (Data Encryption Standard, tedy národní standard, založený na symetrickém algoritmu) vyvinutý v 70. letech v USA a americkou vládou také hojně používaný. Hlavní výhodou symetrických algoritmů je jejich rychlost – jejich aplikace je časově málo náročná. Na druhou stranu je nutné, aby se příjemce i odesílatel dohodli na jednom klíči, který budou znát pouze oni dva (za předpokladu, že chtějí vést zabezpečenou komunikaci). Problémem je tedy distribuce klíče - jak dostat klíč k příjemci aniž jej zachytil někdo nepovolaný? Velkou překážkou, která brání masovému rozšíření symetrické kryptografie je též potřeba vysokého počtu klíčů za předpokladu, že každá dvojice na Internetu chce uskutečňovat bezpečnou komunikaci. V tomto případě je třeba celkem n(n-1)/2 klíčů, což s sebou nese problémy jejich bezpečného uložení a správy (např pro 1000 uživatelů by bylo třeba celkem 499500 klíčů). Proto je využití symetrické kryptografie v bezpečné komunikaci bez jejího propojení s asymetrickou pouze velmi řídké. Široké využití však má symetrická kryptografie v oblasti zajišťování důvěrnosti uložených dat. Pro tyto účely má celá řada SW produktů implementovány asymetrické šifry.

Podívejme se nyní stručně na symetrické algoritmy, kterých se v praxi využívá.

V roce 1974 byl firmou IBM vyvinut algoritmus LUCIFER a stal se kandidátem na americký standard šifrování dat. Posléze v roce 1977 byl jako federální standard přijat a pojmenován DES – Data Encryption Standard. Algoritmus je blokový a šifruje 64 bitů otevřeného textu na 64 bitů šifry. Klíč je 64 bitový, ale každý osmý bit je kontrolní, tedy efektivní délka klíče je 56. Kvůli vyšší bezpečnosti byl přijat standard Triple DES (též TDES, 3DES), který jedna data protáhne algoritmem 3x. Potom je efektivní délka klíče 128 bitů. DES je jednou z nejnapadanějších šifer. I z tohoto důvodu bude nahrazen novým standardem AES (Advanced Encryption Standard).

Autorem algoritmu Blowfish je B. Schneier, který jej publikoval v roce 1993. Tento algoritmus není patentován a je volně šiřitelný. Jde o velmi rychlý, jednoduchý algoritmus, který je možno efektivně implementovat i na malých procesorech, nebo dokonce čipových kartách. Při pečlivém naprogramování se celý algoritmus včetně všech svých datových

struktur vejde do interní cache procesoru i486. Jde o blokovou šifru (šifra je tedy aplikována na jisté bloky dat, nikoli na jednotlivé datové bity) s délkou bloku 64 bitů a klíči dlouhými maximálně 448 bitů. Algoritmus je použitelný ve všech běžných pracovních modech vhodných pro blokové šifry. Míru dosažené bezpečnosti lze regulovat délkou použitého klíče. Rovněž lze omezit počet kol šifrovacího procesu.

Vývoj algoritmu CAST reagoval na neutěšenou situaci na poli šifrovacích algoritmů v polovině 90. let. DES měl v té době už svá nejlepší léta za sebou, a ostatní kvalitní šifry byly patentovány a tudíž drahé (např. IDEA, RC2, RC4). Pojmenován je po svých tvůrcích C. Adams a S. Tavares. Na Internetu byl publikován v květnu 1997 jako RFC 2144. CAST se tak stal kanadskou alternativou k americkému algoritmu Blowfish. Oproti Blowfishi měl CAST výhodu, že dostal certifikát kvality od oficiálního kanadského úřadu pro komunikaci CSE (Communication Security Establishment), používá ho Microsoft ve svých produktech a také je začleněn do známého produktu PGP (Pretty Good Privacy, jehož autorem je Phil Zimmerman). CAST umí pracovat s klíči délky 40 až 128 bitů a bloky o 64 bitech. CAST nyní představuje standard, který je velmi rozšířen a akceptován mnoha společnostmi. Akceptuje jak silné, tak slabé klíče a je velmi bezpečný. Prozatím vyplňuje mezeru, než bude vybrán nový šifrovací standard AES, který nahradí DES.

Autory algoritmu publikovaného v roce 1991 původně pod názvem IPES byli X. Lai a J. Massey. Současný název je akronymem za International Data Encryption Algorithm. **IDEA** vznikla jako vylepšená verze svého předchůdce, algoritmu PES poté, co byla publikována metoda jeho zlomení. IDEA začala úspěšně pronikat do praxe. Je implementována v rámci protokolu SSL nebo jako součást populárního PGP. Jde o blokovou šifru s délkou bloku 64 bitů, pracující s klíčem o délce 128 bitů.

Algoritmus MARS je jedním z pěti současných kandidátů na AES. Vytvořen byl v dílně IBM. Pro MARS hraje i to, že dosavadní standard DES je také z dílny IBM a to algoritmus LUCIFER (viz. DES). Podle tvůrců MARS nabízí větší bezpečnost než Triple-DES s neporovnatelnou rychlostí. Mars je šifra s délkou bloku 128 bitů a proměnlivou délkou klíče.

Tvůrcem úspěšné šifry RC4 nikdo jiný než Ronald Rivest z RSA. RC4 je jednou z nejpoužívanějších proudových šifer pro Internet a komerční využití. Po celých 7 let se RSA

dařilo utajit algoritmus RC4. Poté byla dissasemblována hackerem a její popis umístěn na Internetu. RSA dostala strach o zneužití jejich šifry konkurencí, jelikož nebyla patentována. Tato šifra je řádově 10x rychlejší než DES. Klíč pro RC4 může mít maximálně 256 bytů (2048 bitů). RC4 je velmi zajímavá a neobyčejná a analytickou metodou zatím nenapadnutá šifra. Ani teoretický základ šifry není doposud řádně prozkoumán. RC4 je využita v SSL 3.0 společnosti Netscape, v Microsoft Office, ORACLE Secure SQL nebo v Microsoft Windows 2000.

Druhý algoritmus z dílny Ronalda Rivesta z roku 1994 RC5 přinesl do kryptografie novou myšlenku o použití rotací závislých na datech. Jedná se o velmi pružný algoritmus s mnoha parametry. Šifrovací klíč má 0-255 bytů, počet kol šifrovacího procesu (0-255) a délka slova z hodnot 16, 32, 64, 128 a 256 přičemž algoritmus zpracovává bloky o dvojnásobné délce slova. Pro své použití lze algoritmus přizpůsobit vhodnou volbou parametrů. Velikost slova je rozumné volit v závislosti na velikosti slova používaného procesoru. 128 bitů je to správné číslo, chceme-li algoritmus používat pro hašování. Zvětšování počtu kol vede ke zvyšování bezpečnosti algoritmu na úkor rychlosti. Šest kol postačí pro nenáročné aplikace, 32 pro ty nejnáročnější. Jako rozumná se jeví volba délka slova 32 bitů, 12 kol, 16bytový klíč, což krátce zapíšeme RC5-32/12/16.

Algoritmus RC6 je vylepšená verze RC5, která tímto dosahuje požadavků NIST na nový standard AES. Byly přidány některé funkce - celočíselné násobení v klíči a čtyři pracovní registry místo dvou. Parametrizovaný je stejně jako RC5.

Skipjack je 64bitová symetrická šifra s 80bitovým klíčem.

Další z kandidátů na AES se nazývá Twofish. Twofish pracuje s blokem o délce 128 bitů a proměnlivou délkou klíče až do 256 bitů.

5.3.2 Asymetrické šifrování

Asymetrické algoritmy nazýváme též algoritmy s veřejným klíčem. Princip těchto algoritmů je v tom, že pro každého uživatele existuje dvojice klíčů: *veřejný a tajný*.

Veřejný klíč je všeobecně komukoliv dostupný. Tímto klíčem lze pouze zašifrovat zprávu pro určitého uživatele. Tajný klíč má každý u sebe schovaný a určitým způsobem

chráněný proti odcizení (heslem, na čipové kartě, na magnetické kartě). Tímto tajným klíčem lze provádět odkódování přijatých zpráv.

Velkou výhodou asymetrické kryptografie je snížení počtu klíčů při zabezpečené komunikaci. Jelikož každý uživatel disponuje celkem dvěma klíči (soukromým a veřejným), je za předpokladu n uživatelů zapotřebí celkem 2n klíčů (v případě symetrické kryptografie celkem n(n-1)/2 klíčů). Odpadají i problémy s distribucí veřejného klíče, neboť tento není nutno distribuovat zabezpečeným kanálem.

Z hlediska bezpečnosti je nutné podotknout, že teoreticky je možné z veřejného klíče u všech algoritmů vypočítat klíč tajný. Ale dosud je to výpočetně neproveditelné - se současným výkonem počítačů by se jednalo o tisíciletí. Existují návrhy na zefektivnění kryptoanalýzy, ale pro rozumný počet bitů klíče jsou algoritmy stále bezpečné.

Podívejme se nyní na některé představitele asymetrických šifer.

Algoritmus RSA byl objeven roku 1977 a jeho autoři jsou Ron Rivest, Adi Shamir a Joe Adleman – odtud RSA. Systém je založen na teoreticky jednoduché úvaze: Je snadné vynásobit dvě dlouhá (100-místná) prvočísla, ale bez jejich znalosti je prakticky nemožné zpětně provést rozklad výsledku na původní prvočísla. Součin těchto čísel je tedy veřejný klíč. Přitom obě prvočísla potřebujeme pro dešifrování. Vzhledem k tomu, že není znám rychlý algoritmus na faktorizaci velkého čísla, je algoritmus RSA bezpečný. Velkým problémem není jen faktorizace čísla N, ale problém je i najít sama prvočísla p a q, potřebné k tvorbě klíčů. Najít dostatečně velké prvočíslo je dosti těžké (resp. pomalé), proto se hledají čísla, která jsou prvočísly s vysokou pravděpodobností. Algoritmus RSA je hojně implementován v SW produktech podporujících elektronický podpis.

Diffie-Hellmanova funkce. Již na počátku 70 let uveřejnili pánové Diffie a Hellman svou představu o možnostech šifrování veřejným klíčem. Jejich práce přinesla jednosměrnou DH funkci, která je stále v kryptosystémech používána. I tento algoritmus nachází uplatnění v elektronických podpisech.

El Gamal šifra je v případě systémů založených na diskrétním logaritmu v podstatě analogií RSA.

Eliptické křivky byly zkoumány algebraickou geometrií a teorií čísel více než 150 let, avšak až v roce 1985 přišli nezávisle na sobě Victor Miller (tehdy IBM) a Neal Koblitz (University Of Washington) na jejich použití v rámci systému veřejného klíče. Je třeba si uvědomit, že éra masivního zkoumání algoritmů veřejného klíče začala až v roce 1976. V nejbližších letech po objevu možností využití problému diskrétního logaritmu v kryptografii se zdálo vše vyřešené a použití eliptických křivek se proto jevilo jako nepraktické. Postupem času se ukázalo, že metody veřejného klíče typu RSA jsou relativně pomalé a těžkopádné a že jsou z tohoto hlediska eliptické křivky výhodnější.

Požadavky praxe kladou na kryptografické algoritmy rozporuplné požadavky: kryptografická síla, rychlost a jednoduchost.

5.3.3 Hashovací funkce

Vzorkovací, neboli hashovací, funkce jsou velmi důležité pro kryptografii a tvorbu digitálních podpisů. Jsou to funkce, které umí vytvořit vzorek jakéhokoli souboru, aby byl závislý na všech bitech původního souboru. Výstupem funkce je vzorek (též nazývaný hash, fingerprint či otisk) o pevné délce. Pokud by došlo ke změně jediného bitu v souboru (například v textu šifrované zprávy by přibyla mezera či čárka), výsledkem by byla zcela odlišná hodnota hashovací funkce. Je zřejmé, že hashovací funkce naplňují především potřeby integrity předávaných dat. Nejpoužívanější hashovací funkce jsou popsány v následujících bodech.

MD5 – Message Digest Algorithm 5 (RFC 1321). Tvůrcem algoritmu je známý Ron Rivest (tehdy z MIT). Výstupem funkce je 128-bitový vzorek.

SHA-1 – Secure Hash Algorithm 1. Upravená verze SHA. Tento algoritmus je zaštítěn NIST, která jej publikovala jako svůj standard ve FIPS 180 – 1.

RIPEMD 160 – výstupem této funkce je 160-bitový vzorek (5)

5.3.4 Kvantová kryptografie

Účelem kryptografie je zajistit, aby přenášená informace měla smysluplný (a původní) význam jen pro zamýšleného příjemce, i když se dostane do rukou jiných příjemců. Zajišťuje to systematické šifrování původní zprávy. Dnešní šifrovací mechanizmy jsou dostatečně známy a bezpečnost přenášených informací závisí především na tajném klíči, složeném z náhodně zvolené posloupnosti bitů o dostatečné délce. Jestliže má být klíč tajný a přitom ho

mají znát obě strany komunikace, které plně spoléhají na přenosovou infrastrukturu (nejčastěji veřejnou, jako Internet, a tedy náchylnou k odposlechu), je potřeba vyřešit problém bezpečné distribuce klíčů.

Zatímco v klasické kryptografii se používají nejrůznější matematické metody, aby se útočníkům zamezilo zjištění obsahu přenášené zprávy, kvantová kryptografie k tomu používá zákony fyziky, konkrétně kvantové chování jednotlivých fotonů světla. To zajišťuje, že informace přenášená fotony se při jakémkoli odposlechu změní a jakýkoli útok pak lze snadno detekovat. Úspěšný odposlech přitom útočníkovi neposkytne dostatek informací pro efektivní narušení bezpečnosti.

Kvantová kryptografie se proto výhodně používá pro distribuci klíčů, neboť tok jednotlivých fotonů umožňuje spolehlivé a bezpečné vytvoření tajného klíče mezi dvěma stranami.

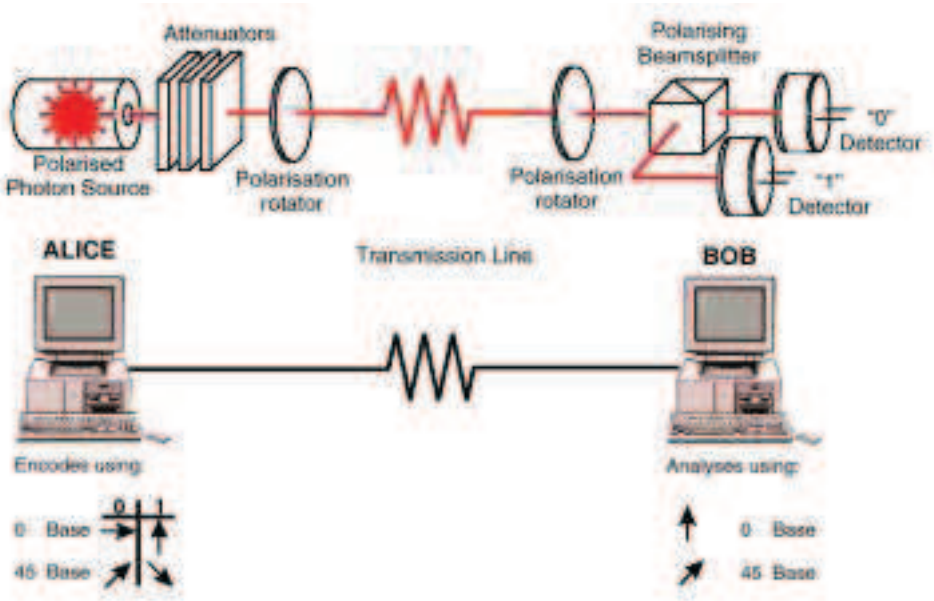
Kvantová kryptografie (quantum cryptography) a quantum computing jsou nové oblasti kvantové mechaniky, které se odehrávají v tzv. Hilbertově prostoru (podle německého matematika Davida Hilberta), kde se subatomické částice vlastně nikdy nenacházejí v konkrétním místě. Kvantové počítače mohou v budoucnu hrát významnou roli v šifrování a mohou také nahradit superpočítače.

Systém kvantové kryptografie je ve skutečnosti systém distribuce klíče (QKD, Quantm-Key Distribution), který váže bezpečnost systému na princip nejistoty kvantové mechaniky. Základem principu nejistoty (Heisenbergův princip) je, že měření prováděné na fyzickém systému pro získávání nějakých informací o daném systému bude mít nutně na systém nějaký vliv, byť velice malý.

Systém kvantové kryptografie je navržen tak, že odesílatel (Adam) připraví fyzický systém do známého kvantového stavu a pošle ho oprávněnému příjemci (Barbora). Barbora provede měření jedné ze dvou určitých veličin (principy kvantové fyziky neumožňují měření obou veličin současně) systému přijatého od Adama. Těchto výměn a měření se provede dostatečné množství a v ideálním případě pak budou mít obě strany komunikace dostatek hodnot, které mohou sloužit jako klíč.

Kvantový systém, který se běžně používá, jsou jednotlivé fotony, tedy částice světla. Každý foton nese jeden bit kvantové informace a označuje se jako qubit (quantum bit). Kromě fotonů by šlo sice použít i jiný kvantový systém, ale světlo se šíří velmi rychle a snadno, a navíc znalosti manipulace s ním jsou v dostatečně pokročilém stádiu. Jednotlivé fotony lze vysílat jak optickým kabelem, tak vzduchem, i když v druhém případě je realizace kvůli atmosférickému prostředí poněkud složitější.

Jako veličina pro měření se nejčastěji používá polarizace fotonů (viz obrázek). V roce 1984 poprvé popsali takový bezpečný kvantový systém distribuce klíče pánové Charles Bennett a Gilles Brassard (BB84). Jako alternativa se používá metoda korelovaných (entangled) stavů, kterou poprvé navrhl pro kvantový systém Artur K. Ekert v roce 1990.



Obrázek 2: Polarizace fontů

Zdroj: (6)

Informace o veličině, kterou Adam nastavil a Barbora měřila, byly vlastně veřejné, ale konkrétní naměřené hodnoty se nikdy nesdělovaly. Takže potenciální útočník by musel zkoušet získávat nějaké informace z kvantového systému, který Adam poslal Barboře. To by se ovšem kvůli principu nejistoty odrazilo na samotném systému. Došlo by k naměření jiné hodnoty než nastavené odesílatelem, takže komunikující strany by se o zlomyslném odposlechu dozvěděly prostým porovnáním příslušných hodnot. Podle objemu informací, které se útočník takto mohl z výměny mezi Adamem a Barborou dozvědět, je pak před

ustavením samotného klíče proveden ještě proces destilace bitů (bit distillation) a zesílení soukromí (privacy amplification).

Kvantový (fotonový) systém distribuce klíče umožní Adamovi a Barboře získat sdílený klíč. Adam vysílá fotony v jedné ze čtyř polarizací: 0, 45, 90 nebo 135 stupňů. Barbora ve svém přijímači měří polarizaci buď v kolmé (0 a 90 stupňů), nebo diagonální bázi (45 a 135 stupňů).

Vlastní distribuce klíče probíhá v několika krocích. Adam vysílá fotony náhodně v některé ze čtyř polarizací.

Obrázek 3: Polarizace 1

Zdroj: (6)

Pro každý přijatý foton si Barbora zvolí náhodný typ měření, buď podle kolmé (+), nebo diagonální báze (X).

Obrázek 4: Polarizace 2

Zdroj: (6)

Výsledky měření si Barbora pro sebe zaznamená.

Obrázek 5:Polarizace 3

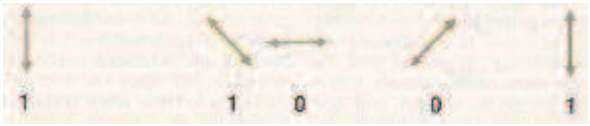
Zdroj: (6)

Po dokončení přenosu Barbora sdělí Adamovi, jaké typy měření se pro jednotlivé přijaté fotony použily (samotné výsledky měření si ale samozřejmě ponechá pro sebe) a Adam jí sdělí, které typy měření pro jednotlivé fotony byly správné. Tato informace při odposlechu případnému útočníkovi nic neřekne.

Obrázek 6: Polarizace 4

Zdroj: (6)

Adam a Barbora si pak ponechají ty výsledky měření, kde se měřila polarizace správně. Tyto případy si převedou na bity (0 nebo 1) a jejich posloupnost bude definovat samotný klíč.



Obrázek 7: Polarizace 5

Zdroj: (6)

Kvantová kryptografie se pomalu přesunuje z laboratorního prostředí do praktického využití pro zajištění maximální bezpečnosti. Nejobtížnější je navrhnout a vybudovat systém vysílače (vhodného pro danou metodu kvantového systému) a přijímače (detektoru) jediného fotonu pro běžné použití, tedy pro spolehlivé překonání dostatečné vzdálenosti.

V 80. letech laboratoř v IBM T. J. Watsonově výzkumném středisku použila kvantový systém na vzdálenost pouhých 30 centimetů s rychlostí 10 bit/s. Od té doby ale uplynulo hodně vody, vyvinuly se nové zdroje fotonů, fotodetektory a lepší optická vlákna, což vše samozřejmě dovoluje řádově vyšší rychlosti budování klíčů (tisíce bitů za vteřinu) i větší vzdálenosti (desítky kilometrů), protože světlo s vyšší vzdáleností podléhá útlumu a rozptýlené fotony lze již jen obtížně zachytit.

Kvantová kryptografie se pomalu propracovává ke skutečně komerčnímu využití, tak se podívejme, s čím konkrétně se můžeme na trhu již setkat. Švýcarská společnost id Quantique před několika lety dosáhla fungování systému na vzdálenost 67 kilometrů a japonská Toshiba před nedávnem oznámila úspěch i na 100 kilometrů po optickém vláknu. Pro větší vzdálenosti se pracuje na kvantových opakovačích teoreticky např. ve formě atomu cesia (přístup se zkouší na California Institute of Technology nebo Harvard University).

Pokusy také probíhají ve volném prostoru, zatím se však dosahuje příliš malých vzdáleností, cca 20 kilometrů (Univerzita Ludwiga Maximillianse v Mnichově).

Většina implementací kvantové kryptografie není uzpůsobena k přenosu dat, ale pouze k vytvoření naprosto tajného klíče. Proto se v praktickém využití systém použije na výměnu klíče pro danou relaci a nějaký jiný přenosový systém pro šifrování zpráv v relaci za využití klíče získaného kvantovou kryptografií. Hybridní šifrovací systémy ostatně nejsou ničím výjimečným ani v klasické kryptografii.

Japonská společnost Japan Science and Technology Corporation si už dala mezinárodně patentovat svůj datový komunikační systém pro optické sítě zabezpečený kvantovým šifrováním. Systém má dvě hlavní složky: vysílač a směrovač. Vysílač generuje optický signál složený z adresové posloupnosti pulsů (pulse train) a jednofotonového pulsu, který slouží jako kvantová šifra. Směrovač analyzuje záhlaví, aby zjistil adresové informace z optického signálu, a přepínač (gate switch) určí cestu signálu jedním z výstupních optických vláken.

V říjnu roku 2003 tři švýcarské společnosti oznámily vybudování infrastruktury klíče založené právě na kvantové kryptografii. Partnery v bezpečné šifrovací infrastruktuře jsou id Quantique, výzkumná společnost v oblasti kvantové kryptografie, WISeKey, poskytovatel služeb pro certifikační autority PKI (Public Key Infrastructure), a OISTE, mezinárodní normalizační orgán pro oblast bezpečných elektronických transakcí. Prvními zákazníky budou pravděpodobně finanční instituce a vládní úřady.

V listopadu 2003 přišla začínající americká společnost MagiQ se svým systémem kvantové kryptografie. Jejich Navajo Secure Gateway (stejně příhodné jméno jako název celé firmy) stojí 50 tisíc dolarů, čímž má velmi konkurovat současné nabídce podobných systémů na trhu. Používá metodu BB84 na doposud nejdelší vzdálenost 120 kilometrů. Systém je určen pro virtuální privátní sítě (VPN) pro finanční instituce, armádu nebo vládu. (6)

6. Návrh řešení

6.1 Získání a zprovoznění kvalifikovaného certifikátu

6.1.1 Vygenerování klíčů a žádosti o certifikát

Ještě před tím, než se s Poštovní certifikační poukázkou navštíví kontaktní místo České pošty, je potřeba vygenerovat si dvojici klíčů a elektronickou žádost o certifikát

1. V prohlížeči Internet Explorer se otevře stránka http://qca.postsignum.cz/www/generators.php.

2. Na stránce se klikne na typ certifikátu, který si chcete nechat vydat. Pokud jste podnikající fyzická osoba (OSVČ), vyberte první položku ze čtveřice možností, tedy Certifikáty určené k ověření elektronického podpisu zaměstnance. Jste-li nepodnikající fyzická osoba (jednotlivec), zvolte možnost Certifikáty určené k ověření elektronického podpisu fyzické osoby.

3. Po kliknutí na příslušný odkaz se zobrazí formulář pro generování žádosti. Tento formulář se vyplní (nutné vyplnit je pouze pole označená hvězdičkou).

U položek **Poskytovatel krypt. služeb** a **Velikost klíče** se ponechají přednastavené hodnoty.

Velmi doporučujeme ponechat zaškrtnutou položku Povolit export soukromého klíče, aby se mohl později soukromý klíč zazálohovat nebo jej přenést do jiné aplikace případně na jiný počítač.

Pokud se zaškrtne položka **Upřesnit zabezpečení**, může se během procesu generování nastavit vysoká úroveň zabezpečení úložiště soukromého klíče (při každém použití soukromého klíče, tj. při podepisování, budete vyzváni k zadání hesla chránícího úložiště).

4. V posledním poli **Název souboru** se udává umístění a jméno souboru, do kterého se uloží elektronická žádost o certifikát.

5. Po vyplnění formuláře se klikne na tlačítko **Vytvořit žádost**. Postupně se zobrazí informační okna, na která se vždy odpovídá **Ano** nebo **OK.**

6. Tím došlo k vygenerování klíčů a vytvoření souboru s elektronickou žádostí o certifikát (viz bod 4.). Zkopíruje se tento soubor na disketu (s touto disketou se později dostavíte se na kontaktní místo – viz dále).

6.1.2 Vyplnění objednávky certifikačních služeb

Nepodnikající fyzická osoba

Na adrese http://qca.postsignum.cz/www/contract.php?customer=FO se stáhne a vyplní objednávka certifikačních služeb.

Poznámka: Doporučuje se zaškrtnout bod 3.7 objednávky. Tím bude Váš certifikát doplněn o identifikátor klienta Ministerstva práce a sociálních věci – jedině s tímto identifikátorem je možné elektronické podávání formulářů státní sociální podpory.

Objednávka se vytiskne ve dvou exemplářích (podepisuje se až na kontaktním místě před pracovníkem České pošty).

Podnikající fyzická osoba (OSVČ)

Na adrese http://qca.postsignum.cz/www/contract.php?customer=OSVC se stáhne a vyplní **objednávka certifikačních služeb**. V objednávce se kromě typu poskytovaných služeb stanovují i oprávněné osoby, které budou zastupovat zákazníka vůči QCA. Zde se doplní údaje o sobě. Objednávku se vytiskne ve dvou exemplářích a podepíše.

Znovu na adrese http://qca.postsignum.cz/www/contract.php?customer=OSVC se stáhne a vyplní **seznam žadatelů**. Tento formulář se skládá z úvodního listu a libovolného počtu příloh. Ve Vašem případě se vyplní pouze jedna příloha, v níž se žádá o vydání certifikátu podle politiky.

Certifikáty pro ověření elektronického podpisu zaměstnance. Seznam žadatelů se vytiskne ve dvou exemplářích. Podepíše se pouze příloha seznamu žadatelů, úvodní list se podepisuje až na kontaktním místě před pracovníkem České pošty.

6.1.3 Návštěva kontaktního místa České pošty (vydání certifikátu)

Nepodnikající fyzická osoba

Dostaví se na kontaktní místo s vyplněnými objednávkami certifikačních služeb a s disketou s uloženou žádostí o certifikát. Předloží se dva doklady totožnosti (občanský průkaz + řidičský průkaz, pas, průkaz ZTP nebo rodný list). Pracovník České pošty akceptuje Vaši objednávku. Po uzavření smlouvy je ihned zahájen proces vydání certifikátu.

Proces vydání certifikátu je zakončen sepsáním protokolu o vydání certifikátu. Vydaný certifikát je uložen na disketu spolu s certifikáty a CRL certifikačních autorit PostSignum QCA.

Podnikající fyzická osoba (OSVČ)

S objednávkami certifikačních služeb, seznamem žadatelů a disketou se žádostí o certifikát se dostaví na kontaktní místo.

Pokud *jste zapsáni v obchodním rejstříku*, musíte s sebou dále přinést originál výpisu z obchodního rejstříku (ne starší než 3 měsíce) nebo notářsky ověřenou kopii výpisu z obchodního rejstříku (originál nesmí být starší než 3 měsíce). Pokud *v obchodním rejstříku zapsáni nejste*, musíte s sebou dále přinést originál jiné zakládací listiny (např. živnostenského listu) nebo notářsky ověřenou kopii jiné zakládací listiny (např. živnostenského listu).

Pro ověření identity se předloží občanský průkaz nebo cestovní pas.

Před pracovníkem České pošty se podepíšete na úvodní list seznamu žadatelů. Údaje o Vaší osobě jsou následně zaneseny do systému. Od tohoto okamžiku může být vydán certifikát, který byl specifikován na seznamu žadatelů.

Předloží se disketu s uloženou žádostí o certifikát a uskuteční se proces vydání certifikátu, který je zakončen sepsáním protokolu o vydání certifikátu. Vydaný certifikát je uložen na disketu spolu s certifikáty a CRL certifikačních autorit PostSignum QCA.

6.1.4 Instalace vydaného certifikátu

Po návštěvě kontaktního místa budete mít na disketě následující soubory:

- **cert_sign.req** – Vaše žádost o certifikát, kterou jste uložili na disketu
- **cert_sign.crt** – Váš vydaný certifikát
- **postsignum_qca_root.crl** – aktuální CRL kořenové certifikační autority PostSignum QCA
- **postsignum_qca_root.crt** – certifikát kořenové certifikační autority PostSignum QCA
- **postsignum_qca_sub.crl** – aktuální CRL podřízené certifikační autority PostSignum QCA
- **postsignum_qca_sub.crt** – certifikát podřízené certifikační autority PostSignum QCA

V tuto chvíli nás zajímá soubor **cert_sign.crt**, který obsahuje vydaný certifikát. Ve Vašem případě se může jmenovat jinak, jeho jméno by však mělo být vždy stejné jako jméno vytvořené elektronické žádosti o certifikát. Popíšeme si jednoduchý postup, jak tento certifikát nainstalovat:

1. V prohlížeči Internet Explorer otevřete stránku
https://qca.postsignum.cz/webgen/cert - install.php .

2. Klikněte na tlačítko **Procházet...** a nalistujte soubor s vydaným certifikátem, který máte na disketě.

3. Klikněte na tlačítko **Instalovat certifikát**. Postupně se budou zobrazovat informační okna, na která vždy odpovídejte **Ano** nebo **OK.**

6.1.5 Instalace certifikátů QCA

Operační systém nemůže ověřit Váš certifikát, dokud nebudou nainstalovány také certifikáty certifikačních autorit PostSignum QCA. Tento postup musí provést jak vlastník certifikátu, tak druhá strana, s níž vlastník certifikátu komunikuje.

Tyto certifikáty naleznete na disketě s vydaným certifikátem. Jedná se o soubory **postsignum_qca_root.crt** a **postsignum_qca_sub.crt** (dostupné jsou také na stránce https://qca.postsignum.cz/www/authorities.php).

Následující postup proveďte nejprve se souborem **postsignum_qca_root.crt** a poté se souborem **postsignum_qca_sub.crt**:

1. Poklepejte dvakrát levým tlačítkem myši na soubor s certifikátem autority. Zobrazí se okno s informacemi o certifikátu.

2. Pokud se v horní části nezobrazuje červená ikona a text „*Certifikát není důvěryhodný*“, je již certifikát v operačním systému nainstalován a další kroky tohoto postupu není nutné provádět. V opačném případě stiskněte tlačítko **Nainstalovat certifikát…**

3. Spustí se průvodce importem certifikátu. Po zobrazení úvodní obrazovky průvodce pokračujte stiskem tlačítka **Další >**.

4. Ponechte nastavenou volbu „*Automaticky vybrat úložiště certifikátů na základě typu certifikátu“* a pokračujte stiskem tlačítka **Další >**.

5. Odsouhlaste poslední obrazovku průvodce stisknutím tlačítka **Dokončit**.

6. Pokud instalujete certifikát autority ze souboru **postsignum_qca_root.crt**, zobrazí se okno s varováním. Operační systém se Vás táže, zda si jste jisti důvěryhodností certifikátu autority PostSignum Root QCA. V okně je zobrazena řada písmen a číslic, kterou si můžete ověřit na webových stránkách PostSignum QCA (http://qca.postsignum.cz) a

webových stránkách Ministerstva informatiky ČR (http://www.micr.cz). V případě, že si jste jisti „nezávadností“ souboru s certifikátem, stiskněte tlačítko **Ano**. (9)

6.2 Použití elektronického podpisu

6.2.1 Mozilla Thunderbird

E-mailový klient Mozilla Thunderbird používá pro ukládání certifikátů své vlastní úložiště. Nepracuje tedy, na rozdíl např. od aplikace Outlook Express, s certifikáty, uloženými v úložišti certifikátů systému Windows (tato vlastnost je dána multiplatformností Thunderbirdu).

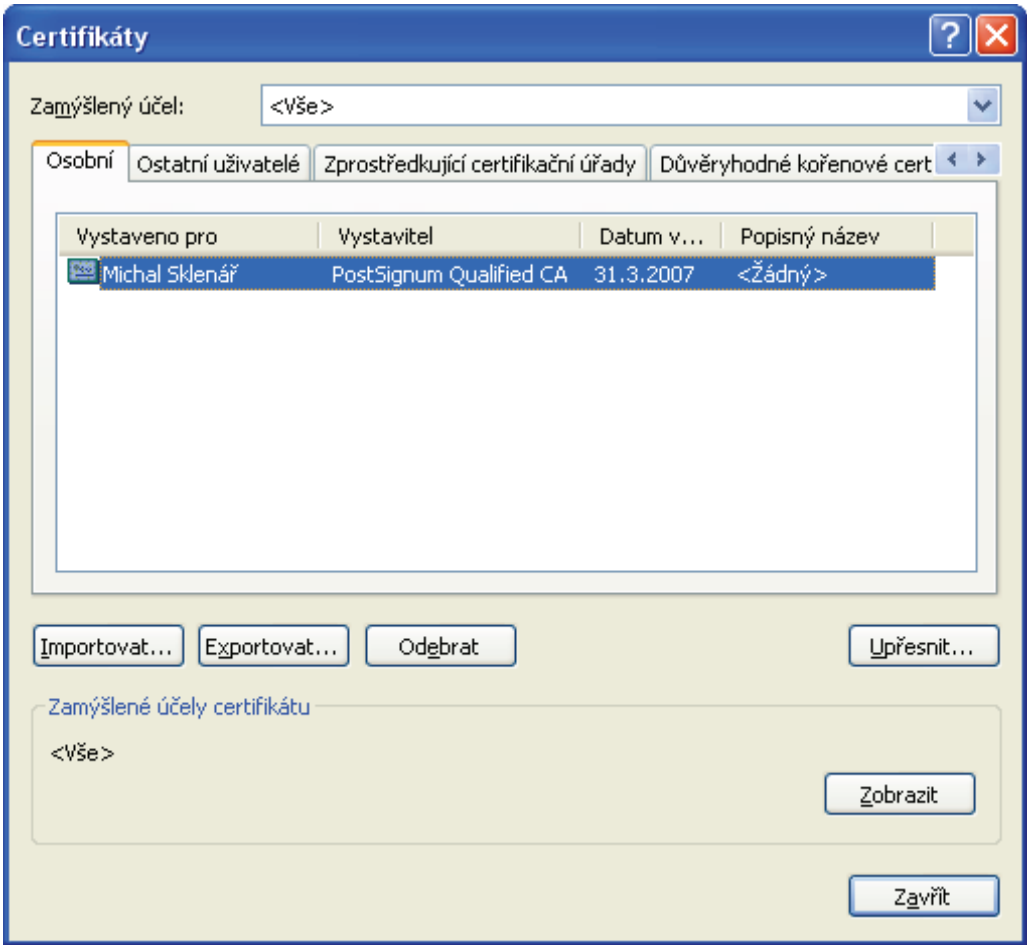
Příslušné certifikáty je tedy nejprve potřeba naimportovat do úložiště certifikátů Thunderbirdu.

Uložení certifikátů do úložiště Thunderbirdu

Postup uložení certifikátů do aplikace Mozilla Thunderbird není složitý – sestává se z exportu certifikátů z úložiště certifikátů Windows a následného importu do aplikace Mozilla Thunderbird.

Export certifikátu

1. Spusťte Internet Explorer.
2. V menu vyberte Nástroje > Možnosti Internetu...
3. Vyberte kartu Obsah a zde v sekci *Certifikáty* klikněte na tlačítko Certifikáty.
4. Otevře se Vám okno *Certifikáty*, kde by jste na kartě Osobní měli vidět svůj certifikát od certifikační autority PostSignum QCA.



Obrázek 8: Použití 1

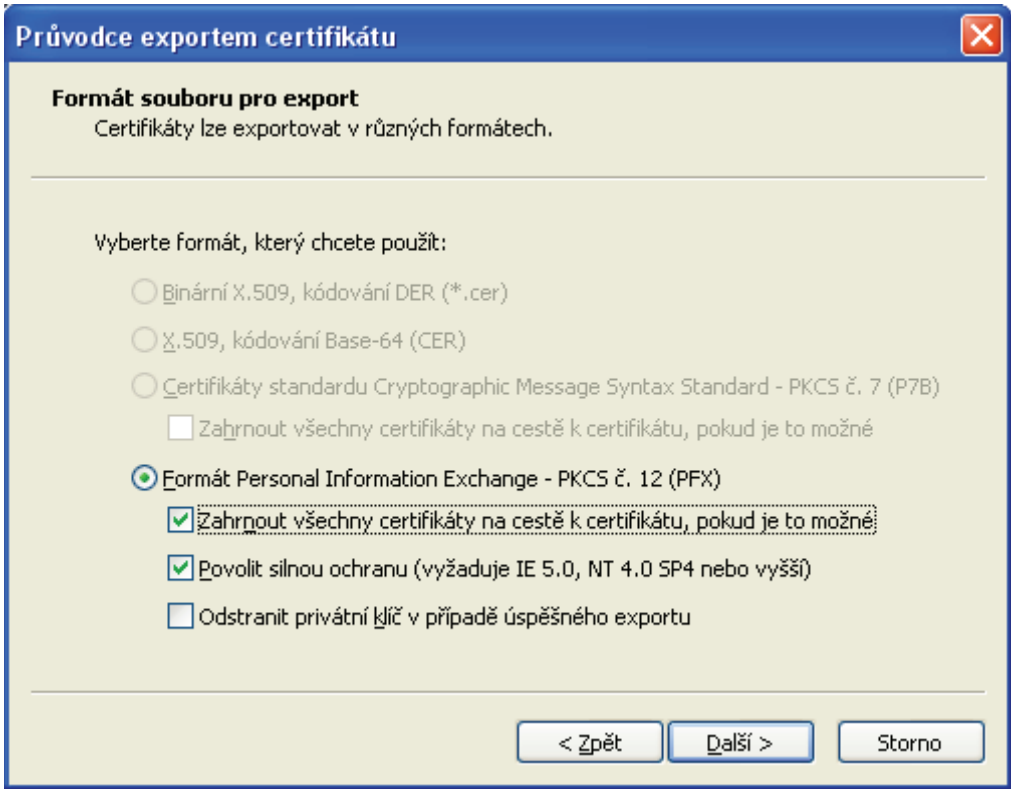
Zdroj: (3)

5. Vyberte tento certifikát a klikněte na tlačítko **Exportovat...**

6. Spustí se *Průvodce exportem certifikátu*. Z uvítání pokračujte tlačítkem **Další >**.

7. Na dotaz, zda s certifikátem exportovat také soukromý klíč, zvolte volbu **Ano, exportovat soukromý klíč** a pokračujte tlačítkem **Další >**.

8. V tomto kroku zaškrtněte volbu **Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné**. Díky tomu nebude potřeba do Thunderbirdu zvlášť importovat kořenové certifikáty QCA. Pokračujte kliknutím na tlačítko **Další >**.



Obrázek 9 : Použití 2

Zdroj: (3)

9. Následuje zadání hesla, kterým se bude chránit vyexportovaný soukromý klíč. Toto později použijete při importu certifikátu. Zadejte tedy heslo a jeho potvrzení a klikněte na **Další >**.

10.Klikněte na **Procházet...** a zvolte název a cestu pro soubor s vyexportovaným certifikátem. Opět pokračujte tlačítkem **Další >** a průvodce dokončete tlačítkem **Dokončit**.

Import certifikátu

1. Spusťte Mozilla Thunderbird.

2. Otevřete okno *Správce certifikátů* – způsob, kterým se k tomuto oknu dostanete, se liší podle verze aplikace (verzi poznáte z nabídky Nápověda > O aplikaci Mozilla Thunderbird)

• *verze 1.0.7*: Nástroje > Možnosti > Ostatní > Certifikáty > Spravovat certifikáty...

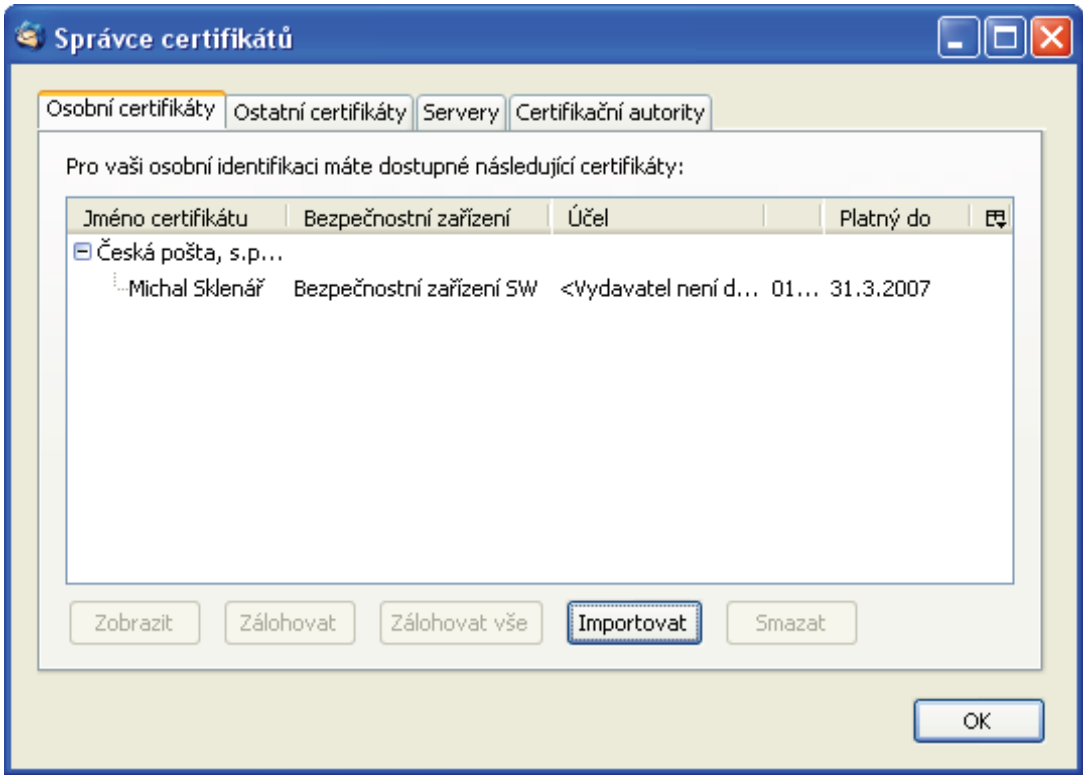
• *verze 1.5 a novější*: Nástroje > Možnosti > Soukromí > Zabezpečení > Certifikáty...

3. Ve správci certifikátů klikněte na kartě Osobní certifikáty na tlačítko Importovat.

4. Nalistujte soubor s vyexportovaným certifikátem (viz bod 10. v kapitole Export certifikátu). Pokud pracujete s certifikáty v aplikaci Mozilla Thunderbird poprvé, budete vyzváni

pro vytvoření hlavního hesla, které chrání Vaše citlivé informace v Thunderbirdu (např. hesla webových stránek nebo právě certifikáty). Zadejte toho heslo a jeho ověření.

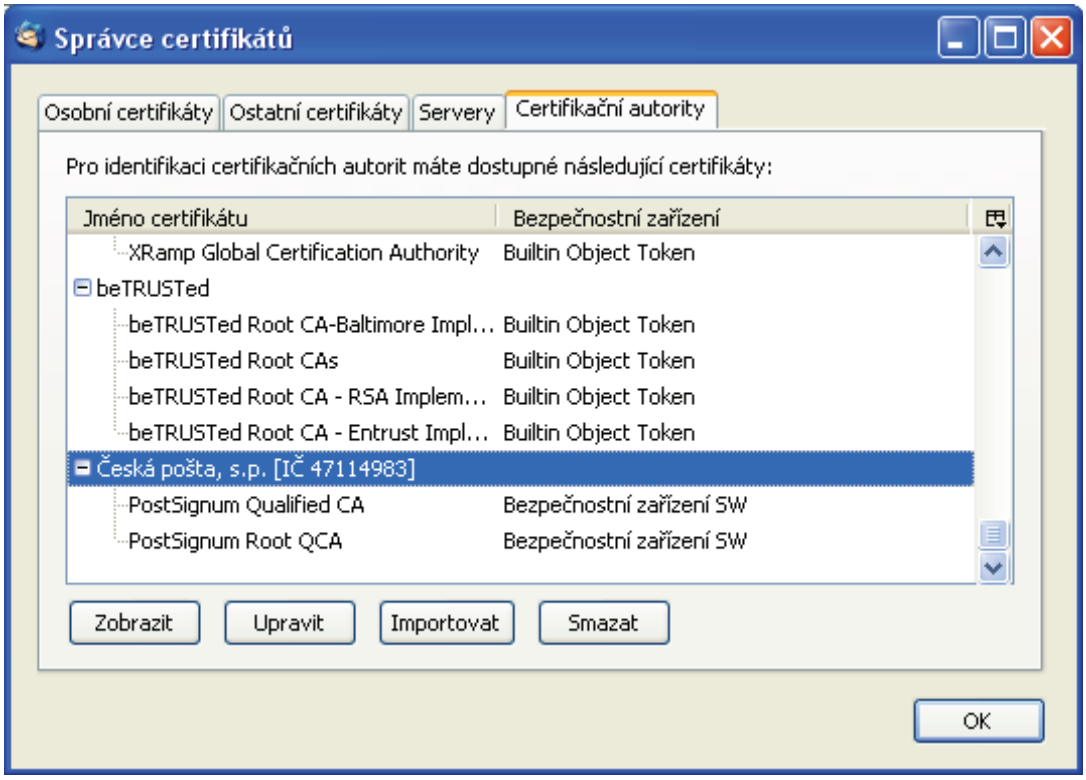
5. Následně budete dotázání na heslo, se kterým byl při exportu certifikát zašifrovaný (viz bod 9. v kapitole Export certifikátu). Zadejte toto heslo a po potvrzení dojde k importu certifikátu.



Obrázek 10 : Použití 3

Zdroj: (3)

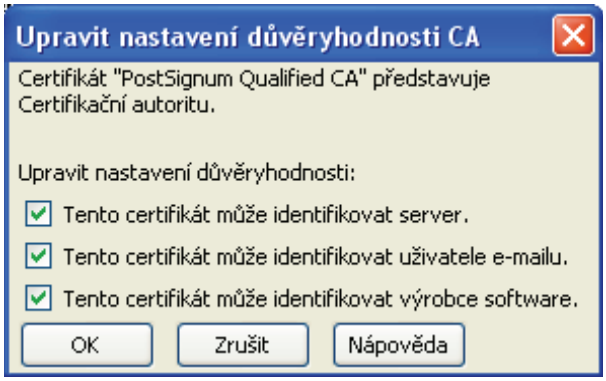
6. Všimněte si, že ve sloupci *Účel* (stále se nacházíme ve správci certifikátů na kartě **Osobní certifikáty**) je u certifikátu text „*Vydavatel není důvěryhodný*“. S certifikátem se sice naimportovaly potřebné certifikáty vydavatele, tedy certifikační autority QCA, nicméně je potřeba je ještě označit jako důvěryhodné. To provedete na kartě **Certifikační autority**. Nalezněte zde větev *Česká pošta, s. p.* (měla by být úplně na konci seznamu certifikačních autorit).



Obrázek 11 : Použití 4

Zdroj: (3)

7. Součástí této větve jsou dva certifikáty: **PostSignum Qualified CA** a **PostSignum Root QCA**. Postupně každý vyberte a klikněte na tlačítko **Upravit**. Zobrazí se okno *Upravit nastavení důvěryhodnosti CA*, kde zaškrtněte všechny tři nabízené možnosti a potvrďte tlačítkem **OK**.



Obrázek 12 :Použití 5

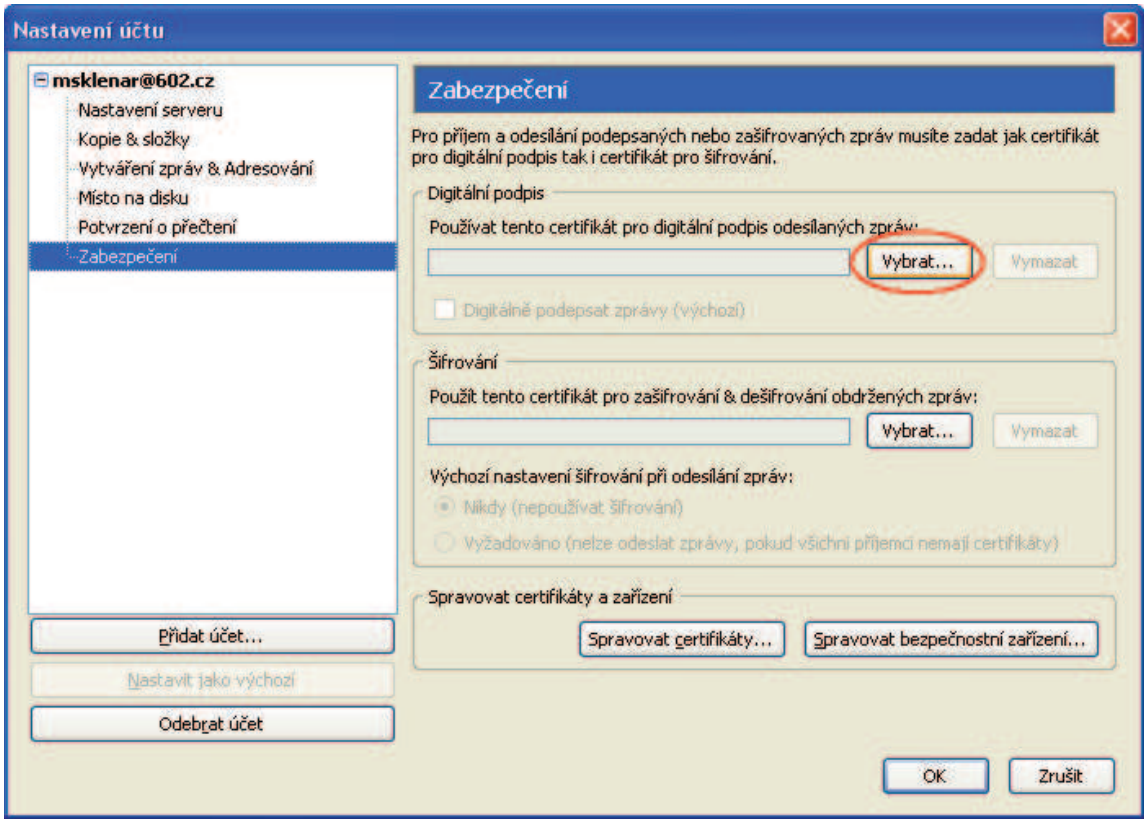
Zdroj: (3)

8. Tím jste s importem certifikátů do aplikace Mozilla Thunderbird hotovi a můžete již bez problémů své zprávy elektronické pošty elektronicky podepisovat.

Odesílání elektronicky podepsaných zpráv

Po úspěšném uložení (importu) certifikátů do úložiště certifikátů Mozilla Thunderbird je již samotné podepisování e-mailových zpráv velice jednoduché. Jediné, co je třeba ještě před odesláním první podepsané zprávy udělat, je nastavení používání Vašeho certifikátu pro elektronický podpis odesílaných zpráv (toto nastavení se provádí samozřejmě pouze jednou, poté si aplikace již pamatuje, jakým certifikátem dokumenty elektronicky podepisovat):

1. V menu **Nástroje** > **Nastavení účtu...** zvolte v levé části okna větev e-mailového účtu, jehož zprávy chcete elektronicky podepisovat. Klikněte na položku **Zabezpečení** a poté v pravé části okna v sekci *Digitální podpis* klikněte na tlačítko **Vybrat...**



Obrázek 13 : Použití 6

Zdroj: (3)

2. V zobrazeném dialogu vyberte požadovaný certifikát. Vlastníte-li jich více, poznáte jej podle vydavatele zobrazeném ve spodní části dialogu. Výběr potvrďte tlačítkem **OK**.

3. Na závěr se Vás aplikace zeptá, zda tentýž certifikát použít také pro šifrování zpráv příjemců. Klikněte na tlačítko **OK**.

Poté, co jste nastavili certifikát pro elektronické podepisování, můžete své zprávy pomocí tohoto certifikátu elektronicky podepisovat. Je to snadné:

1. Běžným způsobem napište novou zprávu.
2. Zvolte v menu **Možnosti** > **Zabezpečení** > **Digitálně podepsat zprávu**.
3. Budete-li požádáni, zadejte hlavní bezpečnostní heslo aplikace Mozilla Thunderbird (viz bod 4. v kapitole Import certifikátu).
4. Zprávu odešlete.

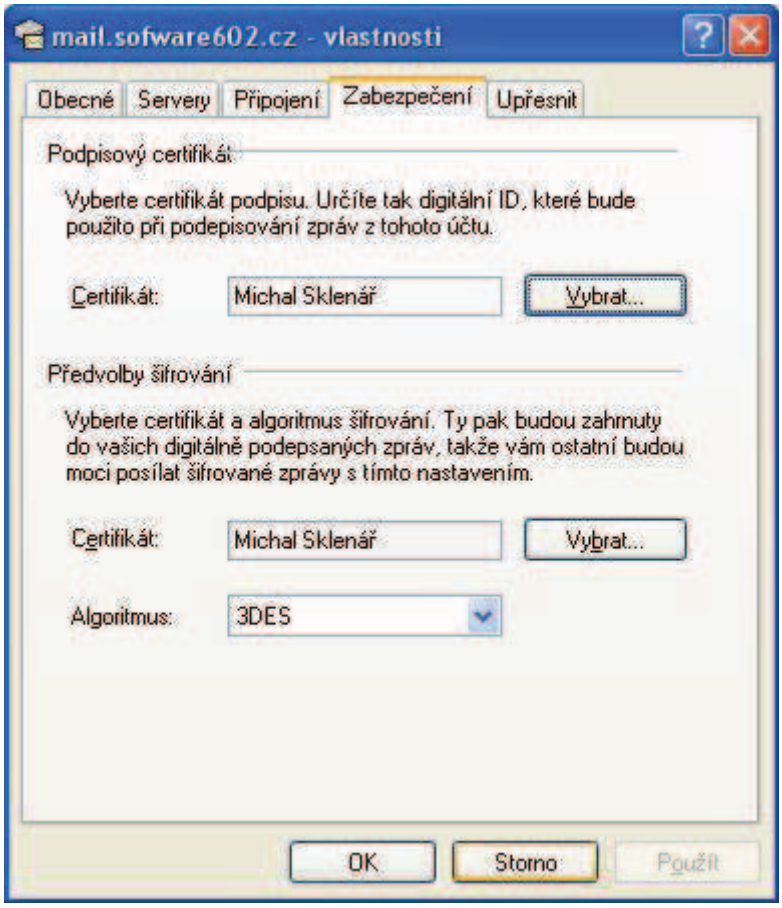
Tím jste odeslali elektronicky podepsanou zprávu. Aby byl Váš elektronický podpis pro příjemce zprávy důvěryhodný, musí tento příjemce vlastnit ve svém úložišti certifikátů certifikáty certifikační autority PostSignum QCA jako důvěryhodné. Jedná se o certifikáty kořenové a podřízené certifikační autority, které je možné stáhnout přímo ze stránek PostSignum QCA na adrese http://qca.postsignum.cz/www/authorities.php. Komunikujete-li elektronicky s e-podatelnou nějakého úřadu, můžete se spolehnout, že druhá strana tyto certifikáty vlastní.

6.2.2 Outlook Express

Na rozdíl od e-mailového klienta Mozilla Thunderbird, nepoužívá Outlook Express pro certifikáty vlastní úložiště (využívá systémové úložiště Windows), proto zde odpadá procedura importu certifikátů do aplikace.

Stejně jako v případě Thunderbirdu, musíte i v Outlook Express vybrat certifikát, kterým se budou elektronicky podepisovat Vaše zprávy. Pokud vlastníte jediný osobní certifikát, měl by jej Outlook Express zvolit automaticky, nicméně raději se přesvědčte. Nastavení se provádí následujícím způsobem:

1. V menu aplikace Outlook Express zvolte **Nástroje** > **Účty...** a v otevřeném okně klikněte na kartu **Pošta**. Vyberte e-mailový účet, jehož zprávy chcete elektronicky podepisovat a klikněte na **Vlastnosti**.
2. V otevřeném okně zvolte kartu **Zabezpečení** a poté v sekci *Podpisový certifikát* klikněte na tlačítko **Vybrat...**
3. Vyberte požadovaný certifikát a volbu potvrďte tlačítkem **OK**.



Obrázek 14 : Použití 7

Zdroj: (3)

Poté co jste nastavili certifikát pro elektronické podepisování, můžete své zprávy pomocí tohoto certifikátu elektronicky podepisovat. Postup je velice podobný jako v případě Mozilla Thunderbird:

1. Běžným způsobem napište novou zprávu.
2. Zvolte v menu **Nástroje** > **Digitálně podepsat** nebo klikněte na tlačítko

Obrázek 15 : Použití 8

Zdroj: (3)

Na panelu nástrojů. Podepsaný dokument je symbolizován ikonkou

Obrázek 16 : Použití 9

Zdroj: (3)

vpravo od adresy

příjemce zprávy.

3. Zprávu odešlete.

Tím jste odeslali elektronicky podepsanou zprávu. Aby byl Váš elektronický podpis pro příjemce zprávy důvěryhodný, musí tento příjemce vlastnit ve svém úložišti certifikátů certifikáty certifikační utority PostSignum QCA jako důvěryhodné. Jedná se o certifikáty kořenové a podřízené certifikační autority, které je možné stáhnout přímo ze stránek PostSignum QCA na adrese http://qca.postsignum.cz/www/authorities.php. Komunikujete-li elektronicky s e-podatelnou nějakého úřadu, můžete se spolehnout, že druhá strana tyto certifikáty vlastní. (3)

6.3 Kde všude lze elektronický podpis využít

6.3.1 Ministerstvo financí (Česká daňová správa)

Ministerstvo financí – ÚFDŘ provozuje aplikaci, která v současné době umožňuje podávat na po Internetu níže uvedené písemnosti, jako elektronická podání pro finanční úřady. Aplikace je umístěna na adrese http://adis.mfcr.cz/adis/jepo.

- Daňové přiznání k silniční dani
- Daňové přiznání k dani z nemovitostí
- Daňové přiznání k DPH
- Daňové přiznání k dani z příjmů právnických osob
- Daňové přiznání k dani z příjmů fyzických osob
- Oznámení o nezdaněných vyplacených částkách fyzickým osobám dle § 34 odst. 5, 8, 9

a 14 zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů,

- Hlášení platebního zprostředkovatele podle § 38fa zákona 586/1992 Sb.
- Vyúčtování daně z příjmů fyzických osob ze závislé činnosti a z funkčních požitků
- Obecné písemnosti (např. žádosti, stížnosti apod. prostřednictvím obecného dokumentu pro daňovou správu)

6.3.2 Česká správa sociálního zabezpečení

K 1. lednu 2006 mohou klienti ČSSZ využít tři níže uvedená elektronická podání.

Na této stránce http://www.cssz.cz/epodani/epodani.asp naleznete rozcestník k informacím, jak elektronicky podávat dokumenty a jak e-podání šifrovat a elektronicky podepisovat.

- Evidenční listy důchodového pojištění

- Přihlášky a odhlášky zaměstnanců k nemocenskému pojištění
- Přehled o příjmech a výdajích OSVČ

6.3.3 Ministerstvo práce a sociálních věcí

Elektronické formuláře státní sociální podpory (SSP) jsou internetovou aplikací sloužící k usnadnění Vaší komunikace s orgány státní správy v oblasti státní sociální podpory. Na stránce http://forms.mpsv.cz/sspforms naleznete následující formuláře:

- Žádost o přídavek na dítě
- Žádost o sociální příplatek
- Žádost o příspěvek na bydlení
- Žádost o rodičovský příspěvek
- Hlášení změn
- Žádost o dávku pěstounské péče - příspěvek na úhradu potřeb dítěte
- Žádost o dávku pěstounské péče - odměna pěstouna
- Žádost o dávku pěstounské péče - příspěvek při převzetí dítěte
- Žádost o dávku pěstounské péče - příspěvek na zakoupení motorového vozidla
- Žádost o příspěvek na péči o dítě v zařízení pro děti vyžadující okamžitou pomoc
- Žádost o porodné
- Žádost o pohřebné

6.3.4 Ministerstvo vnitra

Ministerstvo vnitra v současné době přijímá ve své podatelně elektronicky podepsané dokumenty jako například návrhy na zahájení správního řízení a vydání rozhodnutí, včetně návrhů na přezkoumání rozhodnutí, žádostí o vydání osvědčení, posudků, vyjádření, doporučení a jiných podobných opatření v oblasti státní správy a podání v trestním řízení, kdy je jako orgán činný v trestním řízení příslušný policejní orgán nebo útvar ministerstva vnitra pro inspekční činnost.

Vláda již schválila návrh, který umožňuje žádat o vystavení **občanských průkazů** elektronicky.

Aplikace, umožňující tuto službu, by měla být v budoucnu dostupná z portálu veřejné správy.

6.3.5 Elektronický podpis lze dále uplatnit v těchto případech

• Komunikace s krajskými, městskými či obecními úřady (e-podatelny)

• Komunikace mezi vybranými zdravotními pojišťovnami a poskytovateli zdravotní péče, plátci pojistného i samotnými pojištěnci.

• Např. portál VZP ČR umožňuje pojištěncům

• podávat Oznámení pojištěnce

• požádat o zaslání Přehledu vykázané zdravotní péče na pojištěnce za uplynulý kalendářní rok

• reklamovat Přehled vykázané zdravotní péče na pojištěnce

• Portál OZP

• Přehled OSVČ

• Obecné podání

• Ověření pojištěnce

• Viz také http://www.portalzp.cz

• Komunikace s Komisí pro cenné papíry

• Přijímání celních deklarací od celních deklarantů a komunikace v rámci celního řízení (4)

6.3.6 Ceny certifikátů

Tabulka 3: Kvalifikované certifikáty

Kvalifikované certifikáty		
typ Standard	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	základní cena **752**,-- s DPH
typ Comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací SW I.CA	základní cena prvotního certifikátu **1728**-- s DPH následný (obnovený) kvalifikovaný certifikát základní cena **752** ,-- s DPH

Zdroj: (1)

Tabulka 4: Kvalifikované systémové certifikáty

Kvalifikované systémové certifikáty		
typ Standard **(žadatel má vlastní hardwarové zařízení)**	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	základní cena **780**,--s DPH
typ Comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta - ovládací SW I.CA	základní cena prvotního certifikátu **1756**,--s DPH následný (obnovený) kvalifikovaný systémový certifikát: základní cena **780** ,-- s DPH
Podpisový certifikát ke kvalifikovanému systémovému certifikátu - kvalifikovaný	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	**390**,--s DPH

Zdroj: (1)

Tabulka 5: Komerční certifikáty

Komerční certifikáty		
typ Standard	Doba platnosti 6 měsíců (183 dní) Použití 512 bitového kryptografického klíče	základní cena **322**,-- s DPH
typ Standard	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	základní cena **580**,-- s DPH
typ Comfort	Cena zahrnuje : certifikát - doba platnosti 12 měsíců (365 dní) - použití 1024 kryptografického klíče - čipová karta	základní cena prvotního certifikátu **1556**,-- s DPH následný (obnovený) komerční certifikát

	- ovládací SW I.CA	základní cena **580** ,-- s DPH
Certifikát pro server	Doba platnosti 6 měsíců (183 dní) Použití 512 bitového kryptografického klíče	základní cena **1073**,-- s DPH
Certifikát pro server	Doba platnosti 12 měsíců (365 dní) Použití 1024 bitového kryptografického klíče	základní cena **1931**,-- s DPH

Zdroj: (1)

7. Zhodnocení návrhu řešení a závěr

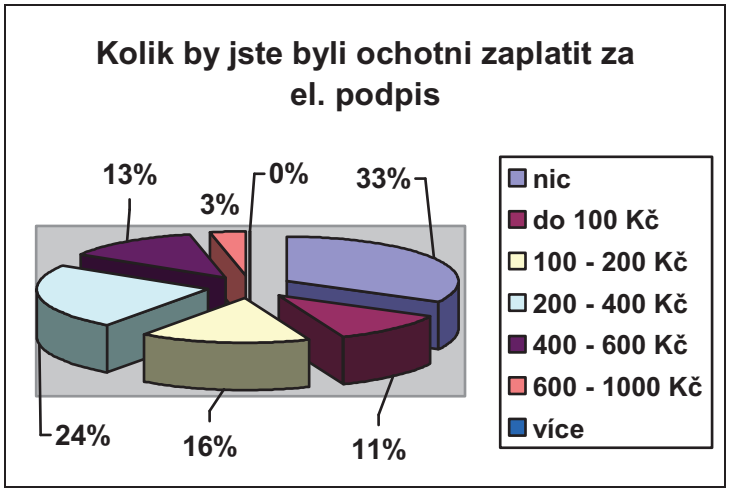
7.1 Vyhodnocení dotazníku

Na dotazník, který obsahuje 13 otázek, odpovídalo 43 osob ženského i mužského pohlaví, různého věku, vzdělání i různých povoláni. Nejmladšímu respondentovi bylo 18 let, nejstaršímu 72 let. Z dotazníku jsem vybral odpovědi na otázku číslo 13 s ukázkou grafu.

13. Kolik by jste byli ochotni zaplatit za elektronický podpis:

nic do 100 Kč 100 – 200 Kč 200 – 400 Kč

400 – 600 Kč 600 – 1000 Kč více



Graf 1: Cena

Zdroj: vlastní

Z dotazníku vyplývá, že podvědomí o elektronickém podpisu je velmi malé, proto také více jak 70% dotazovaných nikdy nepřemýšlelo o zřízení si elektronického podpisu. Většina dotazovaných někdy o elektronickém podpisu někdy slyšela, ovšem ví velmi málo nebo nic o jeho využití a o ceně. Po vysvětlení veškerého využití elektronického podpisu by si tuto službu pořídili především muži, ve věku mezi 20ti až 40ty lety, se středoškolským nebo vysokoškolským vzděláním a s připojením na internet z domu. Z dotazníku dále plyne, že cena, kterou by byli dotazovaní ochotni za elektronický podpis zaplatit by se pohybovala většinou mezi 100 Kč až 600 Kč. Více jak 90 % dotazovaných by bylo důležité, aby dostali k elektronickému podpisu návod na jeho zprovoznění a použití.

Zároveň s psaním diplomové práce jsem si pořídil elektronický podpis. Pořizoval jsem si ho na České poště, Cena byla nižší, než ve výše uvedených tabulkách, protože je to od jiného zprostředkovatele certifikačních služeb. Pořizoval jsem si certifikát pro Ověření elektronického podpisu fyzické osoby v1.20 a stál Kč 190,-. Samotná instalace a zprovoznění elektronického podpisu nebyla složitá a zabrala asi 2 hodiny času. Je zde nevýhodou, že elektronický podpis nelze použít bez např. Outlook Express nebo Mozilla Thunderbird, protože emailové schránky např. na http://www.seznam.cz nebo na http://www.centrum.cz nepodporují podpisové funkce. Certifikát je platný jeden rok.

Vzhledem k ceně mohu doporučit pořízení elektronického podpisu, ušetří a zjednoduší komunikaci s různými ministerstvy a např. pojišťovnami. Myslím si, že v brzké době se ještě použití elektronického podpisu značně rozšíří a bude mezi lidmi stále používanější.

8. Seznam použitých informačních zdrojů

1. *Ceník služeb* [online]. 2007 [cit. 2010-05-16]. Dostupný z WWW: <http://www.ica.cz/home_cs/?acc=cenik_sluzeb>.

2. *Elektronický podpis* [online]. 2006 [cit. 2010-05-16]. Dostupný z WWW: <http://www.axonnet.cz/p_kc_epcr.htm>.

3. *Jak elektronický podpis používat* [online]. 2006 [cit. 2010-05-16]. Dostupný z WWW: <http://www.602.cz/ep/ep-pouziti.html>.

4. *Kde všude lze využít elektronický podpis* [online]. 2006 [cit. 2010-05-16]. Dostupný z WWW: <http://www.602.cz/ep/ep-priklady.html>.

5. KLANDER, Lars. *Hacker Proof : váš počítač, vaše síť a vaše připojení na Internet - Je to opravdu bezpečné?*. [Překlad Kamila Chybová …et al.]. 1. vyd. Brno : Unis Publishing, 1998. 648 s. ISBN 80-86097-15-3

6. PUŽMANOVÁ, Rita. *Lupa* [online]. 2004 [cit. 2010-05-16]. Kvantová kryptografie pro distribuci klíčů. Dostupné z WWW: <http://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/>.

7. ŠILHÁNEK, Radim. *Bezpečnostní aspekty elektronického obchodu*. [s.l.], 1999. 80 s. KIT VŠE. Diplomová práce.

8. VONDRUŠKA, Pavel. *Úvod do klasických a moderních metod šifrování ALG082 : Elektronický podpis* [online]. Verze 1.0. Praha : 2004 [cit. 2010-05-16]. Dostupný z WWW: <http://www.karlin.mff.cuni.cz/~tuma/nciphers/elektronicky_podpis.pdf>.

9. *Získání a instalace Získání a instalace* [online]. 2006 [cit. 2010-05-16]. Dostupný z WWW: <http://www.602.cz/ep/ep-postup.html>.

9. Seznam zkratek

AES - Advanced Encryption Standard

CEN - European Commitee for Standartization

CSE - Communication Security Establishment

DES - Data Encryption Standard

EES - Enhanced Electronic Signature

IDEA - International Data Encryption Algorithm.

MD5 – Message Digest Algorithm

PGP - Pretty Good Privacy

RSA - Ron Rivest, Adi Shamir a Joe Aleman

SHA-1 – Secure Hash Algorithm

SSL - secure sockets layer

10. Seznam obrázků

11. Seznam tabulek

12. Seznam grafů

13. Rejstřík

14. Seznam příloh

Příloha A - Zákonná úprava elektronického podpisu v ČR

Příloha B - Vlastní vytvořený elektronický podpis od PostSignum QCA

Příloha C- Dotazník s grafy

15. Přílohy

15.1 Příloha A

Zákonná úprava elektronického podpisu v ČR

ZÁKON

č. 227 ze dne 29. června 2000

o elektronickém podpisu a o změně některých dalších zákonů

(zákon o elektronickém podpisu)

Změna: 226/2002 Sb., 517/2002 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

Elektronický podpis

§ 1

Účel zákona

Tento zákon upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

§ 2

Vymezení některých pojmů

Pro účely tohoto zákona se rozumí

a) 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,

b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky:

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

c) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou

komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,

d) podepisující osobou fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby,

e) poskytovatelem certifikačních služeb subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

f) akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,

g) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost,

h) 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,

i) daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,

j) daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,

k) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,

l) prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,

m) prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,

n) prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,

o) nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů,

p) akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

§ 3

Soulad s požadavky na podpis

(1) Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem.

(2) Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

§ 4

Soulad s originálem

Použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit.

§ 5

Povinnosti podepisující osoby

(1) Podepisující osoba je povinna

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

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

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

(2) Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů[1]). Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

§ 6

Povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty

(1) Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen

a) zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti kvalifikovaných certifikátů stanovené tímto zákonem,

b) zajistit, aby údaje uvedené v kvalifikovaných certifikátech byly přesné, pravdivé a úplné,

c) před vydáním kvalifikovaného certifikátu bezpečně ověřit odpovídajícími prostředky totožnost osoby, které kvalifikovaný certifikát vydává, případně i její zvláštní znaky, vyžaduje-li to účel kvalifikovaného certifikátu,

d) zjistit, zda v okamžiku vydání kvalifikovaného certifikátu měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát,

e) zajistit, aby se každý mohl ujistit o identitě poskytovatele certifikačních služeb a jeho kvalifikovaném certifikátu,

f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat,

g) zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem,

h) zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát vydán nebo zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám,

i) přijímat do pracovního nebo obdobného poměru osoby, které mají odborné znalosti, zkušenosti a kvalifikaci nezbytnou pro poskytované služby, a které jsou obeznámeny s příslušnými bezpečnostními postupy,

j) používat bezpečné systémy a nástroje elektronického podpisu a zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují; nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou; toto musí být ověřeno Ministerstvem informatiky (dále jen "Ministerstvo"),

k) přijmout odpovídající opatření proti zneužití a padělání kvalifikovaných certifikátů a zajistit utajení dat pro vytváření zaručených elektronických podpisů v případě, že poskytovatel certifikačních služeb umožňuje podepisující osobě jejich vytvoření v rámci poskytovaných služeb,

l) mít k dispozici dostatečné finanční zdroje na provoz v souladu s požadavky uvedenými v tomto zákoně a s ohledem na riziko odpovědnosti za škody,

m) uchovávat veškeré informace a dokumentaci o vydaných kvalifikovaných certifikátech po dobu nejméně 10 let od ukončení platnosti kvalifikovaného certifikátu; informace a dokumentaci může uchovávat v elektronické podobě,

n) před uzavřením smluvního vztahu s osobou, která žádá o vydání kvalifikovaného certifikátu, informovat ji písemně o přesných podmínkách pro užívání kvalifikovaného certifikátu, včetně případných omezení pro jeho použití, a o podmínkách reklamací; je rovněž povinen tuto osobu informovat o tom, zda je či není akreditován Ministerstvem

podle § 10; tyto informace lze předat elektronicky; podstatné části těchto informací musí být na vyžádání k dispozici třetím osobám, které se spoléhají na tento kvalifikovaný certifikát,

o) používat bezpečný systém pro uchovávání kvalifikovaných certifikátů v ověřitelné podobě takovým způsobem, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny porušující tyto bezpečnostní požadavky byly zjevné.

(2) Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, vydává podepisujícím osobám kvalifikované certifikáty na základě smlouvy. Smlouva musí být písemná, jinak je neplatná.

(3) Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, nesmí uchovávat a kopírovat data pro vytváření zaručeného elektronického podpisu osob, kterým poskytuje své certifikační služby.

(4) Pokud byla poskytovateli certifikačních služeb, který vydává kvalifikované certifikáty,

akreditace Ministerstvem odňata, je povinen informovat o této skutečnosti subjekty, kterým poskytuje své certifikační služby a uvést tuto skutečnost v seznamech vedených podle odstavce 1 písm. f) a g).

(5) Není-li poskytovatel certifikačních služeb akreditován Ministerstvem, je povinen ohlásit

Ministerstvu nejméně 30 dnů před vydáním prvního kvalifikovaného certifikátu, že bude vydávat kvalifikované certifikáty.

(6) Pokud poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, uvede v kvalifikovaném certifikátu omezení pro použití tohoto certifikátu včetně omezení hodnoty transakce, pro kterou lze kvalifikovaný certifikát použít, musí být tato omezení rozpoznatelná třetími stranami.

(7) Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.

(8) Poskytovatel certifikačních služeb musí rovněž ukončit platnost kvalifikovaného certifikátu, dozví-li se prokazatelně, že podepisující osoba zemřela nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil[2)], nebo pokud údaje, na základě kterých byl certifikát vydán, přestaly platit.

(9) O veškeré činnosti poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, musí být vedena provozní dokumentace, která musí obsahovat tyto údaje:

a) smlouvu s podepisující osobou o vydání kvalifikovaného certifikátu,

b) vydaný kvalifikovaný certifikát,

c) kopie předložených osobních dokladů podepisující osoby,

d) potvrzení o převzetí kvalifikovaného certifikátu podepisující osobou,

e) přesné časové určení doby platnosti vydaného kvalifikovaného certifikátu.

(10) Zaměstnanci poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji a daty pro vytváření elektronických podpisů podepisujících osob, jsou povinni zachovávat mlčenlivost o osobních údajích, datech pro vytváření elektronických podpisů a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů a dat pro vytváření elektronických podpisů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

§ 7

Odpovědnost za škodu

(1) Za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podle zvláštních právních předpisů[1]).

(2) Poskytovatel certifikačních služeb neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu, která vznikla v důsledku nedodržení omezení pro jeho použití.

§ 8

Ochrana osobních údajů

Ochrana osobních údajů se řídí zvláštním právním předpisem[3]).

§ 9

Akreditace a dozor

(1) Udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb, jakož i dozor nad dodržováním tohoto zákona náleží Ministerstvu.

(2) Ministerstvo

a) uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb subjektům působícím na území České republiky,

b) vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona,

c) vede evidenci udělených akreditací a jejich změn a evidenci poskytovatelů certifikačních služeb, kteří Ministerstvu oznámili, že vydávají kvalifikované certifikáty,

d) pravidelně uveřejňuje přehled udělených akreditací a přehled poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, a to i způsobem umožňujícím dálkový přístup,

e) vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou,

f) plní další povinnosti stanovené tímto zákonem (například § 10 odst. 7, § 13 odst. 2 a § 16 odst. 2).

(3) Za účelem výkonu dozoru je akreditovaný poskytovatel certifikačních služeb vydávající kvalifikované certifikáty povinen pověřeným zaměstnancům Ministerstva umožnit v nezbytně nutném rozsahu vstup do obchodních a provozních prostor, na požádání předložit veškerou dokumentaci, záznamy, doklady, písemnosti a jiné podklady související s jeho činností, umožnit jim v nezbytně nutné míře přístup do svého informačního systému a poskytnout informace a veškerou potřebnou součinnost.

(4) Není-li tímto zákonem stanoveno jinak, postupuje Ministerstvo při výkonu dozoru podle zvláštního právního předpisu[4]).

§ 10

Podmínky udělení akreditace pro poskytování certifikačních služeb

(1) Každý poskytovatel certifikačních služeb může požádat Ministerstvo o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Podání žádosti o akreditaci podléhá správnímu poplatku[5]).

(2) V žádosti o akreditaci podle odstavce 1 musí žadatel doložit

a) obchodní jméno, sídlo a identifikační číslo žadatele,

b) doklad o oprávnění k podnikatelské činnosti a u osoby zapsané do obchodního rejstříku také výpis z obchodního rejstříku ne starší než 3 měsíce,

c) výpis z rejstříku trestů podnikatele - fyzické osoby nebo statutárních představitelů právnické osoby v případě, že žadatelem je právnická osoba, ne starší než 3 měsíce,

d) věcné, personální a organizační předpoklady pro činnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty podle § 6 tohoto zákona,

e) údaj o tom, zda žadatel již vydává nebo hodlá vydávat kvalifikované certifikáty,

f) doklad o zaplacení správního poplatku.

(3) Jestliže žádost neobsahuje všechny požadované údaje, Ministerstvo řízení přeruší a vyzve žadatele, aby ji ve stanovené lhůtě doplnil. Jestliže tak žadatel v této lhůtě neučiní, Ministerstvo řízení zastaví. Správní poplatek se v takovém případě nevrací.

(4) Splňuje-li žadatel všechny podmínky předepsané tímto zákonem pro udělení akreditace, vydá Ministerstvo rozhodnutí, jímž mu akreditaci udělí. V opačném případě žádost o udělení akreditace zamítne.

(5) Akreditovaný poskytovatel certifikačních služeb musí mít sídlo na území České republiky.

(6) Kromě činností uvedených v tomto zákoně může akreditovaný poskytovatel certifikačních služeb bez souhlasu Ministerstva působit jen jako advokát, notář nebo znalec[6]).

(7) Součástí rozhodnutí Ministerstva o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Ministerstvem.

§ 11

V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty, vydávané akreditovanými poskytovateli certifikačních služeb. To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je zaručený elektronický podpis založený na kvalifikovaném certifikátu užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.

§ 12

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,

b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,

c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,

d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,

e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,

f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

§ 13

Povinnosti akreditovaného poskytovatele certifikačních služeb při ukončení činnosti

(1) Akreditovaný poskytovatel certifikačních služeb musí záměr ukončit svou činnost ohlásit Ministerstvu nejméně 3 měsíce před plánovaným datem ukončení činnosti a musí vynaložit veškeré možné úsilí na to, aby platné kvalifikované certifikáty byly převzaty jiným akreditovaným poskytovatelem certifikačních služeb. Akreditovaný poskytovatel certifikačních služeb dále musí prokazatelně informovat každou podepisující osobu, které poskytuje své certifikační služby, o svém záměru ukončit svoji činnost nejméně 2 měsíce předem.

(2) Nemůže-li akreditovaný poskytovatel certifikačních služeb zajistit, aby platné kvalifikované certifikáty převzal jiný akreditovaný poskytovatel certifikačních služeb, je povinen na to včas Ministerstvo upozornit. V takovém případě Ministerstvo převezme evidenci vydaných kvalifikovaných certifikátů a oznámí to dotčeným podepisujícím osobám.

(3) Ustanovení odstavců 1 a 2 se použijí přiměřeně také v případě, když akreditovaný poskytovatel certifikačních služeb zanikne, zemře nebo přestane vykonávat svoji činnost, aniž splní ohlašovací povinnost podle odstavce 1.

§ 14

Opatření k nápravě

(1) Zjistí-li Ministerstvo, že akreditovaný poskytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě sjednal nápravu a případně určí, jaká opatření k odstranění nedostatků je tento poskytovatel certifikačních služeb povinen přijmout.

(2) V případě, že se akreditovaný poskytovatel certifikačních služeb dopustí závažnějšího porušení povinností stanovených tímto zákonem nebo ve stanovené lhůtě

neodstraní nedostatky zjištěné Ministerstvem, je Ministerstvo oprávněno mu udělenou akreditaci odejmout.

(3) Rozhodne-li Ministerstvo o odnětí akreditace, může ukončit současně platnost kvalifikovaných certifikátů vydaných poskytovatelem certifikačních služeb v době platnosti akreditace.

§ 15

Zrušení kvalifikovaného certifikátu

(1) Ministerstvo může nařídit poskytovateli certifikačních služeb jako předběžné opatření[7])

zneplatnění kvalifikovaného certifikátu podepisující osoby, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán nebo pokud byl vydán na základě nepravdivých údajů. Nařízení o zneplatnění kvalifikovaného certifikátu může být vydáno také v případě, kdy bylo zjištěno, že podepisující osoba používá prostředek pro vytváření podpisu, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo změnu podepisovaných údajů.

(2) Seznam certifikátů podle § 6 odst. 1 písm. g) musí obsahovat přesný časový údaj, od kdy byl certifikát zneplatněn. Zneplatněné certifikáty není povoleno opětovně zprovoznit a používat.

§ 16

Uznávání zahraničních certifikátů

(1) Certifikát, který je vydán zahraničním poskytovatelem certifikačních služeb jako kvalifikovaný ve smyslu tohoto zákona, může být používán jako kvalifikovaný certifikát tehdy, je-li uznán poskytovatelem certifikačních služeb, který vydává kvalifikované certifikáty podle tohoto zákona, a za podmínky, že tento poskytovatel certifikačních služeb zaručí ve stejném rozsahu jako u svých kvalifikovaných certifikátů správnost a platnost kvalifikovaného certifikátu vydaného v zahraničí.

(2) Certifikát, který je vydán zahraničním poskytovatelem certifikačních služeb jako kvalifikovaný ve smyslu tohoto zákona, je uznán jako kvalifikovaný certifikát tehdy, pokud to vyplývá z rozhodnutí Ministerstva nebo mezinárodních smluv nebo pokud bude mezi příslušným zahraničním orgánem nebo zahraničním poskytovatelem certifikačních služeb a Ministerstvem uzavřena dohoda o vzájemném uznávání certifikátů.

§ 17

Prostředky pro bezpečné vytváření
a ověřování zaručených elektronických podpisů

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

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

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

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

(2) Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

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

a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,

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

c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,

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

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

f) bylo jasně uvedeno použití pseudonymu,

g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§ 18

Pokuty

(1) Akreditovanému poskytovateli certifikačních služeb nebo poskytovateli certifikačních služeb vydávajícímu kvalifikované certifikáty, který poruší povinnost uloženou mu tímto zákonem, může Ministerstvo uložit pokutu až do výše 10 000 000 Kč.

(2) Pokud akreditovaný poskytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty porušil do jednoho roku ode dne, kdy nabylo rozhodnutí o uložení pokuty právní moci, povinnosti uložené mu tímto zákonem opakovaně, může mu být uložena pokuta do výše 20 000 000 Kč.

(3) Akreditovaný poskytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty, který maří kontrolu prováděnou Ministerstvem, může být potrestán pořádkovou pokutou do výše 1 000 000 Kč, a to i opakovaně.

(4) Osobě, která, byť z nedbalosti, neposkytne Ministerstvu při výkonu kontroly potřebnou součinnost, může být uložena pokuta do výše 25 000 Kč, a to i opakovaně.

(5) Při rozhodování o výši pokuty se přihlíží zejména ke způsobu jednání, míře zavinění, závažnosti, rozsahu, době trvání a následkům protiprávního jednání.

(6) Pokutu lze uložit do jednoho roku ode dne, kdy příslušný orgán porušení povinnosti zjistil, nejdéle však do tří let ode dne, kdy k porušení povinnosti došlo.

(7) Pokutu vybírá Ministerstvo. Pokutu vymáhá územní finanční orgán podle zvláštního právního předpisu[8]).

(8) Výnos pokut je příjmem státního rozpočtu České republiky.

§ 19

Není-li v tomto zákoně stanoveno jinak, vztahuje se na řízení podle tohoto zákona zvláštní právní předpis[9]).

§ 20

Zmocňovací ustanovení

Ministerstvo se zmocňuje vydávat vyhlášky k upřesňování podmínek stanovených v § 6 a 17

a způsobu, jakým se jejich splnění bude dokládat, a k upřesnění požadavků, které musí splňovat nástroje elektronického podpisu, a k náležitostem postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.

ČÁST DRUHÁ

Změna občanského zákoníku

§ 21

Zákon č. 40/1964 Sb., občanský zákoník, ve znění zákona č. 58/1969 Sb., zákona č. 131/1982 Sb., zákona č. 94/1988 Sb., zákona č. 188/1988 Sb., zákona č. 87/1990 Sb.,

zákona č. 105/1990 Sb., zákona č. 116/1990 Sb., zákona č. 87/1991 Sb., zákona č. 509/1991 Sb., zákona č. 264/1992 Sb., zákona č. 267/1994 Sb., zákona č. 104/1995 Sb.,

zákona č. 118/1995 Sb., zákona č. 89/1996 Sb., zákona č. 94/1996 Sb., zákona č. 227/1997 Sb., zákona č. 91/1998 Sb., zákona č. 165/1998 Sb., zákona č. 159/1999 Sb.,

zákona č. 363/1999 Sb., zákona č. 27/2000 Sb. a zákona č. 103/2000 Sb., se mění takto:

V § 40 odst. 3 se doplňuje tato věta: "Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.".

ČÁST TŘETÍ

Změna zákona č. 337/1992 Sb. o správě daní a poplatků

§ 22

Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění zákona č. 35/1993 Sb., zákona č. 157/1993 Sb., zákona č. 302/1993 Sb., zákona č. 315/1993 Sb., zákona č. 323/1993 Sb., zákona č. 85/1994 Sb., zákona č. 255/1994 Sb., zákona č. 59/1995 Sb.,
zákona č. 118/1995 Sb., zákona č. 323/1996 Sb., zákona č. 61/1997 Sb., zákona č. 242/1997 Sb., zákona č. 91/1998 Sb., zákona č. 168/1998 Sb. a zákona č. 29/2000 Sb., se
mění takto:

V § 21 odstavce 2 a 3 znějí:

"(2) Stanoví-li tak tento nebo zvláštní zákon, podávají daňové subjekty o své daňové povinnosti příslušnému správci daně přiznání, hlášení a vyúčtování na předepsaných tiskopisech. Tiskopisy zveřejněné v elektronické podobě lze podepsat elektronicky podle zvláštních předpisů.

(3) Jiná podání v daňových věcech, jako jsou oznámení, žádosti, návrhy, námitky, odvolání apod. lze učinit buď písemně nebo ústně do protokolu nebo elektronicky podepsané podle zvláštních předpisů či za použití jiných přenosových technik (dálnopis, telefax apod.).".

ČÁST ČTVRTÁ

Změna správního řádu

§ 23

Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění zákona č. 29/2000 Sb., se mění takto:

V § 19 odstavec 1 zní:

"(1) Podání lze učinit písemně nebo ústně do protokolu nebo v elektronické podobě podepsané elektronicky podle zvláštních předpisů. Lze je též učinit telegraficky; takové podání obsahující návrh ve věci je třeba písemně nebo ústně do protokolu doplnit nejpozději do 3 dnů.".

ČÁST PÁTÁ

Změna občanského soudního řádu

§ 24

Zákon č. 99/1963 Sb., občanský soudní řád, ve znění zákona č. 36/1967 Sb., zákona č. 158/1969 Sb., zákona č. 49/1973 Sb., zákona č. 20/1975 Sb., zákona č. 133/1982 Sb.,
zákona č. 180/1990 Sb., zákona č. 328/1991 Sb., zákona č. 519/1991 Sb., zákona č. 263/1992 Sb., zákona č. 24/1993 Sb., zákona č. 171/1993 Sb., zákona č. 117/1994 Sb.,
zákona č. 152/1994 Sb., zákona č. 216/1994 Sb., zákona č. 84/1995 Sb., zákona č. 118/1995 Sb., zákona č. 160/1995 Sb., zákona č. 238/1995 Sb., zákona č. 247/1995 Sb.,
nálezu Ústavního soudu č. 31/1996 Sb., zákona č. 142/1996 Sb., nálezu Ústavního soudu
č. 269/1996 Sb., zákona č. 202/1997 Sb., zákona č. 227/1997 Sb., zákona č. 15/1998 Sb.,
zákona č. 91/1998 Sb., zákona č. 165/1998 Sb., zákona č. 326/1999 Sb., zákona č. 360/1999 Sb., nálezu Ústavního soudu č. 2/2000 Sb., zákona č. 27/2000 Sb., zákona č. 30/2000 Sb., zákona č. 46/2000 Sb., zákona č. 105/2000 Sb. a zákona č. 130/2000 Sb., se mění takto:

V § 42 odstavec 1 zní:

"(1) Podání je možno učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky nebo telefaxem.".

ČÁST ŠESTÁ

Změna trestního řádu

§ 25

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění zákona č. 57/1965 Sb., zákona č. 58/1969 Sb., zákona č. 149/1969 Sb., zákona č. 48/1973 Sb., zákona
č. 29/1978 Sb., zákona č. 43/1980 Sb., zákona č. 159/1989 Sb., zákona č. 178/1990 Sb.,
zákona č. 303/1990 Sb., zákona č. 558/1991 Sb., zákona č. 25/1993 Sb., zákona č. 115/1993 Sb., zákona č. 292/1993 Sb., zákona č. 154/1994 Sb., nálezu Ústavního soudu
č. 214/1994 Sb., nálezu Ústavního soudu č. 8/1995 Sb., zákona č. 152/1995 Sb., zákona

č. 150/1997 Sb., zákona č. 209/1997 Sb., zákona č. 148/1998 Sb., zákona č. 166/1998 Sb.,
zákona č. 191/1999 Sb., zákona č. 29/2000 Sb. a zákona č. 30/2000 Sb., se mění takto:

V § 59 odstavec 1 zní:

"(1) Podání se posuzuje vždy podle svého obsahu, i když je nesprávně označeno. Lze je učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky, telefaxem nebo dálnopisem.".

ČÁST SEDMÁ

Změna zákona o ochraně osobních údajů

§ 26

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, se mění takto:

V § 29 se doplňuje odstavec 4, který zní:

"(4) Ministerstvo uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb a provádí dozor nad dodržováním povinností stanovených zákonem o elektronickém podpisu.".

ČÁST OSMÁ

Změna zákona o správních poplatcích

§ 27

Zákon č. 368/1992 Sb., o správních poplatcích, ve znění zákona č. 10/1993 Sb., zákona
č. 72/1994 Sb., zákona č. 85/1994 Sb., zákona č. 273/1994 Sb., zákona č. 36/1995 Sb., zákona
č. 118/1995 Sb., zákona č. 160/1995 Sb., zákona č. 301/1995 Sb., zákona č. 151/1997 Sb.,
zákona č. 305/1997 Sb., zákona č. 149/1998 Sb., zákona č. 157/1998 Sb., zákona
č. 167/1998 Sb., zákona č. 63/1999 Sb., zákona č. 166/1999 Sb., zákona č. 167/1999 Sb.,
zákona č. 223/1999 Sb., zákona č. 326/1999 Sb., zákona č. 352/1999 Sb., zákona
č. 357/1999 Sb., zákona č. 360/1999 Sb., zákona č. 363/1999 Sb., zákona č. 46/2000 Sb.,
zákona č. 62/2000 Sb., zákona č. 117/2000 Sb., zákona č. 133/2000 Sb. a zákona
č. 151/2000 Sb., se mění takto:

1. v příloze k zákonu (Sazebník správních poplatků) se doplňuje nová část XII, která zní:

"ČÁST XII

Řízení podle zákona o elektronickém podpisu

Položka 162

a) podání žádosti o akreditaci poskytovatele certifikačních služeb Kč 100 000,-

b) podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky Kč 10 000,-.".

2. Rejstřík k Sazebníku se doplňuje o část XII, která zní:

"ČÁST XII

Řízení podle zákona o elektronickém podpisu 162.".

3. Tečka za částí XI se vypouští.

ČÁST DEVÁTÁ

Účinnost

§ 28

Tento zákon nabývá účinnosti prvním dnem třetího kalendářního měsíce po dni jeho vyhlášení.

Klaus v.r.

Havel v.r.

Zeman v.r.

1) Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

2) § 10 zákona č. 40/1964 Sb., občanský zákoník, ve znění zákona č. 509/1991 Sb.

3) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

4) Zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

5) Zákon č. 368/1992 Sb., o správních poplatcích, ve znění pozdějších předpisů.

6) Zákon č. 85/1996 Sb., o advokacii, ve znění zákona č. 210/1999 Sb., zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů, zákon č. 36/1967 Sb., o znalcích a tlumočnících.

7) § 43 zákona č. 71/1967 Sb., o správním řízení (správní řád).

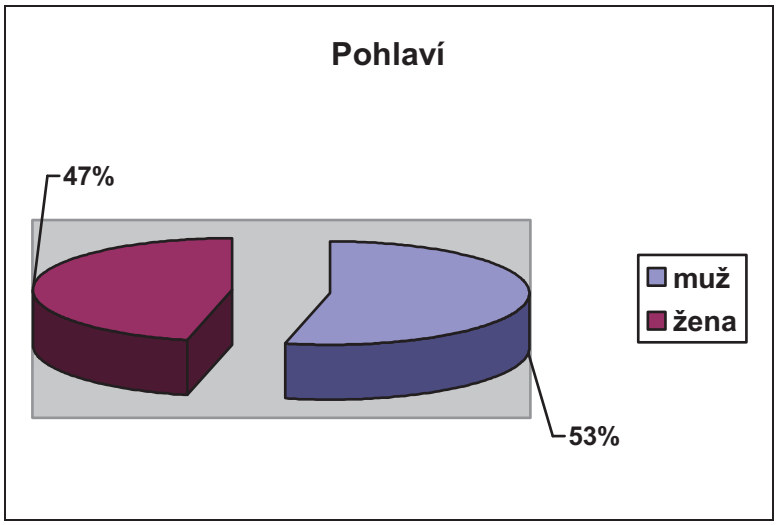
8) Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

9) Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů.

15.2 Příloha C

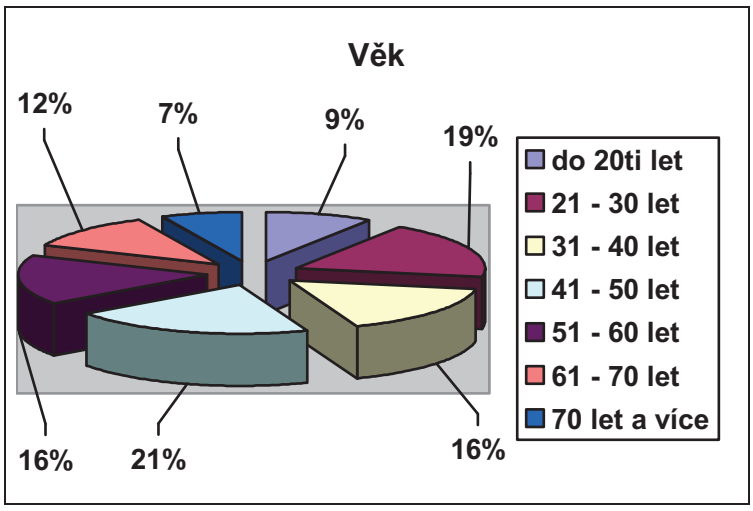
1. Pohlaví:

žena muž



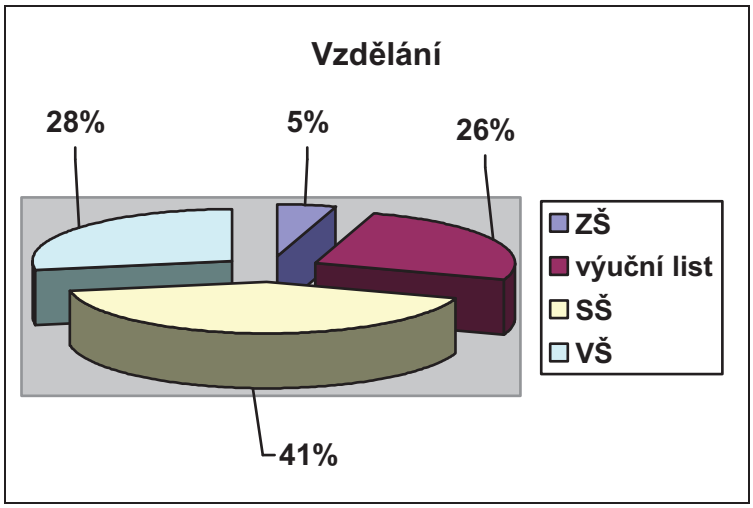
2. Věk:

do 20ti let 21 – 30 let 31 – 40 let 41 – 50 let 51 – 60 let 61 – 70 let více



3. Vzdělání:

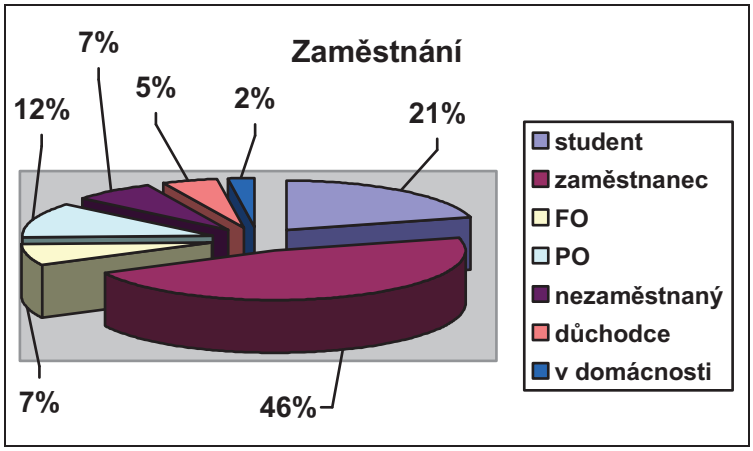
ZŠ vyučen/a SŠ VŠ



4. Zaměstnání:

student zaměstnanec FO PO nezaměstnaný

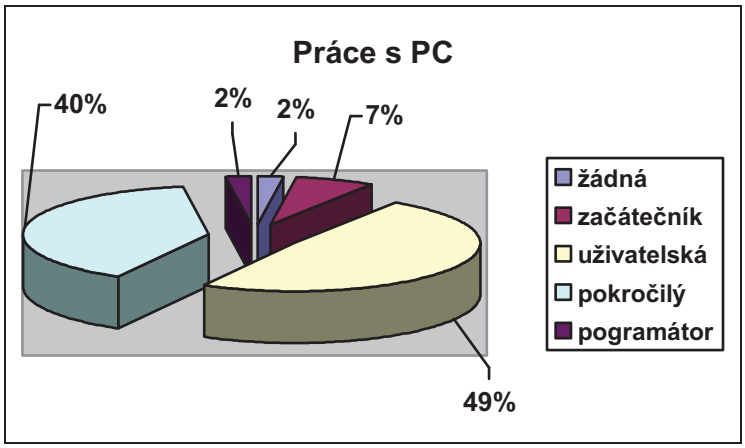
důchodce v domácnosti



5. Práce s PC:

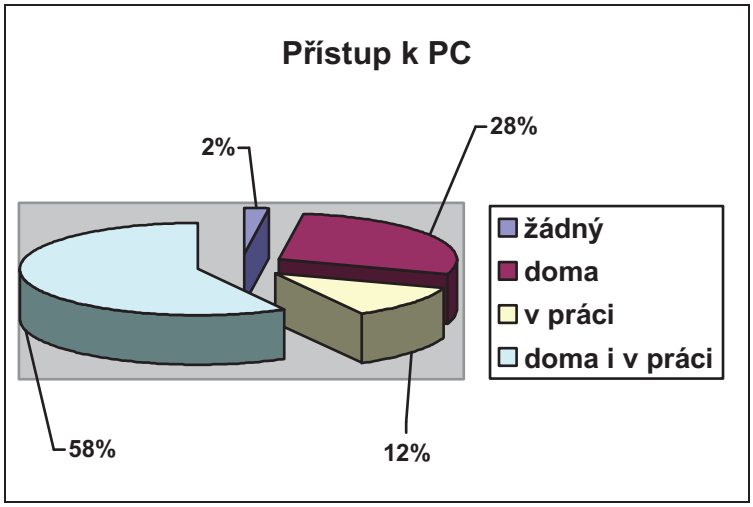
žádná začátečník uživatelská pokročilý programátor

..



6. Přístup k PC:

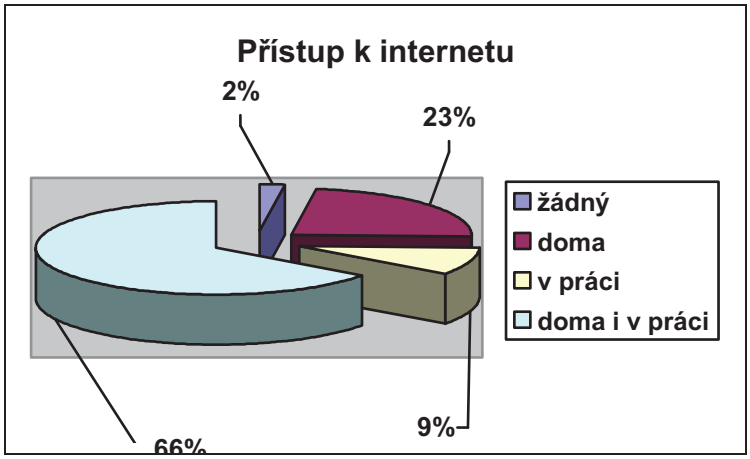
žádný doma v práci doma i v práci



7. Přístup k internetu:

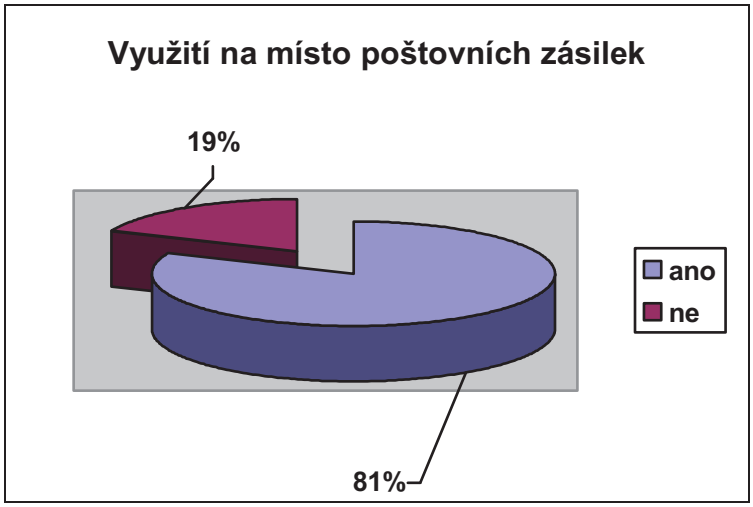
žádný doma v práci mobilní telefon doma i v práci

mobilní telefon, doma, v práci



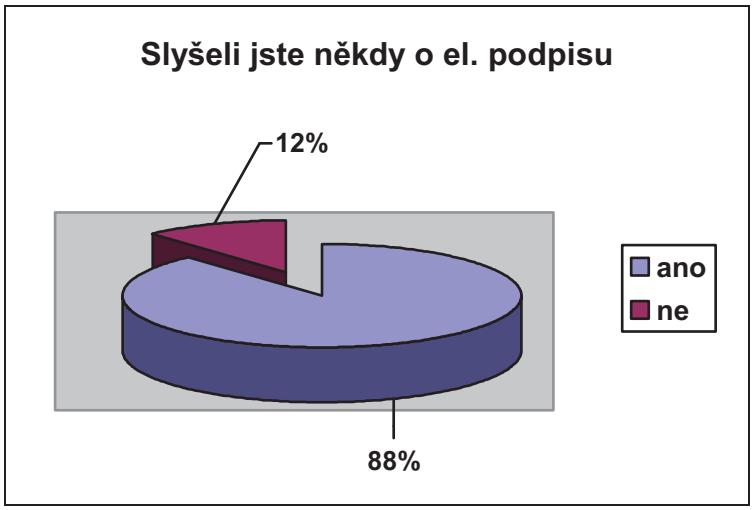
8. Využívali by jste raději el. komunikaci na místo poštovních zásilek, pokud by měla stejnou právní hodnotu:

ano ne



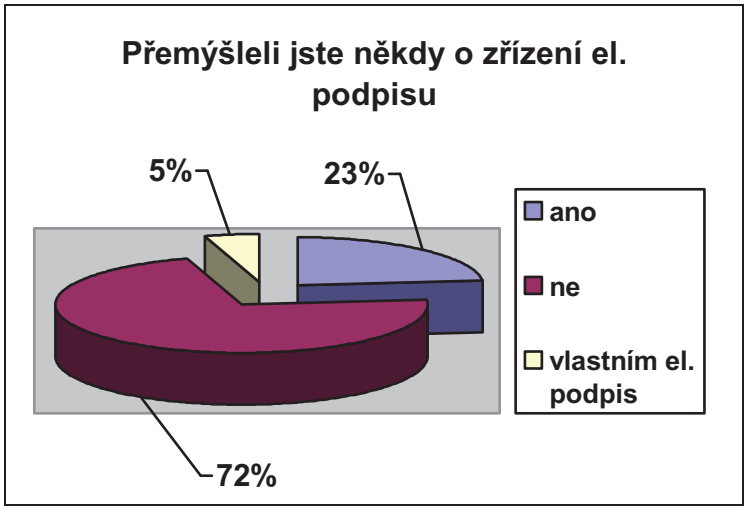
9. Slyšeli jste někdy o elektronickém podpisu:

ano ne



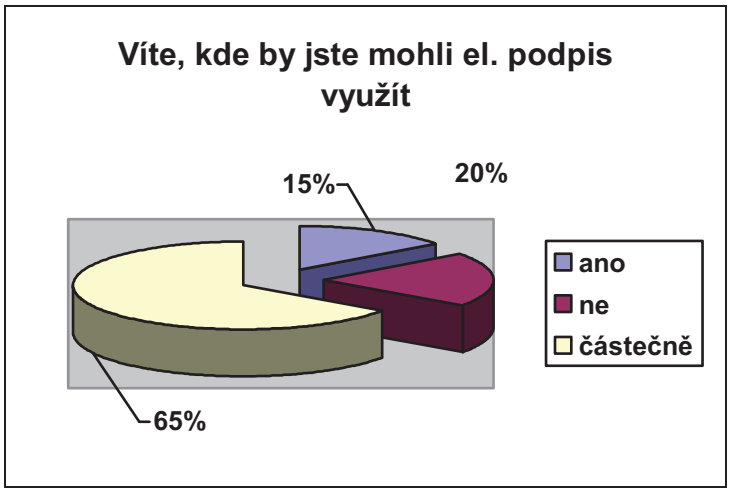
10. Přemýšleli jste někdy o zřízení elektronického podpisu:

ano ne vlastním el. podpis



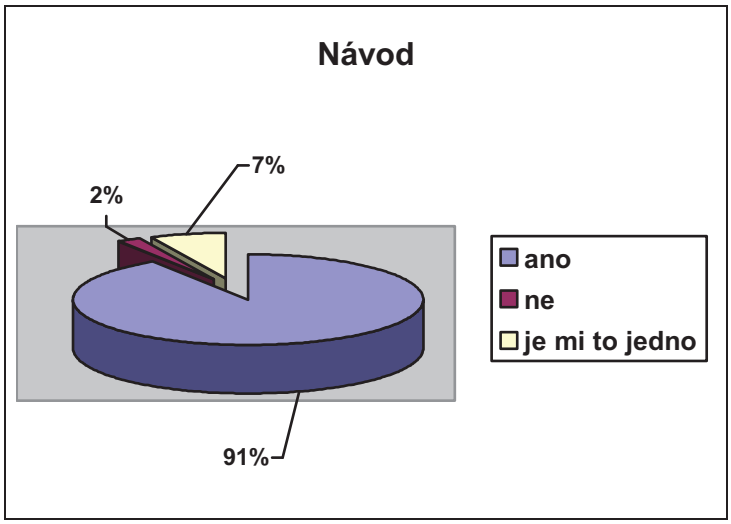
11. Víte, kde by jste mohli elektronický podpis využít:

ano ne částečně



12. Bylo by pro Vás důležité, pokud by jste se rozhodli zřídit si el. podpis, mít srozumitelný návod, na zprovoznění elektronického podpisu:

ano ne je mi to jedno



13. Kolik by jste byli ochotni zaplatit za elektronický podpis:

nic do 100 Kč 100 – 200 Kč 200 – 400 Kč

400 – 600 Kč 600 – 1000 Kč více