

VYSOKÁ ŠKOLA EKONOMICKÁ

Fakulta informatiky a statistiky

Katedra systémovej analýzy

Názov bakalárskej práce:

ZÁKON O ELEKTRONICKÉM PODPISE V ČR A FR

2006

Vypracoval: Juraj Slota

Vedúci bakalárskej práce: Doc. Ing. Prokop Toman, CSc.

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne, len s odborným vedením vedúceho bakalárskej práce Doc. Ing. Prokopom Tomanom, Csc.

Ďalej prehlasujem, že všetky podklady, z ktorých som čerpal, sú uvedené v zozname použitých zdrojov.

V Prahe, dňa 15.12.2006

.....
podpis

Pod'akovanie

Rád by som týmto pod'akovalu pánovi Doc. Ing. Prokopovi Tomanovi, Csc. za užitočné rady a trpezlivosť pri vedení celej práce. Ďalej by som chcel pod'akovať slečne Vierke Geckovej za cenné pripomienky a podporu.

Exekutívne zhrnutie

Elektronický podpis, ktorý dnes funguje takmer výlučne na základe asymetrického šifrovania, nachádza využitie v mnohých oblastiach života firiem i jednotlivcov a jeho plné využitie si vyžiadalo adekvátnu právnu úpravu. Táto bakalárska práca má za cieľ porovnať legislatívu elektronického podpisovania a jej prenesenie do praktických aplikácií eGovernmentu v oboch krajinách.

Zákony o elektronickom podpise ČR aj Francúzska sú založené na Smernici EÚ z roku 1999, ktorej primárnym cieľom bolo vytvoriť európsky rámec pre používanie elektronických podpisov, umožňujúc voľný tok produktov a služieb, spolu so základným uznaním elektronických podpisov v celej EÚ. Zavádza presnú terminológiu, ale zostáva technologicky neutrálna a zabezpečuje tak svoju nadčasovú platnosť.

Hlavné rozdiely medzi Českou a Francúzskou legislatívou spočívajú v odlišnosti mechanizmov akreditácie certifikačných autorít (Francúzsko má tri hierarchické stupne, ČR dva) a vo vyžadovaní kvalifikovaných certifikátov pri komunikácii s aplikáciami verejnej správy. Český zákon takýto certifikát vyžaduje, francúzsky to vyslovene neprikazuje.

Hlavný prínos tejto práce okrem zhodnotenia rozdielov v legislatíve spočíva v porovnaní sofistikovanosti služieb eGovernmentu jednotlivých krajín. Toho je dosiahnuté použitím kategorizácie a metodológie schválenej EÚ, ktoré pracujú s 20 typmi služieb a 4. úrovňami sofistikovanosti podľa intenzity interakcie užívateľa a aplikácie.

V službách fyzickým osobám ČR za Francúzskom výrazne zaostáva (56% vs. 86%), kým služby firmám sú na takmer rovako vysokej úrovni (87% a 90%). Využitie týchto služieb je oveľa intenzívnejšie vo Francúzsku (75% užívateľov Internetu) než v ČR (15,5%).

Napriek rastúcej obľube týchto služieb, cenovej dostupnosti kvalifikovaných certifikátov a právnej istoty týkajúcej sa použitia elektronického podpisu, stoja v ceste ďalšieho rozširovania eGovernmentu problémy s užívateľským rozhraním, strachom z úniku informácií a preferenciou osobného kontaktu.

OBSAH

Exekutívne zhrnutie	4
OBSAH	5
1. Úvod	6
1.1. Princíp fungovania elektronického podpisu	7
1.1.1. Asymetrické šifrovanie	7
1.1.2. Princíp elektronického podpisu	8
1.1.3. Certifikát	9
1.1.4. Certifikačná autorita	9
1.1.5. Zhrnutie	9
1.2. Možnosti využitia elektronického podpisu	9
1.2.1. „Obyčajný“ elektronický podpis	10
1.2.2. Kvalifikovaný elektronický podpis	10
1.2.3. Elektronické značky	12
1.2.4. Časové pečiatky	12
2. Legislatíva elektronického podpisu	13
2.1. Smernica EÚ ako východisko zákonov o elektronickom podpise	13
2.1.1. Kľúčové pojmy	14
2.1.2. Prístup na trh	16
2.1.3. Právne účinky elektronických podpisov	16
2.1.4. Medzinárodné hľadisko	17
2.1.5. Rozhodnutie 2000/709/ES	18
2.1.6. Rozhodnutie 2003/511/ES	18
2.1.7. Zhrnutie	19
2.2. Zákon o elektronickom podpise v ČR	19
2.2.1. Zákon č 227/2000 Zb.	20
2.2.2. Vyhláška a nariadenie vlády o elektronických podateľniach	23
2.2.3. Vyhláška 378 z 19.7.2006 o postupoch kvalifikovaných PCS	23
2.2.4. Zhrnutie	24
2.3. Zákon o elektronickom podpise vo Francúzsku	24
2.3.1. Politický systém Francúzska	25
2.3.2. Zákon 2000-230 z 13 marca 2000	25
2.3.3. Dekrét č. 2001-272 z 30.3.2001	26
2.3.4. Dekrét 2002-535 z 18.4.2002	27
2.3.5. Uznesenie z 26.7.2004	27
2.3.6. Zákon 2004-575 z 21.6.2004	30
2.3.7. Zákon 2004-801 z 6.8.2004	30
2.3.8. Ďalšie dôležité texty	31
2.3.9. Zhrnutie	31
2.4. Porovnanie legislatívy	31
3. Využitie elektronického podpisu pre eGovernment	34
3.1. Elektronický podpis pri komunikácii s orgánmi štátnej moci v ČR	34
3.1.1. Portál zdravotných poisťovní	34
3.1.2. Portál verejnej správy	34
3.1.3. Služby Ministerstva financií - Daňový portál	35
3.1.4. Služby Ministerstva Informatiky	37
3.1.5. Služby Českej správy sociálneho zabezpečenia	37
3.1.6. Služby Generálneho riaditeľstva ciel	39
3.1.7. Služby Ministerstva vnútra	39
3.1.8. Prijatie a spokojnosť so službami	39
3.1.9. Zhrnutie	40

3.2. Využitie elektronického podpisu pri komunikácii s orgánmi štátnej správy vo Francúzsku	40
3.2.1. Počiatky informatizácie Francúzskej spoločnosti	41
3.2.2. Projekt ADELE	41
3.2.3. Dostupné služby Francúzskeho e-Governmentu	42
3.2.4. Prijatie a spokojnosť so službami	44
3.2.5. Zhrnutie	45
3.3. Porovnanie dostupných služieb	45
3.3.1. Dostupnosť kvalifikovaných certifikátov	46
3.3.2. Metodológia	46
3.3.3. Zhodnotenie služieb vo Francúzsku	47
3.3.4. Zhodnotenie služieb v Českej Republike	49
3.4. Porovnanie a zhrnutie	50
4. Záver	52
5. Zoznam použitej literatúry	56
6. Zoznam tabuliek a grafov	60
7. Príloha – Smernica EÚ o elektronickom podpise	61

1. Úvod

K problematike elektronického podpisu som sa dostal okľukou, keď som sa začiatkom štúdia na VŠE začal zaujímať, prečo nič nejde vybaviť cez email. Nielen školská agenda, ale aj vybavenie prechodného pobytu, zriadenie účtu, všetko vyžadovalo aby som bol v správny čas na správnom mieste a hlavne so správnymi formulármi. Keď som potom pri výbere bakalárskej práce natrafil na túto tému, bolo rozhodnuté.

Nebolo tomu tak dávno, keď bol papier jedinou možnosťou, ako zachytiť obsah úradného dokumentu. Dnes, v dobe všadeprítomných na Internet pripojených počítačov je ale používanie písomnej formy dokumentov prinajmenšom zastaralé. Spôsobuje to ťažkosti nielen bežnému človeku – napríklad večné vystávanie vo frontách a závislosť na úradných hodinách, ale aj inštitúciám ktoré sú na takúto formu komunikácie odkázané – potreba ručne spracovať obrovské množstvo dokumentov, archivovať ich a vyhľadávať v nich informácie[SME01].

Preto všade na svete prebieha postupný prechod od papierových dokumentov k elektronickým, a všade na svete nastáva problém zrovnoprávnenia týchto foriem z hľadiska zákona. Niektoré právne poriadky svojim výkladom nezakazujú v podstate žiadny nosič informácií – vo svete financií sú známe prípady kedy banka musela preplatiť šek napísaný farbou na chrbte hovädzieho dobytku. Ale v iných, špeciálne

európskych podmienkach kde prevláda tzv. pozitivistický prístup¹, je potrebné aby technologické možnosti boli podložené právnou úpravou[SME01].

Účelom tejto práce je porovnať a zhodnotiť legislatívny rámec upravujúci elektronické podpisovanie v Českej a Francúzskej republike. Keďže na základe svojho predošlého záujmu o problematiku predpokladám, že sa zákony budú vo veľkej miere podobáť (a teda prínos práce by bol minimálny), rozhodol som sa zhodnotiť, ako sú na tom jednotlivé krajiny so zavádzaním elektronického podpisu do praxe. Táto téma je dosť obširná, preto som zúžil zameranie na služby poskytované samotnými štátmi – tzv. eGovernment. Úvodná časť sa bude zaoberať princípom, na ktorých je elektronický podpis založený a možnostiam jeho využitia. Ďalšie časti potom porovnajú legislatívu a úroveň služieb eGovernmentu v jednotlivých krajinách.

1.1. Princíp fungovania elektronického podpisu

Pre správne pochopenie nasledujúceho textu je užitočné ozrejmiť si princíp, na ktorom je systém elektronického podpisovania postavený. Medzi hlavné pojmy, ktoré je treba pochopiť, patrí tzv. „kľúčový pár“. Jedná sa o terminológiu pochádzajúcu z domény kryptografie, kde sa pojmom „kľúč“ označujú dáta používané pre šifrovanie a dešifrovanie správ. Pri šifrovaní obsahu odosielateľ použije jedinečný kľúč a správu tak zakóduje. Takto utajený obsah je možné odomknúť len pomocou toho istého kľúča – tento spôsob šifrovania sa nazýva symetrický. Symetrické šifrovanie je pre potreby elektronického podpisovania nevhodné z dvoch dôvodov: vyžaduje veľké množstvo kľúčov² a bezpečné doručenie kľúča adresátovi je prinajmenšom problematické. Spomenuté problémy vyriešila technológia asymetrického šifrovania, ktorá sa výborne hodí pre potreby elektronického podpisovania.

1.1.1. Asymetrické šifrovanie

Pri asymetrickom šifrovaní sa používa nie jeden, ale dva kľúče: verejný a súkromný. Obrazne sa dajú opísať ako zámka a jej kľúč. Každý, kto chce aby s ním bolo možné šifrovať komunikáciu, dá verejnosti k dispozícii svoje zámky. Človek, ktorý bude chcieť inej osobe poslať zakódovanú správu,

¹ Platí len to, čo je výslovne uvedené v zákone

² Každá dvojica ľudí by musela mať svoj vlastný kľúč

ju uzamkne pomocou adresátovej zámky. Tak si môže byť istý, že sa správa nedostane do nepovolaných rúk, pretože kľúčom k odomknutiu zámky disponuje iba adresát.

1.1.2. Princíp elektronického podpisu

Elektronické podpisovanie funguje na presne opačnom princípe. Tu už nejde o to, aby správa bola zašifrovaná, ale o istotu, že podpísaná správa skutočne pochádza od odosielateľa a že nebol počas prenosu zmenený jej obsah. Odosielateľ teda pomocou súkromného kľúča a špeciálneho softvéru zašifruje text ktorý chce poslať a výsledok pripojí k správe. Táto príloha sa nazýva elektronický podpis. Prijemca si na základe podpisu overí identitu odosielateľa u certifikačnej autority a získa od nej jeho verejný kľúč. Jeho pomocou dešifruje elektronický podpis, čím získa pôvodný text, ktorý potom porovná s otvoreným textom. Ak sa zhodujú, potvrdí sa totožnosť podpísanej osoby³ a pôvodnosť textu.

Ďalší rozdiel oproti šifrovaniu spočíva v tom, že pomocou súkromného kľúča sa nekóduje celý text správy, ale len jeho „otlačok“, vytvorený hašovacou funkciou. Tým sa dosiahne markantné zrýchlenie, pretože algoritmy používané pre asymetrické šifrovanie sú 100 až 10000 krát pomalšie ako pri symetrickom šifrovaní⁴. Otlacky dokumentu sú pritom dostatočne jednoznačným identifikátorom a prakticky nie je možné aby dva dokumenty mali rovnaký odtlačok.

Namiesto celého textu sa teda pomocou súkromného kľúča zakóduje len odtlačok a výsledok sa pripojí k správe. Prijemca si pre účel overenia spraví odtlačok doručeného dokumentu, a porovná ho s dešifrovaným odtlačkom. Zhoda otlakov zaručí identitu odosielateľa (len správny verejný kľúč vytvorí identický odtlačok) a overí, že dokument nebol zmenený (aj malá zmena by znamenala veľký rozdiel v odtlačku). [HASO01]

³ Len ten, kto pozná súkromný kľúč spojený s daným verejným kľúčom dokáže vyrobiť daný podpis

⁴ Pre podrobnejší výklad o hašovacích funkciách a šifrovacích algorytmoch viz. napr. [HASO01]

1.1.3. Certifikát

Certifikátom rozumieme elektronický dokument podpísaný dôveryhodnou treťou stranou. Táto zaručuje, že verejný kľúč spojený s certifikátom naozaj patrí tomu, kto je označený ako jeho vlastník. Certifikát je verejný a môže ním disponovať každý, s kým hodlá dotýčný komunikovať pomocou zaručeného elektronického podpisu⁵. Obvykle sa pripája k posielanej správe spolu s elektronickým podpisom.

1.1.4. Certifikačná autorita

Certifikačná autorita hrá v systéme elektronického podpisu dôležitú rolu – je dôveryhodnou treťou stranou spomenutou v predchádzajúcej časti. Pôsobí totiž ako garant totožnosti podpisovateľa, čím zabezpečuje dôveryhodnosť celého systému. Zaoberá sa vydávaním certifikátov, ktorými odosielateľ dokazuje svoju identitu. Bez dôveryhodnej certifikačnej autority by si príjemca nemohol, a nemal byť istý, že podpísaná správa skutočne pochádza od osoby uvedenej v podpise. Z dôvodu veľkej zodpovednosti za fungovanie systému sú na certifikačné autority kladené prísne nároky, ktoré vyplývajú zo zákona a súvisiacich predpisov⁶.

1.1.5. Zhrnutie

Elektronický podpis je teda súbor dát vytvorených pomocou špeciálneho softvéru⁷ za použitia súkromného kľúča a odtlačku zasielanej správy. K tejto správe sa pripojí spolu s certifikátom vydaným dôveryhodnou certifikačnou autoritou. Pomocou verejného kľúča spojeného s certifikátom si príjemca môže overiť, že správu skutočne odoslala podpísaná osoba a že obsah správy nebol od jej podpisania zmenený.

1.2. Možnosti využitia elektronického podpisu

Prečo je vôbec zákon o elektronickom podpise potrebný, ak si podľa zákona môžeme zmluvne zjednať elektronický spôsob podpisovania? Podľa p. docenta Smejkalu je pomocou takéhoto zákona lepšie riešiť napríklad otázky zodpovednosti a náhrady

⁵ Môže existovať viacero certifikátov, ak má osoba viacero kľúčov pre rôzne použitie: ako súkromná osoba, ako člen predstavenstva firmy, ako člen záujmového spolku atď.

⁶ Vid'. nasledujúce časti práce

⁷ Alebo hardvéru

škôd. Tento zákon taktiež vytvára systém dohľadu nad certifikačnými autoritami a tým prispieva k zlepšeniu bezpečnosti používania elektronického podpisu. Navyiac uvádza, že do nadobnutia platnosti zákona o elektronicko podpise nebolo možné naplniť literu zákona v prípadoch, kde obecné právne normy hovoria „*písomne*“ a „*podpísané*“.

Potrebuje ho taktiež pre verejnoprávnu sféru, pretože štát a jeho orgány môžu robiť len to, čo im zákon povoľuje. Zákon o elektronickom podpise teda povoľuje orgánom verejnej moci zaviesť elektronickú komunikáciu ako alternatívu ku klasickej písomnej.

Táto kapitola popíše možné využitie elektronického podpisovania a výhody ktoré poskytuje fyzickým aj právnickým osobám, v podnikateľskej aj verejnoprávnej sfére.

1.2.1. „Obyčajný“ elektronický podpis

S obyčajným elektronickým podpisom sa môžeme dnes stretnúť napríklad v bankách pri porovnávaní podpisu na papieri s podpisovým vzorom, ktorý je oskenovaný a uložený v systéme banky. Toto porovnanie je ale len vizuálne a teda čisto subjektívne - podpis záleží od momentálneho stavu podpisujúceho a odhalenie podvrhu záleží len na schopnostiach bankového pracovníka. Medzi obyčajné elektronické podpisy patria aj iné spôsoby pripojenia určitej identifikácie k prenášanej správe – napríklad heslo alebo otlačok prstu. Tieto spôsoby ale nespájajú tajnú informáciu alebo biometrický znak s obsahom správy a tak je možné obyčajný elektronický podpis zneužiť⁸. Podľa definície takýto postup síce „umožňuje overenie totožnosti“, ale na druhej strane vlastne nič nezaručuje. Široké nasadenie obyčajného elektronického podpisu sa preto neočakáva, jeho existencia v zákone vyplýva zo smernice EÚ, ktorá je sama dielom viacerých medzinárodných kompromisov[SME01].

1.2.2. Kvalifikovaný elektronický podpis

Elektronický podpis sa dá využiť všade tam, kde bol donedávna nutný vlastnoručný podpis. Všetky dokumenty je možné previesť z papierovej do elektronickej podoby, takisto sa dajú previesť všetky podpisy. Okrem zrýchlenia a zefektívnenia podpisovania a overovania podpisov elektronický podpis prináša možnosť

⁸ Napríklad kopírovaním, odpočúvaním, vstupom medzi odosielateľ a príjemcu a pod.

podpísať aj veci, ktoré šlo ručne podpísať len ťažko – obsah datového nosiča, fotografiu, prístup do databáze a podobne[SME01].

Z pohľadu bankovníctva, finančníctva a podnikania vôbec má elektronický podpis široké, ba prevratné možnosti uplatnenia. Jedným z najväčších prínosov je zvýšenie bezpečnosti akýchkoľvek elektronických transakcií, najmä v oblastiach, kde sa zatiaľ elektronickým záznamom príslušné orgány bránili – kvôli ich údajnej manipulovateľnosti. Jedná sa o bankovníctvo a finančníctvo, kde je potreba dobrej dokumentácie všetkých operácií. Elektronický podpis môže vyriešiť dôveryhodnosť internetbankingu a on-line nakupovania[SME01].

Taktiež v zdravotníctve by sa mohol uplatniť elektronický zdravotný spis, opatrený digitálnym podpisom. Takýto spis by pacient mohol nosiť stále so sebou. Každý záznam by bol podpísaný príslušným podpisom (lekára, sestričky...) a odpadla by nutnosť prenosu zdravotných spisov pri zmene lekára. Rovnako je možné, aby každý nosil svoj súkromný kľúč so sebou napríklad v mobilnom telefóne, pre použitie pri každodenných transakciách[SME01].

Elektronický podpis nájde uplatnenie aj v „elektronickej justícii“, kde bude slúžiť na podpisovanie dokumentov (vrátane audio a videonahrávok výsluchov svedkov) prídiacich od polície, štátnych zastupiteľstiev a ďalších inštitúcií k súdom, čo zrýchli prácu súdov a zlepši komunikáciu medzi týmito úradmi, nehovoriac o finančných úsporách.[EPR02]

Pre bežného človeka sa dnes ako najdôležitejší prínos elektronického podpisu javí možnosť on-line komunikácie s orgánmi štátnej správy⁹. Postupne sa tak redukuje časová náročnosť niektorých správnych konaní, napr. obstaranie výpisov z katastru nehnuteľností alebo registru trestov sa za pomoci elektronického podpisu a e-podateľní neporovnateľne skráti. Komunikácii s týmito orgánmi sa podrobnejšie venuje siedma kapitola.

⁹ Jedná sa o kvalifikovaný elektronický podpis vytvorený na základe certifikátu od kvalifikovaného PCS a kvalifikovaným prostriedkom pre tvorbu podpisu

1.2.3. Elektronické značky

Elektronické značky, sú de facto elektronické podpisy vytvorené automaticky bez priameho zásahu človeka. Umožňujú tak podpisovanie veľkého množstva automatizovanej korešpondencie. Jedná sa hlavne o:

- Zasielanie výpisov z rôznych registrov¹⁰
- Zasielanie elektronických „doručení“¹¹
- Hromadnú korešpondenciu

Konkrétnym príkladom použitia elektronických značiek je príklad Deutsche Bank, ktorá sa v rámci boja proti phishingu rozhodla elektronicky podpisovať všetky dátové správy ktoré zasiela klientom.

1.2.4. Časové pečiatky

S používaním elektronického podpisu, resp. elektronických značiek, úzko súvisia elektronické časové pečiatky, pretože elektronický podpis ako taký neobsahuje časové údaje o vytvorení dokumentu ani samotného podpisu. Tieto informácie sú pritom nesmierne dôležité najmä pri overovaní pravosti dokumentu, pri súdnom konaní¹² a pod.

Medzi najčastejšie spôsoby využitia kvalifikovaných časových pečiatok patria[HN01]:

- ochrana logových záznamov v auditných súboroch
- elektronické podania
- notárske služby
- uzatváranie elektronických zmlúv
- on-line obchodovanie
- súdne dokazovanie

¹⁰ Najmä kataster nehnuteľností, obchodný register, trestný register

¹¹ Napr. elektronická podateľňa po prijatí podania automaticky odošle správu o prijatí a prípadných nedostatkoch

¹² Tu je vyžadovaná kvalifikovaná časová pečiatka

2. Legislatíva elektronického podpisu

2.1. *Smernica EÚ ako východisko zákonov o elektronickom podpise*

Po osvojení si základného princípu fungovania a použitia elektronického podpisu je možné pristúpiť k rozboru legislatívneho rámca upravujúceho jeho použitie v Českej a Francúzskej republike. Skôr než sa pozornosť zameria na jednotlivé štáty, je dobré oboznámiť sa s normou z ktorej jednotlivé štátne zákony vychádzajú – smernicou EÚ o zásadách Spoločenstva pre elektronické podpisy (ďalej len „Smernica“)

Problém elektronického podpisovania je vskutku celosvetový, zaoberá sa ním OSN aj Európska Únia. Komisia OSN pre medzinárodné obchodné právo (UNCITRAL) vydala „Vzorový zákon o elektronickom obchode“ a ďalej pracuje na celosvetovej právnej úprave elektronického obchodu, pričom elektronické podpisy sú len časťou týchto úvah. Smernica EÚ č. 1999/93/EC zo dňa 13.12.1999 o zásadách Spoločenstva pre elektronické podpisy, ktorá sa stala východiskom pre zákony o elektronickom podpise v jednotlivých krajinách EÚ, zčasti vychádza práve z tohto vzorového zákona.

Primárnym cieľom direktívy bolo vytvoriť európsky rámec pre používanie elektronických podpisov, umožňujúc voľný tok produktov a služieb, spolu so základným uznaním elektronických podpisov v celej EÚ. Medzi hlavné dôvody pre vypracovanie jednotného európskeho rámca pre elektronickú komunikáciu patrili rozdiely v právnom uznaní elektronického podpisu a v akreditácii overovateľov v jednotlivých členských štátoch. Tieto rozdiely boli vnímané ako prekážka používania elektronickej komunikácie a elektronického obchodu, ktorá zabraňuje voľnému pohybu tovaru a služieb na vnútornom trhu (§4). Voľný trh v EÚ zaisťuje voľný pohyb osôb a z tohto dôvodu občania EÚ stále častejšie jednajú s orgánmi iných členských štátov. Európske orgány v tomto smere považujú dostupnosť elektronickej komunikácie za veľmi užitočnú (§7).

Zo zásad proporcionality a subsidiarity uvedených v článku 5 Zmluvy vyplýva, že jednotlivé členské štáty nemôžu samostatne a dostatočným spôsobom dosiahnuť

vytvorenie harmonizovaného právneho rámca pre poskytovanie elektronických podpisov. Preto je vhodné, aby to bolo dosiahnuté v rámci Spoločenstva (§28).

Iniciatíva únie na poli elektronického podpisu siaha minimálne do roku 1997, kedy Európska Komisia predložila dve oznámenia: „o európskej iniciatíve v oblasti elektronického obchodu“ a „o zaistení bezpečnosti a dôveryhodnosti elektronickej komunikácie – smerovanie k európskym zásadám pre digitálne podpisy a šifrovanie“. Prvého decembra toho istého roku Rada Európy vyzvala Komisiu, aby čo najrýchlejšie predložila návrh smernice Európskeho Parlamentu a Rady o digitálnych podpisoch. O dva roky na to, 13. Decembra 1999, bola prijatá smernica 1999/93/ES určená všetkým členským štátom.

2.1.1. Klíčové pojmy

Dôležitým prínosom bolo, samozrejme okrem zjednotenia právnych predpisov, zavedenie presnej terminológie týkajúcej sa problematiky elektronického podpisovania. Aj keď to nebolo cieľom, termíny použité v smernici boli prebraté nielen v členských štátoch, ale aj v prístupujúcich a dokonca aj mimoeurópskych štátoch. Jedná sa o týchto 13 termínov:

- *"elektronický podpis"* - údaj v elektronickej podobe, ktorý je pripojený či logicky spojený s inými elektronickými dátami a ktorý slúži ako metóda overenia pravosti
- *"zaručený elektronický podpis"¹³* – elektronický podpis, ktorý spĺňa tieto požiadavky:
 - je jednoznačne spojený s podpisujúcou sa osobou
 - umožňuje zistiť totožnosť podpisujúcej sa osoby
 - je vytvorený s využitím prostriedkov, ktoré podpisujúca osoba môže mať úplne pod svojou kontrolou
 - je spojený s dátami, ku ktorým sa vzťahuje tak, aby bolo možné zistiť akúkoľvek následnú zmenu týchto dát

Zaručený elektronický podpis je teda vytvorený oveľa premyslenejšou metódou ako obyčajný elektronický podpis a prináša množstvo funkcií, ktoré sa papierovo nedajú ani nebudú dať dosiahnuť: zaručuje integritu správy, identitu

¹³ V ďalšom texte môže byť tento termín nahradený termínom: „kvalifikovaný elektronický podpis“ alebo skratkou KEP resp. ZEP

odosielateľa a nepopierateľnosť – podpísaná osoba nemôže poprieť že danú správu s daným obsahom vytvorila¹⁴[SME01].

- *"podpisujúca sa osoba"* – akákoľvek osoba, ktorá má prostriedok pre tvorbu podpisu a ktorá jedná na svoj účet alebo na účet fyzickej či právnickej osoby alebo subjektu, ktorý zastupuje;
- *"dáta pre tvorbu podpisu"* –unikátne dáta, ako sú kódy alebo súkromné šifrovacie kľúče, ktoré podpisujúca osoba používa k vytvoreniu elektronického podpisu (ďalej „súkromný kľúč“)
- *"prostriedok pre tvorbu podpisu"* – konfigurovaný softwarový alebo hardwarový prostriedok pre využitie dát pre tvorbu podpisu
- *"prostriedok pre bezpečnú tvorbu podpisu"* – prostriedok pre tvorbu podpisu, ktorý spĺňa požiadavky uvedené v prílohe III
- *"dáta pre overovanie podpisu"* - dáta, ako kódy alebo verejné šifrovacie kľúče, ktoré sa používajú pre overovanie elektronického podpisu (ďalej „verejný kľúč“)
- *"prostriedok pre overovanie podpisu"* – konfigurovaný softwarový alebo hardwarový prostriedok pre využitie dát pre overovanie podpisu
- *"osvedčenie"¹⁵* - elektronické potvrdenie, ktoré spája dáta pre overovanie podpisu s určitou osobou a potvrdzuje totožnosť tejto osoby (certifikát)
- *"kvalifikované osvedčenie"* – osvedčenie, ktoré spĺňa požiadavky uvedené v prílohe I a ktoré vydáva overovateľ, ktorý spĺňa požiadavky uvedené v prílohe II;

Smernica EÚ teda podobne ako pri podpisoch zavádza dva druhy certifikátov: „obyčajný“ a „kvalifikovaný“, pričom záruky vyplývajúce z použitia zaručeného elektronického podpisu platia v plnej miere len pri vystavení kvalifikovaného certifikátu[SME01].

- *"overovateľ"¹⁶* – subjekt alebo právnická či fyzická osoba, ktorá vydáva osvedčenia alebo poskytuje iné služby súvisiace s elektronickými podpismi;

¹⁴ Pokiaľ bude existovať platný certifikát spájajúci túto osobu s jej verejným kľúčom

¹⁵ V ďalšom texte bude tento termín nahradený termínom: „certifikát“

¹⁶ V ďalšom texte môže byť tento termín nahradený termínom: „Poskytovateľ certifikačných služieb – PCS“ alebo „Certifikačná autorita – CA“

- *"produkt pre elektronický podpis"* – hardware alebo software alebo jeho zodpovedajúce časti, ktoré sú určené k tomu, aby ich overovateľ používal pre poskytovanie služieb súvisiacich s elektronickými podpismi alebo ktoré sú určené pre tvorbu alebo overovanie elektronických podpisov;
- *"dobrovoľná akreditácia"* - akékoľvek povolenie, ktoré stanoví zvláštne práva a povinnosti pre poskytovanie overovacích služieb a ktoré udeľuje na žiadosť overovateľa verejný alebo súkromný subjekt poverený stanovením týchto práv a povinností a dohľadom nad ich dodržovaním, pričom overovateľ nie je oprávnený vykonávať práva vyplývajúce z povolenia, kým neobdrží rozhodnutie tohoto subjektu.

2.1.2. Prístup na trh

Z pasáže o prístupe na trh vyplývajú pre členské štáty niektoré povinnosti. Je výslovne zakázané podmieňovať poskytovanie certifikačných služieb predbežným povolením, s výnimkou verejného sektoru, kde môžu byť stanovené doplňujúce požiadavky¹⁷. Takisto členské štáty nesmú obmedzovať počet akreditovaných poskytovateľov certifikačných služieb (PCS), ani poskytovanie certifikačných služieb pochádzajúcich z iného štátu.

2.1.3. Právne účinky elektronických podpisov

Členské štáty zaručujú, aby kvalifikované elektronické podpisy¹⁸ spĺňali tie isté právne požiadavky ako ručný podpis a boli prijateľné ako dôkazy pri súdnom konaní. Elektronický podpis nemôže byť odmietnutý ako dôkaz alebo stratiť právny účinok len kvôli tomu, že:

- je v elektronickej podobe
- nie je založený na kvalifikovanom certifikáte
- nie je založený na kvalifikovanom certifikáte od akreditovaného poskytovateľa certifikačných služieb
- nie je vytvorený bezpečným prostriedkom na tvorbu podpisov

¹⁷ Musia byť objektívne, priehľadné, proporcionálne a nediskriminačné a hlavne nesmú prekážať poskytovaniu cezhraničných služieb občanom.

¹⁸ Založené na kvalifikovaných certifikátoch a vytvorené pomocou kvalifikovaných prostriedkov pre vytváranie podpisu

- Taktiež musí byť zaručené, aby PCS ktorý poskytne kvalifikovaný certifikát, bol zodpovedný za škodu¹⁹ osobe, ktorá sa na tento spolieha pre:
 - presnosť údajov v kvalifikovanom certifikáte
 - súlad s požiadavkami direktívy pri vydávaní certifikátu
 - istotu, že držiteľ certifikátu bol v dobe jeho vydania držiteľom dát pre tvorbu EP zodpovedajúcich dátam pre overovanie podpisu uvedeného v certifikáte
 - istotu, že dáta pre tvorbu a overovanie podpisu môžu byť použité doplnujúcim spôsobom v prípadoch, kedy PCS vytvára oboje

V prípade, že PCS obmedzil rozsah použitia certifikátu (napr. stanovil hornú hranicu transakcií pre ktoré môže byť certifikát použitý), nie je zodpovedný za jeho použitie nad rámec tohto obmedzenia.

2.1.4. Medzinárodné hľadisko

Členské štáty musia zaistiť vzájomné právne uznanie elektronického podpisu. Navyiac musia zaručiť právnu rovnocennosť kvalifikovaným certifikátom vydaným v tretích krajinách, pokiaľ:

- PCS spĺňa podmienky uvedené v smernici a bol akreditovaný v rámci dobrovoľného akreditačného systému členského štátu
- PCS so sídlom v členskom štáte splňujúci náležitosti smernice sa za tento certifikát zaručí
- Sú certifikáty alebo PCS uznané na základe dohody medzi EÚ a tretími štátmi alebo organizáciami

Ďalej smernica zaručuje ochranu osobných údajov²⁰, ustanovuje „výbor pre elektronické podpisy“, ktorý má za úlohu bližšie špecifikovať a objasniť požiadavky a kritériá uvedené v smernici a jej prílohách, ako aj normy produktov pre elektronické podpisy²¹. Článok 11 stanovuje povinnosť členských štátov oznámiť Komisii i ostatným členským štátom informácie o dobrovoľných akreditačných systémoch, o subjektoch zodpovedných za akreditáciu a dozor ako aj o všetkých akreditovaných PCS na svojom území.

¹⁹ Okrem prípadov, kedy dokáže že nejednal z nedbalosti

²⁰ čl. 8

²¹ čl. 9 a 10

Smernica z 19.12.1999 vošla do platnosti dňa 19.01.2000 a členské štáty mali 6 mesiacov na jej implementáciu.

Smernica EÚ o elektronických podpisoch je formulovaná dostatočne obecné, bez zbytočného zamerania sa na technické aspekty, čo umožňuje udržať jej platnosť aj keď sa technológie elektronického podpisovania v čase menia. Takisto je ľahko rozšíriteľná o bližšie špecifikácie a objasnenie jednotlivých častí bez zásahu do samotného textu smernice. V týchto prípadoch sa k direktíve postupne pridávajú súvisiace dokumenty, tzv. „rozhodnutia Komisie“.

2.1.5. Rozhodnutie 2000/709/ES

Prvé z nich nedalo na seba dlho čakať a už 6.11.2000 bolo zverejnené rozhodnutie *„o minimálnych kritériách, ku ktorým by členské štáty mali prihliadať pri menovaní subjektov uvedených v čl. 3 odst. 4 Smernice 1999/93/ES Európskeho parlamentu a Rady o zásadách Spoločenstva pre elektronické podpisy“*. Ako naznačuje názov, toto rozhodnutie sa zaoberá minimálnymi kritériami pre subjekty hodnotiace súlad prostriedkov pre bezpečné vytváranie podpisov so Smernicou.

Zavádza pravidlá zabezpečujúce nestrannosť týchto subjektov a tým aj dôveryhodnosť celého systému elektronického podpisovania. Napríklad je nutné, aby sa subjekt ani jeho zamestnanci neangažovali v ostatných činnostiach súvisiacich so systémom EP, ako sú návrh a dodávka techniky pre bezpečnú tvorbu podpisov, poskytovanie certifikačných služieb a pod. Takisto musia byť finančne nezávislé a poistené²².

Rada požiadaviek je kladená aj na zamestnancov akreditačných subjektov, ktorí musia mať riadne technické a odborné vzdelanie, skúsenosti s posudzovaním zhody, musia byť nestranní a musí ich byť dostatočné množstvo.

2.1.6. Rozhodnutie 2003/511/ES

Druhé rozhodnutie dopĺňujúce smernicu bolo vydané 14.7.2003 a týka sa *„zverejnenia referenčných čísel obecné uznávaných štandardov pre zariadenia pre tvorbu elektronických podpisov“*

²² Alebo musia byť prijaté iné opatrenia upravujúce zodpovednosť vyplývajúcu z ich činnosti

Na základe požiadaviek v prílohách II a III Smernice boli v rámci EESSI²³ vyvinuté štandardy pre zariadenia pre tvorbu elektronických podpisov, ktoré boli v súlade so stanoviskom výboru pre elektronický podpis a tak boli ich referenčné čísla uvedené v prílohe rozhodnutia. Štandardy uvedené v prílohe²⁴ by mali členské štáty považovať za splňajúce požiadavky v prílohách. Európska Komisia mala do dvoch rokov zhodnotiť pôsobenie tohto rozhodnutia a podať správu výboru.

2.1.7. Zhrnutie

Smernica EÚ o elektronickom podpise mala širokosiahly dosah na zrovnoprávnenie elektronického podpisu s klasickým. Nariaďuje členským štátom jeho uznávanie pred súdom a vzájomné akceptovanie kvalifikovaných certifikátov medzi štátmi. Text Smernice zaručuje voľný prístup PCS na spoločný európsky trh služieb, čím sleduje presadenie bezpečnej a kompatibilnej elektronickej komunikácie, ktorá je dôležitým faktorom voľného pohybu služieb v rámci EÚ. Smernica je formulovaná obecné s cieľom všeobecnej platnosti do budúcnosti, napriek technologickému vývoju. Podrobnosťami sa zaoberajú následné rozhodnutia ES. Navyše Smernica zavádza spoločnú terminológiu, čo nesmierne zjednodušuje vývoj problematiky.

2.2. Zákon o elektronickom podpise v ČR

V českom právnom poriadku do prijatia zákona o elektronickom podpise neexistovala jednotná právna úprava, ktorá by jednoznačne zakazovala alebo pripúšťala elektronickú formu. Podľa analýzy p. Smejkal [SME01] je len v niektorých právnych predpisoch vyslovene uvedené že dokument musí byť v papierovej forme²⁵. Občiansky zákonník, ktorý je základnou normou českého právneho poriadku vraví že : „*Podpis môže byť nahradený mechanickými prostriedkami v prípadoch, kedy to je obvyklé. Písomná forma je zachovaná, ak je právny úkon vykonaný telegraficky, diaľnopisom alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon vykonala*“.

²³ Európska iniciatíva pre štandardizáciu elektronického podpisu – European Electronic Signature Standardisation Initiative

²⁴ CWA 14167-1, CWA 14167-2, CWA 14169

²⁵ matrika, lodný denník a pod.

Zákon o elektronickom podpise v ČR, tak ako v ostatných krajinách EÚ, vychádza zo Smernice EÚ o zásadách Spoločenstva pre elektronické podpisy²⁶. Do platnosti vstúpil 1.10.2000 pod názvom „*Zákon č. 227/2000 Zb., o elektronickom podpise a o zmene ďalších zákonov*“. Od svojho vzniku bol novelizovaný 3 krát: zákonmi č. 226/2002 Zb., č. 517/2002 Zb. a č. 440/2004 Zb.

Ďalšími súvisiacimi textami sú nariadenia vlády a vyhlášky, ktorými sa zákon o elektronickom podpise vykonáva.

2.2.1. Zákon č 227/2000 Zb.

Najrozsiahlejšou novelou zákona boli zmeny vykonané zákonom č. 440/2004 Zb. Tento predpis reagoval na kritiku odbornej verejnosti poukazujúcej na nedostatky pôvodného zákona. Vláda tieto problémy identifikovala v tzv. „*Bielej knihe elektronického obchodu*“ - jednalo sa o:

- Nekompatibilitu s právom EÚ
- Absenciu časových pečiatok v zákone²⁷
- Možnosť používať zahraničné certifikáty²⁸
- Elektronické podpisovanie správ bez účasti človeka²⁹

Tieto problémy adresuje spomínaná novela z 26.7.2004 a zavádza aj ďalšie vylepšenia resp. kozmetické úpravy zprehľadňujúce text zákona. Napríklad príliš dlhá formulácia „zaručený elektronický podpis založený na kvalifikovanom certifikáte od akreditovaného poskytovateľa certifikačných služieb“ sa mení na zrozumiteľný „uznávaný elektronický podpis“. [HASO01]

Nasleduje stručný opis novelizovaného zákona³⁰.

²⁶ V pôvodnom znení nebol tento zákon dostatočne kompatibilný s právom EÚ, čo vyústilo do jeho novelizácie v roku 2004

²⁷ Absencia časových pečiatok pôsobila podľa [EPR01] napríklad takýto problém: „Ak si kupujúci objedná tovar elektronickou cestou, zaviazne sa ho odobrať a zaplatiť. Predávajúcemu síce vznikne formálna povinnosť tovar dodať, ale tu nastáva problém, ako túto povinnosť kupujúci dokáže. V tejto situácii je len na predávajúcom, či bude zasielať potvrdenie o prijatí objednávky. Zmluva vzniká v momente akceptácie ponuky zo strany nakupujúceho. Ak by ponuka obsahovala ustanovenie, že zmluva vznikne až v momente doručenia potvrdenia o prijatí objednávky, ocitol by sa v nevýhode predávajúci, pretože ten by vznik zmluvy nemohol dokázať. Tím sa dostávame do začarovaného kruhu.“

²⁸ Pôvodný predpis vyžadoval, aby bol kvalifikovaný certifikát vydaný na území ČR – čo je v rozpore so Smernicou

²⁹ Čiže automatické podpisovanie správ serverom, napríklad pri zasielaní výpisov z registrov

³⁰ Problematikou právnej úpravy elektronického podpisu sa zaoberá dostatočné množstvo literatúry, pre podrobnejší popis vid'. napr. [HASO01]

Hneď prvým markantným rozdielom od Smernice je väčší počet pojmov definovaných v zákone. Je ich hneď 26, oproti 13. v Smernici. Medzi tie najdôležitejšie patria „časová pečiatka“, „elektronická značka“, „systémový certifikát“ a „elektronická podateľňa“.

2.2.1.1. Časová pečiatka

Pragraf 2 písmeno r) zákona časovú pečiatku definuje takto:

„kvalifikovanou časovou pečiatkou [je] dátová správa, ktorú vydal kvalifikovaný poskytovateľ certifikačných služieb a ktorá dôveryhodným spôsobom spája dáta v elektronickej podobe s časovým okamihom a zaručuje, že uvedené dáta v elektronickej podobe existovali pred daným časovým okamihom“

Podobne ako v prípade elektronického podpisu a certifikátov, aj pri elektronickej pečiatke rozlišujeme pečiatky kvalifikované a ostatné, pričom jedine kvalifikovaná pečiatka je akceptovateľná súdom. Ich absencia tvorila podstatnú prekážku širšiemu rozšíreniu elektronického podpisu – viď poznámku 27. Spojenie nespochybniteľného časového údaju a konkrétnych dát je nevyhnutné najmä pre účely ich spätného overovania. Pre príklady použitia časových značiek viď kapitolu o využití elektronického podpisu.

Zákon pre poskytovateľov kvalifikovaných časových pečiatok stanovuje tieto náležitosti:

- musí zaistiť, aby časové pečiatky ním vydávané ako kvalifikované obsahovali všetky náležitosti stanovené týmto zákonom
- musí zaistiť, aby časový údaj vložený do kvalifikovanej časovej pečiatky zodpovedal hodnote koordinovaného svetového času pri jej tvorbe
- musí zaistiť, aby dáta v elektronickej podobe ktoré sú predmetom žiadosti o vydanie kvalifikovanej časovej pečiatky, jednoznačne zodpovedali dátam v elektronickej podobe obsiahnutých vo vydannej kvalifikovanej časovej pečiatke
- musí prijať zodpovedajúce opatrenia proti falšovaniu kvalifikovaných časových pečiatok,
- musí poskytovať, na vyžiadanie, tretím osobám podstatné informácie o podmienkach pre využívanie kvalifikovaných časových pečiatok, vrátane

obmedzení pre ich použitie a informácie o tom, či je alebo nie je akreditovaný ministerstvom

- musí vydať kvalifikovanú časovú pečiatku neodkladne po prijatí žiadosti o jej vydanie.

2.2.1.2. Elektronická značka, systémový certifikát

Rozdiel medzi elektronickým podpisom a elektronickou značkou spočíva v tom, že značkou môže disponovať tak fyzická, ako aj právnická osoba alebo organizačná zložka štátu. K podpisovaniu pomocou značky nie je potrebná účasť človeka, využívajú sa automatizované postupy. Systémový certifikát overuje identitu osoby, ktorá tento automat ovláda. Elektronické značky a systémové certifikáty sú nenahraditeľné napr. pri výpisoch zo štátnych registrov. Je dôležité nezamieňať si význam systémového certifikátu a serverového certifikátu³¹.

2.2.1.3. Elektronická podateľňa

Z definície podľa písmena y) druhého paragrafu zákona je elektronická podateľňa:

„ [...] pracovisko orgánu verejnej moci určené pre príjem a odosielanie dátových správ. “

Pomocou nej jednotlivé orgány komunikujú navzájom alebo priamo s občanmi. Povinnosť orgánov verejnej moci zriadiť elektronickú podateľňu je upravená vo vyhláške č. 496/2004 Zb. o elektronických podateľniach. Viac o jednotlivých elektronických podateľniach v nasledujúcich kapitolách.

2.2.1.4. Vzťahy so zahraničím

Novelizovaný zákon odstránil nevyhovujúcu úpravu uznávania zahraničných certifikátov a teda nie je viac nutné, aby bol kvalifikovaný certifikát vydaný na území ČR. Paragraf 16 je teda v plnom súlade so Smernicou.

³¹ Kým systémový certifikát zabezpečuje overenie identity správcu systému, serverový certifikát slúži pre šifrovanie komunikácie s klientom [zdroj - bakula]

2.2.2. Vyhláška a nariadenie vlády o elektronických podateľniach

Prvého januára 2005 nadobudlo účinnosť nariadenie vlády o elektronických podateľniach č. 495/2004 Zb. Stanovuje povinnosť orgánov verejnej moci zriadiť e-podateľne, vybaviť príslušných zamestnancov kvalifikovanými elektronickými podpismi a zaistiť zodpovedajúcim spôsobom ochranu spracovávaných informácií.

V prípade malého objemu elektronickej komunikácie si musia zaistiť aspoň príjem a odosielanie správ prostredníctvom elektronickej podateľne iného úradu.

Dôležité pre občana je, že aj v prípade že správa doručená e-podateľni neobsahuje všetky náležitosti, je orgán verejnej moci povinný toto podanie prijať. Upovedomí odosielateľa o nedostatkoch a poskytne mu primeranú lehotu pre potvrdenie podania, a to aj iným ako elektronickým spôsobom³². Dátum podania je daný prvotným elektronickým podaním. [HN03]

V prílohe vyhlášky č. 496/2004 Zb. sa nachádza spôsob overovania platnosti elektronického podpisu/pečiatky, ako aj odkazy na akreditované štandardy asymetrických algoritmov a hašovacích funkcií .

2.2.3. Vyhláška 378 z 19.7.2006 o postupoch kvalifikovaných PCS

Prvá časť tejto vyhlášky je určená PCS a obsahuje požiadavky na ich postupy pri vydávaní kvalifikovaných certifikátov, kvalifikovaných systémových certifikátov a kvalifikovaných časových pečiatok.

Druhá časť sa vzťahuje na označujúce osoby a to najmä na orgány verejnej moci – obsahuje požiadavky na ochranu súkromných kľúčov používaných k tvorbe elektronických značiek.

Príloha obsahuje zoznam bezpečnostných štandardov pre informačné systémy, riadiace systémy certifikátov, systém riadenia bezpečnosti informácií, pre produkty pre tvorbu podpisov atď.

³² Klasickým písomným alebo ústne do protokolu

2.2.4. Zhrnutie

Doplnením Občianskeho zákonníku zákon o elektronickom podpise zrovnoprávňuje elektronický podpis s klasickým a následne stanovuje práva a povinnosti jednotlivých aktérov, ako aj náležitosti a požiadavky na jednotlivé technické komponenty súvisiace s elektronickým podpisom. Možnosť použitia elektronického podpisu sa ďalej zavádza zmenou hlavných procesnoprávnych noriem³³.

Vyhlášky a nariadenia vlády súvisiace so zákonom podrobnejšie upresňujú požiadavky na aktérov systému – okrem iného stanovujú povinnosť orgánov verejnej moci umožniť komunikáciu s nimi elektronickou cestou.

Česká podoba zákona o elektronickom podpise je po novelizácii v súlade so Smernicou EÚ.

Hlavný prínos zákona nespočíva v technickej rovine, ale v preniknutí elektroniky do „domény“ tradičného papierového dokumentu [SME01]. Bez špecifikácií uvedených v jednotlivých prílohách poskytuje dostatok „manévrovacieho priestoru“ a tak by príchod nových technológií podpisovania nemal vyvolať nutnosť zásadnej novelizácie.

2.3. Zákon o elektronickom podpise vo Francúzsku

Vo Francúzsku sa prvý zákon týkajúci sa elektronického podpisu objavil necelé tri mesiace po uverejnení Smernice. Predchádzali mu prípravné práce v Senáte³⁴, ktoré boli schválené 8.2.2000 a návrh tohto zákona bol posunutý Národnému Zhromaždeniu. To po vypočutí správy³⁵ a následnej diskusii prijalo zákon 2000-230 z 13.3.2000 „o adaptácii dôkazného práva informačným technológiám a týkajúci sa elektronického podpisu“³⁶.

Pred kapitolami o jednotlivých zákonoch je pre orientáciu uvedená stručná charakteristika politického systému vo Francúzsku. Na záver kapitoly je umiestnené krátke zhrnutie.

³³ Zákon č. 337/1992 Zb. o správe daní a poplatkov, § 21 odstavce 2 a 3; Zákon č. 71/1967 Zb. o správnom konaní v znení zákona č. 29/2000 Zb., § 19 odstavec 1; Zákon č. 99/1963 Zb. občiansky súdny poriadok, § 42 odstavec 1; Zákon č. 141/1961 Zb. o trestnom konaní, § 59 odstavec 1

³⁴ Návrh zákona č. 488 (1998-1999), správa p. Charles-a Jolibois č. 203 (1999-2000)

³⁵ Správa p. Christian-a Paul, č. 2197

³⁶ Loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

2.3.1. Politický systém Francúzska

Politický systém Piatej Republiky vo Francúzsku spája črty parlamentnej demokracie so silnou výkonnou mocou a často je nazývaný „polo-prezidentský“.

Legislatívnu moc má dvojkomorový parlament zložený zo Senátu a Národného zhromaždenia. Hlavou štátu je prezident, volený na 5 rokov priamou voľbou. Z ústavy mu plynú dôležité právomoci v oblasti zahraničnej a obrannej politiky, ako aj v domácich záležitostiach. Vláda, zodpovedná Parlamentu a prezidentovi, je vedená premiérom, ktorého menuje a odvoláva prezident.

2.3.2. Zákon 2000-230 z 13 marca 2000

Tento zákon vložil do Občianskeho zákoníku nasledujúce články:

- Čl. 1316 – Písomný dôkaz pozostáva s postupnosti písmen, znakov, čísel alebo iných symbolov majúcich zrozumiteľný význam, bez ohľadu na spôsobe ich zachytenia alebo šírenia
- Čl. 1316-1 – Elektronická písomnosť je prijateľná ako dôkaz v rovnakom rozsahu ako písomnosť na papieri, pokiaľ je možné identifikovať pôvodcu a pokiaľ je uchovaná v stave ktorý zaručuje jej integritu
- Čl. 1316-2 – Keď zákon ani zmluvné strany neurčia inak, sudca rozhoduje v sporoch o písomný dôkaz určením najpravdepodobnejšieho oprávnenia (*titre*), bez ohľadu na jeho nosič.
- Čl. 1316-3 – Písomnosť na elektronickom nosiči má rovnakú dôkazovú moc ako písomnosť na papieri
- Čl. 1316-4 – ...keď je [podpis] elektronický, pozostáva z použitia procedúry garantujúcej prepojenie podpisu s aktom ku ktorému sa pripája. Predpoklad dôveryhodnosti tohto podpisu platí až do dokázania opaku v prípade, keď je identita podpisujúcej osoby a integrita aktu zaručená a podpis bol vytvorený v súlade s podmienkami uvedenými v dekréte Rady Štátu³⁷.

Na niektorých miestach sa ešte zákonom nahrádza slovo „ručne (*de sa main*)“ slovom „osobne (*par lui-même*)“, zo zrejmých dôvodov.

³⁷ Conseil d'Etat

Ako je vidno, tento zákon zmenou a pridaním niektorých článkov upravuje definíciu dôkazu a podpisu a garantuje rovnocennosť elektronického a papierového podpisu. Je to zákon stručný, neobsahuje zmienku o certifikačných autoritách, rôznych stupňoch podpisu a iných náležitostiach zmienených v Smernici. V ešte väčšej miere ako Smernice je tento zákon technologicky neutrálny – zákonodarca ponecháva určenie kritérií dôveryhodnosti na pleciach Rady Štátu (*Conseil d'Etat*) – čo umožňuje väčšiu flexibilitu voči technologickému pokroku.

2.3.3. Dekrét č. 2001-272 z 30.3.2001

Na úpravu týchto záležitostí si vo Francúzsku museli počkať do 30.3.2001, kedy vyšiel dekrét č. 2001-272 „*upravujúci aplikáciu článku 1316-4 Občianskeho Zákonníku a týkajúceho sa elektronického podpisu*“. Tento dekrét viac-menej kopíruje Smernicu, aj keď sa nájde niekoľko rozdielov, napr. nie je definovaný „*produkt pre elektronický podpis*“³⁸.

Článok 1316-4 zákona je dekrétom v článku 2 rozvinutý takto:

„dôveryhodnosť elektronického podpisu platí až do dokázania opaku v prípade, keď sa jedná o zabezpečený elektronický podpis vytvorený pomocou prostriedku pre bezpečnú tvorbu podpisu a keď sa overovanie tohto podpisu opiera o kvalifikovaný certifikát“

Ďalšie články sú rozdelené do štyroch kapitol:

- *Prostriedky pre bezpečnú tvorbu elektronického podpisu* – stanovuje podmienky ktoré musia takéto prostriedky spĺňať a určuje, kto je oprávnený takýto prostriedok vyhlásiť za spĺňajúci požadované kritériá
- *Prostriedky pre overovanie podpisu* – stanovuje podmienky pre certifikáciu týchto prostriedkov
- *Kvalifikované elektronické certifikáty a certifikačné authority* – stanovuje, čo všetko musí kvalifikovaný certifikát obsahovať a aké podmienky musí spĺňať certifikačná autorita poskytujúca kvalifikované podpisy
- *Rôzne dispozície* – stanovuje rozsah pôsobnosti dekrétu na Novú Kaledóniu, francúzsku Polynéziu, ostrovy Wallis a Futuna a Mayotte. Táto klauzula sa nachádza v prevažnej väčšine právnych textov. Keďže pre túto

³⁸ Vid'. predposlednú definíciu v časti o terminológii zavedenej Smernicou

prácu nemá význam, nebude v ďalšom texte spomínaná aj v prípade že sa v popisovaných textoch bude nachádzať

2.3.4. Dekrét 2002-535 z 18.4.2002

O viac než rok vyšiel ďalší dekrét, tentokrát sa týkal hodnotenia a certifikácie bezpečnosti produktov a systémov informačných technológií. Znovu sa jedná o technicky absolútne neutrálny text, ktorého pôsobnosť sa neobmedzuje len na problematiku elektronického podpisu, ale na informačné technológie ako také.

Stanovuje postup podania žiadosti o certifikáciu, postup pri akreditácii certifikačných autorít, upravuje vzťahy so zahraničnými autoritami atď. Zriaďuje „*riadiacu komisiu pre certifikáciu bezpečnosti informačných technológií*“³⁹, ktorá má na starosti tvorbu posudkov pri akreditácii certifikačných centier, pri sporoch týkajúcich sa tejto problematiky atď.⁴⁰. Tvoria ju zástupcovia jednotlivých ministerstiev, okrem prípadov kedy rozhoduje o otázkach týkajúcich sa prostriedkov pre tvorbu a overovanie elektronických podpisov, kedy má ďalších 12 kvalifikovaných osôb volených na tri roky Prvým ministrom.

2.3.5. Uznesenie z 26.7.2004

Ďalším súvisiacim textom je uznesenie z 26.7.2004 týkajúce sa „*uznávania kvalifikácie PCS a akreditácie orgánov ktoré ich hodnotia*“. Je rozdelený na 12 článkov v dvoch kapitolách a prílohu. Pretože sa v ČR problematike francúzskej právnej úpravy elektronického podpisu nevenuje veľa pozornosti, bude nasledovať stručný popis jednotlivých článkov pre potreby neskoršieho porovnania s českou legislatívou.

2.3.5.1. Kapitola 1 – akreditácia orgánov hodnotiacich kvalifikáciu PCS

Článok 1 - Francúzska akreditačná komisia (COFRAC) alebo iný orgán ktorý je signatárom multilaterálnej dohody o vzájomnom uznávaní v rámci spolupráce európskych akreditačných orgánov, ďalej nazývaný akreditačné centrum, je poverený akreditovať orgány hodnotiace kvalifikáciu PCS.

Článok 2 – Žiadosť o akreditáciu musí obsahovať nasledujúce prvky:

³⁹ Direction centrale de la sécurité des systèmes d'information - DSSI

⁴⁰ Táto komisia má na starosti certifikovanie bezpečnosti systémov, nezaobrá sa certifikáciou PCS. Tú upravuje uznesenie z 26.7.2004 popísané v nasledujúcej kapitole.

- Štatút orgánu, jeho vnútorné členenie a všetky dokumenty riadiace jeho fungovanie
- Mená a kvality vedúcich orgánu a členov administratívnej rady alebo iných orgánov zastávajúcich túto funkciu
- Mená a kvality zamestnancov podieľajúcich sa na hodnotení
- Popis aktivít, štruktúry a technických prostriedkov orgánu
- Les comptes des deux exercices precedents
- Popis procedúr a prostriedkov ktoré budú použité pri hodnotení kvalifikácie PCS

Orgán má povinnosť ohlásiť prípadné vzťahy s PCS a opatrenia ktoré urobí pre zabránenie konfliktu záujmov.

Článok 3 – Akreditačné centrum môže od žiadateľa požadovať doplňujúce informácie, vykonať kontrolu v jeho prevádzke. V prípade udelenia akreditácie môže požadovať zvláštne záväzky.

Článok 4 – Akreditácia je platná počas obdobia nepresahujúceho 5 rokov. Akreditované orgány musia oznámiť každú zmenu oproti skutočnostiam platným v dobe podania žiadosti. Počas platnosti akreditácie je vykonávaný pravidelný dohľad podľa dohody o spolupráci európskych akreditačných orgánov

Článok 5 – Akreditačné centrum zverejňuje aktuálny zoznam akreditovaných orgánov.

2.3.5.2. Kapitola 2 – Uznávanie kvalifikácie PCS

Článok 6 – PCS ktorý chce byť uznaný ako kvalifikovaný si vyberá orgán akreditovaný k hodnoteniu svojich aktivít. Je povinný poskytnúť všetky prvky potrebné k správne naplneniu procedúry hodnotenia.

Článok 7 – Hodnotenie je vykonané na náklady PCS. Orgán má za úlohu overiť či je PCS v súlade s požiadavkami na nich kladenými. Tieto technické požiadavky, uvedené v prílohe, upresňujú požiadavky zakotvené v čl. 6 dekrétu z 30. marca 2001.

Článok 8 – Správy o hodnotení sú zasielané do centrálného riaditeľstva bezpečnosti informačných systémov (DCSSI)

Článok 9 – Ak je PCS zhodnotený ako majúci potrebnú kvalifikáciu, akreditovaný orgán dodá atestáciu popisujúcu činnosti pokryté kvalifikáciou ako aj dĺžku jej platnosti, ktorá nesmie prekročiť 3 roky. Počas tohoto obdobia sa PCS podrobí minimálne raz za rok auditu akreditovaným orgánom, ktorý má právo atestáciu suspendovať alebo odobrať.

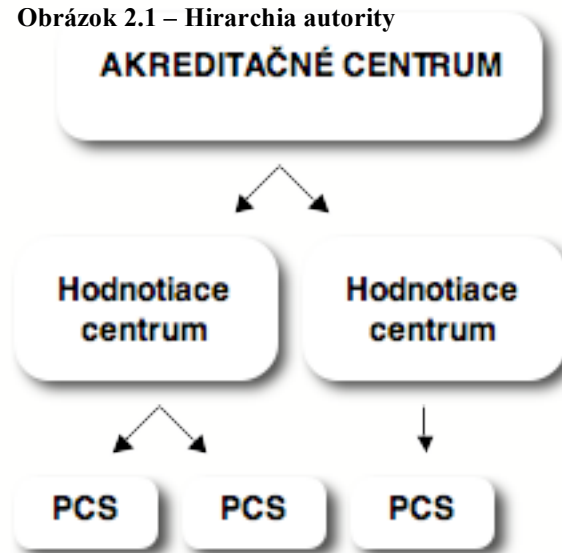
Článok 10 – Poskytovatelia technických služieb PCS poskytujúcich kvalifikované certifikáty môžu takisto požiadať o atestáciu svojich služieb podľa technických kritérií uvedených v prílohe⁴¹

2.3.5.3. Príloha

V prílohe sa nachádza technická špecifikácia bodov f, g a m druhej časti článku dekrétu z 30.3.2001⁴². Kompletný text uznesenia v originále sa nachádza v prílohe, je ale vhodné vyzdvihnúť fakt, že pre preukázanie identity je postačujúci len jeden oficiálny doklad totožnosti opatrený fotografiou.

2.3.5.4. Zhrnutie

Obrázok 2.1 – Hirarchia autority



Hierarchiu autority ako ju definuje toto uznesenie znázorňuje obrázok (obr. 1). Akreditačné centrum poveruje hodnotiace centrá udeľovaním atestácií PCS.

⁴¹ Články 11 a 12 obsahujú len informácie o dátume publikácie a zrušení predchádzajúceho uznesenia

⁴² PCS musí: používať vhodné bezpečnostné postupy, používať produkty a systémy zaručujúce technickú a kryptografickú bezpečnosť funkcií ktoré poskytujú, overiť identitu osoby ktorej je elektronický certifikát vydávaný vyžiadanim preukázania sa preukazom totožnosti; a uchovávať charakteristické znaky a referencie prezentovaných dokladov pre dôkaz identity

2.3.6. Zákon 2004-575 z 21.6.2004

Tento zákon, nazvaný „*pre dôveru v elektronickom obchode*“, sa venuje otázkam bezpečnosti systémov používaných v elektronickej komunikácii a zodpovednosti jednotlivých aktérov. Pre problematiku elektronického podpisu je významný obzvlášť článok 33, ktorý upresňuje režim zodpovednosti PCS poskytujúcich kvalifikované certifikáty. Tento článok stanovuje zodpovednosť PCS voči osobám, ktoré sa primerane spoliehali na certifikát prezentovaný ako kvalifikovaný v týchto prípadoch:

- Informácie obsiahnuté v certifikáte v dobe jeho vydania boli nepresné
- Dáta ktoré musí certifikát obsahovať aby bol uznaný za kvalifikovaný boli neúplné
- Vydaniu certifikátu nepredchádzalo overenie či podpisujúca osoba disponuje súkromným kľúčom zodpovedajúcim verejnému kľúču tohto certifikátu
- PCS nezaznamenali zrušenie certifikátu a túto informáciu neposkytli tretím osobám

PCS nie sú zodpovedný za škody spôsobené použitím certifikátu nad rámec jeho použitia (ktoré musí byť v certifikáte uvedené) alebo ak preukážu, že nejednali zámerne alebo z nedbalosti.

Jedná sa teda o ustanovenia ktoré sa nachádzajú už v Smernici ale do vydania tohto zákona nemali vo Francúzskej legislatíve miesto.

2.3.7. Zákon 2004-801 z 6.8.2004

Necelé dva mesiace na to vyšiel ďalší predpis upravujúci systém elektronického podpisovania. Tento zákon sa týka „*ochrany fyzických osôb s ohľadom na spracovanie osobných údajov*“. Upravuje zákon 78-17 zo 6.1.1978 týkajúceho sa „*informatiky, katalógov a slobôd*“. Stanovuje tak pravidlá práce s osobnými údajmi a sankcie pri porušení týchto pravidiel.

Pre účel práce je významný najmä článok 33, ktorý hovorí:

„Bez výslovného souhlasu dotčené osoby mohou být osobné údaje zozbierané PCS pre potreby vydania a uchovania certifikátov spojených s elektronickým podpisom použité len pre účely pre ktoré boli získané“

2.3.8. Další důležité texty

V októbri 2003 vydala Francúzska agentúra pre e-Government⁴³ dokument *„rámec pre elektronický podpis a politiku bezpečnosti“*⁴⁴. Tento stanovuje 3 úrovne zabezpečenia elektronického podpisu, typové certifikačné politiky, požiadavky na časové pečiatky a pod.

Dokument bol dvakrát aktualizovaný po rozsiahlom pripomienkovaní zo strany verejných aj súkromných predstaviteľov. Najaktuálnejšia je verzia 2.1.⁴⁵ z novembra 2006.

2.3.9. Zhrnutie

Tesne po vydaní Smernice Francúzsko uzákonilo rovnoplatnosť elektronického a papierového podpisu. O rok na to ju preniesli do svojej legislatívy podrobnejšie a ďalšími úpravami približovali významu Smernice. Okrem zákonov upravujú používanie elektronického podpisu dekréty, uznesenia a iné texty. Uznesenie z 26.7.2004 stanovuje trojstupňovú hierarchiu autority certifikácie PCS.

2.4. Porovnanie legislatívy

Legislatíva ČR aj Francúzska zrovnoplatňuje elektronický podpis s klasickým podpisom na papieri. Taktiež upravuje spôsoby jeho použitia vo verejnom sektore, určuje akreditačné authority, definuje požiadavky na bezpečnosť atď. Terminológia použitá v oboch legislatívach je viac-menej identická, preberajú ju z textu Smernice.

Oba štáty upravili svoje zákony tak, aby boli v čo najväčšej miere zosúladené so smernicami a rozhodnutiami platnými pre celú EÚ. Z tohto dôvodu by mala byť právna úprava oboch štátov rovnaká. Aj keď je to zväčša pravda, rozdiely v politickom systéme krajín predsa len dali vzniknúť niekoľkým menším odlišnostiam.

⁴³ ADELE – vid' kapitolu o službách Francúzskeho e-Governmentu

⁴⁴ PRIS - Politique de Référence Intersectorielle de Sécurité

⁴⁵ http://synergies.modernisation.gouv.fr/article.php3?id_article=381

Z formálneho hľadiska sa v ČR viac používajú zákony. Úpravou použitia elektronických podpisov sa zaoberajú: zákon č. 227/2000 Zb., č. 226/2002 Zb., č. 517/2002 Zb., 439/2004 Zb. a č. 440/2004 Zb. Vo Francúzsku sa skôr spoliehajú na dekréty, uznesenia a iné texty vydávané autoritami zodpovednými za aplikáciu elektronického podpisu v rôznych oblastiach⁴⁶.

Z praktického hľadiska je azda najmarkantnejším rozdielom zavedený systém akreditácie PCS. Vo Francúzsku sú uznesením z 26.7.2004 definované orgány⁴⁷ (akreditačné centrá), oprávnené udeľovať atestácie ďalším orgánom, ktoré vykonávajú hodnotenie PCS. V praxi to teda vyzerá tak, že PCS si vyberie orgán ktorý ho má hodnotiť. Ak chce byť považovaný za zákonne kvalifikovaného PCS, musí byť táto hodnotiaca autorita akreditovaná akreditačným centrom⁴⁸.

V ČR je zákonom daná jediná autorita ktorá smie vydávať akreditácie PCS, a tou je Ministerstvo Informatiky. Oproti Francúzsku tu teda chýba jeden hierarchický stupeň. PCS ktorý chce ponúkať certifikáty vhodné pre komunikáciu so štátnou správou teda musí o akreditáciu požiadať priamo Ministerstvo Informatiky. To do dnešného dňa akreditovalo 3. PCS.

Ďalším dôležitým rozdielom je nutnosť používania kvalifikovaných certifikátov pri komunikácii so štátnou správou. Kým ČR tieto kvalifikované certifikáty priamo vyžaduje, vo Francúzsku je možné použiť aj nekvalifikované certifikáty. Jedná sa najmä o certifikáty poskytované zadarmo za účelom použitia konkrétnej aplikácie. Ako príklad slúžia certifikáty pre daňový portál impots.gouv.fr.

Z časového hľadiska je možné konštatovať, že prijímanie legislatívy o elektronickom podpisovaní bolo viac-menej rovnako časovo náročné v oboch krajinách. Prvé zákony o elektronickom podpise boli prijaté v rozmedzí 3 mesiacov s tým, že boli v nasledujúcich rokoch upravované a zosúladované so Smernicou. Legislatíva týkajúca sa verejného obstarávania bola takisto prijatá začiatkom roka 2004 v oboch štátoch.

Rozdiel ale vidíme v prijatí úpravy zavedenia e-Governmentu. V Českej Republike bol už 14.9.2000 schválený text č. 365/2000 Zb. „o informačných systémoch

⁴⁶ DSSI, CNIL, ADELE atď.

⁴⁷ COFRAC

⁴⁸ Vid'. obr. 1

*verejnej správy*⁴⁹“, ktorý spomína aktívne zameranie sa na tvorbu e-Governmentu [IDAB01]. Vo Francúzsku bol podobný text⁵⁰ uzákonený až 8.12.2005 [IDAB02]. To ale neznamená, že sa tejto problematike vo Francúzsku nevenovala pozornosť. Práve naopak. Potvrdzuje to napríklad existencia funkčného daňového portálu od začiatku roka 2005, čiže takmer rok pred schválením uvedeného textu.

Inak sa právna úprava elektronického podpisovania prakticky nelíši, možno s výnimkou v rozdieloch medzi uznávanými prostriedkami pre tvorbu podpisu, ktoré sú spravidla uvedené v prílohách k príslušným právnym textom⁵¹. Tieto rozdiely však vyplývajú skôr z dostupnosti týchto prostriedkov na jednotlivých národných trhoch a nie na rozdielnych bezpečnostných požiadavkách.

⁴⁹ Public Administration Information Systems – zdroj: [IDAB01]

⁵⁰ Ordinance on electronic interactions between public services users and administrative authorities and between Administrations, známy aj ako „teleservice ordonnance“

⁵¹ Francúzsko má týchto prostriedkov schválených viacej ako ČR

3. Využitie elektronického podpisu pre eGovernment

3.1. *Elektronický podpis pri komunikácii s orgánmi štátnej moci v ČR*

Elektronické služby v ČR sa s príchodom cenovo dostupných kvalifikovaných certifikátov⁵² začali tešiť väčšej obľube, ako dokazujú grafy v nasledujúcich kapitolách. Medzi najvyužívanejšie aplikácie využívajúce elektronický podpis patria tie, ktoré sú zastrešené portálom zdravotných poisťovní a portálom verejnej správy. Táto práca sa bude venovať najmä komunikácii štátu s občanom, takže opis služieb poisťovní bude stručný. Pre viac informácií o tomto portále vid' napríklad kapitolu 5.2 v [HASO01].

3.1.1. Portál zdravotných poisťovní

Portál zdravotných poisťovní bol vytvorený piatimi poisťovňami, ktoré zastupujú veľkú časť poisťencov. Ide o aplikáciu podobajúcu sa internetovému bankovníctvu, ktorá umožňuje pohodlné vybavovanie agendy so zdravotnými poisťovňami [HASO01].

Portál ZP poskytuje automatizovaný prístup pri výmene dát typu:

- Odovzdávanie dávok a faktúr
- Hromadné oznámenia zamestnávateľa
- Prehľad platieb zamestnávateľa
- Elektronická podateľňa

3.1.2. Portál verejnej správy

V súčasnej dobe je prístup k službám e-Governmentu Českej Republiky sprostredkovaný Portálom verejnej správy⁵³, ktorý slúži ako jednotná brána, cez ktorú občania a firmy prístupujú k jednotlivým aplikáciám štátnych orgánov.

„ [PVS] je vstupnou bránou do elektronického úradného sveta Českej Republiky⁵⁴“

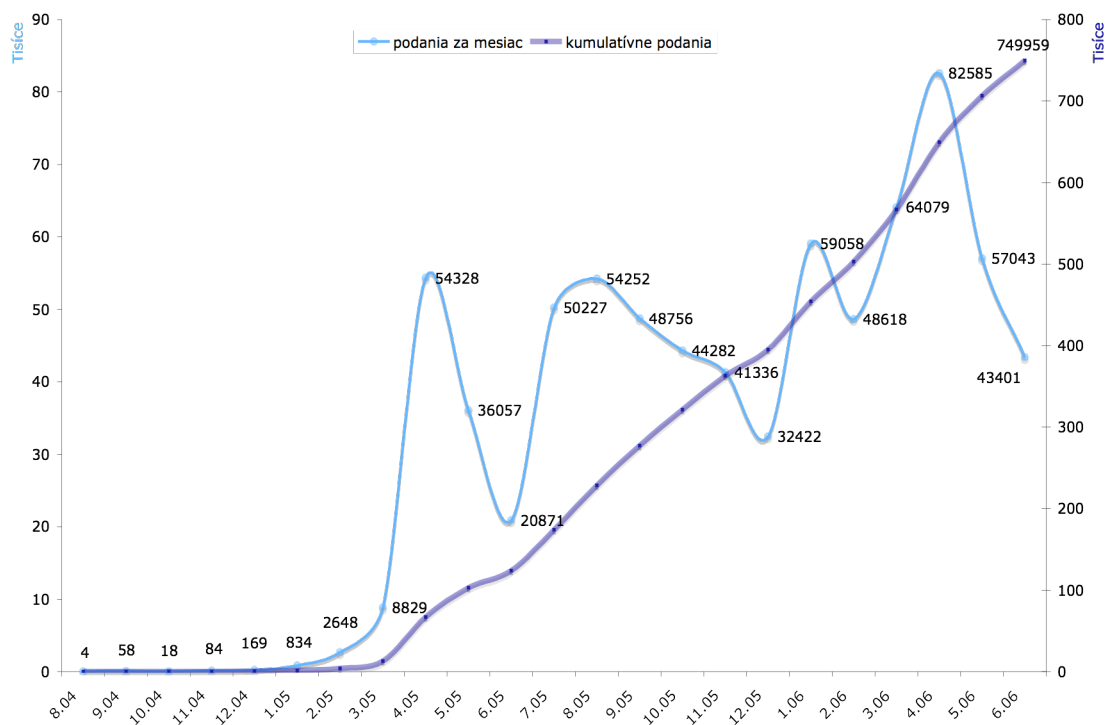
⁵² Od PCS PostSignum, orietačná cena 190 CZK. Dostupnosť sa zvýšila zavedením služby „mobilnej certifikačnej autority“

⁵³ <http://portal.gov.cz/>

Testovacia prevádzka skončila v októbri 2004. Cieľom projektu je zjednodušiť administráciu, uľahčiť komunikáciu občanov a firiem s orgánmi verejnej správy, zabezpečiť jednoduchú a dostupnú výmenu overených informácií a rozšíriť transparentnosť a dôveru vo verejnú správu [IDAB01].

Nasledujúci graf ukazuje prudký nárast využívania služieb poskytovaných cez PVS od začiatku roku 2005. K 21.6.2006 bolo zaznamenaných celkovo 749 959 podaní. Najväčší podiel na tomto majú služby ČSSZ⁵⁵, ktoré využíva väčšina podávateľov cez PVS.

Graf 3.1 - Počet podaní cez portál verejnej správy



Zdroj: Ministerstvo Informatiky ČR, 2006

3.1.3. Služby Ministerstva financií - Daňový portál

V októbri tohto roku spustilo Ministerstvo financií plnú verziu⁵⁶ projektu Daňového portálu⁵⁷, čím umožnilo daňovým subjektom spracovávať podania adresované správcovi daní a nazerať do svojich daňových účtov pomocou elektronickej aplikácie [HN02]. To znamená, že daňový poplatník si cez Daňový portál môže zaisitiť,

⁵⁴ Citácia z [ONL04]

⁵⁵ Česká správa sociálneho zabezpečenia

⁵⁶ Od 3.7.2006 fungoval projekt v pilotnej verzii a bol dostupný len vybraným užívateľom

⁵⁷ <http://adis.mfcr.cz/adis/jepo/index.html>

či finančný úrad eviduje na (poplatníkovom) účte nedoplatok, preplatok alebo je vyrovnaný.

Pre túto komunikáciu je vyžadovaný kvalifikovaný elektronický podpis, ktorý je možné získať u jednej z troch českých certifikačných autorít⁵⁸.

Postup je potom zhruba nasledovný [HN02]:

- Poplatník alebo jeho zástupca podá žiadosť o zriadenie informačnej schránky
- Do 15 dní úrad rozhodne o zriadení schránky
- Po zriadení schránky podá poplatník prihlášku k nazeraniu do tejto schránky⁵⁹ (elektronicky cez daňový portál)
- Následne je schránka prístupná

Je teda potrebné obstarat' si kvalifikovaný elektronický podpis⁶⁰, podať celkom dve žiadosti a počítať s lehotou 15 dní na zriadenie schránky. Keďže spomenuté žiadosti sa podávajú elektronicky je proces pomerne nenáročný. Navyše podľa informácií ministerstva táto aplikácia nekladie žiadne mimoriadne nároky na technickú vybavenosť užívateľovho počítača[CDS02].

V súčasnosti sú dostupné tieto služby:

- Daň z pridanej hodnoty
- Daň z príjmu fyzických osôb
- Daň z príjmu právnických osôb
- Závislá činnosť
- Dialničná daň
- Daň z nehnuteľností
- Oznámenia podľa § 34 zákona č. 337/1992 Zb.
- Hlásenie platobného sprostredkovateľa
- Obecné písomnosti určené Finančnému úradu

⁵⁸ První certifikační autorita, PostSignum, eIdentity.

⁵⁹ Na základě § 34d zákona č.337/1992 Zb., o správě daní a poplatkov

⁶⁰ Musí obsahovat' Identifikátor Ministerstva práce a sociálních věcí

V priebehu nasledujúceho roku by mali byť spojazené ďalšie služby, ako napr. elektronické doručovanie⁶¹, osobný daňový kalendár⁶² alebo nahliadnutie do evidencie spisov finančného úradu [HN02].

Úspešnosť projektu dokazuje štatistika zverejňovaná Českou daňovou správou [ONL02], podľa ktorej bolo v roku 2006 zatiaľ evidovaných 53727 podaní, čo predstavuje nárast oproti roku 2003 o 1300%.

3.1.4. Služby Ministerstva Informatiky

Ministerstvo informatiky spustilo službu „e-Fakturace“, ktorá slúži pre elektronickú fakturáciu dodávateľov MČR. Táto služba zasiela/doručuje faktúry tak, aby ich bolo možné ďalej spracovávať v účtovacích a fakturovacích systémoch. Do 31.12.2006 je služba v pilotnom štádiu, čiže ju môžu využívať len vybraní dodávatelia MČR.

Naviac ministerstvo poskytuje ročný výkaz o poštových službách PS (MI) za rok 2005.

3.1.5. Služby Českej správy sociálneho zabezpečenia

Klienti ČSSZ môžu využívať elektronickú podateľňu ktorá poskytuje tieto služby [ONL01]:

- Evidenčné listy dôchodkového poistenia

Vedenie ELDP je jednou z povinností organizácií nariadených zákonom o organizácii a vykonávaní sociálneho zabezpečenia č. 582/1991 Zb. Za svojich zamestnancov ich vedú organizácie a sú na nich uvedené doby poistenia, výška zárobku a doby vylúčenia.

- Prihlášky a odhlášky zamestnancov k nemocenskému poisteniu
- Prehľad o príjmoch a výdajoch OSVČ za rok 2005

V roku 2007 by mali byť spojazené ďalšie elektronické služby:

- Potvrdenie o štúdiu (teoretickej a praktickej príprave)
- Oznámenia o nástupe do zamestnania

⁶¹ Výmena informácií medzi správcom dane a poplatníkom pomocou e-mailu

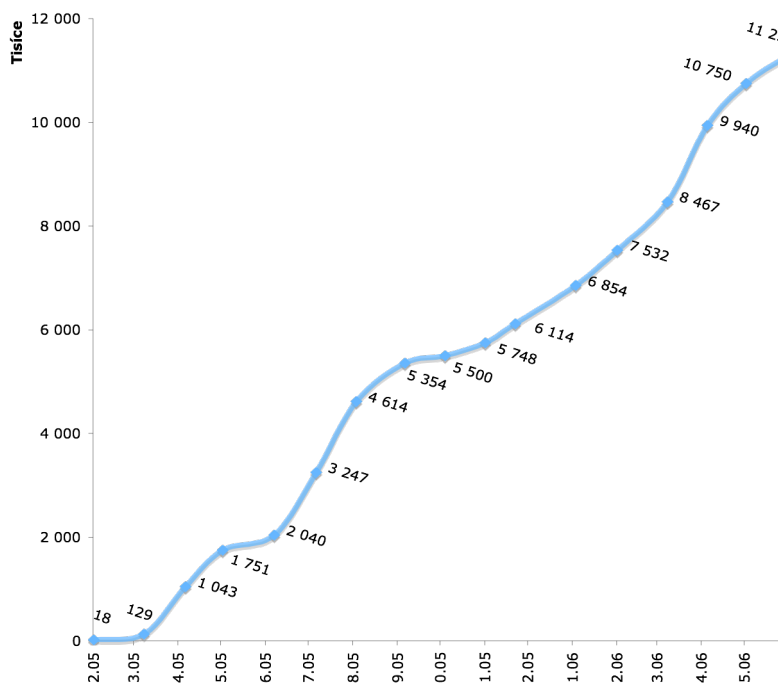
⁶² Prehľad daňových povinností a súvisiacich platieb

▪ Prehľad o príjmoch a výdajoch OSVČ za rok 2006

Do 1.2.2006 vydávala ČSSZ podpisové kľúče ktoré slúžili k zabezpečeniu elektronickej komunikácie. Od tohoto dátumu je pre registráciu k používaniu elektronickej podateľne ČSSZ nutný kvalifikovaný certifikát od jednej z akreditovaných certifikačných autorít [ONL03]. Tento krok zrejme súvisí s cenovou dostupnosťou týchto certifikátov po príchode PSC PostSignum v septembri 2005.

Služby poskytované ČSSZ sa tešia rastúcej obľube. Len počas 8. mesiacov roku 2005 stúpol počet registrovaných užívateľov o viac ako 100% na hodnotu 36549. Počet podaní eELDP stúpol od februára 2005 do 21.6.2006 z 3 219 na 400 453. Služba „prihlášky/odhlášky“ od svojho spustenia v júly 2005, kedy bolo zaznamenaných 24 839 podaní, spracovala k 21.6.2006 celkom 1 148 725 podaní. Za všetky tri prístupné služby bolo prijatých k tomu istému dátumu takmer 10 300 000 záznamov⁶³.

Graf 2 znázorňuje prudký a trvalý nárast počtu prijatých záznamov



Graf 3.2 - Počet prijatých záznamov ČSSZ

Zdroj: ČSSZ, 2006

⁶³ Jedno podanie spravidla obsahuje viac záznamov, napr. v jednom podaní firma obsiahne záznamy za všetkých svojich zamestnancov

3.1.6. Služby Generálneho riaditeľstva ciel

Generálne riaditeľstvo ciel prostredníctvom aplikácií dostupných zo svojich stránok umožňuje colným deklarantom podávať vývozové a dovozové colné prehlásenia elektronicky⁶⁴. Taktiež umožňuje elektronickú komunikáciu v rámci celého colného vybavovania, štatistík a pod.

Donedávna riaditeľstvo ciel poskytovalo kvalifikované certifikáty zadarmo, čomu nastal koniec s príchodom cenovo dostupných certifikátov od PostSignum.

3.1.7. Služby Ministerstva vnútra

Prostredníctvom svojej podateľne umožňuje ministerstvo vnútra podávať napríklad:

- Návrhy na začatie správneho konania
- Návrhy na preskúmanie rozhodnutí
- Žiadosti o vydanie osvedčení, posudkov, vyjadrení a iných podobných opatrení

Vo všeobecnosti prijíma všetky úradné písomnosti v oblasti štátnej správy a trestného konania, kde je ako orgán činný v trestnom konaní príslušný policajný orgán alebo útvar ministerstva vnútra.

3.1.8. Prijatie a spokojnosť so službami

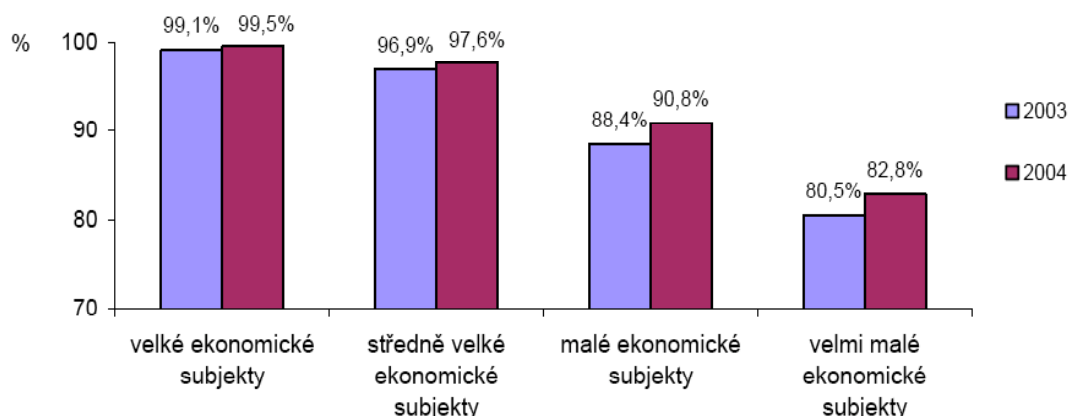
Podľa prieskumu ČSÚ⁶⁵ vykonanom v prvom štvrtroku 2005, využilo Internet pre komunikáciu s verejnou správou celkom 15,5% užívateľov, čo je zhruba 5% obyvateľstva. To predstavuje nárast z 293 tisíc užívateľov v roku 2003 na 432 tisíc, čiže o 67,8 percenta.

Čo sa týka právnických osôb, tie sú vo využívaní elektronickej komunikácie oveľa skúsenejšie, ako dokazuje graf 3. Podľa prieskumu Eurostatu⁶⁶ je v tomto smere ČR na úrovni EÚ 25, a výrazne pred Nemeckom alebo napr. Veľkou Britániou.

⁶⁴ Aplikácia eVývoz

⁶⁵ Šetření o využívání ICT v domácnostech a mezi jednotlivci v roce 2005, ČSÚ

⁶⁶ Community Survey on ICT usage and e-commerce in enterprises for 2004



Zdroj : Výsledky šetření o využívání informačních a komunikačních technologií v podnikatelském sektoru v roce 2004 (2003), ČSÚ

Graf 3.3 - Využívání online komunikácie so štátom

3.1.9. Zhrnutie

Služby českého e-Governmentu sa rýchlo vyvíjajú a už dnes je poskytované množstvo kvalitných služieb, ktoré cez portál verejnej správy uľahčujú komunikáciu najmä firmám. Ako dokazujú štatistiky, obľúbenosť týchto služieb rýchlo stúpa, čo iste do značnej miery súvisí s cenovou a geografickou dostupnosťou kvalifikovaných certifikátov. Ďalším motivačným faktorom je oslobodenie elektronickej agendy od správnych poplatkov, a to až do výšky 2000 CZK.

Do budúca sa počíta so zavádzaním ďalších služieb, ako napríklad prenesenie celej agendy registrácie firiem na Internet, a vylepšovaním existujúcich služieb. Tie sa zatiaľ potýkajú s niektorými technickými nedostatkami typu „fixácia na jeden operačný systém a prehliadač“⁶⁷.

3.2. Využitie elektronického podpisu pri komunikácii s orgánmi štátnej správy vo Francúzsku

Vo Francúzsku je informačná spoločnosť o pár rokov dopredu pred Českou republikou, čomu zodpovedajú aj elektronické služby štátu obyvateľom. Rozsiahly program implementácie e-Governmentu práve vstupuje do finálnej fázy, ale už dnes sú k dispozícii mnohé služby uľahčujúce komunikáciu s úradmi.

Po krátkom úvode do počiatkov Francúzskej informačnej spoločnosti bude nasledovať popis zavádzania elektronickej komunikácie s verejnou správou a

⁶⁷ Transakčná časť daňového portálu vyžaduje Internet Explorer 6 a vyšší, a tým pádom operačný systém Windows

jednotlivých služieb dostupných občanom a firmám. Záver kapitoly ponúka stručné zhrnutie. Informácie v tejto kapitole boli čerpané hlavne z [IDAB02].

3.2.1. Počiatky informatizácie Francúzskej spoločnosti

Na počiatku informatizácie spoločnosti vo Francúzsku stál projekt⁶⁸ Ministerstva vnútra, ktorý mal unikátnym numerickým identifikátorom prepojiť elektronické spisy obsahujúce osobné údaje.

O existencii tohto projektu informoval denník *Le Monde* v polovici sedemdesiatych rokov. Po zverejnení bol projekt ihneď pozastavený nariadením premiéra, ktoré zakázalo prepojovanie administratívnych databáz, kým sa neurčia presné pravidlá automatického spracovávanía dát. V roku 1978 bola publikovaná správa o „Informatizácii spoločnosti“ volajúca po celonárodnej iniciatíve v odbore nazvanom „Telematika“, ktorá mala byť postavená na myšlienke služby verejnosti. Následným prijatím zákona o „Informatike a Slobode“ sa Francúzsko stalo jednou z prvých krajín s legislatívou upravujúcou ochranu dát.

Nasledujúci rok vyhlásila vláda ambiciózny plán rozvoja telematiky založený na vývoji a distribúcii lacného terminálu umožňujúceho prístup k elektronickému telefónnemu zoznamu a iným verejným a komerčným službám – Minitel⁶⁹. Francúzi sú teda s elektronickou komunikáciou oboznámení už dlhšiu dobu.

3.2.2. Projekt ADELE

S príchodom Intrernetu a rozmachom informačných technológií prišla potreba adaptovať komunikáciu štátu s občanmi. Túto potrebu rieši plán *ADELE*⁷⁰, zverejnený 9.2.2004. Obsahuje postup vývoja a nasadenia elektronických služieb, ktoré môžu občania a firmy očakávať najneskôr do konca roku 2007.

Hlavnými strategickými cieľmi ADELE sú:

- *Uľahčiť život občanom, firmám a miestnym autoritám poskytnutím množstva užívateľsky príjemných služieb dostupných všade a všetkým*

⁶⁸ Kódové meno SAFARI – „système automatisé pour les fichiers et le répertoire des individus“

⁶⁹ Minitel je zariadenie pre prístup cez uzatvorenú sieť k službám založeným na Videotexe. Obľúbenosť minitelu bola obrovská, a to až do takej miery že brzdila nástup Internetu, pretože Francúzi so svojou typickou hrdosťou na „svoju“ technológiu ho odmietali prijať. Minitel funguje dodnes.

⁷⁰ *Administration Electronique* – <http://adele.gouv.fr>

- *Vytvoriť dôveru* garantovaním bezpečnosti dát a ich tajnosti. Toho má byť dosiahnuté použitím bezpečných systémov identifikácie a možnosti kontroly používania svojich dát verejnými orgánmi.
- *Prispieť k modernizácii verejnej správy* vylepšením práce verejných zamestnancov a organizácie verejných služieb, a dopomáhať k zníženiu vládnych výdavkov⁷¹

Pre dosiahnutie týchto cieľov sa plán ADELE delí na 140 projektov. Z týchto sú zaujímavé napríklad:

- Vytvorenie personalizovaného administratívneho „priechodu“ – <http://mon.service-public.fr>, ktorý zaistí bezpečný a personalizovaný prístup ku všetkým dostupným verejným službám
- Zavedenie elektronického občianskeho preukazu, ktorý nahradí doterajšie preukazy a umožní jednoduchšie a bezpečnejšie jednanie s vládou a uľahčí niektoré procesy, ako napr. žiadosti o pas
- Zavedenie centralizovanej online služby ohlásenia zmeny adresy
- Prestup k plne elektronickému vydávaniu zbierky zákonov⁷², čo má ušetriť 6 ton papiera denne.

3.2.3. Dostupné služby Francúzskeho e-Governmentu

Podobne ako v Českej republike, aj vo Francúzsku existuje portál – <http://www.service-public.fr> - zastrešujúci jednotlivé služby e-Governmentu a poskytujúci prístup k informáciám pre občanov a firmy. K dnešnému dňu je údajne elektronicky dostupných 60% všetkých dokumentov a formulárov potrebných ku komunikácii s francúzskou verejnou správou⁷³. V blízkej budúcnosti sa má spustiť projekt personalizovaného portálu <http://mon.service-public.fr> ktorý má okrem personalizácie služieb a vzhľadu umožniť jednotné ukladanie dokumentov potrebných pre komunikáciu so štátnou správou a iných súvisiacich dokumentov.

3.2.3.1. Dane

Francúzsky daňový portál „impots.gouv.fr“ umožňuje výpočet, priznanie a platenie dane z príjmu fyzických aj právnických osôb ako aj iných daní. V roku 2005

⁷¹ Predpokladané úspory vládnych výdavkov nasadením ADELE: 5 až 7 mld. EUR ročne

⁷² Journal Officiel

⁷³ V roku 2008 by už mali byť takto dostupné všetky dokumenty

bolo elektronicky uskutočnených 3,74 milióna „navrátení dane z příjmu (income tax returns)“, čo predstavuje 11% z celkového počtu a tvorí trojnásobný nárast oproti roku 2004. V roku 2006 bolo elektronicky podaných 5,7 milióna daňových priznaní, čiže o 2 mil. viac ako v roku 2005.

Tohto roku bol systém daňových priznaní zjednodušený – jednotlivci už nemusia nič vyplňať ani nie sú potrebné ďalšie dokumenty. Daňové priznanie je predvyplnené daňovým úradom, je tu ale stále možnosť online doplnenia alebo opravy.

Pre komunikáciu s aplikáciou nie je potrebné zakúpiť kvalifikovaný certifikát. Ten je na základe žiadosti dodaný bezplatne a má platnosť až tri roky.

Podobne ako v ČR aj vo Francúzsku sa dá podaním elektronického podania ušetriť, a to formou zľavy 20 EUR z dlžnej čiastky. Navyše je pre elektronické podania predĺžená doba, dokiaľ je možné priznať daň, o jeden mesiac.

DPH môžu firmy priznávať a platiť cez aplikáciu Ministerstva ekonomiky, financií a priemyslu na <http://tva.dgi.minefi.gouv.fr/>

3.2.3.2. Trh práce

Národná agentúra pre zamestnanosť – ANPE - prevádzkuje plne funkčnú aplikáciu pre hľadanie práce, kde užívatelia prezerajú ponuky a zverejňujú svoje životopisy⁷⁴.

3.2.3.3. Štátna podpora

- *Podpora v nezamestnanosti* – prostredníctvom asociácie nezamestnanecského poistenia⁷⁵ majú užívatelia prístup k informáciám o podpore, môžu sa online registrovať a sledovať svoj štatút nezamestnaného
- *Prídavky na deti* – online deklarácia výšky príjmu, sťahovanie formulárov, sledovanie platieb a prijatých platieb⁷⁶
- *Študentské pôžičky* – online informácie o typoch pôžičiek a podanie žiadostí o ne⁷⁷

⁷⁴ ANPE – <http://www.anpe.fr/>

⁷⁵ ASSEDIC – <http://www.assedic.fr>

⁷⁶ CNAF – <http://www.caf.fr>

⁷⁷ CNOUS – <http://www.cnous.fr>

- *Zdravotné výdavky* – priame vyrovnanie niektorých nákladov pomocou Sesam-Vitale⁷⁸ smart kariet zdravotného poistenia, online sledovanie platieb⁷⁹

3.2.3.4. Ostané služby pre fyzické osoby

Okrem už spomenutej možnosti ohlásiť zmenu bydliska online je vo Francúzsku občanom dostupných veľa ďalších elektronických služieb:

- *Doručovanie rodných a sobášnych listov*
- *Knížničné služby* – chat s knihovníkom, objednávanie kníh a miest v čítárni
- *Doručovanie výpisov z trestného registru*
- *Registrácia motorových vozidiel* - informácie a formuláre na stiahnutie⁸⁰. Pri kúpe nového vozidla sa žiadosti o registráciu posielajú elektronicky priamo od predajcu.

3.2.3.5. Služby pre právnicke osoby

- *Colná deklarácia*⁸¹
- *Podávanie údajov štatistickému úradu*⁸²
- *Registrácia novej firmy*⁸³
- *Verejné obstarávanie* – Od 1.1.2005 sú všetky verejné orgány povinné prijímať elektronické ponuky na formálne vyhlásené tendre. Všetky ministerstvá, s výnimkou ministerstva obrany⁸⁴, môžu túto požiadavku splniť použitím celoštátnej platformy verejného obstarávania⁸⁵. Táto umožňuje publikovanie vyhlásených tendrov a prijímať elektronické ponuky.

3.2.4. Prijatie a spokojnosť so službami

Podľa štúdie firmy Capgemini [CAPG01] vykonanej v roku 2005 využilo služby e-Governmentu 75% používateľov Internetu, čo predstavuje nárast o 7% oproti

⁷⁸ www.sesam-vitale.fr

⁷⁹ CNOUS – <http://www.cnous.fr>

⁸⁰ [http://vosdroits.service-public.fr/particuliers/N533.xhtml?&n=Transports&l=N18&n=Automobiles et deux-roues&l=N529](http://vosdroits.service-public.fr/particuliers/N533.xhtml?&n=Transports&l=N18&n=Automobiles%20et%20deux-roues&l=N529)

⁸¹ <http://www.douane.gouv.fr/>

⁸² SESSI - <http://www.sessi.fr/>

⁸³ <http://www.cfenet.cci.fr/>

⁸⁴ Toto ministerstvo má vlastný portál

⁸⁵ <http://www.marches-public.gouv.fr>

roku 2004. Tieto pozitívne výsledky sú dôsledkom zvýšenej intenzity používania Internetu (32% Francúzov je online každý deň) a zvýšeného celkového počtu jeho užívateľov (okolo 50% Francúzov má pripojenie k Internetu). Medzi najnavštevovanejšie stránky patrí www.anpe.fr patriace Národnej agentúre pre zamestnanosť.

Okrem zvýšeného počtu užívateľov online služieb štátu štúdia odhalila aj zvýšenú spokojnosť s nimi: 83% opýtaných bolo spokojných s dostupnosťou informácií a 78% považuje tieto služby za dostatočne jednoduché

3.2.5. Zhrnutie

Francúzsko zaviedlo v posledných rokoch kvalitné služby umožňujúce jednoduchý prístup k agendám jednotlivých úradov verejnej moci, čím nadviazalo na svoju tradíciu informatizácie spoločnosti. Národný plán zavádzania e-Governmentu ADELE má do konca roku 2007 sprístupniť na internete všetky formuláre a dokumenty potrebné pre komunikáciu s úradmi. Pre tento účel bol vytvorený portál service-public.gouv.fr, ktorý slúži ako rozcestník k jednotlivým aplikáciám a službám.

Výhodou francúzskych služieb je, že často nevyžadujú zakúpenie kvalifikovaného certifikátu. Ten je distribuovaný zadarmo, navyše projekt ADELE počítá so zavedením elektronického občianskeho preukazu, ktorý v sebe bude obsahovať súkromný kľúč⁸⁶

3.3. Porovnanie dostupných služieb

Porovnávanie legislatívy založenej na spoločnom základe neprináša veľký úžitok. Naopak ako zaujímavé sa javí porovnanie prenesenia tejto legislatívy do konkrétnych aplikácií a služieb. Ako bolo spomenuté v kapitole o možnostiach využitia elektronického podpisu, jeho uplatnenie je naozaj široké a zasahuje do všetkých sfér komunikácie. Preto sa táto práca obmedzila na preskúmanie zavedenia elektronického podpisu a jeho použitia orgánmi, ktoré vytvorili legislatívu upravujúcu jeho použitie. Na nasledujúcich stranách sa teda nachádza porovnanie zavedených služieb e-Governmentu v ČR a Francúzsku.

⁸⁶ Keďže tieto preukazy vydáva štát, odpadá problém overenia kvalifikácie certifikátu

3.3.1. Dostupnosť kvalifikovaných certifikátov

ČR aj Francúzsko vyžadujú pri komunikácii so službami poskytovanými štátom zaručený elektronický podpis. Pred samotným zhodnotením jednotlivých služieb je teda treba načrtnúť, ako sú na tom obe krajiny s dostupnosťou kvalifikovaných certifikátov. Nasledujúca tabuľka udáva počet akreditovaných PCS a orientačné ceny týchto certifikátov.

	ČR	FR
počet PCS	3	16 ⁸⁷
cena certifikátu	190	0 až 57EUR

Tabuľka 3.1 - Počet PCS a cena certifikátov na jeden rok

Vo Francúzsku je teda vyše 5 krát viac PCS ako v ČR a certifikáty sú často poskytované zadarmo⁸⁸, čo má zrejme súvis s väčším rozšírením Internetu a zrejme aj sociálnejšie založenou kultúrou. Univerzálne certifikáty sú tu ale výrazne drahšie. Tu sa vynára otázka praktickej prenositeľnosti kvalifikovaných certifikátov z iných členských krajín.

3.3.2. Metodológia

Za účelom kategorizácie jednotlivých služieb a ich následného porovnania bolo prebratých 20 základných verejných služieb definovaných v dokumente [IDAB03]. Tieto sú ďalej rozdelené na 12 služieb fyzickým osobám:

- Služby spojené s daňou z príjmu
- Hľadanie práce (cez úrady práce)
- Príspevky na sociálne zabezpečenie (Social Security Contributions)
- Osobné dokumenty
- Registrácia motorových vozidiel
- Žiadosti o povolenie k stavbe
- Podania polícii
- Verejné knižnice
- Rodné a sobášne listy – žiadosť a doručenie
- Prihlášky na vysoké školy
- Oznámenia zmeny adresy

⁸⁷ Podľa [ONL05]

⁸⁸ Tieto sú zvyčajne viazané na konkrétnu službu. Napr. daňový portál impots.gouv.fr poskytuje trojročný certifikát zadarmo po zadaní unikátneho identifikátora daňového poplatníka

- Zdravotné služby (zistovanie dostupnosti služieb v nemocniciach, dohováranie návštev...)

a 8 služieb pre fyzické osoby

- Sociálne prídavky zamestnancom (Social Contributions to Employees)
- Korporátna daň
- Daň z pridanej hodnoty
- Registrácia firmy
- Podávanie údajov štatistickému úradu
- Colná deklarácia
- Povolenia týkajúce sa životného prostredia
- Verejné obstarávanie

Ďalej bola použitá metodológia EÚ pre benchmarking online dostupnosti a sofistikovanosti služieb e-Governmentu [IDAB04]. Obidva dokumenty ([IDAB03] a [IDAB04]) boli schválené Radou Európy v marci 2001 v Štokholme. V stručnosti táto metodológia zavádza 4 úrovne sofistikovanosti služieb:

1. *Informácia* – online informácie o verejných službách
2. *Interakcia* – sťahovanie formulárov
3. *Obojstranná interakcia* – spracovanie formulárov, vrátane autentizácie
4. *Transakcia* – plnohodnotné vybavovanie, rozhodovanie a doručovanie (platby)

3.3.3. Zhodnotenie služieb vo Francúzsku

Tabuľka 2 ukazuje dosiahnutú úroveň jednotlivých typov služieb pre fyzické osoby oproti najvyššej možnej hodnote.

Popis služby	Dosiahnutá úroveň	Najvyššia možná úroveň
Služby spojené s daňou z príjmu	4	4
Hľadanie práce (cez úrady práce)	4	4

Popis služby		Dosiahnutá úroveň	Najvyššia možná úroveň
Príspevky na sociálne zabezpečenie	Príspevky v nezamestnaní	4	4
	Detské príspevky	4	4
	Zdravotné výdavky	4	4
	Študentské granty	4	4
Osobné Dokumenty	Pas	1	3
	Vodičský preukaz	2	3
Registrácia motorových vozidiel		3	4
Žiadosti o povolenie k stavbe		3	4
Podania polícii		2	3
Verejné knižnice		4	4
Rodné a sobášne listy		3	3
Prihlášky na vysoké školy		3	4
Oznámenia zmeny adresy		3	3
Zdravotné služby		1	4

Tabuľka 3.2 – úroveň služieb pre fyzické osoby vo Francúzsku

Tabuľka 3.3 ukazuje dosiahnutú úroveň jednotlivých typov služieb pre právnicke osoby oproti najvyššej možnej hodnote

Popis služby	Dosiahnutá úroveň	Najvyššia možná úroveň
Sociálne prídavky zamestnancom	4	4
Korporátna daň	4	4
Daň z pridanej hodnoty	4	4
Registrácia firmy	3	4
Podávanie údajov štatistickému úradu	3	3
Colná deklarácia	4	4
Povolenia týkajúce sa životného prostredia	2	4
Verejné obstarávanie	4	4

Tabuľka 3.3 - úroveň služieb pre právnicke osoby vo Francúzsku

3.3.4. Zhodnotenie služieb v Českej Republike

Analogicky k tabuľkám 3.2 a 3.3 ukazujú tabuľky 3.4 a 3.5 úroveň jednotlivých služieb v Českej Republike.

Popis služby		Dosiahnutá úroveň	Najvyššia možná úroveň
Služby spojené s daňou z príjmu		4	4
Hľadanie práce (cez úrady práce)		3	4
Príspevky na sociálne zabezpečenie	Príspevky v nezamestnaní	2	4
	Príspevky na rodinu	4	4
	Zdravotné výdavky	4	4
	Študentské granty	n/a	4
Osobné dokumenty	Pas	1	3
	Vodičský preukaz	1	3
Registrácia motorových vozidiel		1	4
Žiadosti o povolenie k stavbe		1-2	4
Podania polícii		3	3
Verejné knižnice		1	4
Rodné a sobášne listy		1-2	3
Prihlášky na vysoké školy		2-3	4
Oznámenia zmeny adresy		1	3
Zdravotné služby		0-1	4

Tabuľka 3.4 - úroveň služieb pre fyzické osoby v ČR

Popis služby		Dosiahnutá úroveň	Najvyššia možná úroveň
Sociálne prídavky zamestnancom		3	4
Korporátne daň		4	4
Daň z pridanej hodnoty		4	4
Registrácia firmy		3	4
Podávanie údajov štatistickému úradu		3	3
Colná deklarácia		4	4
Povolenia týkajúce sa životného prostredia		1-2	4
Verejné obstarávanie		4	4

Tabuľka 3.5 - úroveň služieb pre právnické osoby v ČR

Poznámky:

- *Rodné a sobášne listy* – len niektoré miestne úrady poskytujú formuláre online
- *Oznámenia zmeny adresy* – v roku 2006 má byť na portáli verejnej správy spustená jednotná oznamovacia služba pre zmenu adresy
- *Verejné obstarávanie* – dosiahnutá úroveň uvedená v tabuľke počíta so spojením objednávacích a fakturačných procedúr na www.centralni-adresa.cz
- *Verejné knižnice* – neexistuje centrálna správa. Nie všetky knižnice ponúkajú služby cez internet.
- *Podania na políciu* – na rozdiel od úrovne uvedenej v [IDAB01] sú tieto služby skôr na úrovni 3, súdiac z informácií v kapitole 7.7
- *Študentské granty* – v ČR sú doménou súkromného sektoru

3.4. Porovnanie a zhrnutie

V oblasti služieb fyzickým osobám bolo možné dosiahnuť maximálne 59 bodov, v prípade právnických osôb potom 33 bodov. Agregovanú úroveň sofistikovanosti služieb v oboch krajinách vyjadruje tabuľka 3.6

služby	úroveň	ČR	FR
fyzickým osobám	dosiahnutá	33	49
	možná celkom	59	
	v %	56%	83%
právnickým osobám	dosiahnutá	27	28
	možná celkom	31	
	v %	87%	90%
	celkovo v %	66,7%	85,6%

Tabuľka 3.6 – porovnanie sofistikovanosti služieb

Ako je vidno, Česká republika v zavádzaní elektronických služieb občanom výrazne zaostáva za Francúzskom, ktoré ponúka o 27% lepšie služby. Naopak v hodnotení služieb firmám Francúzsko získalo len o jeden bod viac ako ČR, ktorej do najvyššieho možného hodnotenia chýbajú len 4 body.

Problematické sú v Čechách najmä služby elektronického žiadania o študentské granty, online oznámenia o zmene adresy, služby verejných knižníc, registrácia motorových vozidiel a služby spojené s poskytovaním študentských grantov. Ako však vyplýva z poznámok pod tabuľkami 3.4 a 3.5, situácia je v skutočnosti o čosi lepšia – čoskoro bude dostupná centrálna online adresa pre oznamovanie zmeny bydliska a viaceré verejné knižnice štandardne ponúkajú online služby. Takisto

porovnávanie centralizovaných online pôžičiek študentom nie je celkom smerodajné, keďže v ČR sú podobné produkty zväčša⁸⁹ doménou súkromného sektoru.

Obe porovnávané krajiny majú ešte nedostatky v kategóriách „osobné dokumenty“ a „zdravotné služby“, v oblasti služieb pre právnické osoby potom v kategórii „životné prostredie“.

⁸⁹ Medzi tieto produkty patrí aj služba udeľovania ubytovacích štipendií v rámci VŠE, ktorá môže byť považovaná za štátnu službu.

4. Záver

Cieľom tejto bakalárskej práce bolo poskytnúť prehľad o legislatívnej úprave problematiky elektronického podpisovania v Českej Republike a Francúzsku a ich následné porovnanie, vrátane prenesenia zákonodarstva do praktických aplikácií verejnej správy. Prínos práce spočíva v popise legislatívneho rámca upravujúceho elektronický podpis vo Francúzsku, jeho súčasného praktického využitia vo verejnej sfére Česka a Francúzska, a hlavne v zhodnotení odlišností legislatív a úrovne využitia v týchto krajinách.

Práca je logicky rozdelená do troch častí. Prvá popisuje princíp a možnosti využitia elektronického podpisu, druhá sa venuje legislatíve a tretia súčasným využitím elektronického podpisu v aplikáciách e-Governmentu.

Na začiatok je pre lepšiu orientáciu v problematike zaradený popis princípu fungovania elektronického podpisu, ktorý spočíva v použití asymetrického šifrovania pomocou súkromného a verejného kľúča a overovania identity dôveryhodnou treťou stranou - poskytovateľom certifikačných služieb.

Druhá podkapitola prvej časti sa zaoberá možnosťami využitia elektronického podpisu v praktických aplikáciách. Tých je skutočne nespočetne veľa - elektronický podpis je využiteľný nielen tam, kde bol doteraz vyžadovaný podpis ručný, ale aj v prípadoch, kde takýto spôsob nebol možný (databázy, fotografie, hudobné diela atď).

Legislatíva jednotlivých členských štátov EU je založená na Smernici EU o elektronickom podpise, ktorú musia preniesť do svojho zákonodarstva. Je formulovaná technologicky neutrálne a umožňuje tak aby sa technologický vývoj nemusel premietat' do novelizácií. Zrovnoprávňuje elektronický podpis s ručným, nariaďuje vzájomné uznávanie kvalifikovaných certifikátov, určuje právne účinky a zavádza jednotnú terminológiu. Kapitola 2.1 obsahuje základné myšlienky tejto Smernice ako aj následné doplnujúce rozhodnutia upravujúce niektoré podrobnosti.

Kapitola 2.2 prináša stručný pohľad na českú legislatívu, ktorá je po niekoľkých novelizáciách v súlade so Smernicou EU. Zákon 227/2000 Zb. v znení neskorších predpisov zavádza ďalšie termíny nad jej rámec, hlavne "časové pečiatky", "elektronická značka", "systémový certifikát" a "elektronická podateľňa". Elektronický

podpis je zrovnoprávený doplnením a zmenou niektorých článkov Občianskeho zákoníku. Tejto problematike sa venuje viacero publikácií, bakalárskych a diplomových prác na ktoré sa v piatej kapitole odkazuje – táto práca si preto nerobí nároky na podanie vyčerpávajúcej správy o českej legislatíve elektronického podpisu.

Kapitola 2.3 sa zaoberá elektronickým podpisom v zákonodarstve Francúzska, ktorého stručný opis sa nachádza na začiatku kapitoly. Tamojšie zákony sa taktiež opierajú o Smernicu EU a podobne ako zákon 227/2000 v ČR, tak aj francúzsky zákon 2000-230 zrovnoprávňuje elektronický podpis úpravou Občianskeho zákoníku. Tento zákon ale nepreniesol základné myšlienky Smernice, a tak nasledovalo niekoľko dopĺňujúcich zákonov, uznesení a dekrétov, hlavne dekrét č. 2001-272 ktorý ju viacmenej kopíruje. Za zmienku taktiež stojí uznesenie z 26.7.2004 zavádzajúce systém trojstupňovej hierarchie autority pre certifikáciu PCS.

Uzatvorením druhého logického celku práce je tretia podkapitola (2.3) porovnávajúca zákony o elektronickom podpise oboch štátov. Z formálneho hľadiska je tu rozdiel v používaní odlišných právnych textov - kým v ČR sa úprava používania elektronického podpisu prevádza skôr cez zákony, vo Francúzsku sú to rôzne uznesenia, dekréty a odporúčania odborných komisií.

Z praktického hľadiska sú tu dva väčšie rozdiely, a to v systéme akreditácie resp. certifikácie PCS a vyžadovaním kvalifikovaných certifikátov v komunikácii s verejnou správou. V ČR udeľuje akreditácie priamo Ministerstvo Informatiky, kým vo Francúzsku existuje ešte jeden medzistupeň. Vo Francúzsku sú k niektorým aplikáciám poskytované certifikáty zadarmo (a teda nie sú kvalifikované podľa zákona), zatiaľ čo v ČR je pre využívanie elektronických služieb štátu potrebné zakúpiť kvalifikovaný certifikát.

Z časového hľadiska bola legislatíva v oboch krajinách prijímaná zhruba v rovnakom časovom rozmedzí, až na jednu výnimku. Inak majú obidva štáty veľmi podobné podmienky pre používanie elektronického podpisu, zákony sú (po niekoľkých novelizáciách) uvedené do súladu so Smernicou a inými predpisy Únie.

Tretia a posledná logická časť začína zmapovaním dostupných služieb eGovernmentu v ČR a Francúzsku. Prvá podkapitola (3.1) skúma elektronické aplikácie jednotlivých českých ministerstiev a orgánov štátnej správy, ktoré sú sprístupnené cez

Portál Verejnej Správy. Ako dokazujú grafy a štatistiky, tieto služby sa tešia rastúcej obľube. Využíva ich dokonca viac užívateľov Internetu ako v Nemecku alebo Veľkej Británii.

Kapitola (3.2) sa zaoberá službami Francúzskeho eGovernmentu. Tieto sú na celkovo vyššej úrovni čo sa týka počtu ale aj užívateľskej príťažlivosti. Napríklad je možné v jednej aplikácii oznámiť zmenu bydliska všetkým potrebným orgánom. Do roku 2008 má vládny program elektronickej administratívy ADELE sprístupniť všetky formuláre a dokumenty potrebné ku komunikácii so štátnou správou. Obľúbenosť týchto služieb je vysoká a rastúca, používa ich 75% francúzskych používateľov Internetu.

Posledné dve subkapitoly tretej časti porovnávajú úroveň sofistikovanosti služieb eGovernmentu v oboch krajinách. Pre tento účel bolo zvolených 20 kategórií služieb a ich hodnotenie bolo vykonané podľa metodiky Európskej Únie, ktorá zavádza 4 stupne sofistikovanosti. Ďalej boli služby rozdelené podľa určenia buď fyzickým alebo právnickým osobám. Výsledky sú znázornené v prehľadných tabuľkách.

Česká republika je v službách občanom výrazne pozadu za Francúzskom, ale firmám ponúka služby na takmer rovnakej (vysokej) úrovni. To zrejme zčasti vysvetľuje vysokú popularitu týchto služieb vo firmách, zatiaľ čo bežný občan ich využíva ďaleko menej.

Problematické sú v Čechách najmä služby elektronickeho žiadania o študentské granty, online oznámenia o zmene adresy, služby verejných knižníc, registrácia motorových vozidiel a služby spojené s poskytovaním študentských grantov. Obe porovnávané krajiny majú ešte nedostatky v kategóriách „osobné dokumenty“ a „zdravotné služby“, v oblasti služieb pre právnické osoby potom v kategórii „životné prostredie“.

Elektronický podpis sa za 5 rokov od svojho zrovnoprávnenia s klasickým podpisom stal bežnou realitou vo firmách a stále viac ľudí si osvojuje tento užitočný nástroj. Legislatívne je dnes jeho používanie upravené dostatočne komplexne aby nevznikali zbytočné nedorozumenia. Zároveň sú hlavné zákony formulované technologicky neutrálne, čím je zabezpečená ich platnosť aj do budúcnosti. Zosúladením so Smernicou zákony o elektronickej podpise umožňujú voľný pohyb

služieb certifikačných autorít v rámci Únie, čo bolo jedným z hlavných dôvodov jej vzniku. Prívetká závislosť na únijných smerniciach však znamená neochotu jednotlivých vlád prijímať nové zákony, kým nie je jasný ďalší postup európskych zákonodarcov. V prípade pomalého reagovania na vývoj problematiky tak môže EÚ brániť vytváraniu efektívnej právnej úpravy.

Ďalšiemu rozmachu elektronického podpisu a služieb eGovernmentu s ním spojených už dnes v ceste nestojí cenová nedostupnosť kvalifikovaných certifikátov alebo právna neistota okolo ich používania. Štúdia Capgemini [CAPG01] poukazuje na zložitosť aplikácií, užívateľskú „neprívetivosť“ a používanie príliš odbornej terminológie ako hlavné faktory nespokojnosti s týmito službami vo Francúzsku. Taktiež je v tejto súvislosti spomínaný strach z úniku informácií a preferencia osobného kontaktu. Tieto závery by mali byť použité pri zavádzaní „chýbajúcich“ a služieb v Českej republike.

5. Zoznam použitej literatúry

- [CAPG01] **Capgemini Consulting.** *E-Administration : 2005, l'année du changement.* Paris : [s.n.], 2005. 2 s. Dostupný z WWW: <http://www.fr.capgemini.com/m/fr/n/pdf_e-Administration__2005__l__ann__e_du_changemen t.pdf>
- [CDS02] *Základní informace k Daňovému portálu.* [s.l.] : [s.n.], 2006. 1 s. Leták. Dostupný z WWW: <http://cds.mfcr.cz/sys/cds/pdf/PDF_Udesky/Letak.pdf>
- [EPR01] **JEDLIČKA, Vojtěch.** *Elektronický podpis – Princip elektronického podepisování.* ePravo.cz [online]. 2006 [cit. 2006-10-18]. Dostupný z WWW: <<http://www.epravo.cz/v01/tisk.php3?typ=clanky&recid=13244>>
- [EPR02] *Elektronický podpis – Princip elektronického podepisování.* ePravo.cz [online]. 2006 [cit. 2006-10-18]. Dostupný z WWW: <http://www.epravo.cz/v01/index.php3?s1=1&s2=X&s3=X&s4=X&s5=S&s6=1&m=1&recid_cl=45007&typ=clanky>
- [HASO01] **HASMAN, Ondřej.** *Elektronický podpis a poskytovatelé certifikačních služeb.* [s.l.], 2005. 76 s. , 3 Vysoká Škola Ekonomická. Vedoucí diplomové práce Doc. Ing. Prokop TOMAN, CSc.
- [HN01] **ŠTÍCHOVÁ, Kateřina.** *Časové razítko pohlídá platnost smluv.* Hospodářské noviny. 10.8.2006, č. 154, s. 22. Dostupný z WWW: <http://www.epravo.cz/v01/index.php3?s1=1&s2=X&s3=X&s4=X&s5=S&s6=1&m=1&recid_cl=42554&typ=clanky>
- [HN02] **ŠTÍCHOVÁ, Kateřina.** *Daně přes internet v ostrém režimu.* Hospodářské noviny. 09.10.2006, č. 195, s. 30. Dostupný z WWW: <<http://www.epravo.cz/v01/tisk.php3?typ=clanky&recid=43840>>
- [HN03] **Redakce, (ep),** Současnost a budoucnost virtuální komunikace s úřady. Hospodářské noviny. 03.04.2006, č. 066, s. 06

- komerční příloha. Dostupný z WWW:
<<http://www.epravo.cz>>

- [IDAB01] **IDABC - eGovernment observatory.** eGovernment in the Czech Republic. [s.l.] : [s.n.], 2006. 26 s. Dostupný z WWW:
<<http://ec.europa.eu/idabc/servlets/Doc?id=26303>>
- [IDAB02] **IDABC - eGovernment observatory.** eGovernment in France. [s.l.] : [s.n.], 2006. 30 s. Dostupný z WWW:
<<http://ec.europa.eu/idabc/servlets/Doc?id=26656>>
- [IDAB03] *Common list of basic public services.* [s.l.] : [s.n.], 2001. 1 s. Dostupný z WWW:
<<http://ec.europa.eu/idabc/servlets/Doc?id=18402>>
- [IDAB04] **EU eGovernment working group.** *eGovernment Indicators for Benchmarking eEurope.* [s.l.] : [s.n.], 2001. 4 s. Dostupný z WWW:
<<http://ec.europa.eu/idabc/servlets/Doc?id=18401>>
- [ONL01] **ČSSZ.** *e-Podání* [online]. [2006] [cit. 2006-10-18]. Dostupný z WWW: <<http://www.cssz.cz/epodani/epodani.asp>>
- [ONL02] *Statistika České daňové správy* [online]. 2006 [cit. 2006-10-18]. Dostupný z WWW: <<http://cds.mfcr.cz>>
- [ONL03] **ČSSZ.** *Evidenční listy důchodového pojištění - platné od 1.1.2004* [online]. [2006] [cit. 2006-10-18]. Dostupný z WWW:
<http://www.cssz.cz/tiskopisy/ELDP_2004/evidencni_listy_2004.asp>
- [ONL04] **ČSSZ.** *Evidenční listy důchodového pojištění.* [s.l.] : [s.n.], 2006. 2 s. Dostupný z WWW:
<http://www.cssz.cz/tisk/zdroje/letaky_epodani/ELDP_CZ.pdf>
- [ONL05] *Catégories (familles) de certificats référencés PRIS v 1* [online]. 2006 [cit. 2006-11-20]. Dostupný z WWW:
<<http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-references-pris-v1/categories-familles-certificats-references-pris-v-1-506.html#2>>
- [SME01] **SMEJKAL, Vladimír.** *Zákon o elektronickém podpisu* [online]. [2000] [cit. 2006-10-18]. Dostupný z WWW:
<<http://www.shopfinder.cz/svet/clanek.asp?ID=43>>

Zákony

- [VYH01]** Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb
- [ROZ01]** Rozhodnutí Komise č. 2000/709/ES ze dne 6. listopadu 2000 o minimálních kritériích, ke kterým by členské státy měly přihlížet při jmenování subjektů uvedených v čl. 3 odst. 4 směrnice 1999/93/ES Evropského parlamentu a Rady o zásadách Společenství pro elektronické podpisy
- [NAR01]** Nařízení vlády č. 495/2004 Sb, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- [ROZ02]** Rozhodnutie 2003/511/ES o zverejnení referenčných čísel obecně uznávaných štandardov pre zariadenia pre tvorbu elektronických podpisov
- [ZAK01]** Zákon č.227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- [ZAK02]** Zákon č. 517/2002 Sb., kterým se provádějí některá opatření v soustavě ústředních orgánů státní správy a mění některé zákony
- [ZAK03]** Zákon č. 440/2002 Sb., kterým se mění zákon č.227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů ve, znění pozdějších předpisů
- [ZAK04]** Loi 2000-230 du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- [DEC01]** Décret n°2001-272 du 30 mars 2001 Décret pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- [DEC02]** Décret n°2002-535 du 18 avril 2002 Décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information
- [UZN01]** Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation

- [ZAK05]** Loi n°2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique
- [ZAK06]** Loi n°2004-801 du 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

6. Zoznam tabuliek a grafov

Tabuľka 3.1 - Počet PCS a cena certifikátov na jeden rok.....	46
Tabuľka 3.2 – úroveň služieb pre fyzické osoby vo Francúzsku	48
Tabuľka 3.3 - úroveň služieb pre právnické osoby vo Francúzsku.....	48
Tabuľka 3.4 - úroveň služieb pre fyzické osoby v ČR.....	49
Tabuľka 3.5 - úroveň služieb pre právnické osoby v ČR.....	49
Tabuľka 3.6 – porovnanie sofistikovanosti služieb	50
 Graf 3.1 - Počet podaní cez portál verejnej správy	35
Graf 3.2 - Počet prijatých záznamov ČSSZ.....	38
Graf 3.3 - Využívanie online komunikácie so štátom	40
 Obrázok 2.1 – Hierarchia autority	24

7. Príloha – Smernica EÚ o elektronickom podpise

Úřední věstník L 013 , 19/01/2000 S. 0012 - 0020

Směrnice Evropského parlamentu a Rady 1999/93/ES
ze dne 13. prosince 1999
o zásadách Společenství pro elektronické podpisy
EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,
s ohledem na Smlouvu o založení Evropského společenství, a zejména na čl. 47 odst. 2
a články 55 a 95 této smlouvy,
s ohledem na návrh Komise [1],
s ohledem na stanovisko Hospodářského a sociálního výboru [2],
s ohledem na stanovisko Výboru regionů [3],
v souladu s postupem stanoveným v článku 251 Smlouvy [4],
vzhledem k těmto důvodům:

(1) Komise dne 16. dubna 1997 předložila Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení o evropské iniciativě v oblasti elektronického obchodu.

(2) Komise dne 8. října 1997 předložila Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení nazvané "O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování".

(3) Dne 1. prosince 1997 Rada vyzvala Komisi, aby co nejdříve předložila návrh směrnice Evropského parlamentu a Rady o digitálních podpisech.

(4) Elektronická komunikace a obchod vyžadují "elektronické podpisy" a související služby, které umožňují ověřování pravosti dat. Rozdíly v předpisech členských států o právním uznání elektronických podpisů a o akreditaci "ověřovatelů" by mohly vytvořit vážnou překážku používání elektronické komunikace a elektronického obchodu. Vytvoření jasného rámce Společenství, který upraví podmínky používání elektronických podpisů, přispěje k posílení důvěry v nové technologie a k jejich obecnému uznání. Rozdíly v právních předpisech členských států by neměly narušovat volný pohyb zboží a služeb na vnitřním trhu.

(5) Měla by být podporována interoperabilita produktů pro elektronické podpisy. V souladu s článkem 14 Smlouvy zahrnuje vnitřní trh prostor bez vnitřních hranic, v němž je zajištěn volný pohyb zboží. Musí být splněny základní požadavky týkající se produktů pro elektronické podpisy, aby byl zajištěn volný pohyb v rámci vnitřního trhu a vybudována důvěra v elektronické podpisy, aniž je dotčeno nařízení Rady (ES) č. 3381/94 ze dne 19. prosince 1994, kterým se stanoví režim Společenství pro kontroly vývozu zboží dvojího užití [5] a rozhodnutí Rady 94/942/SZBP ze dne 19. prosince 1994 o společném postupu přijatém Radou o kontrole vývozu zboží dvojího užití [6].

(6) Tato směrnice neharmonizuje poskytování služeb v oblasti důvěrnosti informací, pokud se na ně vztahují vnitrostátní právní předpisy o veřejném pořádku nebo veřejné bezpečnosti.

(7) Vnitřní trh zajišťuje volný pohyb osob a z toho důvodu občané Evropské unie a osoby, které v ní mají bydliště, stále častěji jednají s orgány jiných členských

států, než kterých jsou rezidenti. Dostupnost elektronické komunikace by v tomto ohledu mohla být velice užitečná.

(8) Rychlost technického rozvoje a celosvětový rozměr internetu vyžadují přístup otevřený různým technologiím a službám, které umožňují ověřování pravosti dat elektronickou cestou.

(9) Elektronické podpisy budou využívány v mnoha různých případech, což povede ke vzniku celé škály nových služeb a produktů souvisejících s elektronickými podpisy nebo je využívajících. Definice těchto produktů a služeb by neměla být omezena na vydávání a správu osvědčení, ale měla by rovněž zahrnovat ostatní služby a produkty využívající elektronické podpisy nebo s nimi související, jako jsou registrační služby, služby časových datovacích razítek, adresářové služby, výpočetní služby nebo poradenství v oblasti elektronických podpisů.

(10) Vnitřní trh ověřovatelům umožňuje, aby rozvíjeli svou přeshraniční činnost, zvyšovali tak svou konkurenceschopnost a nabízeli spotřebitelům a podnikům nové možnosti bezpečné výměny informací a obchodování elektronickou cestou bez ohledu na hranice. Ověřovatelé by měli mít možnost poskytovat své služby bez předběžného povolení, aby se tak v rámci Společenství podpořilo poskytování ověřovacích služeb prostřednictvím otevřené sítě. Předběžným povolením se rozumí nejenjakékoli povolení, které poskytovatel služby musí získat na základě rozhodnutí vnitrostátních orgánů před tím, než bude oprávněn poskytovat ověřovací služby, ale rovněž jakékoli jiné opatření se stejným účinkem.

(11) Dobrovolné akreditační systémy, které usilují o zajištění vyšší úrovně poskytované služby, mohou ověřovatelům nabídnout vhodný rámec pro další rozvoj jejich služeb, aby dosáhly úrovně důvěryhodnosti, bezpečnosti a kvality požadované vývojem trhu. Je nezbytné, aby tyto systémy podpořily mezi ověřovateli rozvoj pravidel pro řádný výkon činnosti. Ověřovatelé by měly mít možnost volně vstupovat do těchto akreditačních systémů a využívat je.

(12) Je vhodné umožnit, aby ověřovací služby poskytovaly veřejnoprávní jednotky nebo právnické či fyzické osoby, pokud je to v souladu s vnitrostátními právními předpisy. Členské státy by ověřovatelům neměly bránit, aby působili mimo rámec dobrovolných akreditačních systémů. Je vhodné zajistit, aby akreditační systémy neomezovaly hospodářskou soutěž v odvětví ověřovacích služeb.

(13) Členské státy si mohou zvolit způsob, jakým zajistí dohled nad dodržováním této směrnice. Tato směrnice nevylučuje vytvoření systému dohledu v rámci soukromého sektoru. Tato směrnice neukládá ověřovatelům povinnost žádat, aby nad nimi byl vykonáván dohled v rámci jakéhokoli platného akreditačního systému.

(14) Je důležité, aby byla nalezena rovnováha mezi potřebami spotřebitelů a podniků.

(15) Příloha III obsahuje požadavky na prostředky pro bezpečné vytváření podpisů tak, aby byla zajištěna funkčnost zaručených elektronických podpisů. Nezahrnuje celé systémové prostředí, ve kterém se tyto prostředky využívají. Řádné fungování vnitřního trhu vyžaduje, aby Komise a členské státy jednaly rychle a umožnily tak ustavení subjektů, které budou pověřeny hodnocením shody prostředků pro bezpečné vytváření podpisů s přílohou III. Potřeby trhu vyžadují, aby hodnocení shody bylo provedeno včas a účinně.

(16) Tato směrnice podporuje používání a právní uznání elektronických podpisů ve Společenství. Pro elektronické podpisy používané výlučně v systémech, které vyplývají z dobrovolných dohod uzavřených podle soukromého práva mezi určeným počtem účastníků, není nezbytné vytvářet právní rámec. V mezích stanovených vnitrostátními právními předpisy je nezbytné respektovat svobodu smluvních stran

sjednávat si mezi sebou podmínky uznávání elektronických podpisů. Měla by být uznána právní účinnost elektronických podpisů používaných v těchto systémech a jejich přípustnost jako důkazů v soudním řízení.

(17) Cílem této směrnice není harmonizace vnitrostátních právních předpisů týkajících se závazkového práva, zejména uzavírání a provádění smluv, ani jiných formalit nesmluvní povahy týkajících se podpisů. Z tohoto důvodu je nezbytné, aby se ustanovení o právních účincích elektronických podpisů nedotkla požadavků na formu, které upravují vnitrostátní právní předpisy pro uzavírání smluv, ani pravidel, které určují místo uzavření smlouvy.

(18) Uchovávání a kopírování dat pro vytváření podpisu by mohlo ohrozit právní platnost elektronických podpisů.

(19) Elektronické podpisy budou využívány ve veřejném sektoru uvnitř vnitrostátních správních orgánů a orgánů Společenství a při komunikaci mezi těmito orgány navzájem a mezi těmito orgány a občany a hospodářskými subjekty, například v oblasti veřejných zakázek, daní, sociálního zabezpečení, zdravotnictví a soudnictví.

(20) Harmonizovaná kritéria týkající se právních účinků elektronických podpisů budou zárukou jednotného právního rámce ve Společenství. Vnitrostátní právní předpisy upravují různé požadavky týkající se právní platnosti vlastnoručních podpisů. Pro potvrzení totožnosti osoby, která se podepisuje elektronicky, lze použít osvědčení. Zaručené elektronické podpisy založené na kvalifikovaných osvědčeních vedou k zajištění vyššího stupně bezpečnosti. Zaručené elektronické podpisy založené na kvalifikovaných osvědčeních a vytvořené prostředky pro bezpečné vytváření podpisů lze z právního hlediska považovat za rovnocenné vlastnoručním podpisům pouze, pokud jsou splněny požadavky platné pro vlastnoruční podpisy.

(21) Aby došlo k obecnému přijetí metod elektronického ověřování pravosti, je nezbytné zajistit, aby elektronické podpisy mohly být ve všech členských státech používány jako důkazy v soudním řízení. Právní uznání elektronických podpisů by mělo být založeno na objektivních kritériích a nemělo by záviset na povolení dotčených ověřovatelů. Vnitrostátní právní předpisy vymezí právní oblasti, ve kterých lze používat elektronické dokumenty a elektronické podpisy. Touto směrnicí nejsou dotčeny pravomoci vnitrostátního soudu rozhodovat o souladu s požadavky této směrnice ani vnitrostátní předpisy o volném právním hodnocení důkazů.

(22) Ověřovatelé, kteří poskytují ověřovací služby veřejnosti, podléhají vnitrostátním právním předpisům o odpovědnosti.

(23) Rozvoj mezinárodního elektronického obchodu vyžaduje uzavírání přeshraničních dohod týkajících se třetích zemí. Pro zajištění vzájemného propojení na globální úrovni by bylo vhodné uzavírat se třetími zeměmi dohody o mnohostranných pravidlech v oblasti vzájemného uznávání ověřovacích služeb.

(24) Pro zvýšení důvěry uživatelů v elektronickou komunikaci a elektronický obchod je nezbytné, aby ověřovatelé dodržovali právní předpisy o ochraně dat a respektovali soukromí jednotlivců.

(25) Ustanovení o používání pseudonymů v osvědčeních by neměla členským státům bránit, aby vyžadovaly ověřování totožnosti osob podle právních předpisů Společenství nebo podle vnitrostátních právních předpisů.

(26) Opatření nezbytná pro provedení této směrnice jsou přijímána v souladu s rozhodnutím Rady 1999/468/ES ze dne 28. června 1999 o postupech pro výkon prováděcích pravomocí svěřených Komisi [7].

(27) Dva roky po provedení této směrnice ji Komise přezkoumá, aby se mimo jiné přesvědčila, že vývoj technologií nebo změny právního prostředí nevytvořily

překážky pro dosažení cílů, které jsou v ní uvedeny. Komise by měla přezkoumat vliv na související technické oblasti a předložit zprávu Evropskému parlamentu a Radě.

(28) V souladu se zásadami subsidiarity a proporcionality uvedenými v článku 5 Smlouvy není možné, aby členské státy samostatně dostatečným způsobem dosáhly vytvoření harmonizovaného právního rámce pro poskytování elektronických podpisů a souvisejících služeb, a je tedy vhodné, aby toho bylo dosaženo v rámci Společenství. Tato směrnice nestanoví více, než co je nezbytné pro dosažení tohoto cíle,

PŘIJALY TUTO SMĚRNICI:

Článek 1

Oblast působnosti

Účelem této směrnice je usnadnit používání elektronických podpisů a přispět k jejich právnímu uznání. Stanoví právní rámec pro elektronické podpisy a některé ověřovací služby, aby bylo zajištěno řádné fungování vnitřního trhu.

Nevztahuje se na hlediska spojená s uzavíráním a platností smluv či jiných právních závazků, pokud vnitrostátní právní předpisy nebo právní předpisy Společenství upravují požadavky na jejich formu; touto směrnicí nejsou rovněž dotčena pravidla a omezení, která upravují používání dokumentů a která jsou obsažena ve vnitrostátních právních předpisech či právních předpisech Společenství.

Článek 2

Definice

Pro účely této směrnice se rozumí:

1. "elektronickým podpisem" údaj v elektronické podobě, který je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti;
2. "zaručeným elektronickým podpisem" elektronický podpis, který splňuje tyto požadavky:
 - a) je jednoznačně spojen s podepisující osobou,
 - b) umožňuje zjistit totožnost podepisující osoby,
 - c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou, a
 - d) je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoli následnou změnu těchto dat;
3. "podepisující osobou" jakákoli osoba, která má prostředek pro vytváření podpisu a která jedná na svůj účet nebo na účet fyzické či právnické osoby nebo subjektu, které zastupuje;
4. "daty pro vytváření podpisu" jedinečná data, jako jsou kódy nebo soukromé šifrovací klíče, které podepisující osoba používá k vytvoření elektronického podpisu;
5. "prostředkem pro vytváření podpisu" konfigurovaný softwarový nebo hardwarový prostředek pro využití dat pro vytváření podpisu;
6. "prostředkem pro bezpečné vytváření podpisu" prostředek pro vytváření podpisu, který splňuje požadavky uvedené v příloze III;
7. "daty pro ověřování podpisu" data, jako kódy nebo veřejné šifrovací klíče, které se používají pro ověřování elektronického podpisu;
8. "prostředkem pro ověřování podpisu" konfigurovaný softwarový nebo hardwarový prostředek pro využití dat pro ověřování podpisu;

9. "osvědčením" elektronické potvrzení, které spojuje data pro ověřování podpisu s určitou osobou a potvrzuje totožnost této osoby;

10. "kvalifikovaným osvědčením" osvědčení, které splňuje požadavky uvedené v příloze I a které vydává ověřovatel, jenž splňuje požadavky uvedené v příloze II;

11. "ověřovatelem" subjekt nebo právnická či fyzická osoba, která vydává osvědčení nebo poskytuje jiné služby související s elektronickými podpisy;

12. "produktem pro elektronický podpis" hardware nebo software nebo jeho odpovídající části, které jsou určeny k tomu, aby je ověřovatel používal pro poskytování služeb souvisejících s elektronickými podpisy nebo které jsou určeny pro vytváření nebo ověřování elektronických podpisů;

13. "dobrovolnou akreditaci" jakékoli povolení, které stanoví zvláštní práva a povinnosti pro poskytování ověřovacích služeb a které uděluje na žádost dotčeného ověřovatele veřejný nebo soukromý subjekt pověřený stanovením těchto práv a povinností a dohledem nad jejich dodržováním, přičemž ověřovatel není oprávněn vykonávat práva vyplývající z povolení, dokud neobdrží rozhodnutí tohoto subjektu.

Článek 3

Přístup na trh

1. Členské státy nebudou poskytování ověřovacích služeb podmiňovat předběžným povolením.

2. Aniž je dotčen odstavec 1, mohou členské státy zavést nebo zachovat dobrovolné akreditační systémy, jejichž cílem je zlepšit úroveň poskytovaných ověřovacích služeb. Veškeré požadavky na tyto systémy musí být objektivní, průhledné, proporcionální a nediskriminační. Členské státy nesmí omezovat počet akreditovaných ověřovatelů z důvodů, které spadají do oblasti působnosti této směrnice.

3. Každý členský stát zajistí zavedení odpovídajícího systému, který umožní dohled nad ověřovateli, kteří jsou usazeni na jeho území a kteří vydávají kvalifikovaná osvědčení pro veřejnost.

4. Vhodné veřejné či soukromé subjekty pověřené členskými státy stanoví shodu prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III. Komise postupem podle článku 9 vymezí kritéria, podle nichž členské státy stanoví, zda může být subjekt pověřen.

Rozhodnutí subjektů uvedených v prvním pododstavci o shodě s požadavky uvedenými v příloze III bude uznáno všemi členskými státy.

5. Komise může postupem podle článku 9 přidělit a zveřejnit v Úředním věstníku Evropských společenství čísla norem obecně uznávaných pro produkty pro elektronický podpis. Je-li produkt pro elektronický podpis v souladu s těmito normami, předpokládají členské státy, že rovněž splňuje požadavky uvedené v příloze II písm. f) a v příloze III.

6. Členské státy a Komise spolupracují při podporování rozvoje a používání prostředků pro ověřování podpisu s ohledem na doporučení o prostředcích pro bezpečné ověřování podpisu uvedených v příloze IV a v zájmu spotřebitele.

7. Členské státy mohou používání elektronických podpisů ve veřejném sektoru podmínit případnými doplňujícími požadavky. Tyto požadavky musí být objektivní, průhledné, proporcionální a nediskriminační a musí se vztahovat pouze na zvláštní vlastnosti daného použití. Tyto požadavky nesmí vytvářet překážky při poskytování přeshraničních služeb občanům.

Článek 4

Zásady vnitřního trhu

1. Každý členský stát bude pro ověřovatele usazené na svém území a pro služby, které poskytují uplatňovat vnitrostátní právní předpisy, které přijme na základě této směrnice. Členské státy nesmí v oblastech, na které se vztahuje tato směrnice, omezovat poskytování ověřovacích služeb pocházejících z jiného členského státu.

2. Členské státy dbají, aby produkty pro elektronický podpis, které jsou v souladu s touto směrnicí, byly propuštěny do volného oběhu na vnitřním trhu.

Článek 5

Právní účinky elektronických podpisů

1. Členské státy dbají, aby zaručené elektronické podpisy založené na kvalifikovaných osvědčeních a vytvořené pomocí prostředků pro bezpečné vytváření podpisu:

a) splňovaly právní požadavky na podpis ve vztahu k datům v elektronické podobě, stejně jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k údajům vlastnoručně psaným nebo vytištěným na papíře; a

b) byly přijímány jako důkazy v soudním řízení.

2. Členské státy dbají, aby elektronickým podpisům nebyly odpírány právní účinky a aby nebyly odmítány jako důkazy v soudním řízení pouze z důvodu, že:

- mají elektronickou podobu, nebo
- se nezakládají na kvalifikovaném osvědčení, nebo
- se nezakládají na kvalifikovaném osvědčení vydaném akreditovaným ověřovatelem, nebo
- nejsou vytvořeny prostředkem pro bezpečné vytváření podpisu.

Článek 6

Odpovědnost

1. Členské státy přinejmenším zajistí, aby ověřovatel, který pro veřejnost vydává osvědčení jako kvalifikované osvědčení nebo který se veřejnosti za toto osvědčení zaručuje, byl odpovědný za škodu způsobenou jakémukoli subjektu nebo fyzické či právnické osobě, která se na toto osvědčení důvodně spoléhá, pokud jde o:

a) přesnost veškerých informací obsažených v kvalifikovaném osvědčení ke dni jeho vydání a o uvedení veškerých údajů stanovených pro kvalifikované osvědčení;

b) ujištění, že v době vydání osvědčení byla podepisující osoba uvedená v kvalifikovaném osvědčení držitelem dat pro vytváření podpisu odpovídajících datům pro ověřování podpisu uvedeným nebo označeným v osvědčení;

c) ujištění, že data pro vytváření podpisu a data pro ověřování podpisu mohou být použita doplňujícím způsobem v případě, kdy ověřovatel vytváří obě tyto složky,

ledaže ověřovatel prokáže, že nejednal z nedbalosti.

2. Členské státy přinejmenším zajistí, aby ověřovatel, který pro veřejnost vydá osvědčení jako kvalifikované osvědčení, byl odpovědný za škody způsobené jakémukoli subjektu nebo fyzické či právnické osobě, kteří se na toto osvědčení důvodně spoléhají, pokud opomene zaregistrovat odvolání osvědčení, ledaže ověřovatel prokáže, že nejednal z nedbalosti.

3. Členské státy zajistí, aby ověřovatel mohl v kvalifikovaném osvědčení určit omezení pro jeho použití, pokud tato omezení mohou být známá třetím osobám. Ověřovatel neodpovídá za škody vyplývající z použití kvalifikovaného osvědčení, které přesahuje v něm uvedená omezení.

4. Členské státy zajistí, aby ověřovatel mohl v kvalifikovaném osvědčení uvádět mezní hodnoty transakcí, pro které lze osvědčení použít, pokud je toto omezení známé třetí osobám.

Ověřovatel neodpovídá za škody vyplývající z překročení tohoto maximálního omezení.

5. Ustanovením odstavců 1 až 4 není dotčena směrnice Rady 93/13/EHS ze dne 5. dubna 1993 o nepřiměřených podmínkách ve spotřebitelských smlouvách [8].

Článek 7

Mezinárodní hlediska

1. Členské státy zajistí, aby osvědčení, která ověřovatel usazený ve třetí zemi vydá pro veřejnost jako kvalifikovaná osvědčení, byla uznávána jako právně rovnocenná osvědčením vydaným ověřovatelem usazeným ve Společenství, pokud:

a) ověřovatel splňuje podmínky uvedené v této směrnici a byl akreditován v rámci dobrovolného akreditačního systému zřízeného v členském státě; nebo

b) se ověřovatel usazený ve Společenství, který splňuje požadavky uvedené v této směrnici, za toto osvědčení zaručí; nebo

c) jsou osvědčení nebo ověřovatel uznány na základě dvoustranné nebo mnohostranné dohody mezi Společenstvím a třetími zeměmi nebo mezinárodními organizacemi.

2. S cílem usnadnit přeshraniční ověřovací služby s třetími zeměmi a právní uznání zaručených elektronických podpisů pocházejících ze třetích zemí předloží Komise případně návrhy na účinné provádění norem a mezinárodních dohod vztahujících se na ověřovací služby. Zvláště podle potřeby předloží Radě návrhy na odpovídající zmocnění pro jednání o dvoustranných a mnohostranných dohodách se třetími zeměmi a mezinárodními organizacemi. Rada rozhoduje kvalifikovanou většinou.

3. Pokud se Komise dozví, že podniky Společenství mají obtíže s přístupem na trh třetích zemí, může podle potřeby předložit Radě návrhy na udělení nezbytného zmocnění pro sjednání srovnatelných práv pro podniky Společenství v těchto třetích zemích. Rada se usnáší kvalifikovanou většinou.

Opatřeními přijatými v souladu s tímto odstavcem nebudou dotčeny závazky Společenství a členských států vyplývající z příslušných mezinárodních dohod.

Článek 8

Ochrana dat

1. Členské státy zajistí, aby ověřovatelé a vnitrostátní subjekty odpovědné za akreditaci nebo dohled plnily požadavky stanovené ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [9].

2. Členské státy zajistí, aby ověřovatel, který pro veřejnost vydává osvědčení, mohl osobní údaje shromažďovat pouze přímo od dotčené osoby nebo s jejím výslovným souhlasem a výlučně v míře nezbytné pro vydání a uchování osvědčení. Pro jiné účely nelze údaje shromažďovat ani zpracovávat bez výslovného souhlasu dotčené osoby.

3. Aniž jsou dotčeny právní účinky přiznané pseudonymům vnitrostátními právními předpisy, nesmí členské státy ověřovateli bránit, aby v osvědčení místo jména podepisující osoby uvedl pseudonym.

Článek 9

Výbor

1. Komisi je nápomocen "výbor pro elektronické podpisy" (dále jen "výbor").
 2. Odkazuje-li se na tento odstavec, použijí se články 4 a 7 rozhodnutí 1999/468/ES s ohledem na článek 8 zmíněného rozhodnutí.
- Doba uvedená v čl. 4 odst. 3 rozhodnutí 1999/468/ES je tři měsíce.
3. Výbor přijme svůj jednací řád.

Článek 10

Úkoly výboru

Výbor objasní požadavky uvedené v přílohách této směrnice, kritéria uvedená v čl. 3 odst. 4 a obecně uznávané normy pro produkty pro elektronický podpis stanovené a zveřejněné v souladu s čl. 3 odst. 5 postupem podle čl. 9 odst. 2.

Článek 11

Oznámení

1. Členské státy oznámí Komisi a ostatním členským státům:
 - a) informace o dobrovolných akreditačních systémech na vnitrostátní úrovni, jakož i veškeré doplňující požadavky podle čl. 3 odst. 7;
 - b) názvy a sídla vnitrostátních subjektů odpovědných za akreditaci a dohled, jakož i subjektů uvedených v čl. 3 odst. 4;
 - c) názvy a sídla všech vnitrostátních akreditovaných ověřovatelů.
2. Členské státy oznámí veškeré informace poskytované podle odstavce 1 a jejich změny co nejdříve.

Článek 12

Přezkoumání

1. Komise přezkoumá provádění této směrnice a nejpozději do 19. července 2003 o něm podá zprávu Evropskému parlamentu a Radě.
2. V rámci přezkoumání lze mimo jiné stanovit, zda je vhodné změnit oblast působnosti této směrnice s přihlédnutím k rozvoji techniky, trhu a právní úpravy. Zpráva o přezkoumání bude zejména obsahovat zhodnocení hledisek týkajících se harmonizace provedené na základě získaných zkušeností. Ke zprávě budou případně připojeny návrhy právní úpravy.

Článek 13

Provádění

1. Členské státy uvedou v účinnost právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do 19. července 2001. Neprodleně o o nich uvědomí Komisi.

Tato opatření přijatá členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.
2. Členské státy sdělí Komisi znění hlavních ustanovení vnitrostátních právních předpisů, které přijmou v oblasti působnosti této směrnice.

Článek 14

Vstup v platnost

Tato směrnice vstupuje v platnost dnem vyhlášení v Úředním věstníku Evropských společenství.

Článek 15

Určení

Tato směrnice je určena členským státům.

V Bruselu dne 13. prosince 1999.

Za Evropský parlament

předsedkyně

N. Fontaine

Za Radu

předsedkyně

S. Hassi

[1] Úř. věst. C 325, 23.10.1998, s. 5.

[2] Úř. věst. C 40, 15.2.1999, s. 29.

[3] Úř. věst. C 93, 6.4.1999, s. 33.

[4] Stanovisko Evropského parlamentu ze dne 13. ledna 1999 (Úř. věst. C 104, 14.4.1999, s. 33) a rozhodnutí Evropského parlamentu ze dne 27. října 1999 (dosud nezveřejněné v Úředním věstníku). Rozhodnutí Rady ze dne 30. listopadu 1999.

[5] Úř. věst. L 367, 31.12.1994, s. 1. Nařízení naposledy pozměněné nařízením (ES) č. 837/95 (Úř. věst. L 90, 21.4.1995, s. 1).

[6] Úř. věst. L 367, 31.12.1994, s. 8. Nařízení naposledy pozměněné rozhodnutím 99/193/CFSP (Úř. věst. L 73, 19.3.1999, s. 1).

[7] Úř. věst. L 184, 17.7.1999, s. 23.

[8] Úř. věst. L 95, 21.4.1993, s. 29.

[9] Úř. věst. L 281, 23.11.1995, s. 31.

PŘÍLOHA I

Požadavky na kvalifikovaná osvědčení

Kvalifikovaná osvědčení musí obsahovat:

- poznámku, že osvědčení se vydává jako kvalifikované osvědčení;
- označení ověřovatele a název státu, ve kterém je ověřovatel usazen;
- jméno podepisující osoby nebo pseudonym, který je jako takový označen;
- možnost případně uvést zvláštní znaky podepisující osoby, v závislosti na účelu určení osvědčení;
- data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, která má pod kontrolou podepisující osoba;
- označení začátku a konce doby platnosti osvědčení;
- identifikační kód osvědčení;
- zaručený elektronický podpis ověřovatele, který osvědčení vydává;
- případně omezení oblasti použitelnosti osvědčení; a
- případně omezení hodnot transakcí, pro něž lze osvědčení použít.

PŘÍLOHA II

Požadavky na ověřovatele, kteří vydávají kvalifikovaná osvědčení

Ověřovatelé musí:

- prokázat dostatečnou způsobilost pro poskytování ověřovacích služeb;

- b) zajistit provozování rychlého a bezpečného adresáře a bezpečné a okamžité odvolávací služby;
- c) zajistit, aby bylo možné přesně stanovit datum a čas, kdy bylo osvědčení vydáno nebo odvoláno;
- d) vhodnými prostředky v souladu s vnitrostátními právními předpisy ověřit totožnost a případně zvláštní znaky osoby, které je kvalifikované osvědčení vydáváno;
- e) zaměstnávat personál, který má odborné znalosti, zkušenosti a kvalifikaci nezbytné pro poskytování služeb, a zejména schopnosti řízení, odborné znalosti v oblasti technologie elektronických podpisů a důkladnou znalost přiměřených bezpečnostních postupů; rovněž musí používat administrativní a řídicí postupy a metody, které budou přizpůsobeny uznaným normám a budou s nimi v souladu;
- f) používat důvěryhodné systémy a produkty, které jsou chráněny proti pozměňování a které zajišťují technickou a šifrovací bezpečnost funkcí, které tyto systémy a produkty zajišťují;
- g) přijmout opatření proti padělání osvědčení a, pokud ověřovatel vytváří data pro vytváření podpisů, zajistit utajení v průběhu tvorby těchto dat;
- h) mít k dispozici dostatečné finanční zdroje na provoz v souladu s požadavky této směrnice, zejména na převzetí odpovědnosti za škody, např. uzavřením vhodného pojištění;
- i) zaznamenávat veškeré související informace o kvalifikovaných osvědčeních po přiměřenou dobu, zejména pro potřeby poskytnutí důkazu o osvědčení pro účely soudního řízení. Záznam může mít elektronickou podobu;
- j) neuchovávat ani nekopírovat data pro vytváření podpisu osoby, které ověřovatel poskytl klíčové řídicí služby;
- k) před uzavřením smluvního vztahu s osobou, která požaduje na podporu svého elektronického podpisu osvědčení, informovat tuto osobu trvalými komunikačními prostředky o přesných způsobech a podmínkách používání osvědčení, včetně omezení uložených pro jeho použití, existenci dobrovolného akreditačního systému a postupech vyřizování stížností a mimosoudního urovnávání sporů. Tato informace, kterou lze předat elektronickou cestou, musí mít písemnou podobu a musí být ve snadno srozumitelném jazyce. Důležité části této informace musí být na požádání k dispozici třetím osobám, které se spoléhají na toto osvědčení;
- l) používat důvěryhodný systém pro uchovávání osvědčení v podobě, kterou lze ověřit, aby:
 - zařazování a změny dat mohly provádět pouze pověřené osoby,
 - bylo možno kontrolovat pravost informací,
 - osvědčení byla veřejně přístupná k vyhledávání pouze v těch případech, kdy držitel osvědčení poskytl svůj souhlas, a
 - provozovateli byly zjevné jakékoli technické změny zpochybňující tyto bezpečnostní požadavky.

PŘÍLOHA III

Požadavky na prostředky pro bezpečné vytváření elektronických podpisů

1. Prostředky pro bezpečné vytváření podpisů musí vhodnými technickými prostředky a postupy přinejmenším zajistit, aby:

- a) se data pro vytváření podpisu mohla vyskytnout pouze jedenkrát a aby bylo dostatečně zajištěno jejich utajení;
- b) bylo dostatečně zajištěno, že data pro vytváření podpisu nelze odvodit a že podpis je dostupnými technickými prostředky chráněn proti jakémukoli padělání;

c) podepisující osoba měla možnost data pro vytváření spolehlivě chránit proti jejich zneužití třetí osobou.

2. Prostředky pro bezpečné vytváření podpisů nesmí měnit data, která mají být podepsána, ani bránit tomu, aby tato data byla podepisující osobě předložena před procesem podepisování.

PŘÍLOHA IV

Doporučení pro bezpečné ověřování podpisu

Během procesu ověřování podpisu by mělo být s dostatečnou jistotou zajištěno, aby:

- a) data používaná pro ověření podpisu odpovídala datům zobrazeným ověřovateli;
 - b) byl podpis spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen;
 - c) ověřovatel mohl, bude-li to nezbytné, spolehlivě zjistit obsah podepsaných dat;
 - d) pravost a platnost osvědčení vyžádaného při ověřování podpisu byly spolehlivě ověřeny;
 - e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny;
 - f) bylo jasné uvedeno použití pseudonymu; a
 - g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.
-