Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Bakalářská práce

Martin Horyna

2008

Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Použití digitálních certifikátů a razítek

Vypracoval:

Martin Horyna

Vedoucí bakalářské práce:

Ing. Pavel Pokorný

Jindřichův Hradec, duben 2008

VŠE

FAKULTA MANAGEMENTU

Vysoká škola ekonomická v Praze
Jarošovská 1117/II, 377 01 Jindřichův Hradec

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro akademický rok 2006/2007

Název práce:	**Použití digitálních certifikátů a razítek.**
Zadání práce:	Rozbor situace ohledně používání digitálních certifikátů (elektronických podpisů) a elektronických razítek. Dále rozbor právní problematiky, praktické ukázky používání a možnosti využití na FM VŠE.
Jméno studenta:	Ing. Martin Horyna
Ročník:	2.
Obor:	MANAGEMENT
Vedoucí práce:	Ing. Pavel Pokorný
Katedra:	Katedra managementu informací
Termín zadání:	23.6.2006
Termín odevzdání:	Dle vyhlášky o průběhu státních závěrečných zkoušek v ak. roce 2006/2007

V Jindřichově Hradci 23.6.2006

Ing. Vladimír Přibyl
proděkan pro pedagogickou činnost

tel.: 384 417 200 fax: 384 417 277 IČ: CZ61384399 bank. spoj. ČSOB a. s. J. Hradec č. ú. 170822147/0300

Prohlášení

Prohlašuji, že bakalářskou práci na téma

„Použití digitálních certifikátů a razítek“

jsem vypracoval samostatně.

Použitou literaturu a podkladové materiály

uvádím v přiloženém seznamu literatury.

Jindřichův Hradec, duben 2007

.....

podpis studenta

Anotace

Tato práce rozebírá situaci kolem digitálního podpisu. Mapuje rozvoj jak po stránce praktické, tak po stránce právní. V závěru hodnotí zdary, nezdary a nastiňuje směry, kterými by se mohl vývoj ubírat.

duben 2008

Poděkování

Za cenné rady, náměty a inspiraci

bych chtěl poděkovat vedoucímu práce

Ing. Pavlu Pokornému

Úvod

Tato práce se zabývá problematikou využívání digitálních certifikátů a elektronických razítek.

První kapitola shrnuje základní technické poznatky, které jsou následně využity v dalších kapitolách.

Druhá kapitola se zabývá významem certifikátu v praxi. Shrnuje informace o certifikačních autoritách, jejich produktech a možnostech získání certifikátů. Dále přináší souhrn nejdůležitějších aplikací využívající digitálních certifikátů a elektronických razítek u orgánů veřejné správy a v komerčním sektoru.

Třetí kapitola se snaží podchytit právní problematiku, zmapovat jednotlivé důležité zákony významné pro elektronický podpis.

Čtvrtá kapitola sumarizuje využití na škole a přichází s několika návrhy, kudy by se mohla budoucnost ubírat.

Na závěr se zamýšlím nad pokrokem, který se udál v této oblasti za poslední roky. Analyzuji problémy, které nás provázely při uvádění této technologie do praxe. Současně se pokouším o předpověď vývoje a jeho možné směry.

1 Základní informace

Je určitě bez pochyb, že naše společnost prochází bouřlivým rozvojem informačních a komunikačních technologii. Asi si těžko mohl někdo představit před pár desítkami let takový vývoj, kdy se teprve začínaly rodit první počítače a byly doménou pouze armády nebo vědeckých ústavů. Dnes elektronická komunikace prostupuje prakticky všemi součástmi našeho života. Současný život si mnozí z nás už ani nedovedou představit bez mobilního telefonu, internetu nebo mobilní zábavy. V neposlední řadě začíná zasahovat významně do oblasti zprávy dokumentů. Po fázi digitalizace všeho papírového, co firmy, úřady a jiné subjekty měly, přichází etapa, kdy elektronická komunikace začíná plně vytlačovat papír. Myslím, že můžeme směle říci, že není daleko doba, kdy další generace nepoznají co je papírový dokument.

Aby toto tvrzení jednou mohlo platit, bude zapotřebí elektronického podpisu a jeho dalšího rozvoje. Proč tomu tak je? Na to najdeme odpověď, pokud se ohlédneme trochu zpět.

Podstatou každého dokumenty, jenž zakládal určitý právní následek, byl podpis. Ten jednoznačně identifikoval osobu, která dokument vytvořila. Samozřejmě rukopisy je možno více, či méně napodobovat, ale pro náš účel se spokojíme konstatování nemožnosti úplné napodobeniny a možnost odhalení pomocí grafologie.

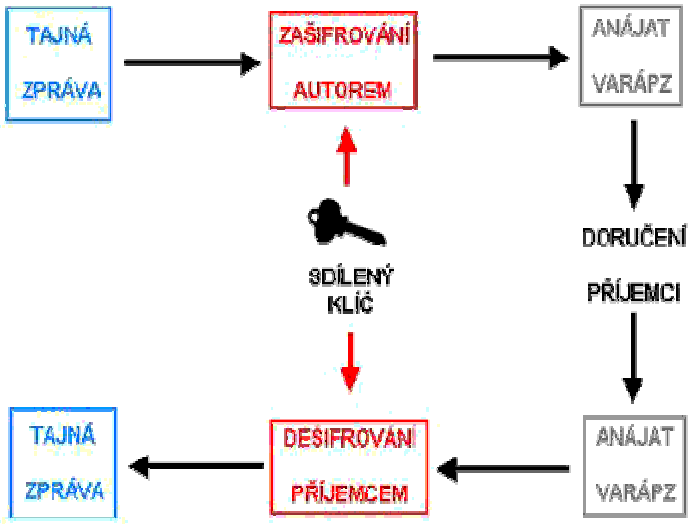
Poněkud jiná situace je u elektronických dokumentů. Jednoznačně identifikovat tvůrce prakticky nelze. Pravděpodobně se asi všichni nesetkali s možnostmi, jak měnit a upravovat již existující dokumenty, ale určitě vědí, že elektronické identitě není radno důvěřovat. Obzvláště pak podvodné emaily a cílené záměny internetových adres apod. Pokud by neexistoval prostředek jako je elektronický podpis, těžko by došla elektronická komunikace současného úspěchu. Klíčovým faktorem pak určitě je pojem šifrování. [12], [1]

1.1 Šifrování

Vědní disciplínu, která se tímto zabývá, nazýváme kryptologie. Již od pradávna se lidé snažili něco utajit – různé formy hlavolamů a přesmyček chránily uložené poklady nebo důvěrné zprávy. Asi největší roli hrála a hraje kryptologie ve vojenství. Kde více může být důležitější, aby vyměňované informace nemohla dekódovat nepřátelská strana. Další podstatný vliv na rozvoj měl rozmach výpočetní techniky, který umožnil hrubou silou rozluštit důmyslné, ale málo zabezpečené šifry.

Vlastní obor kryptologie můžeme dále dělit na kryptografii (kóduje vstupní informace, tak, aby je nebylo možno rozluštit) a kryptoanalýzu (pokouší se najít správný postup, jak šifru prolomit). Základním principem je kódování, tj. přiřazení určité formě jinou formu, kde převodní vztah (klíč) bude kódovat/dekódovat zprávu. Převodní vztah bývá zpravidla nějaká matematická funkce. Dalším úskalím je potom bezpečně předat klíč příjemci zprávy. Vývojem tak vznikly dva různé šifrovací mechanizmy: symetrický a asymetrický.

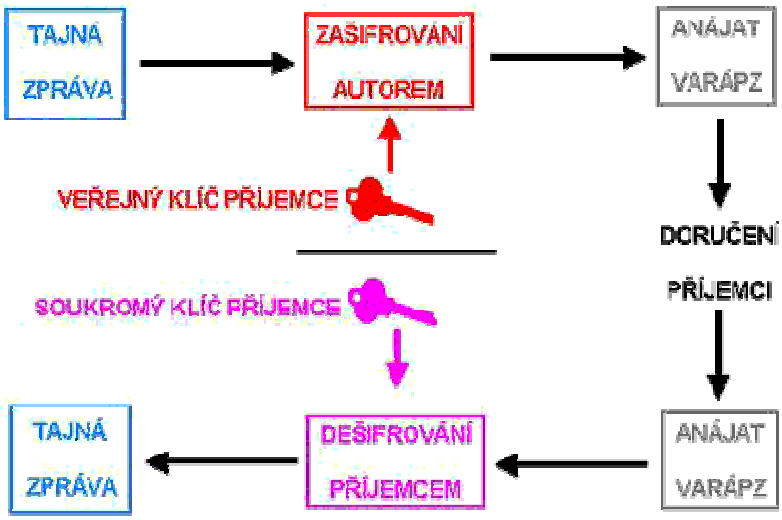
Symetrické kódování - Odesilatel zašifruje zprávu pomocí určitého klíče a příjemce ji pomocí stejného klíče dešifruje. Největší slabinou tohoto řešení je bezpečné předání klíče příjemci. V současné době jsou nejpoužívanější tyto algoritmy DES, 3DES, IDEA a BlowFish, které je možné aplikovat v reálném čase. Nevýhoda algoritmu IDEA je ochrana patentem – nelze volně využívat. S růstem výpočetního výkonu se navýšila délka užívaných klíčů na 128 a více bitů, protože docházelo prolomení šifry „hrubou silou“, tj. spojením výkonu mnoha počítačů. Při dodržení všech bezpečnostních pravidel je u tohoto šifrování zabezpečen obsah přenášené zprávy, ale identifikace původce chybí.



Obrázek 1-1 Symetrické kódování [11]

Asymetrické kódování – Zde je situace poněkud odlišná. Bývají generovány klíče dva – veřejný a soukromý, kde veřejný je dán volně k distribuci a naproti tomu soukromý je maximálně bezpečně ukrýván majitelem (čipové karty, USB tokeny, disketa,…). Vlastností tohoto šifrování je, že jedním klíčem nelze zakódovat a dekódovat zprávu. Zpracování šifry je oproti symetrické podstatně náročnější a pomalejší. V současné době jsou nejpoužívanější RSA a algoritmy na bázi eliptických křivek. RSA vychází z řešení úloh faktorizace velkých čísel. Výhoda metody eliptických křivek je vyšší bezpečnost při kratším klíči a to až 10x.

Pokud bychom nejdříve na zabezpečení zprávy využili symetrického kódování a následně symetrický klíč zakódovali pomocí asymetrického kódování, dostali bychom pak vhodný kompromis o vysokém zabezpečení a relativně rychlý. Tento proces je hojně využíván u PGP. [2], [3], [11]



Obrázek 1-2 Asymetrické šifrování [11]

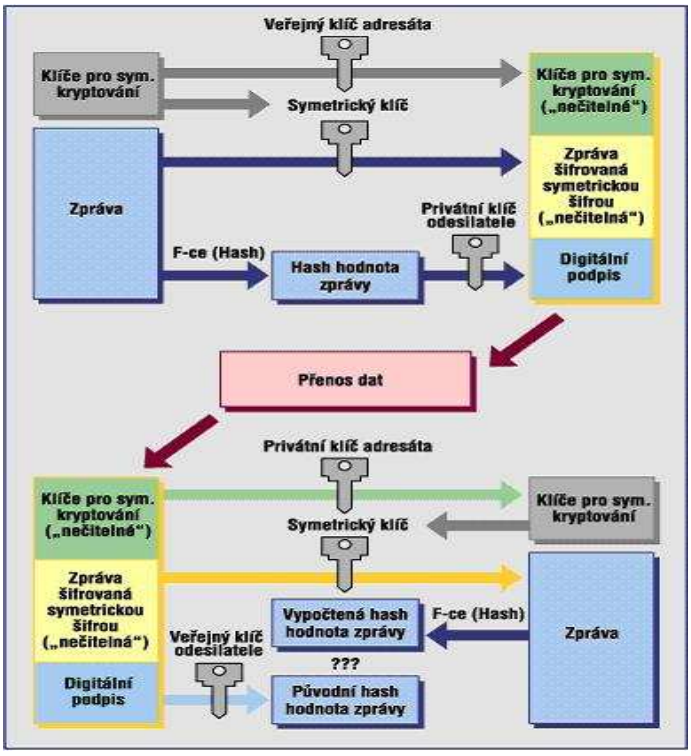
1.2 Praktické realizace

Klíče asymetrického šifrování nemusí sloužit jen k ověřování identit komunikujících subjektů. Slouží také k zabezpečení dokumentu proti následné změně anebo čtení osobou, která není oprávněná. K tomu účelu mohou být použité jen určité vydávané certifikáty. Pokud dokument zašifrujeme veřejným klíčem adresáta, nebude nikdo jiný moci data dešifrovat.

Užití asymetrického šifrování všeobecně na všechny dokumenty není dost dobře možné vzhledem k své výpočetní náročnosti, která by vedla k pomalému zpracování dlouhých dokumentů. Proto se využívá tzv. hashovací funkce, která dokumentu přiřadí jednoznačnou hodnotu pevné délky, která se poté zašifruje soukromým klíčem, vznikne tak digitální podpis odesilatele. Zabezpečení vlastní zprávy proti neautorizovanému čtenáři se provede symetrickým šifrováním (jednodušší a rychlejší). Vlastní symetrický klíč se zašifruje veřejným klíčem adresáta. Extra zabezpečení bychom dosáhli vložením časového razítka náhodně do dokumentu. Takto vytvořenou zprávu zašleme adresátovi.

V prvním kroku dešifrujeme zprávu pomocí soukromého klíče (adresáta), abychom získali symetrický klíč, s pomocí kterého dešifrujeme vlastní zprávu. Dále určíme hash hodnotu zprávy, kterou porovnáme s hodnotou získanou dešifrováním s pomocí veřejného

klíče odesilatele (stáhneme z webu autority, která certifikát vydala). V případě, že hashe nejsou shodné, mohlo dojít pozměnění dat nebo podpisu. [3], [6], [11]



Obrázek 1-3 Zabezpečená komunikace [6]

1.3 Digitální podpis

Digitální podpis patří do široké skupiny elektronických podpisů, kde můžeme například zařadit snímání oční duhovky, a nascanování otisku prstu, dlaně, napsaného podpisu a jiné. V praxi se tyto dva pojmy často zaměňují. Je vytvořen pomocí asymetrického šifrování s dvěma klíči navzájem inverzními a je zaznamenán v digitální podobě.

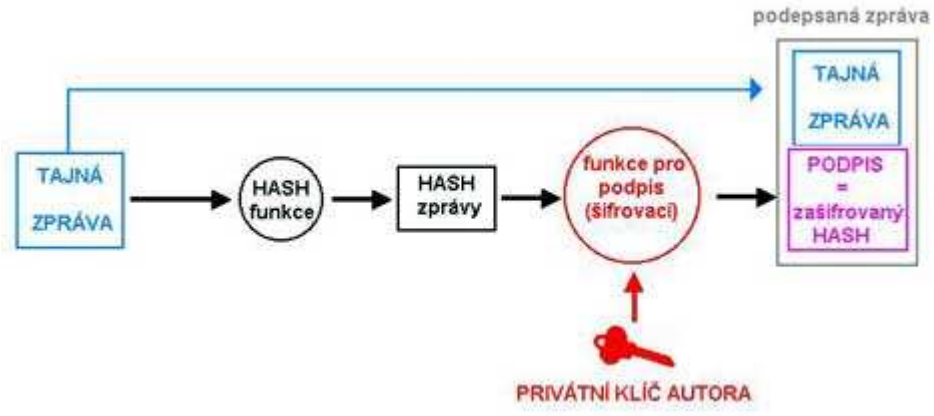
Elektronická komunikace postavená na digitálním podpisu by měla splňovat následující zásady.

- **Zásada důvěrnosti** – zabezpečení proti čtení neoprávněnou osobou dosáhneme zašifrováním zprávy veřejným klíčem adresáta. Zprávu může přečíst jenom majitel soukromého klíče.
- **Zásada integrity** – je zajištěna HASH funkcí, která je aplikována při digitálním podpisu. Ověření přijaté zprávy je založeno na srovnání dekódované HASH hodnoty veřejným klíčem odesilatele a vypočtenou hodnotou. Sebemenší změna by pak znamenala nesoulad těchto dvou hodnot.

- **Zásada neodmítnutelnosti odpovědnosti** – je založeno na jasné identifikaci majitele páru klíčů. Vzhledem k tomu, že klíče lze generovat prakticky neomezeně, musí existovat institut, který by tuto situaci ošetřil. Na scénu zde vstupuje třetí nezávislá strana, která svou autoritou skrze vydaný digitální certifikát stvrzuje pravost a identifikuje subjekt vlastnící klíče. [3], [11], [12]

1.4 Hash

Základem digitálního podpisu je vytvoření HASHe dokumentu. Jakýkoliv dokument je ve své podstatě jenom soubor jedniček a nul. Aplikací hashovací funkce získáme otisk dokumentu. Hashovací funkce je jednosměrná transformace, která z variabilních vstupních veličin vrací textový řetězec pevné délky. Otisk dokumentu je tak zhuštěná hodnota, jinak velmi dlouhého dokumentu, která jednoznačně identifikuje původní soubor. Jakákoliv i drobná změna by znamenala jiný otisk. Inverzí nelze dojít k původnímu dokumentu. Nejpoužívanější jsou algoritmy SHA1, MD2 a MD5. Digitální podpis pak vznikne následným procesem – vytvoříme otisk dokumentu pomocí hashovaní funkce, který následně zašifrujeme privátním klíčem. Zpravidla se zprávou zasílá digitální certifikát. [2], [4], [11]



Obrázek 1-4 Aplikace funkce HASH [11]

1.5 Elektronické značky

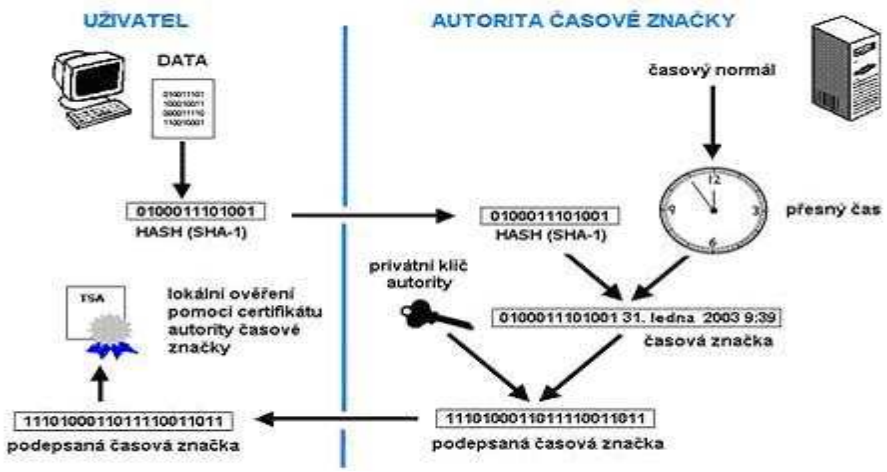
Ve své podstatě se jedná o digitální podpis s rozdílnými právními aspekty. Tak jako klasický podpis vytváří fyzická osoba a obdobou je digitální podpis, stejná analogie platí pro úřední razítko a elektronické značky, které jsou výstupem úřadu nebo stroje resp. informačního systému. K ověřování elektronické značky slouží systémový certifikát. Výhodou elektronické značky je její vazba na právnickou osobu oproti digitálnímu podpisu, který se váže na konkrétní osobu. [13], [14]

1.6 Časové razítko

Pokud se zamyslíme, nad výše uvedenými fakty zjistíme, že proces má jednu významnou slabinu a to určení času. Datum je podstatnou náležitostí většiny dokumentů. Antidatováním bychom tak zdiskreditovali tento důmyslný systém – opožděné podávaní různých daňových přiznání nebo by bylo možné rušit platnost různých dokumentů nahlášením ztráty klíče a následným zneplatněním certifikátu na „black listu“ a v neposlední řadě u dokumentů, které vznikly již dříve, a platnost certifikátu již skončila.

K zamezení takovýchto kroků slouží právě časové razítko, které prokazuje existenci uvedených skutečností krátce před udělením. Razítko vydává autorita časové značky (TSA), jenž funguje na obdobné bázi jako normální autorita. Čas TSA bývá odvozen od velmi přesných celsiových hodin resp. je srovnáván s dalšími alespoň třemi zdroji včetně vlastního.

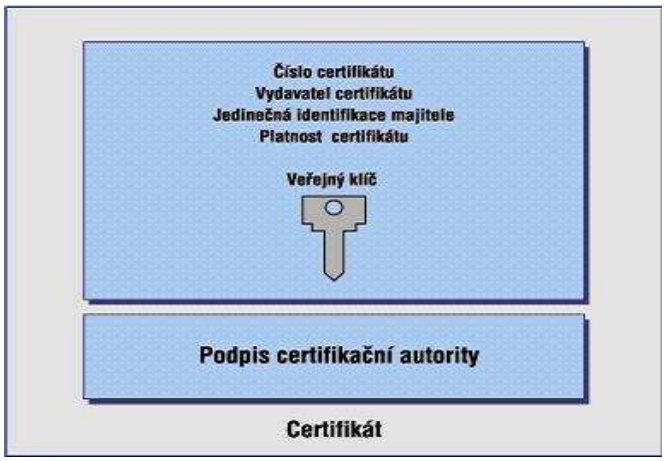
Proces získání značky probíhá následovně – otisk souboru se spolu s dalšími údaji ve standardizovaném formátu zašle elektronicky autoritě, která nazpět zasílá obdržené údaje doplněné o časový údaj, číslo časového razítka, kontrolní součet a název vydavatele, kde celý tento soubor je podepsán soukromým klíčem, jenž zajišťuje důvěryhodnost časového údaje. Tímto krokem je napevno svázán „hash“ s časem. [11], [13]



Obrázek 1-5 časové razítko [11]

1.7 Digitální certifikát

Hlavní složky digitálního certifikátu jsou veřejný klíč a osobní údaje vlastníka. Jde o standardní datový soubor, nejčastěji je využíván formát definovaný normou X.509 tak, aby je bylo možno využívat ve všech systémech bez omezení.



Obrázek 1-6 Digitální certifikát [6]

Certifikát vydává certifikační autorita, která jako nezávislý subjekt autorizuje vlastníka klíče při vzájemné komunikaci subjektů. Certifikát tak funguje v elektronickém světě jako občanský průkaz a certifikační autorita má podobný význam jako notář. Důvěryhodnost toho certifikátu je zaručena podpisem soukromým klíčem autority. Ověření proběhne stáhnutím paritního klíče z webu. Certifikační autorita certifikuje pomocí několika certifikátů, které jsou zastřešeny kořenovým certifikátem. Vzniká tak hierarchie certifikátů. Pro ověření je nutné mít nainstalovány všechny.

Dalšími složkami jsou identifikační údaje (např. i email) počátek a konec platnosti certifikátu – délka platnosti je úměrná síle klíče (resp. jeho délce). Pokud by byla délka klíče malá a platnost nepřiměřeně dlouhá mohlo by dojít k prolomení kódu. Většinou bývá platnost 6 měsíců. Dále pak jméno certifikační autority, která certifikát vydala, sériové číslo (nesmí se opakovat) a jiné. Jako například - omezení nakládání, identifikátor MPSV, link na neplatné certifikáty nebo identifikace testovacího certifikátu. [3], [5], [6]

Jak uvádí zákon č. 227/2000 Sb., § 12 [16], ***Kvalifikovaný certifikát musí obsahovat***

- *označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,*
- *v případě právnické osoby obchodní firma nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,*
- *jméno, popřípadě jména, a příjmení podepisující osoby nebo pseudonym s příslušným označením, že se jedná o pseudonym,*
- *zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,*
- *data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,*

- *elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává,*
- *číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,*
- *počátek a konec platnosti kvalifikovaného certifikátu,*
- *případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,*
- *případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.*

Tvorba certifikátu:

- Generování klíčů – pomocí běžného SW vybavení vygenerujeme klíče
- Žádost – souhrn informací nutných pro vydání
- Předání podkladů autoritě (elektronicky)
- Ověření – kontrola totožnosti (většinou osobně, zaslání notářsky ověřené smlouvy)
- Vydání a předání certifikátu (paměťové medium, web nebo zaslání mailem)

1.8 Certifikační autorita

Certifikační autorita (CA) je svou funkcí podobna notáři. Autorita ztvrzuje identitu vlastníka a správnost certifikátu, tím odstraňuje nutnost utajené výměny klíče mezi stranami. Zajištění správnosti a jedinečnosti údajů je založeno na pravidlech a normách daných zákonem, který platí pro certifikační autority. Zbytek je už jen na domluvě o společné autoritě a zabezpečení vlastního klíče. Na rozdíl od klasického notáře tak není stvrzen jeden podpis, ale systém, který produkuje neomezený počet digitálních podpisů. To dává za vznik smlouvě, která definuje vzájemná práva a povinnosti po celou dobu platnosti certifikátu. Majitel certifikátu je pak povinován aktualizací všech údajů o sobě. V některých případech je potřeba ukončit platnost vydaného certifikátu (změna údajů, prozrazení klíče,…), proto certifikační autorita kromě vydávání a správy certifikátu také publikuje seznam zneplatněných certifikátů (CRL), který je pravidelně aktualizován. Ochrana tohoto seznamu je podobná jako u certifikátu.

Chování, které je pro certifikační autoritu směrodatné, vychází z certifikační politiky, jejíž náležitosti opět vymezuje zákon. Součástí bývá alespoň jedna registrační autorita. Registrační autorita může být vlastní, smluvní nebo mobilní – pouze přijímá a kontroluje žádosti. [3], [6], [14]

2 Rozbor situace používání elektronických podpisů a elektronických razítek

2.1 Certifikáty v praxi

Hlavní rozdíly plynou především v různém užití, technicky se neliší až na určitá identifikační pole a právní následky.

Kvalifikovaný certifikát – je v praxi koncipován zvláště pro zajištění zásad integrity a neodmítnutelnosti, tj. především k zajištění identifikace komunikující osoby a zabezpečení proti pozdějším změnám v zaslaných dokumentech. Samozřejmě jde tímto certifikátem šifrovat, ale některé certifikační autority ve svých politikách omezují použití pouze na předchozí dva účely.

Komerční certifikát – je doporučen pro realizaci zásady důvěrnosti. Hlavním účelem by mělo být tvorba šifrovaného dokumentu a dále využití ve sférách mimo státní správu, která striktně vyžaduje kvalifikované certifikáty

Systémové/serverové certifikáty – oproti předchozím certifikátům může být vydávající osoba státní úřad nebo právnická osoba. Dále může sloužit k zabezpečené komunikaci mezi serverem a klientem např. u webových aplikací. [5], [6], [13]

2.2 Uložiště certifikátu

Jak již bylo řečeno v předešlých odstavcích, digitální podpis je důmyslný systém, ale nejzranitelnější je vlastní manipulace. Získaný certifikát je nutné někam uložit, abychom ho ochránili před zneužitím. Důležitost je stejná jako u PINu k bankovní kartě. Možnosti skladování jsou jak uvnitř počítače, tak vně.

Klíč může být uschován přímo v systému (resp. HDD). Toto řešení v našem výčtu můžeme považovat jako nejhorší. Místo klíče tak musíme střežit nejen vlastní hardware ale i umístněný software.

Uschování na HW vybavení počítače. Nevýhodou je možná rekonfigurace stroje.

Uložení vně počítače je v současnosti nejvyužívanější volbou - USB tokeny, čipové karty apod., kde médium je buď v paměťovém, nebo aktivním režimu. Paměťový režim – modul slouží pouze k uchovávání informací, které se zpracovávají vně. Aktivní režim – vnější aplikace pouze využívají výsledek operace a tím je zajištěna maximální ochrana klíče. V tomto případě je nutná přítomnost procesoru a příslušných jednotek, který pomocí

zavedených algoritmů provádí ověření digitálního podpisu. Klíč je tak „uzavřen“ uvnitř a nikdy neopustí vlastní jádro a ven se dostávají pouze výsledky operací.

Přístup bývá zajištěn PINem resp. PUKem. V případě špatného zadání PINu (PUKu) pak v rámci ochrany může dojít k smazání nebo úplnému zničení. [3], [11], [12]

2.3 Výběr certifikační autority

Na základě poznatků, které byly uvedeny v předchozích odstavcích, můžeme diskutovat otázku správného výběru certifikační autority. Jak uvádí Doležal [12], dělení může být podle následujících kriterií:

- Typ požadovaného certifikátu
- Důvěryhodnost certifikační autority
- Cena a úroveň poskytovaných služeb
- Způsob komunikace a dostupnost registrační autority
- Reference

Dle typu požadovaného certifikátu můžeme rozdělit poskytovatele do třech kategorií

- Akreditované Ministerstvem informatiky a uveřejněné v souladu s § 9 odst. 2, písm. e) zákona č. 227/2000 Sb.
- Komerční poskytovatelé bez akreditace
- Jiní a nekomerční poskytovatelé

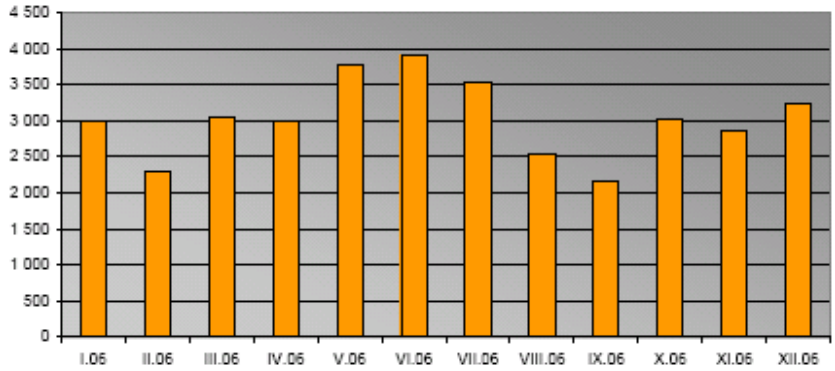
2.3.1 Certifikační autorita akreditovaná MIČR

Poř. číslo	Poskytovatelé certifikačních služeb	Kvalifikované služby
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů. Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.
2.	Česká pošta, s. p., identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů.
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů.

Tabulka 1 Akreditované certifikační autority [12]

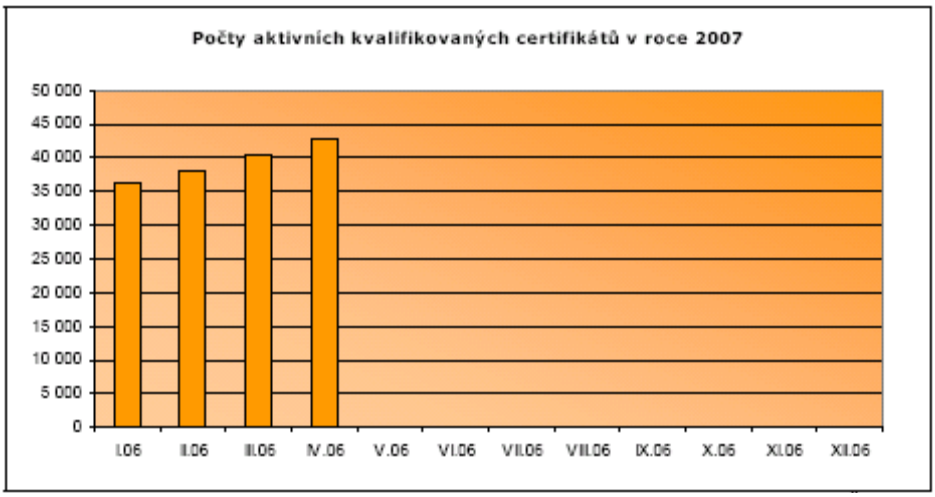
Vyjmenované certifikační autority jsou pro nás důležité, protože vydávají zaručené elektronické podpisy a kvalifikované certifikáty, které jsou jako jediné přípustné pro komunikaci se státní správou.

Během roku 2006 vydaly tyto subjekty 36 356 kvalifikovaných certifikátů a 3 420 614 kvalifikovaných časových razítek. Na konci roku tak bylo registrováno 35 050 platných kvalifikovaných certifikátů. [15]



Tabulka 2 Vydané kvalifikované certifikáty v roce 2006 [15]

Do května 2007 vydaly tyto subjekty 19 593 kvalifikovaných certifikátů (tj. o 73 % více než minulý rok) a 2 253 087 kvalifikovaných časových razítek. Na konci dubna bylo registrováno 43 088 platných kvalifikovaných certifikátů.



Tabulka 3 Počty aktivních kvalifikovaných certifikátů v roce 2007 [15]

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

Jak již název napovídá, vznikla jako první. Nejdříve ve formě projektu v roce 1996 a následně byla roku 2001 založena jako dceřiná společnost PVT, a.s. Od ostatních akreditovaných společností se dále liší možností vydávat kvalifikovaná časová razítka.

V nabídce má následující služby registračních autorit:

Klientská registrační autorita

Smluvní autorita je zřízena na místě dle požadavku klienta, který se nadále stará o správu tohoto střediska. Vhodné pro společnosti s větším počtem zaměstnanců.

Veřejná registrační autorita

Dnes 15 registračních míst provozovaných převážně ve větších městech. Slouží pro příjem a ověřování žádostí.

Mobilní registrační autorita

Po domluvě s klientem je zajištěn výjezd na předem definované místo, kde I.CA zajistí vydání většího počtu certifikátů. Vhodné pro lokality kde se nenachází registrační autorita.

Nabízené služby

Testovací certifikáty

Poskytuje pro ověření funkčnosti technologie použité pro realizaci tvorby elektronického podpisu. Dostupné téměř ihned po zadání, bez nutnosti ověření žádosti v místě registrační autority a zdarma. Certifikát má platnost 14 dní. Vytvoření certifikátu probíhá v pěti krocích.

- Na stránce http://www.ica.cz/home_cs/ vybereme žádost o certifikát/testovací certifikát
- Nainstalujeme kořenové certifikáty přímo z odkazu nebo naimportujeme do internetového prohlížeče patřičné soubory. Dále vybereme z nabízených možností certifikát pro osobu nebo server a dále fyzická osoba, zaměstnanec nebo právnická osoba
- Vybereme typ klíče a zadáme identifikační údaje – jméno, příjmení a email
- Aplikace vygeneruje pár klíčů a potvrdíme žádost
- Žádost odešleme

Kvalifikované certifikáty

Pro získání je nutné ověření na kontaktním pracovišti I.CA. Certifikát má platnost 1 rok. Oproti testovacímu certifikátu nabízí více možností pro umístnění klíče, variant žadatelů a volby komunikačního rozhraní. „Kvalifikované certifikáty, vydané poskytovatelem certifikačních služeb (I.CA) v souladu se zákonem 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů v platném znění, lze používat pro následující účely:

- ověřování elektronických podpisů

- bezpečné ověřování elektronických podpisů
- zajištění neodmítnutelnosti odpovědnosti
- v případě, že je zaručený elektronický podpis založený na kvalifikovaném certifikátu používaný pro autentizaci, musí být podepisující osoba provozovatelem příslušné aplikace informována, zda má nebo nemá možnost se seznámit s daty, které podepisuje
- pokud klient při tvorbě žádosti nastaví odpovídající kritický atribut Key Usage, může využívat kvalifikované certifikáty i pro následující účely:
- NonRepudation (povinný) - klíč bude používán pro vytváření elektronického podpisu
- DigitalSignature (nepovinný) - soukromý klíč bude obecně používán pro vytváření elektronického podpisu (např. v rámci bezpečné elektronické pošty)
- KeyEncipherment (nepovinný) - veřejný klíč obsažený v tomto kvalifikovaném certifikátu bude používán pro účely šifrování v rámci bezpečné elektronické pošty. V prostředí MS Outlook je rovněž nutno tento bit nastavit v případě, že uživatel nemá jiný certifikát, který lze použít k šifrování. Toto neplatí pro verze MS Outlook Express a MS Outlook 2002 SP4 a vyšší.
- DataEncipherment (nepovinný) - veřejný klíč obsažený v tomto kvalifikovaném certifikátu bude používán pro šifrování obecných dat, např. dokumentů “[6]

Kvalifikované certifikáty se dělí na:

- Certifikát standard – uložiště dat je na USB tokenu, v systému apod.
- Certifikát komfort – uložiště dat je na čipové kartě

Kvalifikované systémové certifikáty

Pro získání je nutné ověření na kontaktním pracovišti I.CA. Certifikát má platnost 1 rok. Lze používat pro následující účely:

- ověřování elektronických značek,
- bezpečné ověřování elektronických značek,
- zajištění neodmítnutelnosti odpovědnosti.

Kvalifikovaná časová razítka

Razítko se vydává vlastníkům komerčních certifikátů vydaných I.CA

Komerční certifikáty

Pro získání je nutné ověření na kontaktním pracovišti I.CA. Oproti testovacímu certifikátu nabízí více možností pro umístnění klíče, variant žadatelů a volby komunikačního rozhraní. Certifikát má platnost v závislosti na délce klíče.

Komerční certifikáty se dělí:

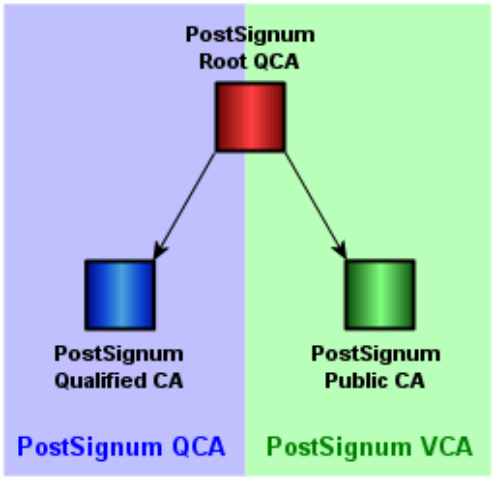
- Certifikát standard – vhodné pro běžné využití
- Certifikát komfort – oproti předchozí variantě je využívána čipová karta a certifikát je používán hlavně pro tvorbu digitálního podpisu
- Certifikát pro server - určeno pro bezpečnou komunikaci serverů

Ostatní služby

Žádost o zneplatnění. Seznam certifikátů. Seznam zneplatněných certifikátů. [6]

2.3.1.2 Česká pošta, s. p. (PostSignum)

Certifikační autority PostSignum tvoří následující stromovou strukturu:



Obrázek 2-1 Struktura PostSignum [7]

Poskytováním se Česká pošta, s. p. zabývá již od roku 1999 neveřejně a od roku 2003 jako veřejná komerční autorita. Certifikát taktéž využívala pro svoji službu registrované elektronické pošty. Služba je elektronickou obdobou zásilky s doručenkou a dodací schránky. V roce 2005 získává akreditaci Ministerstva informatiky.

PostSignum má 7 obchodních míst a 74 kontaktních míst, převážně v bývalých okresních městech. Všechna místa nemají provoz bez omezení. Obdobně jako I.CA nabízí mobilní registrační autoritu, ale pouze pro kvalifikované certifikáty.

PostSignum nikde na svých stránkách nenabízí možnost vydání testovacího certifikátu. [7]

Postup pro vydání certifikátu:

1. Vygenerování klíčů a žádosti o certifikát:
   On-line generování - generování probíhá přímo v prohlížeči a požadavky omezují uživatele hlavně softwarově (Windows 2000/2003/XP, IE6 a výše). Žádost je možné zaslat elektronicky nebo doručit na kontaktní místo.
   Off-line generování – pomocí nástroje PostSignum Tool jsou vygenerována data, jenž je zapotřebí zanést na kontaktní místo.
2. Příprava podkladů před návštěvou České pošty
   Z webových stránek je nutné stáhnout a vyplnit objednávku a zákaznický formulář.
3. Uzavření smlouvy s Českou poštou
   Smlouva je uzavřena na kontaktním místě na základě doručených podkladů.
4. Vydání certifikátu
   Po ověření ze strany české pošty dojde k vydání certifikátu
5. Instalace certifikátu
   Instalace na počítači, kde byla žádost vytvořena (je zde zálohován soukromý klíč, který byl generován při kroku č.1.)

Kvalifikované certifikáty

Certifikáty pro ověření elektronického podpisu zaměstnance, Certifikáty organizace pro ověření elektronické značky, Certifikáty pro ověření elektronického podpisu fyzické osoby, Certifikáty pro ověření elektronické značky fyzické osoby

Komerční certifikáty

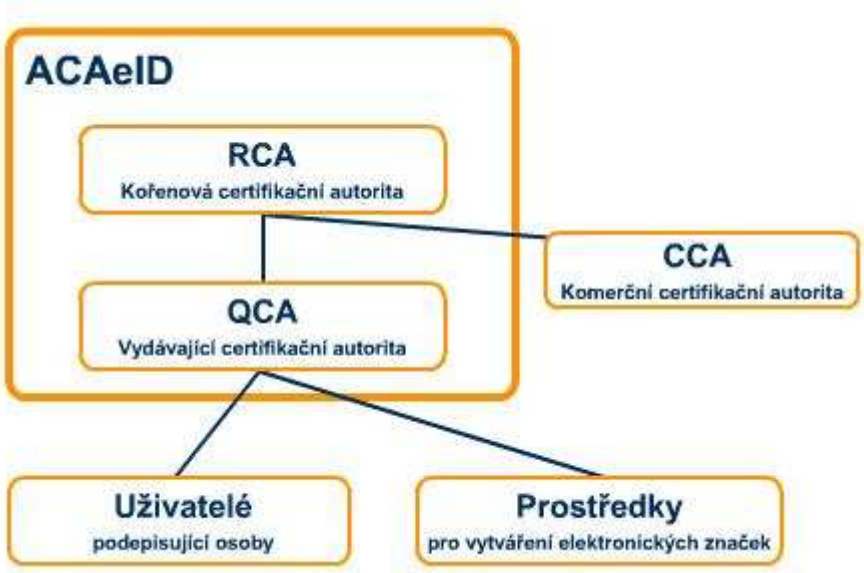
Certifikáty pro zaměstnance a podnikající fyzické osoby, Certifikáty pro technologické komponenty organizace (určeny pro zařízení či aplikace), Šifrovací certifikáty pro skupiny osob (speciální certifikáty, které se používají v aplikaci REP, dalším produktu České pošty), Certifikáty pro fyzické osoby, Certifikáty pro technologické komponenty fyzických osob

Ostatní služby

Žádost o zneplatnění. Seznam certifikátů. Seznam zneplatněných certifikátů. [7]

2.3.1.3 eIdentity a.s.

Společnost vzniká v roce 2004 přejmenováním z poněkud neznámé společnosti Intertel CZ a.s. Společnost odkoupila autoritu od firmy KPN-QWEST (dle informaci uvedených na stránkách společnosti e-Business Services a.s. http://www.e-bs.cz/content.php/company/dcery.htm). V roce 2005 obdržela akreditaci Ministerstva informatiky a stává se třetí akreditovanou autoritou na českém trhu. Certifikáty vydává Akreditovaná certifikační autorita eIdentity a.s. (ACAeID). Certifikační autorita ACAeID tvoří následující stromovou strukturu [8]:



Obrázek 2-2 Struktura eIdentity [8]

eIdentity má pouze jedno kontaktní místo a taktéž jako PostSignum nenabízí testovací certifikát.

Postup pro vydání certifikátu

Kromě finální návštěvy je celá proces komunikace založen na webové aplikaci, kde oproti PostSignum nejsou deklarované žádné systémové omezení.

1. Vytvoření zákaznického účtu

   Při registraci je nutné zadat základní identifikační údaje, kde je následně vygenerován email s přihlašovacím heslem. Následuje doplnění zbylých podrobností.
2. Zákaznický účet

   Slouží jako sumarizace všech zakázek
3. Objednání služby

Přes výběr požadované služby, odsouhlasení návrhu smlouvy a zaplacení zálohové platby je vygenerován pár klíčů a domluven termín návštěvy kontaktního centra

4. Návštěva Registračního místa
   Po ověření všech předložených údajů je vystaven certifikát.

Komerční certifikáty

komerční certifikát pro elektronický podpis, komerční certifikát pro šifrování zpráv, komerční certifikát pro identifikaci, komerční serverový certifikát pro SSL/TLS

Kvalifikované certifikáty

kvalifikovaný certifikát, kvalifikovaný certifikát s vyznačením identifikátoru ministerstva práce a sociálních věcí (MPSV), kvalifikovaný certifikát s vyznačením pracovní pozice v organizaci, kvalifikovaný systémový certifikát

Ostatní služby

Žádost o zneplatnění certifikátu. Seznam certifikátů. Hosting a outsourcing komerčním certifikačním autoritám třetích stran – poskytování služby třetí straně, jenž nevlastní patřičnou infrastrukturu. Balíček certifikátu – vydání dvou certifikátu za přibližně cenu jednoho. [8], [13]

2.3.2 Komerční poskytovatelé bez akreditace

2.3.2.1 Certifikační autorita Czechia, s.r.o.

Zahájila svoji činnost v roce 1999 a to ještě pod jménem Altimo, s.r.o. V roce 2002 vyčleňuje veškeré aktivity od mateřské společnosti a vzniká certifikační autorita Czechia, s.r.o. Registrační autorita nabízí dvě kontaktní místa pro ověřování.

Postup pro vydání certifikátu

Postup začíná podpůrnými informacemi definujícími požadavky na systém a software. Dále je nutné provést instalace kořenových certifikátů, registraci účtu a vyplnění osobních údajů. Pokračujeme výběrem a doplnění základních informací k vybranému certifikátu, kde jsou nabízeny různé úrovně zabezpečení soukromého klíče. Na základě zadaných údajů je připraven návrh smlouvy. K vystavenému certifikátu je zaslána faktura a poté nezbývá než nainstalovat doručený certifikát.

Nabízené certifikáty

Testovací certifikát

Platnost je 1 měsíc s délkou klíče 512 bitů a je poskytován zdarma.

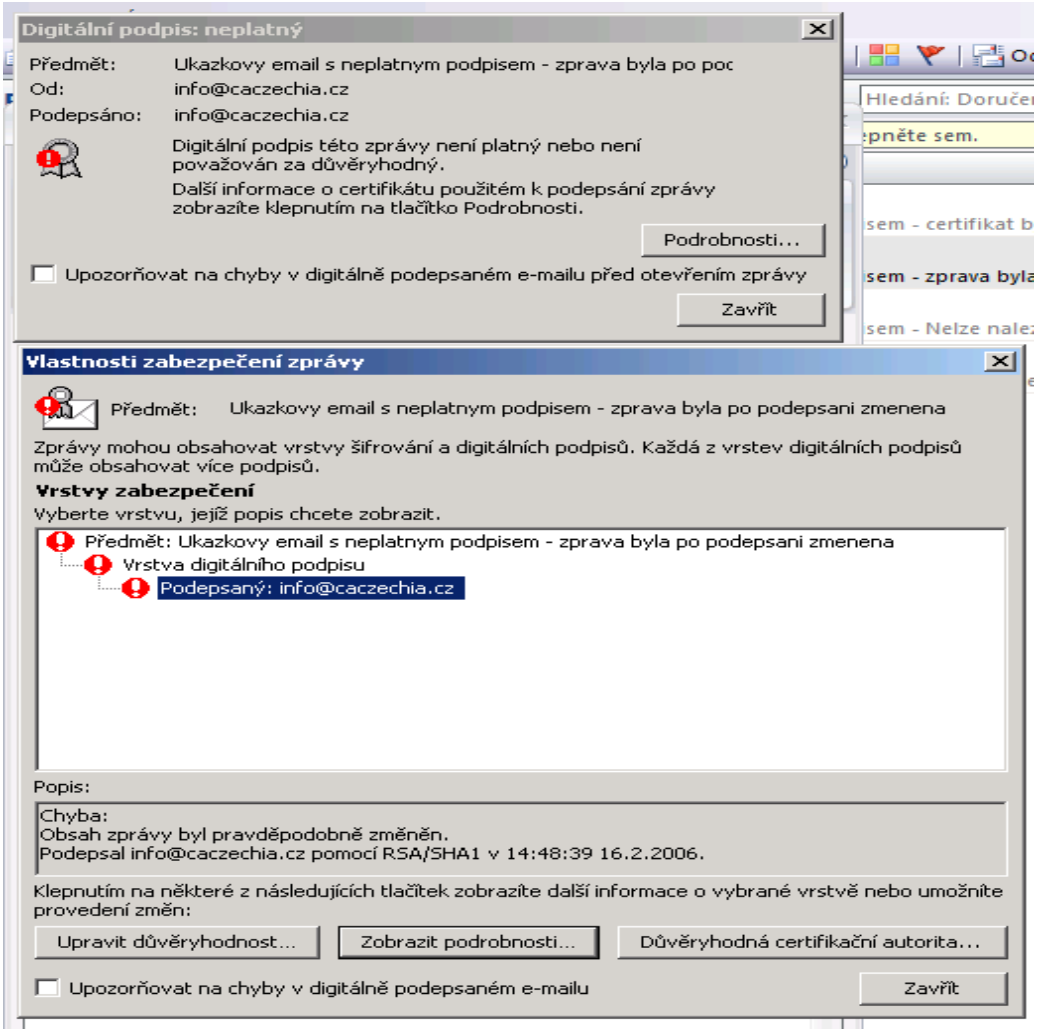
Osobní certifikát

Firemní certifikát

Další služby

Zaslání ukázkového emailu

Zaslání ukázkového emailu s neplatným podpisem – (Nelze nalézt digitální ID, Zpráva byla po podepsání změněna, Platnost certifikátu vypršela, Certifikát byl zneplatněn, Certifikát vydala CA, které zatím nedůvěřujete). Jako ostatní poskytovatelé nabízí zneplatnění certifikátu a jejich seznam. [9]



Obrázek 2-3 Ukázka změněné zprávy po odeslání [9]

2.3.2.2 Certifikační autorita TrustPort (AEC, spol. s r.o.)

Poskytuje zdarma testovací certifikát s platností 1 rok a časové razítko. [10]

2.3.3 Jiní a nekomerční poskytovatelé

Tyto certifikační autority poskytuji služby pouze svým zákazníkům, klientům nebo členů určité komunity.

V oblasti školství - VŠE, CESNET, FEL ČVUT, VŠB, MUNI, apod.

Ostatní - CA InWay, CA Decent Hosting, CA Active 24, apod.

2.4 Srovnání certifikačních autorit

Ve svém srovnání bych vyšel ze sestavené tabulky, která nám umožní srovnat cenové nabídky jednotlivých služeb a dále porovná výše uvedené parametry. Dovolil bych si předznamenat, že moje porovnání nemá jednoznačného vítěze ani poraženého a každá certifikační autorita má čím zaujmout. První certifikační autorita zajisté na první pohled zaujme velikostí, tím že byla první a vlastnickou strukturou (Česká spořitelna, Československá obchodní banka, Telefónica O2 Czech Republic, aj.), což určitě vypovídá o mnohém. Jako jediná vydává kvalifikovaná časová razítka. Dostupnost registrační autority je solidní. Kromě jedné služby vychází jako nejdražší. PostSignumu hraje do karet největší počet poboček registrační autority a agresivní cenová politika některých certifikátů. Oproti I.CA nelze certifikáty využít jako identifikaci a šifrování zároveň (viz. text). eIdentity toto kompenzuje „bundlováním“ certifikátů. Oproti předchozím se jedná o poněkud neznámou společnost, jejíž vize maximálního zjednodušení vydávání certifikátů určitě najde svoje místo. Ačkoliv není Czechia autorizovanou certifikační autoritou zaujala mne možnost zaslání testovacího emailu i s možností demonstrace různých chyb a taktéž testovací certifikát. Mnoho hodnotitelů považuje jako jediný srovnávací parametr cenu. S tímto postupem se neztotožňuji hlavně vzhledem užitné hodnotě produktu a nutností porovnávat další servis poskytovatelů. [12], [13]

Ceny v Kč s DPH	**I.CA**	**Post Signum**	**eIdentity**	**Czechia**	**AEC TrustPort**
Kvalifikovaný certifikát	752	190	702	X	X
Kvalifikovaný systémový certifikát	780	2856	3451	X	X
Kvalifikovaná časová značka	ANO	X	X	X	ANO
Komerční certifikát	580	190	238	159	X
Komerční certifikát pro servery	1931	800	752	1000	X
Testovací certifikát	ANO	X	X	ANO	ANO
Ukázkový email	X	X	X	ANO	X
Balíček 1	X	X	821	X	X
Balíček 2	X	X	3827	X	X

Tabulka 4 Přehled cen certifikačních autorit [vlastní tvorba]

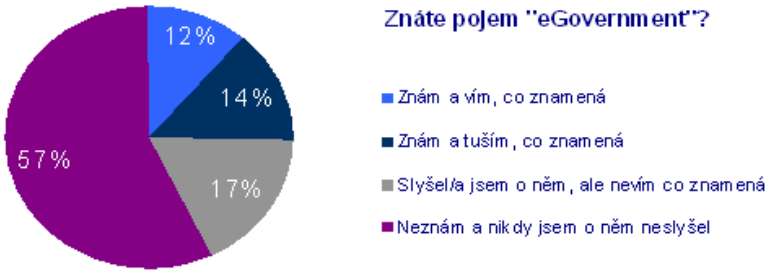
2.5 Využití v reálných aplikacích

Dle různých kriterií by se užití dalo dělit několika způsoby:

- smluvní vztahy (např. elektronický obchod, finanční transakce)
- v privátních systémech (Intranety)
- pro personální potřebu
- identifikace a autorizace (oprávnění přístupu do systému, identifikace webového serveru,…)
- komunikace s veřejnou správou (daňová podání, přenos dokumentů s právními důsledky, oznámení,…) [14]

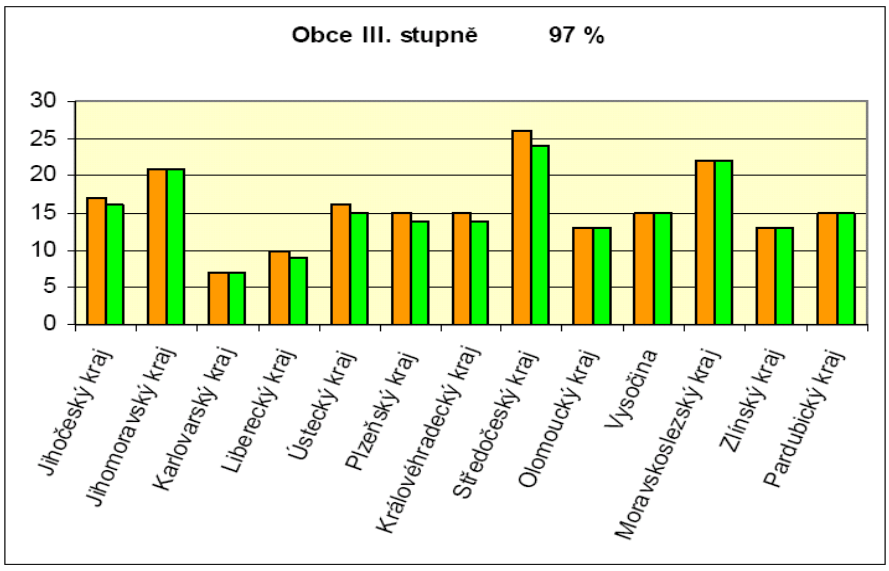
2.5.1 Veřejná správa

Nepochybně bude elektronický podpis jeden z nástrojů budovaného e-Governmentu, který by měl vyřešit nekonečné běhání po úřadech. Celý systém se teprve rodí a jeho prvními krůčky jsou digitalizace údajů, rozvoj informačních systému, rozšíření kontaktních míst apod. Bohužel informovanost není ideální, jak ukazuje následující obrázek. [30]

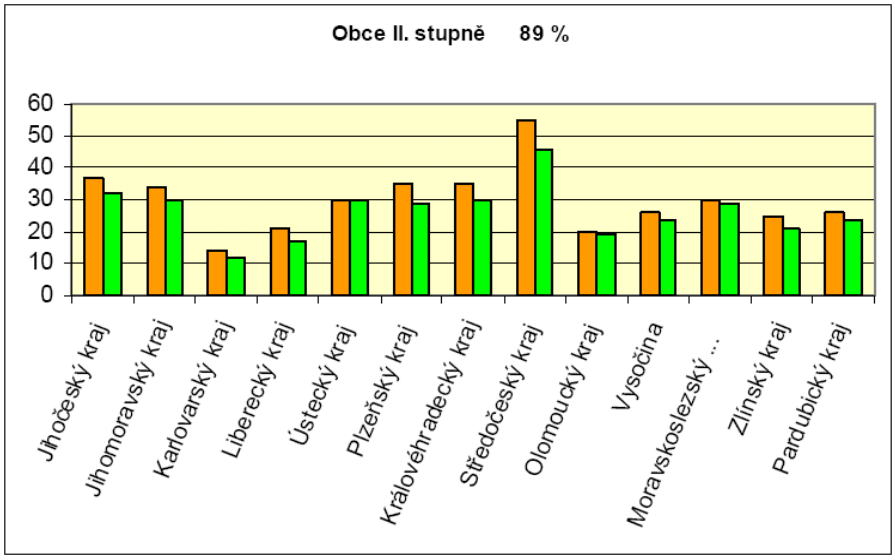


Graf 1 Znalost pojmu „eGovernment“ [30]

Jako vhodný podklad pro srovnání a zmapování rozvoje digitálního podpisu jsem využil článek Vícha [18]. V roce 2004 začíná předávat Ministerstvo informatiky zdarma kvalifikované certifikáty úřadům státní správy. Oproti nelichotivým údajům platným k roku 2004, kde úřady převzaly pouze necelých 800 certifikátů z celkového počtů převyšujícího 6000, se situace radikálně zlepšila. Podle nařízení vlády č. 495/2004 Sb. je jednoznačně stanovena povinnost pro orgány veřejné moci přijímat a odesílat datové zprávy se zaručeným elektronickým podpisem založených na kvalifikovaných certifikátech vydávaných akreditovanými poskytovateli certifikačních služeb. Pro realizaci tohoto procesu se zřizují elektronické podatelny. Jak vyplývá ze zprávy *Informace o zřízení elektronických podatelen u orgánů veřejné moci* [15], která sumarizuje situaci k 1. lednu 2007 jsou výsledky potěšující. V oblasti ústředních orgánu splnilo povinnost 14 z 15 orgánů. U dalších ústředních orgánů to je 10 z 11. Krajské úřady jsou úspěšné na 100%. Z celkového počtu 205 obcí s rozšířenou působností (obce III. st.) splnilo povinnost 198 obcí. Z celkového počtu 388 obcí s pověřeným obecním úřadem (obce II. st.) splnilo povinnost 344 obcí. [12], [15], [19]



Obrázek 2-4 Informace o podatelnách I. [15]



Obrázek 2-5 Informace o podatelnách II. [15]

2.5.1.1 Ministerstvo financí ČR

Vzhledem ke svojí náplni je lídrem v elektronické komunikaci mezi občany a úřadem. Při zahájení činnosti v roce 2003 šlo pouze o 4060 podání, oproti roku 2007 kdy bylo registrováno 132 115 podání se zaručeným digitálním podpisem. Pomocí programu, který je k dispozici na http://adisepo.mfcr.cz/ je možno podávat následující podání:

- Formuláře pro daňovou informační schránku
- Daňové přiznání k silniční dani
- Daňové přiznání k dani z nemovitostí
- Daňové přiznání k dani z přidané hodnoty
- 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

Data je možné zpracovat pomocí webového prohlížeče Microsoft Internet Explorer verze 5 a vyšší (nutné nainstalovat Javu) nebo je načíst jako soubor XML.

Dokument je možné podat podepsaný zaručeným elektronickým podpisem nebo bez, ale pak je nutné doručit tento dokument ještě písemně. [12], [17]

2.5.1.2 Česká daňová správa

Jako složka Ministerstva financi provozuje daňový portál, který usnadňuje komunikaci subjektů s úřadem. Oproti možnostem, které jsou nabízeny na stránkách ministerstva, dochází rozšíření služeb a zvýšení komfortu. Nutným předpokladem je vlastnictví kvalifikovaného certifikátu. Jako veřejné služby jsou nabízeny Elektronická podání pro daňovou správu a Zjištění stavu zpracování elektronických podání. Pro další služby Osobní daňový kalendář, Přehled písemností a Personalizovaná elektronická podání je nutné si nechat zřídit daňovou informační schránku. Ke konci roku 2007 evidovala daňová správa 10800 žádosti o schránku a 326 647 podání (tento údaj se liší od informace získané na stránkách ministerstva). Na rok 2008 se očekává překročení hranice 500 000 podání. [12], [17]

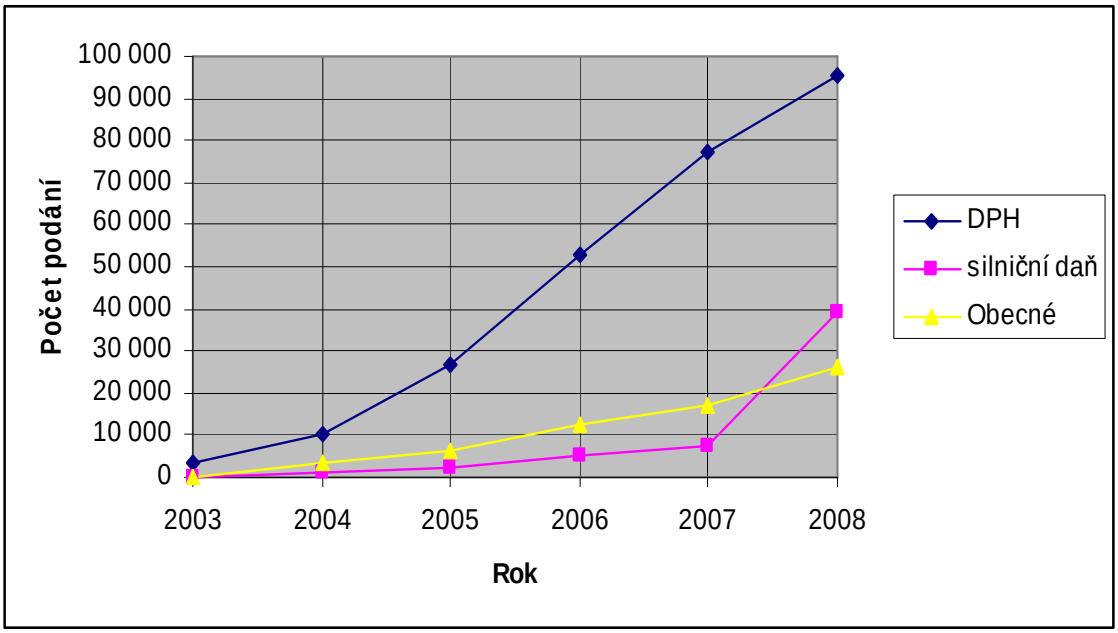
Typ písemnosti (Typ podání)		Rok					
		2003	2004	2005	2006	2007	2008 (31.3.)
Daň z nemovitostí	ZAREP	460	396	703	961	1 264	1 225
	Ost	325	374	1 070	1 257	1 621	1 925
Daň z přidané hodnoty	ZAREP	3 353	10 162	26 965	53 122	77 342	23 933
	Ost	1 773	3 360	4 742	5 410	7 010	1 933
Souhrnné hlášení VIES	ZAREP	0	290	1 410	2 931	4 615	1 406
	Ost	0	121	325	414	456	129
Daň silniční	ZAREP	14	899	2 185	4 830	7 577	9 788
	Ost	789	901	1 077	1 671	1 459	1 594
Daň z příjmů fyzických osob	ZAREP	0	172	1 495	3 105	5 573	1960
	Ost	0	21	1 009	2 149	3 619	5312
Daň z příjmů právnických osob	ZAREP	0	182	1 243	2 613	4 670	1085
	Ost	0	24	260	289	411	393
Oznámení podle § 34 zákona č.337/1992 Sb.	ZAREP	0	4	83	80	158	166
	Ost	71	13	26	40	68	69
Obecná podání	ZAREP	233	3 286	6 385	12 473	17 196	6 596
Hlášení platebního zprostředkovatele	ZAREP	0	0	0	50	134	119
	Ost	0	0	0	116	123	43
Vyúčtování daně z příjmů fyzických osob	ZAREP	0	0	0	1 158	2 736	3 693
	Ost	0	0	0	112	387	475
Žádost o zřízení/zrušení DIS	ZAREP	0	0	0	5 243	5 625	1 865
Přihlášení ke službám daňového portálu	ZAREP	0	0	0	4 842	5 225	1 998
Celkem	ZAREP	**4 060**	**15 391**	**40 469**	**91 408**	**132 115**	**53 853**
	Ost	***2 958***	***4 814***	***8 509***	***11 458***	***15 154***	***11 873***

Tabulka 5 Počty elektronických podání uskutečněných prostřednictvím aplikace EPO [17]

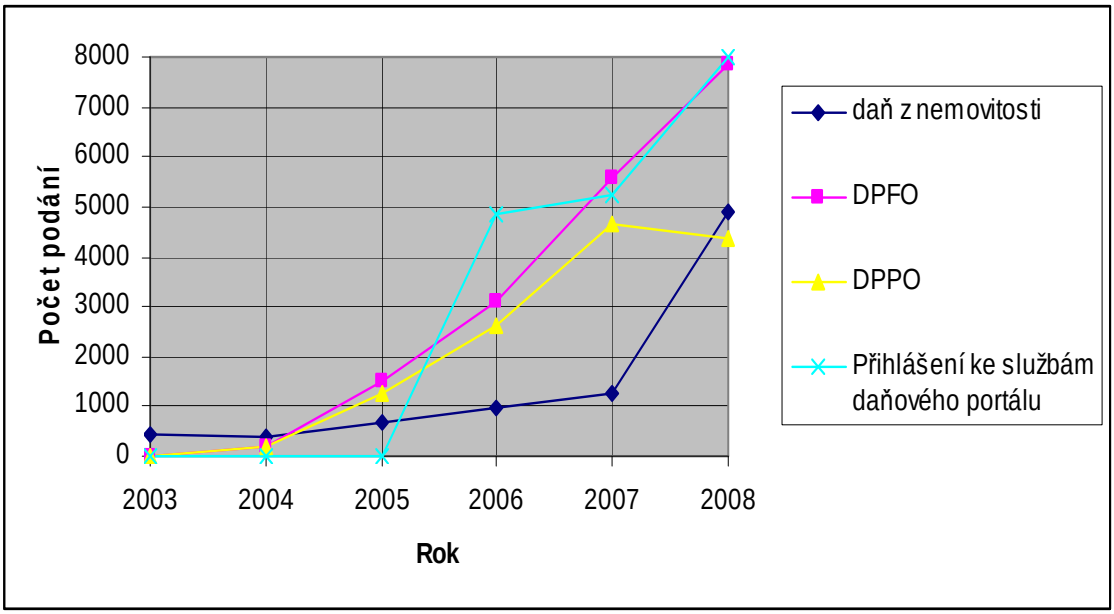
Vysvětlivky k tabulce 5:

Zarep ... S tzv. zaručeným elektronickým podpisem, neboli kvalifikovaným certifikátem obsahujícím informace podle zákona č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů

Ost ... Bez tzv. zaručeného elektronického podpisu



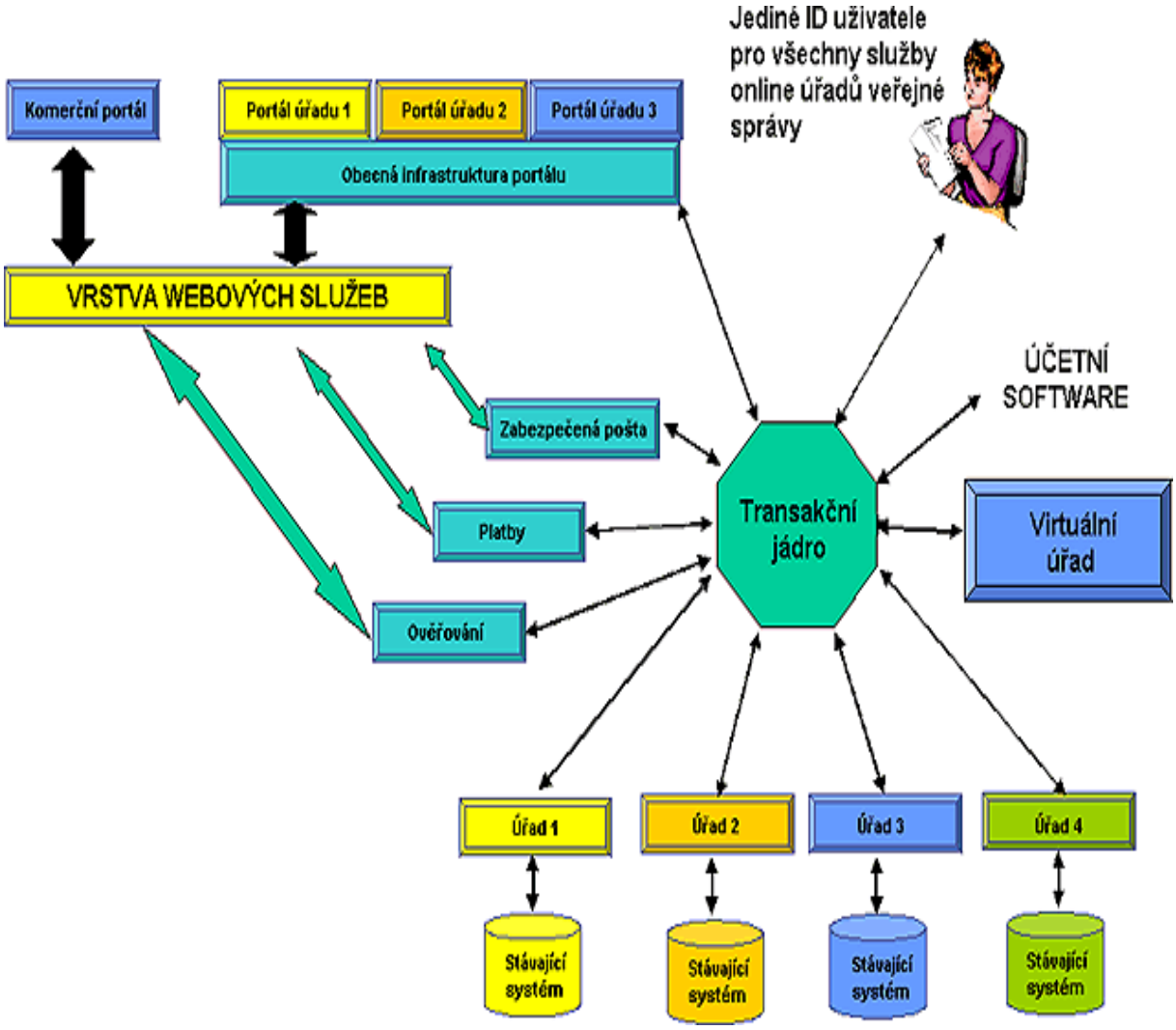
Graf 2 Počty elektronických podání uskutečněných prostřednictvím aplikace EPO I. [17]



Graf 3 Počty elektronických podání uskutečněných prostřednictvím aplikace EPO II. [17]

2.5.1.3 Portál veřejné správy

Na portálu je možno učinit elektronické podání v sekci podání. Aplikace je připravena pro ty z řad občanů, organizací a zplnomocněných zástupců, kteří chtějí využívat elektronické komunikace nabízené ze strany státní správy. Myšlenkou celého projektu je jednotné přístupové místo pro různé druhy podání. Jednotný vstup je realizován např. pro Českou správu sociálního zabezpečení, Ministerstvo financí – daňová správa, Generální ředitelství cel a další. Při registraci do systému je na výběr možného zabezpečení certifikátem nebo uživatelským certifikátem. Registrovaným uživatelů je umožněno přijímání a odesílání formulářů z jednotlivých úřadů. Registrace na portálu je nutná podmínka. K dispozici jsou odkazy na další e-podatelny, která provozují jednotlivá ministerstva. [12], [19]



Obrázek 2-6 aplikace Elektronická podání

2.5.1.4 Česká správa sociálního zabezpečení

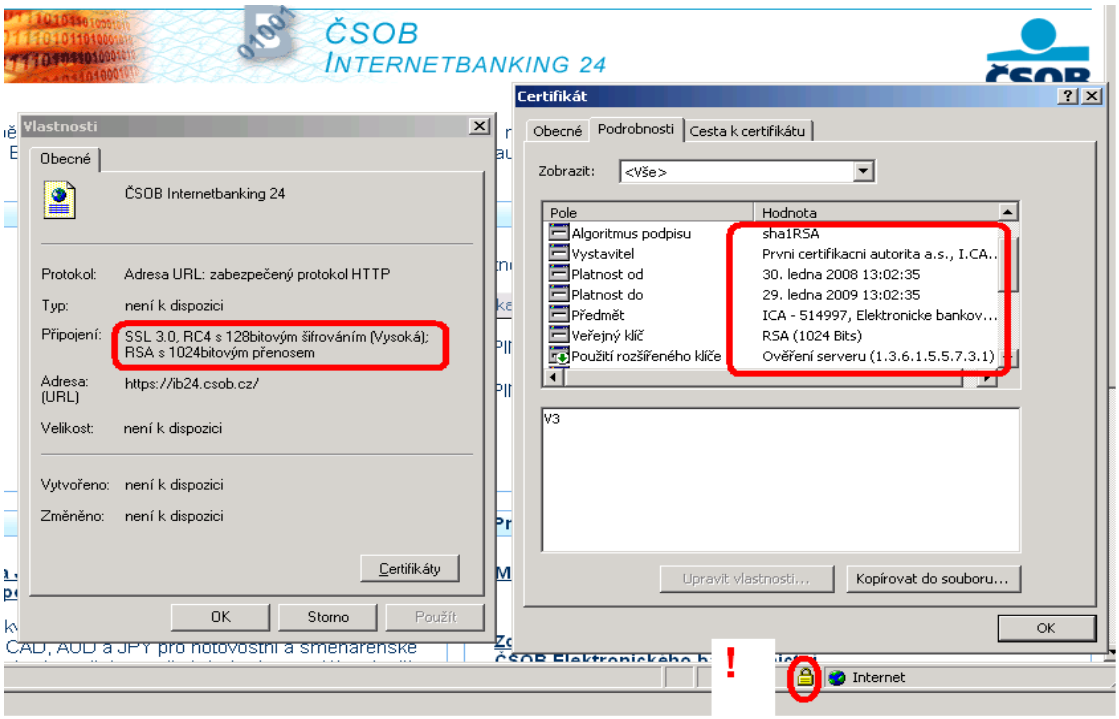
Formuláře je možné podat na paměťovém médiu (CD nebo disketa) v předem definovaném formátu nebo přes výše zmíněnou webovou aplikaci portálu veřejné správy ve formátu xml a elektronicky podepsané. Elektronicky je možno podat Evidenční listy důchodového pojištění (ELDP), přihlášky a odhlášky zaměstnanců k nemocenskému pojištění (P/O) a Přehled o příjmech a výdajích osob samostatně výdělečně činných (Přehled OSVČ). Česká správa sociálního zabezpečení drží prim v poskytování elektronického podání přes portál veřejné správy. Od svého začátku do konce ledna 2008 bylo přijato více než 22 milionů elektronických dokumentů. [12], [22]

2.5.1.5 Ministerstvo práce a sociálních věcí

Opět je v nabídce několik varianta na předání dat. Jako nejjednodušší možnost se nabízí tisk stažených formulářů s následným vyplněním nebo doplnění údajů do elektronického formuláře a uložením na přenosné medium. Jako nejkomfortnější a nejbezpečnější je možnost vyplnit údaje přímo na webu. Pro jednoznačnou identifikaci je využit digitální podpis. Pro zabezpečení komunikace mezi počítačem uživatele a serverem používá aplikace šifrovaný protokol https. Pro bezproblémovou funkčnost je zapotřebí nainstalovat certifikát ministerstva. [12], [23]

2.5.2 Otevřené sítě

Předpokládám, že aniž by většina uživatelů věděla, tak mnohokrát digitální podpis využila (nebo alespoň jeho důležitou součást – asymetrické šifrování). Většina zabezpečené komunikace se tímto způsobem děje na stránkách webových obchodů, veřejných tržištích, přístupech na intranety, stránky dodavatelů, odběratelů a bank. Jednoduše řečeno všude tam, kde se komunikace přesměruje z nezabezpečeného http na zabezpečený https. Přenášená data jsou zabezpečena šifrováním Secure Sockets Layer (SSL) nebo Transport Layer Security (TLS). Princip zabezpečení tak vychází z asymetrického šifrování, které používá již jmenované metody v oddíle - šifrování. Servery tak většinou vlastní certifikáty podepsané nejuznávanějšími certifikačními autoritami jako např. VeriSign, TC TrustCentre aj. Tímto certifikátem pak prokazuji uživateli svoji totožnost a uživatel si může být doopravdy jist identitou serveru. Asi nikdo nebude namítat, když prohlásíme, že to je ze všech vyjmenovaných služeb ta nejvyužívanější. [1], [4], [25]



Obrázek 2-7 Ukázka zabezpečené komunikace webové aplikace [31]

2.5.3 Identifikace a autorizace

2.5.3.1 Bankovní sféra

I zde je využíváno podobných principů, které byly zmíněny v předchozím odstavci. Jednotlivými stupni zabezpečení jsou – šifrovaný přenos http, heslo a podepisování certifikátem. Certifikát bývá uložen obvykle na čipové kartě nebo USB tokenu. Uživatel využívá dodatečný hardware (čtečka čipových karet), který si musí nainstalovat na svůj počítač. [3], [12], [13]

Obrázek 2-8 USB token [26]

2.5.3.2 Komerční sféra

Asi největší pole působnosti se dnes otvírá mezi dodavateli a odběrateli. Jejich často komplikovaná komunikace skládající se z množství faxů, dopisů a telefonátů se nahrazuje

čistě elektronickou komunikací, kdy se identifikace a zabezpečení realizuje přes digitální podpis. Protistrany si také stále častě umožňují přístup do vlastních systémů s využitím tohoto zabezpečení. [4]

2.5.4 Intranety a privátní užití

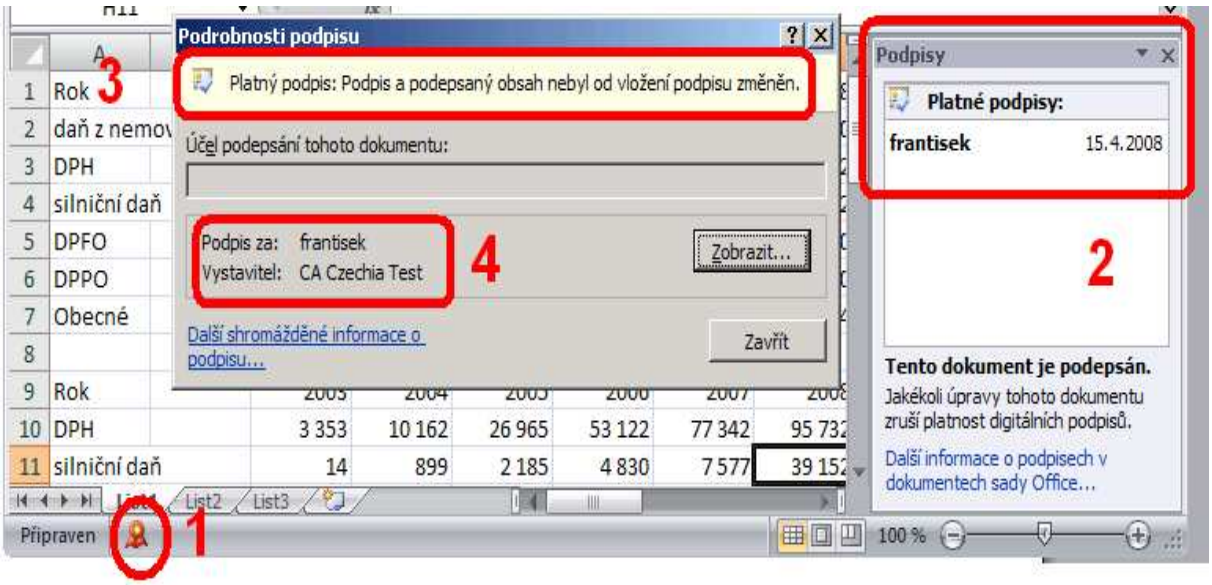
Technické řešení se v této oblasti podobá oblasti otevřené sítě. V rámci určitého subjektu probíhá zabezpečená komunikace výše popsaným systémem. Prakticky ani nelze vyjmenovat možné aplikace, ale namátkově uveďme – logování do firemních aplikací, intranetu, emailu, vystavování faktur apod.

2.5.4.1 Kancelářské aplikace

Po získání a instalaci certifikátu (popsáno v kapitolách 1 a 2) je možné využít digitální podpis v různých kancelářských aplikacích.

Aplikace Microsoft Office 2007 (Word, Excel a PowerPoint)

Sledem příkazů ze základního menu (Připravit/Přidat digitální podpis) můžeme dokument digitálně podepsat.

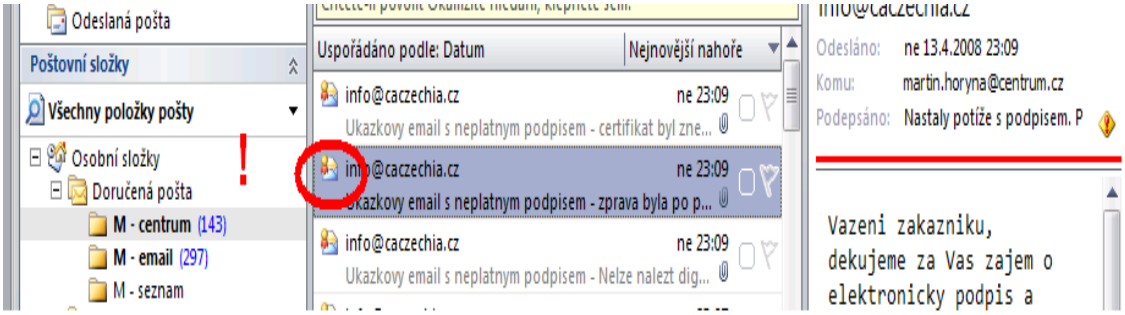


Obrázek 2-9 Zabezpečení v aplikacích Microsoft Office [32]

Zabezpečený dokument signalizuje na dolní liště dokumentu červený fáborek. Poklepáním se rozbalí okno podpisu, kde máme možnost přes podrobnosti podpisu zjistit další informace. Dokumenty jsou chráněny proti úpravám, které by následovaly po podpisu.

Microsoft Office 2007 Outlook

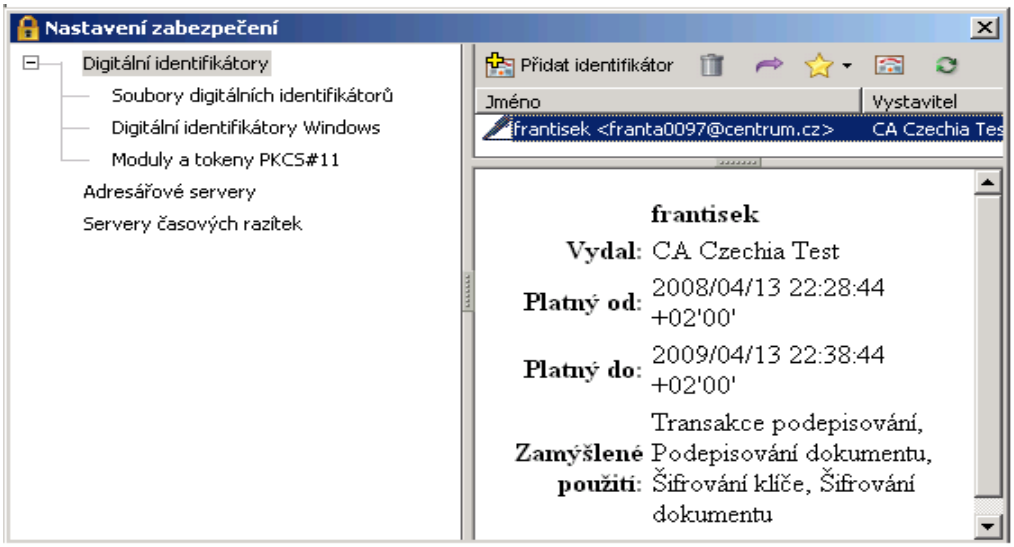
Podepsaný příchozí email signalizuje opět stejná ikona jako v předchozích aplikacích, která je umístněná u hlavičky emailu. Opět poklepáním zjistíme další podrobnosti (platnost, neplatnost, informace o odesilateli). Odchozí email můžeme označit digitálním podpisem volbou v možnostech odeslání. [32]



Obrázek 2-10 Podepsaný email [32]

Adobe Reader

Umožňuje digitálně podepsat, pouze pokud dokument PDF obsahuje speciální práva užívání (nebo u verze Adobe Acrobat bez omezení).



Obrázek 2-11 Zabezpečení v Adobe Readeru [33]

V obou případech lze dokumenty podepsat viditelně přímo do dokumentu nebo přidáním neviditelného digitálního podpisu. Pro podpis lze využít již získané certifikáty od certifikační autority nebo si vystavit vlastní. Další aplikace umožňující digitální podpis dokumentu – AutoCAD, Zoner Photo Studio, OpenOffice aj.

3 Právní problematika

Vývoj právních norem v oblasti elektronického podpisu a technologii s tímto spojených je dán harmonizací s evropskými normami. Kde klíčovou roli hraje Směrnice Evropského Parlamentu a Rady 1999/93/EC. Ve své podstatě jsou naše normy odvozeny nebo tvořeny tak, aby byly maximálně v souladu. [5], [6], [15]

3.1 Hlavní normy

Asi nejdůležitějším krokem bylo přijetí zákona **č. 227/2000 Sb.,** (zákon o elektronickém podpisu). Upravuje používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb. Jako první jsou vymezeny používané pojmy a definovány práva a povinnosti podepisující osoby a osob poskytujících certifikační služby. Dále jsou definovány kontrolní mechanizmy, odpovědnost za škodu, ochranu osobních údajů a sankce za porušení norem. Velmi důležité jsou náležitosti vydávaných certifikátů a především rozdíl mezi elektronickým podpisem a zaručeným elektronickým podpisem.

Zaručený elektronický podpis:

- 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

Je jako jediný akceptován při komunikaci s orgány veřejné moci. V textu je dále zmíněno uznávání zahraničních certifikátů a vymezení požadavků na prostředky pro bezpečné vytváření a ověřování. Následuje souhrn zákonů, jimiž jsou provedeny změny v zákoně č. 227/2000 Sb.

zákona č. 226/2002 Sb.

Upravuje předchozí zákon o rozšíření definice v § 11 o požadavek na údaje, které musí obsahovat kvalifikovaný certifikát používaný v oblasti orgánů veřejné moci.

zákona č. 517/2002 Sb.

Provedeny změny v soustavě orgánů státní správy (zřízení Ministerstva informatiky) a určité změny v názvosloví.

zákona č. 440/2004 Sb.

Upravuje vymezení pojmů v § 2, rozšiřuje o § 3a, definuje použití kvalifikované značky založené na kvalifikovaném systémovém certifikátu, mění povinnosti označující osoby, držitele certifikátu a kvalifikovaného poskytovatele certifikačních služeb. Dále se upravují a rozšiřují podmínky pro náležitosti jednotlivých certifikátů a značek, kvalifikovaného časového razítka, prostředky pro vytváření, správní delikty, přestupky aj.

3.2 Další normy

Nařízení vlády č.304/2001 Sb. ze dne 25.7.2001

Tímto nařízením je prováděn zákon č. 227/2000 Sb., speciálně povinnost orgánů veřejné správy přijímat podání v elektronické formě. Funkcionalita je zajištěna vznikem elektronických podatelen, pověřením zaměstnance úřadu, který je vybaven vlastním kvalifikovaným certifikátem, který obsahuje náležitosti stanovené zákonem a který zabezpečuje příjem a odesílání, přičemž práce v podatelně musí být organizována tak, aby byla zaručena neprodlená kontrola všech náležitostí zprávy (čitelnost, platný a zaručený kvalifikovaný certifikát, aj.).

Vyhláška Úřadu pro ochranu osobních údajů č.366/2001 Sb. ze dne 3.10.2001

„upřesňuje podmínky stanovené v § 2 a 17 o elektronickém podpisu a způsob, jakým se jejich splnění bude dokládat, a požadavky, které musí splňovat nástroje elektronického podpisu, a náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.“

Nařízení vlády č. 495/2004 Sb. ze dne 25.srpna 2004

Rozšiřuje to, co již bylo zmíněno v Nařízení vlády č.304/2001 Sb. Obsahuje souhrn pravidel pro provoz elektronických podatelen, zveřejňování oznámení a informací na úřední desce.

Vyhláška č. 496/2004 Sb. ze dne 29.července 2004 o elektronických podatelnách

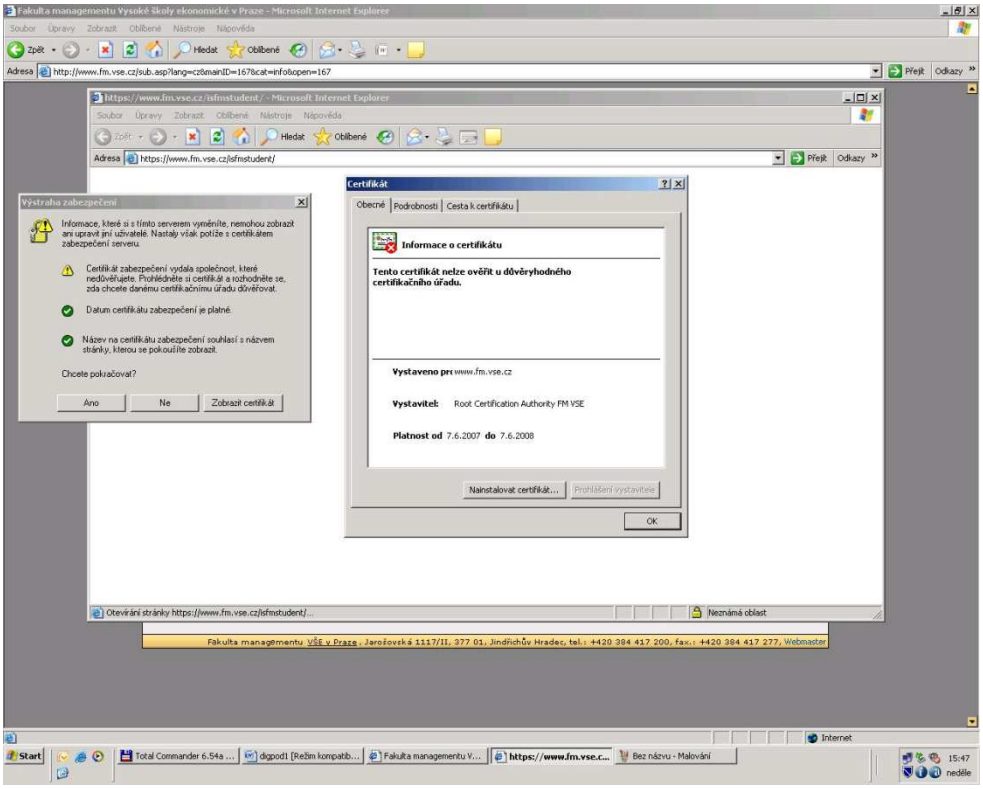
Navazuje na Nařízení vlády č. 495/2004 Sb. a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády. Detailně popisuje proces přijmutí datové zprávy a postup k jednoznačné identifikaci odesílajícího. Dále je popsán postup jak postupovat v případě, kdy zpráva vyhovuje požadavkům zákona. Jako další požadavky jsou uvedeny způsob evidence, potvrzení zprávy a záloha odeslaných zpráv.

Zákon č. 110/2007 Sb.

Předmětem tohoto zákona je zrušení Ministerstva informatiky a přechod pod Ministerstvo vnitra a návazných změn, které se zrušením souvisejí. [5], [6], [15], [16]

4 Využití na Fakultě managementu VŠE

První využití, které bych rád zmínil je vzdálený přístup po internetu do aplikací. Zabezpečená komunikace přes https je využita pro osobní zabezpečené stránky, webmail, menza, rozvrhy, www aplikace klokan, e-learningový systém Moodle, diskusní fórum KAPR a dále přístupy na servery jako např. teta a gama. Principy této zabezpečené komunikace byly popsány v předchozí kapitole, a proto se jim již nebudeme věnovat. Další využití je zabezpečený přístupu do WiFi sítě provozované v prostorách budov školy. Dále bych zmínil Certifikační autoritu Vysoké školy ekonomické, která vydává serverové certifikáty třídy 2. [24]



Obrázek 4-1 Zabezpečený přístup na aplikace školy [24]

4.1 Návrh dalšího využití

Možné využité digitálního podpisu na škole bych rozdělil do následujících kapitol

- Identifikace školy
- Identifikace učitele
- Identifikace studenta
- Zabezpečení proti změně a utajení dokumentů

4.1.1 Identifikace školy

Škola by pro určitý druh komunikace směrem ven využívala digitálního podpisu a tím by zajistila nepopiratelnost autorství zprávy. Využití by poté našlo např. při distribuci výsledků přijímacího řízení. Automatizovaný systém, který by na základě digitalizace testu a s možností využití čárového kódu pro identifikaci studenta automaticky vyhodnotil přijímací řízení jako celek a následně systém rozeslal rozhodnutí elektronicky, ale opatřený elektronickou značkou. Škola by musela vlastnit systémový certifikát. Přínosem by bylo výrazné zjednodušení a zlevnění agendy spojené s přijímacím řízením.

Dle informací na webových stránkách by měl být nahrazen v blízké budoucnosti informační systém fakulty celoškolským Integrovaným Studijním Informačním Systémem (ISIS). Komunikace bude opět zabezpečena přes https. Certifikační autoritou pro ověření je CA VŠE. V současné době systém neumí generovat elektronické dokumenty ověřené digitálním certifikátem či razítkem (např. index nebo výsledek přijímacího řízení). V současnosti není ani možnost následně tisknutelných elektronických podpisů. [3], [12], [24], [27], [28]

4.1.2 Identifikace učitele

Navrhoval bych využívat podpis při přístupu do všech systému spojených s vedením agendy o studentech. Toto řešení by časem mohl vyústit v čistě elektronickou agendu bez použití papíru a nutnosti jeho archivace. Systém by tak byl zabezpečen proti neautorizovanému přístupu. Otázku by pak představovalo volbu uložení certifikátu a jeho zneužití. [12], [27]

4.1.3 Identifikace studenta

Dnes je využívána čipová karta s funkcí peněženky pro kopírování. Záměrem do budoucna je možnost rozšíření o ukládání certifikátu. [24]

4.1.4 Zabezpečení proti změně a utajení dokumentů

Ani u této kapitoly se nerýsuje úplně jasné využití. V první řadě si kladu otázku, jaká data by musela být takto zabezpečována. Při kontrole svojí školní emailové adresy mne nenapadá, které zprávy by bylo nutné šifrovat stejně tak spousta dalších dat která jsou k dispozici přes různé webové aplikace. Výjimku zde asi tvoří osobní data uchovávaná školou. Poněkud více by se nám odpověď rozkryla, pokud bychom připustili existenci výše

navrhovaného čistě elektronického vedení veškeré školní agendy. V tomto případě by určité způsoby komunikace a uložení dat bylo vhodné zabezpečit. Např. záznamy vytvořené učitelem, by byly opatřeny digitálním podpisem s časovým razítkem, tím by se zabránilo pozdějšímu pozměnění. Podobných příkladů bychom mohli určitě uvést i více. [3], [13], [14], [27]

Závěr

V této práci jsem se pokusil zmapovat situaci ohledně požívání digitálních certifikátů a elektronických razítek jak po právní tak po praktické stránce. V závěru práce jsem nastínil možnosti využití v rámci naší školy.

Digitální podpis má širší vazby na elektronické podatelny, ochranu osobních údajů, informační systémy státní správy, požadavky na autorizované poskytovatele certifikačních služeb a další. Ke každé této oblasti se vztahuje řada zákonu a vyhlášek, provádějící tyto zákony, a pak pochopení veškerých vazeb znamená hledat jednotlivé fragmenty v těchto zákonech. Odstup některých zákonů nebyl nejkratší. Časové razítko a systémové certifikáty mohly být doopravdy do zákonu implementovány rychleji. Jádro problému, pokud to tak můžeme nazývat, bych viděl někde jinde. [16]

„Dětskými nemocemi“ si prošlo asi každé zavádění nových systémů, které logicky vyvolává odpor lidí, kteří se musí učit novým věcem. Rezervovaný přístupu byl námětem mnoha článku v letech 2003. Mnohem významnější dopad měl nedostatek vhodných aplikací k použití. V prvopočátku se určitě nejednalo o nejjednodušší proceduru, kterou musel žadatel absolvovat a k výraznému zjednodušení tak nedocházelo. Elektronický podpis byl výsadou zkušenějších uživatelů. Průměrní uživatelé asi trochu tápali a zavedení na první pokus nezvládli.

Na jednu jedinou problematiku jsem v žádném článku nenarazil (ovšem nevylučuji výskyt) a to je podíl domácností připojených k internetu. Ani v nejmenším diskutující nepovažovali za důležité tuto otázku rozpracovat. Jak mohli využívat uživatele internetu digitální podpis v začátcích implementace? Odpověď zní špatně. Zkusme se na chvíli vrátit o několik roků nazpět. Jen pro zajímavost, podle odhadu OECD bylo v červenci 1997 napojeno v ČR necelých 5 počítačů do internetu na 1000 obyvatel oproti cca 50 počítačů v severských zemích (http://www.nw.com/). Novější data pocházejí z dubna 2008 a ze statistik vyplývá 32 procent domácností připojených k internetu. Dle mého názoru tak autoři článků prostě zapomněli na fakt, že uživatele neměli odkud využívat služeb digitálního podpisu. Na závěr si dovolím malou poznámku – ADSL k nám přichází kolem roku 2002 a jen stěží bych službu 192/64 kbps nazval širokopásmovou a to již nemluvím o cenách. [12], [13], [27]

Nepochybně rozvoj poznamenalo i slabé konkurenční prostředí v počátcích poskytování služeb autorizovaných certifikačních autorit. Tato situace se zlepšila rozšířením počtu z jedné na současné tři. Určitě můžeme směle prohlásit, že za největším rozmachem

stojí rozvoj aplikací na straně státní správy. Dnes můžeme v podstatě většinu daní platit elektronicky. Zkušenější občané zpracují svoje daně v různých programech a odešlou podepsané na úřad. Ještě většího významu toto nabývá u právnických subjektů, kde tato agenda zaměstnává mnoho lidí a techniky. Firmám dnes již postačí vést daňovou a účetní dokumentaci v elektronické formě. Asi ne všichni z nás dovedou docenit tento benefit. Počínaje úsporou času, materiálu a lidské práce a lepší konkurenceschopností konče. Dalším impulzem pro rozvoj bude e-government, jehož součástí je Czech Point, e-podatelny, e-justice a další. Celý proces se nese v duchu rozvoje komunikační infrastruktury veřejné správy, digitalizaci a položení základu rovnosti elektronické a písemné komunikace. Hlavním rysem by mělo být zjednodušení komunikace občanů a firem s veřejnou zprávou. Tento boj nebude jednoduchý a výsledkem může být všeobecný přínos spočívající v optimalizaci úředních rozhodnutí, vedoucí v konečném důsledku k rychlejším, spolehlivějším a levnějším procesům anebo „černá díra“, kam zmizí velké množství peněz daňových poplatníku. O tom, že cesta bude nelehká a trnitá, vypovídá i vývoj okolo Czech Pointu a jeho zabezpečení. Podle všech dostupných indicii je zabezpečení vázáno pouze na uživatelské jméno a heslo, nepředstavující veliké zabezpečení. [28], [27], [14]

Dalším tahounem rozvoje používaní digitálního certifikátu jsou komerční aplikace. Dle mého názoru můžeme být s touto oblastí plně spokojeni. Rozvoj aplikací internetového bankovnictví, webových obchodů a intranetů je uspokojující. Docela dobře si dnes dovedu představit rozvoj v oblasti dodavatelsko-odběratelských vztahů. Kde budou jednotlivé aplikace komunikovat mezi sebou a zasílat si elektronické faktury digitálně podepsané pomocí systémových certifikátů. Firmy budou přistupovat navzájem do svých informačních systémů pomocí zabezpečené komunikace a optimalizovat toky materiálu. I tady nás tak může potkat podobná zkušenost jako s mobilními telefony, bez kterých si dnes již nedovedeme život představit. [3]

Seznam zkratek

TS	– time stamp
TSA	– time stamping authority
HDD	– hard disk drive
RSA	– Rivest-Shamir-Adleman
CRL	– certificate revocation list
USB	– Universal Serial Bus
PGP	– Pretty Good Privacy
SHA1	– Secure Hash Algorithm
MD2	– Message Digest Algorithm 2
I.CA	– První certifikační autorita
ACAeID	– Akreditovaná certifikační autorita eIdentity
XML	– eXtensible Markup Language
http	– Hypertext Transfer Protocol
HTTPS	– Hypertext Transfer Protocol over Secure Socket Layer
SSL	– Secure Sockets Layer
TSL	– Transport Layer Security
PIN	– Personal Identification Number
PUK	– Personal Unblocking Key
WiFi	– Wireless Fidelity
ISIS	– Integrovaný Studijní Informační Systéme
RELDP	– Roční evidenční list důchodového pojištění
MPSVČR	– Ministerstvo práce a sociálních věcí České republiky
MIČR	– Ministerstvo informatiky České republiky
MVČR	– Ministerstvo vnitra České republiky
ADSL	– Asymetric Digital Subscriber Line
ČR	– Česká republika
DPH	– daň z přidané hodnoty
PDF	– Portable Document Format

Literatura

[1] DOSEDĚL,T.: *Počítačová bezpečnost a ochrana dat*, Computer Press, Brno, 2004

[2] VONDRUŠKA,P.: *Kryptologie, šifrování a tajná písma*, Albatros, edice: OKO Brno, 2006

[3] SMEJKAL, V., BUDIŠ, P., KODL, J., MATES, P.: *Digitální podpis od A do Z*, Grada, Praha 2005. ISBN 80-247-0555-9

[4] PŘIBYL, J.: *Informační bezpečnost a utajování zpráv*, ČVUT, FEL vydavatelství ČVUT, Praha 2004

[5] BOSÁKOVÁ, D. A KOL.: *Elektronický podpis*, Grada, Praha 2002

Webové odkazy

[6] První certifikační autorita, a.s. (I.CA), http://www.ica.cz/home_cs/, [on line], cit: 2006

[7] Certifikační autorita PostSignum, http://www.postsignum.cz/ , [on line], cit: 2007

[8] eIdentity a.s., https://www.eidentity.cz/app [on line], cit: 2008

[9] Certifikační autorita Czechia, s.r.o., http://www.caczechia.cz/default.asp?init=0 , [on line], cit: 2004

[10] Certifikační autorita TrustPort, http://www.trustcert.cz/ , [on line], cit: 2007

[11] Pravdy o elektronickém podpisu a šifrování, http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=244&clanekID=245, [on line], cit: 2003

[12] Zoner software, s.r.o., http://interval.cz/e-komerce, [on line], cit: 2002, 2003, 2004

[13] Jiří Peterka – archiv článků a přednášek, http://www.earchiv.cz, [on line], cit: 2002, 2003, 2005

[14] Informační systémy veřejné správy, http://www.isvs.cz, [on line]

[15] Ministerstvo informatiky ČR, http://www.micr.cz, [on line], cit: 2005

[16] Ministerstvo vnitra ČR, http://www.mvcr.cz, [on line], cit: 2007

[17] Ministerstvo financi ČR, http://www.mfcr.cz, [on line], cit: 2008

[18] Vícha, K., E-podpis za lidovku?, http://interval.cz/clanky/e-podpis-za-lidovku/, [on line], cit: 2004

[19] Portál veřejné správy, http://portal.gov.cz/wps/portal/_s.155/6966/place, [on line], cit: 2008

[20] Co je to aplikace Elektronická podání?, http://www.microsoft.com/cze/government/epodani.mspx, [on line], cit: 29. září 2003

[21] Elektronická podání na Portálu veřejné správy využívá už 50 000 uživatelů, http://www.microsoft.com/cze/casestudies/micr_50000.mspx, [on line], cit:27.září 2006

[22] Česká správa sociálního zabezpečení, http://www.cssz.cz/cz/novinky/, [on line], cit: 2008

[23] Ministerstvo práce a sociálních věcí, http://www.mpsv.cz/cs/, [on line], cit: 2008

[24] Fakulta managementu VŠE, http://www.fm.vse.cz/, [on line], cit: 2008

[25] Wikipedie, otevřená encyklopedie, http://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana, [on line], cit: 2008

[26] ASKON INTERNATIONAL s.r.o., produkty, http://www.askon.cz/index.php?YVdSZlpHOWpkVzFsYm5ROU1UZzFNZz09, [on line], cit: 2008

[27] Lupa – server o českém internetu, http://www.lupa.cz, [on line]

[28] Hospodářské noviny, http://hn.ihned.cz/c3-23376020-500000_d-de-civitate-electronica, [on line], cit: 2008

[29] Počítač už má 40 procent domácností, http://www.novinky.cz/clanek/137104-pocitac-uz-ma-40-procent-domacnosti.html, [on line], cit: 8.4.2008

[30] eGovernment nám zjednoduší život, říkají internetoví uživatelé v ČR, http://www.marketingovenoviny.cz/index.php3?Action=View&ARTICLE_ID=5991, [on line], cit: 18.3.2008

[31] ČSOB Internetbanking 24, https://ib24.csob.cz/, [on line], cit: 18.3.2008

[32] Jak zjistit, zda je digitální podpis důvěryhodný, Nápověda a postupy, http://office.microsoft.com/cs-cz/help/HA012308751029.aspx, [on line], cit: 2008

[33] Krejčí, R., Elektronický podpis v Adobe Readeru a Acrobatu 8, Rubrika: PDF - Adobe Acrobat, http://www.grafika.cz/art/pdf/aa8podpis2.html, [on line], cit: 26.03.2007

Seznam obrázků

Seznam tabulek

Seznam grafů

Přílohy

Certifikát pro přístup do aplikace FM VŠE [24]

Verze V3
Seriové číslo 49 19 a8 c7 00 00 00 00 00 2e
Algoritmus sha1RSA
Vystavitel CN = Root Certification Authority FM VSE
DC = fm
DC = vse
DC = cz
Platnost od 7. června 2007 10:26:55
Platnost do 7. června 2008 10:36:55
Předmět CN = www.fm.vse.cz
OU = Fakulta managementu
O = Vysoka skola ekonomicka
L = Jindrichuv Hradec
S = Czech
C = CZ
Veřejný klíč RSA (1024Bits)
30 81 89 02 81 81 00 c9 fd e4 a6 69 7d 43 ca 01 11 c9 b3 78 8c 0c cb f7 76 68 62 d3 5b 7d f8 8b 26 56 93 bd ca 89 15 fa 85 5b 54 5d 33 0b 4d f9 7a 9f f9 37 ff 01 d5 69 cb d8 47 56 20 64 df b4 5f 83 4e d5 11 43 af db a5 0f 8d cb 3a 3f 1d 1a 4c 30 83 94 d1 3a c9 9e 07 d3 b4 9d 11 de 93 ad 44 51 06 c9 25 cf c2 bd 43 fd 06 9f 5d 8e af a3 ae 7a f8 3f 4a 47 5f de 7d 4f 49 03 82 61 e1 5a 7f 30 46 b8 18 06 c5 02 03 01 00 01
Schopnost protokolu SMIME [1]Podpora formátu SMIME
ID objektu=1.2.840.113549.3.2
Parametry=02 02 00 80
[2]Podpora formátu SMIME
ID objektu=1.2.840.113549.3.4
Parametry=02 02 00 80
[3]Podpora formátu SMIME
ID objektu=1.3.14.3.2.7
[4]Podpora formátu SMIME
ID objektu=1.2.840.113549.3.7
Použití rozšířeného klíče Ověření serveru (1.3.6.1.5.5.7.3.1)
Identifikátor klíče předmětu 9a 1d 9f 5d 71 48 fd 62 ed fa 29 2f ab fb ee f7 10 01 9d ad
Identifikátor klíče úřadu ID klíče=80 4d 6f 92 8e a7 12 01 24 59 7c 35 ae 50 da 53 60 06 da 27
Distribuční místa seznamu odvolaných certifikátů
[1]Distribuční místo CRL
Název distribučního místa:
Jméno a příjmení:
URL=http://deneb.fm.vse.cz/CertEnroll/Root%20Certification%20Authority%20FM%20VSE.crl
URL=file://\\DENEB.fm.vse.cz\CertEnroll\Root Certification Authority FM VSE.crl
Přístup k informacím úřadu
[1]Přístup k informacím úřadu
Přístupová metoda=Vystavitel certifikátu úřadu(1.3.6.1.5.5.7.48.2)
Alternativní název:

URL=http://deneb.fm.vse.cz/CertEnroll/DENEB.fm.vse.cz_Root%20Certification%20Authority%20FM%20VSE.crt
[2]Přístup k informacím úřadu
Přístupová metoda=Vystavitel certifikátu úřadu(1.3.6.1.5.5.7.48.2)
Alternativní název:
URL=file://\\DENEB.fm.vse.cz\CertEnroll\DENEB.fm.vse.cz_Root Certification Authority FM VSE.crt
Požití klíče Digitální podpis, Neodvolatelnost, Zakódování klíče, Zakódování dat (f0)
Algoritmus miniatury sha1
Miniatura 41 00 5b 9a bb 8a 27 5c 87 65 e9 ba a8 7b 8f 24 99 07 01 fa