Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Šifrování elektronické pošty

Lenka Fořtíková

Česká zemědělská univerzita v Praze | Provozně ekonomická fakulta

Katedra informačních technologií | Akademický rok 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Lenka Fořtíková

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 16 určuje tuto bakalářskou práci.

Název práce: **Sifrovani elektronicke posty**

Osnova bakalářské práce:

1. Úvod
2. Cíl práce a metodika
3. Teoretická východiska
4. Analytická část
5. Výsledky a diskuse
6. Závěr
7. Seznam použitých zdrojů
8. Přílohy

Rozsah hlavní textové části: 30 - 40 stran

Doporučené zdroje:

Kryptografie : průvodce pro každého / Fred Piper, Sean Murphy ; přeložil Pavel Mondschein. - 1. vyd.. - Praha : Dokořán, 2006. - 157 s. ISBN 80-7363-074-5

Šifrování a biometrika aneb tajemné bity a dotyky / Ondřej Bitto. - 1. vyd.. - Kralice : Computer Media, 2005. - 168 s. ISBN 80-86686-48-5

Applied cryptography : protocols, algorithms, and source code in C / Bruce Schneier. - 2nd ed.. - New York (NY) : Wiley & Sons, 1996. - xxiii, 758 s. ISBN 0-471-11709-9

E-mail security : how to keep your electronic messages private / Bruce Schneier. - New York [etc.] : Wiley & Sons, 1995. - 365 s. ISBN 0-471-05318-X

Digitální svět / Nicholas Negroponte. - 1. vyd.. - Praha : Management Press, 2001. - 207 s. ISBN 80-7261-046-5

PGP : pretty good privacy / Simson Garfinkel. - 1. vyd.. - Praha : Computer Press, 1998. - xxxi, 373 s. ISBN 80-7226-054-5

Vedoucí bakalářské práce: **RNDr. Dagmar Brechlerová, Ph.D.**

Termín odevzdání bakalářské práce: duben 2011

.....
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

.....
Děkan

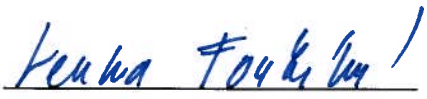
V Praze dne: 19. 2. 2010

Evidováno děkanátem PEF pod č.j.: KIT-259-10B

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Šifrování elektronické pošty" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 24. listopadu 2011



Poděkování

Ráda bych touto cestou poděkovala mojí vedoucí bakalářské práce RNDr. Dagmar Brechlerové, Ph.D. a mé rodině za podporu během mých studií.

Šifrování elektronické pošty

E-mail encryption

Souhrn

Tato bakalářská práce se zabývá problematikou nelegálního zneužití informací a citlivých dat získaných prostřednictvím nezabezpečené e-mailové komunikace. Cílem práce je seznámit laického čtenáře s obecnými postupy k zajištění bezpečnosti dat, s kryptografickými metodami a systémy, nastínit funkci soukromých a veřejných klíčů při posílání e-mailových zpráv a navrhnout vhodnou kombinaci zabezpečení elektronické pošty pomocí kryptografických mechanismů podle předem zadaných požadavků.

Summary

This thesis deals with the illegal acquisition and misuse of sensitive information and data gained through an unsecured e-mail communication. The aim is to acquaint the lay reader with the general procedures for ensuring data security, cryptographic methods and systems, to outline the function of private and public key when sending e mail messages and to propose a suitable combination of email security using cryptographic mechanisms according to pre-specified requirements.

Klíčová slova: kryptografie, šifrování, soukromý klíč, veřejný klíč, certifikát, elektronický podpis, certifikační autorita, zabezpečení, elektronická pošta, časové razítko

Keywords: cryptography, encryption, private key, public key, certificate, an electronic signature certification authority, security, e-mail, time stamp

OBSAH

SEZNAM OBRÁZKŮ

1. ÚVOD

V dnešní době, kdy platí, že „čas jsou peníze“, a kdy Internet nabízí pro své uživatele stále více služeb a slaví obrovský rozmach, je e-mailová komunikace naprosto běžnou a každodenně lidmi po celém světě využívanou službou. Jak v osobním, tak v pracovním životě jsou přes Internet sdílené soukromé informace, údaje a data různého druhu a důvěrnosti. Je tedy zcela nepřípustné, aby tyto informace mohl někdo nepovolaný číst, měnit, nebo využít ke svému zisku a škodě druhého. Mnohdy si ani sami uživatelé neuvědomují, jaká nebezpečí hrozí, pokud svá důvěrná data nijak neochrání.

Služby e-mailové komunikace jsou vnímány automaticky jako náležitě a dostatečně zabezpečené. Realita je ovšem jiná. E-mailová komunikace, včetně přenosů dat, je bohužel zabezpečena pouze základními funkcemi a pro profesionální útočníky poměrně snadno napadnutelná a zneužitelná.

Tato bakalářská práce se zabývá problematikou nelegálního zneužití informací a citlivých dat získaných prostřednictvím nezabezpečené e-mailové komunikace. Navrhuje kombinaci zabezpečení, pomocí nichž lze s využitím kryptografických metod e-mailovou komunikaci ochránit.

Téma bakalářské práce je velmi aktuální, jelikož se kryptografie stává díky rychle se rozvíjejícímu odvětví informační technologie neodkladnou a nezbytnou součástí našeho každodenního života v moderním světě.

2. CÍL PRÁCE A METODIKA

Cílem práce je seznámit laického čtenáře s obecnými postupy k zajištění bezpečnosti dat, s kryptografickými metodami a systémy. Dále práce vysvětluje funkci soukromých a veřejných klíčů při posílání e-mailových zpráv a navrhuje vhodnou kombinaci zabezpečení pomocí kryptografických aplikací a mechanismů v souvislosti s používáním elektronické pošty.

Při psaní práce jsou informace převážně čerpány z četby doporučené literatury, částečně na Internetu. Teoretická část popisuje možnosti a obecné metody pro zabezpečení dat. V analytické části je navrženo kryptografické zabezpečení elektronické pošty, detailněji rozebrány tři mechanismy a to elektronické podepisování, časové razítko a použití TLS zabezpečeného protokolu. V závěru práce shrnuje výsledky a celkový přínos práce.

3. TEORETICKÁ VÝCHODISKA

3.1 Kryptologie, kryptografie a kryptoanalýza

Kryptologie je vědní obor, který se zabývá utajením obsahu zpráv. Dělí se na kryptografii, kryptoanalýzu a v současnosti je do kryptologie stále častěji zahrnována i steganografie.

Kryptografie je věda, jejíž název pochází z řeckých slov kryptós (*skrytý*) a gráphein (*psát*). „*Cílem kryptografie není utajit samu existenci zprávy, ale její význam, a to pomocí šifrování. Aby nešlo zprávu přečíst, pozmění se podle pravidel předem dohodnutých mezi odesilatelem a příjemcem. Pokud taková zpráva padne do rukou nepříteli, je nečitelná. Nezná-li nepřítel použitá šifrovací pravidla, pak se mu podaří zjistit obsah zprávy jen s velkým úsilím, anebo vůbec ne.*“[1]

Kryptoanalýza se zabývá problematikou luštění a prolamování ochranných šifer a nalézá metody k proniknutí do kryptografických systémů. Cílem kryptoanalýzy je získání otevřeného textu, anebo alespoň části zašifrovaných informací.

Trochu rozdílně funguje steganografie, která má za úkol skrýt předávanou zprávu do takové podoby, aby nepřítel nepoznal, že je zpráva předávána. Takto předávaná zpráva je většinou skryta ve zprávě jiné, zpravidla je ve srozumitelné podobě. Jako dobrý příklad poslouží metoda, která zahrnuje používání neviditelných inkoustů. Kromě jednodušších metod může steganografie poskytnout metody také mnohem složitější a vyspělejší, jako jsou například zprávy ukryté do obrázku.

V současné době je kryptografie vědním oborem vyučovaným na mnoha univerzitách, používají ji vlády a armádní složky z celého světa, nachází uplatnění v podnikatelském sektoru, ale je vhodná i pro využití v osobním životě.

3.2 Historie a vývoj

Kryptologie ovlivňuje lidstvo již po tisíce let. Níže jsou uvedeny některé nejdůležitější události a mezníky v dějinách.

Skytalé, jež je jistý druh šifrování hojně používaný Sparťany během válečného období, vznikl již v 5. století před naším letopočtem. „*Tento systém se skládal ze dvou*

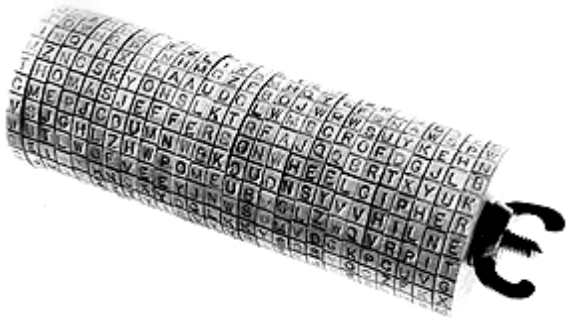
[1] SINGH, S., *Kniha kódů a šifer*, s. 21

shodných holí („skytalé“, někdy psáno „scytale“) přesně stanovené šířky. Na prvou hůl se navinul pás látky, papyru nebo pergamenu a na tento materiál se směrem dolů po celé délce hole napsala zpráva. Pás s textem se sejmul a posel jej odnesl na místo určení. Tam byl pás látky navinut na druhou hůl a zpráva mohla být přečtena.“[2] Mimochodem fungování skytalé popsal ve své knize Plútarchovy životopisy II. (*Plutarch´s Lives, Volume II*) významný řecký spisovatel, filozof a historik Plútarchos.

Julius Caesar, císař římský, popsal ve svých zápiscích o válce galské Caesarovu šifru, kterou používal při své korespondenci. „*Známý životopisec Suetonius popisuje, jak jím zavedený systém přesně vypadal. Každé písmeno zprávy bylo změněno za písmeno, které leželo o tři místa dále v abecedě. Suetonius dále popisuje, že Ceasarův synovec Augustus používal podobný (jednodušší) systém. Nahradil písmeno otevřeného textu písmenem stojícím v abecedě těsně za ním. Výjimkou bylo poslední písmeno X, které nahradil dvojicí AA.*“[3] Popis jiných Ceasarem používaných a mnohem složitějších šifrových systémů se bohužel nedochoval.

Thomas Jefferson, jež byl v pořadí třetím americkým prezidentem, vynalezl v té době dosud nejsilnější kryptografický systém, takzvaný šifrátor.

Obrázek 1 - Šifrátor Thomase Jeffersona



Zdroj: zpracováno dle *VONDRUŠKA, P., Kryptologie, šifrování a tajná písma,* s. 241

Nicméně Thomass Jefferson nepřestal používat tehdy používané šifry a svůj vynález odložil. Ten byl skoro po více jak sto letech znovuobjeven v Kongresové knihovně a následně po desítky let používán americkým námořnictvem. „*Základem je osa, na které je navlečeno 36 disků. Každý disk je po obvodu rozdělen na 26 částí. Do rozdělených částí*

[2] VONDRUŠKA, P., *Kryptologie, šifrování a tajná písma*, s. 197
[3] VONDRUŠKA, P., *Kryptologie, šifrování a tajná písma*, s. 202

je napsána promíchaná abeceda. Jednotlivé disky jsou volné, aby bylo možné je lehce přehazovat. Každý disk má také vlastní číslo, aby bylo možné jednoznačně určit nastavení nástroje. Šifruje se tak, že se nastaví otevřený text (plain text) v jedné řadě napříč jednotlivými disky. Po nastavení se vybere jedna z 25 zbývajících řad, ze které se opíše šifrovaný text.“[4]

První tištěná kniha o kryptografii (*Polygraphia*) vyšla roku 1518 a je dílem Johanna Trithemiuse. „*V pátém díle, který je z kryptografického hlediska nejvýznamnější, je uvedena šifrovací tabulka, tzv. „tabula recta“, která je základem pro polyalfabetické šifry.*

Abcdefghijklmnopqrstuvwxyz
bcdefghijklmnopqrstuvwxyza
cdefghijklmnopqrstuvwxyzab
defghijklmnopqrstuvwxyzabc
efghijklmnopqrstuvwxyzabcd
...
zabcdefghijklmnopqrstuvwxy

Trithemius používal této tabulky k polyalfabetickému šifrování velmi prostě a jednoduše. První písmeno otevřeného textu zašifroval pomocí první abecedy, druhé písmeno pomocí druhé abecedy, atd. Slovo OKO by se zašifrovalo touto metodou jako OLQ.“[5]

V roce 1553 vyšlo další významné dílo (*La Cifra del Sig*) od Giovaniho Bastista Belasa, ve kterém autor popisuje kryptografický systém založený na znalosti hesla, v současnosti tento systém odpovídá použití tajného klíče. Později, roku 1967, vzniklo komplexní dílo o kryptografii od autora Davida Kahna s názvem Luštitelé kódů (*The Codebreakers*). Simon Singh vydal v roce 2003 Knihu kódů a šifer (*The Code Book*).

Avšak z historie kryptografie se nedochovaly pouze knihy. V mnoha muzeích po celém světě jsou k nahlédnutí různé šifrovací přístroje a artefakty.

Muzeum výpočetní techniky Bletchley Park, které bylo během 2. světové války sídlem britských "lamačů kódů", názorně ukazuje vývoj počítačů a celého oboru. Nachází se zde sbírka některých funkčních i nefunkčních modelů počítačů, které se zapsaly do historie. Za zmínku také stojí, že se tu nachází největší sbírka strojů enigma v Evropě, jako

---

4 VONDRUŠKA, P., *Kryptologie, šifrování a tajná písma*, s. 241
5 VONDRUŠKA, P., *Kryptologie, šifrování a tajná písma*, s. 218

jsou například Abwehr Enigma – G312, Army and Air Force Enigma – A16991 a Naval Enigma – M1322. A navíc právě v Bletchley Park prolomil Alan Turing se svým týmem německou šifru Enigma.

Obrázek 2 - Abwehr Enigma – G312

Zdroj: zpracováno dle *http://www.bletchleypark.org.uk/edu/archives/cryptcoll.rhtm*

Mezi další z významných muzeí se řadí Národní muzeum kryptologie v Marylandu. Nachází se v blízkosti ústředí NSA a nabízí ke shlédnutí sbírku tisíců artefaktů. Toto muzeum původně sloužilo k uchovávání artefaktů NSA a bylo místem pro zaměstnance agentury, kde mohli čerpat informace z dosavadních poznatků o kryptografii. Díky obrovskému úspěchu bylo muzeum v roce 1993 otevřeno pro i širokou veřejnost.

3.3 Internet

Internet je rozsáhlý globální otevřený informační systém vzájemně propojených počítačových sítí, ve kterých probíhá komunikace mezi počítači pomocí soustavy protokolů TCP/IP. Název TCP/IP vznikl spojením jmen dvou nejvýznamnějších protokolů z celé soustavy, a to protokolu IP a TCP protokolu. Protokol IP je protokolem síťové vrstvy a má za úkol přepravu dat na místo jejich určení, a to na principu paketového přenosu. TCP je transportním protokolem, který sám využívá služby IP protokolu, ale navíc garantuje spolehlivé doručování dat ve správném pořadí. Paket je blok dat přenášených v počítačové síti.

3.4 Elektronická pošta

Elektronická pošta je v dnešní době nejpoužívanější službou počítačových sítí. Čas, během něhož se zpráva dostane od odesilatele k příjemci, se snížil na minimum. S pomocí elektronické pošty a s využitím počítačové sítě je zpráva doručena příjemci kdekoliv na světě během několika vteřin.

3.4.1 Poštovní schránka a e-mailová zpráva

Chce-li uživatel začít využívat elektronickou poštu, musí si nejprve založit poštovní schránku. Schránka je místo na disku a pro určení místa doručení musí mít poštovní schránka svou adresu, kterou určuje uzlový počítač a identifikátor poštovní schránky v rámci tohoto počítače. Může náležet jednomu uživateli, více uživatelům, nebo může být vytvořena smyšleně za účelem nějaké krátkodobé aktivity. E-mailová zpráva má přesně danou formu. Skládá se z hlavičky a z těla e-mailu. Tělo zprávy je čistý text a nejsou žádná pravidla, jak má vypadat. Na druhou stranu hlavička uchovává, podle přesně daných pravidel, informace o odesilateli, příjemci, data a času odeslání, a předmětu zprávy.

3.4.2 Princip doručení e-mailové zprávy

E-mailovou zprávu, její vytvoření, odeslání a doručení obstarávají tři programy. Pro komunikaci s uživatelem slouží uživatelská složka, neboli poštovní klient MUC. Pro přenos zpráv od odesilatele k příjemci se používá přenosové složky MTA, jinak také nazýváno poštovní server. Došlou zprávu do příjemcovy schránky dle nastavených kritérií doručuje program MDA.

Mezi poštovní klienty se mimo jiné řadí Microsoft Office Outlook, Opera nebo Mozilla Thunderbird. Každý poštovní klient obsahuje vhodný editor, díky kterému může uživatel zprávy vytvářet, editovat, rušit a mazat. Zprávy připravené k odeslání poté předává poštovnímu serveru. Stará se taktéž o vybírání a spravování poštovní schránky, k tomu využívá protokolů POP3 nebo IMAP.

Poštovní server, MTA, potřebuje získat ke svému fungování informace o příjemci, tedy kam má zprávu doručit. Po přijetí zprávy zjistí, jestli náleží jeho lokálnímu počítači. Pokud ne, pošle zprávu dalšímu serveru. Jelikož je více serverů, respektive přenosových

složek, musí být určena pravidla, jednotné konvence a protokoly, podle kterých spolupráce mezi složkami probíhá. Taková spolupráce se nazývá systém přenosu zpráv. Pokud přenos probíhá mezi různými poštovními systémy, tak přechod, tedy transformaci zpráv, mezi nimi zajišťuje takzvaný e-mail gataway. Mezi hlavní používané MTA patří Postfix, Microsoft Exchange, nebo Sendmail.

Po doručení zprávy příslušnému MDA buď dojde k lokálnímu doručení zprávy do příjemcovy schránky, nebo uložení zprávy do úložiště zpráv. Pokud je zpráva uložena do úložiště zpráv, zůstává tam až do chvíle, kdy příjemce zadá požadavek na její vyzvednutí a přečtení. Pro vyzvednutí zprávy musí MDA kontaktovat server, který poskytuje přístup k příslušnému úložišti zpráv. Server po ověření žádosti zašle e-mail MDA, který zprávu doručí příjemci. MDA umí kromě samotného doručování zpráv do příjemcovy schránky také pracovat jako dobrý nástroj pro filtrování zpráv. Po nastavení uživatelem dokáže automaticky odpovídat, ukládat zprávy do předem určených složek, ale také odstraňovat nevyžádanou poštu nebo spam a viry. Mezi MDA, které umí jak doručovat, tak třídit došlé zprávy, patří například Maildrop nebo Procmail.

3.4.3 Poštovní protokol SMTP

Protokol SMTP je internetový protokol určený pro přenos e-mailových zpráv. Jeho architektura je postavena na bázi klient server. Klient zahájí TCP komunikaci se serverem, ten se zpět ohlásí svou uvítací zprávou. Tato zpráva obsahuje kromě dalších informací také trojčíslí označující stav požadovaného příkazu. Z trojčíslí lze zjistit, zda byla požadovaná akce úspěšná a příkaz byl přijat, nebo server očekává další informace od klienta, či příkaz nebyl přijat z důvodu trvalého nebo dočasného problému. Následně klient zašle své DNS jméno, načež sever zašle zpět také své DNS jméno a seznam rozšíření, tedy přidaných funkcích, které používá. Klient zasílá serveru informaci o odesilateli, server odesilatele akceptuje, nebo neakceptuje. Následovně klient zasílá informaci o příjemci, pokud jich je více, opakuje se tento krok tolikrát, kolik je příjemců. Pokaždé server zašle informaci, zda akceptuje příjemce. Nyní dochází ze strany klienta k příkazu značícím samotný přenos e-mailové zprávy. Server následně předá klientovi instrukce o správném označení konce zprávy. Po samotném přenosu server vrátí klientovi informaci o zařazení zprávy do fronty, včetně její identifikace. Klient v tuto chvíli ukončí komunikaci.

3.4.4 Chyby doručení

SMTP poštovní protokol umí rozeznat dva typy chyb, které mohou nastat během doručování e-mailové zprávy. Trvalá chyba nastane, pokud neexistuje server, nebo uživatel. Druhý typ je dočasná chyba a to znamená, že server nekomunikuje, je zaneprázdněný nebo je dočasně nedostupný. V tomto případě probíhají pravidelné pokusy o doručení e-mailové zprávy, a když stále po nastavené lhůtě nelze zprávu doručit, pošle se odesilateli notifikace o nedoručení zprávy a zpráva se zahodí.

3.4.5 POP3 a IMAP4

POP3 je internetový protokol, který umožňuje uživateli stahovat e-mailové zprávy ze serveru do jeho lokální schránky na počítači. Je založen na off-line principu. "*POP3 klient zpravidla navazuje spojení na port 110/tcp serveru. Po navázání spojení se server představí a je v tzv. autentizačním stavu, tj. čeká na autentizaci uživatele. Po kladné autentizaci uživatele se komunikace přepne do transakčního stavu, kdy uživatel může manipulovat s e-maily ve své poštovní schránce na POP3 serveru. Na závěr relace přejde klient do stavu UPDATE, kdy se teprve provedou veškeré změny v poštovní schránce na serveru.*"[6] Autentizací se rozumí autentizace klienta k POP3 serveru, a to pomocí uživatelského jména a hesla. Ovšem komunikace, včetně vyžádání a předání si přihlašovacích údajů probíhá nezabezpečeně, tudíž může dojít k jejich odposlechnutí.

Propracovanější IMAP4 protokol pracuje podobně jako POP3 protokol, ale navíc poskytuje možnost práce se schránkou v režimu on-line. IMAP4 používá pro své spojení port 143/tcp.

3.5 Jak Internet funguje

Internet pracuje pomocí protokolů TCP/IP, které jsou velmi odolné proti různým poruchám a jejich fungování je velmi efektivní. Bohužel je nutné podotknout, že jsou také nespolehlivé a nezabezpečené.

IP protokol původní data rozdělí do potřebného počtu bloků, které se nazývají datagramy. Tyto IP datagramy následně přenáší nespojovaným způsobem, přenášená data

---

[6] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, s. 450

nešifruje a není předem známo, kudy budou datagramy cestovat. Jelikož mohou být „stejná data“ rozdělena do více datagramů, mohou cestovat různými cestami. Pokud se některá data poškodí, IP protokol to sice zjistí, ale nehledá, kde a proč se data poškodila, nezjedná nápravu a tato poškozená data zahodí.

Tento kanál lze zaměnit a použít TCP transportní protokol, který je spojovaný a navíc velmi spolehlivý. TCP sice nepoužívá kryptografické metody k zabezpečení přenášených dat, ale na aplikační vrstvě je možné použití šifrování, nebo jiných zabezpečujících systémů a metod.

TCP/IP se skládá ze čtyř vrstev. Vrstva nejnižší úrovně se nazývá vrstvou síťového rozhraní. Tato vrstva řídí konkrétní přenosové cesty a stará se o příjem a vysílání paketů. Paket je formátovaný blok dat, který obsahuje IP adresu, atributy a data. Pakety jsou zabaleny do rámců, „obálek“, a tyto rámce poté putují po síti. O doručení paketů od odesilatele k příjemci se stará síťová vrstva a jejich přenos zajišťuje transportní vrstva. Nejvyšší vrstvou je vrstva aplikační, která zajišťuje přístup a komunikaci aplikací s transportní vrstvou.

3.6 Rizika Internetu

V současném moderním světě se jako hlavní komunikační kanál využívá Internet. Pomocí Internetu lze například získávat různé informace, provádět elektronické objednávky, platit za zboží, obchodovat, investovat, komunikovat se státními institucemi a úřady, nebo zasílat e-mailové zprávy. Internet je zdrojem poskytujícím mnoho různých služeb a informací.

Nicméně je na místě také otázka, zdali to, co je na internetu, pochází z důvěryhodných zdrojů? Kam nebo komu se dostanou data námi svěřená Internetu? Chatujeme-li si s někým, je to opravdu ten příjemně vypadající mladý muž nebo krásná žena, jak usuzujeme podle profilové fotografie? A ve chvíli, kdy nám přijde e-mail, jak si můžeme ověřit, že je opravdu zaslaný od toho, od koho předpokládáme? Jsme si stoprocentně jisti, že ten, s kým komunikujeme, je opravdu ten, koho myslíme?

Velkým nebezpečím na Internetu jsou nejen lidé, kteří Internet zneužívají k podvodným aktivitám, ale dalším slabým článkem je také chování aplikací. Některé aplikace požadují uživatelské údaje, jako je přihlašovací jméno a heslo, ale přitom tyto

údaje přenáší nezabezpečeně a data nešifrují. Ta potom putují sítí jako čistý otevřený text, který je snadno zneužitelný.

S elektronickou poštou je to podobné jako s klasickou poštovní korespondencí. „*Většina lidí před odesláním dopisu zalepí obálku. Když se jich zeptáte, proč to dělají, odpoví vám většinou něco na způsob „vlastně ani nevím“, „je to zvyk“, „proč ne?“ nebo třeba „dělá to tak každý“. Mezi odůvodněnějšími odpověďmi pravděpodobně budou argumenty jako „aby dopis nevypadl“ či „aby si jej nemohl přečíst každý“.*“[7] Dalším problémem je právě posílání zpráv nezabezpečenou elektronickou poštou. Pokud nebudou zavedena bezpečností opatření, e-mail nedokáže zaručit soukromí. Překvapivě je u zprávy poměrně jednoduché změnit hlavičku a zprávu zaslat jménem někoho jiného. Kromě toho nejsou e-mailové zprávy standardně šifrovány a mnoho poskytovatelů připojení k Internetu si ukládá na své servery před doručením kopie všech e-mailových zpráv a tyto zprávy tam mohou zůstat několik týdnů, nebo i měsíců. A v neposlední řadě je rizikový také přenos e-mailových zpráv. Ty putují sítí po nezabezpečených kanálech, a proto není tak obtížné zprávu zachytit a přečíst.

3.7 Ochrana dat

Data a informace se ukládají do paměti počítače, do databází, jsou posílána elektronickou poštou anebo tisknuta na papír. Ne všechna data lze zpřístupnit všem uživatelům. Data musí být chráněna zejména proti neoprávněné změně, před zničením a musí být zajištěna jejich důvěrnost.

Existuje několik možností, jak svá citlivá data ochránit. Od základních nastavení na osobním počítači, instalaci ochranných programů, až po hardwarovou či personální bezpečnost. Níže budou popsána ta nejdůležitější základní zabezpečení.

3.7.1 Hardware, nosiče informací

Ochrana dat využitím kryptografie může být neúčinná a zbytečná, pokud se také nezabezpečí hardwarové místo, na kterém jsou uložena sdílená tajemství a další kryptografická aktiva. Pokud jsou taková aktiva uložena na lokálním disku, je třeba předpokládat možnost napadení škodlivými programy z Internetu, které mohou mimo jiné získat přístupová hesla nebo přečíst zprávu ještě předtím, než byla zašifrována.

---

[7] PIPER, F., MURPHY, S., *Kryptografie : průvodce pro každého*, s. 7

Řešením pro uchování aktiv mohou být hardwarové klíče. Tyto hardwarové klíče jsou přímo spojeny s počítačem přes příslušné rozhranní, jako jsou například USB, PCI nebo sériový port. Mezi nejpoužívanější hardwarové klíče se řadí čipové karty nebo USB klíče.

V neposlední řadě je rovněž velmi důležitá dobrá fyzická bezpečnost nosičů aktiv, odolnost proti nepřízni přírodních vlivů a proti případným pokusům o poškození či zničení narušitelem.

3.7.2 Personální bezpečnost

Místo, kde jsou data uložena, musí být chráněno proti fyzickému proniknutí. Chráněná data a celý fyzický systém je potřeba zajistit uzamknutím, či uložením do trezoru, případně nechat dozorovat pracovníkem ostrahy, který kontroluje oprávněnost vstupu či přístupu ke chráněnému systému.

Kromě hardwarových zabezpečení je také důležité zajištění personální bezpečnosti, tedy zajistit ochranu logického přístupu k datům. Tuto problematiku řeší identifikace a autentizační metody. Během identifikace uživatel uvede, kdo je, jež následně během autentizace prokazuje. Mezi autentizační metody patří například zadání hesla, nebo prokázání se autentizačním předmětem. V současnosti je nejběžněji používaným autentizačním předmětem vstupní karta s čipem. Další možností autentizace je důkaz biometrické vlastnosti, například dnes již celkem běžná autentizace otiskem prstu. Vyspělejší autentizační systém dokáže provést autentizaci na základě snímání oční sítnice či duhovky.

3.7.3 Záložní zdroje

„*Do oblasti fyzické bezpečnosti můžeme zařadit i ochranu před nekvalitním napájením. Existují zařízení, které dokáží zajistit nejen kvalitu dodávaného proudu (tedy stabilitu jeho úrovně), ale i ochranu před neočekávanými špičkami či výpadky. Obecné označení takového zařízení je záložní zdroj, ale existuje více druhů.*“[8]

Akumulátor, jež je zařízení mezi napájecí sítí a počítačem, se stále dobíjí a pokud dojde k výpadku sítě, je schopen počítač napájet až několik hodin.

---

[8] DOSEDĚL, T., *Počítačová bezpečnost a ochrana dat*, s. 55

Oproti tomu je generátor elektrického proudu poháněn motorem a doba jeho napájení závisí na stavu paliva. Spustí se v případě absolutního selhání síťového nebo akumulátorového napájení.

3.7.4 Antivirový systém

V současnosti je základní nutností kvalitní antivirový systém, zejména používá-li se systém Microsoft Windows. Jde o komplexní antivirové řešení, které identifikuje a odstraňuje počítačové viry, škodlivé skripty, červy šířící se elektronickou poštou, ale také zabraňuje stažení infikovaných souborů do počítače uživatele.

Existuje mnoho metod fungování antivirových programů. Mezi významné metody se řadí například sledování nainstalovaných programů a jejich chování antivirovým programem. Pokud se nainstalovaný program zachová neočekávaně, vyšle antivirový program uživateli upozornění s nabídkou řešení. Další metodou je vyhledávání a kontrola dat antivirovým programem ve virových databázích. Virové databáze jsou neustále aktualizovány, vzhledem k rychle se vyvíjejícím a nově vznikajícím virům.

Pro zajištění spolehlivého zabezpečení by se měl antivirový systém pravidelně aktualizovat. Nicméně aktualizace dnes již probíhají automaticky bez asistence uživatele.

3.7.5 Antispyware program

Spyware je program, který pomocí Internetu odesílá data z počítače, aniž by o tom uživatel věděl. Ochranou jsou antispyware programy, které spyware dokáží spolehlivě nalézat, blokovat a odstraňovat.

3.7.6 Antispam program

Nevyžádané sdělení šířené přes Internet, většinou komerčního rázu, se nazývá spam. Dříve se do spamu řadily reklamní e-maily, v současnosti jsou však postižena také například diskusní fóra a další druhy Internetové komunikace. Program, chránící uživatele před spamem, se nazývá antispam.

3.7.7 Firewall

Firewall je síťové zařízení, které kontroluje informace přicházející z Internetu. Podle jeho nastavení informace buď zablokuje, nebo jim umožní projít do počítače. Brání

tedy počítač uživatele před útočníky a škodlivým softwarem. Také ale dokáže zabránit rozesílání škodlivého softwaru do dalších počítačů. Nastavení pravidel pro komunikaci přes firewall se nazývá Bezpečnostní politika firewallu.

3.7.8 Hesla

Kromě softwarových ochran, jako jsou výše zmíněné antivirové, antispyware, antispamové programy a firewall, je možné použít dlouhodobá či jednorázová hesla. Jelikož jsou hesla většinou přenášena nezabezpečeně, existuje reálná možnost jejich zneužití. Východiskem jsou jednorázová hesla, která jsou platná pouze pro jednu danou transakci a nedají se znovu použít.

3.8 Šifrování

Šifrovací, jinak také šifrový nebo kryptografický systém je systém používaný ke změně otevřeného textu na text nesrozumitelný pro kohokoliv jiného kromě příjemce. Otevřený text je původní text zprávy před zašifrováním. „*Pokud nějaký šifrový systém použijeme na zpracování nějaké zprávy, tak říkáme, že zprávu šifrujeme, nebo že jsme ji zašifrovali. Osoba, která šifrování provádí, se nazývá šifrant nebo šifrér.*“[9]

Vhledem k rozdílu mezi pojmy šifra a kód je nutné poznamenat následující. „*Pomocí šifry nebo přesněji šifrovacího systému se odesílatel a adresát snaží utajit obsah zprávy před nepovolanou osobou. Smyslem kódu není zprávu utajit, ale upravit ji tak, aby ji bylo možné dále příslušným technickým prostředkem zpracovávat, např. přenést nějakým kanálem. Kódovaná zpráva může být na základě znalosti příslušného kódování převedena zpět do původního tvaru.*“[10]

V otevřených sítích, kde nejsou přenosové kanály bezpečné, je rozumné přenášené údaje zabezpečit. Například pomocí kryptografie. Ta se používá mimo jiné k ověření identifikace a autentizace, autorizace, zachování integrity dat, auditingu, zajištění důvěrnosti dat, neodmítnutelnosti autorství a zachování dostupnosti.

Identifikace slouží k ověření autora.

Autentizace potom k ověření, že příslušné údaje o autorovi souhlasí.

---

[9] VONDRUŠKA, P., *Kryptografie, šifrování a tajná písma*, s. 11

[10] VONDRUŠKA, P., *Kryptografie, šifrování a tajná písma*, s. 15

Autorizace souvisí s oprávněním určitého uživatele k přístupu či nějaké aktivitě. Různí uživatelé mají různá oprávnění.

Pro ověření **zachování integrity dat** zjišťujeme, zdali původní data nebyla změněna.

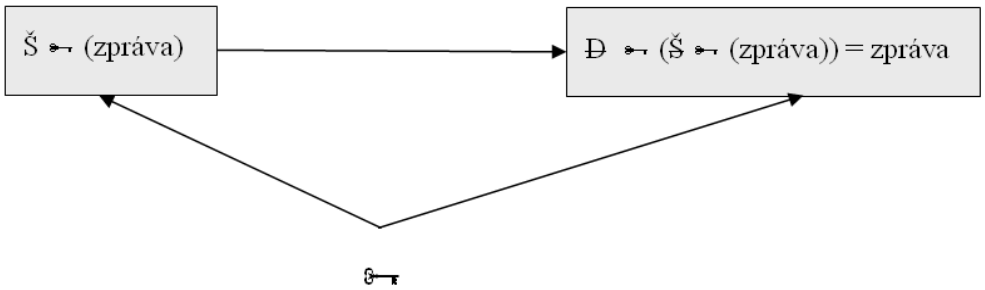
Důvěrnost dat zajistíme pomocí šifrování, které zaručí, že nikdo nepověřený nepřečte důvěrná data.

Auditing poskytuje informace o historii, to znamená informaci o tom, kdo kdy co udělal. Tyto informace jsou výhodné pro případné řešení incidentů.

3.8.1 Symetrické šifrování

Symetrické šifrování se zakládá na jednom tajném šifrovacím klíči. Ten si musí oba účastníci před začátkem vzájemné komunikace vyměnit a nesmějí ho sdílet s nikým dalším. Poté odesilatel před odesláním zprávu zašifruje tajným klíčem a příjemce přijatou zprávu dešifruje stejným tajným klíčem.

Obrázek 3 - Symetrické šifrování



Zdroj: zpracováno dle DOSTÁLEK, L. a kol.*, Velký průvodce infrastrukturou PKI a technologií elektronického podpisu,* s. 24

3.8.2 Asymetrické šifrování

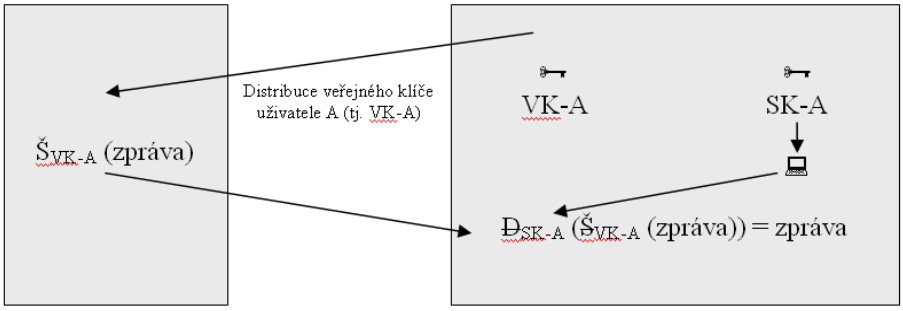
Při asymetrickém šifrování se používá dvojice klíčů, kterou tvoří veřejný a soukromý klíč. Asymetricky je možné šifrovat dvěma způsoby, a to s odlišným použitím páru klíčů.

První varianta je šifrování veřejným klíčem a dešifrování soukromým klíčem. V tomto případě musí příjemce nejdříve vygenerovat soukromý klíč, který si uschová,

a veřejný klíč, který může nezabezpečeně zaslat komukoliv, s kým chce komunikovat. Odesilatel tedy zprávu zašifruje veřejným klíčem příjemce, a pouze příjemce může zprávu dešifrovat svým soukromým klíčem.

Použitím druhé varianty se data zašifrují privátním klíčem odesilatele a dešifrují veřejným klíčem odesilatele. Obdobně jako v první variantě odesilatel generuje dva klíče. Zašifruje zprávu svým soukromým klíčem, s tím rozdílem, že dešifrovat zprávu může kdokoliv, kdo vlastní veřejný klíč odesilatele.

Obrázek 4 - Asymetrické šifrování



VK-A	veřejný klíč uživatele A
SK-A	soukromý klíč uživatele A
ŠVK-A	šifrování veřejným klíček uživatele A
DSK-A	dešifrování soukromým klíčem uživatele A

Zdroj: zpracováno dle DOSTÁLEK, L. a kol., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu,* s. 26

3.8.3 Funkce hash

Jedná se o jednocestnou funkci, která z jakkoli dlouhého textu vytvoří krátký řetězec, otisk. Tento otisk může být spočten pomocí starších a slabších algoritmů, jako je MD-5 s velikostí výstupu 16 B, nebo SHA-1 s velikostí výstupu 20 B. Také lze použít jakýkoliv z novějších algoritmů, například SHA-256, patřící do skupiny algoritmů SHA-2. Tyto algoritmy jsou mnohem silnější a rozsáhlejší, a proto vypočtou otisk o větší velikosti výstupu než MD-5 nebo SHA-1.

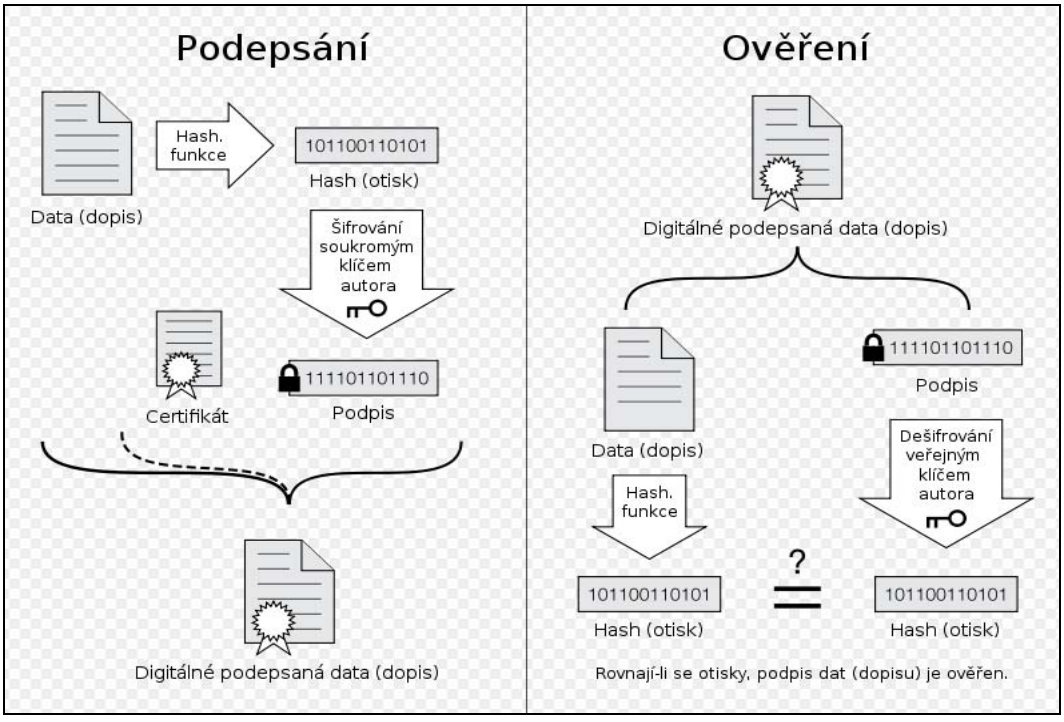
3.8.4 Časová razítka

Časové razítko je k dokumentu připojená informace o času jeho vytvoření. V podstatě jde o jistý důkaz o tom, že elektronický dokument nebo zpráva nejpozději v daný okamžik existovala.

3.8.5 Digitální podpis

Digitální podpis je vytvořen pomocí asymetrické šifry. Jelikož by šifrování celé zprávy bylo výpočetně náročné, je z dat nejprve sejmut otisk (*hash*), který má přesně danou velikost. Tento otisk se poté zašifruje pomocí soukromého klíče odesilatele a přiloží ke zprávě jako digitální podpis. Příjemce si nejdříve z dat přijaté zprávy vytvoří obdobným způsobem svůj nový otisk. Poté pomocí veřejného klíče odesilatele dešifruje digitální podpis obdržený ve zprávě, ze kterého získá otisk původní. Pokud jsou oba otisky stejné, nebyla data ve zprávě během přenosu nijak pozměněna.

Obrázek 5 - Digitální podpis a jeho ověření



Zdroj: zpracováno dle
http://cs.wikipedia.org/wiki/Soubor:Digital_Signature_diagram_cs.svg

3.8.6 Certifikát

Certifikát je vydaný a digitálně podepsaný veřejný klíč uživatele akreditovaným poskytovatelem certifikačních služeb, tedy certifikační autoritu. Certifikát je zpravidla vydávaný na dobu jednoho roku, a to především z důvodu snížení možnosti jeho zneužití, ztráty privátního klíče nebo oslabení použitého algoritmu certifikátu.

3.9 Zákon č. 227/2000 Sb.

Zákon č. 227/2000 Sb., o elektronickém podpisu byl ve Sbírce zákonů zveřejněn dne 29. června 2000 a nabyl účinnosti prvním dnem třetího kalendářního měsíce po dni jeho zveřejnění.

Vychází ze Směrnice Evropského unie 1999/93/EC o zásadách Společenství pro elektronické podpisy ze dne 13. prosince 1999.

Zákon byl již několikrát novelizován. Novela č. 440/2004 Sb., která je účinná od 26. července 2004 zavádí dva nové pojmy, a to kvalifikované časové razítko a elektronická značka. K této novelizaci zákona uvedlo Ministerstvo vnitra České republiky na svých internetových stránkách následující komentář:

"*Dne 26. července 2004 nabyla účinnosti novela zákona o elektronickém podpisu (č. 440/2004 Sb.). Tento předpis nově zavádí pojem „kvalifikované časové razítko", které prokazuje existenci elektronického dokumentu v čase. Další novinkou je možnost používat „elektronické značky". Pro ty se stejně jako pro zaručený elektronický podpis používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy.*"[11]

Dle prvního paragrafu zákona o elektronickém podpisu "Účel zákona" lze lehce odvodit význam vytvoření tohoto zákona:

"*Tento zákon upravuje v souladu s právem Evropských společenství*[12] *používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu*

[11] Zpracováno dle *http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx*

[12] Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem." [13]

Dále v § 4 "Soulad s originálem" je uvedeno: "*Použití zaručeného elektronického podpisu nebo elektronické značky zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit.*"[14]

[13] *Systém ASPI* [počítačový program]. Verze 13+ pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s., 2011. Systém pro práci s právními informacemi.

[14] *Systém ASPI* [počítačový program]. Verze 13+ pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s., 2011. Systém pro práci s právními informacemi.

4. ANALYTICKÁ ČÁST

V analytické části navrhuji vhodné kryptografické zabezpečení e-mailové pošty pro implementaci v advokátní kanceláři. Ze získaných informací a požadavků na zabezpečení zvolím aplikace, které ke svému fungování využívají kryptografických metod. Následně detailněji analyzuji dvě mnou zvolené aplikace. V závěru kapitoly vyhodnotím vhodnost a funkčnost mnou navrženého zabezpečení.

4.1 Požadavky na zabezpečení

V advokátní kanceláři, kterou jsem si vybrala pro tuto práci, je e-mailová komunikace velmi využívaným komunikačním prostředkem. Je důležité poznamenat, že informace zasílané prostřednictvím elektronické pošty jsou velmi důvěrného rázu a v mnoha případě by jejich vyzrazení mohlo mít nedozírné následky, a to zejména pro klienty advokátní kanceláře a budoucnost jejich společností. Vzhledem k důležitosti zachování důvěrnosti dat, je hlavním požadavkem zabezpečit data proti kompromitaci. Dalším požadavkem je bezpečná a zákonem uznávaná komunikace s úřady a státními organizacemi, jako jsou například Finanční úřad, Česká správa sociálního zabezpečení, zdravotní pojišťovny nebo elektronická komunikace s Obchodním rejstříkem. Dalším požadavkem je komunikace s obchodními partnery a klienty, kteří zprávy nepožadují šifrovat, nicméně by rádi ověřili, zda při přenosu zprávy nedošlo k neoprávněné změně jejího obsahu včetně zajištění identifikace autora.

Navržená zabezpečení musí být kompatibilní a funkční s operačním systémem Microsoft Windows XP 2002 a použitelná v aplikaci pro správu e-mailů Microsoft Office Outlook 2003. Navržené zabezpečení musí být možné ovládat pomocí českého a anglického jazyka.

Vzhledem k výše uvedeným požadavkům navrhuji použití elektronického podepisování, časového razítka a zabezpečeného protokolu TLS.

V analytické části provedu detailní analýzu obou zmíněných kryptografických zabezpečení, v závěru shrnu výsledky a uvedu doporučení k implementaci navrženého zabezpečení.

4.2 Elektronické podepisování

4.2.1 Certifikační autorita

„*Certifikační autorita (CA) je nezávislá třetí strana, která vydává certifikáty. Slovní spojení „certifikační autorita“ lze ale chápat dvojím způsobem: buď jako aplikaci (vydávající certifikáty) nebo jako instituci (zajišťující proces vydávání certifikátů). Jako instituce může být realizována jako samostatná firma nebo jako samostatný útvar v rámci firmy.*“[15]

Během sběru informací o certifikačních autoritách jsem zjistila, že v České republice zajišťují vydávání a správu certifikátů následující akreditované CA: První certifikační autorita, a.s., Česká pošta, s. p. a eIdentity a. s.

První certifikační autorita, a.s., dále jen I.CA, vznikla roku 1996 a v roce 2002 jí byla udělena akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. I.CA nabízí kvalifikované a komerční certifikáty, které slouží k vytváření a ověřování elektronických podpisů a šifrování. Dále lze u I.CA zažádat o kvalifikovaná časová razítka, I.CA Secom, ale je také možné využít placených konzultačních služeb a školení.

Certifikační autoritě České pošty, s. p. Postsignum byla udělena akreditace v červenci roku 2005. Postsignum poskytuje vydávání kvalifikovaných a komerčních certifikátů a kvalifikovaného časového razítka.

eIdentity a. s. je akreditovaným poskytovatelem certifikačních služeb od září roku 2005. eIdentity poskytuje kvalifikované a komerční certifikáty a také, jako dvě výše uvedené certifkační autority, nabízí kvalifikovaná časová razítka.

Vydávání a správa certifikátů je upravena zákonem č. 227/2000 Sb., o elektronickém podpisu.

4.2.2 Registrační autorita

RA je součást certifikační autority a je to místo, kde dochází k ověření identity žadatele o certifikát. RA také generuje požadavky na vytvoření certifikátu, které následně

---

[15] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, s. 76

certifikační autoritě zasílá. Některé certifikační autority nabízejí mobilní registrační místo, tedy kontrolu a vytvoření certifikátu přímo u žadatele o certifikát.

4.2.3 Elektronický podpis

Elektronický podpis je termín vytvořený tvůrci zákona pro jeho použití v legislativě. Jedná se o digitální podpis, tedy identifikační údaj připojený k zasílanému dokumentu, který dokáže zaručit, že dokument vytvořila určitá osoba nebo systém.

4.2.4 Kvalifikovaný certifikát a elektronický podpis

Kvalifikovaným podpisem je většinou označován zaručený elektronický podpis, který pomocí kryptografických metod zajišťuje jak integritu, tak autentizaci podepsané osoby. Zaručený elektronický podpis se využívá pro komunikaci se státními organizacemi a úřady, jeho použití je ošetřeno Zákonem č. 227/2000 Sb., o elektronickém podpisu.

4.2.5 Komerční certifikát a elektronický podpis

Komerční certifikát se používá k elektronickému podepisování a to zejména pro e-mailovou komunikaci s obchodními partnery nebo podepisování různých elektronických souborů. Je také vhodný pro šifrování a autentizaci. Tento druh elektronického podpisu ovšem není akceptovatelný státními organizacemi a úřady.

4.2.6 Generování žádosti

Jak jsem zjistila, žádost o certifikát lze podat přes on-line formulář prostřednictvím internetových stránek certifikační autority nebo pro maximální bezpečnost s využitím off-line formuláře.

Aby byla online žádost úspěšně generována, musí být na počítači uživatele nainstalovaný operační systém Microsoft Windows 7, Vista nebo XP a použít internetový prohlížeč Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari nebo Opera. Pro správné fungování webových stránek je vhodná a doporučená instalace softwaru Java Runtime Enviroment (minimální požadovaná verze 1.6.0_21). V prohlížeči musí být zapnuta podpora jazyka Java, skriptování Javascript a ukládání cookies. Tyto systémové požadavky platí pro generování on-line žádosti u certfikačních autorit I.CA a Postsignum.

Proběhne-li generace žádosti v pořádku, zobrazí se žádost ve formátu PKC#10 a v tuto chvíli je možné uložení žádosti na disk.

4.2.7 Dokumenty potřebné k získání certifikátu

Pro vystavení certifikátu musí žadatel navštívit některou z registračních autorit, jejíchž seznam je přístupný na internetových stránkách certifikační autority. Na schůzku je nutné přinést vygenerovanou žádost na přenositelném paměťovém médiu a požadované následující dokumenty.

Žádá-li o certifikát nepodnikající fyzická osoba, musí se prokázat platným občanským průkazem a jedním dalším dokladem totožnosti. Podnikatel navíc musí doložit dokument o existenci společnosti. Pokud o certifikát žádá zaměstnanec, předloží kromě dvou průkazů totožnosti také dokument o existenci společnosti a potvrzení o pracovním poměru od zaměstnavatele.

Na základě plné moci je možné žadatele o certifikát zastoupit zmocněncem, který kromě plné moci překládá také dva průkazy totožnosti.

Registrační autorita na místě provede kontrolu údajů vyplněných v žádosti s údaji v dokumentech požadovaných pro získání certifikátu, bude sepsána smluvní dokumentace související s vydáním certifikátu, předán příslušný certifikát, obdržena čipová karta a její bezpečnostní prvky, tedy PIN a PUK.

4.2.8 Návrh zabezpečení

Vzhledem k požadavkům advokátní kanceláře navrhuji použití kvalifikovaného a komerčního certifikátu, pro uložení kryptografických aktiv je vhodná čipová karta a USB token.

4.2.9 Čipová karta

Navrhuji použití čipové karty Starcos 3.0 od výrobce Giesecke&Devrient. V České republice se tato čipová karta se stala v roce 2010 první certifikovanou čipovou kartu pro vytváření elektronického podpisu a její použití je v souladu se Zákonem č. 227/2000 Sb. o elektronickém podpisu. Data jsou na této čipové kartě chráněna pomocí PIN a PUK čísla.

4.2.10 USB Token

USB Token je mobilní zařízení sloužící jako úložiště dat, které se přes USB port může lehce propojit s jakýmkoliv počítačem, který USB portem disponuje. USB token je vzhledem ke své velikosti snadno přenositelný a tudíž k dispozici kdekoliv na cestách. Společně s čipovými kartami, které se do něj vkládají, tvoří jedno zařízení, které dokáže zaručit bezpečný tok informací.

Navrhuji použití USB Tokenu SCR3320, který je po instalaci vhodného ovladače plně kompatibilní s operačním systémem Microsoft Windows, tedy plní zadané podmínky na zabezpečení.

4.2.11 Aplikace pro správu certifikátů a párů klíčů

Aplikace pro správu certifikátů a párů klíčů se využívají především pro generování párů klíčů na čipové kartě a s tím spojené vytváření žádosti o certifikát, importování vydaného certifikátu, ostatních certifikátů podporovaných certifikační autoritou a certifikátů obchodních partnerů. Přes aplikaci je možné nastavení nového PIN nebo čipovou kartu odblokovat pomocí PUK kódu.

Dále jsou aplikace schopny spravovat volný prostor na čipové kartě, eventuelně je možné jejich prostřednictvím na kartu ukládat volně přístupné nezabezpečené dokumenty, nebo dokumenty, pro jejichž otevření je nutné zadání PIN kódu.

Příhodnou aplikací pro správu certifikátů a párů klíčů, která splňuje systémové požadavky, je aplikace Secure Store I.CA. Je plně kompatibilní s operačním systémem Microsoft Windows a navíc díky komponentě SecureStore CSP je spustitelná pod e-mailovou aplikací Microsoft Office Outlook. Vhledem k tomu, že aplikace Secure Store podporuje českou i anglickou jazykovou verzi, tak splňuje taktéž zadané jazykové požadavky.

4.2.12 Záloha certifikátu a soukromého klíče

Zálohu certifikátu a soukromého klíče do počítače nemusíme provádět. V mém projektu je navrženo použití čipové karty Starcos 3.0 a USB tokenu SCR3320, na nichž je certifikát a soukromý klíč již zazálohován.

4.2.13 Aplikace pro tvorbu elektronického podpisu

Elektronicky podepisovat a šifrovat pomocí certifikátů lze velmi snadno v aplikaci Microsoft Office Outlook. Po vybrání a nastavení certifikátu v nastavení zabezpečení snadno podepíšeme novou e-mailovou zprávu kliknutím na ikonku obálky s pečetí.

4.3 Časové razítko

Digitální podpis spojuje dokument s autorem, časové razítko spojuje dokument s časem. Časové razítko a jeho funkce je velmi dobrým doplňkem v komunikaci s úřady, ale také při vedení účetnictví nebo pro obchodní komunikaci využívající elektronické podepisování. Časové razítko slouží jako důkaz o tom, kdy byl daný dokument podepsán.

V České republice zajišťuje vydávání časových razítek První certifikační autorita, a.s., eIdentity a. s. nebo Postsignum.

4.3.1 Autorita pro vydávání časových razítek TSA

Časové razítko je datovou strukturou, „*která mj. obsahuje čas, otisk z dokumentu, jméno vydavatele razítka a pořadové číslo. To vše je stvrzeno nezávislou třetí stranou – Autoritou pro vydávání časových razítek (Time Stamping Authority). Časové razítko tak slouží jako důkaz, že dokument (přesněji řečeno otisk z dokumentu) existoval v daném čase. Dokument je v časovém razítku reprezentován pomocí tzv. message imprint, což je dvojice: otisk z dokumentu a algoritmus pro výpočet otisku, kterým byl otisk z dokumentu spočten.*“ [16] Přes všechna pozitiva má časové razítko jednu nevýhodu. Spojuje sice dokument s časem jeho existence, nedokáže však určit konkrétní osobu, která měla dokument daný čas v držení.

Razítkovat můžeme dokumenty, auditní záznamy, nebo je také možné vytvořit časové razítko z digitálního podpisu.

Časové razítko vytvořené z digitálního podpisu je vhodné použít například u dokumentů či smluv, jejichž platnost a účinnost je dlouhodobá. Jelikož se elektronický podpis ověřuje příslušným certifikátem, který je standardně platný jeden rok, není možné elektronický podpis po uplynutí platnosti daného certifikátu ověřit. Později by mohlo dojít

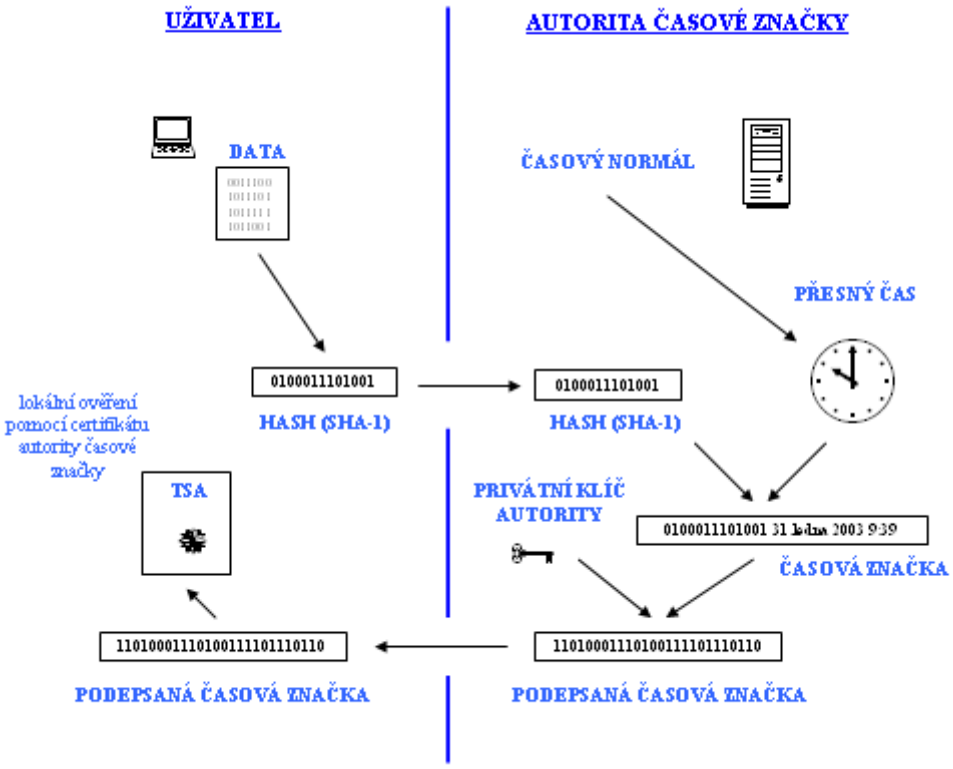
---

[16] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, s. 345

ke zpochybnění platnosti takto elektronicky podepsaného dokumentu. Možným řešením je časové orazítkování elektronického podpisu patřícímu osobě, která dokument podepsala, a to v době, kdy se tak stalo. Tím lze získat důkaz o tom, že byl daný dokument nebo smlouva podepsán v době platnosti certifikátu podepisující osoby a že byl skutečně podepisující osobou podepsán.

Na druhou stranu je časové razítko platné pouze tak dlouho, jak dlouho je platný certifikát TSA, která datovou strukturu, respektive časové razítko, elektronicky podepsala.

Obrázek 6 - Časové razítko



Zdroj: zpracováno dle *http://www.svetsiti.cz/clanek.asp?cid=2540*

4.3.2 Určení a věrohodnost času

Autorita pro vydávání časových razítek by měla být schopna garantovat časové údaje, které udává ve svých časových razítkách.

Například I. CA. na svých internetových stránkách uvádí, že její časová razítka obsahují časový údaj s odchylkou maximálně 1 sekunda od UTC (+/- 500 ms).

4.3.3 Protokol TSP

TSP je protokol pro vydávání časových razítek a sestává se z žádosti o časové razítko a odpovědi na tuto žádost. Odpovědí je buď nahlášení chyby, nebo přímo vydané časové razítko. TSA nezkoumá identitu a pokud je žádost formálně správná, vydá časové razítko vždy. Je dobré vědět, že se TSA nikdy nemůže dostat k citlivým údajům, jelikož se v žádosti posílá pouze otisk dokumentu, textu nebo digitálního podpisu, který je potřeba orazítkovat. TSA po obdržení žádosti vytvoří dopověď, ve které je opět otisk ze zaslané žádosti navíc doplněný o časový údaj a elektronický podpis TSA, tedy časové razítko.

4.3.4 Transportní protokoly

Žádost je zasílána prostřednictvím protokolů TCP, případně protokolu UDP. Pro tuto komunikaci je pro TSA vyhrazen port 318/tcp a 318/udp.

Další možností je komunikovat prostřednictví HTTP nebo elektronické pošty.

4.3.5 Ověření časového razítka

Ověřit časové razítko můžeme pomocí certifikátu a digitálního podpisu náležícímu TSA, který časové razítko vydala.

4.3.6 Platnost časového razítka

Platnost časového razítka se odvíjí od platnosti certifikátu, pomocí níž TSA časové razítko vytvořila a elektronicky podepsala.

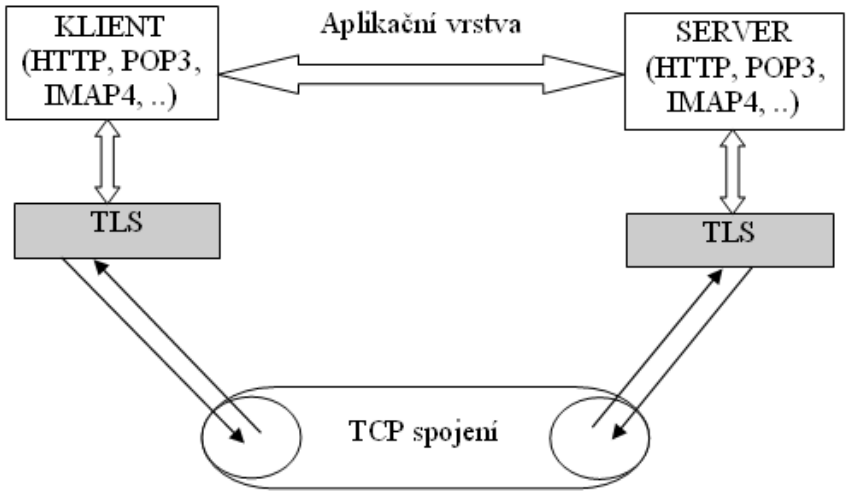
4.4 Protokol TLS

Pro případy, kdy nemusí, nebo nemůže, být použito elektronické podepisování nebo časové razítko, je možné použít šifrovaný komunikační kanál pro komunikaci s e-mailovým serverem. Konkrétně protokol TLS, který šifruje přenášená data, zajišťuje jejich integritu a na základě certifikátů umožňuje navíc ověřit identitu klienta i serveru. TLS protokol tedy zaručuje bezpečný tok dat sítí.

4.4.1 Jak TLS funguje?

Data pro přenos Internetem jsou předávána aplikačními protokoly protokolu TCP. "*Protokol TCP je navržen jako duplexní komunikační protokol, tj. protokol tvořící dva samostatné kanály. Jeden pro přenos dat z klienta na server a druhý pro přenos ze serveru na klienta.*"[17] Protokol TLS je vrstva vložená mezi aplikační a TCP protokoly, jak je vidět na obrázku č. 7.

Obrázek 7 - Protokol TLS



Zdroj: zpracováno dle *DOSTÁLEK, L. a kol., Velký průvodce infrastrukturou PKI a technologií elektronického podpisu,* s. 381

Protokol TLS tvoří HP a RLP protokoly. Přes protokol HP „*se obě strany dohodnou na protokolové svitě (kryptografických algoritmech) i kryptografickém materiálu (kryptografické klíče a sdílená tajemství). Protokol HP se aktivuje bezprostředně po navázání TCP spojení a podle potřeby i během spojení. Protokol HP všechny kryptografické informace připraví nikoliv jako aktuální kryptografické parametry, ale jen jako připravované kryptografické parametry.*"[18]

---

[17] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, s. 381

[18] DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M., *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, s. 383

HP protokol je složen z dvou dalších protokolů CCSP a AP. Protokol CCSP připravené kryptografické parametry zkopíruje na aktuální kryptografické parametry, podle nichž se aktuálně šifruje. Nakonec je tu protokol AP, přes který si mohou strany vzájemně oznamovat případné závady a chyby.

Podle výše uvedených informací je zřejmé, že HP protokol připraví RLP aktuální kryptografické algoritmy, které budou použity, a ostatní parametry zpracování. Protokol RLP následně zařizuje komunikaci s aplikačními protokoly, přijatá data šifruje, respektive dešifruje, a dále počítá z nich, respektive ověřuje, kontrolní kryptografický součet.

4.4.2 TLS Protokol a elektronická pošta

Během přenosu pomocí zabezpečeného TLS protokolu putují sítí nezašifrovaná data, která jsou šifrována odesílající stranou a dešifrována přijímající stranou tolikrát, přes kolik poštovních serverů projdou. Stoprocentně jisti, že zpráva nebyla nijak odposlechnuta, si můžeme být pouze v případě, kdy shledáme důvěryhodnými všechny poštovní servery, přes které zpráva prochází.

4.4.3 Spojení protokolu SMTP přes TLS

Pokud server podporuje rozšíření pro komunikaci přes TLS protokol, vypíše po zahájení spojení a vzájemném uvedení DNS jmen klientovi seznam rozšíření, obsahující mimo jiné také STARTTLS. Klient odpoví STARTTLS, a je-li server připraven, vrátí odpověď *220 Go ahead*, čímž zahájí bezpečnou komunikaci.

Ráda bych zdůraznila, že by klient měl mít před zahájením spojení nainstalován certifikát SMTP serveru. Když totiž během komunikace dojde ke zbrklému akceptování nějakého serverového certifikátu, může dojít ke komunikaci s podvodným serverem, jehož jediný cíl je získání našich tajných informací.

4.4.4 Spojení protokolu POP3 přes TLS

Obdobně je možné zabezpečit spojení protokolu POP3 pomocí TLS protokolu. Zabezpečená komunikace se zahajuje příkazem STLS ze strany klienta a odpovědí *+OK Begin TLS negotiation* na straně serveru.

Ze stejného důvodu, jako jsem uvedla výše, je vhodné před zahájením spojení instalovat certifikát POP3 serveru.

4.4.5 Implementace protokolu TLS

Abychom mohli začít používat zabezpečený přenos e-mailové korespondence přes TLS protokol, musíme přidat podporu pro TLS v MTA programu a provést několik přípravných kroků. MTA programy jsou například Microsoft Exchange Server, Sendmail a Postfix.

4.4.6 Příprava programů

Před zahájením přenosu dat přes TLS protokol, musíme na přenos nejprve připravit používané MTA programy, respektive servery. Někdy je potřeba instalace dodatečného balíčku, případně u programů využívajících POP3, IMAP nebo SMTP serveru stačí instalace chybějící komponenty.

4.4.7 Příprava Certifikátu

Jsou dvě možnosti získání certifikátu. První možností je vytvoření a samopodepsání certifikátu přes openssl nástroj, druhou možností je mít certifikát podepsaný důvěryhodnou autoritou. V druhém případě je nutné vygenerovat požadavek, certifikát zaplatit a nechat podepsat u certifikační autority. Získány certifikát a příslušný soukromý klíč se poté nainstaluje tak, aby k němu měly přístup všechny programy, které by ho pro svou funkčnost požadovaly. Místo, kde je soukromý klíč uložen, se poté nastavuje při konfiguraci programů.

4.4.8 Konfigurace

Nyní dochází k nastavení chování systému, navázání cest k místu uložení certifikátu a soukromého klíče a samotné spuštění TLS protokolu. Pod chováním systému si lze představit nastavení síly šifrových algoritmů, nebo použití funkce ověřování klientů.

4.4.9 Uložení zpráv

Přenos zpráv sice probíhá zabezpečeně, ale problém nastává po uložení zprávy. Zprávy se většinou ukládají v nešifrované podobě, jsou tedy lehce napadnutelné.

5. VÝSLEDKY A DISKUSE

Během studie problematiky jsem zjistila, že dle Zákona č. 227/2000 Sb., o elektronickém podpisu se pro komunikaci s úřady, státní správou a samosprávou musí používat zaručený elektronický podpis. Pokud je tedy jedním z požadavků právě komunikace s úřady, mohu použití kvalifikovaného certifikátu jako první zabezpečovací prvek navrhnout.

Ovšem dle mého názoru je nevýhodou zaručeného elektronického podepisování to, že elektronické podepisování pouze ověřuje, že data nebyla nijak změněna, ale samotný text zprávy putuje po síti jako čistý text. Tedy text přístupný komukoliv. Protože zaručený elektronický podpis samotný text zprávy nešifruje, rozhodla jsem se použít kromě zaručeného elektronického podpisu, a jeho ověření podle příslušného kvalifikovaného certifikátu i certifikát komerční, který plní úlohu při šifrování, autentizaci a navíc je vhodný pro běžnou obchodní komunikaci.

Jak z analytické části vyplývá, je možné o certifikát zažádat on-line, nebo lze použít bezpečnější způsob a žádost vytvořit pomocí off-line formuláře.

Podle mého názoru je časové razítko a jeho funkce dobrým doplňkem v komunikaci s úřady, ale také při vedení účetnictví nebo pro obchodní komunikaci využívající elektronické podepisování. Dále se může časové razítko použít jako důkaz o tom, kdy byl daný dokument podepsán, což má nesporně velká pozitiva. Nevýhodou je to, že časové razítko nedokáže určit konkrétní osobu, která měla dokument v daný čas v držení. Nicméně je možné tento nedostatek vyřešit vytvořením časového razítka z digitálního podpisu, které potvrzuje, že konkrétní osoba skutečně v tu dobu dokument podepsala. Z těchto důvodů proto také navrhuji zahrnutí a použití časového razítka jako další prvek v kombinaci zabezpečení.

Kromě elektronického podepisování a použití časového razítka lze zabezpečit e-mailovou komunikaci pomocí protokolu TLS. Výhodou TLS je, že ho lze využít s jakýmkoli aplikačním protokolem a poskytuje šifrování přenášených dat.

V neposlední řade je nutné myslet také na prevenci a nakládat z důvěrnými informacemi opatrně. Důležité je nezapomenout na to, jak se zašifrovanými, případně jinak zabezpečenými daty, manipulovat, a jak kryptografický materiál uchovávat.

Kryptografické zabezpečení, které jsem v této práci navrhla, není jistě jedním z nejdokonalejších, ale jsem přesvědčena, že v závislosti na zadané požadavky je vyhovující. Aby se elektronická pošta včetně přenosu e-mailových zpráv stala mnohem bezpečnější, je samozřejmě možné výše popsané zabezpečení rozšířit o další bezpečnostní prvky, programy, aplikace, a další bezpečnostní mechanismy. Například použit virtuální sítě, nebo nezávislé šifrovací programy, jako jsou PGP nebo GNU Privacy Guard.

V současnosti dochází k bouřlivému rozvoji kvantové kryptografie, která staví na základech kvantové mechaniky. Jistě velmi brzy může dojít k tomu, že se mnou navržená kombinace zabezpečení stane poněkud zastaralou a nedostačující. Ovšem na druhou stranu, z informací mě známých, není zatím použití kvantové kryptografie upraveno zákonem, a dokud se tak nestane, nebude bude možné použití kvantové kryptografie jako státem uznávanou metodu kryptografického zabezpečení. Kromě toho brání praktickému využití kvantové kryptografie také vysoké finanční náklady.

6. ZÁVĚR

Hlavním cílem této bakalářské práce bylo navrhnout zabezpečení e-mailové pošty pro implementaci v advokátní kanceláři. K takto stanovenému cíli jsem přistoupila dvěma způsoby. Zaprvé studií a analýzou aktuálně dostupných obecných ochran a kryptografických mechanismů. Za druhé jsem dle požadavků na zabezpečení další analýzou a na základě dosažených znalostí navrhnula kombinaci kryptografického zabezpečení, jako je elektronický podpis, využití časového razítka a zabezpečení toku dat po Internetu pomocí protokolu TLS.

Jsem přesvědčena, že mnou navrhované zabezpečení splňuje požadavky na kryptografickou ochranu, která byla požadována. Implementace kryptografického zabezpečení je reálná a splňuje veškeré systémové požadavky. Chápu a připouštím, že zabezpečení může být dále rozšířeno. Je možné využít například virtuální privátní sítě nebo šifrování zpráv pomocí nezávislých šifrovacích programů PGP nebo GNU Privacy Guard.

Mám-li hodnotit přínos této práce, stala se zdrojem informací a nových poznatků nejen pro mě, ale věřím, že i pro její laskavé čtenáře, laiky v této problematice. Současně vzhledem k procentu uživatelů operačního systému Microsoft Windows v České republice může sloužit i jako nastínění možných a dostupných řešení pro zabezpečení soukromých a citlivých informací.

7. SEZNAM POUŽITÝCH ZDROJŮ

7.1 Soupis citací

SINGH, Simon. *Kniha kódů a šifer*. 1. vydání. Praha: Dokořán, s.r.o. ve spolupráci s nakladatelstvím Argo, 2003. 384 s. ISBN 80-86569-18-7 (Dokořán, s.r.o.), ISBN 80-7203-499-5 (Agro).

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vydání. Praha: Albatros nakladatelství, a.s., 2006. 400 s. ISBN: 80-00-01888-8.

DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta, KNOTEK, Miroslav. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2. aktualizované vydání. Brno: Computer Press, a.s., 2009. 542 s. ISBN 978-80-251-2619-6.

PIPER, Fred, MURPHY, Sean. *Kryptografie: průvodce pro každého*. 1. vydání Praha: Dokořán, 2006. 157 s. ISBN 80-7363-074-5.

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. 1. vydání. Brno: Computer Press, a.s., 2004. 190 s. ISBN: 80-251-0106-1.

7.2 Použitá literatura

PIPER, Fred, MURPHY, Sean. *Kryptografie: průvodce pro každého*. 1. vydání Praha: Dokořán, 2006. 157 s. ISBN 80-7363-074-5.

DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta, KNOTEK, Mirosav. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2. aktualizované vydání. Brno: Computer Press, a.s., 2009. 542 s. ISBN 978-80-251-2619-6.

SINGH, Simon. *Kniha kódů a šifer.* 1. vydání. Praha: Dokořán, s.r.o. ve spolupráci s nakladatelstvím Argo, 2003. 384 s. ISBN 80-86569-18-7 (Dokořán, s.r.o.), ISBN 80-7203-499-5 (Agro).

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vydání. Praha: Albatros nakladatelství, a.s., 2006. 400 s. ISBN: 80-00-01888-8.

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. 1. vydání. Brno: Computer Press, a.s., 2004. 190 s. ISBN: 80-251-0106-1.

BITTO, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotyky*. 1. vydání. Kralice: Computer Media, 2005. 168 s. ISBN 80-86686-48-5.

NEGROPONTE, Nicholas. *Digitální svět*. 1. vydání. Praha: Management Press, 2001. 207 s. ISBN 80-7261-046-5.

Bletchleypark.org.uk/edu/archives/cryptcoll.rhtm [online]. c2005 [cit. 2011-08-10]. Archival COLLECTIONS. Dostupné z WWW: <http://www.bletchleypark.org.uk/edu/archives/cryptcoll.rhtm>.

Nsa.gov/about/cryptologic_heritage/museum/ [online]. 15.1.2009 [cit. 2011-07-10]. National Cryptologic Museum. Dostupné z WWW: <http://www.nsa.gov/about/cryptologic_heritage/museum/ >.

Spymuseum.org/ [online]. c2011 [cit. 2011-08-12]. Spy Museum. Dostupné z WWW: <http://www.spymuseum.org/>.

Earchiv.cz/i_serial.php3 [online]. c2011 [cit. 2011-07-18]. Jiří Peterka: Seriály. Dostupné z WWW: <http://www.earchiv.cz/i_serial.php3>.

Antivirovecentrum.cz/ [online]. c1998 - 2011 [cit. 2011-07-25]. ESET NOD32, AVG, Avast a další. *Dostupné* z WWW: <http://www.antivirovecentrum.cz/>.

Cs.wikipedia.org/wiki/Soubor:Digital_Signature_diagram_cs.svg [online]. 29.6.2009 [cit. 2011-10-20]. Soubor: Digital Signature diagram cs.svg - Wikipedie. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Soubor:Digital_Signature_diagram_cs.svg>.

Mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx [online]. c2010 [cit. 2011-09-10]. Zákon č. 227/2000 Sb., o elektronickém podpisu - Ministerstvo vnitra České republiky. Dostupné z WWW: <http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

Ica.cz/Aplikace-stazeni.aspx [online]. c2011 [cit. 2011-09-08]. I.CA a.s. | Aplikace ke stažení. Dostupné z WWW: <http://www.ica.cz/Aplikace-stazeni.aspx>.

Ica.cz/Default.aspx [online] [cit. 2011-09-08]. c2011. I.CA a.s. | Home Page. Dostupné z WWW: <http://www.ica.cz/Default.aspx>.

JELÍNEK, Lukáš. *Abclinuxu.cz/clanky/site/stavime-postovni-server-12-tls* [online]. 25. 1. 2010 [cit. 2011-10-10]. Stavíme poštovní server – 12 (TLS). Dostupné z WWW: <http://www.abclinuxu.cz/clanky/site/stavime-postovni-server-12-tls>.

Mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx [online]. c2010 [cit. 2011-11-10]. Přehled udělených akreditací - Ministerstvo vnitra České republiky. Dostupné z WWW: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

Earchiv.cz/b05/b0600001.php3 [online]. c2011 [cit. 2011-11-17]. Jiří Peterka: Báječný svět počítačových sítí, část III. - Rodina protokolů TCP/IP . Dostupné z WWW: <http://www.earchiv.cz/b05/b0600001.php3>.

Svetsiti.cz/clanek.asp?cid=2540 [online]. 10. června 2003 [cit. 2011-11-17]. Pravdy o elektronickém podpisu a šifrování (9) - když podpis, tak s časovou značkou. Dostupné z WWW: <http://www.svetsiti.cz/clanek.asp?cid=2540>.

Systém ASPI [počítačový program]. Verze 13+ pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s., 2011. Systém pro práci s právními informacemi.

8. SEZNAM ZKRATEK

AP	Alert Protocol
CCSP	Change Cipher Specification Protocol
DNS	Domain Name System
HP	Handshake Protocol
I. CA	První certifikační autorita, a.s.
IMAP	Internet Message Access Protocol
IP	Internet Protocol
MDA	Mail Delivery Agent
MTA	Message Transfer Agents
MTS	Message Transfer System
MUC	Mail User Client
NSA	National Security Agency
POP3	Post Office Protocol Version 3
RA	Crypto Service Provider
RLP	Record Layer Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSA	Time Stamping Authority
UDP.....	User Datagram Protocol