Západočeská univerzita v Plzni

Fakulta právnická

Bakalářská práce

Plzeň 2013 **Stanislav WOLNÝ**

Západočeská univerzita v Plzni

Fakulta právnická

Katedra veřejné správy

BAKALÁŘSKÁ PRÁCE

Elektronický podpis v podmínkách státní právy

Autor: Stanislav WOLNÝ

Vedoucí bakalářské práce: JUDr. Tomáš LOUDA, CSc.

Zadavací list 1

Zadavací list 2

Prohlášení:

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu. Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/200 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon).

V Praze 26.8.2013

Poděkování

Děkuji vedoucímu bakalářské práce JUDr. Tomáši LOUDOVI, CSc. za účinnou metodickou, pedagogickou, odbornou ale i lidskou pomoc při zpracování mé bakalářské práce.

V Praze dne 26. srpna 2013 ……...

podpis autora

Anotace

Hlavním cílem mé bakalářské práce je podat ucelený pohled na problematiku týkající se elektronického podpisu. Elektronický podpis je, dle mého názoru, jednou z technologií, kde lze očekávat výraznější rozšíření mezi odbornou i laickou veřejností. První část mé bakalářské práce je věnována popisu fungování elektronického podpisu, vysvětlení základních pojmů a platné legislativě. V druhé části se na základě praktických znalostí věnuji problematice získání EP, včetně porovnání certifikačních autorit a využití EP ve veřejné a státní správě, konkrétně pak využití EP na Ministerstvu obrany. V závěrečné části zmiňuji možnosti EP do budoucna a navrhuji pár jednoduchých opatření k masivnějšímu rozšíření EP, jak v soukromém sektoru, tak i v sektoru státní a veřejné správy.

Klíčová slova: elektronický podpis, elektronická značka, datová zpráva, certifikační autorita, e-OP,

Annotation

The main objective of this bachelor work is the electronic signature. The goal is provide a comprehensive view of the issues regarding the electronic signature. The electronic signature is, one of the technologies which can be more pronounced expansion of the professional and general public. The first part of my thesis are devoted to describing the operation of the electronic signature, the explanation of basic concepts and relevant legislation. The second part is based on practical experience with pay problems obtaining ES, including a comparison of CAs and the use of ES in the public and government, specifically the use of ES by the Ministry of Defence. In the final section is mentioned the possibility of ES in the future and suggest several simple steps to massive expansion of ES, in the private sector and in the public sector and public administration.

Key words: electronic signature, electronic mark, data report, certification autority,e-ID,

OBSAH

Úvod

Nástup tzv. informační společnosti byl velmi rychlý a vývoj moderních technologií stále pokračuje. Přináší však s sebou i změnu v komunikaci. Sice klasická komunikace je stále používaná, ale v současné době již elektronická korespondence téměř vytlačila tradiční formu papírovou. Vývojem prošla i státní a veřejná správa, kde elektronických dokumentů stále přibývá. Ale stejně jako ve světě papírových dokumentů či tiskopisů, které musí být vlastnoručně podepsány, je nutné opatřit podpisem i elektronické dokumenty. K tomu je zapotřebí právě elektronického podpisu, který nás identifikuje stejně jako náš vlastnoruční podpis a nevyžaduje tak fyzickou přítomnost osoby na místě předávání dokumentu. Elektronický podpis tak přináší usnadnění našich povinností. Největším přínosem je v oblasti elektronického obchodování a při komunikaci s orgány veřejné správy. V oblasti veřejné správy dochází k neustálému rozšiřování elektronické formy a to nejen vzájemně mezi úřady, ale i mezi úřady a ostatními subjekty.

Hlavním důvodem kodifikace elektronického podpisu byl fakt, že bez ní bychom daleko hůře překonávali zábrany a předsudky, které máme vůči čemukoliv novému. Zejména pak ti, kteří jsou zaměstnáni ve veřejných službách, neboť podnikatelský sektor si svou cestu k elektronickému podepisování začal hledat již dříve.

Dnem 1.10.2001 nabylo účinnosti nařízení vlády č. 304 ze dne 25. července 2001, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Na základě tohoto a dalších nařízení vlády byla zřízena elektronická podatelna. Vyhláška č. 496/2004 Sb., k elektronickým podatelnám, která upravuje postup, jak mají orgány veřejné moci přijímat a odesílat datové zprávy prostřednictvím elektronické podatelny. Tato vyhláška navazuje na nařízení vlády č. 495/2004 Sb., k elektronickým podatelnám, které nařizuje orgánům veřejné moci elektronickou podatelnu zřídit a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády. Vyhlášky nabyly účinnosti k 1. lednu 2005.

V druhé polovině roku 2009 přinesla vyhláška 191/2009 Sb., orgánům veřejné správy a některým dalším orgánům povinnost, využívat datové schránky jako jediný prostředek ke komunikaci a alespoň u těchto subjektů je tak dnes papírová komunikace zcela nahrazena elektronickou formou. Toho lze označit za nejrazantnější změnu v oblasti státní správy v historii České republiky.

Ve své práci se budu zabývat právě využitím elektronického podpisu především v komunikaci se státní a veřejnou správou. Mým záměrem je přiblížit tuto problematiku běžnému občanovi, či řadovému zaměstnanci veřejné moci.

Cílem mé práce je posoudit možnosti využívání elektronického podpisu a zamyslet nad jeho dalším využitím.

V první části své práce vysvětlím základní pojmy spojené s elektronickým podpisem, a jeho zakotvení v legislativě. V dalších částech objasním způsob fungování i způsob, jakým si můžeme tento podpis pořídit. Dále porovnám možnosti certifikačních autorit, akreditovaných v České republice a popíšu využití elektronického podpisu v komunikaci s veřejnou mocí. Zvláště se zaměřím na praktické využití elektronického podpisu na Ministerstvu obrany.

1. ELEKTRONICKÝ PODPIS

Do poloviny devadesátých let v České republice neexistovala ucelená koncepce státní politiky v oblasti informačních systémů. Vznik elektronického podpisu v ČR se spojuje s rokem 1999 a dokumentem nazývaným Státní informační politika - cesta k informační společnosti. Jedná se o první ucelenou koncepci státu v oblasti budování tzv. informační společnosti. V tomto dokumentu bylo mimo jiné konstatováno, že pro rozvoj informační společnosti v České republice chybí legislativní zázemí, které by se zabývalo oblastí elektronického obchodu, elektronického podpisu a používání dokumentů v elektronické podobě. Jedním z prioritních úkolů bylo uzákonit elektronický podpis a dát dokumentům v elektronické podobě stejnou právní váhu jako dokumentům klasickým.

V prosinci 1999, byla přijata směrnice Evropské Unie pro elektronický podpis.[1] Krátce po tomto přijetí došlo ke shodě zástupců Úřadu pro státní informační systém na dalším společném postupu při prosazování přijetí zákona o elektronickém podpisu. Právě z tohoto postupu pak vycházel návrh zákona o elektronickém podpisu, který byl v červenci 2000 pod číslem 227/2000 Sb. přijat Parlamentem České republiky.

1.1. Význam elektronického podpisu

Elektronický podpis je v oblasti digitálních dat tímtéž, co je běžný podpis v „normálním životě“. V podstatě se dá využít všude tam, kde je dnes nutný vlastnoruční podpis. Jelikož je dnes možné všechny dokumenty převést z papírové do elektronické podoby, je nutné, aby i podpisy bylo možné převést do elektronické podoby.

Elektronické podepisování a také ověřování elektronických podpisů je takto nesrovnatelně rychlejší a efektivnější, neboť je možné podepsat i takové formáty, které ručně podepsat v podstatě nejdou, jako jsou např. přístupy do databází, obsah CD ROM

[1] Směrnice evropského parlamentu a rady 1999/93ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy [online]. [cit. 2011-02-14]. Dostupný z WWW: <http//:www.eur-lex.europa.eu/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:CS:PDF>.

a dalších záznamových médií. Elektronický podpis je dnes jedním z hlavních nástrojů identifikace a autentizace fyzických osob v internetovém prostředí.[2]

1.2. Základní pojmy spojené s elektronickým podpisem

Klíčové pojmy spojené s elektronickým podpisem jsou definovány v zákoně o elektronickém podpisu č.227/2000 Sb. o elektronickém podpisu, a v souvisejících právních předpisech a to pouze ve vztahu k elektronickému podpisu. Považuji za důležité, aby byly pospány pohromadě a na začátku mé práce.

1.2.1. Zaručený elektronický podpis

Zaručeným elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené. Musí splňovat několik požadavků. Mezi tyto požadavky patří jednoznačné spojení zaručeného elektronického podpisu s podepisující osobou. Podepisující osoba musí být ve vztahu k datové zprávě jednoznačně identifikována. Zaručený elektronický podpis je třeba vytvořit a připojit k datové zprávě takovými prostředky, které podepisující osoba může udržet pod svou výhradní kontrolou. Důležitým požadavkem je také připojení zaručeného elektronického podpisu k datové zprávě tak, aby bylo zjistit jakoukoliv následnou změnu původních dat.

1.2.2. Elektronická značka

Elektronická značka představuje údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

[2] SMEJKAL, Vladimír. *Elektronický podpis v praxi* [online]. 2001, [cit. 2008-02-25]. Dostupné na WWW: <http://pravniradce.ihned.cz/c4-10078240-10025905-F00000_detail-elektronicky-podpis-v-praxi>

- Jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
- Byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
- Jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné identifikovat jakoukoli následnou změnu dat.

1.2.3. Elektronická podatelna

Elektronická podatelna slouží k přijímání (vstupu) a vypravování (výstupu) elektronických dokumentů do a z úřadu. Tvoří ji souhrn technického vybavení, umožňující se připojit prostřednictvím datových sití na elektronickou poštovní schránku podatelny, uložit a evidovat doručenou elektronickou poštu a postoupit ji k dalšímu vyřízení. Nedílnou součástí elektronické podatelny je také obsluha e-podatelny a pravidla pro zacházení s elektronickými písemnostmi, nejčastěji ve formě spisového řádu a návodu pro obsluhu technického vybavení. Obsluha e-podatelny je také povinna ověřit platnost elektronického podpisu a kvalifikovaného certifikátu, pokud jsou k doručené datové zprávě připojeny.

1.2.4. Datová zpráva

Datová zpráva představuje elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat je na záznamových médiích, použitých při zpracování a přenosu dat elektronickou formou.

1.2.5. Podepisující osoba

Podepisující osoba je zpravidla fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby.

1.2.6. Označující osoba

Označující osoba je buď fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou.

1.2.7 Držitel certifikátu

Držitel certifikátu je fyzická nebo právnická osoba, nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán.

1.2.8. Certifikát

Certifikát představuje datovou zprávu, která je vydána poskytovatelem certifikačních služeb. Spojuje data pro ověřování elektronických podpisů podepisující osobou a umožňuje ověřit její identitu a také spojuje data pro ověřování elektronických značek a označující osobou a umožňuje ověřit její identitu. Poskytovatelé certifikačních služeb zpravidla poskytují kvalifikované a komerční osobní certifikáty a kvalifikované a komerční systémové certifikáty. Kvalifikovaný certifikát, na rozdíl od komerčního, musí splňovat náležitosti přesně vymezené v zákoně a musí být vydán kvalifikovaným poskytovatelem certifikačních služeb.

1.2.9. Poskytovatel certifikačních služeb – Certifikační autorita CA

Poskytovatel certifikačních služeb je fyzická či právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. Akreditovaným poskytovatelem je ten, jemuž byla udělena akreditace podle § 10 zákona č.227/200 Sb.. Kvalifikovaným poskytovatelem je ten, který vydává kvalifikované certifikáty nebo kvalifikované

systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů a splnil ohlašovací povinnost podle § 6 zákona č.227/2000 Sb.

1.2.10 CRL – Certificate revocation list

Seznam zneplatněných certifikátů. Seznam je součástí webových aplikací Certifikačních autorit, je on-line a je pravidelně aktualizován. Jsou v něm uvedeny zneplatněné certifikáty, ať už na žádost držitele či jiného subjektu. Žádosti o zneplatnění se podávají nejčastěji z důvodu ztráty nosiče s elektronickým podpisem (flash, token, atd.) nebo při podezření na kompromitaci soukromého klíče.

1.2.11. Kvalifikované časové razítko

Kvalifikované časové razítko představuje datovou zprávu, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě a časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým razítkem.

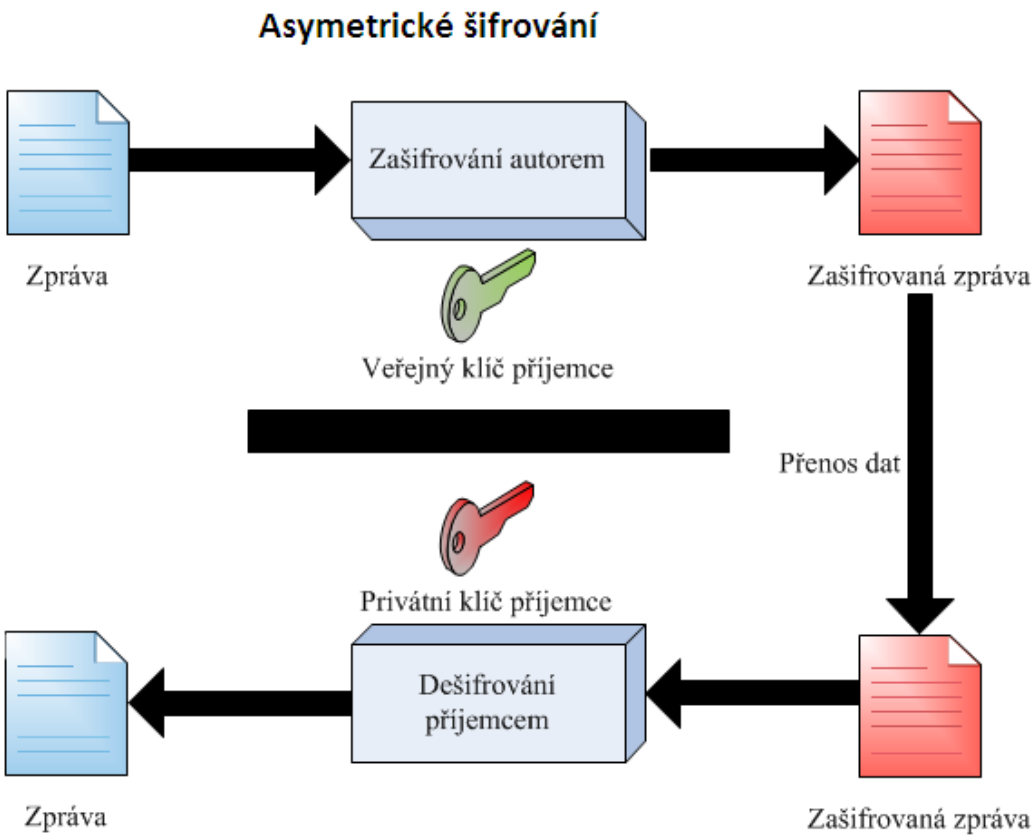
1.2.12. Prostředky pro vytváření elektronického podpisu

Prostředky pro vytváření elektronického podpisu představují technické zařízení nebo programové vybavení, které se používá k vytváření elektronického podpisu.

1.2.13. Asymetrická kryptografie

Asymetrická kryptografie je určitá oblast kryptografie, kde každý subjekt systému vlastní dvojici klíčů. Jeden klíč se používá k šifrování a druhý k dešifrování. U elektronického podpisu nemluvíme o šifrovacím a dešifrovacím klíči, ale o veřejné a privátním (soukromém) klíči. Podstata spočívá v tom, že dat šifrovaná veřejným klíčem

lze dešifrovat pouze se znalostí privátního klíče a naopak. Privátní klíč by měl být maximálně chráněn majitelem, zatímco druhý klíč je naopak zveřejněn u poskytovatele certifikačních služeb. Je-li zpráva zašifrována privátním klíčem a příjemce zprávy má k dispozici odpovídající veřejný klíč, je schopen zprávu dešifrovat. Vzhledem ke skutečnosti, že veřejný klíč je vystaven v internetu nelze tuto zprávu chápat jako zašifrovanou v plném smyslu slova, ale pouze za autorizovanou.

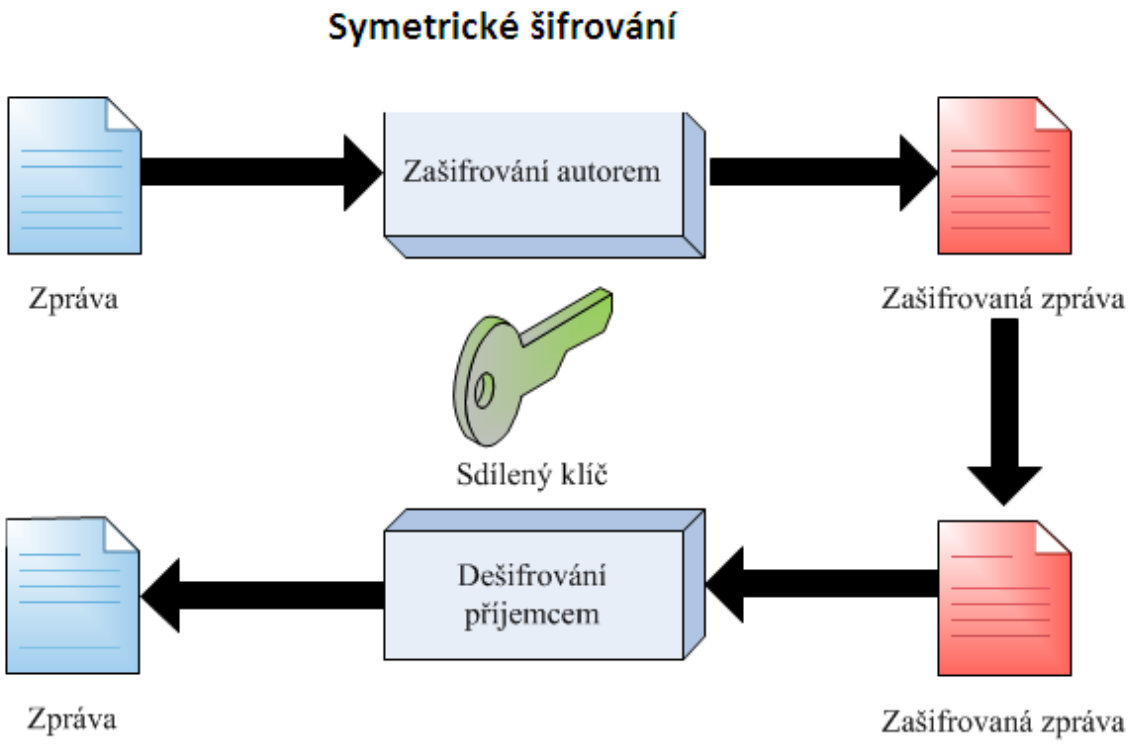


Obr: 1, [Zdroj: vlastní zpracování]

1.2.14. Symetrická kryptografie

Symetrické šifrování je založeno na jediném šifrovacím klíči, který musí být znám jak odesilateli, tak příjemci. Znamená to, že stejný klíč, který byl použit k zašifrování zprávy na straně odesilatele, bude použit také na straně příjemce. Největší slabinou

tohoto systému je obtížná distribuce klíče. Vzhledem ke svému charakteru se hodí spíše ke komunikaci dvou stran, které se navzájem znají, a je mezi nimi možná zabezpečená distribuce klíče. Jedná se o klasické šifrování, které se, vzhledem k vysokým výkonům počítačů a tím poměrně reálné možnosti prolomení šifry tzv. silou, již opouští.



Obr: 2 , [Zdroj: Vlastní zpracování]

1.2.15. Privátní klíč

Privátní klíč představuje data, které slouží k vytváření elektronického podpisu. Podle zákona č.227/2000 Sb. Jsou to jedinečná data, která si každý zájemce generuje prostřednictvím aplikace pro generování klíčů u poskytovatele certifikačních služeb.

1.2.16. Veřejný klíč

Veřejný klíč představuje data, které slouží k ověřování elektronického podpisu. Tato data si každý zájemce také generuje prostřednictvím aplikace pro generování klíčů současně s daty pro vytváření elektronického podpisu.

1.2.17. Hashovací funkce

Použití asymetrické kryptografie k šifrování a dešifrování elektronického podpisu je mnohem pomalejší než použití symetrické kryptografie. Proto se při tvorbě elektronického podpisu nešifruje celá zpráva, ale nejprve se na zprávu použije tzv. hashovací funkce. Hash je jednocestná funkce, která z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky. Výsledný řetězec (otisk) by měl maximálně charakterizovat původní text.[3]

Typická velikost výsledného textu je 16 B (algoritmus MD-5) nebo 20 B (algoritmus SH-1). V dnešní době se již tyto algoritmy vesměs považují za slabé, proto se stále častěji setkáváme s novými algoritmy produkujícími delší otisky: SHA-224 (otisk dlouhý 28 B), SHA-256 (otisk 32 B), SHA-384 (otisk 48 B) a SHA-2 s otiskem dlouhým 64 B. Charakterizuje ji vstup, což je libovolně velký datový tok a výstup, což je datový tok pevné délky. U elektronického podpisu se hashovaní funkce zpravidla používá k výpočtu tzv. otisku podepisované zprávy. Jednocestnou funkcí se rozumí algoritmy, které nejsou výpočetně náročné. Je však výpočetně velice náročné k výsledku nalézt původní text.[4]

Bezpečnost hashovacích funkcí je jedním z klíčových parametrů bezpečnosti elektronického podpisu. Národní bezpečnostní úřad nařídil certifikačním autoritám k 31.12.2010 přejít od hashovaní funkce SHA-1 na novou generaci hashovacích funkcí SHA-2. Poskytovatelé certifikačních služeb ukončili používání algoritmu SHA-1 při vydávání kvalifikovaných certifikátů k 31.12.2009. Pro vytváření elektronického

[3] DOSTÁLEK, Libor. VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. Vyd. Brno: Computer Press, 2006. 536 s. ISBN: 80-251-0828-7.
[4] KATZ, Jonathan. Digital Signatures. 1 st ed London: Springer, 2010. 183 s. ISBN 978-0-387-2771-0.

podpisu je možné po přechodnou dobu používat algoritmus SHA-1, nejdéle však do 31.12.2010.[5]

1.3. Bezpečnost elektronického podpisu

Bezpečnost elektronického podpisu vyplývá ze způsobu použití a ze zvolené ověřovací metody. Významnou roli zde hraje výběr poskytovatele certifikačních služeb a to především ve vazbě na způsob ověřování údajů potřebných k vydání elektronického podpisu a certifikátu. Mezi hlavní rizika patří takzvané generování elektronického podpisu do prostředí operačního systému (přímo do konkrétního počítače), kde může dojít, při napadení počítače, ke zcizení (okopírování) a uživatel o tom neví. Při vydání podpisu do tokenu, flash paměti či smart karty (kontaktní čip), je při ztrátě nebo odcizení postupováno podobně jako při ztrátě bankovních karet. Po nahlášení je elektronický podpis ihned zneplatněn s uvedením přesného času a ve stejný okamžik je aktualizován tzv. CRL. Takže při řádném ověření zprávy na straně adresáta je jasné, že je podpis neplatný. Jedná se tak o pochybení na straně příjemce.

2. LEGISLATIVA

V mezinárodním měřítku se průkopníkem standardizace a legalizace elektronického podpisu stala komise OSN pro mezinárodní právo UNCITRAL – United Nations Commission on International Trade Law, která byla založena Rezolucí OSN č 2205(XX) ze dne 17. Prosince 1966.[6] Byla založena za účelem odstraňování právních překážek v mezinárodním obchodu a koordinovat rozvoj mezinárodního obchodního práva. Komise má v současnosti 60 členských států, přičemž Českou republiku v komisi zastupuje Ministerstvo průmyslu a obchodu.

Nejdůležitější dokumenty komise UNCITRAL z oblasti elektronického podpisu jsou:

[5] Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu [online]. [cit. 2011-02-21]. Dostupný z WWW: http://www.mvcr.cz/soubor/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronického-podpisu.aspx.
[6] UNCITRAL [online].[cit. 2011-02-14]. Dostupný z:http://www.uncitral.org.

- Doporučení UNCITRAL týkající se právní závaznosti elektronických údajů (1985);
- Vzorový zákon UNCITRAL o elektronickém obchodu (1996);
- Vzorový zákon o elektronickém podpisu (2001);
- Úmluva o užití elektronických sdělení v mezinárodním obchodě (2005).

Z pohledu standardizace a legalizace elektronického podpisu bylo důležitým okamžikem předložení a schválení vzorového zákona o elektronickém obchodu Valným shromážděním OSN v prosinci 1996. Zákon obsahuje následující hlavní body:[7]

1. Obecná opatření
   1.1. Okruh aplikace
   1.2. Definice pojmů
   1.3. Interpretace
   1.4. Změna úmluv
2. Aplikace právních požadavků na datové zprávy
   2.1. Aplikace rozpoznání datových zpráv
   2.2. Dokument
   2.3. Popis
   2.4. Originál
   2.5. Přístupnost a průkazná váha
   2.6. Uchovávání datových zpráv

3. Komunikace datovými zprávami
   3.1. Vytváření a platnost kontraktů
   3.2. Rozpoznávání účastníků datových zpráv
   3.3. Atributy datových zpráv
   3.4. Potvrzení přijetí
   3.5. Čas a místo odeslání a přijetí datových zpráv

[7] Budiš, Petr. Elektronický podpis a jeho aplikace v praxi. 1. Vyd. Olomouc:ANAG, 2008. 160 s.ISBN 978-80-7263-465-1.

Následně po schválení výše uvedeného zákona, zahájila komice UNCITRAL přípravu příslušných podkladů pro oblast elektronického podpisu a poskytování certifikačních služeb. Přípravy se zúčastnilo 50 států a mezinárodních organizací a byla završena v roce 2001 předložením a schválením vzorového zákona UNCITRAL o elektronickém podpisu. Komise vydala doporučení, zvážit využití tohoto zákona při tvorbě domácích právních předpisů signatářských států.

Zákon UNCITRAL o elektronickém podpisu se dělí na dvě samostatné části. První část v podstatě popisuje hlavní pojmy, definice a terminologii. Druhá část je ve své podstatě návod k vytvoření modelového zákona o elektronickém podpisu. Obsahuje následující body:

1. Účel a původ modelového zákona
   - 1.1. Účel
   - 1.2. Podklady
   - 1.3. Historie
2. Modelový zákon jako nástroj pro harmonizaci zákonů
3. Obecné znaky elektronického podpisu
   - 3.1. Funkce podpisu
   - 3.2. Digitální podpis a jiné podpisy
   - 3.3. Elektronický podpis založený na jiných technikách než kryptografii s veřejnými klíči
   - 3.4. Elektronický podpis založený na kryptografii s veřejnými klíči
   - 3.5. Technické pojmy a terminologie
     - 3.5.1. Kryptografie
     - 3.5.2. Veřejné a soukromé klíče
     - 3.5.3. Hash funkce
     - 3.5.4. Digitální podpis
     - 3.5.5. Ověření digitálního podpisu
   - 3.6. Infrastruktura veřejných klíčů a poskytovatelé certifikačních služeb
     - 3.6.1. Infrastruktura veřejných klíčů
     - 3.6.2. Poskytovatelé certifikačních služeb
4. Hlavní charakteristiky modelového zákona

4.1. Legislativní podstata modelového zákona
4.2. Vztah s UNCITRAL modelovým zákonem o elektronickém obchodu
4.3. Soustava pravidel doplněná technickými předpisy a kontraktem
4.4. Základní pravidla pro zapojené strany
4.5. Technologický neutrální rámec
4.6. Nediskriminace zahraničních elektronických podpisů
5. Podpora od UNCITRAL
5.1. Podpora v navrhování legislativy
5.2. Informace na interpretaci legislativy založené na modelovém zákonu

Oba tyto vzorové zákony vycházejí ve své úpravě z důsledného technologicky neutrálního přístupu. Rozlišují pouze pojmy písemnost, originál, podpis, elektronická notářská činnost a zaručená kopie. Specifikují pouze obecný přístup k elektronickým podpisům. Vzhledem ke skutečnosti, že v elektronické komunikaci jde vývoj velmi rychle dopředu, je takový přístup svým způsobem zastaralý.

2.1. Legislativa v EU

Vývoj legislativy v oblasti elektronického podpisu v Evropské unii, je charakterizován dohodou členských států na jednotném řešení problematiky elektronického podpisu. Dohoda byla převedena do podoby unijního práva ve formě Směrnice EU 1999/93/ES, o zásadách Společenství pro elektronický podpis, schválenou Evropským parlamentem a Radou dne 13. prosince 1999.

Tato směrnice, se především zabývá zaručeným elektronickým podpisem a jeho právní platností při připojení k elektronickému dokumentu. Směrnice stanovuje základní požadavky, které musí být splněny poskytovateli služeb spojených s elektronickým podpisem a certifikáty, a další požadavky vztahující se k podepisující i ověřující straně.

Samotná směrnice vychází z několika základních principů:

- Jedním z nejdůležitějších je technologická neutralita. Není zde udána žádná konkrétní technologie, což umožňuje využívat další metody.
- Musí existovat systém dohledu nad poskytovateli certifikačních služeb, včetně instituce ověřující správnost zařízení pro vytváření elektronických podpisů. Taková zařízení musí mít povolen volný pohyb na trhu členských zemí EU.
- Pro poskytovatele certifikačních služeb není definováno žádné schéma pro autorizaci provádění těchto služeb tak, aby byla umožněna inovace v budoucnosti.
- Další podmínkou je neexistence omezení počtů poskytovatelů certifikačních služeb.
- Je zde upravena zákonná platnost elektronických podpisů tak, aby nemohlo být odmítnuto jejich použití na základě skutečnosti, že jsou v elektronické podobě a aby byla zaručena ekvivalence s vlastnoručním podpisem. S tím souvisí i požadavek uznávání elektronických podpisů coby důkazních prostředků.

Požadavek na akceptování dokumentů opatřených zaručeným elektronickým podpisem jako důkazu při soudním řízení nebo při komunikaci s orgány státní a veřejné správy souvisí s tím, že zaručený elektronický podpis je k datům v elektronické podobě ve stejném vztahu, jako vlastnoruční podpis k psanému dokumentu.

Směrnice 1999/93/ES ukládá členským státům Evropské unie přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Počítá také s tím, že v každé členské zemi bude ustanoveno vlastní akreditační schéma pro poskytovatele certifikačních služeb. Kvalifikované certifikáty vydané poskytovateli certifikačních služeb podle národního akreditačního schématu jednotlivé členské země, musí být právně uznatelné v ostatních členských zemích EU.

Komisi EU a ostatním členským zemím jsou členské země EU povinny poskytovat následující informace:

- O národním akreditačním schématu
- Jména a adresy národních institucí zodpovědných za akreditaci a dohled
- Jména a adresy všech poskytovatelů certifikačních služeb.

Oblast terminologie ve vztahu k elektronickému podpisu je jednou z klíčových oblastí, obsažených ve výše uvedené směrnici. Stanoví přesný obsah celé řady souvisejících pojmů jako data pro vytváření podpisu, podepisující osoba, data pro ověřování podpisu, atd. Tyto pojmy jsou následně přenášeny do národních legislativ a výrazným způsobem tak zvyšují srozumitelnost.

2.2. Legislativa v ČR

Zásadním momentem v problematice používání elektronického podpisu v ČR, byl rok 2000. V tomto roce ČR jako třetí země na světě přijala zákon upravující užívání elektronického podpisu. Schválením zákona č. 227/2000 Sb., o elektronickém podpisu, byl vytvořen základní legislativní předpoklad pro to, aby pomocí moderních informačních technologií a prostředků dálkového přístupu byly zajištěny podobné podmínky jak pro uživatele, kteří informace zpracovávají v listinné podobě, tak i pro uživatele, kteří informace zpracovávají v elektronické podobě pomocí datových zpráv.

2.2.1 Zákon č.227/2000 Sb., o elektronickém podpisu

Tento zákon upravuje používání elektronického podpisu, poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Zákon byl schválen 29 června 2000 a vstoupil v platnost 1.října 2000. Vychází ze Směrnice EU 1999/93/ES, o zásadách Společenství pro elektronický podpis, schválenou Evropským parlamentem a Radou.

Snahou předkladatelů bylo, aby zákon byl co nejobecnější v rovině technologií, tak aby při změně technologie nemuselo docházet ke změně zákona. Zákon taktéž definuje základní pojmy, postupy a subjekty práva účastnící se na vytváření, používání a ověřování elektronických podpisů a zaručených elektronických podpisů jako prostředků umožňujících používání elektronických dokumentů způsobem, který je v souladu s obecně závaznými právními normami. Zákon rozlišuje čtyři možné varianty používání podpisů a certifikátu, přičemž nejdůležitější je rozdíl mezi stupni podpisů a certifikátu, která definuje takto:

- Elektronickým podpisem, rozumíme údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě;
- Zaručeným elektronickým podpisem, rozumíme elektronický podpis, který splňuje následující požadavky:
    - Je jednoznačně spojen s podepisující osobou;
    - Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě;
    - Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou;
    - Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat;
- Certifikátem se rozumí datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost;
- Kvalifikovaným certifikátem se rozumí certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb splňujícím podmínky stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávajících kvalifikované certifikáty.

Zákon vymezuje podmínky kladené na poskytovatele certifikačních služeb, a rozlišuje dvě kategorie poskytovatelů certifikačních služeb:

- Akreditované poskytovatele certifikačních služeb dozorovým orgánem, tj. Úřadem pro ochranu osobních údajů.;
- Ostatní poskytovatele certifikačních služeb, u kterých aspoň platí oznamovací povinnosti 30 dní před vydáním prvního kvalifikovaného certifikátu.

Z důvodu značně liberálního přístupu zákonodárce a zcela v souladu se Směrnicí EU 1999/93/ES, o zásadách Společenství pro elektronický podpis, schválenou Evropským parlamentem a Radou, byl do zákona začleněn požadavek § 11, že v oblasti orgánů veřejné moci je možné používat pouze zaručený elektronický podpis a kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb. Ostatní poskytovatelé mohou fungovat pouze pro soukromoprávní subjekty.

„Akreditovaným poskytovatelem certifikačních služeb“ je poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona a prováděcí vyhlášky Úřadu pro ochranu osobních údajů.[8]

Zákon také doplnil a upravil platnost několika právních předpisů a norem, z nichž nejdůležitější jsou:

- Doplnění v ustanovení § 40, občanského zákoníku, týkajících se písemných právních úkonů a podepisování, tak že § 40 odst. 3 a 4 nyní zní:
    - „(3) Písemný právní úkon je platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí byt jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Podpis může být nahrazen mechanickými prostředky v případech, kdy je to obvyklé. Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních právních předpisů.“
    - „(4) Písemná forma je zachována, je-li právní úkon učiněn telegraficky, dálnopisem nebo elektronickými prostředky, jež umožňují zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila.“
- Změna zákona o správě daní a poplatků, tak že §21 odst. 2 a 3 nyní zní:
    - „(2) Stanoví-li tak tento nebo zvláštní zákon, podávají daňové subjekty a své daňové povinnosti příslušnému správci daně přiznání, hlášení a vyúčtování na předepsaných tiskopisech. Tiskopisy zveřejněné v elektronické podobě lze podepsat elektronicky podle zvláštních předpisů.
    - (3) Jiná podání v daňových věcech, jako jsou oznámení, žádosti, návrhy, námitky, odvolání apod., lze učinit buď písemně nebo ústně do protokolu nebo elektronicky podepsané podle zvláštních předpisů či za použití jiných přenosových technik (dálnopis, telefax apod.).“
- Změna správního řádu, tak že §19 odst. 1 zní:
    - „(1) Podání lze učinit písemně nebo ústně do protokolu nebo v elektronické podobě podepsané elektronicky podle zvláštních předpisů.

[8] Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb. o upřesnění podmínek stanovených v §6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

Lze je též učinit telegraficky; takové podání obsahující návrh ve věci, je třeba písemně nebo ústně do protokolu doplnit nejpozději do 3 dnů.“

- Změna občanského soudního řádu, tak že §42 odst. 1 věta první zní:
  - „Podání je možno učinit písemně, ústně do protokolu, elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky nebo telefaxem.“
- Změna trestního řádu, tak že § 59 odst. 1 zní:
  - „(1) Podání se posuzuje vždy podle svého obsahu, i když je nesprávně označeno. Lze je učinit písemně, ústně do protokolu, elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky, telefaxem nebo dálnopisem.“
- Změna zákona o ochraně osobních údajů, tak v § 29 se doplňuje odst. 4, který zní:
  - „(4) Úřad uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb a provádí dozor nad dodržováním povinností stanovených zákonem o elektronickém podpisu.“
- Změna zákona o správních poplatcích, tak že v příloze k zákonu (sazebník správních poplatků) se doplňuje nová část XII, která zní:
  - Položka 162
    a) Podání žádosti o akreditaci poskytovatele certifikačních služeb

       100000.- Kč
    b) Podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky
       10 000.- Kč

2.2.2. Novelizace zákona o elektronickém podpisu

Zákon č. 227/2000 Sb o elektronickém podpisu, byl do dnešní doby několikrát novelizován. Například zákonem č. 226/2002 Sb., se doplňují v § 11 na konci odstavce tyto věty: „To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám.

Pokud je zaručený elektronický podpis založený na kvalifikovaném certifikátu užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.“

Zřízením Ministerstva informatiky zákonem č. 517/2002 Sb., byla převedena akreditace a dozor nad poskytovateli certifikačních služeb z Úřadu pro ochranu osobních údajů na Ministerstvo informatiky.

Na základě definování problémů v oblasti elektronického podpisu v dokumentu „Bílá kniha elektronického obchodu“, byl schválen zákon č. 440/2004 Sb., novela zákona o elektronickém podpisu. Tato norma nabyla účinnosti dne. 26. Července 2004 a zavádí do našeho právního řádu dvě důležité novinky, které mají vztah především k orgánům veřejné moci. Jsou to:

- Elektronická značka, kterou se rozumí údaje v elektronické podobě, které jsou připojeny k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:
    - Jsou jednoznačně spojené s označující osobou a umožňující její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
    - Byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
    - Jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat. Kvalifikovaný systémový certifikát je obdobou kvalifikovaného certifikátu, který může být vydán nejenom fyzické osobě ale i právnické osobě (majiteli označujícího zařízení).

Jak je z výše uvedeného textu patrné je elektronická značka vlastně elektronický podpis vytvořený technickým zařízením. Nejedná se, o podpis protože je vytvářená technickým zařízením v podstatě automatizovaně.[9] Rozdíl je také v seznámení se

[9] Podle občanského zákoníku jakožto obecného právního předpisu může právní úkon, jehož součástí je podpis, učinit pouze a jen fyzická osoba. Právní úkony právnické osoby činí ti, kteří k tomu oprávnění smlouvou o zřízení právnické osoby, zakládací listinou nebo zákonem, případně další osoby, pokud je to stanoveno ve vnitřních předpisech právnické osoby nebo je to vzhledem k jejich pracovnímu zařazení obvyklé. Jinými slovy-podepsat, a to ani elektronicky, se nemůže sama právnická osoba, nemůže se ale podepsat ani zařízení bez lidské obsluhy.

s obsahem zprávy. U podepsání elektronickým podpis se má za to, že podepisující osoba se seznámila s obsahem datové zprávy. U elektronické značky se vytváří právní fikce opačná, tj. má se za to, že označující osoba označila datovou zprávu bez předchozí kontroly obsahu datové zprávy. Používání elektronické značky mělo zásadní vliv na činnost veřejné moci v oblasti tzv. e-govermentu.

- Elektronická veřejná listina, jedná se o písemnost orgánu veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem. Tato listina má stejné právní účinky jako veřejná listina vydaná tímto orgánem. Znamená to, že při úředním, respektive soudním jednání se nemusí dokazovat jejich obsah (na rozdíl od listin soukromých).

Novela zákona o elektronickém podpisu zavádí do našeho právního časové razítko. Jedná se o nástroj, který hodnověrným způsobem zajišťuje přiřazení aktuálního časového údaje k elektronickému dokumentu. Můžeme tak získat informaci (důkaz) o tom, že uvedený dokument existoval v určitém čase. To může mít zásadní význam v řadě případů, např. při podání daňového přiznání či nabídky v soutěži o veřejnou zakázku atd. Novela také definuje kvalifikované časové razítko, jako datovou zprávu, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která musí obsahovat:

- Číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb;
- Označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal;
- Označení kvalifikovaného poskytovatele certifikačních služeb;
- Hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka;
- Data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno;
- Elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

Další změna zákona o elektronickém podpisu, nastala v roce 2007, kdy došlo zákonem č.110/2007 Sb., ke zrušení Ministerstva informatiky a tím k převedení kompetencí v oblasti elektronického podpisu na Ministerstva vnitra České republiky.

Poslední důležitou novelizací je zákon č. 167/2012 Sb., jehož hlavním přínosem je, že aplikuje „rozhodnutí Komise 2011/130/EU ze dne 25. Února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu," a rozhodnutí Komise Evropských společenství 2009/767/ES ze dne 16. Října 2009, kterým se stanoví opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst" podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu. Což ve své postatě umožňuje používání uznávaného elektronického podpisu a značky vydaném poskytovatelem usazeném mimo území ČR , nad kterým je prováděn dohled podle přepisů Evropské unie.

2.2.3. Nařízení vlády č. 304/2001 Sb., o elektronickém podpisu

Nařízení vlády ukládá povinnost orgánům veřejné moci zřídit elektronické podatelny a přijímat podání opatřená elektronickým podpisem. Jejich úkol je přijímání a potvrzování přijetí podání a příprava na jejich následného zpracování. Podatelny zpracovávají podání podle zákona o správě daní a poplatků, musí také zajišťovat doručování písemností na e-mailovou adresu žadatele.

Součástí činnosti podatelny musí být především kontrola čitelnosti podání (tj. zda je zpráva v některém z akceptovatelných formátů a zda neobsahuje viry). Dále zda kvalifikovaný certifikát žadatele je platný a zda jej vydal akreditovaný poskytovatel. Pokud podání nebude mít tyto náležitosti, musí orgán veřejné moci postupovat podle předpisů upravujících odstraňování vad podání.

Elektronická adresa podatelny musí být ve formátu posta@<doména orgánu>. Cz podle standartu ISVS č. 002/01. 03. Ostatní technické a programové vybavení musí odpovídat standardům ISVS vydaným ve Věstníku ÚVIS.

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

Atest ve smyslu zákona 365/2000 Sb., o informačních systémech veřejné správy, provádí několik komerčních subjektů, jejichž seznam je na stránkách ISVS. O atest může žádat jak dodavatel systému, tak orgán veřejné moci, který podatelnu provozuje. Pokud orgány veřejné moci již provozují elektronickou podatelnu bez jejího atestu, musí jej zajistit a to z vlastních prostředků.

S účinností od 1. 1. 2005 jej novelizuje nařízení vlády č. 495/2004 Sb. k e-podatelnám a vyhláška č. 496/2004 Sb. k e-podatelnám

2.2.4. Nařízení vlády č. 495/2004 Sb., kterým se prování zákon č. 227/2000 Sb.

Provozování elektronické podatelny se považuje za splněné rovněž v případě, kdy orgán veřejné moci dohodne s jiným orgánem veřejné moci, že bude přijímat a odesílat datové zprávy prostřednictvím jím provozované elektronické podatelny. Dále je nutné, aby provozovatel vybavil zaměstnance, kteří jsou oprávněni činit právní úkony v oblasti orgánů veřejné moci, kvalifikovanými certifikáty vydanými akreditovanými poskytovateli certifikačních služeb.

Orgán veřejné moci musí zveřejnit na své úřední desce informace potřebné k doručování datových zpráv orgánu veřejné moci. Těmito informacemi jsou alespoň:

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

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

2.2.5. Vyhláška č. 496/2004 Sb., o elektronických podatelnách

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

Především upravuje případy, kdy je zpráva přijata, kam se ukládá a jakým způsobem se eviduje, jak se potvrzuje doručení datové zprávy. Dále definuje povinnosti při odesílání datových zpráv.

Údaj, na jehož základě je možné osobu jednoznačně identifikovat, se uvádí ve struktuře desetimístného čísla v desítkové soustavě a je spravován ústředním orgánem státní správy. Jeho hodnota není zaměnitelná s rodným číslem a nesmí být osobním údajem zvláštního právního předpisu.

2.2.6. Vyhláška Ministerstva vnitra č. 212/2012 Sb., vyhláška o ověřování platnosti zaručeného elektronického podpisu

Zákonem 167/2012 byly zrušeno Nařízení vlády č. 495/2004 Sb., a bylo nahrazeno Vyhláškou Ministerstvo vnitra č. 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky,

kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka. Tato vyhláška nabyla účinnosti dne 1. července 2012.

3. METODIKA

Podstatou komunikace s veřejnou mocí je uznávaný elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Proto bych se rád, v následující kapitole věnoval popisu fungování elektronického podpisu, porovnání certifikačních autorit a problematice získání uznávaného elektronického podpisu. A vzhledem k tomu, že mám osobní zkušenost, jak na straně žadatele o kvalifikovaný certifikát, tak také na straně poskytovatele kvalifikovaného zaměstnaneckého certifikátu, budu se věnovat této problematice v obou rovinách.

3.1. Fungování elektronického podpisu

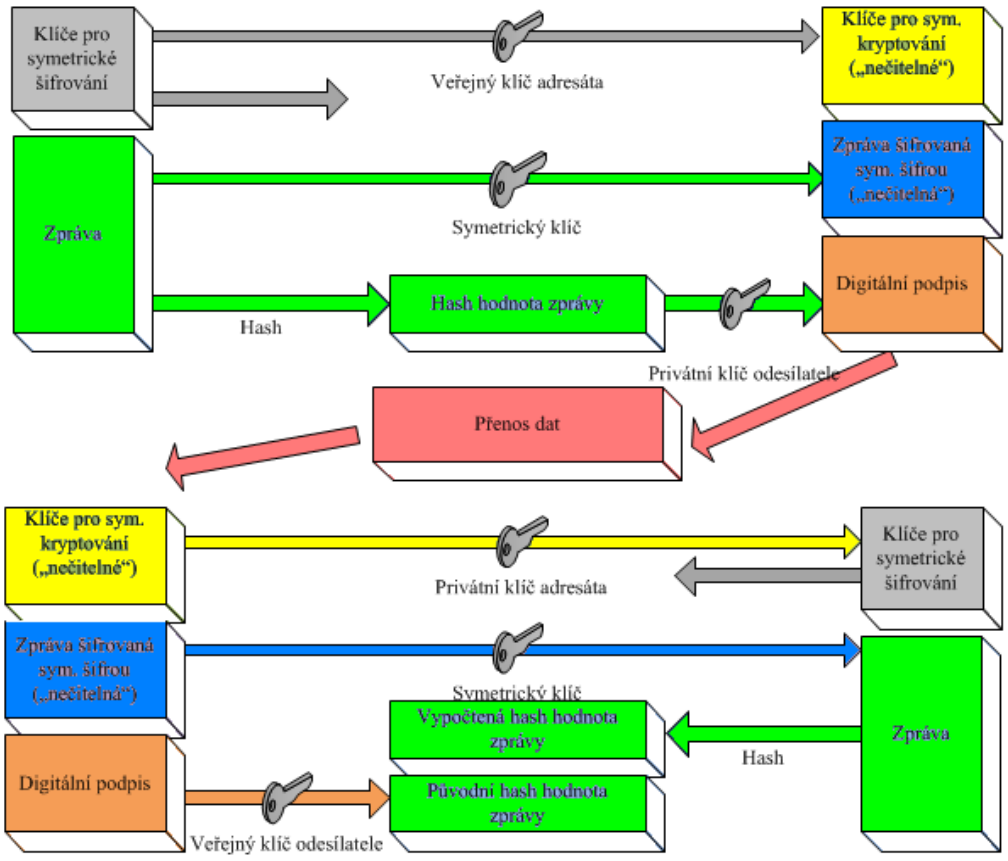
Při vytváření elektronického podpisu musí existovat data v elektronické podobě, která chce podepisující osoba podepsat. Není to tak dávno, co si většina lidí myslela, že elektronický podpis je pouze naskenovaný obrázek vlastnoručního podpisu, který je přidán k elektronické zprávě jako příloha. Takhle to samozřejmě nefunguje. Nejdůležitější pojmy pro správné pochopení fungování elektronického podpisu jsem popsal v předchozí kapitole.

Zabezpečenou komunikaci s využitím elektronického podpisu lze popsat takto:

- Odesilatel zprávy nejprve vytvoří hash hodnotu zprávy (součet) a tu zašifruje svým privátním klíčem, čímž zprávu elektronicky podepíše (vznikne elektronický podpis zprávy).
- Následně se celá zpráva zašifruje symetrickým klíčem (zajištění důvěrnosti zprávy). Symetrická šifra se používá z důvodu podstatně větší rychlosti šifrování.

- Samotný symetrický klíč je poté zašifrován veřejným klíčem adresáta, čímž je zaručeno, že se k tomuto klíči dostane pouze adresát se svým privátním klíčem, který ho užije k dešifrování zprávy.
- Zašifrovaná a elektronicky podepsaná zpráva je zaslána po Internetu adresátovi.
- Adresát zprávu dešifruje za pomocí svého soukromého klíče a získá přístup k symetrickému klíči.
- Celá zpráva se dešifruje pomocí symetrického klíče.
- Adresát zprávu ověří pomocí veřejného klíče odesilatele (ověření elektronického podpisu) a výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hash hodnotou z elektronického podpisu. Pokud jsou srovnávané hash hodnoty shodné, je zřejmé, že zpráva nebyla během podepsání a přenosu změněna (kontrola integrity zprávy).

Zabezpečená komunikace s EP



Obr: 3, [Zdroj: vlastní zpracování]

Vzhledem ke složitosti výše popsaného postupu není ani odesilatel ani adresát v roli specialisty na šifrování a dešifrování, ale pouze uživatel „prostředků pro vytváření elektronického podpisu“, což v tomto případě představuje technické a hlavně programové vybavení. Bez intuitivního programového vybavení by nejspíše elektronický podpis zůstal pouze pro odborníky na IT technologie a pro pár nadšenců.

3.2. Získání kvalifikovaného certifikátu

3.2.1. Obecný postup

V případě, že chceme používat uznávaný elektronický podpis pro komunikaci se státní a veřejnou zprávou, musíme k jeho vydání využít jednu ze tří akreditovaných certifikačních autorit.(viz.kapitola 3.3).

Při rozhodování je třeba zvážit několik aspektů.

- vybrat CA s přihlédnutím k ceně certifikátu
- zvážit účel použití uznávaného elektronického podpisu
- zvolit úložiště certifikátu (token, smart karta, MS Windows, atd.)

Po výběru certifikační autority a přihlášení do její webové aplikace, je dalším krokem vygenerování páru klíčů (veřejný, soukromý). V tomto okamžiku se musíme rozhodnout, zda bude pár klíčů generován jako exportovatelný, či nikoliv. Toto má zásadní vliv na budoucí použití elektronického podpisu. Zbývá jen vyplnit a uložit on-line formulář „Generování žádosti o vydání certifikátu“.

Po vygenerování žádosti je třeba zaznamenat ID žádosti pro vydání certifikátu. Bez znalosti ID nelze certifikát vystavit. Na nejbližší pobočce registrační autority[10] dojde k úřednímu ověření osobních údajů, uvedených v žádosti o generování certifikátu. Po uhrazení poplatku dojde k vygenerování certifikátu. Na základě našeho výběru je

[10] Registrační autoritou se rozumí subjekt smluvně zajišťující úřední ověření osobních údajů pro certifikační autoritu, může jím být certifikační autorita sama.

kvalifikovaný certifikát vydán buď na přenosném mediu, nebo zaslán elektronickou poštou nebo je možno ho získat z webových stránek certifikační autority.

Dalším krokem je instalace certifikátu do úložiště osobních certifikátů operačního systému. Pro bezproblémovou funkci různých aplikací a schopnost operačního systému správně vyhodnotit platnost elektronického podpisu je nezbytné zkontrolovat instalaci kořenového certifikátu certifikační autority. Kořenový certifikát certifikačních autorit je, kromě CA eIdentity, součástí operačních systému Windows. U certifikační autority eIdentity je třeba instalovat kořenový certifikát do úložiště důvěryhodných kořenových certifikátů operačního systému Windows. Tento certifikát je dostupný z webové aplikace výše uvedené CA.

3.2.2. Specifika výdaje zaměstnaneckého kvalifikovaného certifikátu

Na rozdíl od běžného žadatele, u zaměstnanců je postup výdeje certifikátu upraven smlouvou mezi certifikační autoritou a příslušnou právnickou osobou, či organizační složkou státu. Konkrétně na Ministerstvu obrany to byla v letech 2010 až 2012 smlouva s eIdentity a současné době smlouva s PostSignum. Výdej je specifický v následujících bodech:

- o způsobu uložení certifikátu rozhoduje MO
- osobní údaje, nutné pro vydání certifikátu, jsou rozšířeny o údaj o zastávané funkci, osobní identifikátor a identifikátor organizační jednotky
- osobní údaje žadatele nejsou zadávány do systému přímo žadatelem, ale prostřednictvím registrační autority MO (neveřejná).
- registrační autorita MO svým souhlasem potvrzuje oprávněnost žádosti
- výdej certifikátu probíhá pouze na výdejním místě v prostorách MO

Zaměstnanecký kvalifikovaný certifikát MO slouží nejen k podepisování datových zpráv, ale i k autorizovanému přístupu do interních systémů MO.

3.3. Certifikační autority

3.3.1. První certifikační autorita

Je prvním akreditovaným poskytovatelem certifikačních služeb v ČR pro oblast vydávání kvalifikovaných certifikátů podle zákona č. 227/200 Sb., o elektronickém podpisu a o změně některých zákonů. Byla akreditována 18.3.2002 Úřadem pro ochranu osobních údajů. V roce 2006 ji byla rozšířena akreditace Ministerstvem informatiky o možnost vydávat kvalifikované certifikáty a kvalifikované časové razítko. V současnosti poskytuje tyto služby:

- Vydání kvalifikovaného certifikátu
- Vydání kvalifikovaného systémového certifikátu
- Vydání komerčního osobního certifikátu
- Vydání komerčního serverového certifikátu
- Vydání kvalifikovaného časového razítka
- Dálkový přístup do seznamu zneplatněných certifikátů – CRL
- Možnost využití testovacího certifikátu.

Společnost První certifikační autorita, a.s., vydává v souladu s doporučením technické specifikace ETSI[11] TS 102 176-1 kvalifikované certifikáty s využitím hashovacích funkcí SHA-256 a SHA-512 v kombinaci s algoritmem RSA a délkou klíče 2048 bitů.

3.3.2. eIDENTITY a.s.

Ministerstvo informatiky ČR udělilo, dne 27.9.2005 akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb firmě eIdentity a.s.. Akreditovaná certifikační autorita eIdentity je tvořena kořenovou certifikační autoritou (RCA), která vydává kvalifikované systémové certifikáty pouze podřízeným autoritám (QCA a CCA). QCA poskytuje tyto služby:

- Vydání kvalifikovaného certifikátu;

[11] European Telecomunications Standarts Institute

- Vydání kvalifikovaného certifikátu s vyznačením identifikátoru ministerstva práce a sociálních věcí (MPSV);
- Vydání kvalifikovaného certifikátu s vyznačením pracovní pozice v organizaci (tzv. zaměstnanecký certifikát);
- Vydání kvalifikovaného systémového certifikátu;
- Vydání kvalifikovaného časového razítka;

CCA poskytuje tyto služby:

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

3.3.3. Česká pošta s. p.

Česká pošta je akreditovaným poskytovatelem certifikačních služeb na základě akreditace udělené Ministerstvem informatiky ČR, dne 3.8.2005. Certifikační autoritou České posty s.p. je PostSignum QCA. Úkolem certifikační autority PostSignum QCA je především vydávat a spravovat certifikáty certifikačních autorit PostSignum RooT QCA, PostSignum Qualified certifikační autority a zákazníkům české pošty v souladu a definovanými certifikačními politikami. Certifikační autorita poskytuje tyto služby:

- Vydání kvalifikovaného certifikátu;
- Vydání kvaltovaného systémového certifikátu (elektronická značka);
- Vydání kvalifikovaného časového razítka;
- Vydání komerčního certifikátu;
- Vydání komerčního serverového certifikátu.

Služby registračních autorit jsou zajišťovány poskytovatelem certifikačních služeb nebo externím subjektem na základě smlouva s Českou poštou s.p., jako poskytovatelem certifikačních služeb. Registrační autority zajišťují zejména tyto služby:

- Přijímají (registrují) žádosti o certifikát, schvalují je nebo zamítají v souladu s platnými certifikačními politikami;

- Ověřují totožnost žadatelů o certifikát;
- Zajišťují předání vydaného certifikátu žadateli;
- Zneplatňují certifikáty podle platných certifikačních politik.

Registrační autority zajišťované externím subjektem mohou poskytovat jen vybrané služby z výše uvedeného seznamu, což je stanoveno ve smlouvě mezi externím subjektem a Českou poštou.

3.4. Srovnání akreditovaných certifikačních autorit

Certifikační autority lze srovnávat dle mnoha rozličných kritérií. Z hlediska nejčastěji poskytované služby pro běžného uživatele, tj. výdej kvalifikovaného osobního certifikátu, jsou nejdůležitější tyto:

- Cena certifikátu;
- Rozsah služeb certifikační autority (prodloužení, rozšíření);
- Dostupnost certifikační autority;
- Důvěryhodnost certifikační autority.

Z ceníků uvedených na internetových stránkách je zřejmé, že nejlevnější je nabídka České pošty. Rozsah služeb je u všech uvedených certifikačních autorit srovnatelný, jinak strukturovaná nabídky eIdentity vypadá na první pohled jako nejobsáhlejší ale po podrobnějším průzkumu zjistíme, že se jedná pouze o modifikace jednotlivých certifikátu. Naopak eIdentity jako jediná neposkytuje testovací certifikát. V kategorii dostupnosti certifikační autority a hlavně registrační autority samozřejmě nemůžou ostatní dvě certifikační autority konkurovat české poště, která díky svým pobočkám jednoznačně vítězí v oblastech mimo Prahu.

Tab. 1 Porovnání cen certifikačních autorit s DPH.

	Certifikační autority		
Služby	PostSignum	I. CA	aIdentity
Kvalifikovaný osobní certifikát	396 Kč	495 Kč	478 Kč
Kvalifikovaný systémový certifikát	780 Kč	780 Kč	1113Kč
Komerční osobní certifikát	348 Kč	395 Kč	357.Kč
Komerční serverový certifikát	800 Kč	1170 Kč	1083 Kč
Zneplatnění certifikátu	Zdarma	Zdarma	Zdarma
Testovací certifikát	Zdarma	Zdarma	ne

Zdroj: [vlastní zpracování]

Pro stanovení důvěryhodnosti jednotlivých certifikačních autorit, je potřeba velmi důkladně prostudovat webové stránky a zvýšenou pozornost věnovat certifikačním politikám, a také takovým věcem jako je technická podpora, nápověda, zabezpečení webové aplikace atd.. Z vlastní zkušenosti mohu prohlásit, že v tomto ohledu je lehce vzadu PostSignum. Asi je to dáno poskytováním služeb hlavně pro nejběžnější klientelu, která je ovšem limitována technickými znalostmi a také přístupem k programovému vybavení. Jedná se o tak nepodstatné rozdíly, které nemají vliv na důvěryhodnost produktů výše uvedených certifikačních autorit. Doporučit, tak lze všechny tři certifikační autority. Myslím si, že v konečném rozhodování budou hrát hlavní roli cena a dostupnost, a v tom jednoznačně vítězí nabídka České pošty

Tab. 2 Porovnání certifikátů a služeb certifikačních autorit.

	Certifikační autority		
Služby	PostSignum	I.CA	aIdentity
Kvalifikovaný osobní certifikát	√	√	√
Kvalifikovaný systémový certifikát	√	√	√
Komerční osobní certifikát	√	√	√
Komerční serverový certifikát	√	√	√
Zneplatnění certifikátu	√	√	√
Testovací certifikát	√	√	√
Zneplatnění certifikátu	√	√	√
CRL	√	√	√
Testovací certifikát	√	√	Θ

Zdroj: [vlastní zpracování]

4. ELEKTRONICKÝ PODPIS V PODMÍNKÁCH STÁTNÍ SPRÁVY

Systém komunikace s elektronickým podpisem vychází z toho, že některé dokumenty existují pouze v elektronické podobě. Z tohoto důvodu nelze systém

s elektronickým podpisem zavádět osamoceně pouze v rámci jednoho úřadu státní správy, ale postupně na všech úřadech státní správy, zejména u soudů.

Práce s elektronickými dokumenty, zejména pak s dokumenty opatřenými elektronickým podpisem, vyžaduje i odpovídající technické zabezpečení na výrazně vyšší úrovni než u běžných systémů. Musí zaručovat bezpečné uložení a ochranu všech dokumentů, aby nemohlo dojít k jejich úmyslnému či neúmyslnému poškození, umožňovat trvalý přístup všech oprávněných pracovníků a má rovněž vyšší nároky na prokazování totožnosti všech uživatelů systému. Vzhledem k finanční náročnosti takových systémů je třeba je realizovat pokud možno jako centralizované, což v řadě případů opět může vést k organizačním změnám v rámci úřadu. Opodstatněná je zde i nedůvěra státních úředníků k elektronicky uloženým datům a práci s nimi.

Nelze opomenout fakt, že i ti, kteří chtějí elektronický podpis používat, si musí obstarat příslušné programové a technické vybavení. V případě komunikace s orgány veřejné je vyžadován zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb.

4.1. Vývoj elektronické komunikace ve státní správě do roku 2009

Před rokem 2000 byly možnosti elektronické komunikace se státní a veřejnou správou velmi omezené. Zásadním momentem bylo schválení zákona č. 227/2000 Sb., o elektronickém podpisu a následné vydání Nařízení vlády č. 304/2001 Sb., o elektronickém podpisu. Díky tomu bylo možné komunikovat se státní a veřejnou správou pomocí elektronických formulářů opatřených elektronickým podpisem.

Po stanovení závazných pravidel pro používání elektronického podpisu došlo k počátku elektronické komunikace. V prvních několika letech šlo, více méně o jednoduchou emailovou komunikaci na úřední emailovou adresu jednotlivých centrálních úřadů státní správy. Postupem času se k centrálním úřadům přidaly další subjekty veřejné správy. Schválením zákona o elektronických podatelnách v roce 2004 docházelo k postupnému zřizování tzv. e-podatelen jednotlivých úřadů. Přesto že došlo k podstatnému zjednodušení elektronické komunikace, pořád se jednalo pouze o několik

málo webových aplikací. V té době byly na Portálu veřejné správy v aplikaci Elektronické podání dostupné pouze následující služby:

- Služby Generálního ředitelství cel
- Služby Ministerstva práce a sociálních věcí
- Služby Ministerstva financí
- Služby Ministerstva průmyslu a obchodu
- Služby Ministerstva dopravy
- Služby Ministerstva životního prostředí

Ve smyslu elektronické komunikace, tj. nahrazení papírové formy většiny dokumentů formou elektronickou, se dá hovořit pouze o Celní správě ČR. Všichni si velmi dobře pamatujeme na situace na celních úřadech před zavedením elektronické formy komunikace. Celní správa ČR byla ve své podstatě donucena, obrovským nárůstem individuálního dovozu k masivní elektronizaci.

V souvislosti se vstupem české republiky do EU se ČR zapojila do projektu Evropské komise v oblasti cel, tzv. e-Customs. Hlavním cílem projektu e-Customs je dosažení 100% celních prohlášení pouze v elektronické podobě. Celní správa České republiky se zapojila též do projektu e-Vývoz [12]. Cílem systému e-Vývoz je umožnit elektronické podávání celního prohlášení do režimu vývozu a naplnit tak požadavky Evropské komise. Systém e-Vývoz umožňuje celním úřadům v režimu vývozu elektronickou výměnu informací, která automatizuje činnosti v rámci samotné vývozní operace a zvyšuje účinnost kontroly. Deklarantům zároveň umožňuje podání právně závazného celního prohlášení elektronicky, podepsaného zaručeným elektronickým podpisem. Systém obsahuje tři domény:

- společná doména – propojuje informační systémy jednotlivých členských států EU a jedná se o provozní a monitorovací služby
- národní doména – propojuje informační systém celní správy se všemi celními orgány v ČR. Zároveň umožňuje propojení na společnou a vnější doménu.

[12] e-Vývoz – elektronické celní prohlášení v režimu vývozu.

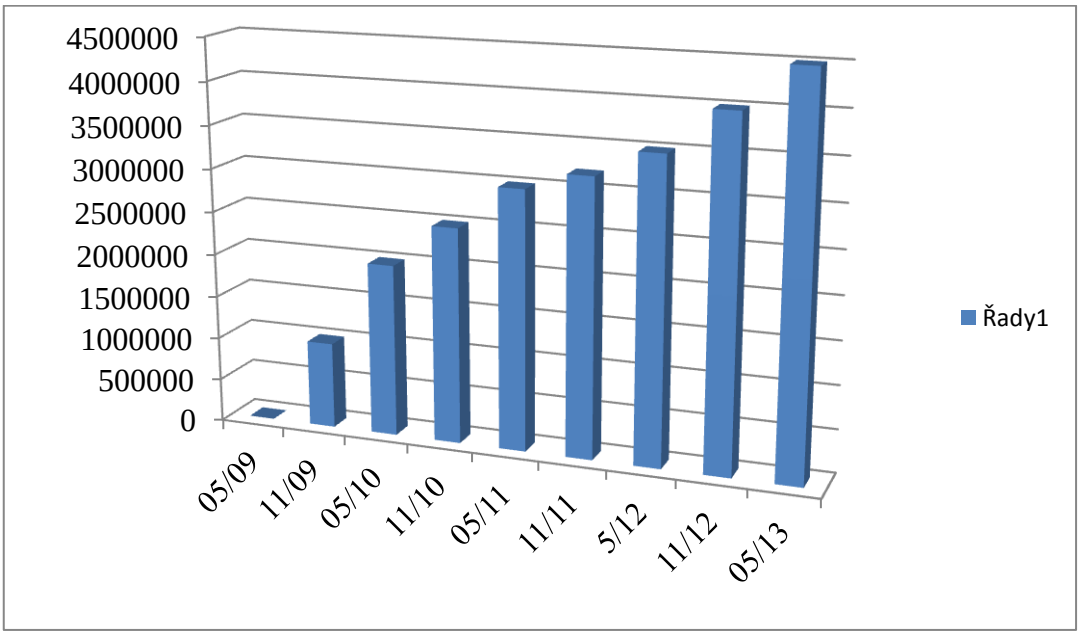
- vnější doména – propojuje deklaranta a celní úřad vývozu, umožňuje elektronické podání vývozního celního prohlášení a veškerou komunikaci spojenou s tímto úkonem.

Od 1. července 2009 se Celní správa České republiky zapojila i do projektu e-Dovoz[13]. K zavedení systému e-Dovozu vedly EU v neposlední řadě bezpečnostní důvody. Jedná se o předcházení dovozu nebezpečného, či jinak rizikového zboží, tak že celní řízení proběhne elektronicky ještě mimo území našeho státu.

4.2. Aktuální stav elektronické komunikace ve státní správě

Zákon č 300/2008 Sb., o elektronických úkonech a autorizované konverzi, umožnil zřízení datových schránek jiným subjektům než orgánům veřejné moci. Následná novelizace v polovině roku 2009 zavedla tolik diskutovanou povinnost orgánů veřejné moci doručovat dokumenty přednostně do zřízené datové schránky. Jak ukazuje následující graf, došlo k obrovskému nárůstu počtů datových zpráv.

Graf:1 Nárůst počtu datových zpráv po roce 2009



[13] e-Dovoz – elektronické celní prohlášení v režimu dovozu.

Jednotlivá ministerstva byla zahlcena datovou komunikací a tak byla donucena urychlit proces elektronizace. Komunikace veřejné správy s občanem je vedena prostřednictvím e-podatelen a datových schránek přijímajících datové zprávy. V současnosti probíhá elektronická komunikace s orgány státní správy prostřednictvím webových aplikací jednotlivých ministerstev a k tomu zřízených portálů:

- Ministerstvo práce a sociálních věcí
    - integrovaný portál MPSV
- Ministerstvo financí
    - daňový portál elektronické služby finanční správy České republiky
    - celní správa
- Ministerstvo vnitra
    - informační systém datových schránek
    - CzechPoint
- Ministerstvo pro místní rozvoj
    - Elektronické tržiště veřejné správy

Jedním z neviditelnějších a řekl bych i nejúspěšnějších projektů je CzechPOINT. Jedná se o projekt iniciativy eStat.cz, Ministerstva vnitra ČR a České pošty. Název CzechPOINT představuje zkratku: Český podací ověřovací a informační terminál.

CzechPOINT je garantovanou službou pro komunikaci se státem prostřednictvím jednoho universálního místa. V konečné fázi se předpokládá, že občan bude schopen své záležitosti ve vztahu k veřejné moci realizovat z pohodlí domova prostřednictvím internetu a datových schránek. Jedním ze základních předpokladů je rozšíření zaručeného elektronického podpisu mezi laickou veřejnost. Projekt CzechPOINT neznamená konec specializovaných pracovišť úřadů, jako například katastrální úřad ale soustředí se pouze na vydávání výpisu, kdež to specializovaný úřad bude nadále spravovat a aktualizovat příslušné registry.

Ve stejném období byl spuštěn projekt „Základní registry veřejné správy“. Aby mohlo dojít ke spuštění výše uvedeného projektu, bylo nezbytné schválit příslušnou právní úpravu. V roce 2009 tak došlo k přijetí zákona č. 111/2009 Sb., o základních

registrech a zákona č. 227/2009 Sb. Tyto zákony vytvořily předpoklad pro spuštění systému registrů k 1.7.2010 ve zkušebním provozu a rok později v ostrém provozu.

Hlavním prvkem systému je tzv. referenční údaj, který je vymezen speciálním zákonem a který je uchován v jednom základním registru. Ostatní registry tento údaj ze základního registru přebírají. Všechny oprávněné orgány veřejné moci musí mít přístup do základního registru z důvodu aktualizace vedených údajů.[14]

Třetím neméně významným projektem současné státní správy je eOP. Jedná se nový elektronický občanský průkaz, kterým bude možné identifikovat občana České republiky do základních registrů veřejné správy a dalších informačních systémů veřejné správy. Vedle standardního občanského průkazu existuje občanský průkaz s implementovaným kontaktním čipem, na který je možné si nechat vygenerovat zaručený elektronický podpis.

5. ELEKTRONICKÝ PODPIS V PODMÍNKÁCH MINISTERSTVA OBRANY

5.1. Zřízení a oblast působnosti Ministerstva obrany

Ministerstvo bylo zřízeno s účinností od 8. prosince 1992 zákonem č. 548/1992 Sb., kterým byl změněn zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky. Tento kompetenční zákon (ve znění pozdějších předpisů) vymezuje základní působnost ministerstva. Ministerstvo obrany je tak ústředním orgánem státní správy zejména pro:

- Zabezpečování obrany České republiky
- Zřízení Armády České republiky
- Správou vojenských újezdů

[14] MATES, Pavel, SMEJKAL, Vladimír. E-government v českém právu. Vyd. Linde Praha a.s. – právnické a ekonomické nakladatelství a knihkupectví Bohumily Hořínkové a Jana Tuláčka, 2006. 244 s. ISBN80-7201-614-8

Ministerstvo obrany jako orgán pro zabezpečování obrany:

- podílí se na zpracování návrhu vojenské obranné politiky státu
- připravuje koncepci operační přípravy státního území
- navrhuje potřebné opatření k zajištění obrany státu vládě, radě obrany a prezidentu České republiky
- koordinuje činnost ústředních orgánů, správních orgánů a orgánů samosprávy a právnických osob důležitých pro obranu státu při přípravě k obraně
- řídí vojenské zpravodajství
- zabezpečuje nedotknutelnost vzdušného prostoru České republiky a koordinaci vojenského letového provozu s civilním letovým provozem
- organizuje a provádí opatření k mobilizaci Armády České republiky k vedení evidence občanů podléhající branné povinnosti a k vedení evidence věcných prostředků, které budou za branné pohotovosti poskytnuty pro potřeby AČR
- povolává občany České republiky k plnění branné povinnosti.

Z výše uvedeného výčtu činnosti zabezpečovaných Ministerstvem obrany vyplývá, že jeho činnost je zaměřena spíše k odborné veřejnosti a hlavně vůči jiným subjektů státní a veřejné zprávy. Z tohoto důvodu je i elektronická komunikace úřadu MO v podstatě omezena na standardní provoz datové schránky a e-podatelny. Většina elektronické korespondence laické veřejnosti s MO je vedena formou běžné emailové korespondence bez autorizace elektronickým podpisem.

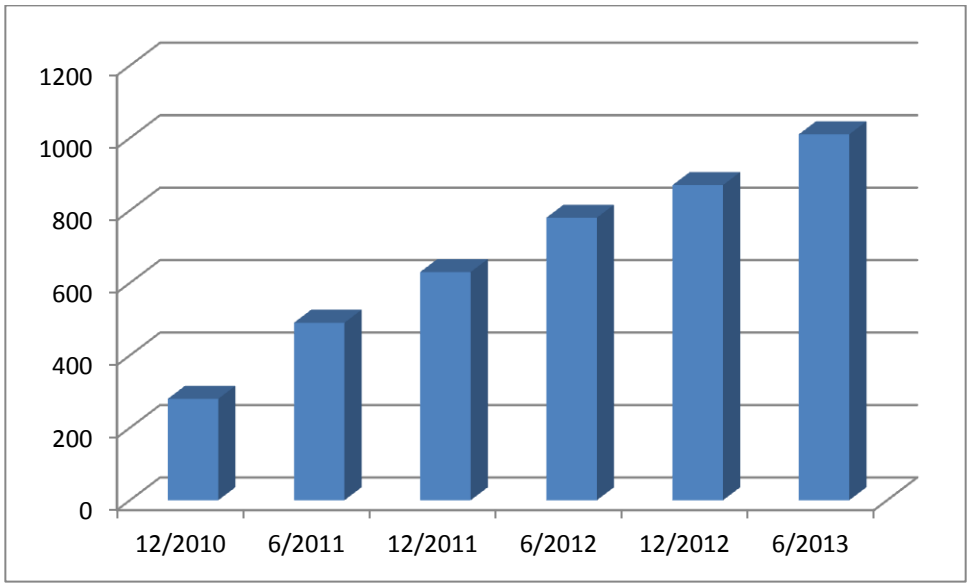
5.2. Využívání elektronického podpisu na Ministerstvu obrany

Elektronický podpis na MO, je v gesci „Odboru bezpečnosti MO“, který v roce 2009 rozhodl o nákupu kvalifikovaných certifikátu pro potřeby MO. V následujícím roce proběhla veřejná soutěž na autorizovaného poskytovatele certifikačních služeb. Vítězem se stala CA eIdetity, která následně uzavřela smlouvu o poskytování zaměstnaneckých kvalifikovaných certifikátu. Vzhledem ke skutečnosti, že eIdentity využívá jako registrační autoritu smluvní subjekty, bylo MO nuceno najít subjekt, který bude odpovídat bezpečnostním standardům nastaveným Odborem bezpečnosti.

Bylo zvažováno několik variant, ale nakonec bylo vydávání svěřeno „Oddělení řízení a správy bezpečnostních systému Velitelství ochranné služby Vojenské policie“. Myslím si, že výběr vojenské policie jako registrační autority není v souladu s platnou legislativou. Vojenská policie byla zřízena zákonem č.124/1992 Sb., o vojenské policii, kde se činnost, ve smyslu registrační autority ani jiná podobná nevyskytuje. MO na tuto skutečnost zareagovalo zařazením této činnosti do novely zákona o vojenské policii, který se nachází ve schvalovacím procesu v Poslanecké sněmovně Parlamentu České republiky.

Výdej elektronického podpisu, založeném na zaměstnaneckém kvalifikovaném certifikátu, byl zahájen dne 1.10.2010. Z důvodu maximální bezpečnosti výše uvedeného elektronického podpisu je vydáván na bezkontaktní kartě Cotag, vybavené kontaktním čipem. Z rozhodnutí ředitele odboru bezpečnosti MO, byl elektronický podpis vydáván pouze ředitelům (velitelům) samostatných organizačních celků MO a jejich zástupcům. Po rozšíření vydávání na další odborné orgány MO je počet ročně vydaných certifikátu cca. 1000 kusů.

Graf: 2 Vývoj počtu vydaných elektronických podpisů



Zdroj: Vlastní zpracování

Jedním z prvních systému, kde bylo zavedeno používání elektronického podpisu na MO, byl „Systém elektronické podpory obchodování“ (SEPO). Systém SEPO byl od 1.1. 2006 do 30.6.2012 elektronickým nástrojem Ministerstva obrany pro nabývání majetku, pořizování služeb a stavebních prací realizovaných formou veřejných zakázek malého rozsahu ve smyslu zákona č. 137/ 2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů. Elektronický podpis sloužil k autorizaci odpovědných zaměstnanců při řešení jednotlivých zakázek. Na základě usnesení vlády ČR ze dne 10. května 2010 rozhodlo MO o zrušení systému SEPO a využíváni e-tržiště Tendermarket. Využití EP je zde stejné jako v SEPO.

Dalším systémem, ve kterém je povinnost používat k autorizaci elektronický podpis na MO, je archivní a spisová služba MO, která je součásti štábního informačního systému (ŠIS AČR). Výše uvedený systém v současnosti postupně nahrazuje klasické spisovny a je přímo zodpovědný za autorizovanou konverzi dokumentů MO a AČR.

Nejnovějším systémem kde bylo zavedeno používání EP je „státní pokladna“. Jedna se o centrální systém účetních informací státu (CSÚIS), který je určen ke shromažďování účetních záznamů od vybraných účetních jednotek.

U některých organizační celky MO využívají nové rozhraní v systému CzechPOINT a to CzechPOINT@ofifice. Toto rozhraní bylo vytvořeno za účelem autorizované konverze z moci úřední a pro výpis nebo opis z Rejstříku trestů. Autorizovaná konverze z moci úřední slouží pro vnitřní potřebu úřadu, zajišťuje převedení dokumentů z listinné podoby do elektronické a naopak.

Vojenská policie využívá zaručený elektronický podpis založený na kvalifikovaném zaměstnaneckém certifikátu k zabezpečené komunikaci s Národním bezpečnostním úřadem.

ZÁVĚR

Uplynulo již třináct let od doby, co byl uznávaný elektronický podpis kodifikován do našeho právního řádu zákonem č.227/2000 Sb., o elektronickém podpisu. Za tuto dobu se stal elektronický podpis nedílnou součástí e-Governmentu a pro uživatele orientující se v dané problematice běžnou záležitostí, která jim usnadňuje život, obzvláště při komunikaci s orgány státní a veřejné správy. Ale je ještě mnoho těch, co nemají tušení co vlastně elektronický podpis je a jak by se dal využít v běžném životě.

Paradoxně na tom má velký podíl velmi úspěšný projekt Ministerstva vnitra a České pošty „CzechPoint“. Pro lidi co často nekomunikují se státní a veřejnou správou se elektronický podpis nevyplatí. Pořizovací cena nejlevnějšího elektronického podpisu stále převyšuje náklady běžného uživatele za úřední ověření podpisu na přepážce CzechPoint. Doufám, že má bakalářská práce pomohla, alespoň malým dílem, ke zviditelnění elektronického podpisu a možností s ním spojených.

Pravdou je, že Česká republika je v současnosti vnímána zahraničními subjekty, jako vynikající partner, co se týká zavádění nejnovějších poznatků v oblasti elektronického podpisu a vždy byla v podstatě mezi prvními v implementaci závěrů mezinárodních odborných komisí. Bohužel na domácí frontě už to tak slibně nevypadá. Například trojí změna akreditační autority poněkud zkomplikovala plynulé zavádění systému a jeho následný provoz. Zároveň je třeba vyzdvihnout zaměstnance, kteří mají tuto problematiku na starosti a i v tom nepříliš stabilním prostředí české politiky, dokázali to, co se v mnoha ostatních členských státech EU dodnes nepodařilo. Za to mají můj velký obdiv.

Velmi slibným počinem je zavádění tzv. e-OP (občanský průkaz s kontaktním čipem). Jedinou vadou na kráse celého projektu e-OP je výše poplatku za jeho vydání, který aktuálně činí 500 Kč. Považoval bych za efektivnější, kdyby byl projekt e-OP spolufinancován s přispěním fondů EU. Při masivnějším rozšíření elektronického podpisu implementovaného do kontaktního čipu by odpadlo dilema, zda použít token, přenosnou paměť či jiné záznamové médium. Napadá mě velmi zajímavý způsob, jak zajistit rozšíření elektronického podpisu pro širokou veřejnost. Mám tím na mysli, že by vytvoření účtu na sociálních sítích např. Facebook bylo podmíněno zřízením

elektronického podpisu. Tím by odpadly problémy s podvodně registrovanými účty a zároveň by došlo k obrovskému rozmachu této technologie. Ale to se asi nestane. Považoval bych za velký úspěch, kdyby alespoň ve státní a veřejné správě bylo využívání elektronického podpisu, nějakým způsobem spojeno s registrací do budovaného státního informačního systému, popř. do jeho jednotlivých částí. A tím by se dostal do většího povědomí ve státním sektoru.

CONCLUSION

Thirteen years have been passed since a recognized electronic signature codified in our legal system law č.227/2000 Name it., The electronic signature. During this time it became an integral part of the electronic signature of e-Government and for users focusing on the issue of ordinary matter that makes life easier for people who communicating with government and public administration. But there are many of those who have no idea what an electronic signature is and how it could be used in everyday life.

Paradoxically, it has a large proportion of very successful project of the Ministry of Interior and the Czech Post "CzechPoint". For people who often do not communicate with the state and public administration, electronic signature worthwhile. The purchase price of the cheapest electronic signature still exceeds the cost of the current user for the official signature verification at the counter CzechPoint. I hope that my bachelor work thesis help, at least in small part, to the visibility of the electronic signature and opportunities associated.

Czech Republic is currently perceived by foreign entities such excellent partner in introducing the latest knowledge in the field of electronic signature and has always been essentially among the first to implement the conclusions of the international expert committees. However, on the home front so it does not look promising. For example, a threefold change accreditation authority rather complicated smooth implementation of the system and its subsequent operation. It is also about to be commended for employees who have to worry about this issue, and even the very stable environment

Czech politics, did what in many other EU Member States still failed. For that they have my admiration.

Very promising achievement is the introduction of e-ID (identification card with contact chip). The only shortcoming of the project e-OP is the fee for his release, which currently amounts to 500 CZK. I would consider more effective if the project e-OP co-financed with the contribution of EU funds. With its mass of electronic signature embedded in a contact chip would be no dilemma whether to use a token, portable memory or other storage medium. It occurs to me a very interesting way of ensuring the use of electronic signatures for the general public. I mean, that would create an account on social networking sites such as Facebook was the establishment of an electronic signature. This would be no problems with fraudulently registered accounts and at the same time there has been a huge boom in this technology. But that is about to happen. I would consider it a great success, at least if the state and public administration to use electronic signature in some way connected with registration built into the national information system, or. into individual parts. And that would be in greater awareness in the public sector.

Literatura

DOSTÁLEK, Libor. VOHNOUTOVÁ, Marta. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 1. Vyd Brno: Computer Press, 2006. s. 536 ISBN: 80-251-0828-7.

BUDIŠ,Petr. *Elektronický podpis a jeho aplikace v praxi*. 1. Vyd. Olomou: Anag, 2008. 160 s. ISBN 978-80-7263-465-1.

KOBÍK,J., KOHOUTKOVÁ, A. *Daňový řád s komentářem*. Olomouc: Nakladatelství Anag. 2010. S. 960.

MATES, Pavel, SMEJKAL, Vladimír. *E-government v českém právu*. Vyd. Linde Praha a.s. – právnické a ekonomické nakladatelství a knihkupectví Bohumily Hořínkové a Jana Tuláčka, 2006. 244 s. ISBN80-7201-614-8

BOSÁKOVÁ, Dagmar. *Elektronický podpis: přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů*. Olomouc: Anag. 2002. 141. S. ISBN 80-7263-125-X.

LOUDA, T. et al *Modernizace veřejné správy v Evropě a České republice*. 1. Vyd. Plzeň: Aleš Čeněk, 2006. 351 s. ISBN 80-7380-0001-2.

JAŠEK, R. et al. Informační technologie ve veřejné správě. 1. Vyd. UTB Zlín 2007. ISBN 978-80-7318-607-4.

ŠTĚDROŇ, B. *Úvod do e-governmentu v České republice: právní a technický průvodce.* 1. Vyd. Praha: Úřad vlády České republiky, 2007. 172 s. ISBN 978-80-87041-25-3.

LIDINSKÝ, V. et al. eGovernment bezpečně. 1. Vyd. Praha: Grada Publishing, 2008. 145 s. ISBN 978-80-247-2462-1.

KATZ, Jonathan. *Digital signatures*. 1st ed. London:Springer 2010 183 s. ISBN 978-0-387-27711-0.

VANÍČEK, Z. et al. *Právní aspekty eGovernmentu v ČR*. Praha: Linde Praha, 2011. 200 s. ISBN 978-80-7201-855-0.

POLČÁK, R. *Práva a evropská informační společnost*. Brno: Masarykova univerzita, 2009. 203 s.

Zákony:

Zákon č. 227/2000 Sb., elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

Zákon č. 440/2004 Sb., kterým se mění zákon č. 227/2000 Sb., elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

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

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů

Nařízení vlády č. 495/2004 Sb., kterým se prování zákon č. 227/2000 Sb., elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

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

Vyhláška Ministerstva vnitra č. 212/2012 Sb., vyhláška o ověřování platnosti zaručeného elektronického podpisu

Internetové zdroje:

Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu [online]. [cit. 2011-02-21]. Dostupný z WWW: http://www.mvcr.cz/soubor/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronického-podpisu.aspx

Směrnice evropského parlamentu a rady 1999/93ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy [online]. [cit. 2011-02-14]. Dostupný z WWW:

SMEJKAL, Vladimír. *Elektronický podpis v praxi* [online]. 2001, [cit. 2008-02-25]. Dostupné na WWW: http://pravniradce.ihned.cz/c4-10078240-10025905-F00000_detail-elektronicky-podpis-v-praxi

UNCITRAL [online].[cit. 2011-02-14]. Dostupný z:http://www.uncitral.org

http://www.mocr.army.cz/ministr-a-ministerstvo/pusobnost-a-cinnosti/pusobnost-a-cinnosti-5131/

http://www.mocr.army.cz/dokumenty-a-legislativa/dokumenty/zakony-a-provadeci-pravni-predpisy-172/

Oficiální webové adresy:

www.mvcr.cz
www.mpsv.cz
www.army.cz
www.mmr.cz
www.mfcr.cz
www.postsignum.cz
www.ica.cz
www.eidentity.cz
www.eportal.cz
www.gov.cz
www.mojedatovaschranka.cz
www.statnipokladna.cz