Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Bakalářská práce

Elektronický podpis v právní úpravě a praxi

Vedoucí bakalářské práce: Mgr. Ivana Hájková

Vypracoval: Jan Hobza

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Elektronický podpis v právní úpravě a praxi“ vypracoval samostatně s použitím pramenů uvedených v seznamu použité literatury a po odborných konzultacích.

V Praze dne 25. března 2001

……
Jan Hobza

Poděkování

Touto cestou bych chtěl zejména poděkovat Mgr. Ivaně Hájkové, RNDr. Dagmar Brechlerové, Mgr. Pavlu Vondruškovi a doc. Ing. Vladimíru Smejkalovi, CSc., za jejich cenné rady a odborné konzultace, které mi v průběhu zpracovávání poskytovali.

Elektronický podpis v právní úpravě a praxi
Electronic signature in law and practice

Souhrn

Se vstupem do 21. století je zřejmé, že rozvoj moderní společnosti se neobejde bez rychlé a bezpečné komunikace. K tomu, aby komunikace v nezaručeném prostředí, kterým je například Internet, byla bezpečná, pomáhá právě elektronický podpis. Správně vytvořený elektronický podpis mimo jiné identifikuje podepisující osobu a zaručuje integritu zaslaného dokumentu.

Česká republika přijala zákon o elektronickém podpisu, který zrovnoprávňuje elektronický podpis s vlastnoručním a umožňuje jeho používání i na úrovni orgánů veřejné moci. Výhody, které nám zákon poskytuje, budeme moci využívat až po vydání tzv. prováděcí vyhlášky k zákonu, která je nezbytným technickým doplňkem zákona. Nic nám ale nebrání, používat elektronický podpis již nyní, bude-li naše komunikace založená na smluvním ujednání. Zákon o elektronickém podpisu vychází ze Směrnice EU 1999/93/ES, která sjednocuje používání elektronického podpisu na území EU.

Klíčová slova

Elektronický podpis, certifikační autorita, kvalifikovaný certifikát, akreditace, Zákon o elektronickém podpisu, Směrnice EU, asymetrická kryptografie, klíč.

Summary

It becomes obvious with the entrance of 21st cetury, that the growth of a modern society would not be possible without fast and safe communication. Electronic signature helps to create a safe communication chanel even in an unsecure environment as the Internet. Correctly created electronic signature identifies the undrsigned person and gives security of the integrity of the document.

Czech republic accepted the Electronic signature Act, which emancipates the electronic signature to a holograph signature and allows its application on the level of state power body. It will be possible to make any use of those facilities, which the Act brings into life, when is issued the executive edict for this Act. On the other hand, there is no reason not to use the electronic signature already, as long as the communication is

based on contract arrangement. The electronic signature act is based on the EU directive 1999/93/ES, which consolidates the use of electronic signature in the EU domain.

Keywords

Electronic signature, certification authority, qualified certificate, accreditation, Electronic signature act, EU directive, asymmetric cryptography, key.

Obsah

1. Úvod

V dnešní době neexistuje oblast našeho života, kde bychom se nesetkali s počítačem. V zaměstnání, v obchodě, u lékaře, samozřejmě v bance, ale zcela určitě v kterémkoli úřadě veřejné či státní správy přicházíme do styku s výpočetní a informační technikou. Postupný přechod od papírových dokumentů k elektronickým probíhá všude ve světě a všude ve světě je tedy problém zrovnoprávnění elektronického zápisu s papírovým z hlediska zákona více než aktuální. Některé právní řády umožňují výkladem svých norem nelpět na konkrétním nosiči informací, ale speciálně v podmínkách kontinentálního právního systému, ve kterém převládá pozitivistický přístup, je třeba technologické možnosti podložit právní úpravou.

Klíčovou roli v této problematice hraje právě podpis, resp. elektronický podpis. E-podpis se dá využít všude tam, kde je dnes nutné úřední razítko či ruční podpis občana nebo úředníka. Všechny dokumenty, které zatím známe v papírové podobě, lze převést na dokumenty elektronické a všechny podpisy je možné nahradit jejich elektronickou formou. Podepisovat i ověřovat podpisy lze takto nesrovnatelně rychleji a efektivněji; je možné podepsat dokonce i to, co lze ručně opatřit podpisem jen velmi těžko – obsah diskety, fotografii, přístupy do databáze apod.

V této souvislosti je třeba si uvědomit, že existují v zásadě tři druhy podpisu:

a) Určitá posloupnost znaků, která reprezentuje určitou osobu. Takovýto podpis může být nahrazen i mechanickým prostředkem a má nejnižší právní váhu. Plní tedy pouze funkci identifikační a to bez jakékoli právní záruky. Takovýto podpis, byť by se jednalo o posloupnost znaků v elektronické podobě, není elektronickým podpisem.

b) Vlastnoruční podpis, který splňuje požadavky ObčZ, má již mnohem vyšší právní váhu. Plní funkci jak identifikační, tak autentizační, neboli umožňuje ověření totožnosti podpisu identifikované osoby s daným podpisem. Tyto funkce elektronický podpis splňuje, jedná se však o tzv. „obyčejný“ elektronický podpis.

c) Nejvyšší právní váhu má „papírový“ podpis ověřený. Tuto formu vyžadují např. zvláštní právní úkony stanovené v obchodním zákoníku. Jedná se o podpis provedený před třetí osobou (nejčastěji notářem), která ověří totožnost podepisující osoby. Takovýto podpis plní i funkci legalizační. V této souvislosti můžeme hovořit o tzv. zaručeném elektronickém podpisu.

Zaručený elektronický podpis však poskytuje oběma stranám další funkce, kterých s běžným papírovým podpisem nemůžeme nikdy dosáhnout. Takovýto podpis navíc zaručuje integritu podepsané zprávy. Příjemce má tedy jistotu, že zpráva od momentu jejího podepsání již nebyla změněna.

Je zřejmé, že zaručený elektronický podpis přináší do soukromého, ale hlavně do obchodního života mnohé vítané kvality a perspektivy. Není proto s podivem, že se ve většině vyspělých států stává elektronický podpis součástí právního řádu. Význam zákonodárství o elektronickém podpisu podtrhuje skutečnost, že 30. června 2000 prezident Clinton podepsal nový federální zákon o digitálních podpisech, přestože většina států v USA již tyto zákony uvedla do praxe. Na tomto příkladě je vidět složitost přibližování elektronického světa ke klasickému prostředí papírových dokumentů. Zároveň je však dokladem rozvoje informační revoluce, která si vynucuje změny nejen ve stylu práce a v životním stylu vůbec, ale i v základních právních pojmech a procedurách. Tlak na změnu hodnot vytváří především dramatický rozvoj elektronického obchodování.

Zakotvení elektronického podpisu a očekávaný následný rozvoj elektronického obchodu v ČR by měl přinést značné efekty pro národní hospodářství státu, protože elektronický obchod bude významným motorem růstu světové ekonomiky v 21. století a klíčovým faktorem konkurenceschopnosti. Stejně tak může vnést zcela nové směry do výkonu veřejné správy, kdy lze reálně očekávat vytvoření paralelní možnosti ke styku občana a úřadu prostřednictvím elektronické pošty (z domu, zaměstnání či tzv. internetových kiosků). Lze si tedy představit např. zasílání daňových přiznání, odhlášení motorového vozidla nebo jiných úředních dokumentů tímto způsobem.

2. Cíl a metodika práce

2.1. Cíl práce

Bakalářská práce Elektronický podpis v právní úpravě a praxi si klade za cíl analýzu stávající situace elektronického podpisu v oblasti práva s návazností na praktické využití elektronického podpisu a certifikace. Vzhledem k aktuálnosti a obecné neznalosti daného problému, vychází v řadě médií články, které tuto problematiku značně zkreslují a zamlžují. V této práci se tedy pokouším objektivně popsat problematiku elektronického podpisu a podat výklad některých právních norem, které tuto problematiku řeší a které jsou či budou pro Českou republiku závazné. Poznatky, které v průběhu práce získám, použiji pro nastínění řešení problémů spojených se zaváděním elektronického podpisu do právního řádu České republiky. Zaměřím se též na technickou stránku věci, která je nezbytná pro ucelené chápání problému.

2.2. Metodika práce

V první části práce se zaměřím na stěžejní právní dokument z oblasti elektronického podpisu, kterým je zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů ze dne 29. června 2000. V této části se pokusím podat jeho výklad a zhodnocení.

Druhým bodem mé práce bude výklad vyhlášky Úřadu pro ochranu osobních údajů, kterou se provádí § 6 a § 17 zákona o elektronickém podpisu. Tato vyhláška byla v době zpracovávání této práce v tzv. mezirezortním jednání vlády a měla by vstoupit v platnost v polovině roku 2001.

Třetím bodem mé práce bude popis přístupu Evropské unie k řešené problematice a srovnání našeho a evropského postupu v oblasti elektronického podpisu.

Jak již bylo uvedeno, zaměřím se ve své práci také na technologickou stránku provádění elektronického podpisu a pokusím se dát do souvislosti poznatky zjištěné při zkoumání právní úpravy se závěry zkoumání této praktické stránky daného problému.

Závěrem své práce zhodnotím zjištěné poznatky a pokusím se nastínit řešení problémů, které jsou spojené s právní úpravou elektronického podpisu, a co tato úprava bude znamenat pro praxi.

Ve své práci budu především čerpat z litery platných právních norem a to jak domácích, tak zahraničních. Vzhledem k novosti zkoumaného problému, neexistuje zatím žádný komplexní výkladový pramen, o který bych se mohl při své práci opírat.

Budu tedy vycházet především z odborných konzultací a z elektronických odborných článků publikovaných na Internetu.

3. Přehled platné právní úpravy v ČR

Česká republika se zařadila mezi první evropské země, které legalizovaly moderní elektronickou formu zpracování dokumentů. Stalo se tak 1. října 2000, kdy nabyl účinnosti zákon č. 227/2000 Sb., o elektronickém podpisu. Význam a důsledky tohoto zákona přesahují běžné legislativní úpravy. Schválením tohoto zákona byla uskutečněna novela všech hlavních procesních norem: občanského soudního řádu, správního řádu, trestního řádu a zákona o správě daní a poplatků, v nichž byla zakotvena alternativní možnost elektronického podání opatřeného zaručeným elektronickým podpisem. Rovněž byla provedena novela § 40 občanského zákoníku upravujícího podepisování[23]. Zákon o elektronickém podpisu a o změně některých dalších zákonů je zcela samozřejmě zaměřen na právní aspekty problematiky mnohem více než na technické řešení. Vzhledem k překotnému vývoji v technologii podpisových schémat by tak měl zůstat zákon pevným bodem pro výchozí technické aplikace elektronického podpisu. Ty jsou naopak předmět prováděcí Vyhlášky Úřadu pro ochranu osobních údajů[24].

Prováděcí vyhláška má za úkol doplňovat zákon o elektronickém podpisu konkrétními požadavky kladenými jak na uživatele e-podpisu, tak na tzv. důvěryhodné strany. V době dokončování této práce nebyla ještě známa konečná a schválená verze této prováděcí vyhlášky. Odborné veřejnosti již ale byly dány k diskusi některé její teze a byly stanoveny hlavní body, které tato vyhláška musí bezesporu obsahovat.

Tyto dva akty spolu tvoří stavební kámen rozvoje elektronického podpisu, potažmo rozvoje elektronického obchodu v České republice. Oba vznikly, resp. vznikají, v souladu se vznikem adekvátních norem EU. Předmětem našeho dalšího zkoumání bude tedy rozbor a srovnání právní úpravy elektronického podpisu na úrovni EU a v ČR.

3.1. Zákon č. 227/2000 o elektronickém podpisu

3.1.1. Vznik zákona o elektronickém podpisu

Zákon vznikl na základě iniciativy podnikatelské sféry (konkrétně Sdružení pro informační společnost neboli SPIS) a poslanců Parlamentu ČR. Jeho autorem je skupina odborníků v oblasti IT a práva vedená doc. Smejkalem a doc. Matesem. Zákon o elektronickém podpisu byl poskytnut k diskusi celé odborné veřejnosti a po zapracování značného množství připomínek byl předložen vládě 8.11.1999 jako poslanecká iniciativa místopředsedů čtyř politických stran: I. Langera, S. Grosse, V. Mlynáře a

C. Svobody. Vláda tento návrh odmítla a vrátila jej k přepracování tak, aby zákon odpovídal požadavkům směrnice EU č.1999/93/EC[19]. V květnu 2000 schválila Poslanecká sněmovna parlamentu téměř jednohlasně poslanecký návrh zákona o elektronickém podpisu a změně některých dalších zákonů. Posléze s ním vyslovil souhlas senát a 10. července jej podepsal i prezident republiky. Dne 1. října 2000 vstoupil v platnost.

3.1.2. Pojmy

Zákon definuje 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.

3.1.3. Zaručený elektronický podpis

Zákon o elektronickém podpisu (dále jen ZoEP) rozlišuje v § 2 pojem elektronický podpis a zaručený elektronický podpis. Elektronický podpis je zde definován jako údaj v elektronické podobě, který je připojen k datové zprávě nebo je s ní logicky spojen a který umožňuje ověření totožnosti podepsané osoby ve vztahu k datové zprávě[23]. Naproti tomu zaručený elektronický podpis musí splňovat podle § 2 ZoEP čtyři podmínky:

a) je jednoznačně spojen s podepisující osobou,
b) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
c) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
d) je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoli následnou změnu dat[23].

V § 3 odst. 2 ZoEP se dále o zaručeném elektronickém podpisu říká, že použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu[23]. Zaručený elektronický podpis podle § 4, který zní: použití zaručeného elektronického podpisu zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána, toto porušení bude možno zjistit, umožňuje ověření souladu přijaté datové zprávy s podepsanou datovou zprávou neboli originálem[23].

V dalším textu zákona není nijak upraveno používání ani další vlastnosti „běžného“ elektronického podpisu. Praktické použití elektronického podpisu není tedy

podloženo zákonem a je tedy nutné vztahy, založené na tomto elektronickém podpisu, upravit smluvně podle principu smluvní volnosti[20]. V případě, že by neexistovala smluvní úprava vztahů zúčastněných stran, která by řešila spor založený na běžném elektronickém podpisu, mohl by být za určitých okolností v rámci důkazního řízení vyhodnocen elektronický podpis jako zaručený elektronický podpis a spor by se řešil podle zákona o elektronickém podpisu. ZoEP podporuje běžný elektronický podpis jen minimálně.

Zaručený elektronický podpis, který splňuje požadavky § 2 písm. b ZoEP, byl vytvořen pomocí prostředků pro bezpečné vytváření elektronického podpisu (§ 2 písm. m) a je založený na kvalifikovaném certifikátu (§ 2 písm. h) již dává oběma stranám záruky dle zákona[23].

Je tedy zřejmé, že množina zaručených elektronických podpisů je podmnožinou elektronických podpisů.

3.1.4. Prostředek pro bezpečné vytváření elektronického podpisu

Zákon dále rozlišuje pojmy prostředek pro vytváření elektronických podpisů a prostředek pro bezpečné vytváření elektronických podpisů. § 2 písm. k zní: prostředkem pro vytváření elektronických podpisů se rozumí technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů[23]. Prostředek pro bezpečné vytváření elektronických podpisů je definován v § 2 písm. m takto: prostředkem pro bezpečné vytváření elektronických podpisů se rozumí prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem[23]. Akreditovaní poskytovatelé a poskytovatelé certifikačních služeb vydávající kvalifikované certifikáty jsou podle § 3 odst. 2) a § 6 písm. j povinni používat bezpečné systémy a nástroje elektronického podpisu, jejichž součástí jsou prostředky pro bezpečné vytváření elektronických podpisů. Prostředky pro ověřování elektronického podpisu a prostředky pro bezpečné ověřování elektronického podpisu jsou též zákonem analogicky rozlišeny. ZoEP v § 17 stanovuje požadavky na tyto bezpečné prostředky. Používání běžných prostředků pro vytváření a ověřování elektronického podpisu zákon nijak neupravuje. Zákon poskytuje oporu pro elektronický podpis takový, jaký je definován v § 3 odst. 2) čili podpis vytvořený zmíněnými prostředky pro bezpečné vytváření elektronického podpisu.

3.1.5. Kvalifikovaný certifikát

V ZoEP se dále rozlišují pojmy certifikát a kvalifikovaný certifikát. Podle § 2 písm. g ZoEP se certifikátem rozumí datová zpráva, která je vydána poskytovatelem

certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost[23]. Certifikát tedy nemusí obsahovat informace o totožnosti osoby, musí ale obsahovat data identifikující podepisující osobu. Musí zde být též možnost, pomocí těchto dat, zjistit totožnost podepisující osoby; totožnost osoby prokáže poskytovatel certifikačních služeb. Zákon neklade na běžný certifikát žádná další omezení. Běžný certifikát má tedy vůči kvalifikovanému certifikátu podobnou váhu jako elektronický podpis a zaručený elektronický podpis[21]. V § 6 odst. 7) ZoEP však stojí, že poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů[23]. Budeme-li výklad tohoto odstavce brát naprosto doslovně, znamenalo by to, že bude-li poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, (§ 6) vydávat též běžné certifikáty, musel by s nimi za určitých okolností zacházet jako s kvalifikovanými certifikáty. Takovýto výklad tedy paradoxně klade větší břemeno na poskytovatele certifikačních služeb vydávající kvalifikované certifikáty než na poskytovatele certifikačních služeb, ač se jedná o certifikát se stejnou právní vahou. Z kontextu je ale zřejmé, že tvůrce zákona zde pojmem certifikát míní kvalifikovaný certifikát[21].

Kvalifikovaný certifikát je takový certifikát, který splňuje požadavky § 2 písm. h: certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty[23]. Zákon stanoví náležitosti kvalifikovaného certifikátu v § 12. Abychom mohli označit certifikát za kvalifikovaný, musí být vydán poskytovatelem certifikačních služeb vydávající kvalifikované certifikáty, který splňuje podmínky § 6 ZoEP.

Kvalifikovaný certifikát je tedy též podmnožinou množiny certifikátů.

3.1.6. Poskytovatelé certifikačních služeb

Zákon dále definuje a rozlišuje tři úrovně poskytování certifikačních služeb. Na nejnižší úrovni definuje poskytovatele certifikačních služeb podle § 2 písm. e. Poskytovatelem certifikačních služeb je subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy[23]. Jak jsme viděli, takto vydané certifikáty nemají v ZoEP oporu a instituce „běžného“ poskytovatele certifikačních služeb je tedy závislá na smluvních ujednáních[20].

Na mnohem vyšší úrovni je v zákoně definován institut poskytovatele certifikačních služeb vydávající kvalifikované certifikáty. Povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty jsou předmětem § 6 ZoEP. § 6 mimo jiné ukládá poskytovateli:

- zajistit, aby kvalifikované certifikáty jím vydané odpovídaly ZoEP,
- bezpečně ověřit totožnost osoby,
- zjistit, zda data pro vytváření elektronických podpisů odpovídají datům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát,
- vedení a zpřístupnění seznamu platných a zneplatněných certifikátů,
- používat bezpečné nástroje elektronického podpisu schválené Úřadem pro ochranu osobních údajů,
- uchovávat veškeré informace a dokumentaci o vydaných kvalifikovaných certifikátech po dobu nejméně 10 let od data zneplatnění,
- vést provozní dokumentaci o veškeré činnosti poskytovatele i s vydanými kvalifikovanými certifikáty.

V § 6 odst. 2) se dále stanoví, že poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, vydává podepisujícím osobám kvalifikované certifikáty na základě smlouvy. Smlouva musí být písemná, jinak je neplatná[23]. Definice písemné formy je po novele občanského zákoníku rozšířena v § 40 odst. 4 ObčZ takto: 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[26]. Bude-li tedy takováto smlouva podepsána zaručeným elektronickým podpisem, bude zachována její platnost. Další povinností stanovenou v § 6 odst. 5) ZoEP je, že poskytovatel certifikačních služeb vydávající kvalifikované certifikáty, není-li akreditován Úřadem (rozumí se Úřadem pro ochranu osobních údajů), je povinen ohlásit Úřadu nejméně 30 dnů před vydáním prvního kvalifikovaného certifikátu, že bude vydávat kvalifikované certifikáty[23]. Úřad pak podle § 9 ZoEP vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona[23]. Pokud poskytovatel neoznámí vydávání kvalifikovaných certifikátů, nesplní podmínky pro poskytovatele certifikačních služeb vydávající kvalifikované

certifikáty podle tohoto zákona a ani jeho certifikáty nebudou moci být označeny za kvalifikované.

Na nejvyšší úrovni stojí instituce akreditovaného poskytovatele certifikačních služeb.

Dle § 10 odst. 1) může každý poskytovatel certifikačních služeb požádat Úřad o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Působnost této normy je omezena § 10 odst. 7): součástí rozhodnutí Úřadu o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem[23]. Poskytovatel tedy musí vydávat kvalifikované certifikáty. V § 10 odst. 5) a 6) se dále zužuje okruh možných kandidátů na akreditovaného poskytovatele. Tím může být pouze poskytovatel se sídlem na území České republiky a zároveň, kromě činností uvedených v ZoEP, může akreditovaný poskytovatel certifikačních služeb bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec[23]. Obsah žádosti o akreditaci je stanoven v § 10 odst. 2). Výhodou akreditace je možnost působení v oblasti orgánů veřejné moci (§ 11). Toto působení se týká komunikace mezi samotnými orgány veřejné moci a též mezi veřejností a jednotlivými orgány veřejné moci. Podle § 9 odst. 2) ZoEP, vykonává Úřad nad akreditovanými poskytovateli dozor, uděluje a odnímá akreditace, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona, vede a uveřejňuje seznam akreditovaných poskytovatelů, vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou a plní další povinnosti stanovené ZoEP. Za účelem výkonu dozoru je akreditovaný poskytovatel certifikačních služeb vydávající kvalifikované certifikáty povinen pověřeným zaměstnancům Úřadu umožnit v nezbytně nutném rozsahu vstup do obchodních a provozních prostor, na požádání předložit veškerou dokumentaci, záznamy, doklady, písemnosti a jiné podklady související s jeho činností, umožnit jim v nezbytně nutné míře přístup do svého informačního systému a poskytnout informace a veškerou potřebnou součinnost - § 9 odst. 3) ZoEP. Tento odstavec se vztahuje pouze na akreditované poskytovatele certifikačních služeb. Je tedy otázkou, jakým způsobem bude Úřad provádět kontrolu poskytovatelů certifikačních služeb vydávající kvalifikované certifikáty.

Pokud akreditovaný poskytovatel hodlá ukončit svou činnost, postupuje podle § 13 ZoEP. Zákon mu v takovém případě klade povinnost vynaložit veškeré možné úsilí na to, aby platné kvalifikované certifikáty byly převzaty jiným akreditovaným poskytovatelem certifikačních služeb. Není-li akreditovaný poskytovatel schopen

zajistit, aby platné kvalifikované certifikáty převzal jiný akreditovaný poskytovatel certifikačních služeb, nebo dojde k zániku akreditovaného poskytovatele, Úřad převezme evidenci vydaných kvalifikovaných certifikátů a oznámí to dotčeným podepisujícím osobám[23].

Jak bylo uvedeno, Úřad vykonává nad akreditovanými poskytovateli a poskytovateli certifikačních služeb vydávající kvalifikované certifikáty dozor. Zjistí-li Úřad, že akreditovaný poskytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě sjednal nápravu, a případně určí, jaká opatření k odstranění nedostatků je tento poskytovatel certifikačních služeb povinen přijmout - § 14 odst. 1) ZoEP. V případě závažnějšího porušení zákona je Úřad dále oprávněn udělenou akreditaci odejmout a může současně ukončit platnost kvalifikovaných certifikátů vydaných dotyčným poskytovatelem.

3.1.7. Nápravná opatření

Pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán nebo pokud byl vydán na základě nepravdivých údajů, může Úřad, v souladu s § 15 ZoEP, nařídit poskytovateli certifikačních služeb jako předběžné opatření zneplatnění kvalifikovaného certifikátu. Takovýto certifikát zákon nedovoluje opětovně zprovoznit. Na certifikát zneplatněný nařízením Úřadu se též vztahuje § 6 písm. g, h ZoEP.

Úřad je podle § 18 ZoEP oprávněn, při porušení povinností uložených tímto zákonem, ukládat akreditovanému poskytovateli certifikačních služeb nebo poskytovateli certifikačních služeb vydávajícímu kvalifikované certifikáty pokuty. Pokuty mohou dosahovat výše 10 000 000,- Kč a při recidivě až 20 000 000,- Kč. Úřad může ukládat pokuty i jednotlivým osobám, které, byť z nedbalosti, neposkytnou Úřadu při výkonu kontroly potřebnou součinnost, a to do výše 25 000,- Kč, a to i opakovaně - §18 odst. 4) ZoEP. Výnos pokut je příjmem státního rozpočtu České republiky[23].

3.1.8. Zahraniční certifikáty

Pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty zákon nestanoví povinnost mít sídlo na území České republiky. Není tedy ze zákona zakázáno, aby zahraniční společnost, pokud splní požadavky § 6 ZoEP, vydávala pro subjekty v České republice kvalifikované certifikáty. V takovém případě by, de lege lata, Úřad pro ochranu osobních údajů musel provádět dozor nad zahraniční společností a v případě porušení ZoEP ukládat i takové společnosti pokuty. Došlo by tak ke kolizi mezinárodního práva. Takovouto situaci je možné řešit několika způsoby:

1. novelou ZoEP,
2. mezinárodní smlouvou,
3. neuznáním zahraničního poskytovatele jako poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty z důvodů nemožnosti plnění § 9 ZoEP[20].

Bude-li chtít takovýto poskytovatel vydávat kvalifikované certifikáty v České republice, bude nutné postupovat podle § 16 ZoEP. Podle tohoto paragrafu je možné uznat zahraniční certifikáty jako kvalifikované certifikáty podle ZoEP jestliže:

1. Úřad rozhodne o uznání kvalifikovaného certifikátu nebo
2. existuje mezinárodní smlouva, na jejímž základě je daný certifikát uznaný jako kvalifikovaný podle ZoEP nebo
3. je-li uznán poskytovatelem certifikačních služeb, který vydává kvalifikované certifikáty podle tohoto zákona, a za podmínky, že tento poskytovatel certifikačních služeb zaručí ve stejném rozsahu jako u svých kvalifikovaných certifikátů správnost a platnost kvalifikovaného certifikátu vydaného v zahraničí[23].

3.1.9. Povinnosti podepisující osoby

Zákon působí též na podepisující osoby. Podepisující osoba je tedy podle § 5 odst. 1) povinna:

a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití[23]. Co se rozumí náležitou péčí ve vztahu k výše uvedenému, není příliš snadné vyložit. Obecně však lze konstatovat, že jde o takové zacházení, které nejenom, že je na potřebné odborné úrovni, ale spočívá i v dodržování výše uvedených zásad.

b) uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu[23]. Zde je vyjádřena oznamovací povinnost ve vztahu k poskytovateli certifikačních služeb ohledně existence, byť sebemenší možnosti hrozby nebezpečí, zneužití programového vybavení, jehož je k podpisu užito. Výraz neprodleně je třeba chápat vzhledem k okamžiku zjištění samotné možnosti takové hrozby (a tedy subjektivně).

c) podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu[23]. Povinnost podávat (tedy i opakovaně) přesné, pravdivé a úplné informace poskytovateli služeb je zde stanovena

pouze ve vztahu vůči kvalifikovanému certifikátu a nikoli tedy certifikátu běžnému. V § 5 odst. 2) se dále říká, že za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů (Občanského zákoníku). Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn[23].

Občanský zákoník vychází při úpravě obecné odpovědnosti za škodu ze zavinění předpokládaného. To znamená, že je to poškozený, kdo musí v jednotlivém případě prokazovat porušení právní povinnosti. Elektronický podpis tedy klade také nemalé nároky na zodpovědnost strany příjemce podpisu[26].

3.1.10 Povinnosti poskytovatele

Zákon o elektronickém podpisu stanoví obdobně odpovědnost poskytovatele certifikačních služeb. Tato je stanovena v § 7 odst. 1): za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podle zvláštních právních předpisů[23] (též Občanského zákoníku).

3.1.11. Ohrožení elektronického podpisu

Zaručený elektronický podpis má oproti vlastnoručnímu podpisu několik výhod. To hlavní je výše zmíněná záruka integrity (tedy záruka shody přijaté zprávy s podepsanou, tj. s originálem). Nevýhodou zaručeného elektronického podpisu oproti vlastnoručnímu je nejistota (ač malá), že zprávu, kterou příjemce obdrží, nepodepsala osoba uvedená v certifikátu[18]. Uveďme následující fiktivní příklad:

J.H. je uživatel zaručeného elektronického podpisu. Data pro vytváření elektronického podpisu (§ 2 písm. i ZoEP) uchovává na pevném disku svého PC, jsou uložena pouze na jednom místě a jsou chráněna přístupovým heslem. Na PC běží operační systém Windows 95 a je připojen k Internetu. Můžeme tedy říci, že se jedná o velmi běžný případ bezpečného zacházení s daty pro vytváření elektronického podpisu a uživatel splňuje podmínky § 5 ZoEP. Předpokládejme, že

a) dojde k vyloupení bytu pana J.H. a je zcizeno dotyčné PC nebo

b) při připojení pana J.H. od sítě Internet se do systému PC dostane zručný hacker a zkopíruje data pro vytváření elektronického podpisu (operační systém Windows je bez použití kvalitního firewallu velice lehké takto napadnout[1]). V obou případech pak může dojít k jednorázovému nebo i opakovanému zneužití zaručeného elektronického podpisu, a způsobit tak škodu velkého rozsahu. Pachatel tak může učinit

v takovém časovém intervalu, aniž by J.H. mohl včasně jednat podle § 5 odst. 1) písm. b. Kdo v takovém případě bude odpovídat za škodu?

Odpověď nalezneme v zákoně č.40/1964 Sb. ČR v platném znění (Občanský zákon), jehož § 34 a následující upravují to, čemu se v našem právním řádu říká právní úkon. K tomu aby došlo ke vzniku, změně nebo zániku práv a povinností, je třeba, aby šlo o platný právní úkon. Právní úkon (dle § 34 OZ) zahrnuje následující pojmové znaky: Projevy vůle směřující ke vzniku, změně nebo zániku (zrušení) práv a povinností nebo ke způsobení jiných právních následků, které právní předpisy s takovými projevy vůle spojují[26]. Z uvedených znaků má klíčový význam jednota vůle a jejího projevu. To znamená, že k tomu , aby vznikl právní úkon, je třeba, aby byly dány obě jeho základní složky, tj. jak vůle, tak i její adekvátní projev. Kdyby nebylo vůle (např. pro fyzické či jiné donucení), nebylo by ani právního úkonu, a tedy ani žádného přímého závazku. Právního úkonu by však nebylo ani tehdy, kdyby se nedostávalo projevu, stejně tak, kdyby projev vůle učinila jiná osoba, než ta, která právní úkon podepsala[18]. Požadavek existence vůle však vyvolává některé problémy. V našem případě půjde o řešení problému, zda vůle projevená elektronickým podpisem je skutečně vůlí osoby vlastníka dat pro vytváření elektronického podpisu. Pravidlem je, že vůle projevená právním úkonem je vůle toho, kdo ji projevuje[18]. To však není bezvýjimečné. Pokud dojde ke zneužití dat pro vytváření elektronického podpisu (např. v důsledku jeho neoprávněného zkopírování), je zřejmé, že nejde o právní úkon, ale o úkon protiprávní. To však bude třeba dokázat. Problém tedy opět spočívá v určení osoby, která právní úkon skutečně učinila. Takový případ je v některých aspektech srovnatelný s krádeží osobních dokladů (např. OP) a jejich následného zneužití[20]. Dokazování by při soudním řízení v takovémto případě bylo poměrně problematické. Je ale pravdou, že některé části soudního řízení jsou založeny na zásadě volného hodnocení důkazů, která spočívá na skutečnosti, že soud provedené důkazy hodnotí podle svých vlastních závěrů (své úvahy) a v jejich vzájemné souvislosti. (§ 132 Občanského soudního řádu)[18]. A je tedy opravdu možné, že by se v konkrétním případě podařilo dokázat, že datovou zprávu podepsala či naopak nepodepsala osoba uvedená na certifikátu.

Elektronický podpis se poměrně jednoduše vyrovnává s možností změny podepsaných dat v průběhu přenosu od adresáta k příjemci. Nezaručí nám ale, že podpis provedla osoba, které data pro vytváření elektronického podpisu skutečně patří. Vlastníkům těchto dat nezbývá než zacházet s nimi s nejvyšší opatrností.

3.2. Předběžné zhodnocení

Snahou předkladatelů bylo, aby zákon byl co nejobecnější a technologicky nejméně závislý, neboť při každé změně technologie by jinak bylo třeba měnit text zákona. Předkládaný návrh zákon byl průběžně konzultován s představiteli Evropských společenství i UNCITRAL a je v souladu se záměry, které jsou oběma mezinárodními institucemi připravovány[19].

V zákoně existuje několik nesrovnalostí, které prověří až praxe používání elektronického podpisu. Můžeme však konstatovat, že zákon splňuje základní požadavky Evropských společenství[25]:

1. Právní uznání elektronických podpisů a jejich zrovnoprávnění s vlastnoručními podpisy ve všech případech neupravených zvláštními předpisy. Novela § 40 Občanského zákoníku za současného nabytí účinnosti navrhovaného zákona o elektronickém podpisu vytváří dostatečné předpoklady pro stejnou právní platnost zaručených elektronických podpisů jako vlastnoručních podpisů, které mohou být bez nutnosti změn dalších procesních norem používány jako důkaz v občanskoprávních i trestněprávních soudních nebo arbitrážních řízeních.

2. Zajištění volného pohybu všech výrobků a služeb vztahujících se k elektronickým podpisům, kdy tato činnost není omezena a podléhá pouze právnímu řádu a kontrole státu původu. Předložený zákon předpokládá po jistou dobu, pravděpodobně odpovídající době přípravy ke vstupu do EU, existenci dvou druhů poskytovatelů certifikačních služeb – akreditovaných a neakreditovaných. Vzhledem ke zkušenostem z jiných oblastí se autoři zákona rozhodli za účelem zvýšení důvěryhodnosti zaručeného elektronického podpisu podmínit službu jeho ověřování udělením licence. Nic ovšem nebrání stranám, aby se dohodly na používání obyčejného elektronického podpisu nebo aby ověřovatelé informací fungovali i bez akreditace.

3. Důvěryhodnost, kdy právní předpis určuje minimální pravidla a požadavky na vytvoření důvěryhodnosti poskytovatelů certifikačních služeb, kteří zodpovídají za platnost obsahu certifikátu. Technické a programové komponenty, které umožní ověřovat nebo vytvořit zaručený elektronický podpis, musí v sobě zahrnovat taková bezpečnostní opatření, aby nemohlo dojít k jeho zneužití. Úřad vydá vyhlášku, v níž stanoví podrobnosti týkající se věcných, personálních a organizačních předpokladů pro činnost ověřovatele a k obsahu bezpečnostní dokumentace. Zákon tak klade na bedra Úřadu nemalé břemeno.

4. Nezávislost na technologickém řešení, kdy vzhledem k tempu technologických inovací musí právní předpis umožnit právní rozeznávání elektronických podpisů nezávisle na použitých technologiích. Český zákon o elektronickém podpisu je vytvořen tak, aby byl naprosto technologicky nezávislý. Navrhovaný zákon není spojen s žádnou konkrétní metodou, takže vyhovuje všem možným technologickým řešením, jež se mohou v blízké nebo vzdálenější budoucnosti objevit.

5. Rozsah působnosti právního předpisu, který musí pokrývat vydávání certifikátů veřejnosti, zaměřený na identifikaci odesílatele elektronických údajů či dat. Návrh zákona umožňuje využívání elektronických podpisů jak ve veřejnoprávní sféře, tak mezi subjekty soukromého práva. Zákon tedy neklade překážky v dalším používání již existujících systémů, včetně smluvního zabezpečení v soukromoprávní sféře.

6. Mezinárodní působnost, kdy jsou zahrnuty mechanismy a postupy umožňující spolupráci s dalšími státy na bázi mezinárodních smluv. Zákon předpokládá uznávání zahraničních osvědčení a to buď na základě rozhodnutí Úřadu, nebo z mezinárodních smluv nebo pokud bude uzavřena dohoda o vzájemném uznávání osvědčení.

3.3. Podzákonné předpisy

Zákon o elektronickém podpisu tvoří teoretický a dosti obecný rámec pro používání elektronického podpisu. Svou technickou nezatížeností si klade nároky být jakýmsi stálým bodem na poli dynamicky se měnících informačních technologií. V souladu se směrnicí Evropské unie, na jejíchž základech vznikl, zůstává relativně abstraktní v definování práv a povinností zúčastněných stran při používání elektronického podpisu. Z těchto důvodů není možné, bez zavedení dalších právních předpisů, plně využívat možnosti, které samotný zákon poskytuje. Zákon totiž předpokládá existenci prováděcích vyhlášek, které jednak upraví konkrétní postupy používání elektronického podpisu v oblasti orgánů veřejné moci a které stanoví konkrétní požadavky na nástroje a subjekty podle § 6 a § 17 ZoEP.

Předpis upravující postupy používání elektronického podpisu v oblasti orgánů veřejné moci bude mít pravděpodobně podobu Vládního nařízení a stanoví se jím práva a povinnosti jednotlivých orgánů ve vztahu k elektronické komunikaci se soukromoprávními subjekty a dalšími orgány veřejné moci. V této kapitole se budeme zabývat prováděcím přepisem, který se týká konkrétního naplnění § 6 a § 17 ZoEP.

Bohužel, v době zpracovávání této práce, nebyla ještě schválena konečná verze vyhlášky Úřadu pro ochranu osobních údajů (dále jen Vyhláška), kterou se provádí § 6 a § 17 ZoEP. Důvodů pro tuto situaci je několik.

3.4. Vyhláška Úřadu pro ochranu osobních údajů

3.4.1. Příprava vyhlášky

Vyhláška má za úkol stanovit konkrétní technické parametry nástrojů a postupů při realizaci norem ZoEP. Aby bylo možné realizovat elektronický podpis a certifikaci na nadnárodní úrovni, je nutné, aby systémy ostatních států používaly kompatibilní technologie. V tomto ohledu hledá a přejímá EU řadu technických norem pro elektronický podpis, které tento požadavek splňují. Na členských státech pak je, aby tyto normy začlenily do svých právních systémů. Proces specifikace a začleňování těchto norem do legislativy je vzhledem k jejich důležitosti a složitosti velice náročná procedura a jako taková vyžaduje poměrně dost času. Ve směrnici EU je stanovena lhůta pro naplnění této procedury do 19. července 2001[26]. Uvážíme-li, že Česká republika uvedla v platnost zákon o elektronickém podpisu jako třetí ze států západní a střední Evropy, nemůžeme se pozastavit nad faktem, že proces tvorby a začleňování zmíněných technických norem ve státech EU, nebyl ještě zdaleka dokončen. Jestliže

budeme požadovat, aby naše elektronické podpisy byly přenositelné i za hranice naší republiky, a jestliže počítáme se vstupem České republiky do struktur EU, musí být systémy elektronického podpisu podloženy takovými právními normami, které budou v souladu s ještě nedokončenými předpisy EU.

Existuje zde ještě jeden důvod, proč zatím nemáme platnou prováděcí Vyhlášku. V ZoEP v § 20 se Úřad zmocňuje vydávat vyhlášky k upřesňování podmínek stanovených v § 6 a § 17 a způsobu, jakým se jejich splnění bude dokládat, a k upřesnění požadavků, které musí splňovat nástroje elektronického podpisu, a k náležitostem postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky. Na to, aby byly vyhlášky Úřadu pro ochranu osobních údajů platné a účinné, pouze tento paragraf nestačí. V zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, kterým se mimo jiné zřizuje Úřad, je totiž nevhodně definováno jeho postavení. Z nedostatků mimo jiné vyplývá: a) Úřad nemůže podat ústavní stížnost; b) Úřad nemůže publikovat vyhlášku ve Sbírce zákonů, kterou podle ZoEP má vydat a ta tedy nemůže být obecně závazná[7]. Je tedy nezbytně nutné provést novelu tohoto zákona.

Navzdory těmto problémům Úřad vydal k odborné diskusi již řadu tezí této Vyhlášky. První z nich byla na světě již v listopadu roku 2000 a na její adresu přišla dlouhá řada odborných právních a technických připomínek. V průběhu následujících tří měsíců Úřad, respektive jeho pracovní skupina pro elektronický podpis, postupně uveřejnila dva návrhy znění Vyhlášky. Poslední přepracovaná verze z 9. března 2001 je podle názorů většiny zainteresovaných odborníků na úrovni požadované směrnicí EU a nedostatky, které se v ní vyskytují, jsou považovány za kosmetické[19].

V dalším textu se zaměříme na podrobnější analýzu systému důvěry, o který se elektronické podpisy musí opírat, a na to, jak by tento systém měla upravovat či již upravuje zmíněná prováděcí Vyhláška.

3.4.2. Infrastruktura poskytování certifikačních služeb

Klíčovým mechanismem implementace soudobých IT aplikací provozovaných v otevřených sdílených sítích (v sítích s nedostatečně zaručenou úrovní bezpečnosti) a požadujících záruky za autentičnost a bezpečnost, tedy i aplikací založených na používání elektronických podpisů, je a zřejmě dlouho bude asymetrická kryptografie (nebo-li kryptografie veřejným klíčem – viz kapitola 5.1.)[7]. Používání asymetrické kryptografie si vynucuje dostupnost pomocné infrastruktury pro důvěryhodné zveřejňování veřejných klíčů a identity jejich vlastníků a pro správu související

s takovou činností. Je zvykem tuto infrastrukturu nazývat PKI – Public Key Infrastructure[7].

PKI tvoří kombinace software, hardware, firmware, kryptografických technologií a poskytování potřebných služeb. PKI vytváří provozní prostředí, ve kterém lze v rámci nezaručeně bezpečného síťového prostředí (např. Internet) podporovat bezpečnost komunikačních a aplikačních transakcí mezi koncovými stranami. PKI umožňuje používat bezpečnostní mechanismy asymetrické kryptografie jak při implementaci bezpečnostních služeb důvěrnosti (šifrování), tak i při implementaci bezpečnostních služeb nepopiratelnosti (podepisování). PKI je ale universálním nástrojem vhodným např. i pro podporu bezpečnostních služeb řízení přístupu, pokud certifikát potvrzuje odpovídající autorizaci jeho vlastníka[7].

3.4.3. Autority

Je zřejmé, že klíčovou roli v PKI hraje certifikační autorita. Certifikační autority patří mezi entity bezpečnostních struktur, které souhrnně označujeme jako poskytovatele důvěryhodných služeb(Trusted Service Provider – TSP)[7]. TSP podporují ustanovení vztahu důvěry mezi zúčastněnými stranami poskytováním podpůrných služeb – vydávají certifikáty, podporují křížové uznávání certifikátů vydávaných různými poskytovateli certifikačních služeb, generují časová razítka, udržují a vydávají seznamy neplatných certifikátů, umožňují on-line přístup do databáze certifikátů, přijímají požadavky na zneplatnění apod. Mezi základní typy TSP v universálně používaných PKI patří:

1. certifikační autorita,
2. registrační autorita,
3. atributová autorita,
4. depozitní autorita,
5. časová autorita

a další.

1. Certifikační autorita (CA) je poskytovatelem certifikátů. Na základě registrace, ověření totožnosti a konkrétních požadavků na obsah certifikátu, vydává žadatelům certifikáty[17]. CA tyto certifikáty podepisuje, aby byla zajištěna jejich integrita. Jak vidíme, úloha CA je v PKI klíčovou.

2. Registrační autorita (RA) je důvěryhodná třetí strana, která verifikuje správnost určitých specifických dat jí poskytnutých, tzn. ověřuje totožnost osoby. Dále provádí notářskou službu v tom smyslu, že vytváří nepopiratelný důkaz o platnosti a

správnosti tvrzení entity, že je vlastníkem určitých dat, o platnosti a statutu digitálního certifikátu entity, resp. o platnosti a správnosti jiného podpisu entity. Ověřuje tedy, zda data pro vytváření elektronického podpisu (soukromý klíč) odpovídají datům pro ověřování elektronického podpisu (veřejný klíč)[17]. Na rozhodnutí RA závisí důvěryhodnost celého systému a musí být proto kladeny na RA nejvyšší požadavky.

3. Atributová autorita (AA) přiděluje privilegia žadatelům, která jsou potom součástí kvalifikovaných certifikátů, nebo častěji, vydává vlastní atributové certifikáty. V praxi je pak nutné použít jak kvalifikovaný, tak atributový certifikát. Kvalifikovaný certifikát se liší od atributového certifikátu v tom, že obsahuje veřejný klíč, tady data pro ověřování elektronického podpisu[7]. Součástí informace zpracovávané AA jsou i další identifikující data.

4. Depozitní autorita (DA) publikuje a uchovává seznamy platných a zneplatněných certifikátů[17]. Na tuto autoritu jsou kladeny vysoké požadavky především z hlediska hardwarového a softwarového vybavení. Je nutné, aby uvedené seznamy byl stále přístupné, byly v co nejkratší možné době aktualizovány, byly bezpečné a zároveň uchovávaly data po dlouhou dobu (v ZoEP § 6 písm m je stanovena doba 10 let).

5. Časová autorita (ČA, někdy též autorita časových značek) je služba, která umožňuje umístit prokazatelně v čase existenci digitálního dokumentu, tvoří složku služeb prováděných s cílem zajistit nepopiratelnost. ČA tedy vytváří prostředek sloužící k důkazu existence v určitém časovém okamžiku. To lze použít např. k ověření, zda digitální podpis provedený k určité zprávě byl vytvořen předtím, než odpovídající certifikát byl odvolán, a tedy lze i odvolaný certifikát veřejného klíče použít k ověření příslušného elektronického podpisu. ČA také může indikovat časový moment, ve kterém byl doručen určitý dokument. Lze takto také např. dokumentovat, kdy proběhla určitá transakce. Proces tvorby časové značky je následující: a) žádající entita zasílá příslušný požadavek na ČA (TimeStampReq), b) ČA zasílá příslušnou odpověď (TimeStampResp)[17]. Po obdržení odpovědi žádající osoba ověří chybový stav odpovědi a ověří různá pole v časové značce a samozřejmě také platnost digitálního podpisu této časové značky. Speciálně musí také ověřit, že to, co bylo časově „označkováno“, odpovídá tomu, co bylo s tímto požadavkem zasláno. Tento proces se děje interaktivně, proto ČA musí být schopna i ve velmi krátkém čase obsloužit velké množství požadavků. Na ČA jsou tedy kladeny následující požadavky: a) musí používat důvěryhodný časový zdroj, b) musí vložit důvěryhodnou hodnotu času do každého

časového razítka, c) každé nové časové razítko musí v sobě obsahovat monotónně rostoucí celé číslo, d) časové razítko musí být vytvořeno ihned po obdržení příslušného požadavku, jakmile to lze, e) v každém časovém razítku musí být obsažen identifikátor, který jednoznačně určuje bezpečnostní politiku, na jejímž základě bylo příslušné časové razítko vytvářeno, f) časové razítko se vytváří pouze pro otisk časového momentu (hash), g) ověřit typ použité hashovací funkce a ověřit, že délka hashe odpovídá příslušnému algoritmu, h) neověřovat zaslaný otisk jiným způsobem (než ověření jeho délky), i) nevkládat libovolný identifikační znak entity, která zaslala požadavek, do časové značky, j) podepisovat každou časovou značku klíčem, který byl vygenerován výlučně pro tyto účely, a vyznačit tuto vlastnost na certifikátu příslušného klíče, k) vložit další informace do časové značky, pokud to obsahuje příslušný požadavek, využít k tomu příslušná rozšíření (tato rozšíření musí být samozřejmě podporována příslušnou ČA, v opačném případě je výstupem hlášená chyba)[17].

Mezi další typy TSP patří vydavatelé a ověřovatelé politik, vydávaných pro řízení jednotlivých autorit[7]. Těmito vydavateli jsou většinou statutární orány poskytovatele certifikačních služeb. Tématem certifikačních politik se budeme zabývat později.

3.4.4. Formy zajištění PKI

Poskytovatelé důvěryhodných služeb (výše uvedené typy TSP) spolu vytváří informační systém pro certifikační služby, který poskytovatel používá pro zajištění certifikačních služeb[7] (termín informační systém pro certifikační služby používá Vyhláška a je ekvivalentem pro výše uvedenou PKI) . Tento informační systém je možné v praxi realizovat dvěma způsoby: a) celý informační systém je součástí systému jednoho poskytovatele certifikačních služeb, b) části informačního systému (jednotlivé autority) pracují pro poskytovatele certifikačních služeb na základě smluvního ujednání, tj. nejsou součástí jednoho právního subjektu. Vyhláška umožňuje provozování obou těchto forem informačního systému. Pro variantu b) stanoví v § 6 odst. 2), že poskytovatel je odpovědný za soulad výkonu certifikačních služeb se všemi dokumenty Předpisové základny, a to i v případech, kdy některé části certifikačních služeb zajišťuje prostřednictvím smluvních partnerů[24]. Skutečnosti, které poskytovatel uvádí v dokumentech tvořících Předpisovou základnu, jsou pro jeho činnost závazné, tj. to, co poskytovatel deklaruje, musí dodržovat. Pokud využívá k zajištění své činnosti smluvních partnerů, je jeho povinností zajistit dodržování vyhlášených zásad i u těchto partnerů. Vztah smluvních partnerů je dále v § 6 odst. 8) upraven takto: Poskytovatel je

povinen v rozsahu odpovídajícím vykonávané činnosti seznámit smluvní partnery s platným zněním Certifikační politiky a Certifikační prováděcí směrnice (viz kapitola 3.4.7.)[24]. Smluvní partneři, kteří pro poskytovatele vykonávají činnosti v oblasti poskytování certifikačních služeb, musí mít odpovídající znalost dokumentů Předpisové základny, která je dostačující pro výkon předmětné činnosti. Zajištění této znalosti v odpovídajícím rozsahu je povinností poskytovatele. Vztahu poskytovatele a jeho smluvních partnerů se dále týká § 22 Vyhlášky. Podle odst. 1) je poskytovatel oprávněn certifikační služby nebo jejich části, v praxi poskytovatelé běžně využívají služeb jiných subjektů a to zejména při registraci, zajistit na základě písemné smlouvy prostřednictvím smluvních partnerů. Činnost musí být prováděna v souladu s dokumenty Předpisové základny. Odpovědnost za zajišťování certifikačních služeb vůči žadatelům, držitelům a osobám spoléhajícím na certifikát nese poskytovatel[24]. Poskytovatelé certifikačních služeb jsou tedy povinni zajisti dodržování veškerých souvisejících přepisů, a to ať se jedná o jejich vlastní činnost, či činnost smluvních partnerů. Vyhláška tedy dále upravuje práva a povinnosti pouze poskytovatelů certifikačních služeb, kteří musí zajisti jejich naplnění. V § 22 odst. 2) se ještě omezuje platnost odst.1). Dvě klíčové činnosti certifikačních služeb, tj. vydávání kvalifikovaných certifikátů a seznamu zneplatněných kvalifikovaných certifikátů, musí totiž vždy vykonávat pouze poskytovatel[24].

3.4.5. Požadavky na certifikáty

Při vytváření kvalifikovaného certifikátu postupuje poskytovatel (rozumí se poskytovatel certifikačních služeb podle § 2 písm. e Vyhlášky) podle § 3 Vyhlášky: poskytovatel je povinen zajistit, že každému jím vydanému kvalifikovanému certifikátu je přiděleno unikátní číslo a uplatnit veškerá účelná opatření, která minimalizují možnost neoprávněné manipulace při přidělování těchto čísel[24]. Unikátní číslo je přidělováno každému vydanému certifikátu, není přípustné, aby bylo použito číslo, které již bylo v minulosti přiděleno, byť by se jednalo o číslo, které bylo přiděleno certifikátu, který byl již zneplatněn. Jedná se o mezinárodně vžitou praxi, obecně uznávanou, která je deklarována například v dokumentu RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile[17]. Toto číslo se následně používá jako identifikátor (primární klíč) certifikátu, například na seznamu zneplatněných certifikátů.

Při zneplatnění kvalifikovaného certifikátu postupuje poskytovatel podle § 4 Vyhlášky. V ZoEP v § 6 odst. 7) se stanoví, že platnost kvalifikovaného certifikátu musí

být poskytovatelem ukončena neprodleně. Vyhláška v § 4 odst. 2) toto ustanovení upřesňuje následovně: Poskytovatel je povinen vynaložit nejvyšší možné úsilí a uskutečnit veškerá opatření, aby doba mezi přijetím požadavku na zneplatnění kvalifikovaného certifikátu, který byl uplatněn v souladu s Certifikační politikou a Certifikační prováděcí směrnicí, a uvedením v seznamu zneplatněných kvalifikovaných certifikátů a zveřejněním tohoto seznamu byla co nejkratší. Tato doba by neměla činit více jak 24 hodin[24]. Při akceptování možností současných technologií a při požadavku na uplatnění požadavku na zneplatnění hodnověrným způsobem, který vyloučí možnost zneužití (například zneplatnění jinou osobou než je držitel kvalifikovaného certifikátu), je nezbytné tento požadavek vymezit uvedenými 24 hodinami. Dokumenty, které navazují na směrnici Evropského parlamentu a rady o elektronických podpisech, např. Draft ETSI TS 101 456 V0.0.15 (2000-11) Policy requirements for certification authorities issuing qualified certificates, vymezují tuto dobu obdobně[17].

Poskytovatel je při zneplatnění kvalifikovaného certifikátu povinen zajistit, že držitel, jehož kvalifikovaný certifikát byl zneplatněn, je bez zbytečného prodlení o této skutečnosti informován. Součástí této informace je uvedení času, kdy ke zneplatnění došlo[24]. Ke standardním povinnostem poskytovatele, který vydává z hlediska bezpečnosti vyšší formy certifikátů, patří uvedená povinnost. Tím poskytovatel potvrzuje držiteli, že jeho požadavek na zneplatnění byl realizován, resp. že byl jeho kvalifikovaný certifikát, z důvodů uvedených v ZoEP, zneplatněn. Postup při předávání této informace není standardy upraven a je tedy na poskytovateli, aby jej specifikoval. Další povinnosti poskytovatele se týkají depozitní autority. Pro tu Vyhláška stanoví, aby: a) aktualizovaný seznam zneplatněných kvalifikovaných certifikátů byl zveřejněn alespoň jedenkrát denně, b) seznam zneplatněných kvalifikovaných certifikátů byl veřejně přístupný do doby vydání nového seznamu, c) seznam zneplatněných kvalifikovaných certifikátů byl podepsán kvalifikovaným elektronickým podpisem poskytovatele[24]. Seznam zneplatněných certifikátů je jedním ze základních prvků komunikace s využitím elektronického podpisu založeného na kvalifikovaném certifikátu. Seznam slouží osobám, které spoléhají na kvalifikovaný certifikát (spoléhajícím osobám), k ověření, zda daný kvalifikovaný certifikát je platný. Seznam, opatřený kvalifikovaným podpisem poskytovatele, musí být trvale veřejně přístupný a nejméně jedenkrát denně aktualizovaný. Požadavek na podepsání kvalifikovaným elektronickým podpisem poskytovatele vyplývá z ustanovení § 6 odst. 1 písm. j) ZoEP,

kterým se poskytovateli ukládá používat bezpečné nástroje elektronického podpisu. Pro depozitní autoritu ukládá Vyhláška další povinnosti v § 4 odst. 5), podle kterého je poskytovatel povinen umožnit nepřetržitý příjem požadavků na zneplatnění kvalifikovaného certifikátu, zaslaných v elektronické formě. Poskytovatel je povinen zajistit nepřetržitou dostupnost informací o zneplatněných kvalifikovaných certifikátech způsobem umožňujícím dálkový přístup[24]. Poskytovatel musí umožnit držitelům, aby mohli kdykoliv elektronicky zaslat své požadavky na zneplatnění svých kvalifikovaných certifikátů (typicky e-mailovou poštou) a musí dále zajistit, aby seznam zneplatněných kvalifikovaných certifikátů byl nepřetržitě dostupný "způsobem umožňujícím dálkový přístup" (typicky prostřednictvím Internetu).

3.4.6. Důvěryhodnost poskytovatele

Velice důležitým aspektem důvěryhodnosti poskytovaných služeb je ověření důvěryhodnosti poskytovatele. Zmínili jsme se, že seznamy zneplatněných kvalifikovaných certifikátů musí být podepisovány kvalifikovaným elektronickým podpisem poskytovatele. V § 5 odst. 1) Vyhlášky se o datech pro vytváření kvalifikovaného elektronického podpisu poskytovatele dále říká, že data pro vytváření elektronického podpisu, k nimž byl vydán kvalifikovaný certifikát poskytovatele a která jsou obsažená v kvalifikovaných certifikátech poskytovatele, je poskytovatel povinen používat výhradně pro podepisování vydávaných kvalifikovaných certifikátů a seznamu zneplatněných kvalifikovaných certifikátů[24]. Pro kvalifikované certifikáty poskytovatele stanoví Vyhláška, že při zveřejňování svých kvalifikovaných certifikátů osobám spoléhajícím na certifikát je poskytovatel povinen zajistit, že jsou dostupné nejméně dvěma na sobě nezávislými způsoby[24]. Důvodem pro požadavek na zveřejnění dvěma nezávislými způsoby je možnost ověření jejich správnosti (autenticity). Předpokládá se, a praxe taková je, že držitel od poskytovatele po podpisu smlouvy o vydání kvalifikovaného certifikátu obdrží zároveň jeho kvalifikovaný certifikát[17].

Z uvedených skutečností vyplývá, že osoba spoléhající na certifikát (§ 2 písm. d Vyhlášky) opírá svou důvěru v něj o kvalifikovaný certifikát poskytovatele. Tomuto certifikátu tedy musí důvěřovat. V praxi se pro ověření důvěryhodnosti kvalifikovaných certifikátů poskytovatelů používá tzv. křížová certifikace[7]. Jedná se o bilaterální výměnu veřejných klíčů dvou samostatných a na sobě nezávislých poskytovatelů certifikačních služeb. V takovémto případě každý z nich ručí za důvěru v kvalifikovaný certifikát druhého poskytovatele a tím je zaručena i důvěra osobě spoléhající na

certifikát tohoto poskytovatele. Tento systém ověřování se nazývá síťový, neboť vztahy ověřování certifikátů mezi poskytovateli vytváří složitou síť. V praxi se používá i jiná, obdobná struktura ověřování kvalifikovaných certifikátů poskytovatelů. Místo obousměrné certifikace mezi různými poskytovateli se používá jednosměrná, stromová struktura ověřování. Má několik úrovní, přičemž poskytovatelé na vyšší úrovni ověřují certifikáty poskytovatelů na nižší úrovni. Řetěz certifikací však nemůže být nekonečný a poslední certifikát potom zůstává necertifikovaný. To je kořenový kvalifikovaný certifikát a uživateli (spoléhající osobě) nezbývá, než mu věřit[7]. ZoEP ani Vyhláška neupravují žádný z výše zmíněných systémů ověřování kvalifikovaných certifikátů poskytovatelů. Ze ZoEP však vyplývá, že důvěra ve kvalifikované certifikáty akreditovaných poskytovatelů se opírá o důvěru v Úřad, který akreditaci udělil[21]. Takovýto systém můžeme označit jako dvouúrovňový certifikační strom. Je ale docela pravděpodobné, že poskytovatelé certifikačních služeb budou s cílem zvýšit svou konkurenceschopnost uzavírat bilaterální smlouvy o ověřování kvalifikovaných certifikátů, aniž by byli k tomuto nuceni.

3.4.7. Předpisová základna

Důvěryhodnost jednotlivých TSP je dána deklarovanou a uznávanou politikou (pravidla plnění poskytovaných služeb), při jejichž uplatnění se poskytované služby považují za bezpečné. Pro naplnění požadavku na kompatibilitu a koherenci informačních systémů pro poskytování certifikačních služeb na nadnárodní úrovni vzniká řada technických norem různých organizací, které konkrétně specifikují tyto politiky. Jak již bylo zmíněno, úkolem současného legislativního snažení v oblasti elektronických podpisů je výběr a začlenění těchto norem do právního řádu.

Vyhláška Úřadu pro ochranu osobních údajů vychází především z dokumentu RFC 3039 Internet X.509 Public Key Infrastructure Qualified Certificates Profile. V § 6 odst. 1) je uveden výčet dokumentů, které je poskytovatel povinen zpracovat a v písemné podobě uchovat. Jsou jimi:

1) Certifikační politika,
2) Certifikační prováděcí směrnice,
3) Celková bezpečnostní politika,
4) Systémová bezpečnostní politika,
5) Plán pro zvládání krizových situací a Plán obnovy[24].

Souhrn těchto dokumentů budeme označovat pojmem Předpisová základna. V těchto dokumentech poskytovatel zejména deklaruje, jaké služby a jakým způsobem zajišťuje,

jak je zajištěna celková bezpečnost organizace poskytovatele a bezpečnost informačního systému pro certifikační služby, jaké jsou postupy uplatněné v případě bezpečnostního incidentu a postupy vedoucí k nápravě. Vzhledem k tomu, že dokumenty Předpisové základny tvoří základ pro činnost poskytovatele a jsou pro jeho další činnost závazné, je nezbytné, aby byly schvalovány statutárním orgánem, podle § 6 odst. 3). V návaznosti na tento odstavec, se poskytovateli ukládá povinnost, podle § 6 odst. 4), schvalování změn v těchto dokumentech týmž orgánem. Výjimku tvoří Havarijní plán a Plán obnovy, kde by požadavek na schvalování statutárním orgánem mohl vést k prodlení, které by mohlo negativně ovlivnit kontinuitu poskytování služeb. Je však nezbytné, aby orgán, který je oprávněn změny v uvedených dokumentech schvalovat, byl statutárním orgánem určen. Pro jasnou komunikaci mezi poskytovatelem, žadatelem a osobami spoléhajícími na kvalifikovaný certifikát je nezbytně nutné, aby měli přístup alespoň k těm částem Předpisové základny, které upravují jejich činnost. Podle § 6 odst. 7 Vyhlášky, je poskytovatel povinen umožnit subjektům, jejichž činnost je dokumenty Předpisové základny upravena, seznámit se s těmi změnami v Předpisové základně, které se jejich činnosti týkají[24]. Vzhledem k předpokládanému počtu držitelů není možné stanovit povinnost seznámit se změnami. Subjekty spoléhající na certifikát poskytovatel nezná, a tedy i zde se může jednat pouze o povinnost umožnit seznámení se se změnami. Vyhláška v dalším textu upravuje požadavky na jednotlivé dokumenty Předpisové základny.

1) Certifikační politiku definuje § 7 odst. takto: Certifikační politika je soubor pravidel vztahujících se k vydávání a další správě kvalifikovaných certifikátů, použití a akceptace kvalifikovaných certifikátů a ochraně (nakládání, správě) párových dat. Tato pravidla se vztahují na poskytovatele, žadatele, držitele, osoby spoléhající na certifikát a na smluvní partnery. Při zpracování Certifikační politiky se doporučuje použít dokument RFC 2527 Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework[24]. Dokument Certifikační politika je obecně (v mezinárodním kontextu) vyžadován při provozování certifikačních služeb. Je základním dokumentem poskytovatele, ve kterém deklaruje pravidla pro všechny subjekty, které na poskytování certifikačních služeb participují, tj. pro poskytovatele, žadatele, držitele, osoby spoléhající na certifikát a na smluvní partnery. RFC 2527 Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework je mezinárodně uznávaným dokumentem, na jehož základě se certifikační politiky poskytovatelů zpracovávají, přičemž se respektuje jeho obsah i struktura[17]. Tento

dokument, jako základní dokument poskytovatele, je svým charakterem a obsahem určen ke zveřejnění. Podle § 6 odst. 6) je poskytovatel povinen zajistit zveřejnění Certifikační politiky v plném znění (předpokládá se v českém jazyce). Povinným obsahem Certifikační politiky je popis vlastností, které musí splňovat párová data, která si vytváří žadatel a k nimž má být vydán kvalifikovaný certifikát. Kryptografické algoritmy a jejich parametry, které mohou být pro párová data použity, jsou uvedeny v příloze 1 Vyhlášky.

2) Při zpracovávání Certifikační prováděcí směrnice postupují poskytovatelé podle § 8 Vyhlášky. Dokument Certifikační prováděcí směrnice úzce navazuje na dokument Certifikační politika. Certifikační politika stanoví pravidla a Certifikační prováděcí směrnice postupy zajišťující tato pravidla. Stejně jako u Certifikační politiky, Vyhláška doporučuje postupovat podle dokumentu RFC 2527 Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework. Poskytovatel je povinen v Certifikační prováděcí směrnici definovat činnosti, na které jsou z hlediska náležitého fungování certifikačních služeb kladeny zvýšené nároky. Jedná se zejména o takové činnosti, u kterých selhání osoby při jejich výkonu má vliv na informační bezpečnost - § 8 odst. 2) Vyhlášky. Poskytovatel je povinen zajistit provedení auditu této směrnice. Tento audit se provádí před zahájením vydávání kvalifikovaných certifikátů, dále podle plánu poskytovatele, nejméně však jednou ročně. Audit se rovněž provádí vždy, kdy dojde k podstatným změnám Certifikační prováděcí směrnice. Auditem se ověřuje, zda Certifikační prováděcí směrnice splňuje požadavky uvedené v zákoně, v této vyhlášce a je zpracována v souladu s dokumentem RFC 2527 Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework[24].

3) Dokument Celková bezpečnostní politika představuje soubor kritérií pro hodnocení bezpečnosti informačního systému na úrovni vrcholového managementu. V dokumentu jsou deklarovány zásady bezpečnosti a vrcholový management prohlašuje, že tyto zásady bezpečnosti bude dodržovat jako východiska a hodnotící kritéria pro své všechny další kroky. Požadavky na tento dokument jsou upraveny v § 9 Vyhlášky. Vyhláška v § 9 odst. 2) stanoví, že poskytovatel je povinen Celkovou bezpečnostní politiku zpracovat v souladu s touto vyhláškou a s požadavky ČSN/ISO/IEC TR 13335 nebo ISO 17799[24]. ISO 17799 se stane v roce 2001 až 2002 ČSN. Stejně jako Certifikační politika, i dokument Celková bezpečnostní politika je určen ke zveřejnění[17]. Ti, kdo hodlají využívat certifikačních služeb poskytovatele, se mohou

seznámit s cíli a způsobem zajištění celkové bezpečnosti organizace poskytovatele a rozhodnout se, zda jeho služeb využijí. Vyhláška stanoví pro Celkovou bezpečnostní politiku též povinnost auditu. Tento audit se provádí před zahájením vydávání kvalifikovaných certifikátů, dle plánu poskytovatele, nejméně však jednou za dva roky a dále vždy, kdy dojde k podstatným změnám Celkové bezpečnostní politiky[24]. Auditem se ověřuje, zda Celková bezpečnostní politika splňuje požadavky Vyhlášky a požadavky ČSN/ISO/IEC TR 13335 nebo ISO 17799.

4) Na rozdíl do Celkové bezpečnostní politiky, která se týká celkové bezpečnosti organizace poskytovatele, se Systémová bezpečnostní politika zabývá konkrétním informačním systémem poskytovatele, který je užíván pro zajištění certifikačních služeb. Obsahuje požadavky a postup řešení, které se k tomuto informačnímu systému vztahují. Systémová bezpečnostní politika se nezveřejňuje, neboť její zveřejnění by mohlo poškodit zájmy poskytovatele a ohrozit bezpečnost provozovaného informačního systému[17]. Dokument Systémová bezpečnostní politika musí dle § 10 odst. 1) Vyhlášky obsahovat: a) způsob implementace Celkové bezpečnostní politiky ve vztahu k informačnímu systému pro certifikační služby, b) popis, jak je oddělen informační systém pro certifikační služby od jiných informačních systémů poskytovatele, c) způsob ochrany dat a jiných prvků informačního systému pro certifikační služby, d) konkrétní hrozby zjištěné analýzou rizik, e) konkrétní bezpečnostní opatření, f) způsob nakládání s informacemi zařazenými do jednotlivých stupňů klasifikace, uvedené v Celkové bezpečnostní politice[24]. Zpracování Systémové bezpečnostní politiky se musí řídit ZoEP, Vyhláškou a normou ČSN/ISO/IEC TR 13335 nebo ISO 17799. Poskytovatel je, analogicky s Celkovou bezpečnostní politikou, povinen zajistit provedení auditu i u Systémové bezpečnostní politiky.

5) Plán pro zvládání krizových situací a Plán obnovy stanoví postupy, které jsou uplatněny v případě bezpečnostního incidentu a postupy vedoucí k nápravě[24]. Tyto dokumenty slouží pro zachování dostupnosti informací a služeb. Definují kritické oblasti, určují postupy a jejich zachování v případě vzniku mimořádných událostí, rozpracovávají řešení kritických a mimořádných událostí do podoby konkrétních postupů a procedur. Tyto plány typicky zahrnují postupy týkající se reakce na mimořádnou událost, obnovy základních funkcí, prozatímního provozu, obnovy plného provozu . Plán pro zvládání krizových situací a Plán obnovy je standardně vyžadován při provozování informačních systémů[17]. Vyhláška pro tyto dokumenty nestanoví vzorovou normu. Obsah obou Plánů je tedy plně v kompetenci poskytovatele.

3.4.8. Další podmínky udělení akreditace

Zákon č. 227/2000 Sb., o elektronickém podpisu v § 10 Podmínky udělení akreditace pro poskytování certifikačních služeb odst. 2 písm. d) ukládá žadateli o akreditaci doložení věcných, personálních a organizačních předpokladů pro činnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty podle § 6 tohoto zákona. Vyhláška konkretizuje tyto podmínky v § 12. Splnění věcných, personálních a organizačních předpokladů se dokládá následujícími dokumenty: a) dokumenty, které tvoří předpisovou základnu podle § 6 odst. 1), b) výsledky provedených auditů Certifikační prováděcí směrnice, Celkové bezpečnostní politiky a Systémové bezpečnostní politiky, c) seznamem jmen osob, které pro poskytovatele vykonávají činnosti uvedené v § 8 odst. 2), tedy osob provádějících audit, s uvedením jejich kvalifikace a délky praxe[24].

Úřad musí dále podle § 6 odst. 1) písm. j ZoEP posoudit, zda systémy a nástroje elektronického podpisu odpovídají zákonu a Vyhlášce. Tato povinnost není v § 12 uvedena, vyplývá však ze zákona.

Velmi důležitým aspektem poskytování certifikačních služeb je zaznamenávání událostí spojených s touto činností a dlouhodobé uchovávání těchto záznamů. Zaznamenávání událostí slouží pro možnost následného dohledání událostí, které u poskytovatele nastaly a které mohou být využity jako podklady pro případné soudní řízení[21]. Proto, aby záznamy událostí plnily předpokládaný účel, je nutné s nimi nakládat bezpečným způsobem. K tomu patří i bezpečný způsob jejich zničení, který lze doložit například protokolem o jejich zničení. Takovýto postup je vyžadován paragrafem 13 odst. 2) Vyhlášky. Podle § 6 odst. 9) ZoEP musí provozní dokumentace obsahovat:

a) smlouvu s podepisující osobou o vydání kvalifikovaného certifikátu,
b) vydaný kvalifikovaný certifikát,
c) kopie předložených osobních dokladů podepisující osoby,
d) potvrzení o převzetí kvalifikovaného certifikátu podepisující osobou,
e) přesné časové určení doby platnosti vydaného kvalifikovaného certifikátu[24].

Na toto ustanovení navazuje § 13 odst. 3) Vyhlášky. Stanoví, že zaznamenávány jsou všechny informace a události vztahující se k registraci a životnímu cyklu vydávaných kvalifikovaných certifikátů, zejména pak: a) identifikace místa uložení provozní (výše zmíněné) dokumentace, b) identifikační údaje osoby, která provedla

ověření totožnosti žadatele, c) obchodní název poskytovatele, který žádost o vydání kvalifikovaného certifikátu přijal, nebo smluvního partnera, který pro poskytovatele tuto činnost zajišťuje, d) všechny požadavky na zneplatnění kvalifikovaných certifikátů a záznamy o jejich zneplatnění, e) všechny požadavky na vydání kvalifikovaných certifikátů[24].

Vyhláška v odst. 4) také upravuje povinnost zaznamenávání událostí vztahujících se k párovým datům poskytovatele a kvalifikovaným certifikátům poskytovatele. Párovými daty poskytovatele a jeho kvalifikovaným certifikátem se "certifikují", tj. stvrzují údaje v kvalifikovaných certifikátech, které poskytovatel vydává[17]. Je tedy nezbytné všechny související události zaznamenávat. Podle odst. 5) je poskytovatel povinen opatřit zaznamenávané události časovým údajem, tj. údajem o době, kdy nastaly. Jakým způsobem poskytovatel čas určí a záznam provede, je povinen deklarovat v Certifikační prováděcí směrnici. Jedná se zde o časová razítka aplikovaná na interní dokumentaci.

V této souvislosti je třeba upozornit, že ani ZoEP ani Vyhláška neobsahují ustanovení, které by upravovalo používání časových razítek při procesu podepisování. Poskytovatel certifikačních služeb tedy není žádným právním předpisem nucen poskytovat služby ČA mimo své interní potřeby. Důsledky vyplývající z používání elektronického podpisu neopatřeného časovým razítkem byly uvedeny v kapitole 3.1.11. Takovýto podpis by při sporu o platnost podepsaného dokumentu pozbýval své právní váhy. Tvůrci ZoEP i Vyhlášky tedy „mlčky“ předpokládají, a praxe je taková, že poskytovatelé provozují služby ČA dobrovolně[17]. Důvodem k tomu je finanční a nárokové rozlišení služeb poskytovatele. Bude-li žadatel vyžadovat používání časových razítek při posílání a doručování elektronických dokumentů, cena takové služba vzroste. Naopak, jestliže situace nebude vyžadovat potvrzení času při výměně elektronických dokumentů (posílání soukromých e-mailů, placení limonády mobilním telefonem, apod.), nebude ČA potvrzovat přijetí a odeslání, a cena takovéto služby bude výrazně menší[17].

3.4.9. Požadavky na technické vybavení

Do této chvíle jsme se zabývali právy a povinnostmi, které klade Vyhláška spolu se ZoEP na služby a dokumenty poskytovatele certifikačních služeb. V další části se zaměříme na požadavky, které jsou kladeny na technické vybavení poskytovatele, potažmo držitele (§ 2 Vyhlášky).

V procesu tvorby a používání elektronického podpisu stojí nástroje pro vytváření párových dat (§ 2 písm. i Vyhlášky) na prvním místě. Tyto nástroje musí být z hlediska kryptografie dostatečně bezpečné. Tato podmínka se považuje za splněnou, pokud nástroj splňuje hodnocení podle Security Requirements for Cryptographic Modules (FIPS 140-1) úroveň 3[24]. Security Requirements for Cryptographic Modules (FIPS 140-1) je standardem, který vydal National Institute of Standards and Technology v USA jako Federal Information Processing Standard. Je běžně užívaný pro hodnocení bezpečnosti kryptografických modulů. Prozatím neexistuje česká či mezinárodní norma, která by jej nahradila. Z tohoto důvodu například i Rakousko uvádí FIPS ve vyhlášce ke svému zákonu o elektronickém podpisu[17]. Příslušné orgány EU avizují, že v budoucnu budou usilovat o zpracování normy, která by FIPS v evropských podmínkách nahradila, neboť si uvědomují obtížnost při zavádění standardu jiného státu do národních legislativ. Párová data si může žadatel vygenerovat sám na vlastní nebezpečí nebo může o jejich vygenerování požádat poskytovatele. V takovém případě je povinen poskytovatel nakládat před jejich předáním žadateli bezpečným způsobem a předat je žadateli tak, aby nebyla vyzrazena. Postup při nakládání s párovými daty žadatele před jejich předáním žadateli a při předání žadateli stanoví poskytovatel v Certifikační prováděcí směrnici. Zároveň je poskytovatel povinen zajistit, že párová data, pokud je poskytovatel pro žadatele vytváří, splňují parametry uvedené v příloze 1 Vyhlášky[24]. Poskytovatel je přirozeně povinen (podle § 14 odst. 4) doložit Úřadu používání výše zmíněného postupu a splnění požadavku podle odst. 1) v dokumentech Předpisové základny.

Vysoké nároky na bezpečnost musí být kladeny i na párová data poskytovatele. Vyhláška stanoví, že nástroje pro tvorbu párových dat poskytovatele musí splňovat stejné podmínky jako nástroje pro vytváření párových dat pro žadatele podle § 14 odst. 1) a zároveň musí být použity kryptografické algoritmy splňující parametry uvedené v příloze 1 Vyhlášky[24]. Vytváření párových dat poskytovatele musí provádět, podle § 15 odst. 1), pouze osoba k tomu určená a provádí je způsobem definovaným v Certifikační prováděcí směrnici[24]. Dalšími osobami, které mohou manipulovat s jeho daty pro vytváření elektronického podpisu jsou osoby vykonávající audit podle § 8 odst. 3). Pro data pro vytváření elektronického podpisu poskytovatele neplatí § 6 odst. 3) ZoEP. Poskytovatel naopak musí vlastnit záložní kopie těchto dat a musí zabezpečit jejich stejnou nebo vyšší bezpečnost, než bezpečnost dat určených pro používání. Po ukončení jejich životního cyklu, musí data prokazatelně zničit[24]. Zničení dat pro

vytváření elektronického podpisu poskytovatele znemožní neoprávněnou manipulaci s nimi. Prokazatelné zničení lze doložit například protokolem o zničení.

Data pro vytváření elektronického podpisu poskytovatele se smějí, jak již bylo uvedeno, používat výhradně pro podepisování kvalifikovaných certifikátů a seznamu zneplatněných certifikátů. Vyhláška v § 16 upravuje používání kryptografických hardwarových prostředků užívaných poskytovatelem pro aplikaci těchto dat. S kryptografickým hardwarovým prostředkem užívaným pro podepisování kvalifikovaných certifikátů a seznamu zneplatněných certifikátů musí být při jeho skladování, přepravě a uvádění do provozu nakládáno bezpečným způsobem, tj. musí být zachovány podmínky uvedené v § 17 odst. 1) písm. a - d. V případě ukončení činnosti tohoto prostředku musí být data v něm uložená zničena. Prokazatelné zničení se prokazuje například protokolem. Splnění těchto požadavků musí poskytovatel na požádání Úřadu doložit[24].

ZoEP vymezuje prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů v § 16. Vyhláška upřesňuje požadavky na tyto ve svém § 16. Prostředek musí zajistit, aby podepisující osoba:

a) byla nucena projevit svoji vůli k podepsání dokumentu,
b) se mohla seznámit (plně) s obsahem podepisovaného dokumentu,
d) byla nucena zadat přístupové heslo nebo byl uplatněn jiný obdobný autentizační mechanismus[24].

Je zde znát jasná snaha předcházet problému hledání projevu vůle při odcizení dat pro vytváření elektronického podpisu. Problém autentizace a autentizačního mechanismu může při zajištění bezpečnosti daného prostředku výrazně snížit riziko neoprávněného použití elektronického podpisu[17]. Vyhláška dále stanoví, že prostředek pro bezpečné vytváření elektronického podpisu musí být hodnotitelný podle ISO 15408 na míru záruky EAL 3 nebo podle ITSEC verze 1.2 úroveň E 3. Nosiče, na které je možné data pro vytváření elektronického podpisu ukládat, musí být hodnotitelné podle Security Requirements for Cryptographic Modules (FIPS 140-1) úroveň 2[24]. Poskytovatel, dříve než začne používat určitý prostředek pro bezpečné vytváření elektronického podpisu, musí poskytnout spolu se žádostí specifický popis jeho komponent Úřadu. Ten buď používání schválí, či ne. Seznam těchto komponent je uveden v příloze č.2. Úřad může rozhodnout o době přípustné pro užívání, pokud se objeví "bezpečnostní díry" - pak již prostředek nesplňuje stanovené požadavky a Úřad rozhodne, že takový prostředek nelze nadále považovat za bezpečný a jeho další

používání by bylo považováno za porušení zákona. Pro prostředek pro bezpečné ověřování elektronického podpisu platí § 16 odst. 4). Tento prostředek musí být též hodnotitelný podle ISO 15408 na míru záruky EAL 3 nebo podle ITSEC verze 1.2 úroveň E 3 a poskytovatel musí při schvalování používání tohoto prostředku postupovat analogicky s prostředkem pro bezpečné vytváření elektronického podpisu[24].

Na informační systém poskytovatele se vztahuje § 18. Informační systém musí být podle odst. 1) hodnotitelný na míru záruky EAL 4 podle ISO 15408 nebo úroveň E 3 podle ITSEC verze 1.2[24]. Norma ISO 15408 bude v průběhu tohoto roku přijata jako ČSN. ITSEC (Information technology Security Evaluation Criteria) jsou harmonizovanými kritérii pro hodnocení bezpečnosti informačních systémů. Byla vydána Evropskou komisí v roce 1991 a publikována Úřadem pro oficiální publikace Evropských společenství pod číslem (90) 314. Vydání v České republice a v českém jazyce zajistilo v roce 1993 Ministerstvo hospodářství ČR. ITSEC je mezinárodně (zejména v rámci Evropy) uznávaným dokumentech s charakterem normy a běžně se užívá k hodnocení bezpečnosti informačních systémů[3]. Jako ISO nebyl přijat proto, že se předpokládalo jeho nahrazením následným dokumentem, Common Criteria for Information Technology Security Evaluation, na jehož vniku se podílely i mimoevropské státy. Tento dokument byl po svém vzniku přijat jako ISO 15408, ovšem ITSEC plně nenahradil[3]. Z tohoto důvodu se v současné době užívají pro hodnocení bezpečnosti informačních systémů, zejména v Evropě, souběžně oba dokumenty. ITSEC nelze v plném rozsahu nahradit žádnou jinou normou či normami. Z tohoto důvodu uvádí ITSEC například i Rakousko ve své vyhlášce k zákonu o elektronickém podpisu.

3.4.10. Bezpečnost

Vyhláška v § 18 odst. 4) upravuje chování poskytovatele v situaci, kdy dojde k vyzrazení dat pro vytváření elektronického podpisu poskytovatele. Vyzrazení dat pro vytváření elektronického podpisu poskytovatele je závažným bezpečnostním incidentem, při němž hrozí zneužití vyzrazených dat. Z tohoto důvodu je v takovém případě nezbytné, aby poskytovatel informaci o vyzrazení zveřejnil a zároveň zneplatnil kvalifikované certifikáty, které mohou být vyzrazením ovlivněny. Poskytovatel je povinen stanovit v Havarijním plánu a Plánu obnovy postup, který uplatní v případě vyzrazení jeho dat pro vytváření elektronického podpisu poskytovatele. Zároveň je povinen stanovit lhůty, ve kterých stanovená opatření uplatní.

Výše uvedené požadavky se považují za splněné, pokud byly shledány splněnými při auditu Certifikační prováděcí směrnice, Celkové bezpečnostní politiky a Systémové bezpečnostní politiky (při auditu dokumentů Předpisové základny)[24].

Vyhláška se zabývá i tzv. objektovou bezpečností. Pro stanovení požadavků na objektovou bezpečnost s výhodou využívá platné vyhlášky Národního bezpečnostního úřadu o objektové bezpečnosti. Jako postačující se stanoví splnění požadavků, které vyhláška stanoví pro stupeň důvěrné[3].

Jak ZoEP, tak Vyhláška kladou požadavky na osoby vykonávající certifikační nebo související služby. Osoby vykonávající tyto činnosti musí být odborně způsobilé a poskytovatel jim musí zajišťovat průběžná školení[24]. Odpovídající odbornost osob, které certifikační služby zajišťují, je předpokladem jejich náležitého fungování. Odbornost je nezbytné průběžně zvyšovat formou školení. Bezpečnostní vědomí je uvědomění si všech aspektů bezpečnosti při poskytování certifikačních služeb a uzpůsobení vlastního chování tak, aby byla stanovená úroveň bezpečnosti dodržována. Zvláštní omezení je kladeno na osoby vykonávající činnosti uvedené v § 8 odst.3), které nesmí mít záznam v rejstříku trestů. Jedná se o činnosti, na které jsou z hlediska náležitého fungování certifikačních služeb kladeny zvýšené nároky a u kterých selhání osoby při jejich výkonu má vliv na informační bezpečnost. Účastníci elektronické komunikace s využitím elektronického podpisu musí mít záruku, že tyto činnosti vykonávají osoby, které jsou důvěryhodné. Absence záznamu v rejstříku trestů je jedním z výrazů důvěryhodnosti. Vyhláška dále po těchto osobách požaduje nezbytnou kvalifikaci. Tu definuje § 24 Vyhlášky následovně: a) ukončené vysokoškolské vzdělání a 3 roky praxe, b) ukončené vyšší odborné nebo úplné střední odborné vzdělání a 5 let praxe[24]. Poskytovatel může podle odst. 2) zkrátit v jednotlivých případech délku praxe až o jednu třetinu. V mimořádných situacích je nutné, aby osoby uvedené v § 8 odst. 3) byly zastoupeny při výkonu činnosti jinými osobami. Pro tyto případy je nezbytné stanovit, které osoby jsou oprávněné k zastupování, za jakých podmínek a jaké kontrolní mechanismy jsou v takovém případě uplatněny.

3.4.11. Audit

Audit, jak z Vyhlášky vyplývá, je pro bezpečné fungování a důvěryhodnost poskytovatele velice podstatná událost. Na osoby provádějící audit jsou tedy kladeny vysoké nároky. § 21 ještě omezuje okruh osob, které audit mohou provádět. Audit totiž mohou provádět pouze osoby, které mají ukončené vysokoškolské vzdělání příslušného

technického nebo příslušného přírodovědného směru a 6 let odborné praxe. Audit nesmí u poskytovatele provést osoba, která:

a. má majetkovou účast ve společnosti poskytovatele,
b. je společníkem poskytovatele, statutárním orgánem nebo členem statutárního orgánu poskytovatele, anebo je v pracovním nebo obdobném vztahu k poskytovateli,
c. je osobou blízkou osobám, jejichž postavení by mohlo ovlivnit její činnost[24].

3.4.12. Ukončení činnosti poskytovatele

Ukončení činnosti poskytovatele, který spravuje kvalifikované certifikáty, které vydal, postihne vždy do určité míry negativně držitele a osoby spoléhající na certifikát. Poskytovateli se ukládá, aby tyto negativní důsledky svými opatřeními minimalizoval. Zákon v tomto smyslu ukládá v § 13 akreditovanému poskytovateli, aby vynaložil veškeré možné úsilí na to, aby platné kvalifikované certifikáty byly převzaty jiným akreditovaným poskytovatelem certifikačních služeb. Ustanovení Vyhlášky v § 23 odst. 5) ukládá poskytovatelům vydávajícím kvalifikované certifikáty, a to ať jsou či nejsou Úřadem akreditováni, aby v případě, že zajistí správu vydaných kvalifikovaných certifikátů u jiného poskytovatele, byly podmínky poskytování certifikačních služeb u obou poskytovatelů srovnatelné. Poskytovateli se též ukládá povinnost v Certifikační prováděcí směrnici stanovit postup, který bude uplatněn v případě ukončení jeho činnosti[24]. Postup, který poskytovatel uplatní v případě ukončení své činnosti, musí stanovit již v době, kdy vydá první kvalifikovaný certifikát a musí jej popsat v Certifikační prováděcí směrnici. Žadatel má tedy možnost seznámit se s tímto postupem ještě před uzavřením smlouvy o poskytování certifikačních služeb. Zákon akreditovanému poskytovateli v § 13 ukládá, aby prokazatelně informoval každou podepisující osobu, které poskytuje své certifikační služby, o svém záměru ukončit svoji činnost nejméně 2 měsíce předem. Další povinnosti akreditovaného poskytovatele se týkají jeho povinností k Úřadu. Ustanovení Vyhlášky § 23 odst. 3 písm. a) - d) specifikují povinnosti poskytovatele, který vydává kvalifikované certifikáty, a to ať je či není Úřadem akreditován. K těmto povinnostem patří zpřístupnění informace o ukončení činnosti všem dotčeným subjektům, ukončení vydávání kvalifikovaných certifikátů, uchování údajů získaných při registraci a záznamů událostí a prokazatelné zničení dat pro vytváření elektronického podpisu poskytovatele. Poskytovatel je dále povinen stanovit, jak bude postupováno v případě, že tyto povinnosti nebude schopen

splnit sám, resp. který subjekt předmětné činnosti zajistí, a jak je převod činností zajištěn[24].

V ZoEP je v § 6 odst. 1) písm. l požadováno, aby poskytovatel měl k dispozici dostatečné finanční zdroje na provoz. Vyhláška toto ustanovení v § 25 konkretizuje. Požaduje se, aby poskytovatel měl k dispozici takové finanční zdroje na provoz, tj. na poskytování certifikačních služeb, které jsou dostačující na současný provoz a provoz v časovém horizontu 3 let. Dostatečnost finančních zdrojů musí poskytovatel doložit výroční zprávou[24].

3.4.13. Přílohy

K Vyhlášce je připojen text obsahující dvě přílohy. Příloha č. 1 osahuje technické požadavky na minimální kryptografické parametry. Tyto požadavky musí splňovat párová data držitele a párová data poskytovatele resp. nástroje pro jejich vytváření. Příloha č. 2 obsahuje specifické komponenty, které je třeba podrobně popsat při popisu prostředků pro bezpečné vytváření elektronického podpisu a při popisu prostředků pro bezpečné ověřování elektronického podpisu. Tyto komponenty se vztahují jak k důvěryhodnému prostředí, tak k vlastním aplikacím elektronického podpisu.

3.5. Předběžné zhodnocení

Prováděcí Vyhláška Úřadu pro ochranu osobních údajů má za úkol konkretizovat požadavky na držitele a poskytovatele certifikačních služeb. V řadě aspektů je však „němá“ a poskytuje tak volnost vývoji na trhu certifikačních služeb. Tato situace je v souladu s požadavky EU.

Po vydání Vyhlášky se budou moci v České republice fungující poskytovatelé certifikačních služeb, a případně další zájemci o provozování této činnosti, rozhodnout – buď zůstanou “vně” zákona, nebo budou vydávat kvalifikované certifikáty a učiní opatření pro splnění příslušných ustanovení zákona a připravovaných prováděcích předpisů, případně, opět po splnění příslušných zákonných předpokladů, požádají Úřad o akreditaci.

4. Přístup EU k elektronickému podpisu

4.1. Vývoj elektronického podpisu

Elektronický podpis je na soukromoprávní úrovni používán již řadu let. Počátky používání digitálního podpisu sahají do sedmdesátých let dvacátého století. V té době začal v USA rozvoj asymetrické kryptografie, která je základem digitálního podepisování[1]. S rozmachem elektronické komunikace, a internetu především, vzrostla i poptávka po bezpečné elektronické komunikaci. Vznikla celá řada šifrovacích algoritmů (RSA, DSS, později systémy na bázi eliptických křivek), které dokázaly za určitých podmínek bezpečnost zajistit[1,16].

Hlavními uživately elektronického podpisu byly bankovní ústavy a velké korporace. Mezi těmito subjekty se rozvinula rozsáhlá síť výměny elektronických dat. Důsledkem toho bylo sjednocení různých dat pro vytváření elektronického podpisu jednotlivých uživatelů v jeden klíč, viz. kapitola 5.3. Každý subjekt elektronické komunikace tak mohl používat jeden vlastní klíč k podepisování dat pro více různých adresátů. I když tato komunikace byla relativně bezpečná, vznikaly zde požadavky na ověření a důvěru v tento klíč. Řešením byli poskytovatelé certifikačních služeb neboli tzv. důvěryhodné třetí strany. Stávaly se jimi většinou firmy zajišťující výše zmíněnou komunikaci dotyčných stran. Služby spojené s poskytováním certifikačních služeb byly pouze doplňkem jejich hlavní činnosti a jejich cena byla symbolická[1].

V současné době je množství uživatelů elektronického podpisu mnohem větší než kdykoli v minulosti. Díky nízkým, doplňkovým cenám využívá služby poskytovatelů certifikačních služeb široká řada uživatelů. Jejich komunikace prostřednictvím elektronických podpisů je však omezena pouze na soukromoprávní sféru. Také nerovnoprávnost elektronického podpisu a vlastnoručního podpisu stále klade omezení pro používání elektronické komunikace. V řadě zemí to však již neplatí[1].

USA, které jsou kolébkou většiny šifrovacích algoritmů díky svým vojenským výzkumným programům, uvedly v roce 1995 v platnost vůbec první zákon, který zrovnoprávňuje elektronický a vlastnoruční podpis a umožňuje komunikaci s orgány veřejné moci v elektronické podobě. Tento zákon byl přijat ve státě Utah a brzy jeho vzor následovalo ostatních 50 států federace[10]. V roce 2000 byl v USA konečně přijat i Federální zákon o používání digitálního podpisu, který sjednocuje právní úpravu na území USA. Symbolickou, ale důležitou úlohu při zrovnoprávnění elektronického a

vlastnoručního podpisu měla dohoda o podpoře pro elektronický obchod. Americký prezident Clinton a irský ministerský předseda Ahern ji 4. září 1998 podepsali elektronicky. Bylo to poprvé, co byl elektronický podpis použit na takto vysoké úrovni.

Dohoda je zajímavá sama o sobě, neboť se vyjadřuje ke všem klíčovým otázkám elektronického obchodování. Například se zde říká, že klíčovou roli v elektronickém obchodě hraje liberalizace telekomunikačního trhu a že elektronický obchod zvýší životní úroveň obou států. Dále se prohlašuje, že role vlád spočívá ve vytvoření jasného a konzistentního právního rámce pro elektronický obchod a ve vytvoření konkurenčního prostředí, v kterém by se mohl rozvíjet a zajistit adekvátní ochranu veřejných zájmů v oblastech, jako je soukromí, intelektuální vlastnická práva, prevence proti podvodům, ochrana zákazníků a bezpečnost. Dohoda se vyjadřuje i k tolik diskutovaným daním z elektronického obchodu a dokonce i k systému doménových jmen[10].

Na Evropském kontinentě je situace podobná. V roce 1997 byly v řadě států EU přijaty zákony upravující používání elektronického podpisu, které byly více či méně kompatibilní. V Německu byl přijat zákon upravující rámcové podmínky pro ověřování platnosti digitálního podpisu v souvislosti se zákonem o informacích a telekomunikacích[10]. Německý zákon mimo jiné stanoví pravidla pro vznik systému certifikačních autorit na základě volné soutěže a pravidla pro jejich uznávání a kontrolu, definuje minimální požadavky na bezpečnost certifikačních autorit. Zákon neomezuje použití technických prostředků pro digitální podpis na žádné národní standardy a vytváří tak široké možnosti pro budoucí integraci tohoto systému do mezinárodního prostředí. Německý zákon uznává privátní podepisovací klíč jako unikát, kterým je možno jednoznačně prokázat autenticitu jeho použití danou osobou a zároveň stanovuje požadavek ochrany tohoto klíče všemi dostupnými a organizačními prostředky[10].

Podobný zákon jako SRN měly i Velká Británie, Itálie a jiné evropské státy. Tyto zákony ale vycházely z různých paradigmat a pohledů na problematiku. Proto, aby mohly být elektronické podpisy používány internacionálně, bylo nutné vytvořit universální pravidla pro jejich používání. Možnosti řešení byly v podstatě dvě: I. vydat zvláštní vzorový zákon – např. o elektronickém obchodu, jehož začleněním do legislativ jednotlivých států by se sjednotila úprava problematiky nebo II. vydat závazný přepis, na jehož základě by se v jednotlivých státech vytvořila právní úprava, která by byla v souladu s tímto předpisem a tím by se zabezpečila interoperabilita postupů elektronického podpisu na nadnárodní úrovni[22].

4.2. Vzorový zákon o elektronickém podpisu

První možnost ukazuje Vzorový zákon o elektronickém obchodu Komise OSN pro mezinárodní obchodní právo (UNCITRAL). Jde o návrh velmi obecný, který má sloužit všem zemím, jež v souladu s technologickým pokrokem potřebují modernizovat svoji legislativu. Obecnost tohoto návrhu, který je výsledkem mnoha kompromisů typických pro dokumenty OSN, je zřejmě na překážku jeho aplikování do právních řádů členských zemí[19]. Charakteristickým rysem elektronického obchodu je, že zahrnuje datové zprávy, což představuje podstatný rozdíl oproti tradičním dokumentům v tištěné formě. Vzorový zákon vychází z úvahy, že uživatelé budou potřebovat ucelený soubor pravidel, použitelných na různé druhy komunikačních prostředků, které by bylo možné při jejich používání vzájemně zaměnit, a že zásadně žádný z komunikačních prostředků není z rozsahu Vzorovým zákonem navrhovaných řešení vyloučen, protože je nutno přihlédnout k budoucímu technickému vývoji. Vzorový zákon spočívá na „funkčně ekvivalentním přístupu“, vycházející z analýzy účelů a funkcí, vyžadovaných od tradičních, na papíře vytištěných dokumentů, vzhledem k tomu, do jaké míry tyto účely či funkce lze realizovat elektronicko-komerčními prostředky[19]. Např. mezi prostředky, které dokument na papíře poskytuje, náleží: jistota, že každý si může dokument přečíst; možnost zajistit, aby dokument nepodléhal změnám času; taková jeho reprodukce, aby každá ze stran mohla vlastnit kopii se stejnými údaji; umožnit ověření údajů podpisem; zajistit, aby dokument existoval v takové formě, kterou by bylo možné předložit úřadům a soudním dvorům. Datovou zprávu samu o sobě nelze považovat za naprostý ekvivalent dokumentu vytištěného na papíře pouze z toho důvodu, že její povaha je rozdílná a nutně nesplňuje veškeré možné funkce jako papírový dokument. Je třeba zdůraznit, že i při všech uvedených funkcích papíru může elektronický záznam poskytnout stejnou úroveň jistoty jako papír a (ve většině případů) podstatně vyšší úroveň spolehlivosti a rychlosti, zejména s ohledem na identifikaci zdroje dat za předpokladu, že bude splněna řada technických a právních požadavků. Přijetí funkčně ekvivalentního přístupu by podle vzorového zákona nemělo vyústit u elektronického obchodu v uložení přísnějších požadavků na bezpečnost (a s tím i spojených nákladů), než je tomu u dokumentů na papíře[19]. Klíčová myšlenka zákona, že informaci nelze upřít právní důsledky, platnost nebo vykonatelnost jen proto, že má formu datové zprávy, je jistým převratem v doposud omezeném chápání písemností a dokumentace jakožto informací výlučně spjatých s papírovým nosičem.

Vzorový zákon se však nesetkal s očekávanou odezvou. Proč zatím nebyl tento návrh aplikován do právních řádů členských zemí OSN, má zřejmě více důvodů, mezi nimiž nepochybně figurují:

- obecnost, která je výsledkem mnoha kompromisů,
- z toho vyplývající obtížná aplikovatelnost,
- snaha většiny států nezavádět zvláštní právní úpravy tam, kde postačí stávající norma nebo její novelizace[19].

Začlenění zákona o elektronickém obchodu ve smyslu dokumentu UNCITRAL do našeho právního řádu – buď jakožto zvláštního zákona, nebo v rámci jiného zákona – by sice vytvořilo kýžené legislativní podmínky pro opravdový, nikoliv jen očekávaný rozvoj elektronického obchodování, problémem je, že by si rozsáhlý zákon vyžádal poměrně značné množství legislativních prací a to jak na zákonu samotném, tak na platných právních normách souvisejících. Navíc snaha je právě opačná – neatomizovat právní řád speciálními normami, ale homogenizovat jej v podobě co nejobecnějších právních úprav[19].

4.3. Směrnice Evropského parlamentu a rady 1999/93/ES

Evropská společenství, přestože členské státy mají daleko homogennější právní systémy, než členové OSN, se vydalo druhou cestou: vydáním směrnice, která stanoví pravidla hry pro jeden z nejdůležitějších aspektů elektronické komunikace, tj. elektronický podpis – s tím, že budou následovat další kroky upravující v rámci stávajícího právního rámce např. otázku odpovědnosti za škodu, obchodování na dálku, cel a daní, dálkového zaměstnání a podobně[19]. To je asi vhodnější cesta, což potvrzuje i skutečnost, že práce na normě pro elektronický podpis přes počáteční pomalý rozjezd byly rychle dokončeny a dne 13. prosince 1999 byla podepsána závazná směrnice Evropského parlamentu a rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (dále jen Směrnice), takže bylo možné i český návrh zákona připravovat paralelně s návrhem evropským.

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. Směrnice podporuje používání a právní uznání elektronických podpisů ve Společenství. Členským státům ukládá, aby své právní předpisy uvedly v soulad s ní do července roku 2001[25]. Směrnice je poměrně obecná, záměrně technicky neutrální, ale zároveň již deklaruje následné úsilí o

soulad v konkrétních požadavcích na technické i jiné aspekty elektronického podpisu. Důvodem je požadavek, aby byl elektronický podpis takový, aby v případě potřeby mohl být uznán i v jiném státě, než ve kterém byl pořízen, resp. aby mohl být uznán certifikát k danému klíči vydaný. Jinými slovy, požadavky na různé druhy elektronických podpisů a různé typy certifikátů musí být v zemích, kde se vzájemné uznávání předpokládá, jednotné. Zmíněné deklarované úsilí ES má už i konkrétní podobu. Na základě výzvy Evropské komise připravují evropské instituce a iniciativy dokumenty, jejichž obsahem je konkretizace těchto požadavků. Za nejvýznamnější lze v této oblasti považovat aktivity ETSI (European Telecommunications Standards Institute), EESSI (European Electronic Signature Standardization Initiative) a CEN (European Committee for Standardization)[22]. Zde již postupně vznikají dokumenty rozpracovávající i navazující na směrnici. Tyto dokumenty byly pro Úřad důležitým zdrojem informací pro tvorbu návrhu vyhlášky. Tak bude možné dosáhnout kompatibility s ES nejen samotným textem zákona, ale rovněž stanovením shodných podmínek pro vlastní fungování elektronického podpisu.

Předpisy, které vznikly před přijetím směrnice, jsou v současné době podrobovány revizi. Známý je příklad Německa, které již v roce 1997 jako první stát v Evropě schválilo zákon upravující náležitosti digitálního podpisu a následně vybudovalo rozsáhlou infrastrukturu. V současné době v Německu probíhají rozsáhlé změny v rámci harmonizace s ES[25].

4.3.1. Akreditace

Směrnice má 15 článků a 4 přílohy. Vzhledem k tomu, že český ZoEP vychází právě z této Směrnice, řada norem obou předpisů má stejný či podobný výklad. V článku 2 Směrnice jsou definovány pojmy spojené s používáním elektronického podpisu. Pojem akreditace resp. dobrovolná akreditace je zde definován šířeji než je tomu v ZoEP. Dobrovolnou akreditací se podle Směrnice rozumí 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[25]. ZoEP již konkrétně stanoví, že subjektem pro ověřování a udílení akreditace má být státní Úřad pro ochranu osobních údajů a konkrétně stanoví jeho práva a povinnosti. Tím je částečně naplněn i článek 3, který stanoví, že každý členský stát je povinen zajistit zavedení odpovídajícího systému

kontroly, který umožní dohled nad ověřovateli, kteří jsou usazeni na jeho území a kteří vydávají kvalifikovaná osvědčení pro veřejnost[25].

4.3.2. Odlišnosti českého zákona o elektronickém podpisu a směrnice EU

Jestliže jsme tvrdili, že ZoEP vychází ze Směrnice a je s ní plně kompatibilní, pak toto tvrzení musíme poopravit. ZoEP, resp. několik jeho ustanovení, je totiž v nepřímém rozporu se Směrnicí, za což je Komisí EU kritizován[17]. Jedná se především o článek 3 odst. 7 a článek 4 odst. 1 Směrnice. Ty říkají, že členské státy (mezi které bychom mohli patřit za několik let i my) 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 specifické vlastnosti daného použití. Tyto požadavky nesmí vytvářet překážky při poskytování přeshraničních služeb občanům[25]. Článek 4 odst. 1 dále říká, že každý členský stát bude pro ověřovatele usazené na svém území a pro služby, které poskytují, uplatňovat vnitrostátní právní předpisy. Členské státy nesmí v oblastech, na které se vztahuje tato směrnice, omezovat poskytování ověřovacích služeb pocházejících z jiného členského státu[25]. Naproti tomu ustanovení ZoEP tvrdí, že v oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty, vydávané akreditovanými poskytovateli certifikačních služeb, kteří mají sídlo na území České republiky, a zároveň tito poskytovatelé (ale i ostatní poskytovatelé certifikačních služeb vydávající kvalifikované certifikáty, pro které je ZoEP závazný) mohou bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec[23]. Vzniká zde hned několik kolizních situací:

1. Ač to Směrnice vyžaduje, náš ZoEP neumožňuje komunikaci zahraničních subjektů s našimi orgány veřejné moci prostřednictvím zahraničního poskytovatele. Tato situace se v době, kdy nejsme součástí EU, dá obejít uznáním zahraničního poskytovatele českým akreditovaným poskytovatelem nebo bilaterální smlouvou o uznávání certifikátů[17]. V případě, že daná ustanovení ZoEP budou stále v platnosti i v době naší anexe s EU, bude zákon v rozporu se Směrnicí, neboť bude klást překážky při poskytování přeshraničních služeb občanům.
2. Požadavek, aby akreditovaný poskytovatel mohl působit bez souhlasu Úřadu jen jako advokát, notář nebo znalec, je dle Komise EU značně diskriminační a porušuje tak článek 3 odstavec 7 Směrnice. V praxi je existence poskytovatelů certifikačních služeb (potencionálních akreditovaných poskytovatelů) podmíněna existencí jiné výdělečné činnosti daného subjektu, která mu umožňuje dosahovat přiměřených zisků.

Z toho důvodu jsou poskytovatelé schopni vydávat certifikáty a poskytovat služby s tím spojené za tak nízkou cenu, jaká je dnes běžná[17]. Bude-li chtít advokát, notář nebo znalec získat akreditaci na poskytování certifikačních služeb a bude-li chtít poskytovat plnohodnotné služby s tím spojené (časová razítka, on-line přístup k zneplatněným certifikátům apod.), bude ho investice do hardwarového a softwarového vybavení stát v současných cenách 40 až 50 milionů Kč[22]. Podle stejných odhadů by při omezené poptávce musel kvalifikovaný certifikát stát okolo 1 500,- Kč, což je o 400% více, než je současná běžná cena[22]. Je tedy otázkou, jaké bude množství žádostí o akreditaci a jak se k danému problému postaví Úřad, který má ve věci poslední slovo.

4.3.3. Uznávání elektronického podpisu

Směrnice v článku 5 stanoví, že členské státy musí dbát, aby elektronickým podpisům nebyla odpírána právní účinnost 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[25]. ZoEP tento požadavek řeší v několika krocích. Podle § 3 odst. 1) je nutné považovat elektronický dokument za podepsaný, pokud je opatřen elektronickým podpisem. A v paragrafech 21 až 27 provádí zákon novelizaci hlavních předpisů sbírky, ve kterých staví elektronický podpis dle tohoto zákona za rovnocenný vlastnoručním podpisům.

ZoEP v § 7 Odpovědnost za škodu resp. § 6 Povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty naplňuje požadavky článku 6 Směrnice o odpovědnosti poskytovatele. Podobně je tomu v případě článku 7 Mezinárodní hlediska.

4.3.4. Výbor pro elektronický podpis

Dle článku 9 a 10 se zřizuje Výbor pro elektronické podpisy, který má objasnit požadavky uvedené v přílohách této směrnice, kritéria uvedená v čl. 3 odst. 4 a obecně uznávané normy pro produkty pro elektronický podpis. Jeho činnost je dosti podobná Úřadu. Aby se naše úprava příliš nelišila od evropských norem, vycházel Úřad při zpracovávání Vyhlášky z výsledků zmíněného Výboru.

4.3.5. Přílohy

Obsahem příloh Směrnice jsou požadavky na kvalifikovaná ověření, na ověřovatele, kteří vydávají kvalifikovaná osvědčení, požadavky na prostředky pro

bezpečné vytváření elektronických podpisů a doporučení pro bezpečné ověřování podpisu. Tyto požadavky obsahuje též ZoEP a byly již zmíněny v kapitole 3.1.

4.3.6. Přezkoumání

Směrnice respektuje vývoj IT a proto ukládá Komisi, aby nejpozději do 19. července 2003 přezkoumala tuto Směrnici a její provádění[25].

Kontrola plnění požadavků této směrnice probíhá již i v současné době a netýká se pouze členských států EU. V rámci přizpůsobování práva kandidátských zemí prochází tímto kontrolním mechanismem i Česká republika. Ač je ZoEP v naší zemi poměrně vychvalovaný, Komise EU se nevyhýbá kritickým slovům na adresu tohoto zákona[17].

5. Užívání elektronického podpisu v současné praxi

Zákon o elektronickém podpisu, Směrnice Evropského parlamentu a rady o zásadách Společenství pro elektronické podpisy, ani Federální zákon USA týkající se digitálního podpisu nepřinášejí do současné praxe elektronické komunikace příliš nového. Ba naopak, vytváří legislativní rámec pro již osvědčené postupy bezpečného přenášení dat v elektronické podobě. Vhodně tak reagují na boom elektronického obchodu a elektronické komunikace jako takové, neboť právě v těchto oblastech se digitální podpis používá již řadu let. V této kapitole se proto hlouběji seznámíme s algoritmy vytváření, používání a ošetřování elektronického podpisu, které jsou v současné praxi užívané a které jsou nově i naším právním řádem vyžadovány.

V dalším textu uvádíme řadu pojmů, jejichž znalost je pro pochopení věci nezbytná. V příloze č. 1 je uveden jejich stručný výklad, definice.

5.1. Úvod do asymetrické kryptografie

Pojem elektronický - resp. digitální podpis se začal objevovat souběžně se vznikem asymetrické kryptografie již v druhé polovině sedmdesátých let dvacátého století[1]. Asymetrická kryptografie používá pro účely zabezpečení dat propojenou dvojici klíčů. První klíč (soukromý) slouží k šifrování dat a vytváří se jím digitální podpis. Druhý (veřejný) klíč slouží k dešifrování podpisu. Důležitou vlastností asymetrické kryptografie je používání jednocestných funkcí[6,10]. Je to funkce, u níž je snadné pro všechna x vypočítat hodnotu y, ale pro všechna y se nedají vypočítat x. Kryptografie s veřejným klíčem využívá tuto asymetrii k vytvoření funkcí, u kterých platí dvě základní pravidla:

- je snadné provést dopřednou operaci – tedy šifrování,
- je však velmi obtížné tuto operaci invertovat (dešifrovat) bez znalosti informací, které k tomu potřebuji (veřejný klíč)[1].

Kryptografie implementuje princip jednocestné funkce použitím dvou odlišných klíčů, které jsou však ve vzájemné vazbě a jsou vytvořeny současně. Jeden klíč lze použít pouze k zašifrování, druhý pouze k dešifrování. Jejich matematický vztah je tedy založen na tom, že se požaduje veřejný klíč k invertování operace se soukromým klíčem. Znamená to, že jedna osoba, která má soukromý klíč, může provést operaci, kterou může každý, kdo vlastní veřejný klíč, invertovat[1]. Jedná se zjevně o způsob použití při digitálním podepisování. ZoEP používá pro pojem soukromý klíč pojem data

pro vytváření elektronického podpisu a pro pojem veřejný klíč pojem data pro ověřování elektronického podpisu.

Digitální podpis se používá tehdy, je-li zasílán šifrovaný nebo nešifrovaný (otevřený) text, a odesílatel chce zajistit:

- aby příjemci mohli ověřit, že zpráva přichází skutečně od odesilatele,
- aby příjemci mohli ověřit, zda text nebyl pozměněn poté, co jej odesílatel podepsal[1].

Samotná zpráva může, ale také nemusí být během přenosu zašifrována. V takovém případě je osvědčený postup podepsat zprávu před jejím šifrováním – odesílatel totiž ví, co podepisuje. V praxi elektronických podpisů se soukromým klíčem nešifruje celá zpráva[1]. Takový postup by vzhledem k rychlosti asymetrické kryptografie zabíral příliš mnoho času. Do procesu podepisování tak vstupuje další matematická operace, která ze zprávy vytvoří kratší otisk neboli haš, který je podepisován (šifrován).

5.2. Úvod do hašování

Haš vzniká pomocí funkce hašování (hashing), která ze zadaného velkého množství dat vrací mnohem menší objem dat, který však jednoznačně vypovídá o obsahu dokumentu[8]. Při změně jen jednoho bitu zprávy se musí hodnota haše změnit. Pro potřeby kryptografie musí být funkce hašování jednosměrná. Známe-li hodnotu haše (a máme-li rovněž původní dokument, ze kterého byl haš vypočítán), mělo by být velmi obtížné vytvořit jiný dokument se stejnou hašovací hodnotou. Silná hašovací funkce musí tedy vyhovovat následujícím požadavkům:

- musí být jednosměrná, tedy nesmí být možné z hodnoty haše odvodit původní zprávu,
- musí být nekolizní, nesmí být možné dostat na dvě různé výchozí zprávy tutéž hodnotu haše[8].

Poté, co je haš původní zprávy zašifrován, je odeslán příjemci. Ten jej pomocí veřejného klíče dešifruje a z původní zprávy (otevřeného textu), kterou mu odesílatel též pošle, vytvoří stejným způsobem nový haš[8]. Má tak k dispozici dva haše vytvořené z jedné zprávy. Podle výše uvedených požadavků na hašovací funkci by v případě neporušenosti zprávy byly oba haše identické. V takovém případě se příjemce může spolehnout na text zaslaného dokumentu.

5.3. Třetí důvěryhodná strana

V rozsáhlých sítích s velkým počtem uživatelů vzniká problém s budováním velkého počtu důvěryhodných kanálů mezi uživateli, pomocí kterých by se daly bezpečně přenášet veřejné klíče. Pokud by se budoval důvěryhodný kanál typu každý s každým, dosáhl by počet těchto kanálů obrovských hodnot. Počet důvěryhodných kanálů v síti s X uživateli je roven hodnotě K=X.(X-1)/2, což při stu koncových uživatelů dává hodnotu 4950. Optimální řešení je vytvořit statut certifikační autority[1]. Uživatelé budují důvěryhodné kanály pouze k této certifikační autoritě. (Počet kanálů je nyní pouze K=X-1, při stu uživatelů tedy 99 kanálů). Tato certifikační autorita pak může sloužit též jako ověřovatel totožnosti a zajišťovat jiné služby spojené s digitálním podpisem.

5.3.1. Funkce poskytovatele certifikačních služeb

Šifrování informací nabízí řadu nepopiratelných výhod, ale vyžaduje dodržování nových pravidel provozu, především zavedení režimu klíčové infrastruktury – PKI. Ani sebelepší šifrovací mechanismus totiž nepřinese požadovaný bezpečnostní efekt, nemá-li důvěryhodnou distribuci, uložení a ničení svých šifrovacích a dešifrovacích klíčů[3]. Zajistit jejich bezpečné uložení a ničení a zajistit jejich spolehlivou distribuci je komplikované. Pro bezpečnou distribuci klíčů mezi jednotlivými uživateli se nabízejí dvě základní řešení:

- distribuce klíčů zajištěná certifikační autoritou nebo
- vzájemná výměna klíčů mezi uživateli (jak jsme viděli, takovéto řešení však přináší mnoho problémů)[3].

Problém distribuce veřejných klíčů lze optimálně řešit prostřednictvím certifikátů. Certifikát je zpráva, schválená třetí důvěryhodnou stranou, která zahrnuje veřejný klíč uživatele a další atributy (jméno či pseudonym uživatele, identifikační číslo certifikátu, dobu platnosti certifikátu apod. viz. ZoEP). Třetí důvěryhodná strana je certifikační orgán, nebo lépe poskytovatel certifikačních služeb, kterému důvěřují všichni účastníci komunikace[2]. Povinnosti poskytovatele certifikačních služeb vyplývají ze zákona (viz. kapitola 3.1.).

5.3.2. Certifikát

Aby se mohla druhá strana spolehnout na certifikát, je nutno zabezpečit jeho integritu. Toho lze dosáhnout tím, že poskytovatel certifikačních služeb podepíše všechny jím vydané certifikáty svým vlastním soukromým klíčem. Certifikát je tedy

podepsaný dokument, který potvrzuje shodu veřejného klíče s dalšími, výše zmíněnými atributy[3].

Tvorba certifikátu probíhá v několika krocích:

1. Generování klíčů – žadatel vygeneruje pomocí hardwarového či softwarového prostředku oba klíče. Tento krok může za uživatele učinit i certifikační autorita.
2. Ověření a odsouhlasení informací – žadatel za své fyzické přítomnosti na místě registrační autority (součást infrastruktury poskytovatele) ověří souvislost obou klíčů (soukromého a veřejného), prokáže svou totožnost a uvede informace, které musí obsahovat certifikát. Součástí tohoto kroku je uzavření smlouvy a seznámení žadatele se všemi jeho právy a povinnostmi.
3. Vytvoření a odsouhlasení certifikátu – certifikační autorita vytvoří certifikát, podepíše jej svým soukromým klíčem a zveřejní jej na seznamu certifikátů. Je samozřejmé, že žadatel (resp. uživatel) obdrží kopii certifikátu[1].

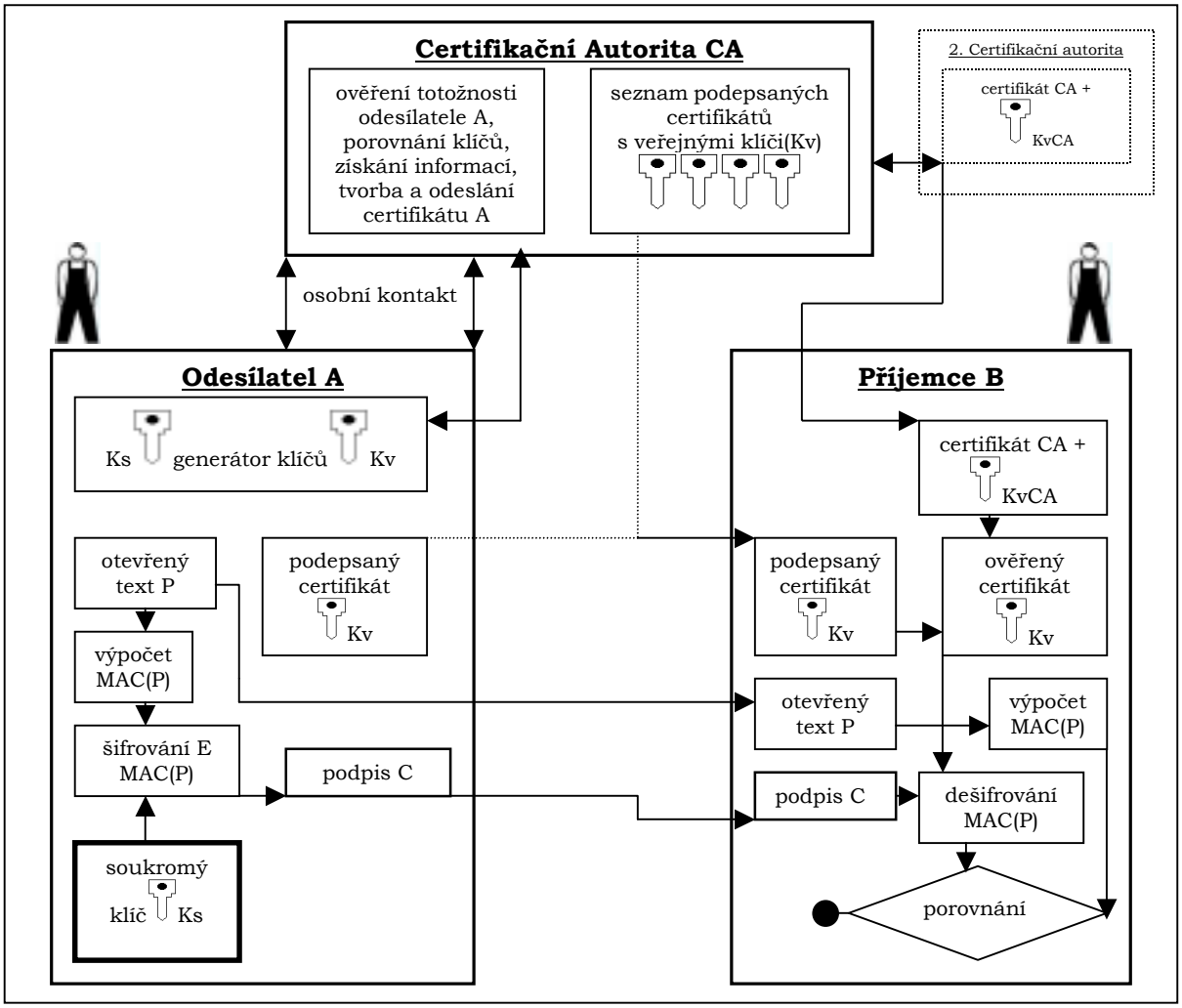
Certifikáty musí mít omezenou délku platnosti – životnosti. Omezená doba platnosti je velmi důležitá, protože pokroky při zvyšování výkonnosti výpočetní techniky a možnost, že se objeví v šifrovacích algoritmech mezery, mohou způsobit, že certifikáty přestanou být spolehlivé[17]. Je důležité je zrušit také tehdy, je-li zneužit soukromý klíč nebo např. tehdy, když uživatel – majitel klíče změní zaměstnání. Zrušený certifikát se ukládá do seznamu zneplatněných certifikátů. Toto opatření je nutné, aby se dalo prověřit, zda daný použitý certifikát je skutečně platný.

5.3.3. Elektronický podpis

Požívání elektronického podpisu probíhá též v několika krocích. Jejich zjednodušené schéma vypadá asi takto:

1. Vytvoření haše (MAC(P))– uživatel vytvoří z předmětného dokumentu otisk.
2. Podepsání haše – uživatel použije svůj soukromý klíč, který do té doby musí mít na nejvýše chráněném místě, k zašifrování otisku zprávy. Pokud to podmínky vyžadují, může uživatel zažádat časovou autoritu poskytovatele o zaslání časového razítka pro tento podpis (časová autorita je součástí infrastruktury poskytovatele).
3. Odeslání dat – uživatel posílá druhé komunikující straně otevřený dokument spolu se svým elektronickým podpisem. Součástí tohoto souboru dat může být i certifikát uživatele.
4. Příjem dat – druhá strana (příjemce) přebírá data. Při tomto kroku může příjemce znovu požádat časovou autoritu o zaslání časového razítka na příjem zprávy.

5. Ověření certifikátu – příjemce získá certifikát uživatele z přístupného místa poskytovatele a ověří shodu informací.
6. Dešifrování – pokud mají oba klíče souvislost, příjemce dokáže dešifrovat elektronický podpis uživatele.
7. Vytvoření a porovnání haše – dešifrováním podpisu získal příjemce haš uživatele. Z přijatého otevřeného dokumentu vytvoří svůj nový haš a oba tyto otisky porovná.
8. Potvrzení – pokud jsou oba haše identické, příjemce přijal platný dokument.



Obrázek č. 1

Na obrázku č. 1 jsou zjednodušeně znázorněny výše zmíněné postupy. Účastníci komunikace v našem případě nepoužívají utajení otevřeného textu pomocí šifrování. Do celého procesu vstupuje též druhá certifikační autorita, která poskytnutím certifikátu CA potvrdí její důvěryhodnost a tím i důvěryhodnost certifikátu, které CA vydává. Dle ZoEP je vyžadován i osobní kontakt při získávání údajů od žadatele a zjišťování jeho totožnosti.

5.4. Asymetrická kryptografie a hašování

K tomu, aby byl digitální resp. elektronický podpis universálně použitelný, je nutné, aby prostředky pro jeho tvorbu a ověřování pracovaly na stejných principech. Tyto prostředky musí být též dostatečně bezpečné a odolné vůči útokům. Tato snaha vedla ke stanovení základních požadavků na asymetrickou kryptografii a hašovací funkce, jež jsou (nebo mají být) zachyceny v právních dokumentech jednotlivých států. Vyhláška vyžaduje používání algoritmů RSA, DSA, či DSA založených na eliptických křivkách a při hašování mají být požívány funkce MD5, SHA-1, nebo RIPMED-160[24].

5.4.1. RSA

4. dubna 1977 oznámili L. Rivest, A. Shamir a L. Adleman z Massachusetts Institute of Technology objev prvního v praxi použitelného šifrovacího systému s veřejným klíčem. Ten byl posléze pojmenován podle počátečních písmen jejich příjmení – RSA. Algoritmus RSA je považován za jeden z nejlepších, jedinou jeho nevýhodou je značná časová náročnost[1]. Tu řeší digitální podpis používáním krátkého otisku zprávy.

RSA je založena na faktu, že je velice obtížné (pro velká čísla časově nemožné) rozložit čísla, kde každé je součinem dvou velkých prvočísel[6]. Nejprve tedy generujeme náhodně a nepredikovatelně dvě dostatečně velká prvočísla P a Q. Minimální délka těchto čísel, kterou vyžaduje Vyhláška, je 1024 bitů. To odpovídá dekadickému číslu o více než 100 cifrách[6]. Dále spočítáme číslo N=PQ a hodnotu Eulerovi funkce $\Phi=(P-1)(Q-1)$. Dále nalezneme číslo E takové, kde $1<E<\Phi$ a NSD(E, Φ)=1. V dalším kroku spočteme číslo D takové, že $1<D<\Phi$ a $ED=1 \bmod \Phi$. Veřejným klíčem je v našem případě (N,E) a soukromým klíčem je (N,D)[1].

Známe-li hodnoty obou klíčů, můžeme přistoupit k vlastnímu šifrování. Předpokládejme, že jsme předali druhé straně (příjemci) náš veřejný klíč (N,E). Svým soukromým klíčem zašifrujeme zprávu M podle vzorce $C=M^D \bmod N$. C je tedy samotný digitální podpis. Podpis C zašleme příjemci, který vlastní veřejný klíč (N,E). Ten provede $C^E \bmod N=M$. Získal tedy původní zprávu M[1].

5.4.2. DSA

Tento protokol umožňuje dvěma uživatelům vyměnit si tajný klíč pomocí veřejných medií. Neobsahuje žádnou metodu umožňující podpis zaslané zprávy, ani není možné provést autentizaci, že daný klíč skutečně pochází od daného uživatele[1].

Bezpečnost tohoto algoritmu závisí na obtížnosti řešení úlohy diskrétního logaritmu (obvykle je složitost této úlohy považována za ekvivalentní složitosti úlohy faktorizace). Jádrem jednoho z druhů DSA (Diffie-Hellman) je fakt, že pro velká čísla Z a prvočísla A a P (všechna například 200ciferná), je snadné vypočítat číslo X podle vztahu $X=A^Z$ mod P, je na to třeba pouze přibližně $2\log_2 Z$ násobení, zatímco na výpočet čísla Z (diskrétního logaritmu) ze známého čísla X potřebujeme přibližně odmocninu z P násobení (tedy přibližně 10^{100})[16]. Takový výpočet je opět časově velice náročný. Princip metody, která umožňuje rychle mocnit velká čísla, spočívá v rozkladu exponentu a postupném násobení a mocnění mezivýsledků. Například $X=Z^{49}=Z^{(32+16+1)}=(((((Z^2)^2)^2)^2)^2)^2)*((((Z^2)^2)^2)^2)*Z$. Tato výpočetní operace nyní vyžaduje pouze 11 násobení a nikoliv 48.

Výměna a tvorba klíčů probíhá v několika krocích.

1. Obě strany vygenerují sejná prvočísla A a P.
2. Strana A nalezne takové Z_A, kde $1 <= Z_A <= P-2$. Strana B nalezne takové Z_B, kde $1 <= Z_B <= P-2$.
3. Strana A vypočítá zprávu $X_A = A^{Z_A} \bmod P$. Strana B vypočítá zprávu $X_B = A^{Z_B} \bmod P$.
4. Obě stany si vymění zprávy X_A a X_B.
5. Strana A nalezne klíč $K=(A^{Z_B})^{Z_A} \bmod P$; a strana B nalezne stejný klíč $K=(A^{Z_A})^{Z_B} \bmod P$[16].

Ve Spojených státech byl Diffie-Hellmanův systém pro výměnu klíčů patentován (M. E. Hellman and R. C. Merkle: Public Key Cryptographic Apparatus and Method. US Patent 4,218,582, 1980), ale patent vypršel 29.dubna 1997[16].

5.4.3. Eliptické křivky

Matematická teorie hledá cesty, jak zlepšit vlastnosti systémů s veřejným klíčem. Jestliže v dosažené rychlosti šifrování se zatím žádné význačně změny nerýsují, je tomu jinak z hlediska velikosti použitých klíčů. V tomto směru význačná zlepšení přináší implementace (90 léta) systémů s veřejným klíčem na bázi tzv. eliptických křivek. V roce 1985 přišli nezávisle na sobě Neil Koblitz a Victor Miller k návrhu využívat pro kryptografické účely grupy založené na eliptických křivkách[16].

Primární výhodou kryptosystémů na bázi eliptických křivek je jejich velká kryptografická bezpečnost vzhledem k dané velikosti klíče[16]. Význačně kratší délka klíčů (např. oproti RSA) vede ke kratším certifikátům i menším parametrům systému a tedy i k větší výpočetní efektivnosti algoritmů. Druhá výhoda je v tom, že fakticky

všechna již známá použití v systémech na bázi diskrétního logaritmu (kryptografické protokoly, DSA apod.) lze převést do systémů na bázi eliptických křivek. Pro danou množinu parametrů eliptického kryptosystému je dvojice soukromý a veřejný klíč vytvářena následovně. Soukromý klíč S je celé číslo náhodně vygenerované v intervalu $0 << S < r$. Veřejný klíč je bod W na eliptické křivce spočtený jako $W = S*G$. Číslo r je řád bodu G, pro který musí platit $r>2^{160}$ a zároveň je dělitelem řádu eliptické křivky E. Bod G=(x,y) je definován kořeny eliptické rovnice E: $y^2 + xy = x^2 + ax^2 + b$. Pro použití obou klíčů mohou platit výše zmíněná pravidla použití klíčů RSA[16].

Při generování konkrétních eliptických křivek (pro kryptografické účely) je vhodné generovat parametry křivky náhodně. Pomocí tzv. seedu lze zabezpečit dokonce, že strana, která příslušnou křivku generovala, může později prokázat, že daná křivka skutečně náhodně vygenerována byla[16]. Touto cestou ujistí druhou stranu, že v systému nejsou žádná skrytá zadní vrátka, která umožňují první straně získání nějakých výhod (např. vypočtení soukromého klíče druhé strany). Tomu, aby eliptické křivky již dnes plně nahradily RSA a byly více než důstojným nástupcem starších kryptosystémů, již tedy nic nebrání a fakticky se tak již i děje. RSA stále ještě bude používána v řadě existujících systémů a zůstane tak ještě po nějakou dobu dominantním používaným kryptosystémem s veřejným klíčem. Pokud se však jedná o přípravu budoucích systémů, jsou přednosti eliptických kryptosystémů nesporné. Tabulka č. 1 ukazuje, při jakých délkách klíčů jsou bezpečnosti jednotlivých systémů na srovnatelné úrovni.

délka klíče	blokové šifry	RSA	Eliptické křivky
	56	417	105
	64	682	120
	80	1464	149
	86	1881	161
	109	4047	206

Tabulka č. 1

5.4.4. MD5

Hašovací funkce, které Vyhláška povoluje, vytvoří z velmi dlouhé zprávy M (soubor dat o délce až 2^{64} bitů) hašovací kód o délce 128, resp. 160 bitů. Kompresi uvedených hašovacích funkcí zajišťuje tzv. kompresní funkce (f). U zmíněných funkcí je zpráva M před vlastním hašováním doplněna a zarovnána na celistvý počet 512

bitových bloků M_i, i=1..n, a dále je definována inicializační hodnota IV (konstanta příslušné hašovací funkce). Proces hašování využívá kompresní funkci MD5 iterativně takto:

$$H_0=IV,$$
$$H_i=f(H_{i-1},M_i),\ i=1..n,$$
$$H(M)=H_n[9].$$

Autorem hašovacích funkcí MD (Message Digest) je R. Rivest, zakladatel RSA Data Security Inc. Jako první z řady MD vznikla MD2 (1989), která je bajtově orientovaná a od svých 32bitových následovníků se odlišuje i zjevnou pomalostí. V roce 1990 byla vytvořena hašovací funkce MD4. Funkce byla rychlejší, avšak byla kolizní. Na podzim roku 1995 tento fakt dokázal pracovník německé informační služby Hans Dobbertin. Verze MD5 byla vydána v roce 1991[9]. Funkce MD5 používá 128bitový kód a je zhruba o 33% pomalejší, než MD4[16]. V neprospěch této funkce přispívá i fakt, že Hans Dobbertin dokázal i v jejím případě nalézt kolizi (1996), a také je zde obecná námitka proti používání 128bitových kódů. V roce 1994 byl P. Oorschotem a M. Wienerem navržen stroj, který je schopen vygenerovat 2^{64} kódů a tudíž realizuje tzv. narozeninový paradox u 128bitového kódu. V praxi znamená narozeninový paradox možnost nalezení kolize u $2^{d/2}$ zpráv s pravděpodobností 50%. Z této skutečnosti vyplývá, že hašovací funkce používající 128bitové kódy jsou se současnou technologií prolomitelné. Vzhledem k těmto skutečnostem se sám autor R. Rivest rozhodl nedoporučit funkci MD5 pro používání v digitálních podpisech[9].

I přes tyto nedostatky, povoluje Vyhláška používání MD5 pro elektronický podpis. Děje se tak proto, že MD5 je široce rozšířena např. v bankovní sféře a její zákaz by znamenal značné komplikace. Její konkrétní popis je možné najít v RFC 1319-21[17].

5.4.5. SHA-1

SHA-1 byla vytvořena americkou tajnou službou NSA americkým úřadem pro normalizaci NIST byla vyhlášena 17. 4. 1995 jako standard v oficiálním dokumentu Federal Information Processing Standards Publication 180-1 (FIPS PUB 180-1)[8]. Je určena nejen pro potřeby algoritmu digitálního podpisu (DSA), ale i pro všechny aplikace ve státním sektoru, kde je požadována bezpečná hašovací funkce. SHA-1 tak nahradila svoji předchůdkyni SHA, definovanou v FIPS PUB 180 z 11. 5. 1993. Dokumenty jsou nazvány Secure Hash Standard (SHS), přičemž vlastní algoritmus se nazývá Secure Hash Algorithm (SHA). Rozdíl mezi definicí SHA-1 a SHA je nepatrný:

SHA-1 má v příkazovém řádku hlavní smyčky (viz dále) jednu jednobitovou rotaci navíc, ale rozdíl mezi jejich bezpečností je velký[8]. Funkce SHA-1je považována za bezpečnou, zatímco SHA nikoli.

SHA-1 byla navržena jako standardní hašovací funkce se vstupem od 0 až do 2^{64}-1 bitů a výstupem 160 bitů. Myšlenkově vychází z návrhu algoritmu MD4 od R. Rivesta (1990), ale velmi posiluje jeho vnitřní funkce, takže zatímco u MD4 již byly nalezeny kolize, SHA-1 je vůči nim považována za rezistentní. Důležitou úlohu zde hraje také délka kódu. Jestliže jsme uvedli, že současná technologie je schopná v dosažitelném čase najít kolizi hašovací funkce, jejíž kód má délku 128 bitů, pak stejná technologie by našla kolizi u 160bitového kódu až za 2^{16} násobek (princip narozeninového paradoxu) této doby. Podle známého Moorova zákonu bude možné najít kolizi u funkcí se 160bitovým kódem až za zhruba 24 let[8].

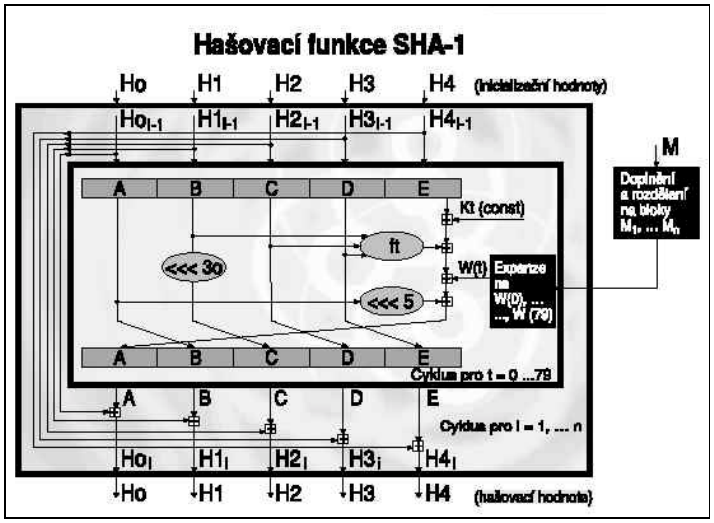
Algoritmus SHA-1sestává z několika hlavních kroků, které si v dalším odstavci popíšeme.

Nejprve dojde k doplnění zprávy M na délku, která je celočíselným násobkem 512 bitů. Výpočet hašovací hodnoty se provádí postupným zpracováním bloků M_1 až M_n:

1. Každé M_i rozdělíme na 16 slov W(0) až W(15).
2. Provedeme expanzi na slova W(16) až W(79).
3. Proměnné A až E nastavíme na konkrétní hodnoty konstant H_0 až H_4.
4. V následujících 80 rundách přimícháváme dle vzorce slova W do konstant A až E.
5. Aktualizujeme hodnoty H_0 až H_4 přičtením závěrečných hodnot A až E[8].

Po zpracování posledního bloku M_n je hašovací hodnota definována jako 160bitový řetězec tvořený slovy H_0 až H_4.

Na obrázku č. 2 je znázorněn zjednodušený postup hašování SHA-1.



Obrázek č. 2

5.4.6. RIPEMD-160

Funkce RIPEMD byla navržena v rámci projektu RACE Integrity Primitives Evaluation (RIPE) Komise Evropských společenství, který měl pomoci evropské standardizaci kryptografických funkcí. V rámci projektu (završen v polovině 90. let) byly hodnoceny a navrženy různé kryptografické nástroje. RIPEMD vychází z MD4, ale je bezpečnostně posílena[9]. Zajímavé je rozdělení kompresní funkce na dvě a kombinace jejich výsledků v závěru zpracování každého bloku. Kolize u ní nebyly nalezeny (jen v její zeslabené variantě), ale nevýhodou je 128bitový kód. Proto v roce 1996 H. Dobbertin a dva Belgičané A. Bosselaers a B. Preenel (již mimo projekt RIPE) navrhli RIPEMD-160 se 160bitovým hašovacím kódem[9]. Zesiluje původní RIPEMD a výsledkem je velice kvalitní návrh hašovací funkce (viz tabulka č. 2). Navrhli také variantu RIPEMD-128 se 128bitovým kódem jako náhražku RIPEMD tam, kde nelze použít kód 160bitový.

Pro ty, kdo vyžadují ještě vyšší bezpečnost, byly vytvořeny dokonce i RIPEMD-256 a RIPEMD-320. Vznikly vytvořením dvou paralelních linií zpracování dat pomocí kompresních funkcí RIPEMD-128 a RIPEMD-160, v nichž jsou navíc vzájemně kombinovány jejich vnitřní stavy[9].

RIPEMD-160 je nejvážnějším dnešním protikandidátem SHA-1 a byla začleněna do mezinárodního standardu ISO/IEC 10118-3, společně s RIPEMD-128 a SHA-1. RIPEMD-128, 160, 256 a 320 jsou zaregistrovány jako funkce společnosti TeleTrustT, ale patří do freewaru a mohou se bezplatně použít i pro komerční účely[17].

hašovací funkce	**MD2**	**MD4**	**MD5**	**RIPEMD**	**RIPEMD--128**	**RIPEMD--160**	**SHA-0**	**SHA-1**
hašovací kód	128 bitů	128 bitů	128 bitů	128 bitů	128 bitů	160 bitů	160 bitů	160 bitů
poznámka				2 paralelní linie	2 paralelní linie	2 paralelní linie		
bezpečnost	kolize kompresní funkce,1995, malá délka kódu	kolize celé MD4, 1995, malá délka kódu	kolize kompresní funkce, 1996, malá délka kódu	malá délka kódu	malá délka kódu	**bezpečná**	kolize kompresní funkce (ale vysoká složitost nalezení – 2^{61})	**bezpečná**
tvůrce a licenční politika	R. Rivest, RSA, licenční poplatek			TeleTrusT, freeware			vytvořila NSA, vydal NIST jako standard USA	
vznik	1989	1990	1991	1992 – 5	1996	1996	1993	1995
dokument	RFC 1319	RFC 1320	RFC 1321	link viz infotipy	link viz infotipy	link viz infotipy	NIST FIPS PUB 180	NIST FIPS PUB 180-1
orientační rychlost [Mb/s] v C (Pentium, 90 MHz)		81	60		36	19	21	21
orientační rychlost [Mb/s] v ASM (Pentium, 90 MHz)	4	191	136	96	78	45	55	55

Tabulka č. 2

5.5. Situace na českém trhu poskytovatelů certifikačních služeb

Na českém trhu poskytovatelů certifikačních služeb působí již řadu let několik firem. Mezi hlavní z nich patří PVT a.s., jejíž pobočka I.CA poskytuje komplexní služby PKI. V České republice dále působí jako certifikační autority firmy AEC s.r.o., KPNQuest, Autis s.r.o. a stejné služby poskytuje i Česká pošta.

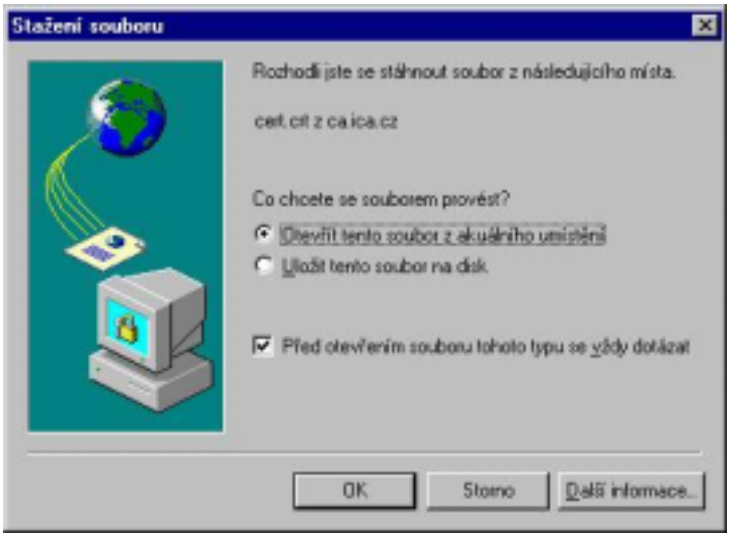
Ceny služeb jednotlivých poskytovatelů jsou v zásadě stejné a jejich technologie se též příliš neliší. Pokud ale vezmeme v úvahu podmínky kladené na poskytovatele certifikačních služeb poskytující kvalifikované certifikáty podle ZoEP, nejlépe jim vyhovuje I.CA[17]. Při realizaci digitálního podpisu používá kryptosystémů založených na různých funkcích, které podporuje systém uživatele a které odpovídají normám EU. I.CA poskytuje v oblasti elektronického podpisu dva okruhy služeb:

1. certifikáty pro fyzické osoby – vydávají se na dobu platnosti půl roku a jejich cena je 300,- Kč/ks,
2. certifikáty serverové – vydávají se na dobu platnosti půl roku a jejich cena je 1 000,- Kč/ks. Serverové certifikáty slouží k prokazování zabezpečení provozovaného serveru v síti Internet a potvrzují tak jeho důvěryhodnost. S tématikou této práce však serverové certifikáty příliš nesouvisí, proto se jimi nebudeme zabývat.

5.5.1. Příklad získání a užití elektronického podpisu

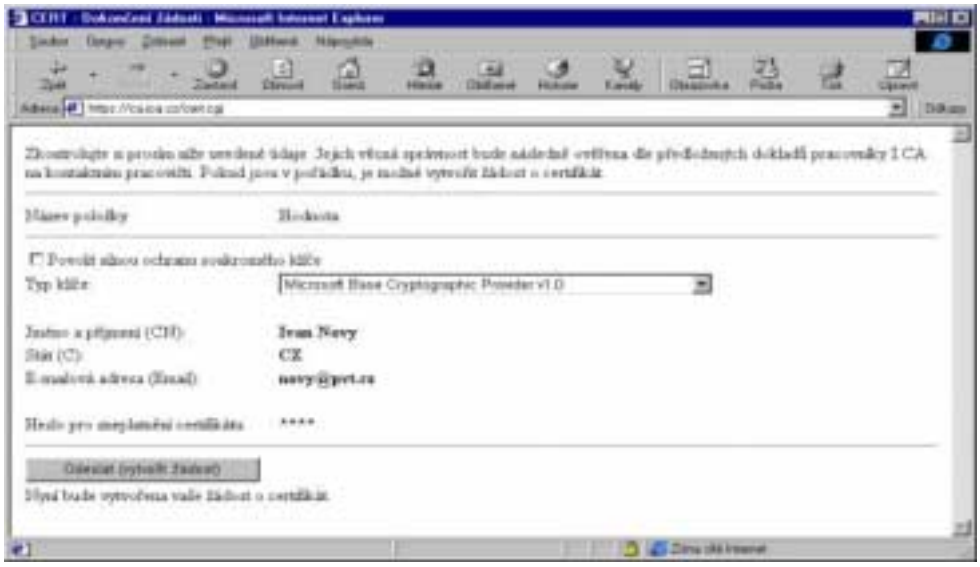
Získání a používání certifikátu od I.CA ve svém celku odpovídá požadavkům ZoEP a Vyhlášky a platí pro něj postup zmíněný v kapitole 5.3.2. Konkrétní kroky toho postupu si zde pro názornost předvedeme. Předpokládejme, že ke komunikaci, kterou budeme chtít opatřit elektronickým podpisem, budeme používat MS Outlook Express, který je v současnosti hojně rozšířený. MS Outlook Express používá jako SHA-1 se 512bitovým kódem a RSA s omezenou délkou klíče[17]. Tato délka je různá pro jednotlivé verze MS OE a bude při aplikaci zákona způsobovat řešitelné problémy (např. nadstavbovou instalací vyššího zabezpečení). Při použití jiného mailového klienta by se následující postup musel analogicky obměnit.

1. Z domovské webové adresy http://www.ica.cz/ica_cert.html je nejprve nutné nainstalovat certifikát certifikační autority, který je potřebný k zabezpečené komunikaci s certifikační autoritou (obrázek č. 3 a 4)[5].



Obrázek č. 3 a 4

2. Dalším krokem je vyplnění žádosti o osobní certifikát. Osobní certifikáty vydávané I.CA je možné získat na adrese:http://www.ica.cz/osobni_cert.html. Údaje v žádosti musí být pravdivé a budou součástí pozdější kontroly (obrázek č. 5)[5].



Obrázek č. 5

Po vyplnění tohoto formuláře je vaše žádost zaslána ke kontrole na I.CA. Pokud je žádost formálně v pořádku, je vytvořena konečná podoba elektronické žádosti (Obrázek č. 6), kterou je nutné si nahrát na disketu a navštívit s ní nebližší pracoviště registrační autority. Seznam pracovišť je uveden na http://www.ica.cz/.

Obrázek č. 6

3. Návštěva certifikační (registrační) autority, při které se provede kontrola všech údajů potřebných k právoplatnému provozu certifikátu. Po návštěvě registrační autority je zaslána e-mailovou zpráva "Osobní Certifikát" ve formátech "HTM", "TXT", "PEM" a "DER", dále "Certifikát Certifikační autority I.CA" a "CRL" (Seznam zneplatněných certifikátů) ve stejných formátech. Aktivací odkazu "HTM" osobního Certifikátu se otevře dokument obsahující mimo jiné i odkaz pro nainstalování tohoto osobního certifikátu do systému[5].
4. Než začneme odesílat podepsanou poštu, je nutné náš certifikát přidružit k poštovnímu účtu, se kterým je ho možné používat. To učiníme klepnutím na nabídku Nástroje a zvolením příkazu Účty. Vybereme účet, se kterým chceme používat digitální ID, klepneme na tlačítko Vlastnosti, a dále zvolíme Zabezpečení. Zaškrtneme políčko Použít digitální ID při odesílání zabezpečených zpráv, a potom klikneme na pole Digitální ID. Zvolíme digitální ID, které chceme přidružit k tomuto účtu (Obrázek č. 7)[5]. (Zobrazí se pouze ta digitální ID, která mají stejné elektronické adresy, jako je elektronická adresa účtu.)

Obrázek č.7

5. Součástí každého certifikátu je nenahraditelný soukromý klíč, který je uložen v počítači. Dojde-li k jeho ztrátě, nebude možné pomocí certifikátu nadále odesílat podepsanou poštu nebo číst zašifrované zprávy. Doporučuje se vytvořit si záložní kopii certifikátu pro případ, že dojde k poškození nebo ztrátě souboru, jež obsahuje zmíněný prostředek. Chceme-li vytvořit záložní kopii certifikátu, spustíme aplikaci Internet Explorer, klepneme na nabídku Zobrazit a pak zvolíme příkaz Možnosti sítě Internet. Klepneme na kartu Obsah a pak na tlačítko Osobní. Tlačítka Importovat a na této stránce vám umožňují spravovat certifikáty[5].

Pokud máme certifikát, můžeme odesílat zabezpečenou elektronickou poštu. Tato funkce aplikace Outlook Express zabezpečuje ochranu komunikace v síti Internet dvěma způsoby: pomocí digitálních podpisů a šifrování. Digitální podpisy, které zaručují příjemci zprávy, že jejím odesílatelem jsme skutečně my a že zpráva nebyla během přenosu poškozena, umožňují podepsání jakékoli elektronické pošty. Šifrování odesílané elektronické pošty zajišťuje, že obsah zprávy nemůže během přenosu přečíst žádný jiný uživatel než její příjemce.

Aplikace Outlook Express používá normu S/MIME a ostatní uživatelé mohou číst námi napsanou elektronickou poštu pomocí programů, které podporují tuto technologii[17]. My můžeme naopak číst zprávy dalších uživatelů, pokud byly

vytvořeny pomocí programů podporujících technologii S/MIME. Aplikace Outlook Express má vestavěnou zabezpečenou poštu a nabízí jednoduché uživatelské prostředí pro následující funkce:

- Odesílání podepsané pošty - Podepsaná elektronická pošta umožňuje příjemci zprávy ověřit naši identitu. Chceme-li digitálně podepsat zprávu elektronické pošty, klepneme na nabídku Nástroje a pak zvolíme příkaz Digitálně podepsat (nebo použijeme tlačítko na panelu nástrojů zprávy). Pokud chceme odesílat podepsanou poštu, je nutné mít vlastní certifikát(viz výše).
- Příjem podepsané pošty - Podepsaná elektronická pošta od jiných uživatelů umožňuje kontrolovat věrohodnost zprávy (např. zda zprávu skutečně odeslal uvedený odesílatel či zda nebyla poškozena během přenosu). Podepsané elektronické zprávy jsou označeny speciální ikonou. Problémy s přijatou podepsanou elektronickou poštou (popsané v bezpečnostních varováních aplikace Outlook Express) mohou znamenat, že zpráva byla poškozena nebo nepochází od uvedeného odesílatele.
- Odesílání zašifrované pošty - Šifrování elektronické pošty zabraňuje dalším uživatelům číst zprávy během přenosu. Pokud chceme šifrovat elektronickou poštu, je nezbytné mít k dispozici certifikát uživatele, kterému zprávu odesíláme. Tento certifikát musí být součástí údajů o příslušné osobě v Adresáři. Chceme-li odeslat zašifrovanou poštu, klepneme na nabídku Nástroje a pak zvolíme příkaz Šifrovat (nebo použijeme tlačítko na panelu nástrojů zprávy).
- Příjem zašifrované pošty - Obdržíme-li zašifrovanou poštovní zprávu, můžeme si být téměř jisti, že ji nečetl nikdo jiný. Aplikace Outlook Express provádí automatické dešifrování elektronických zpráv za předpokladu, že máme v počítači nainstalován správný certifikát.
- Odesílání certifikátu dalším uživatelům - Pokud chceme, aby nám ostatní uživatelé mohli posílat zašifrovanou poštu, musejí mít k dispozici náš certifikát. Pokud jej chceme poslat, jednoduše odešleme digitálně podepsanou poštu (viz výše) a aplikace Outlook Express automaticky zahrne váš certifikát.
- Získání certifikátů dalších uživatelů - Chceme-li ostatním uživatelům posílat zašifrovanou poštu, musíte mít k dispozici jejich certifikát. Aplikace Outlook Express je prvním poštovním programem, který umožňuje získávat certifikát prostřednictvím adresářových služeb. Pokud chceme najít certifikát, klepneme

na nabídku Úpravy a pak zvolíme příkaz Najít osoby. Vybereme adresářovou službu, ve které chceme hledat certifikát, v příslušném poli pro hledání uvedeme jméno nebo elektronickou adresu příjemce a pak klepneme na tlačítko Najít. Vybereme nalezené položky v okně výsledků hledání a klepneme na možnost Přidat do Adresáře. (Dalším způsobem, jak získat certifikát jiného uživatele, je příjem podepsané pošty od příslušné osoby. Chceme-li přidat certifikát z části podepsané pošty do Adresáře, klepneme na nabídku Soubor a zvolíme příkaz Vlastnosti. Klepneme na kartu Zabezpečení a pak na tlačítko Přidat digitální ID do Adresáře.)

- Změna statutu důvěryhodnosti digitálního ID - Přidáme-li do Adresáře certifikát dalšího uživatele, bude mu přidělen statut, který označuje, zda důvěřujeme jednotlivci, skupině či společnosti, jimž byl certifikát vydán. Pokud nás vlastník příslušného certifikát upozorní, že má podezření, že soukromý klíč certifikátu byl narušen, bude zřejmě nezbytné změnit jeho statut na Výslovně nedůvěřovat. Další informace nalezneme v rejstříku nápovědy aplikace Outlook Express pod heslem Statut důvěryhodnosti certifikátu.

5.6. Předběžné zhodnocení

Praxe elektronického podpisu není pro jeho uživatele nijak složitá. O to větší nároky jsou kladeny na poskytovatele certifikačních služeb. ZoEP spolu s Vyhláškou podmínky pro provozování certifikačních autorit ještě zpřísňují. Je tedy otázkou, který ze současných poskytovatelů se rozhodne vstoupit do mezí určených zákonem a poskytovat tomu adekvátní služby. Odborné odhady tvrdí, že technologie odpovídající zákonu mají hodnotu pohybující se v rozmezí 40 až 50 milionů Kč[17].

Je velice pravděpodobné, že prvním, kdo se pokusí o získání akreditace podle zákona, bude PVT a.s., která má ze všech českých poskytovatelů největší kapitál. Na uživatele elektronického podpisu však číhá také jeden problém. Většina současných klientů, kteří podporují digitální podepisování, neodpovídá požadavkům Vyhlášky na použití asymetrické kryptografie. Bude tedy nevyhnutelné upravit kryptosystémy dotyčných aplikací vhodnou nadstavbou. Na druhé straně musíme poznamenat, že současný stav používání elektronického podpisu v České republice je na vysoké úrovni. Jaká bude situace v době, kdy bude plně v provozu ZoEP, je otázkou.

6. Poznatky zjištěné při zkoumání, návrhy a doporučení

Zavádění elektronického podpisu do právního řádu je v celém západním světě věcí posledních let a měsíců. Zatímco některé členské státy Evropské unie mají tento proces již za sebou a existuje na jejich území již zaběhnutý systém poskytovatelů certifikačních služeb, samotná Evropská unie přistoupila k právnímu řešení elektronického podpisu teprve nedávno. Důvodů pro tento krok je několik. V rámci celé unie je třeba sjednotit úpravu používání elektronického podpisu a provozu certifikačních autorit tak, aby byly tyto služby přenositelné za hranice jednotlivých členských států, případně za hranice unie. Deklarovaným cílem je pak ochrana zákazníka. Dále je nutné donutit všechny členské státy, aby do svých právních řádů zapracovaly úpravu elektronického podpisu, která je nezbytnou součástí rozvoje elektronického obchodu. Pro státy jako je Německo či Rakousko znamená vydání Směrnice jisté komplikace. Zavedené systémy certifikačních autorit spolu s právní úpravou elektronického podpisu je v těchto případech nutné přehodnotit a uvést v soulad s dikcí Směrnice. Rakousko tyto kroky již podniklo a 1.1.2001 vstoupil v platnost nový rakouský zákon o elektronickém podpisu. Podobným tempem postupují legislativní práce i v Německu.

6.1. Směrnice Evropského parlamentu a rady 1999/93/ES

Směrnice EU je velice liberální. Poskytuje prostor pro působení celé škály certifikačních autorit, které vydávají certifikáty na různé úrovni zabezpečení. Po členských státech požaduje, aby podmínky pro udílení akreditací byly objektivní, průhledné, proporcionální a nediskriminační a musí se vztahovat pouze na specifické vlastnosti daného použití. Tyto požadavky nesmí vytvářet překážky při poskytování přeshraničních služeb občanům. Dalším a velice podstatným aspektem Směrnice je požadavek, aby členské státy zajistili zrovnoprávnění vlastnoručních a kvalifikovaných elektronický podpisů. Zároveň musí členské státy dbát, aby elektronickým podpisům nebyla odpírána právní účinnost 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 poskytovatelem nebo nejsou vytvořeny prostředkem pro bezpečné vytváření podpisu. Směrnice zároveň poskytuje dostatečnou svobodu pro individuální řešení dané problematiky jednotlivých států. Ač je Směrnice technicky nezávislá a velice kvalitně zpracovaná, stanovuje datum 19. července 2003 jako termín, do kterého by měla být

přezkoumána. Zároveň stanoví členským státům, aby uvedly v platnost právní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do 19. července 2001.

6.2. Právní úprava elektronického podpisu v České republice

Česká republika, ač není členským státem EU, je vázána dohodami o přidružení, ve kterých se zavazuje, že bude přibližovat svůj právní řád právu EU. Je tedy naprosto nezbytné, aby naše právní úprava elektronického podpisu byla v souladu se Směrnicí EU.

Při zpracovávání ZoEP se oddělily dvě skupiny odborníků, které zaujímaly dva odlišné pohledy na problém. Jednu skupinu odborníků vedl doc. Smejkal a druhá skupina se prezentovala na zasedání v Třešti v únoru 2000. Výsledkem jejich názorových sporů byl návrh zákona o elektronickém podpisu, který poslanec Mlynář 7.3.2000 předložil Hospodářskému výboru parlamentu. Po zapracování všech připomínek a požadavků politických kruhů byl zákon 29. června 2000 přijat.

ZoEP v řadě paragrafů naplňuje požadavky Směrnice EU. Problematickými pasážemi jsou § 10 odst. 6) a především § 11. Jsou totiž v rozporu s požadavky Směrnice na nediskriminační postup státu vůči poskytovatelům certifikačních služeb. K zařazení § 11 pravděpodobně vedla snaha zajistit podpisům v oblasti veřejné moci co největší důvěru – bezpečnost. V tom případě mohl být dokonce stanoven požadavek na použití kvalifikovaného podpisu (§ 3 odst. 2), který je chápán v EU jako ekvivalent vlastnoručního podpisu. K tomu, aby byl nějaký podpis kvalifikovaný (tedy splnil podmínky § 3 odst. 2), musí být mimo požadavku, že se jedná o zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem, který vydává kvalifikovaný certifikát (nemusí být tedy akreditovaný), navíc splněn požadavek, že podpis byl vytvořen pomocí bezpečného podpisového prostředku. Na druhou stranu v případě přísné dikce paragrafu 11 - … je možné používat pouze …- by to mohl být spíše další problém. Řešení by byla drahá a odrazovala by v používání tohoto způsobu komunikace. Mnohem výhodnější by bylo umožnit orgánům veřejné moci vyhlašovat bezpečnostní profily pro jednotlivé konkrétní agendy – tedy vyhlásit akceptovatelný způsob podpisu příjemcem (jak se o tom uvažuje v EU) – pro různé agendy. Např. při e-mail dotazu typu – zda má úřad otevřeno v pátek večer – se zdá splnění požadavků paragrafu 11 poněkud přehnaně úzkostlivé (podobně jako tento příklad samotný) a bránící elektronické komunikaci na místo její podpory.

Dalším možným řešením § 11 je vybudování poskytovatele certifikačních služeb z řad orgánů veřejné moci a po splnění podmínek vyhlášky a ZoEP zažádat o akreditaci na Úřadu. Tato cesta je ovšem velice nákladná; při splnění všech podmínek § 6 a § 10 se bude cena takového řešení pohybovat v desítkách milionů Kč. Navíc z § 10 odst. 6) plyne, že poskytuje-li někdo služby jako akreditovaný poskytovatel, nemůže provádět jako další činnost jiné něž taxativně vyjmenované služby – tedy např. svoji činnost jako orgán veřejné moci. Je zde sice možnost výjimky, ale není dále stanoveno, jak při udělení či neudělení má Úřad postupovat. Můžeme tedy pouze předpokládat, že teprve nařízení vlády, kterým se využití elektronického podpisu upravuje v oblasti veřejné moci, tyto problémy nějakým způsobem odstraní nebo alespoň uvede na pravou míru. Pokud by se tak nestalo, byla by totiž nasnadě novela zákona o elektronickém podpisu, která by tyto diskriminující požadavky upravila. Podobné hlasy se objevují i z řad Komise EU, která na březnovém zasedání v Paříži upozornila na nesrovnalosti v českém zákoně o elektronickém podpisu.

6.2.1. Východiska zákona o elektronickém podpisu

Z uvedeného vyplývá, že zákon o elektronickém podpisu vychází ve své úpravě z teze silných akreditovaných poskytovatelů certifikačních služeb, kteří poskytují úplnou škálu certifikačních služeb. Na trhu certifikátů je pak o tyto služby vysoký zájem a jednotlivé subjekty si volí z ucelené nabídky jim vyhovující produkt. Tato teze však není správná. Na tomto místě je třeba si uvědomit, že první zde byl elektronický podpis a až po něm poskytovatel certifikačních služeb. Potřeba bezpečné elektronické komunikace si ve svém vývoji vyžádala třetí důvěryhodnou stranu, která řešila tuto otázku a to na úrovni požadované konkrétními dvěma stranami. Její řešení bylo velice konkrétní a lokální. Poskytovatelé certifikačních služeb řešily nabídku až po vzniku poptávky. Tato skutečnost je tedy zrcadlově obrácená proti tezi zákonodárců. Naplněním jejich teze by vznikali poskytovatelé certifikačních služeb, jejichž technologie by měla hodnotu desítek milionů. Poptávka po elektronickém podpisu je však omezená, a tak ceny produktů těchto poskytovatelů by se pohybovaly v řádu tisíc. Uživatel by si jistě rozmyslel, zda bude daňové přiznání podávat e-mailem či zda dojde na úřad osobně.

Jak na tuto situaci zareagují stávající poskytovatelé certifikačních služeb a zda se někdo pokusí získat akreditaci podle zákona, je otázkou. V takovém případě bude muset poskytovatel přehodnotit své technologické prostředky podle znění Vyhlášky a uvést její požadavky v provoz. Jak jsme viděli, technologie současných českých

poskytovatelů jsou na vysoké úrovni, a tak tento technický aspekt nebude případnému žadateli činit větší potíže. Jinak tomu bude v případě plnění požadavků zákona o elektronickém podpisu.

7. Závěr

Se vstupem do 21.století je více než kdy jasné, že prosperující společnost musí zvládnout nejmodernější technologie, zapojit se do elektronického obchodu, zajistit bezpečnou a důvěrnou komunikaci mezi jednotlivými občany, zajistit ochranu osobních dat, zajistit vyřizování požadavků občanů na státní správu, zavést elektronické peníze a v neposlední řadě zajistit uznání elektronického podpisu, jako jednoho se základních kamenů elektronické společnosti. Lidé ve společnosti, která nezajistí tyto zcela zásadní úlohy, nemohou počítat s tím, že se zařadí mezi moderní, prosperující národy. Při vytváření prostředí legislativního, ekonomického, vědeckého je potřeba respektovat daný stav v Evropské unii. V případě základních zákonů a právních norem pak jsme přímo povinni slaďovat naše zákony se zákony platnými v EU. U nově přijímaných zákonů je tedy jedinou správnou cestou tyto zákony již přijímat ve tvaru, který je slučitelný se zákony v EU.

Zákon o elektronickém podpisu je naprosto nezbytným základem k budování moderní společnosti, v pravém slova smyslu nám může otevřít dveře do velkého obchodu 21. století. Po prostudování právních předpisů spojených s úpravou elektronického podpisu můžeme konstatovat, že jsme na dobré cestě k vytvoření podmínek pro rozvoj moderní ekonomiky elektronického charakteru. Zákon o elektronickém podpisu je sedmimílovým krokem na cestě ke zrovnoprávnění vlastnoručního a digitálního podpisu. Tento důsledek skýtá široké možnosti uplatnění nových technologií a jejich rozvoje. Běžným uživatelům dává možnost bezpečné komunikace na všech úrovních a to vše v čase nesrovnatelně rychlejším, než bylo zvykem. Právní úprava elektronického podpisu je zcela nutnou a bezpodmínečnou kapitolou vstupu České republiky do společnosti západních států.

Výše zmíněné přínosy a výhody vyžadují určitý kvalitativní obrat v přístupu k informačním technologiím. ZoEP ani Vyhláška nejsou schopny zaručit, že orgány veřejné moci budou v dostatečné míře schopny zvládnout požadavky kvalifikovaného elektronické podpisu. Ani řadoví uživatelé elektronického podpisu nebudou mít méně povinností při uchovávání soukromých klíčů, dodržování všech bezpečnostních postupů a zvládání krizových situací. A konečně nejvíce zatěžovanou skupinou budou samotní poskytovatelé certifikačních služeb. Nároky a požadavky na ně jsou nemalé a zároveň pokuty a tresty za porušení (i nedbalostní) jejich povinností jsou velice vysoké. Odpovědnost tedy leží na celé společnosti. Jakým způsobem se s novou elektronickou

realitou vypořádá a zda zavedení elektronického podpisu bude mít spíše pozitivní dopad na hospodářství než negativní dopad ve formě nových forem podvodů a tunelářství, to je otázka, na kterou je v současné době těžké hledat odpovědi.

Cesta nastoupená zákonem o elektronickém podpisu není ovšem cestou optimální. Řada ustanovení a požadavků na důvěryhodné třetí strany je spíše svazující než liberální. Zákon sice vychází ze Směrnice EU, ale v některých ustanovení se s ní přímo rozchází. Na oblast elektronické komunikace orgánů veřejné moci jsou kladeny příliš velké nároky, které jsou v rozporu s požadavky EU.

Na další úrovni stojí vyhláška Úřadu pro ochranu osobních údajů. V poslední době jsme v médiích různé kvality poslouchali rozhořčené kritiky postupu Úřadu při sestavování této vyhlášky. V souvislosti s těmito je nutné si uvědomit, že tvorba prováděcích předpisů k zákonu o elektronickém podpisu je nejen poměrně složitým legislativním problémem, ale především otázkou odborně technickou, kde výsledek z důvodu bezpečnosti a kompatibility nesmí být hnán kupředu snahou být první v Evropě, ale snahou spolu s ostatními dorazit do bezpečného cíle. Navzdory těmto tlakům se podařilo sestavit dokument, kterému je v této chvíli velmi málo co vytknout. Počátkem března 2001 byla Vyhláška přijata do meziresortního jednání vlády a dostala se tak do dalšího kola tahanic, kde proti sobě stojí zájmy různých kruhů. Je tedy otázkou, jaké úpravy se tento dokument dočká před svým schválením.

Spojení práva a informatiky je netriviální. Zákon o elektronickém podpisu, vyhláška Úřadu pro ochranu osobních údajů, direktiva EU a další předpisy týkající se elektronického podpisu řeší tuto velmi nelehkou úlohu spojení dvou odlišných vědních disciplín s různou úspěšností. Není však možné jednoznačně odsuzovat odlišné přístupy a řešení této problematiky už z toho důvodu, že aplikace různých odborných názorů do litery zákona je věcí individuálního postoje a z různých úhlů pohledu se tato realita vždy jeví odlišně. Hlavním cílem je tedy najít společný hlas a vůli k vytvoření takových dokumentů, jež by splňovaly požadavky společnosti a požadavky praxe užívání výpočetní techniky.

Hlavním pramenem a zdrojem informací této bakalářské práce byly právě takovéto dokumenty, v nichž se odrážely názory jednotlivých skupin odborníků, které se v určitých bodech odlišovaly. Při zpracovávání jsem se snažil postupovat pokud možno nestranně a hledat objektivní kvality a nedostatky současné situace elektronického podpisu v právní úpravě i v praxi. Jedná-li se o takto složitou mezioborovou disciplínu, je nalézání řešení zmíněných nedostatků též velice obtížný

problém. Při této práci jsem vycházel především z odborných konzultací a z elektronických zdrojů publikovaných na Internetu.

Práce na tomto dokumentu byla pro mne velkým přínosem a v průběhu jeho zpracovávání jsem si vytvořil řadu perspektivních odborných kontaktů a vztahů. Je tedy mým přáním se touto problematikou nadále zabývat a pokusit se v budoucnu o zlepšení elektronické komunikace na jakékoli úrovni. Stejně tak doufám, že i tato práce byla alespoň minimálním přínosem k pochopení a řešení problematiky elektronického podpisu.

Seznam použité literatury

1. DOBDA, Luboš. *Ochrana dat v informačních systémech.* 1. vyd. Praha: Grada Publishing, 1998. 288 s. ISBN 80-7169-479-7.

2. SMEJKAL, Vladimír. *Internet @ §§§.* Ilustroval Roman Klinský1. vyd. Praha: Grada Publishing, 1999.168 s. ISBN 80-7169-765-6.

3. HNÁČEK, Petr. *Certifikace veřejných klíčů a podpora legislativy. In Elektronický podpis.* Seminář ČAČK. 1. vyd. 2000. s. 43-62.

4. STAUDEK, Jan. *Úvod do technologie elektronického podpisu. In Elektronický podpis.* Seminář ČAČK. 1. vyd. 2000. s. 7-20.

5. MATYÁŠ, Vladimír. *Naučte se digitálně podepisovat. In Bezpečnost informačních systémů v bankovním sektoru.* Konference SI. 1. vyd. 1999 s. 58-60.

6. KODL, Jindřich. *E-podpis: podpisy v elektronickém prostředí komunikačních sítí. In Vesmír.* Listopad 2000, č. 79, s. 611-613.

7. STAUDEK, Jan. *Můžeme elektronicky podepisovat. In DSM.* Duben 2000, č. 4, s. 40-43.

8. KLÍMA, Vlastimil. *Hašovací funkce a kódy: výživná haše. In Chip.* Březen 1999, č. 3, s. 40-43.

9. KLÍMA, Vlastimil. *Hašovací funkce a kódy: jak se melou data. In Chip.* Duben 1999, č. 4, s. 44-46.

10. KLÍMA, Vlastimil. *Digitální podpis: až nás podepíše počítač…. In Chip.* Květen 1999, č. 5, s. 36-39.

11. KLÍMA, Vlastimil. *DSS: podpis bez pera i papíru. In Chip.* Květen 1999, č. 5, s. 40-42.

12. KLÍMA, Vlastimil. *Moderní kryptografické metody: bude nás podepisovat RSA?. In Chip.* Září 2000, č. 9, s. 50-52.

13. ROSA, Tomáš. *Schémata digitálního podpisu: podpis pro pokročilé. In Chip.* Listopad 2000, č. 11, s. 174-178.

14. ROSA, Tomáš. *Schémata digitálního podpisu: podpis pro pokročilé 2. In Chip.* Prosinec 2000, č. 12, s. 172-176.

15. ROSA, Tomáš. *Schémata digitálního podpisu: vybrané problémy podpisových schémat. In Chip.* Leden 2001, č. 1, s. 134-137.

16. PINKAVA, Jaroslav. *Přednáška I.-III. In Elektronický podpis-využití v bankovnictví.* [online]. Prosinec 2000, 1. vyd. [cit. 2000-12-20]. Dostupné z <http://www.mujweb.cz/veda/gcucmp/>.

17. VONDRUŠKA, Pavel. *Přednáška IV., VI., VII. In Elektronický podpis-využití v bankovnictví.* [online]. Prosinec 2000, 1. vyd. [cit. 2000-12-22]. Dostupné z <http://www.mujweb.cz/veda/gcucmp/>.

18. MATEJKA, Ján. *Krádež elektronického podpisu, aneb s čím tvůrci zákona (ne)počítali?* [online]. c2000, poslední revize 24.10.2000 [cit. 2001-01-10]. Dostupné z <http://www.root.cz/>.

19. SMEJKAL, Vladimír. *Elektronický podpis se blíží.* [online] c2000, poslední revize 10.10.2000 [cit. 2001-01-12]. Dostupné z <http://www.e-podpisy.cz>.

20. SMEJKAL, Vladimír. *Právní aspekty zákona č. 227/2000 Sb. o elektronickém podpisu (ZoEP).* [online] c2000, poslední revize 17.11.2000 [cit. 2001-01-22]. Dostupné z <http://www.e-podpisy.cz>.

21. SMEJKAL, Vladimír. *FAQ.* [online] c2000, poslední revize 10.11.2000 [cit. 2000-12-17]. Dostupné z <http://www.e-podpisy.cz>.

22. Úřad pro ochranu osobních údajů. *Odůvodnění.* [online] c2001, poslední revize březen 2001 [cit. 2001-03-10]. Dostupné z <http://www.uoou.cz>.

Seznam použitých právních předpisů

23. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů ze dne 29. června 2000.

24. Teze vyhlášky Úřadu pro ochranu osobních údajů, kterou se provádí § 6 a § 17 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů.

25. Směrnice Evropského parlamentu a rady 1999/93/ES, o zásadách Společenství pro elektronické podpisy ze dne 13. prosince 1999.

26. Zákon č. 40/1964 Sb., ve znění pozdějších předpisů. (Občanský zákoník).

Příloha č. 1

Slovník pojmů

Dešifrování (Dencryption) – proces opačný k šifrování (značeno D). Dešifrování vyjádříme formálním zápisem P=D(K,C).

Digitální podpis (Digital Signature) – šifrovaná data logicky spojená se zprávou, která umožňuje identifikaci odesílatele a ověření neporušenosti zprávy od chvíle podpisu.

Elektronický podpis (Electronical Signature) – širší pojetí digitálního podpisu. Kromě samotného digitálního podpisu zahrnuje další metody identifikace podepisující osoby, jakými jsou biometrické metody identifikace (struktura oční duhovky, otisk prstů, hlas apod.)

Kryptoanalýza (Cryptoanalysis) – věda o luštění šifer. Zabývá se hledáním způsobů, jak šifrovaný text neautorizovaně dešifrovat.

Kryptografický klíč, šifrovací klíč (Cryptographic Key) – směnný prvek šifrovacího algoritmu. Používá se k šifrování a dešifrování zprávy. Musí jej tedy znát odesílatel i příjemce. Kdo má přístup ke klíči, má přístup i k šifře. Proto se musí ochraně klíčů věnovat velká pozornost. Klíč je velmi zranitelným místem šifry (značeno K).

Kryptografie (Cryptography) – věda o tvorbě šifer. Využívá metody šifrování, aby ukryla citlivá data a informace před nepovoleným přístupem.

Kryptologie (Cryptology) – obecná věda o šifrování, o tvorbě a luštění šifer. Zahrnuje dvě odvětví – Kryptografii a Kryptoanalýzu.

Kryptosystém (Cryptosystem) – logický systém, který umožňuje šifrování a dešifrování dat.

Otevřený text (Plaintext) – originální tvar zprávy (značeno P).

Otevřený text (Plaintext) – originální tvar zprávy (značeno P).

Šifrování (Encryption) – proces, při němž konkrétní kryptografická metoda transformuje otevřený text pomocí kryptografického algoritmu a šifrovacího klíče do šifrovaného textu. Ten potom obecně vypadá jako náhodný shluk znaků. U transformace se provádí pro utajení obsahu zprávy (značeno E). Formální zápis šifrování je C=E(K,P).

Šifrovaný text, šifra (Ciphertext) – tvar zprávy po zašifrování (značeno C).

Příloha č. 2

ZÁKON

č. 227 ze dne 29. června 2000

o elektronickém podpisu a o změně některých dalších zákonů

(zákon o elektronickém podpisu)

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

ELEKTRONICKÝ PODPIS

§ 1

Účel zákona

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

§ 2

Vymezení některých pojmů

Pro účely tohoto zákona se rozumí

a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě,
b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky:
   1. je jednoznačně spojen s podepisující osobou,
   2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
   3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
   4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat;
c) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,
d) podepisující osobou fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby,

e) poskytovatelem certifikačních služeb subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,
f) akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,
g) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost,
h) kvalifikovaným certifikátem certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty,
i) daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,
j) daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,
k) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,
l) prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,
m) prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,
n) prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,
o) nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů,
p) akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

§ 3

Soulad s požadavky na podpis

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

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

§ 4

Soulad s originálem

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

§ 5

Povinnosti podepisující osoby

(1) Podepisující osoba je povinna

a) zacházet s prostředky jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
b) uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,
c) podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

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

§ 6

Povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty

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

a) zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti kvalifikovaných certifikátů stanovené tímto zákonem,
b) zajistit, aby údaje uvedené v kvalifikovaných certifikátech byly přesné, pravdivé a úplné,
c) před vydáním kvalifikovaného certifikátu bezpečně ověřit odpovídajícími prostředky totožnost osoby, které kvalifikovaný certifikát vydává, případně i její zvláštní znaky, vyžaduje-li to účel kvalifikovaného certifikátu,
d) zjistit, zda v okamžiku vydání kvalifikovaného certifikátu měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát,
e) zajistit, aby se každý mohl ujistit o identitě poskytovatele certifikačních služeb a jeho kvalifikovaném certifikátu,
f) zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat,
g) zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem,
h) zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát vydán nebo zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám,
i) přijímat do pracovního nebo obdobného poměru osoby, které mají odborné znalosti,

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

zkušenosti a kvalifikaci nezbytnou pro poskytované služby, a které jsou obeznámeny s příslušnými bezpečnostními postupy,

j) používat bezpečné systémy a nástroje elektronického podpisu a zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují; nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou; toto musí být ověřeno Úřadem pro ochranu osobních údajů (dále jen „Úřad“),

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

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

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

n) před uzavřením smluvního vztahu s osobou, která žádá o vydání kvalifikovaného certifikátu, informovat ji písemně o přesných podmínkách pro užívání kvalifikovaného certifikátu, včetně případných omezení pro jeho použití, a o podmínkách reklamací; je rovněž povinen tuto osobu informovat o tom, zda je či není akreditován Úřadem podle § 10; tyto informace lze předat elektronicky; podstatné části těchto informací musí být na vyžádání k dispozici třetím osobám, které se spoléhají na tento kvalifikovaný certifikát,

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

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

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

(4) Pokud byla poskytovateli certifikačních služeb, který vydává kvalifikované certifikáty, akreditace Úřadem odňata, je povinen informovat o této skutečnosti subjekty, kterým poskytuje své certifikační služby a uvést tuto skutečnost v seznamech vedených podle odstavce 1 písm. f) a g).

(5) Není-li poskytovatel certifikačních služeb akreditován Úřadem, je povinen ohlásit Úřadu nejméně 30 dnů před vydáním prvního kvalifikovaného certifikátu, že bude vydávat kvalifikované certifikáty.

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

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

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

(9) O veškeré činnosti poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, musí být vedena provozní dokumentace, která musí obsahovat tyto údaje:
a) smlouvu s podepisující osobou o vydání kvalifikovaného certifikátu,
b) vydaný kvalifikovaný certifikát,
c) kopie předložených osobních dokladů podepisující osoby,
d) potvrzení o převzetí kvalifikovaného certifikátu podepisující osobou,
e) přesné časové určení doby platnosti vydaného kvalifikovaného certifikátu.

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

§ 7

Odpovědnost za škodu

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

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

§ 8

Ochrana osobních údajů

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

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

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

§ 9

Akreditace a dozor

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

(2) Úřad
a) uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb subjektům působícím na území České republiky,
b) vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona,
c) vede evidenci udělených akreditací a jejich změn a evidenci poskytovatelů certifikačních služeb, kteří Úřadu oznámili, že vydávají kvalifikované certifikáty,
d) pravidelně uveřejňuje přehled udělených akreditací a přehled poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, a to i způsobem umožňujícím dálkový přístup,
e) vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou,
f) plní další povinnosti stanovené tímto zákonem (například § 10 odst. 7, § 13 odst. 2 a § 16 odst. 2).

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

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

§ 10

Podmínky udělení akreditace pro poskytování certifikačních služeb

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

(2) V žádosti o akreditaci podle odstavce 1 musí žadatel doložit
a) obchodní jméno, sídlo a identifikační číslo žadatele,
b) doklad o oprávnění k podnikatelské činnosti a u osoby zapsané do obchodního rejstříku také výpis z obchodního rejstříku ne starší než 3 měsíce,
c) výpis z rejstříku trestů podnikatele – fyzické osoby nebo statutárních představitelů právnické osoby v případě, že žadatelem je právnická osoba, ne starší než 3 měsíce,

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

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

d) věcné, personální a organizační předpoklady pro činnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty podle § 6 tohoto zákona,
e) údaj o tom, zda žadatel již vydává nebo hodlá vydávat kvalifikované certifikáty,
f) doklad o zaplacení správního poplatku.

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

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

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

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

(7) Součástí rozhodnutí Úřadu o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem.

§ 11

V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty, vydávané akreditovanými poskytovateli certifikačních služeb.

§ 12

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat
a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,
b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,
c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,
d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává,
g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

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

h) počátek a konec platnosti kvalifikovaného certifikátu,
i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,
j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

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

§ 13

Povinnosti akreditovaného poskytovatele certifikačních služeb při ukončení činnosti

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

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

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

§ 14

Opatření k nápravě

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

(2) V případě, že se akreditovaný poskytovatel certifikačních služeb dopustí závažnějšího porušení povinností stanovených tímto zákonem nebo ve stanovené lhůtě neodstraní nedostatky zjištěné Úřadem, je Úřad oprávněn mu udělenou akreditaci odejmout.

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

§ 15

Zrušení kvalifikovaného certifikátu

(1) Úřad může nařídit poskytovateli certifikačních služeb jako předběžné opatření[7]) zneplatnění kvalifikovaného certifikátu podepisující osoby, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán nebo pokud byl vydán na základě nepravdivých údajů. Nařízení o zneplatnění kvalifikovaného certifikátu může být vydáno také v případě, kdy bylo zjištěno, že podepisující osoba používá prostředek pro vytváření podpisu, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo změnu podepisovaných údajů.

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

§ 16

Uznávání zahraničních certifikátů

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

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

§ 17

Prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů

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

a) data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno,
b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie,
c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti

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

zneužití třetí osobou.

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

(3) Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby
a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,
b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,
c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,
d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,
e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,
f) bylo jasně uvedeno použití pseudonymu,
g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§ 18

Pokuty

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

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

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

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

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

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

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

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

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

§ 19

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

§ 20

Zmocňovací ustanovení

Úřad se zmocňuje vydávat vyhlášky k upřesňování podmínek stanovených v § 6 a 17 a způsobu, jakým se jejich splnění bude dokládat, a k upřesnění požadavků, které musí splňovat nástroje elektronického podpisu, a k náležitostem postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.

ČÁST DRUHÁ
Změna občanského zákoníku

§ 21

Zákon č. 40/1964 Sb., občanský zákoník, ve znění zákona č. 58/1969 Sb., zákona č. 131/1982 Sb., zákona č. 94/1988 Sb., zákona č. 188/1988 Sb., zákona č. 87/1990 Sb., zákona č. 105/1990 Sb., zákona č. 116/1990 Sb., zákona č. 87/1991 Sb., zákona č. 509/1991 Sb., zákona č. 264/1992 Sb., zákona č. 267/1994 Sb., zákona č. 104/1995 Sb., zákona č. 118/1995 Sb., zákona č. 89/1996 Sb., zákona č. 94/1996 Sb., zákona č. 227/1997 Sb., zákona č. 91/1998 Sb., zákona č. 165/1998 Sb., zákona č. 159/1999 Sb., zákona č. 363/1999 Sb., zákona č. 27/2000 Sb. a zákona č. 103/2000 Sb., se mění takto:

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

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

§ 22

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

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

V § 21 odstavce 2 a 3 znějí:

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

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

ČÁST ČTVRTÁ

Změna správního řádu

§ 23

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

V § 19 odstavec 1 zní:

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

ČÁST PÁTÁ

Změna občanského soudního řádu

§ 24

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

V § 42 odstavec 1 zní:

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

ČÁST ŠESTÁ

Změna trestního řádu

§ 25

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění zákona č. 57/1965 Sb., zákona č. 58/1969 Sb., zákona č. 149/1969 Sb., zákona č. 48/1973 Sb., zákona č. 29/1978 Sb., zákona č. 43/1980 Sb., zákona č. 159/1989 Sb., zákona č. 178/1990 Sb., zákona č. 303/1990 Sb., zákona č. 558/1991 Sb., zákona č. 25/1993 Sb., zákona č. 115/1993 Sb., zákona č. 292/1993 Sb., zákona č. 154/1994 Sb., nálezu Ústavního soudu č. 214/1994 Sb., nálezu Ústavního soudu č. 8/1995 Sb., zákona č. 152/1995 Sb., zákona č. 150/1997 Sb., zákona č. 209/1997 Sb., zákona č. 148/1998 Sb., zákona č. 166/1998 Sb., zákona č. 191/1999 Sb., zákona č. 29/2000 Sb. a zákona č. 30/2000 Sb., se mění takto:

V § 59 odstavec 1 zní:

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

ČÁST SEDMÁ

Změna zákona o ochraně osobních údajů

§ 26

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

V § 29 se doplňuje odstavec 4, který zní:

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

ČÁST OSMÁ

Změna zákona o správních poplatcích

§ 27

Zákon č. 368/1992 Sb., o správních poplatcích, ve znění zákona č. 10/1993 Sb., zákona č. 72/1994 Sb., zákona č. 85/1994 Sb., zákona č. 273/1994 Sb., zákona č. 36/1995 Sb., zákona č. 118/1995 Sb., zákona č. 160/1995 Sb., zákona č. 301/1995 Sb.,

zákona č. 151/1997 Sb., zákona č. 305/1997 Sb., zákona č. 149/1998 Sb., zákona č. 157/1998 Sb., zákona č. 167/1998 Sb., zákona č. 63/1999 Sb., zákona č. 166/1999 Sb., zákona č. 167/1999 Sb., zákona č. 223/1999 Sb., zákona č. 326/1999 Sb., zákona č. 352/1999 Sb., zákona č. 357/1999 Sb., zákona č. 360/1999 Sb., zákona č. 363/1999 Sb., zákona č. 46/2000 Sb., zákona č. 62/2000 Sb., zákona č. 117/2000 Sb., zákona č. 133/2000 Sb. a zákona č. 151/2000 Sb., se mění takto:

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

„ČÁST XII
Řízení podle zákona o elektronickém podpisu

Položka 162
a) podání žádosti o akreditaci poskytovatele certifikačních služeb Kč 100 000,-
b) podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky Kč 10 000,-.“.

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

„ČÁST XII

Řízení podle zákona o elektronickém podpisu 162.“.

3. Tečka za částí XI se vypouští.

ČÁST DEVÁTÁ
ÚČINNOST

§ 28

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

Klaus v.r.

Havel v.r.

Zeman v.r.

Příloha č. 3

Vyhláška

Úřadu pro ochranu osobních údajů

ze dne …….. 2001

o povinnostech poskytovatelů vydávajících kvalifikované certifikáty a o požadavcích, které musí splňovat nástroje elektronického podpisu

Úřad pro ochranu osobních údajů stanoví podle § 20 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu):

ČÁST PRVNÍ

OBECNÁ USTANOVENÍ

§ 1

Předmět úpravy

Tato vyhláška se vztahuje na poskytovatele certifikačních služeb vydávající kvalifikované certifikáty a stanoví požadavky, které musí splňovat nástroje elektronického podpisu.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí:

a. žadatelem osoba, která požádala poskytovatele certifikačních služeb o vydání kvalifikovaného certifikátu,
b. žadatelem o akreditaci žadatel o udělení akreditace k působení jako akreditovaný poskytovatel certifikačních služeb,
c. držitelem fyzická osoba, která má data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu, a které poskytovatel vydal kvalifikovaný certifikát k datům pro ověřování elektronického podpisu,
d. osobou spoléhající na certifikát osoba, která opírá své jednání o důvěru v kvalifikovaný certifikát a zaručený elektronický podpis ověřený s použitím tohoto kvalifikovaného certifikátu,

e. poskytovatelem poskytovatel certifikačních služeb vydávající kvalifikované certifikáty,
f. smluvním partnerem osoba, která na základě smlouvy zajišťuje poskytovateli certifikační služby nebo jejich části,
g. registrací úkony, které provádí poskytovatel a při nichž zaznamenává požadavek žadatele na vydání kvalifikovaného certifikátu, zaznamenává a ověřuje údaje, které jsou požadovány pro vydání kvalifikovaného certifikátu, a pořizuje a ukládá kopie dokumentů, které žadatel předložil,
h. kvalifikovaným elektronickým podpisem zaručený elektronický podpis, který je založen na kvalifikovaném certifikátu a který byl vytvořen pomocí prostředku pro bezpečné vytváření podpisu,
i. párovými daty data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu,
j. párovými daty poskytovatele data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu, která poskytovatel používá pouze pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny,
k. informačním systémem pro certifikační služby informační systém, který poskytovatel používá pro zajištění certifikačních služeb,
l. správou kvalifikovaných certifikátů soubor činností, které poskytovatel v souvislosti s kvalifikovanými certifikáty vykonává.

ČÁST DRUHÁ

POŽADAVKY NA SPRÁVU KVALIFIKOVANÝCH CERTIFIKÁTŮ

§ 3

Vytváření kvalifikovaného certifikátu

Poskytovatel je povinen zajistit, že každému jím vydanému kvalifikovanému certifikátu je přiděleno unikátní číslo a uplatnit veškerá účelná opatření, která minimalizují možnost neoprávněné manipulace při přidělování těchto čísel.

§ 4

Zneplatnění kvalifikovaného certifikátu

(1) Poskytovatel je povinen zajistit zneplatnění kvalifikovaného certifikátu a vydávání a zveřejňování seznamu kvalifikovaných certifikátů, které byly zneplatněny, ve lhůtách, za podmínek a při dodržení postupů stanovených v Certifikační politice a Certifikační prováděcí směrnici.

(2) Poskytovatel je povinen vynaložit nejvyšší možné úsilí a uskutečnit veškerá opatření, aby doba mezi přijetím požadavku na zneplatnění kvalifikovaného certifikátu, který byl uplatněn v souladu s Certifikační politikou a Certifikační prováděcí směrnicí, a uvedením v seznamu kvalifikovaných certifikátů, které byly zneplatněny, a

zveřejněním tohoto seznamu byla co nejkratší. Tato doba by neměla činit více jak 24 hodin.

(3) Poskytovatel je povinen zajistit, že držitel, jehož kvalifikovaný certifikát byl zneplatněn, je bez zbytečného prodlení o této skutečnosti informován. Součástí této informace je uvedení času, kdy ke zneplatnění došlo. Postup při předávání této informace je poskytovatel povinen uvést v Certifikační politice.

(4) Poskytovatel je povinen zajistit, že při vydávání seznamů kvalifikovaných certifikátů, které byly zneplatněny::

a. nový seznam kvalifikovaných certifikátů, které byly zneplatněny, je zveřejněn alespoň jedenkrát denně,
b. seznam kvalifikovaných certifikátů, které byly zneplatněny, je veřejně přístupný do doby vydání nového seznamu,
c. seznam kvalifikovaných certifikátů, které byly zneplatněny, je podepsán kvalifikovaným elektronickým podpisem poskytovatele,
d. seznam kvalifikovaných certifikátů, které byly zneplatněny, obsahuje seznam všech kvalifikovaných certifikátů, které byly zneplatněny a u kterých dosud neuplynula doba jejich platnosti.

(5) Poskytovatel je povinen umožnit nepřetržitý příjem požadavků na zneplatnění kvalifikovaného certifikátu, zaslaných v elektronické formě. Poskytovatel je povinen zajistit nepřetržitou dostupnost informací o zneplatněných kvalifikovaných certifikátech způsobem umožňujícím dálkový přístup.

(6) Způsob, jakým poskytovatel postupuje při zajištění požadavků uvedených v odst. 5, je povinen stanovit v Certifikační politice.

(7) V případě selhání informačního systému pro certifikační služby, nebo faktoru, který není pod kontrolou poskytovatele, je poskytovatel povinen vynaložit veškeré možné úsilí k tomu, aby nedostupnost certifikačních služeb nepřekročila dobu stanovenou Certifikační prováděcí směrnicí a postupovat podle Plánu pro zvládání krizových situací a Plánu obnovy.

§ 5

Kvalifikovaný certifikát poskytovatele

(1) Poskytovatel je povinen zajistit, že pro podepisování kvalifikovaných certifikátů, které vydává, a seznamů kvalifikovaných certifikátů, které byly zneplatněny, jsou používána data pro vytváření elektronického podpisu určená výhradě pro tyto účely. K těmto datům pro vytváření elektronického podpisu musí být vydán kvalifikovaný certifikát.

(2) Poskytovatel je povinen stanovit v Certifikační prováděcí směrnici dobu platnosti svých kvalifikovaných certifikátů.

(3) Při zveřejňování svých kvalifikovaných certifikátů osobám spoléhajícím na certifikát je poskytovatel povinen zajistit, že jsou dostupné nejméně dvěma na sobě nezávislými způsoby.

ČÁST TŘETÍ

DOKUMENTACE

§ 6

Předpisová základna

(1) Poskytovatel je povinen zpracovat a v písemné podobě uchovat následující dokumenty:

a. Certifikační politiku,
b. Certifikační prováděcí směrnici,
c. Celkovou bezpečnostní politiku,
d. Systémovou bezpečnostní politiku,
e. Plán pro zvládání krizových situací a Plán obnovy.

(2) Poskytovatel je odpovědný za soulad výkonu certifikačních služeb se všemi dokumenty Předpisové základny, a to i v případech, kdy některé části certifikačních služeb zajišťuje prostřednictvím smluvních partnerů.

(3) Všechny dokumenty Předpisové základny musí být schváleny statutárním orgánem poskytovatele.

(4) Jakákoliv změna obsahu dokumentů Předpisové základny uvedených v odst. 1 písm. a) – e) podléhá schválení statutárním orgánem poskytovatele. Před tímto schválením nelze provádět jakékoliv změny v činnostech, které dokumenty popisují. Pro schvalování změn v Plánu pro zvládání krizových situací a Plánu obnovy je statutární orgán poskytovatele oprávněn stanovit jiný postup, který zajistí, že změny v těchto dokumentech jsou prováděny operativně a v souladu s požadavky na informační bezpečnost a zajištění kontinuity poskytovaných služeb. Všechny verze dokumentů Předpisové základny musí být uchovány nejméně po dobu 10 let.

(5) Statutární orgán poskytovatele je povinen stanovit v Certifikační politice proces revize a aktualizace dokumentů Předpisové základny. Procesu revize a aktualizace musí být dokumenty Předpisové základny podrobeny alespoň jednou ročně.

(6) Poskytovatel je povinen zajistit trvalé zveřejnění platné Certifikační politiky a platné Celkové bezpečnostní politiky v plném znění. Jiné dokumenty Předpisové základny poskytovatel v plném znění nezveřejňuje, je však povinen umožnit subjektům, jejichž činnost je těmito dokumenty upravena, seznámit se s nimi v nezbytném rozsahu.

(7) Poskytovatel je povinen umožnit subjektům, jejichž činnost je dokumenty Předpisové základny upravena, seznámit se s těmi změnami v Předpisové základně,

které se jejich činnosti týkají, a to dříve, než poskytovatel tyto změny uplatní. Poskytovatel je povinen v Certifikační politice stanovit minimální počet kalendářních dnů mezi zveřejněním těchto změn v dokumentech Předpisové základny a jejich uplatněním.

(8) Poskytovatel je povinen v rozsahu odpovídajícím vykonávané činnosti seznámit smluvní partnery s platným zněním Certifikační politiky a Certifikační prováděcí směrnice.

§ 7

Certifikační politika

(1) Všechny aspekty, které se vztahují na poskytovatele, žadatele, držitele, osoby spoléhající na certifikát a na smluvní partnery a které souvisejí s vydáváním kvalifikovaných certifikátů, jejich další správou, použitím, akceptací a všechny aspekty související s nakládáním s párovými daty je poskytovatel povinen zpracovat do dokumentu Certifikační politika. Tento požadavek se považuje za splněný, pokud je při zpracování Certifikační politiky postupováno v souladu s dokumentem RFC 2527 Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (dále jen "internetový standard certifikace").

(2) Certifikační politika musí obsahovat popis vlastností, které musí splňovat párová data, která si vytváří žadatel a k nimž má být vydán kvalifikovaný certifikát. Kryptografické algoritmy a jejich parametry, které musí být pro párová data použity, jsou uvedeny v příloze č.1 této vyhlášky.

§ 8

Certifikační prováděcí směrnice

(1) Všechny aspekty související s postupy při vydávání a následné správě kvalifikovaných certifikátů je poskytovatel povinen zpracovat do dokumentu Certifikační prováděcí směrnice. Tento požadavek se považuje za splněný, pokud je při zpracování Certifikační prováděcí směrnice postupováno v souladu s internetovým standardem certifikace.

(2) Poskytovatel je povinen v Certifikační prováděcí směrnici definovat činnosti, na které jsou z hlediska bezpečnosti certifikačních služeb a jejich náležitého fungování kladeny zvýšené nároky a popsat, jakým způsobem jsou vykonávány. Jedná se zejména o takové činnosti, u kterých selhání osoby při jejich výkonu má vliv na informační bezpečnost.

(3) Poskytovatel je povinen zajistit ve smyslu § 21 provedení auditu své Certifikační prováděcí směrnice. Auditem se ověřuje, zda Certifikační prováděcí směrnice splňuje požadavky uvedené v zákoně č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (dále jen "zákon") a zda při jejím zpracování bylo postupováno v souladu s internetovým standardem certifikace. Tento audit se provádí před zahájením vydávání kvalifikovaných certifikátů, dále podle plánu poskytovatele,

nejméně však jednou ročně. Audit se rovněž provádí vždy, když dojde k podstatným změnám Certifikační prováděcí směrnice.

§ 9

Celková bezpečnostní politika

(1) Celková bezpečnostní politika stanoví cíle a způsob zajištění celkové bezpečnosti organizace poskytovatele. Poskytovatel je povinen Celkovou bezpečnostní politiku zpracovat v souladu s požadavky uvedenými v ČSN/ISO/IEC TR 13335 nebo ISO 17799.

(2) Poskytovatel je povinen zajistit ve smyslu § 21 provedení auditu své Celkové bezpečnostní politiky, a tím ověřit, zda splňuje požadavky uvedené v zákoně a v ČSN/ISO/IEC TR 13335 nebo ISO 17799. Tento audit se provádí před zahájením vydávání kvalifikovaných certifikátů, dále podle plánu poskytovatele, nejméně však jednou ročně. Audit se rovněž provádí vždy, když dojde k podstatným změnám Celkové bezpečnostní politiky.

§ 10

Systémová bezpečnostní politika

(1) Poskytovatel je povinen zpracovat Systémovou bezpečnostní politiku v souladu s požadavky uvedenými v ČSN/ISO/IEC TR 13335 nebo ISO 17779. Systémová bezpečnostní politika upravuje zejména:

a. způsob implementace Celkové bezpečnostní politiky ve vztahu k informačnímu systému pro certifikační služby,
b. popis, jak je oddělen informační systém pro certifikační služby od jiných informačních systémů poskytovatele,
c. způsob ochrany dat a jiných prvků informačního systému pro certifikační služby,
d. jak čelit konkrétním hrozbám zjištěným analýzou rizik,
e. konkrétní bezpečnostní opatření,
f. způsob nakládání s informacemi zařazenými do jednotlivých stupňů klasifikace, uvedené v Celkové bezpečnostní politice.

(2) Poskytovatel je povinen zajistit ve smyslu § 21 provedení auditu své Systémové bezpečnostní politiky, jímž se ověřuje, zda splňuje požadavky uvedené v zákoně a v ČSN/ISO/IEC TR 13335 nebo ISO 17779. Tento audit se provádí před zahájením vydávání kvalifikovaných certifikátů, dále podle plánu poskytovatele, nejméně však jednou ročně. Audit se rovněž provádí vždy, když dojde k podstatným změnám Systémové bezpečnostní politiky.

§ 11

Plán pro zvládání krizových situací a Plán obnovy

Plán pro zvládání krizových situací a Plán obnovy stanoví postupy, které jsou uplatněny v případě bezpečnostního incidentu a postupy vedoucí k nápravě.

§12

Dokládání věcných, personálních a organizačních předpokladů poskytovatelů

Splnění věcných, personálních a organizačních předpokladů se dokládá následujícími dokumenty:

a. dokumenty, které tvoří předpisovou základnu podle § 6 odst. 1,
b. výsledky provedených auditů podle § 8 odst. 3, § 9 odst. 2, § 10 odst. 2 a § 18 odst. 2,
c. seznamem jmen osob, které pro poskytovatele vykonávají činnosti uvedené v § 8 odst. 2 s uvedením jejich kvalifikace a délky praxe.

§ 13

Záznamy událostí

(1) Poskytovatel je povinen zajistit zaznamenávání informací a událostí vztahujících se k vydání a další správě všech vydaných kvalifikovaných certifikátů a zajistit uchování pořízených záznamů po dobu nejméně 10 let od ukončení platnosti příslušného kvalifikovaného certifikátu, a to nejméně v rozsahu uvedeném v odst. 3 a 4. Poskytovatel je povinen stanovit v Certifikační politice dobu, po kterou tyto záznamy uchovává.

(2) Poskytovatel je povinen zajistit, že všechny informace uvedené v odst. 1 jsou pořizovány, uchovávány a zpracovávány bezpečným způsobem, se zachováním jejich dostupnosti, integrity, časové autentičnosti a důvěrnosti, a po uplynutí doby stanovené pro uchování záznamů je povinen je bezpečným způsobem prokazatelně zničit.

(3) Zaznamenávány jsou všechny informace a události vztahující se k registraci a životnímu cyklu vydávaných kvalifikovaných certifikátů, zejména pak:

a. identifikace místa uložení provozní dokumentace,
b. identifikační údaje osoby, která provedla ověření totožnosti žadatele,
c. obchodní název poskytovatele, který žádost o vydání kvalifikovaného certifikátu přijal, nebo smluvního partnera, který pro poskytovatele tuto činnost zajišťuje,
d. všechny požadavky na zneplatnění kvalifikovaných certifikátů a záznamy o jejich zneplatnění,
e. všechny požadavky na vydání kvalifikovaných certifikátů.

(4) Poskytovatel dále zaznamenává zejména:

a. všechny události vztahující se k životnímu cyklu jeho párových dat,

b. všechny události vztahující se k životnímu cyklu jeho kvalifikovaných certifikátů.

(5) Poskytovatel je povinen zaznamenávat čas zaznamenávaných událostí a stanovit v Certifikační prováděcí směrnici způsob určení času a provedení záznamu času.

ČÁST ČTVRTÁ

ZAJIŠŤOVÁNÍ BEZPEČNOSTI

Párová data

§ 14

Vytváření párových dat pro žadatele

(1) Nástroj elektronického podpisu, který je určen k vytváření párových dat pro žadatele, musí být dostatečně bezpečný z hlediska kryptografické bezpečnosti. Tato podmínka se považuje za splněnou, pokud tento nástroj splňuje hodnocení podle Federal Information Processing Standard 140-1 úroveň 3 (dále jen ”standard pro hodnocení bezpečnosti kryptografických modulů”).

(2) Poskytovatel je povinen zajistit, že párová data, pokud je poskytovatel pro žadatele vytváří, splňují parametry uvedené v příloze 1 této vyhlášky.

(3) S párovými daty žadatele je povinen poskytovatel nakládat před jejich předáním žadateli bezpečným způsobem a předat je žadateli tak, aby nebyla vyzrazena. Postup při nakládání s párovými daty žadatele před jejich předáním žadateli a při předání žadateli stanoví poskytovatel v Certifikační prováděcí směrnici.

§ 15

Párová data poskytovatele

(1) Párová data poskytovatele vytváří pouze osoba k tomu poskytovatelem určená a provádí je způsobem definovaným v Certifikační prováděcí směrnici.

(2) K vytváření párových dat poskytovatele se musí použít bezpečný nástroj elektronického podpisu. Tato podmínka se považuje za splněnou, pokud tento nástroj splňuje standard pro hodnocení bezpečnosti kryptografických modulů úroveň 3 a jsou použity kryptografické algoritmy splňující parametry uvedené v příloze č. 1.

(3) Poskytovatel je povinen zajistit, že:

a. s jeho daty pro vytváření elektronického podpisu je nakládáno bezpečným způsobem,
b. jeho data pro vytváření elektronického podpisu jsou zajištěna tak, že s nimi smí nakládat pouze osoba k tomu poskytovatelem určená.

(4) Záložní kopie dat pro vytváření elektronického podpisu poskytovatele musí podléhat stejné nebo vyšší úrovni bezpečnostních opatření jako data pro vytváření elektronického podpisu určená k používání.

(5) Poskytovatel je povinen svá data pro vytváření elektronického podpisu, včetně jejich záložních kopií, prokazatelně zničit po ukončení jejich životního cyklu.

§ 16

Prostředky pro bezpečné vytváření elektronického podpisu

a pro bezpečné ověřování elektronického podpisu

(1) Prostředek pro bezpečné vytváření elektronického podpisu musí mít takové vlastnosti, které před podepsáním datové zprávy zajistí, aby podepisující osoba:

a. byla nucena projevit svoji vůli k podepsání datové zprávy,
b. se mohla seznámit s obsahem podepisované datové zprávy,
c. byla nucena zadat přístupové heslo nebo byl uplatněn jiný obdobný autentizační mechanismus.

(2) Prostředek pro bezpečné vytváření elektronického podpisu musí být hodnotitelný podle ISO 15408 na míru záruky EAL 3 nebo podle Kritérií hodnocení bezpečnosti informačních systémů - úroveň E 3. Prostředek pro bezpečné vytváření elektronického podpisu je považován za hodnotitelný, pokud je připraven k hodnocení podle uvedené normy. Připraveností k hodnocení se rozumí splnění podmínek, které norma stanoví a zpracování dokumentace, kterou norma požaduje. Připravenost k hodnocení musí být konstatována auditem ve smyslu § 21.

(3) Data pro vytváření elektronického podpisu, se kterými prostředek pro bezpečné vytváření podpisu pracuje, musí být bezpečně uložena na nosiči. Nosič musí být hodnocen podle standardu pro hodnocení bezpečnosti kryptografických modulů úroveň 2. Při použití jiného hodnocení musí být doloženo, že výsledky se rovnají hodnocení podle tohoto standardu.

(4) Prostředek pro bezpečné ověřování elektronického podpisu musí být hodnotitelný podle ISO 15408 na míru záruky EAL 3 nebo podle Kritérií hodnocení bezpečnosti informačních systémů - úroveň E 3. Prostředek pro bezpečné ověřování elektronického podpisu je považován za hodnotitelný, pokud je připraven k hodnocení podle uvedené normy. Připraveností k hodnocení se rozumí splnění podmínek, které norma stanoví a zpracování dokumentace, kterou norma požaduje. Připravenost k hodnocení musí být konstatována auditem ve smyslu § 21.

(5) O možnosti používání prostředku pro bezpečné vytváření anebo ověřování elektronického podpisu rozhoduje Úřad na základě žádosti. Součástí žádosti je písemná zpráva, kterou je audit zakončen, a podrobný popis specifických komponent, které má prostředek pro bezpečné vytváření elektronického podpisu implementovány. Seznam těchto komponent je uveden v příloze č. 2 této vyhlášky.

§ 17

Náležitosti používání prostředku pro bezpečné vytváření elektronického podpisu poskytovatelem

(1) Poskytovatel je povinen zajistit, že:

a. s prostředkem pro bezpečné vytváření elektronického podpisu užívaným pro podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, není možné neoprávněně manipulovat během jeho skladování a přepravy, přičemž přepravou se rozumí zejména přeprava mezi místem skladování a místem použití,
b. prostředek pro bezpečné vytváření elektronického podpisu užívaný pro podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, lze uvést do provozu za podmínky aktivní součinnosti alespoň dvou osob, které jsou pro tuto činnost poskytovatelem určeny,
c. ke změně provozního režimu prostředku pro bezpečné vytváření elektronického podpisu užívaného pro podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, může dojít pouze za podmínky aktivní součinnosti alespoň dvou osob, které jsou pro tuto činnost poskytovatelem určeny,
d. data pro vytváření elektronického podpisu uložená v prostředku pro bezpečné vytváření elektronického podpisu a užívaná pro podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, jsou prokazatelně zničena v případě ukončení činnosti tohoto prostředku.

(2) Poskytovatel je povinen doložit Úřadu používání takového postupu a splnění požadavku podle odst. 1 v dokumentech Předpisové základny. Úřad je oprávněn si u poskytovatele vyžádat doplňující informace k posouzení, případně provést šetření u poskytovatele.

§ 18

Informační systém pro certifikační služby a zajištění informační bezpečnosti

(1) Poskytovatel je povinen zajistit, že při zajišťování certifikačních služeb jsou používány informační systémy, které jsou chráněny proti nežádoucím změnám. Tato podmínka se považuje za splněnou, pokud je informační systém pro certifikační služby hodnotitelný podle ISO 15408 na míru záruky EAL 4 nebo podle Kritérií hodnocení bezpečnosti informačních systémů - úroveň E 3.

(2) Informační systém pro certifikační služby je považován za hodnotitelný, pokud je připraven k hodnocení podle normy uvedené v odst. 1. Připraveností k hodnocení se rozumí splnění podmínek, které norma stanoví a zpracování dokumentace, kterou norma požaduje. Připravenost k hodnocení musí být konstatována auditem ve smyslu § 21.

(3) Analýza bezpečnostních požadavků na informační systém pro certifikační služby, který vytváří poskytovatel nebo je pro něj vytvářen, musí být provedena již ve fázi návrhu a specifikace požadavků na tento systém.

(4) V případě vyzrazení dat pro vytváření elektronického podpisu poskytovatele je poskytovatel povinen zejména zajistit:

a. zpřístupnění této informace osobám spoléhajícím na certifikát,

b) zneplatnění všech kvalifikovaných certifikátů, které mohou být ovlivněny vyzrazením dat pro vytváření elektronického podpisu poskytovatele.

(5) Způsob a lhůty k odst. 4 a) - b) stanoví poskytovatel v Plánu pro zvládání krizových situací a v Plánu obnovy. Základní informaci o způsobu a lhůtách zveřejní v souladu s § 6 odst. 6.

(6) Poskytovatel je povinen zajistit průběžné sledování požadavků na kapacitu informačního systému používaného pro certifikační služby, vyhodnocovat je a případně provádět změny, které zajistí odpovídající funkci systému. Tyto změny musí být prováděny ve shodě se způsoby a postupy stanovenými v dokumentech Předpisové základny.

(7) Požadavky uvedené v odst. 3 - 6 se považují za splněné, pokud byly shledány splněnými při auditu Certifikační prováděcí směrnice, Celkové bezpečnostní politiky a Systémové bezpečnostní politiky.

§ 19

Objektová bezpečnost

Při poskytování certifikačních služeb musí způsob zabezpečení ochrany objektů, technické prostředky, použití technických prostředků, podmínky nasazení fyzické ostrahy a režimová opatření pro účely objektové bezpečnosti splňovat podmínky, které stanoví zvláštní předpis pro ochranu utajovaných skutečností ve stupni “důvěrné”.

§ 20

Personální bezpečnost

(1) Poskytovatel je povinen zajistit, že certifikační služby vykonávají osoby, které mají odborné znalosti, zkušenosti a kvalifikaci nezbytnou pro poskytování certifikačních služeb a odpovídající konkrétnímu pracovnímu zařazení. Poskytovatel je povinen zajistit pro tyto osoby průběžná školení pro zajištění stálé odborné způsobilosti a vytvořit podmínky pro získávání, udržování a zvyšování bezpečnostního vědomí.

(2) Poskytovatel je povinen zajistit, že osoby vykonávající certifikační služby, jsou seznámeny s dokumenty Předpisové základny v rozsahu, která odpovídá jejich pracovnímu zařazení. Dále je povinen zajistit průběžnou kontrolu povinností, které byly těmto osobám uloženy.

(3) Poskytovatel je povinen v Certifikační prováděcí směrnici stanovit, jak je zajištěn výkon činností uvedených v § 8 odst. 2 v případech, kdy osoby určené pro výkon těchto činností nejsou schopny příslušnou činnost po určitou dobu vykonávat. Poskytovatel je

povinen zejména stanovit, které osoby jsou oprávněny určené osoby zastoupit, za jakých okolností a jaké kontroly jejich činnosti jsou uplatněny.

(4) Osoba, která pro poskytovatele vykonává činnost podle § 8 odst. 2, musí být bezúhonná, spolehlivá a musí být do své funkce jmenována statutárním orgánem. Za bezúhonného se pro účely této vyhlášky považuje ten, kdo nebyl pravomocně odsouzen pro úmyslně spáchaný trestný čin, nebo trestný čin spáchaný z nedbalosti, jehož skutková podstata souvisí s poskytováním certifikačních služeb, pokud se na něho nehledí, jako by nebyl odsouzen.

(5) Požadavky uvedené v odst. 1 – 4 se považují za splněné, pokud byly shledány splněnými ve smyslu § 21 při auditu dokumentů Certifikační prováděcí směrnice, Celkové bezpečnostní politiky a Systémové bezpečnostní politiky.

§ 21

Audit

(1) Auditem se rozumí činnost, která je prováděna za účelem ověření, zda určité činnosti jsou vykonávány stanoveným způsobem. Audit je zakončen písemnou zprávou.

(2) Osoby provádějící audit musí být bezúhonné a odborně způsobilé.

(3) Pro vymezení bezúhonnosti platí přiměřeně ustanovení § 20 odst. 4. Bezúhonnost se dokládá výpisem z evidence Rejstříku trestů ne starším než 3 měsíce.

(4) Předpokladem pro prokázání odborné způsobilosti k provádění auditů je ukončené vysokoškolské vzdělání příslušného technického nebo příslušného přírodovědného směru a 6 let odborné praxe. Odbornou způsobilost posuzuje Úřad na základě zkoušky. Předseda Úřadu může rozhodnout, že se této podmínky u významných odborníků z praxe neužije.

(5) Audit nesmí u poskytovatele provést osoba, která:

a. má majetkovou účast ve společnosti poskytovatele,
b. je společníkem poskytovatele, statutárním orgánem nebo členem statutárního orgánu poskytovatele, anebo je v pracovním nebo obdobném vztahu k poskytovateli,
c. je osobou blízkou osobám, jejichž postavení by mohlo ovlivnit její činnost.

ČÁST PÁTÁ

ZAJIŠŤOVÁNÍ CERTIFIKAČNÍCH SLUŽEB

PROSTŘEDNICTVÍM SMLUVNÍCH PARTNERŮ

§ 22

(1) Poskytovatel je oprávněn certifikační služby nebo jejich části zajistit na základě písemné smlouvy prostřednictvím smluvních partnerů. Činnost musí být prováděna v souladu s dokumenty Předpisové základny. Odpovědnost za zajišťování certifikačních služeb vůči žadatelům, držitelům a osobám spoléhajícím na certifikát nese poskytovatel.

(2) Vytváření kvalifikovaných certifikátů a vytváření seznamu kvalifikovaných certifikátů, které byly zneplatněny, nelze zajišťovat prostřednictvím smluvních partnerů.

ČÁST ŠESTÁ

UKONČENÍ ČINNOSTI POSKYTOVATELE

§ 23

(1) Poskytovatel je povinen učinit nezbytná opatření, která pro držitele a osoby spoléhající na certifikát minimalizují nepříznivé následky ukončení poskytování certifikačních služeb.

(2) Poskytovatel je povinen v Certifikační prováděcí směrnici stanovit postup, který bude uplatněn v případě ukončení jeho činnosti.

(3) Poskytovatel je povinen zejména zajistit tyto činnosti a stanovit postup při jejich zajištění:

a. zpřístupnění informace o ukončení své činnosti všem osobám spoléhajícím na certifikát, držitelům a jiným osobám, se kterými má smluvní nebo jiné obdobné vztahy týkající se poskytování certifikačních služeb,
b. ukončení vydávání kvalifikovaných certifikátů,
c. uchování údajů získaných při registraci a záznamů událostí po dobu, kterou pro jejich uchování stanoví Certifikační prováděcí směrnice, nejméně však 10 let od ukončení platnosti vydaných kvalifikovaných certifikátů,
d. prokazatelné zničení dat pro vytváření elektronického podpisu poskytovatele.

(4) Poskytovatel je povinen stanovit postup ke splnění požadavků uvedených v odst. 3 v případě, že je nebude poskytovatel schopen splnit sám, resp. na který subjekt tyto činnosti přecházejí a jak je převod činností zajištěn; výjimkou z tohoto ustanovení jsou mimořádné události jakými mohou být stávky, občanské nepokoje, válečný stav, přírodní katastrofy nebo jiné výsledky působení vyšší moci.

(5) V případě, že poskytovatel smluvně zajistí správu vydaných platných kvalifikovaných certifikátů jiným poskytovatelem, je poskytovatel, který bude správu kvalifikovaných certifikátů zajišťovat povinen zajistit srovnatelné podmínky certifikačních služeb, jaké jsou stanoveny v Certifikační politice a Certifikační prováděcí směrnici poskytovatele, který ukončuje svoji činnost.

ČÁST SEDMÁ

NĚKTERÉ DALŠÍ POVINNOSTI POSKYTOVATELE CERTIFIKAČNÍCH SLUŽEB

§ 24

Kvalifikace

(1) Kvalifikací nezbytnou pro výkon činností uvedených v § 8 odst. 2 se rozumí:

a. ukončené vysokoškolské vzdělání a 3 roky praxe,
b. ukončené vyšší odborné nebo úplné střední odborné vzdělání a 5 let praxe.

(2) Poskytovatel je oprávněn v jednotlivých případech zkrátit délku uvedené praxe až o jednu třetinu stanovené délky na základě přezkoušení, při němž pracovník prokáže dostatečné znalosti k výkonu důvěryhodné funkce.

§ 25

Finanční zdroje

(1) Dostatečností finančních zdrojů poskytovatele na provoz podle § 6 odst. 1 písm. l) zákona o elektronickém podpisu se rozumí schopnost finančně zabezpečit řádné provozování certifikačních služeb a schopnost zabezpečit současné a budoucí závazky z těchto služeb nejméně na období 3 let.

(2) Dostatečnost finančních zdrojů se dokládá výroční zprávou, jejímž obsahem je přehled obchodní činnosti poskytovatele související s poskytováním certifikačních služeb v uplynulém roce a předpoklady jeho dalšího podnikání v této oblasti.

§ 26

Účinnost

Tato vyhláška nabývá účinnosti dnem vyhlášení a pozbývá platnosti dnem 31. prosince 2003.

Příloha č.1 k vyhlášce č. …./ … Sb.

Kryptografické parametry

Hashovací funkce:
a) MD5
b) SHA-1
c) RIPEMD-160
Asymetrická kryptografie:
a) RSA
b) DSA
c) DSA variace založené na eliptických křivkách:
- ISO/IEC 14883-3, Příloha A.2.2 ("analogie Agnew-Mullin-Vanstone"),
- IEEE standard P1363, oddíl 5.3.3 ("verze Nyberg-Rueppel "),
- IEEE standard P 1363 [5], oddíl 5.3.4 ("verze DSA").
Minimální délka klíče:
1024 bitů RSA
1024 bitů DSA
161 bitů variace DSA založené na eliptických křivkách
112 bitů Triple DES
128 bitů Rijndael

Příloha č. 2 k vyhlášce č. …/ … Sb.

Specifické komponenty

Komponenty vztahující se k důvěryhodnému prostředí
Komponenta
a. prohlížení podepsaných datových zpráv
b. prohlížení atributů elektronického podpisu,
c. interakce podpisující osoby s prostředkem pro bezpečné vytváření/ověřování elektronického podpisu (interakce pod kontrolou uživatele),
d. zajišťující způsob a postup autentizace (např. čipová karta s PINem) podepisující osoby na základě autentizujících dat anebo biometrických vlastností,
e. připravující pro datovou zprávu příslušný otisk,
f. řídící interakci mezi systémem a prostředkem pro bezpečné vytváření/ověřování elektronického podpisu.

Komponenty vztahující se k vlastním aplikacím
Komponenta
a. pro výběr datové zprávy,
b. pro vlastní vytváření datové zprávy (např. vestavěný textový editor),
c. zobrazující úplný obsah kvalifikovaného certifikátu podepisující osoby,
d. vytvářející výstupní normalizované formáty,
e. používaná pro získání kvalifikovaného certifikátu podepisující osoby,
f. používaná pro získání časové značky (pokud je používána),
g. zobrazující jméno vlastníka prostředku pro bezpečné vytváření elektronického podpisu.