ELEKTRONICKÝ PODPIS

přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů

kolektiv autorů

Nakladatelství ANAG

ISBN 80-7263-125-X

OBSAH

1. Úvodní slovo autorů 5

2. Právní úprava elektronického podpisu v ČR 10

2.1 Zákon o elektronickém podpisu 13

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) 13

2.2 Vyhláška o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu 31

Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu 31

2.3 Nařízení vlády, kterým se provádí zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) 41

Nařízení vlády č. 304/2001 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) 41

2.4 Požadavky zveřejněné ve Věstníku Úřadu pro ochranu osobních údajů č. 12/2001 43

3. Elektronický podpis v Evropském společenství 44

3.1 Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy (pracovní překlad) 44

3.2 Přehled současné právní úpravy elektronického podpisu v členských státech ES 60

4. Komentář a výklad k vyhlášce č. 366/2001 Sb. 62

5. Abeceda elektronického podpisu 94

6. Typy elektronických podpisů 102
6.1 Úvodní pojmy 102
6.2 Elektronický podpis (General Electronic Signature) 103
6.3 Zaručený elektronický podpis (Advanced Electronic Signature) 104
6.4 Zaručený elektronický podpis založený na kvalifikovaném certifikátu (Advanced Electronic Signature Using Qualified Certificate) 107
6.5 Kvalifikovaný podpis (Qualified Electronic Signature) 110
6.6 „Vylepšený“ elektronický podpis (Enhanced electronic signature) 111
6.7 Kvalifikovaný podpis určený pro archivaci dat (Qualified Electronic Signature with Long-term Validity) 112
7. Prostředek pro bezpečné vytváření elektronického podpisu a nástroj elektronického podpisu 114
7.1 Prostředek pro bezpečné vytváření a ověřování zaručených elektronických podpisů 114
7.2 Nástroj elektronického podpisu 117
7.3 Evropská unie 118
8. Vysvětlení základních pojmů 120

1. ÚVODNÍ SLOVO AUTORŮ

V současné době se stáváme svědky zajímavého jevu: u nově vznikajících dokumentů začíná nad tradiční formou převažovat forma elektronická. Některé vznikají přímo v elektronické podobě, jiné převodem z formy tradiční.

Dokumenty pořízené v tradiční podobě mohou být opatřeny vlastnoručním podpisem. Vyvstává otázka, jak tento podpis nahradit ve světě elektronickém. Převodem z tradiční podoby do elektronické přicházejí dokumenty o vlastnoruční podpis, který byl jejich součástí, nebo se takový podpis stává nedůvěryhodným. To platí například pro zprávy zaslané faxem.

Elektronických dokumentů stále přibývá, jejich předávání je snadné a rychlé a uživatelé si výhody, které tento způsob komunikace přináší, uvědomují. Proto je nezbytné najít metodu, která v elektronickém světě umožní provést úkon odpovídající vlastnoručnímu podpisu.

Požadavky na elektronický podpis můžeme vyjádřit pojmy neporušenost, identifikace, nepopiratelnost. Podepsaný dokument nesmí být změněn (neporušenost), musí být možné určit osobu, která se podepsala (identifikace), a zajistit, aby tato osoba nemohla svůj podpis popřít (nepopiratelnost). V případě právního sporu musí být navíc zajištěna neodmítnutelnost elektronického podpisu (právní akceptovatelnost). Pokud elektronický podpis všechny tyto požadavky splňuje, nazýváme jej zaručený elektronický podpis.

Na elektronický podpis je možné klást i jiné požadavky, např. požadavek na utajení obsahu dokumentu před nepovolanou osobou nebo požadavek na prokázání existence dokumentu v daném čase. Tyto požadavky nepatří mezi vlastnosti podpisu vlastnoručního, a proto se nestaly ani požadavky na definici podpisu elektronického. V případě potřeby je ale možné je splnit pomocí navazujících služeb, například šifrováním nebo použitím časových razítek.

Existuje celá řada typů elektronického podpisu. Typ použitého podpisu záleží především na povaze podepsané zprávy. Protože komunikace má dvě strany – odesilatele zprávy a jejího příjemce – musí mezi nimi existovat určitá forma dohody o povaze zprávy, resp. její závažnosti. Příjemce zprávy stanoví, jaký typ elektronického podpisu je pro zprávy, které obdrží, přijatelný. Odesilatel zprávy buď podmínky příjemce akceptuje, nebo neakceptuje a v tom případě použije dosud užívanou formu komunikace, tj. zpravidla předání dokumentu v tradiční podobě s vlastnoručním podpisem. Požadovaný typ elektronického podpisu může být stanoven i právním předpisem, podobně

jako některé právní předpisy stanoví typ vlastnoručního podpisu, například podpisu ověřeného notářem.

Použitý typ elektronického podpisu může souviset také s tím, zda se komunikující znají nebo ne. Pokud se znají, příjemci nebude činit problém se ujistit, zda zprávu podepsal skutečně odesilatel, případně že doručená zpráva je identická se zprávou přijatou. Pokud se odesilatel s příjemcem neznají, je potřeba možnost ověření zajistit jiným způsobem, tj. jiným typem elektronického podpisu, než je například jméno napsané z klávesnice.

Zprávy s běžným informativním obsahem se podepisují zpravidla pouze jménem napsaným z klávesnice. Pro zprávy závažného obsahu se volí jiné typy podpisů (jsou popsány v kapitole „Typy elektronických podpisů“).

Od elektronického podpisu bychom neměli očekávat o moc více, než očekáváme od vlastnoručního podpisu. V běžném životě se spoléháme velmi často na podpis, který je pouhým „klikyhákem“ a kterému důvěřujeme, aniž je notářsky ověřen nebo máme příslušný podpisový vzor nebo daný podpis či jeho tvůrce známe. Jednotlivé typy podpisů nám poskytnou rozdílný „komfort“ a při jejich použití je možné získat řadu dalších informací, předaných důvěryhodným způsobem, a to zejména v případě, že jsou spojeny s certifikáty. Tak je dosahováno vyšší míry bezpečí této formy komunikace.

Někdy je elektronický podpis chápán jako cosi velmi složitého, něco, co je mimo možnost chápání lidí, kteří nejsou odborníky v dané oblasti. Příčinou je patrně fakt, že často není zcela rozlišována hranice, nakolik musí problematice kryptografických klíčů, příslušnému softwaru a případně hardwaru porozumět člověk, který elektronický podpis používá pouze pro podepisování, nakolik odborný pracovník poskytovatele certifikačních služeb, nakolik ten, kdo „staví“ certifikační autoritu atd. Pro „uživatele“ elektronického podpisu, tj. pro podepisující osoby, je náročnost srovnatelná s používáním běžných aplikací. Zjednodušeně řečeno, pokud uživatel umí pracovat s elektronickou poštou, nebude pro něj elektronické podepisování činit žádný problém. Pro překonání prvotních nesnází platí do značné míry to, co v případě používání jiných prostředků – je dobré si přečíst návod.

Tato publikace je určena především pro poskytovatele certifikačních služeb, protože její stěžejní částí je výklad k vyhlášce č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu. Pouze některá ustanovení této vyhlášky se týkají běžného uživatele. Aby byla publikace přínosem pro co nejširší okruh čtenářů, jsou připojeny kapitoly, které objasňují základní pojmy a postupy související s používáním elektronického podpisu.

V souvislosti se zákonem o elektronickém podpisu je nutné zdůraznit skutečnost, která není všeobecně známá, a sice že tento zákon neomezuje používání elektronického podpisu v soukromoprávní oblasti, tj. například při komunikaci bank s jejich klienty, mezi firmami, v elektronickém obchodu, mezi občany atd. V těchto případech je na komunikujících subjektech, zda použijí tuto formu komunikace a jaký typ elektronického podpisu, případně certifikátu a jakého poskytovatele certifikačních služeb zvolí. Pouze v tom případě, že se zcela svobodně rozhodnou používat kvalifikované certifikáty ve smyslu tohoto zákona, případně vydané akreditovanými poskytovateli, musí se jednotlivé strany řídit příslušnými ustanoveními zákona.

Obdobná situace je v případě poskytovatelů certifikačních služeb. Ne všem je určen tento zákon, resp. ne na všechny poskytovatele se tento zákon vztahuje. Certifikační autority fungující na školách, v bankách, podnicích, tedy všechny tyto subjekty, zůstávají mimo rámec zákona o elektronickém podpisu, pokud se však samy dobrovolně nerozhodnou jinak. V čem spočívá toto rozhodnutí? Poskytovatelé certifikačních služeb se pod „režim“ zákona dostávají tehdy, pokud se rozhodnou, že budou vydávat certifikáty s označením „kvalifikované certifikáty“, nebo se rozhodnou, že požádají Úřad pro ochranu osobních údajů o udělení akreditace. A k čemu kvalifikované certifikáty a akreditace? Souvisejí s tím, co už bylo uvedeno v úvodu, tj. s podmínkami, které jsou zvoleny pro určitý typ komunikace. Například provozovatel elektronického obchodu z důvodu vyšší bezpečnosti stanoví, že bude uznávat pouze kvalifikované certifikáty. Chtějí-li zákazníci využít jím nabízené služby, musí ke komunikaci použít kvalifikované certifikáty a akceptovat tak práva a povinnosti, které v takovém případě ze zákona o elektronickém podpisu vyplývají. Jiným příkladem může být komunikace v oblasti veřejné moci, kde zákon o elektronickém podpisu stanoví, že je možné používat pouze kvalifikované certifikáty vydané akreditovanými poskytovateli.

Vraťme se ještě ke vztahu pojmů poskytovatel certifikačních služeb a certifikační autorita. Do doby vydání evropské směrnice se užíval název certifikační autorita nebo důvěryhodná třetí strana, směrnice zavedla pojem poskytovatel certifikačních služeb. Tento pojem byl převzat i do zákona o elektronickém podpisu. Protože je na vůli poskytovatelů, jaký název pro své firmy zvolí, je možné se poměrně často setkat s názvem certifikační autorita. Navíc, některé z těchto firem byly založeny i několik let před vydáním směrnice.

Pro ty, kteří se rozhodnou elektronický podpis používat, uvádíme ještě jednu praktickou radu. Pokud se rozhodnou využít služeb některého poskytovatele certifikačních služeb, prvním krokem by mělo být seznámení s jeho certifikační politikou. Jedná se o dokument, který obsahuje vše, co by měl uživatel o službách daného poskytovatele vědět. Naprostá většina poskytovatelů nabízí i řadu praktických návodů. Tyto dokumenty jsou zpravidla dostupné na jejich webových stránkách.

Publikace, kterou právě čtete, je rozdělena do osmi částí. Po tomto krátkém úvodu následuje kapitola „Právní úprava elektronického podpisu v ČR“, která obsahuje úplné znění právních předpisů, které upravují oblast elektronického podpisu v České republice. Těmito předpisy jsou zákon o elektronickém podpisu, již zmiňovaná vyhláška a nařízení vlády, kterými se provádí zákon o elektronickém podpisu.

Vyhláška Úřadu pro ochranu osobních údajů mimo jiné ukládá, aby ve svém věstníku zveřejnil požadavky na celkovou bezpečnostní politiku, systémovou bezpečnostní politiku a na kryptografické funkce. Úřad pro ochranu osobních údajů tak již učinil a tyto informace jsou rovněž v naší publikaci uvedeny.

Třetí část je věnována elektronickému podpisu v Evropské unii a tvoří ji dva dokumenty. Prvním je pracovní překlad Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy. Členské státy ES jsou povinny promítnout tuto Směrnici do svých národních legislativ. Tento předpis se tedy nepřebírá v plném znění, ale jeho principy mohou být do jednotlivých právních řádů promítnuty způsobem, který každý jednotlivý stát považuje za adekvátní. Nemusejí tedy být ve všech státech přijímány zvláštní zákony o elektronickém podpisu, ale principy směrnice mohou být začleněny do jiných zákonů. Druhý dokument obsahuje stručný přehled současné právní úpravy elektronického podpisu v jednotlivých členských státech ES.

Čtvrtá kapitola obsahuje podrobné komentované paragrafové znění vyhlášky k zákonu o elektronickém podpisu. Tato část by měla pomoci především těm subjektům, které hodlají vydávat kvalifikované certifikáty nebo se připravují k akreditaci. Použitelná je i pro dovozce a prodejce nástrojů elektronického podpisu a dále pro výrobce a dovozce prostředků pro bezpečné vytváření a ověřování elektronického podpisu. Určena je dále samozřejmě těm, kteří se profesně elektronickým podpisem zabývají, a to od právníků přes informatiky, kryptology po pracovníky státní správy a v neposlední řadě management firem, které se chystají elektronický podpis využívat.

Pro nejširší veřejnost jsou určeny závěrečné kapitoly „ABC elektronického podpisu“, „Typy elektronických podpisů“, „Prostředek pro bezpečné vytváření elektronického podpisu“ a „Nástroj elektronického podpisu“, které mají za úkol čtenáře seznámit s nejrůznějšími aspekty elektronického podpisu. Každá z těchto kapitol je psána jinou formou, a to od výkladu pro úplné začátečníky až po odborný výklad různých typů elektronických podpisů a vysvětlení rozdílu mezi nástrojem a prostředkem elektronického podpisu. V závěrečné kapitole „Vysvětlení základních pojmů“ nalezne čtenář řadu informací, které by mu měly pomoci při studiu materiálů o elektronickém podpisu.

Autoři doufají, že publikace přispěje k pochopení principů elektronického podpisu a zvýší důvěru v něj. Odpovědi na otázky by zde měli najít všichni, kteří se o elektronický podpis zajímají.

2. PRÁVNÍ ÚPRAVA ELEKTRONICKÉHO PODPISU V ČR

Přijetím zákona o elektronickém podpisu byly již v roce 2000 v České republice naplněny cíle jeho předkladatelů, které směřovaly k tomu, aby došlo k vytvoření základních legislativních předpokladů pro to, aby prostřednictvím moderních informačních technologií a s pomocí prostředků dálkového přístupu byly zajištěny stejné nebo obdobné podmínky jak pro uživatele, kteří zpracovávají informace, dokumenty nebo jiné podklady v listinné psané nebo tištěné formě, tak i pro uživatele, kteří informace zpracovávají v elektronické formě pomocí datových zpráv. Tímto základním právním předpisem byl odstraněn dosud obecně existující a přijímaný rozpor při zacházení s informacemi zpracovávanými jako datové zprávy a informacemi v listinné formě – dokumenty na papíře.

Dalším významným záměrem tvůrců zákona o elektronickém podpisu je využívat prostředky elektronického podpisu i pro komunikaci v oblasti veřejné moci a pro rozvoj elektronického obchodu a usnadnit tak provádění obchodních transakcí.

Protože v právním řádu České republiky neexistovala před přijetím zákona o elektronickém podpisu jednotná právní úprava, která by zcela jednoznačně připouštěla možnost existence elektronické formy dokumentu typu smlouvy, podání, žádosti, žaloby, rozhodnutí apod., nebo naopak zakazovala elektronickou formu komunikace a předávání dokumentace, bylo nezbytné učinit tento základní krok. Snaha zákonodárce současně byla taková, aby zákon o elektronickém podpisu jako základní právní předpis pro tuto oblast byl z hlediska jeho obsahu a rozsahu co nejobecnější a současně technologicky pokud možno co nejméně závislý, aby při případné změně technologie nemuselo docházet současně i ke změně textu zákona o elektronickém podpisu. Bylo tedy nezbytné zajistit, aby pro vytváření i ověřování (zaručených) elektronických podpisů bylo možno používat všechny standardizované postupy a využívat dostupné technologické prostředky, které však budou současně obsahovat i dostatečná bezpečnostní opatření, která mohou účinně zabránit zneužití elektronického podpisu.

Existence zákona, který obsahuje základní právní podmínky pro vytváření a používání elektronického podpisu v České republice, umožnila současně i přípravu některých základních předpisů pro aplikaci tohoto zákona v oblasti veřejné správy. Proto bylo v návaznosti na zákon o elektronickém

podpisu přijato nařízení vlády č. 304/2001 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Jeho obsahem je právní úprava základních organizačně technických opatření orgánů veřejné moci včetně územních samosprávných celků provádějících výkon státní správy v rámci přenesené působnosti. Těmito opatřeními bude zabezpečena povinnost těchto orgánů přijmout podání učiněné v elektronické podobě a podepsané elektronicky a také činit úkony v elektronické podobě a podepsané elektronicky, bude-li toto právo orgánů veřejné moci stanoveno zvláštním předpisem. Pro orgány veřejné moci toto nařízení současně stanoví povinnost zřídit pro příjem a odesílání datových zpráv pracoviště splňující požadavky na technické a programové vybavení podle standardů vydaných Úřadem pro veřejné informační systémy a umožňující používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Zákon o elektronickém podpisu sice předpokládal, že Úřad pro ochranu osobních údajů vydá potřebnou prováděcí vyhlášku, ale tvůrci zákona jakoby pozapomněli na skutečnost, že Úřad pro ochranu osobních údajů, který byl zřízen zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, neměl zmocnění pro vydávání prováděcích právních předpisů. Proto musela být krátce po schválení zákona o elektronickém podpisu v roce 2000 iniciována novela zákona o ochraně osobních údajů, jejíž součástí je mimo jiné ustanovení, které obsahuje zmocnění pro Úřad pro ochranu osobních údajů vydat vyhlášku k provedení zákona o elektronickém podpisu. Toto ustanovení však nabylo účinnosti až dnem 31. května 2001, kdy teprve mohl Úřad pro ochranu osobních údajů oficiálně předložit do meziresortního připomínkového řízení návrh vyhlášky, jejímž cílem bylo upřesnit podmínky stanovené v § 6 a 17 zákona o elektronickém podpisu a způsob, jakým se jejich splnění bude dokládat, a požadavky, které musí splňovat nástroje elektronického podpisu, a náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.

Vyhláška Úřadu pro ochranu osobních údajů ze dne 3. října 2001 byla vydána podle zmocnění obsaženého v § 20 zákona o elektronickém podpisu a publikována ve Sbírce zákonů pod č. 366/2001 Sb. jako vyhláška o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu s účinností od 10. října 2001.

Posledním dokumentem uvedeným v této kapitole je text z Věstníku č. 12 Úřadu pro ochranu osobních údajů, kterým se upřesňují některé požadavky na celkovou bezpečnostní politiku, systémovou bezpečnostní politiku a na výsledek hodnocení kryptografických funkcí, které používá nástroj elektronického podpisu.

2.1 ZÁKON O ELEKTRONICKÉM PODPISU

Zákon č. 227/2000 Sb.,
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 veš-

keré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

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

§ 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, 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.

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

§ 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.

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

§ 8
Ochrana osobních údajů

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

[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)]

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

§ 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,
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.

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

§ 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,
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.

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

§ 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 kvali-

fikovaný 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 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)]

[9)] Zákon č. 71/1967 Sb., ve znění zákona č. 29/2000 Sb.

§ 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., zákona č. 29/2000 Sb., zákona č. 159/2000 Sb. a zákona č. 218/2000 Sb., se mění takto:

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., zákona č. 130/2000 Sb., zákona č. 155/2000 Sb. a zákona č. 220/2000 Sb., se mění takto:

V § 42 odst. 1 věta první zní: „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., zákona č. 151/2000 Sb., zákona č. 153/2000 Sb., zákona č. 154/2000 Sb., zákona č. 156/2000 Sb. a zákona č. 158/2000 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.*)

*) *Red. pozn.: tj. 1. října 2000.*

2.2 VYHLÁŠKA O UPŘESNĚNÍ PODMÍNEK STANOVENÝCH V § 6 a 17 ZÁKONA O ELEKTRONICKÉM PODPISU A O UPŘESNĚNÍ POŽADAVKŮ NA NÁSTROJE ELEKTRONICKÉHO PODPISU

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

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

§ 1
Předmět úpravy

Tato vyhláška upřesňuje podmínky stanovené v § 6 a 17 zákona o elektronickém podpisu a způsob, jakým se jejich splnění bude dokládat, a požadavky, které musí splňovat nástroje elektronického podpisu, a náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.

§ 2

Způsob dokládání splnění povinností stanovených v § 6 zákona o elektronickém podpisu

(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty dokládá splnění povinností stanovených v § 6 zákona o elektronickém podpisu těmito dokumenty

a) certifikační politikou,
b) certifikační prováděcí směrnicí,
c) celkovou bezpečnostní politikou,
d) systémovou bezpečnostní politikou,
e) plánem pro zvládání krizových situací a plánem obnovy a

f) odhadem dostatečnosti finančních zdrojů a doklady o tom, že disponuje těmito finančními zdroji.

(2) Obsahem certifikační politiky je zejména

a) stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy, a
b) popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být vydán kvalifikovaný certifikát; kryptografické algoritmy a jejich parametry, které musí být pro tato data použity, jsou uvedeny v příloze č. 1 této vyhlášky.

(3) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty umožňuje trvalý dálkový přístup ke své certifikační politice.

(4) Obsahem certifikační prováděcí směrnice je zejména stanovení postupů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.

(5) Obsahem celkové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(6) Obsahem systémové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění bezpečnosti informačního systému, jehož prostřednictvím poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajišťuje služby spojené s elektronickými podpisy (dále jen „informační systém pro certifikační služby“). Systémová bezpečnostní politika obsahuje zejména

a) způsob uplatnění celkové bezpečnostní politiky ve vztahu k informačnímu systému pro certifikační služby,
b) popis vazeb mezi informačním systémem pro certifikační služby a jinými informačními systémy, které provozuje poskytovatel certifikačních služeb vydávající kvalifikované certifikáty,
c) způsob ochrany dat a jiných prvků informačního systému pro certifikační služby,
d) popis bezpečnostních opatření a
e) vyhodnocení analýzy rizik.

(7) Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku Úřad zveřejňuje ve Věstníku Úřadu.

(8) Obsahem plánu pro zvládání krizových situací je zejména stanovení postupů, které jsou uplatněny v případě mimořádné události. Mimořádnou událostí se pro účely této vyhlášky rozumí událost, která ohrožuje poskytování služeb spojených s elektronickými podpisy a která nastává zejména v důsledku selhání informačního systému nebo výskytu faktoru, který není pod kontrolou poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(9) Obsahem plánu obnovy je zejména stanovení postupů pro obnovu řádné funkce informačního systému pro certifikační služby.

(10) Při zajišťování služeb spojených s elektronickými podpisy poskytovatel certifikačních služeb vydávající kvalifikované certifikáty postupuje podle dokumentů uvedených v odstavci 1 písm. a) až f).

(11) Dostatečností finančních zdrojů je schopnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty finančně zabezpečit řádné provozování služeb spojených s elektronickými podpisy i s ohledem na riziko odpovědnosti za škody.

§ 3

Bezpečnost postupu při vydávání kvalifikovaných certifikátů a provozování seznamu kvalifikovaných certifikátů, které byly zneplatněny

(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje zaručeným elektronickým podpisem kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Tento zaručený elektronický podpis musí být založený na kvalifikovaném certifikátu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

(2) Nástroj elektronického podpisu používaný pro podepisování podle odstavce 1 nelze použít pro jiné účely.

(3) Uvedení do provozu a změna provozního režimu nástroje elektronického podpisu používaného pro podepisování podle odstavce 1 vyžadují, aby je prováděly současně nejméně dvě fyzické osoby, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty.

(4) V případě, že jsou data pro vytváření elektronického podpisu používána pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, nelze je použít pro jiné účely.

(5) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí dostupnost svého kvalifikovaného certifikátu nejméně dvěma na sobě nezávislými způsoby.

(6) Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné.

(7) Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin. Tento údaj obsahuje číslo kvalifikovaného certifikátu unikátní u poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, datum a čas s uvedením hodiny, minuty a sekundy, od kdy byl kvalifikovaný certifikát zneplatněn.

§ 4
Bezpečnost informačního systému pro certifikační služby

(1) Používaný informační systém pro certifikační služby se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost a prokazatelnost jejich původu a pokud odpovídá požadavkům technické normy upravující oblast informační bezpečnosti.[1)]

(2) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí zaznamenávání událostí při

a) vydání kvalifikovaných certifikátů,
b) ukončení platnosti kvalifikovaných certifikátů,
c) nakládání s daty pro vytváření elektronického podpisu a jim odpovídajícími daty pro ověřování elektronického podpisu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty (dále jen „párová data poskytovatele“), a to během jejich celého životního cyklu, a
d) nakládání s kvalifikovaným certifikátem poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, a to během celého životního cyklu tohoto certifikátu.

(3) Záznamy o událostech podle odstavce 2 musí být pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, dostupnosti, integrity, časové autentičnosti a důvěrnosti těchto záznamů.

(4) Prostory, kde dochází k činnosti podle odstavců 1 až 3 a podle § 5 odst. 1, musí být zabezpečeny obdobně jako objekty kategorie „D“ podle zvláštního právního předpisu.[2)]

(5) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) a k) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty pořizuje písemné záznamy o tom, že osoby jím určené k zajišťování služeb spojených s elektronickými podpisy jsou

a) seznamovány v potřebném rozsahu s dokumenty uvedenými v § 2 odst. 1 písm. a) až e) a
b) proškolovány tak, aby jejich odborné předpoklady odpovídaly vykonávané činnosti.

---

1) ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

2) Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.

§ 5
Bezpečnost postupu při nakládání s párovými daty poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty

(1) Při vytváření, používání a uchovávání párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být jakákoliv manipulace s těmito daty prováděna

a) výhradně fyzickými osobami, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty,
b) podle postupů stanovených certifikační prováděcí směrnicí a
c) v souladu se systémovou bezpečnostní politikou.

(2) Při vytváření párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být použity kryptografické algoritmy a jejich parametry, které jsou uvedeny v příloze č. 2 této vyhlášky.

(3) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty je povinen svá data pro vytváření elektronického podpisu zničit po ukončení jejich životního cyklu; o tom pořizuje zápis, který obsahuje

a) popis způsobu zničení dat,
b) datum zničení dat,
c) datum pořízení zápisu a

d) jméno, příjmení a podpis osoby určené poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty k tomu, aby zničení dat zajistila.

(4) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty v případě neoprávněného použití nebo vzniku důvodné obavy ze zneužití svých dat pro vytváření elektronického podpisu užívaných pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, je bezodkladně povinen

a) ukončit platnost svého kvalifikovaného certifikátu, který byl k těmto datům vydán,
b) ukončit platnost kvalifikovaných certifikátů, které byly těmito daty podepsány,
c) zpřístupnit informaci o ukončení platnosti svého kvalifikovaného certifikátu s uvedením důvodu ukončení platnosti, a to nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné, a
d) informovat osoby, které byly dotčeny ukončením platnosti kvalifikovaného certifikátu podle písmene a) o ukončení platnosti jejich kvalifikovaných certifikátů vydaných tímto poskytovatelem certifikačních služeb. V informaci musí být uveden důvod ukončení platnosti kvalifikovaného certifikátu podle písmene a).

§ 6

Ověření bezpečnosti používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují

Požadavek na bezpečnost používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují, se považuje za splněný, pokud je doložen

a) dokumenty uvedenými v § 2 odst. 1 písm. a) až e),
b) výsledkem hodnocení, podle něhož jsou splněny požadavky technické normy upravující oblast informační bezpečnosti,[1)] a
c) písemným posudkem, jehož součástí je potvrzení, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy upravující oblast informační bezpečnosti,[3)] je používání informačního systému pro certifikační služby v souladu se způsoby zajištění bezpečnosti stanovenými v dokumentech uvedených v § 2 odst. 1 písm. c) a d). Kontrola bezpečnostní shody musí být prováděna opakovaně, a to vždy nejpozději do 12 měsíců od provedení poslední kontroly bezpečnostní shody.

[1)] ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

[3)] ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1 – 3.

§ 7

Prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

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

a) byla informována, že používá tento prostředek, a
b) zadala přístupové heslo nebo byl uplatněn jiný obdobný autentizační mechanismus.

(2) Prostředek pro bezpečné vytváření zaručeného elektronického podpisu musí používat kryptografické algoritmy a jejich parametry, které jsou uvedeny v příloze č. 2 této vyhlášky.

(3) Prostředek pro bezpečné vytváření zaručeného elektronického podpisu vyžaduje dostatečnou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek odpovídá požadavkům technické normy upravující oblast informační bezpečnosti.[1)]

(4) Splnění požadavků na prostředek pro bezpečné vytváření zaručeného elektronického podpisu stanovených v § 17 zákona o elektronickém podpisu se dokládá

a) výsledkem hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu a seznamem technických norem upravujících oblast informační bezpečnosti, podle kterých byl hodnocen, a
b) podrobným popisem funkce a technickou dokumentací prostředku pro bezpečné vytváření zaručeného elektronického podpisu.

(5) Požadavky uvedené v odstavcích 2 až 4 musí splňovat rovněž prostředek pro bezpečné ověřování zaručeného elektronického podpisu.

[1)] ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4

§ 8
Náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu

(1) Úřad vyhodnocuje na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

(2) Žádost podle odstavce 1 musí obsahovat

a) podrobný popis funkce a technickou dokumentaci nástroje elektronického podpisu podle odstavce 1 a
b) výsledek hodnocení kryptografických funkcí, které používá nástroj elektronického podpisu podle odstavce 1 a které musí odpovídat požadavkům Úřadu na kryptografické moduly. Tyto požadavky Úřad zveřejňuje ve Věstníku Úřadu. Toto hodnocení zajišťuje zpravidla dodavatel příslušného nástroje elektronického podpisu.

(3) Pokud nástroj elektronického podpisu podle odstavce 1 splňuje požadavky stanovené zákonem o elektronickém podpisu a Úřad vysloví shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, zveřejňuje Úřad ve Věstníku Úřadu.

§ 9
Účinnost

Tato vyhláška nabývá účinnosti dnem vyhlášení.*)

*) *Red. pozn.: tj. 10. října 2001.*

Příloha č. 1 k vyhlášce č. 366/2001 Sb.

Kryptografické algoritmy a jejich parametry pro data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu, a k nimž má být vydán kvalifikovaný certifikát

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	emsa-pss	SHA1
003	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	–	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	–	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	–	SHA1
008	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	MD5
009	RSA	MinModLen=1020	emsa-pss	MD5

Příloha č. 2 k vyhlášce č. 366/2001 Sb.

Kryptografické algoritmy a jejich parametry pro vytváření párových dat poskytovatele a pro prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

Podpisová schémata

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus pro generování klíčů	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	–	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	–	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	–	SHA1

Algoritmy pro generování klíčů

Označení generátoru klíčů	Používané označení	Asymetrický algoritmus	Metoda generování náhodných čísel	Parametry náhodného generátoru
4.01	rsagen1	RSA	trueran	EntropyBits≥128
4.02	dsagen1	DSA	trueran nebo pseuran (FIPS 186-2)	EntropyBits≥128 nebo SeedLen≥128
4.03	ecgen1	ECDSA-F_p nebo ECDSA-$F2^m$	trueran nebo pseuran	EntropyBits≥128 nebo SeedLen≥128

Metody generování náhodných čísel

Označení náhodného generátoru	Používané jméno	Parametry náhodného generátoru
5.01	trueran	EntropyBits
5.02	pseuran	SeedLen
5.03	FIPS 186-2-31	SeedLen
5.04	FIPS 186-2-32	SeedLen

2.3 NAŘÍZENÍ VLÁDY, KTERÝM SE PROVÁDÍ ZÁKON O ELEKTRONICKÉM PODPISU A O ZMĚNĚ NĚKTERÝCH DALŠÍCH ZÁKONŮ (ZÁKON O ELEKTRONICKÉM PODPISU)

Nařízení vlády č. 304/2001 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

Vláda nařizuje k provedení zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu):

§ 1

(1) Pokud ze zvláštních právních předpisů[1)] vyplývá pro orgány veřejné moci povinnost přijmout podání učiněné v elektronické podobě, podepsané elektronicky, anebo stanoví-li zvláštní právní předpis právo orgánů veřejné moci činit úkony v elektronické podobě, podepsané elektronicky, orgány veřejné moci, včetně územních samosprávných celků provádějících výkon státní správy v rámci přenesené působnosti, přijmou k zajištění postupu podle zvláštních právních předpisů tato organizačně technická opatření:

a) zřídí podle povahy a rozsahu své činnosti jedno nebo více pracovišť pro příjem a odesílání datových zpráv (dále jen „elektronická podatelna“), vybavených potřebnými zařízeními připojenými k veřejné datové síti, popřípadě jiným datovým sítím, splňujícími požadavky na technické a programové vybavení podle standardů vydaných Úřadem pro veřejné informační systémy a umožňujícími používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb,
b) pověří v souladu se svým organizačním řádem nebo jiným vnitřním organizačním opatřením zaměstnance vytvářením a ověřováním zaručených elektronických podpisů a vybaví je k tomu potřebnými prostředky a kvalifikovaným certifikátem vydaným akreditovaným poskytovatelem certifikačních služeb na základě smlouvy mezi orgánem veřejné moci a akreditovaným poskytovatelem certifikačních služeb,
c) organizují práce v elektronické podatelně tak, aby bylo zajištěno přijímání a odesílání datových zpráv a neprodlená kontrola, zejména zda přijaté

podání v elektronické podobě je čitelné, zda je podepsala osoba uvedená na kvalifikovaném certifikátu a zda je certifikát platný; při připojení bez nepřetržitého přístupu k veřejné datové síti zajistí, aby k tomuto připojení došlo opakovaně během pracovní doby, a zároveň, aby bylo zjištěno, zda nepřišla elektronická pošta, a současně, aby byla odeslána elektronická pošta připravená k odeslání, a to nejméně na počátku a před koncem pracovní doby,

d) zajistí příjem podání v elektronické podatelně i v případě, že je přímo předáno na technickém nosiči dat,

e) zveřejní elektronické adresy svých elektronických podatelen a seznam kvalifikovaných certifikátů příslušných zaměstnanců nebo elektronické adresy, na nichž se kvalifikované certifikáty nacházejí, a formáty datových zpráv, které jsou způsobilé přijmout, a to na své úřední desce, popřípadě jiným vhodným způsobem, jakož i způsobem umožňujícím dálkový přístup.

(2) Kvalifikovaný certifikát podle odstavce 1 písm. b) obsahuje kromě náležitostí stanovených v § 12 odst. 1 zákona o elektronickém podpisu i označení (název) orgánu veřejné moci, jeho organizačního útvaru a funkce zaměstnance.

(3) Pokud orgán veřejné moci při kontrole podle odstavce 1 písm. c) zjistí, že podání doručené v elektronické podobě nebo jeho část je nečitelné, datová zpráva neobsahuje platný kvalifikovaný certifikát nebo že datová zpráva neobsahuje adresu veřejně přístupného seznamu kvalifikovaných certifikátů a jednoznačné identifikační číslo kvalifikovaného certifikátu, postupuje podle příslušných ustanovení zvláštních právních předpisů upravujících odstraňování vad podání.

[1)] Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.
Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů.
Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

§ 2

Toto nařízení nabývá účinnosti dnem 1. října 2001.

2.4 POŽADAVKY ZVEŘEJNĚNÉ VE VĚSTNÍKU ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ č. 12/2001

Úřad zveřejňuje požadavky podle § 2 odst. 7 a § 8 odst. 2 písm. b) vyhlášky č. 366/2001 Sb.

Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku

Při zpracování dokumentů celková bezpečnostní politika a systémová bezpečnostní politika se postupuje dle požadavků těchto norem:

- ISO 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti
- ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1 – 3.

Požadavky na kryptografické funkce

Výsledek hodnocení kryptografických funkcí, které používá nástroj elektronického podpisu pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, musí odpovídat požadavkům na kryptografické moduly dle:

Standard pro hodnocení bezpečnosti kryptografických modulů vydaný National institute of standards and technology v USA – FIPS PUB 140-1 úroveň 3.

3. ELEKTRONICKÝ PODPIS V EVROPSKÉM SPOLEČENSTVÍ

3.1 SMĚRNICE 1999/93/ES, O ZÁSADÁCH SPOLEČENSTVÍ PRO ELEKTRONICKÉ PODPISY (PRACOVNÍ PŘEKLAD)

Směrnice 1999/93/EC Evropského parlamentu a Rady, o zásadách společenství pro elektronické podpisy

Evropský parlament a Rada Evropské unie,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na čl. 47 odst. 2, články 55 a 95 této smlouvy,
s ohledem na návrh Komise[1)],
s ohledem na stanovisko Hospodářského a sociálního výboru[2)],
s ohledem na stanovisko Výboru regionů[3)],
v souladu s postupem podle článku 251 Smlouvy[4)],
vzhledem k tomu, že

(1) Komise předložila dne 16. dubna 1997 Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení o evropské iniciativě v oblasti elektronického obchodu;
(2) Komise předložila dne 8. října 1997 Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení nazvané „O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – K evropským zásadám pro digitální podpisy a šifrování“;
(3) dne 1. prosince 1997 Rada vyzvala Komisi, aby co nejdříve předložila návrh směrnice Evropského parlamentu a Rady o digitálních podpisech;

[1)] Úř. věst. č. C 325, 23.10.1998, s. 5.
[2)] Úř. věst. č. C 40, 15.2.1999, s. 29.
[3)] Úř. věst. č. C 93, 6.4.1999, s. 33.
[4)] Stanovisko Evropského parlamentu ze dne 13. ledna 1999 (Úř. věst. č. C 104, 14. 4.1999, s. 49), společné stanovisko Rady ze dne 28. června 1999 (Úř. věst. č. C 243, 27. 8.1999, s. 33) a Rozhodnutí Evropského parlamentu ze dne 27. října 1999 (doposud nepublikováno v Úředním věstníku).

(4) elektronická komunikace a obchod vyžadují „elektronické podpisy“ a s nimi související služby umožňující autentizaci dat; rozdíly v předpisech členských států týkajících se právního uznání elektronických podpisů a akreditace poskytovatelů certifikačních služeb by mohly vytvořit vážnou překážku používání elektronické komunikace a elektronického obchodu; vytvoření jasného rámce Společenství, který upraví podmínky vztahující se k elektronickým podpisům, posílí důvěru v nové technologie a jejich obecné uznání; legislativa členských států by neměla bránit volnému pohybu zboží a služeb na vnitřním trhu;
(5) měla by být podporována interoperabilita produktů elektronického podpisu; v souladu s článkem 14 Smlouvy tvoří vnitřní trh oblast bez vnitřních hranic, v jejímž v rámci je zajištěn volný pohyb zboží; musí být splněny základní požadavky, jež jsou specifické v oblasti produktů elektronického podpisu, aby byl zajištěn volný pohyb v rámci vnitřního trhu a vybudována důvěra v elektronické podpisy, aniž by tím bylo dotčeno Nařízení Rady (ES) č. 3381/94 z 19. prosince 1994, kterým se stanoví zásady Společenství pro kontrolu vývozu zboží dvojího užití[5)] a Rozhodnutí Rady 94/942/CFSP z 19. prosince 1994 o společném postupu přijatém Radou týkajícím se kontroly vývozu zboží dvojího užití[6)];
(6) tato směrnice neharmonizuje opatření týkající se služeb v oblasti důvěrných informací, které se řídí právními předpisy o veřejném pořádku nebo veřejné bezpečnosti jednotlivých členských států;
(7) vnitřní trh zajišťuje volný pohyb osob a v důsledku toho občané členských států ES a jiné osoby zde sídlící stále častěji jednají s orgány jiných členských států; dostupnost elektronické komunikace by v tomto ohledu mohla být velice užitečná ;
(8) rychlý technický rozvoj a globální charakter internetu vyžadují přístup otevřený různým technologiím a službám, které umožňují autentizaci dat elektronickou cestou;
(9) elektronické podpisy budou používány v různých situacích a v různých aplikacích, což povede ke vzniku celé škály nových služeb a produktů souvisejících s elektronickými podpisy nebo je využívajících;

[5)] Úř. věst. č. L 367, 31.12.1994, s. 1. Nařízení pozměněné nařízením (ES) č. 837/95 (Úř. věst. č. L 90, 21.4.1995, s. 1).
[6)] Úř. věst. č. L 367, 31.12.1994, s. 8. Nařízení pozměněné rozhodnutím 99/193/CFSP(Úř. věst. č. L 73, 19.3.1999, s. 1).

definice těchto produktů a služeb by neměla být omezena na vydávání certifikátů a jejich správu, ale měla by také zahrnovat ostatní služby a produkty využívající elektronické podpisy nebo s nimi související, jako jsou registrační služby, služby časových značek, adresářové služby, výpočetní služby nebo poradenství v oblasti elektronických podpisů;

(10) vnitřní trh umožňuje poskytovatelům certifikační služby rozvíjet přes hraniční činnost, a tak zvyšovat svoji konkurenceschopnost a nabízet spotřebitelům a podnikům nové příležitosti bezpečné výměny informací a obchodování elektronickou cestou bez ohledu na hranice; poskytovatelé by měli mít možnost poskytovat své služby, aniž by byli k této činnosti autorizováni, aby se tak v rámci Společenství podpořilo poskytování certifikačních služeb prostřednictvím otevřených sítí; autorizací se rozumí nejen jakákoliv autorizace, kterou poskytovatel certifikační služby musí získat od vnitrostátních orgánů před tím, než bude oprávněn poskytovat certifikační služby, ale i jakékoli jiné opatření se stejným účinkem;

(11) dobrovolné akreditační systémy, jejichž cílem je zajištění vyšší úrovně poskytování služeb, mohou poskytovatelům certifikačních služeb nabídnout vhodný rámec pro další rozvoj jejich služeb a pro dosažení úrovně důvěryhodnosti, bezpečnosti a kvality požadované vývojem trhu; uvedené systémy by měly podpořit mezi poskytovateli certifikačních služeb rozvoj „best practice“; mělo by být ponecháno na poskytovatelích certifikačních služeb, zda budou vstupovat do těchto akreditačních systémů a využívat je;

(12) certifikační služby mohou nabízet buď veřejnoprávní subjekty nebo právnické či fyzické osoby, které jsou založeny v souladu s vnitrostátními právními předpisy; členské státy by neměly bránit poskytovatelům certifikačních služeb, aby působili mimo rámec dobrovolných akreditačních systémů; mělo by být zajištěno, aby tyto akreditační systémy neomezovaly soutěž v oblasti certifikačních služeb;

(13) členské státy si mohou zvolit způsob, jakým zajistí dohled nad dodržováním této směrnice; tato směrnice nevylučuje vytvoření systému dohledu na bázi soukromého sektoru; tato směrnice nezavazuje poskytovatele certifikačních služeb, aby se nacházeli pod dohledem jakéhokoli platného akreditačního systému;

(14) je důležité, aby bylo dosaženo rovnováhy mezi potřebami spotřebitelů a výrobců;

(15) příloha III obsahuje požadavky na prostředky pro bezpečné vytváření podpisů tak, aby byla zajištěna funkčnost zaručených elektronických podpisů; nepokrývá celý systém prostředí, ve kterém se tyto prostředky používají; fungování vnitřního trhu vyžaduje, aby Komise a členské státy jednaly rychle a umožnily tak ustanovení subjektů, které budou pověřeny vyhodnocování shody prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III; pro splnění požadavků trhu je nezbytné, aby vyhodnocování shody bylo prováděno včas a efektivně;

(16) tato směrnice přispívá k používání a k právnímu uznání elektronických podpisů v rámci Společenství; pro elektronické podpisy používané výlučně v systémech, které jsou provozovány na základě dobrovolných dohod uzavřených podle soukromého práva určitým počtem účastníků, není nezbytný regulační rámec; v mezích stanovených vnitrostátními předpisy je nezbytné respektovat svobodu smluvních stran sjednávat si mezi sebou podmínky uznávání elektronických podpisů; měla by být uznána právní účinnost elektronických podpisů používaných v takových systémech a jejich přípustnost jako důkazů v soudním řízení;

(17) cílem této směrnice není harmonizace vnitrostátních právních předpisů týkajících se smluvních vztahů, zejména uzavírání a realizace smluv, ani jiných náležitostí nesmluvní podstaty týkajících se podpisů; z tohoto důvodu je nezbytné, aby se ustanovení o právních účincích elektronických podpisů nedotkla požadavků na formu, které upravují vnitrostátní právní předpisy pro uzavírání smluv, ani pravidel upravujících místo uzavření smlouvy;

(18) uchovávání a kopírování dat pro vytváření podpisů by mohlo ohrozit právní platnost elektronických podpisů;

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

(20) harmonizovaná kritéria týkající se právních účinků elektronických podpisů budou zárukou jednotného právního rámce Společenství; vnitrostátní právní předpisy upravují různé požadavky týkající se právní platnosti vlastnoručních podpisů; pro potvrzení totožnosti osoby, která se elektronicky podepisuje, lze použít certifikáty; zaručené

elektronické podpisy založené na kvalifikovaných certifikátech vedou k zajištění vyšší úrovně bezpečnosti; zaručené elektronické podpisy založené na kvalifikovaných certifikátech a vytvořené prostředky pro bezpečné vytváření podpisů lze z právního hlediska považovat za rovnocenné vlastnoručním podpisům pouze za předpokladu, že jsou naplněny požadavky na vlastnoruční podpisy;

(21) aby došlo k obecnému přijetí elektronických autentizačních metod, je třeba zajistit, aby elektronické podpisy mohly být ve všech členských státech používány jako důkazy v soudním řízení; právní uznání elektronických podpisů by mělo být založeno na objektivních kritériích a nemělo by záviset na autorizaci poskytovatelů certifikačních služeb; vnitrostátní právní předpisy vymezí právní oblasti, ve kterých lze používat elektronické dokumenty a elektronické podpisy; touto směrnicí nejsou dotčeny pravomoci vnitrostátního soudu rozhodovat o souladu s požadavky této směrnice ani vnitrostátní předpisy o volném právním hodnocení důkazů;

(22) poskytovatelé certifikačních služeb, kteří poskytující certifikační služby veřejnosti, podléhají vnitrostátním právním předpisům o odpovědnosti;

(23) rozvoj mezinárodního elektronického obchodu vyžaduje uzavírání přes hraničních dohod týkajících se třetích států; pro zajištění interoperabilty na globální úrovni bude výhodné uzavírat se třetími státy dohody o mnohostranných pravidlech v oblasti vzájemného uznávání certifikačních služeb;

(24) pro zvýšení důvěry uživatelů v elektronickou komunikaci a elektronický obchod je nezbytné, aby poskytovatelé certifikačních služeb dodržovali právní předpisy o ochraně dat a soukromí jednotlivců;

(25) ustanovení o používání pseudonymů v certifikátech by neměla bránit členským státům, aby vyžadovaly ověřování totožnosti osob podle vnitrostátních právních předpisů či právních předpisů Společenství;

(26) opatření nezbytná pro zavedené této směrnice jsou přijímána v souladu s Rozhodnutím Rady 1999/468/ES z 28. června 1999 o postupech pro výkon prováděcích pravomocí svěřených Komisi[7)];

[7)] OJ L 184, 17. 7. 1999, p. 23.

(27) dva roky po zavedení této směrnice ji Komise přezkoumá, aby se mimo jiné přesvědčila, že vývoj technologií nebo změny v právním prostředí nevytvořily překážky pro dosažení cílů v této směrnici stanovených; Komise by měla přezkoumat vliv na související technické oblasti a předložit zprávu Evropskému parlamentu a Radě;

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

Přijaly tuto směrnici:

Článek 1
Působnost

Účelem této směrnice je umožnit použití elektronických podpisů a přispět k jejich právnímu uznávání. Aby bylo možné zajistit řádné fungování vnitřního trhu, stanovuje tato směrnice právní rámec pro elektronické podpisy a některé certifikační služby.

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

Článek 2
Definice

Pro účely této směrnice:

(1) „elektronickým podpisem“ se rozumí data v elektronické podobě, která jsou připojena k jiným elektronickým datům nebo jsou s nimi logicky spojena a která slouží jako metoda autentizace;

(2) „zaručeným elektronickým podpisem*)“ se rozumí elektronický podpis, který splňuje tyto požadavky:
  (a) je jednoznačně spojen s podepisující osobou;
  (b) umožňuje identifikovat podepisující osobu;
  (c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou;
  (d) je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoliv následnou změnu těchto dat;

(3) „podepisující osobou“ se rozumí jakákoliv osoba, která má prostředek pro vytváření podpisu a která jedná svým jménem nebo jménem jiné fyzické nebo právnické osoby nebo subjektu, který zastupuje;

(4) „daty pro vytváření podpisu“ se rozumí jedinečná data, jako jsou kódy nebo soukromé kryptografické klíče, která podepisující osoba používá k vytváření elektronického podpisu;

(5) „prostředkem pro vytváření podpisu“ se rozumí konfigurovaný software nebo hardware používaný k implementaci dat pro vytváření podpisu;

(6) „prostředkem pro bezpečné vytváření podpisu“ se rozumí prostředek pro vytváření podpisu, který splňuje požadavky uvedené v příloze III;

(7) „daty pro ověřování podpisu“ se rozumí data, jako jsou kódy nebo veřejné kryptografické klíče, která se používají pro ověřování elektronického podpisu;

(8) „prostředkem pro ověřování podpisu“ se rozumí konfigurovaný software nebo hardware používaný k implementaci dat pro ověřování podpisu;

(9) „certifikátem“ se rozumí elektronické osvědčení, které spojuje data pro ověřování podpisu s určitou osobou a potvrzuje identitu této osoby;

(10) „kvalifikovaným certifikátem“ se rozumí certifikát, který splňuje požadavky uvedené v příloze I a je vydán poskytovatelem certifikačních služeb, který splňuje požadavky uvedené v příloze II;

(11) „poskytovatelem certifikačních služeb“ se rozumí subjekt nebo právnická či fyzická osoba, která vydává certifikáty nebo poskytuje jiné služby spojené s elektronickými podpisy;

(12) „produktem elektronického podpisu“ se rozumí hardware nebo software, nebo jejich součásti, který je určen k tomu, aby jej poskytovatel certifikačních služeb používal pro zajištění služeb vztahujících se k elektronickým podpisům nebo který je určen pro vytváření nebo ověřování elektronických podpisů;

(13) „dobrovolnou akreditací“ se rozumí jakákoliv autorizace, která stanoví zvláštní práva a povinnosti pro poskytování certifikačních služeb a kterou uděluje na žádost dotčeného poskytovatele certifikačních služeb veřejnoprávní či soukromý subjekt pověřený stanovením těchto práv a povinností a dohledem nad jejich dodržováním, přičemž poskytovatel certifikačních služeb není oprávněn vykonávat práva vyplývající z autorizace, dokud neobdrží rozhodnutí od tohoto subjektu.

*) V originálu "advanced electronic signature", pojem „zaručený elektronický podpis“ je použit v zákonu o elektronickém podpisu.

Článek 3
Přístup na trh

1. Členské státy nebudou poskytování certifikačních služeb podmiňovat autorizací.
2. Aniž by tím bylo dotčeno ustanovení odstavce 1, mohou členské státy zavést nebo ponechat v platnosti dobrovolné akreditační systémy, jejichž cílem je zvýšit úroveň zajišťování certifikačních služeb. Veškeré podmínky spojené s těmito systémy musí být objektivní, transparentní, úměrné a nediskriminační. Členské státy nesmí omezovat počet akreditovaných poskytovatelů certifikačních služeb z důvodů, které spadají do působnosti této směrnice.
3. Každý členský stát zajistí zavedení odpovídajícího systému, který umožní dohled nad poskytovateli certifikačních služeb, kteří vydávají kvalifikované certifikáty pro veřejnost a mají sídlo na jeho území.
4. Příslušné veřejnoprávní či soukromé subjekty pověřené členskými státy stanoví shodu prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III. V souladu s postupem uvedeným v článku 9 stanoví Komise kritéria, podle nichž členské státy stanoví, zda může být daný subjekt pověřen.

   Rozhodnutí subjektů, které jsou uvedeny v prvním pododstavci, o shodě s požadavky uvedenými v příloze III uznají všechny členské státy.
5. Komise může v souladu s postupem uvedeným v článku 9 stanovit a zveřejnit v Úředním věstníku Evropských společenství referenční čísla obecně uznávaných standardů pro produkty elektronického podpisu. Pokud produkt elektronického podpisu splňuje tyto standardy, předpokládají členské státy, že rovněž existuje shoda s požadavky uvedenými v příloze II, bodě f) a v příloze III.

6. Členské státy a Komise spolupracují při podpoře rozvoje a používání prostředků pro ověřování podpisu s ohledem na doporučení pro bezpečné ověřování uvedené v příloze IV a v zájmu spotřebitele.
7. Členské státy mohou používání elektronických podpisů ve veřejnoprávním sektoru podmínit případnými doplňujícími požadavky. Tyto požadavky musí být objektivní, transparentní, úměrné a nediskriminační a musí se vztahovat výlučně na specifické vlastnosti daného použití. Tyto podmínky nesmějí vytvářet překážky pro přes hraniční služby.

Článek 4
Zásady vnitřního trhu

1. Každý členský stát bude pro poskytovatele certifikačních služeb se sídlem na svém území a pro služby, které poskytují, uplatňovat vnitrostátní předpisy, které přijme v souladu s touto směrnicí. Členské státy nesmí v oblastech, na které se vztahuje tato směrnice, omezovat poskytování certifikačních služeb pocházejících z jiného členského státu.
2. Členské státy umožní volný oběh produktů elektronického podpisu, které jsou v souladu s touto směrnicí, na vnitřním trhu.

Článek 5
Právní účinky elektronických podpisů

1. Členské státy zajistí, aby zaručené elektronické podpisy založené na kvalifikovaných certifikátech a vytvořené pomocí prostředků pro bezpečné vytváření podpisu:
   (a) splňovaly právní požadavky na podpis ve vztahu k datům v elektronické podobě stejně, jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k datům na papíře; a
   (b) byly přijímány jako důkazy v soudním řízení.
2. Členské státy zajistí, aby elektronickým podpisům nebyla odpírána právní účinnost a aby nebyly odmítány jako důkazy v soudním řízení pouze z toho důvodu, že:
   - jsou v elektronické podobě, nebo
   - nejsou založeny na kvalifikovaném certifikátu, nebo
   - nejsou založeny na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb, nebo
   - nejsou vytvořeny pomocí prostředku pro bezpečné vytváření podpisu.

Článek 6
Odpovědnost

1. Členské státy zajistí, aby poskytovatel certifikačních služeb, který vydá pro veřejnost certifikát jako kvalifikovaný certifikát nebo který se veřejnosti za takový certifikát zaručí, byl odpovědný za škodu způsobenou jakémukoliv subjektu nebo právnické či fyzické osobě, která se na tento certifikát důvodně spoléhá, a to přinejmenším:
   (a) pokud jde o přesnost veškerých informací obsažených v kvalifikovaném certifikátu v době jeho vydání a o uvedení veškerých předepsaných údajů pro kvalifikovaný certifikát;
   (b) pokud jde o ujištění, že v době vydání certifikátu měla podepisující osoba uvedená v kvalifikovaném certifikátu data pro vytváření podpisu odpovídající datům pro ověřování podpisu, která jsou uvedena v certifikátu nebo z něj identifikovatelná;
   (c) pokud jde o ujištění, že data pro vytváření podpisu a data pro ověřování podpisu mohou být použita doplňujícím způsobem v těch případech, kdy poskytovatel certifikačních služeb generuje oboje tato data;

   ledaže poskytovatel certifikačních služeb prokáže, že nejednal nedbale.
2. Členské státy přinejmenším zajistí, aby poskytovatel certifikačních služeb, který vydá certifikát jako kvalifikovaný certifikát, byl odpovědný za škody způsobené kterémukoliv subjektu nebo právnické či fyzické osobě, které se na tento certifikát důvodně spoléhají, pokud opomene zaregistrovat revokaci certifikátu, ledaže poskytovatel certifikačních služeb prokáže, že nejednal nedbale.
3. Členské státy zajistí, aby poskytovatel certifikačních služeb mohl v kvalifikovaném certifikátu uvést omezení pro jeho použití za předpokladu, že omezení je rozpoznatelné třetími stranami. Poskytovatel certifikačních služeb není odpovědný za škody vyplývající z použití kvalifikovaného certifikátu, které přesahuje omezení v něm uvedená.
4. Členské státy zajistí, aby poskytovatel certifikačních služeb mohl v kvalifikovaném certifikátu uvést omezení hodnoty transakce, pro kterou lze certifikát použít za předpokladu, že omezení je rozpoznatelné třetími stranami.

   Poskytovatel certifikačních služeb není odpovědný za škody vyplývající z překročení tohoto maximálního omezení.

5. Ustanovením odstavců 1 až 4 není dotčena Směrnice Rady 93/13/EHS z 5. dubna 1993 o nerovných podmínkách ve spotřebitelských smlouvách (o zneužití postavení ve spotřebitelských smlouvách)[8].

Článek 7
Mezinárodní hlediska

1. Členské státy zajistí, aby certifikáty, které poskytovatel certifikačních služeb se sídlem ve třetím státu vydá jako kvalifikované certifikáty, byly uznávány jako právně rovnocenné certifikátům vydaným poskytovatelem certifikačních služeb se sídlem ve Společenství, pokud:
   (a) poskytovatel certifikačních služeb splňuje podmínky uvedené v této směrnici a byl akreditován v rámci dobrovolného akreditačního systému ustanoveného v členském státě; nebo
   (b) poskytovatel certifikačních služeb se sídlem ve Společenství, který splňuje podmínky uvedené v této směrnici, se za tento certifikát zaručí; nebo
   (c) certifikát nebo poskytovatel certifikačních služeb je uznáván na základě dvoustranné nebo mnohostranné dohody mezi Společenstvím a třetími státy nebo mezinárodními organizacemi.
2. S cílem usnadnit přes hraniční certifikační služby s třetími státy a právní uznání zaručených elektronických podpisů pocházejících ze třetích států učiní Komise v oblastech, kde je to vhodné, návrhy vedoucí k efektivní implementaci standardů a mezinárodních dohod vztahujících se k certifikačním službám. V případě potřeby předloží Radě návrhy na odpovídající zmocnění pro jednání o dvoustranných a mnohostranných dohodách se třetími státy a mezinárodními organizacemi. Rada rozhoduje kvalifikovanou většinou.
3. Kdykoliv bude Komise informována o obtížích s přístupem na trh třetích států, může předložit Radě návrhy na udělení odpovídajícího zmocnění pro vyjednávání srovnatelných práv pro působení Společenství v těchto třetích státech. Rada se usnáší kvalifikovanou většinou.

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

[8] Úř. věst. č. L 95, 21.4.1993, s. 29.

Článek 8
Ochrana dat

1. Členské státy zajistí, aby poskytovatelé certifikačních služeb a vnitrostátní subjekty odpovědné za akreditaci nebo dohled plnily požadavky stanovené ve směrnici Evropského parlamentu a Rady 95/46/ES z 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[9].
2. Členské státy zajistí, aby poskytovatel certifikačních služeb, který vydává certifikáty pro veřejnost, mohl shromažďovat osobní údaje získané pouze přímo od dotčené osoby nebo s jejím výslovným souhlasem a pouze v rozsahu nezbytném pro vydání a správu certifikátu. Pro jiné účely nelze údaje shromažďovat ani zpracovávat bez výslovného souhlasu dotčené osoby.
3. Aniž jsou dotčeny právní účinky přiznané vnitrostátními předpisy pseudonymům, nesmějí členské státy bránit poskytovatelům certifikačních služeb, aby v certifikátu namísto jména podepisující osoby uvedli pseudonym.

Článek 9
Výbor

1. Komisi je nápomocen Výbor pro elektronický podpis, dále nazývaný „Výbor“.
2. Odkazuje-li se na toto ustanovení, použijí se články 4 a 7 Rozhodnutí 1999/468/ES s ohledem na článek 8 uvedeného rozhodnutí.

   Doba uvedená v čl. 4 odst. 3 Rozhodnutí 1999/468/ES je tři měsíce.
3. Výbor přijme svůj jednací řád.

Článek 10
Cíle výboru

Výbor objasní požadavky uvedené v přílohách této směrnice, kritéria uvedená v čl. 3 odst. 4 a všeobecně uznávané standardy pro produkty elektronického podpisu stanovené a zveřejněné v souladu s čl. 3 odst. 5, a to v souladu s postupem uvedeným v čl. 9 odst. 2.

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

Článek 11
Oznámení

1. Členské státy oznámí Komisi a ostatním členským státům:
   (a) informace o dobrovolných akreditačních systémech na vnitrostátní úrovni, včetně veškerých doplňujících požadavků podle čl. 3 odst. 7;
   (b) názvy a sídla vnitrostátních orgánů odpovědných za akreditaci a dohled, jakož i subjektů uvedených v čl. 3 odst. 4;
   (c) názvy a sídla všech vnitrostátních akreditovaných poskytovatelů certifikačních služeb.
2. Členské státy oznámí veškeré informace uvedené v odstavci 1 co nejdříve, což platí i pro případné změny.

Článek 12
Přezkoumání

1. Komise přezkoumá působení této směrnice a podá o něm zprávu Evropskému parlamentu a Radě nejpozději do 19. července 2003.
2. V rámci přezkoumání lze mimo jiné stanovit, zda je vhodné změnit působnost této směrnice s přihlédnutím k rozvoji techniky, trhu a právního rámce. Zpráva bude obsahovat na základě získaných zkušeností zejména zhodnocení hledisek týkajících se harmonizace. V případě potřeby budou ke zprávě připojeny legislativní návrhy.

Článek 13
Realizace

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

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

Článek 14
Nabytí účinnosti

Tato směrnice nabývá účinnosti dnem vyhlášení v Úředním věstníku Evropských společenství.

Článek 15
Určení

Tato směrnice je určena členským státům.

V Bruselu dne 13. prosince 1999

Příloha I

Požadavky na kvalifikované certifikáty

Kvalifikované certifikáty musí obsahovat:

(a) označení, že certifikát je vydán jako kvalifikovaný certifikát;
(b) označení poskytovatele certifikačních služeb a státu, ve kterém má poskytovatel sídlo;
(c) jméno podepisující osoby nebo pseudonym, který je jako takový označen;
(d) zvláštní znaky podepisující osoby, pokud jsou důležité pro účel, pro nějž je certifikát určen;
(e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, která jsou pod kontrolou podepisující osoby;
(f) označení počátku a konce doby platnosti certifikátu;
(g) identifikační kód certifikátu;
(h) zaručený elektronický podpis poskytovatele certifikačních služeb, který certifikát vydává;
(i) případně omezení použitelnosti certifikátu; a
(j) případně omezení hodnot transakcí, pro něž lze certifikát použít.

Příloha II

Požadavky na poskytovatele certifikačních služeb, kteří vydávají kvalifikované certifikáty

Poskytovatelé certifikačních služeb musí:

(a) prokázat spolehlivost nezbytnou pro poskytování certifikačních služeb;

(b) zajistit provozování rychlého a bezpečného seznamu a bezpečné a okamžité revokační služby;

(c) zajistit, aby datum a čas, kdy je certifikát vydán nebo revokován, mohly být přesně určeny;

(d) ověřit odpovídajícími prostředky v souladu s vnitrostátními právními předpisy totožnost a případně zvláštní znaky osoby, které je kvalifikovaný certifikát vydáván;

(e) zaměstnávat personál, který má odborné znalosti, zkušenosti a kvalifikaci nezbytné pro poskytování služeb, zejména schopnosti řízení, odborné znalosti v oblasti technologie elektronických podpisů a důkladnou znalost příslušných bezpečnostních postupů; rovněž musí používat adekvátní administrativní a řídící postupy, které odpovídají uznávaným standardům a jsou s nimi ve shodě;

(f) používat důvěryhodné systémy a produkty, které jsou chráněny proti modifikacím, a zajistit technickou a kryptografickou bezpečnost postupů, které tyto systémy a produkty podporují;

(g) přijmout opatření proti padělání certifikátů a pokud poskytovatel certifikačních služeb generuje data pro vytváření podpisu, zajistit jejich utajení v průběhu generování těchto dat;

(h) mít k dispozici dostatečné finanční zdroje na provoz v souladu s požadavky uvedenými v této směrnici, a zejména k tomu, aby mohl nést odpovědnost za vzniklé škody, např. uzavřením vhodného pojištění;

(i) zaznamenávat veškeré informace vztahující se ke kvalifikovaným certifikátům a uchovávat je po přiměřenou dobu, především pro potřeby poskytnutí důkazu o certifikaci pro účely soudního řízení. Záznamy mohou být v elektronické podobě;

(j) neuchovávat ani nekopírovat data pro vytváření podpisu osoby, které poskytovatel certifikačních služeb poskytl službu klíčového hospodářství;

(k) před uzavřením smluvního vztahu s osobou, která požaduje certifikát na podporu svého elektronického podpisu, informovat tuto osobu pomocí komunikačních prostředků umožňujících trvalý dálkový přístup

o přesných lhůtách a podmínkách použití certifikátu, včetně veškerých omezení stanovených pro jeho použití, o existenci dobrovolného akreditačního systému a o postupech při řešení reklamací a sporů. Tyto informace, které lze předat elektronickou cestou, musí mít písemnou podobu a musí být ve snadno srozumitelném jazyce. Příslušné části těchto informací musí být na vyžádání k dispozici třetím stranám, které se spoléhají na tento certifikát;

(l) používat důvěryhodný systém pro uchovávání certifikátů v ověřitelné podobě takovým způsobem, aby:
- vstupy a změny mohly provádět pouze pověřené osoby,
- bylo možno kontrolovat autentičnost informací,
- certifikáty byly veřejně přístupné pro vyhledávání pouze tehdy, pokud k tomu držitel certifikátu poskytl souhlas a
- operátorovi byly zjevné jakékoliv technické změny porušující tyto bezpečnostní požadavky.

Příloha III

Požadavky na prostředek pro bezpečné vytváření podpisu

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

(a) se data pro vytváření podpisu používaná pro generování podpisu mohla vyskytnout pouze jedenkrát a aby bylo dostatečně zajištěno jejich utajení;

(b) bylo dostatečně zajištěno, že data pro vytváření podpisu používaná pro generování podpisu nelze odvodit a že podpis je chráněn současnou dostupnou technologií proti padělání ;

(c) podepisující osoba měla možnost svá data pro vytváření podpisu používaná pro generování podpisu spolehlivě chránit proti jejich zneužití třetí osobou.

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

Příloha IV

Doporučení pro bezpečné ověřování podpisu

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

(a) data používaná pro ověřování podpisu odpovídala datům zobrazeným ověřovateli;
(b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl správně zobrazen;
(c) ověřovatel mohl, podle potřeby, spolehlivě zjistit obsah podepsaných dat;
(d) bylo možno spolehlivě ověřit pravost a platnost certifikátu nezbytného v době ověřování podpisu;
(e) výsledek ověření a identita podepisující osoby byly správně zobrazeny;
(f) použití pseudonymu bylo jasně označeno; a
(g) všechny změny ovlivňující bezpečnost mohly být odhaleny.

3.2 PŘEHLED SOUČASNÉ PRÁVNÍ ÚPRAVY ELEKTRONICKÉHO PODPISU V ČLENSKÝCH STÁTECH ES

Evropský parlament a Rada přijaly v prosinci roku 1999 Směrnici 1999/93/ES, o zásadách Společenství pro elektronické podpisy. Tento dokument ukládá členským státům Evropské unie přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí (požadavky na právní akceptovatelnost e-podpisu, vytvoření dobrovolných akreditačních schémat, vzájemné uznávání certifikátů apod.). Termín, do kdy měly být tyto zásady v jednotlivých právních systémech implementovány, byl 19. červenec 2001. Jaký je (byl k 1. 11. 2001) skutečný stav, vyplývá z přehledové tabulky na následující straně.

Stát	Datum	Právní úprava	Pracovní překlad
Belgie	20.10.2000 14.6.2001	Law introducing means of electronic signature into the legal procedure Draft Law on certification services	Zákon o změně základních právních předpisů v souvislosti s elektronickým podpisem Návrh zákona o certifikačních službách
Dánsko	31.5. 2000	Electronic Signature Act	Zákon o elektronickém podpisu
Finsko	2000 8.3.2001	The Act on Electronic Service in the Administration Electronic Signature Act	Zákon o elektronické službě v administrativě. Zákon o elektronickém podpisu
Francie	13.3.2000 30.3.2001	Act adapting the right on proof and evidence to information technologies and on electronic signature Decree for the application of article 1316-4 of the civil code and relating to the signature electronic	Zákon o elektronickém podpisu a o změně norem důkazního práva Vyhláška k aplikaci článku 1316-4 občanského zákoníku v souvislosti s elektronickým podpisem
Holandsko	17.5.2001 12.1.2001	Draft Act on electronic signature Development plan of internet commerce	Návrh zákona o elektronickém podpisu Plán rozvoje internetového obchodu
Irsko	20.8.2000	Electronic Commerce Act	Zákon o elektronickém obchodu
Itálie	15.3.1997 10.11.1997 8.2.1999	Law on public administration Presidential decree concerning the creation, storage and transmission of digital documents by means of computer-based systems The Technical rules for creation, storage and transmission of digital documents in the sense of the Presidential decree no. 513/97	Zákon o veřejné administrativě Prezidentská vyhláška o tvorbě, ukládání a výměně elektronických dokumentů Technická pravidla pro tvorbu, ukládání a výměnu elektronických dokumentů ve smyslu Prezidentské vyhlášky číslo 513/97
Lucembursko	14.8. 2000 1.1.2001	Electronic Commerce Law Order relating to the electronic signatures, the electronic payment and the creation of the committee for electronic commerce	Zákon o elektronickém obchodu Nařízení vlády vztahující se k elektronickému podpisu, elektronickým platbám a vytvářející komisi pro elektronický obchod
Německo	2001	Law Governing Framework Conditions for Electronic Signatures and Amending Other regulations	Zákon upravující základní podmínky elektronického podpisu a o změně některých dalších předpisů
Portugalsko	2.8. 1999 25.8.1999 25.9.2000 29.8.2000	Digital Signature law Resolution of the Council of Ministers Law on accreditation authority Administrative Rule on civil liability insurance of certification agencies	Zákon o digitálním podpisu Rezoluce rady ministrů Zákon o dozoru a akreditaci PCS Nařízení o povinném pojištění PCS
Rakousko	1.1.2000 2.2. 2000	Federal Electronic Signature Law Electronic Signature order	Federální zákon o elektronickém podpisu Nařízení k federálnímu zákonu o elektronickém podpisu
Řecko	28.9.1999	Draft Presidential Decree on electronic signatures and related certification services	Návrh vyhlášky Prezidenta republiky o elektronických podpisech a certifikačních službách
Španělsko	17.9.1999 21.2.2000	Royal Decree on Digital Signatures Order on regulation of accreditation and certification	Královský zákon o digitálních podpisech Nařízení o regulaci akreditace PCS a certifikaci produktů pro PCS
Švédsko	1.1.2001	The Act on Qualified Electronic Signatures	Zákon o kvalifikovaných elektronických podpisech
Velká Británie	25.5.2000	The Electronic Communications Act	Zákon o elektronické komunikaci

Informace byly převzaty z interní studie Úřadu pro ochranu osobních údajů (ÚOOÚ), kterou připravil Bc. Jan Hobza a jejíž podstatná část je dostupná na Internetové adrese Úřadu (http://www.uoou.cz).

4. KOMENTÁŘ A VÝKLAD K VYHLÁŠCE č. 366/2001 Sb.

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

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

§ 1
Předmět úpravy

Tato vyhláška upřesňuje podmínky stanovené v § 6 a 17 zákona o elektronickém podpisu a způsob, jakým se jejich splnění bude dokládat, a požadavky, které musí splňovat nástroje elektronického podpisu, a náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu s těmito požadavky.

Komentář

Předmět úpravy je stanoven podle § 20 zákona o elektronickém podpisu, který obsahuje zmocnění pro Úřad pro ochranu osobních údajů (dále jen „Úřad“) k vydání vyhlášky, jejíž základní rámec je vymezen obsahem tohoto ustanovení. Předmět úpravy, který je obsahem § 1 vyhlášky, vychází nejen ze zmocňovacího § 20 zákona o elektronickém podpisu, ale navazuje na § 6 a 17 zákona o elektronickém podpisu. Obsahem § 6 zákona o elektronickém podpisu jsou povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty. K jeho provedení směřují ve vyhlášce § 2 až 6. Obsahem § 17 zákona o elektronickém podpisu jsou požadavky na prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů. K jeho provedení směřuje ve vyhlášce § 7.

§ 2
Způsob dokládání splnění povinností stanovených v § 6 zákona o elektronickém podpisu

(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty dokládá splnění povinností stanovených v § 6 zákona o elektronickém podpisu těmito dokumenty

a) certifikační politikou,
b) certifikační prováděcí směrnicí,
c) celkovou bezpečnostní politikou,
d) systémovou bezpečnostní politikou,
e) plánem pro zvládání krizových situací a plánem obnovy a
f) odhadem dostatečnosti finančních zdrojů a doklady o tom, že disponuje těmito finančními zdroji.

Komentář

Výčet dokumentů uvedených v odstavci 1 je způsob, jakým zákon očekává (stanoví) splnění povinností, které poskytovateli certifikačních služeb vydávajícímu kvalifikované certifikáty (dále jen „poskytovatel“) ukládá zákon o elektronickém podpisu v § 6. Dokumenty uvedené pod písmeny a) až e) jsou vždy (v mezinárodním kontextu) vyžadovány při poskytovatelem zajišťovaných službách spojených s elektronickými podpisy, dokumenty uvedené pod písmeny c) až f) vycházejí z příslušných ustanovení zákona o elektronickém podpisu, která od poskytovatele certifikačních služeb očekávají naplnění a doložení některých základních předpokladů pro výkon této činnosti. V těchto dokumentech poskytovatel deklaruje, jaké služby a jakým způsobem hodlá zajišťovat, jak bude zajištěna celková bezpečnost vnitřní (struktury) organizace poskytovatele a v jejím rámci bezpečnost informačního systému zajišťujícího služby spojené s elektronickými podpisy, jaké postupy budou uplatněny v případě mimořádných událostí a jaké postupy budou užity pro případ nutnosti obnovení řádné funkce informačního systému zajišťujícího služby spojené s elektronickými podpisy. Popis veškerých těchto skutečností je z hlediska Úřadu nezbytný pro možnost časově neomezeného sledování, zda bude v praxi poskytovatelem postupováno vždy tak, jak bylo předem stanoveno s cílem dosažení nejvyšší možné míry bezpečnosti; jedná se o sledování jak ze strany poskytovatele, tak Úřadu při výkonu dozoru; v případě certifikační politiky, která se bude zveřejňovat, i jednotlivými osobami, které budou služby využívat.

(2) Obsahem certifikační politiky je zejména

a) stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy, a

b) popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být vydán kvalifikovaný certifikát; kryptografické algoritmy a jejich parametry, které musí být pro tato data použity, jsou uvedeny v příloze č. 1 této vyhlášky.

Komentář

Dokument certifikační politika je základním dokumentem charakterizujícím zásadní východiska pro činnost poskytovatele. V praxi se pro zpracování certifikační politiky používá nejčastěji jako metodický návod dokument RFC 2527 Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. Vzhledem k tomu, že vyhláška blíže nestanoví strukturu dokumentu certifikační politika, Úřad vydal její doporučenou osnovu. Tato doporučená osnova je již v současné době předávána zájemcům z řad poskytovatelů certifikačních služeb.

Předpokládá se, že obsahem certifikační politiky musí být zejména:

- *kontakty na registrační autority,*
- *kontakty na poskytovatele certifikačních služeb,*
- *povinnosti jednotlivých subjektů (registrační autority, poskytovatele certifikačních služeb, žadatele),*
- *odpovědnost za škodu,*
- *poplatky za služby spojené se správou certifikátů,*
- *za služby spojené se správou certifikátů, přístup ke zveřejňovaným informacím (seznam všech vydaných kvalifikovaných certifikátů, seznam kvalifikovaných certifikátů, které byly zneplatněny),*
- *zásady ochrany informací,*
- *informace o auditu,*
- *způsob ověření vazby mezi daty na vytváření a ověření elektronického podpisu žadatele,*
- *způsob prokázání identity fyzické osoby žadatele,*
- *vzor žádosti o vydání kvalifikovaného certifikátu,*
- *podmínky pro vydání a převzetí kvalifikovaného certifikátu,*
- *vzor žádosti o ukončení platnosti kvalifikovaného certifikátu,*
- *obecné bezpečnostní mechanizmy pro oblasti fyzické, procedurální a personální bezpečnosti,*

- *způsob distribuce kvalifikovaného certifikátu poskytovatele klientům,*
- *seznam položek v kvalifikovaném certifikátu (povinné, doporučené, možné),*
- *způsob dokládání informací zapsaných v kvalifikovaném certifikátu atd.*

Nedílnou a důležitou součástí certifikační politiky musí být i popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu (viz § 6 odst. 1 písm. d) zákona o elektronickém podpisu), která si vytváří osoba žádající o vydání kvalifikovaného certifikátu, a k nimž má být vydán kvalifikovaný certifikát.

Obsahem vyhlášky je vymezení (s odkazem na přílohu č. 1) kryptografických algoritmů a jejich parametrů, které jsou mezinárodně používány a považovány za bezpečné pro tyto účely. Stanovení přípustných kryptografických algoritmů a jejich parametrů je nezbytné pro možnost uznávání elektronických podpisů a kvalifikovaných certifikátů za hranice jednotlivých států. Poskytovatel musí vymezit ve své certifikační politice, jaké algoritmy, včetně podmínek na jejich parametry, hodlá přijímat v žádosti o vydání kvalifikovaného certifikátu.

(3) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty umožňuje trvalý dálkový přístup ke své certifikační politice.

Komentář

Dokument certifikační politika je určen ke zveřejnění, neboť vždy obsahuje zásady, které poskytovatel vydávající kvalifikované certifikáty hodlá uplatňovat při zajišťování služeb spojených s elektronickými podpisy a se kterými se mají seznámit zejména ty osoby, které jeho služeb již využívají nebo je hodlají využívat. Na základě obsahu tohoto dokumentu se může totiž každý individuálně rozhodnout, zda použije nabízené služby či nikoliv, a ten, kdo je již využívá, může tak zhodnotit, zda jsou v praxi naplněny zásady, které jsou v tomto dokumentu poskytovatelem deklarovány. Vzhledem k tomu, že převážná část kontaktů s poskytovatelem je realizována prostřednictvím Internetu, je žádoucí, aby certifikační politika byla rovněž tímto způsobem přístupná. V praxi se zatím používá jako nejčastější způsob zveřejnění tohoto dokumentu jeho zpřístupnění na webovských stránkách poskytovatele. Certifikační politika bývá dostupná rovněž na všech kontaktních místech registračních autorit. V elektronické podobě se dokument certifikační politika často předává žadatelům o certifikát individuálně.

(4) Obsahem certifikační prováděcí směrnice je zejména stanovení postupů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.

Komentář

Dokument certifikační prováděcí směrnice musí úzce navazovat na dokument certifikační politika. Zatímco certifikační politika stanoví zásady, které poskytovatel vydávající kvalifi-

kované certifikáty bude uplatňovat při zajišťování služeb spojených s elektronickými podpisy, certifikační prováděcí směrnice má stanovit konkrétní postupy poskytovatele, které povedou k naplnění těchto zásad. Formální struktura tohoto dokumentu je po obsahové stránce fakticky totožná se strukturou dokumentu certifikační politika. Opět se při zpracování vychází z dokumentu RFC 2527 Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. Současně lze využít Úřadem doporučenou osnovu certifikační prováděcí směrnice (viz komentář k odstavci 2). Tato doporučená osnova je předávána Úřadem všem zájemcům z řad možných budoucích poskytovatelů certifikačních služeb. Na rozdíl od dokumentu certifikační politika však dokument certifikační prováděcí směrnice jako celek není dokumentem určeným ke zveřejnění. Záleží pouze na rozhodnutí poskytovatele, zda zveřejní určité části certifikační prováděcí směrnice. Zpravidla se bude jednat o informace, které mají význam pro budoucí klienty poskytovatele. Často se budou zveřejňovat informace související s prováděnými audity a jejich výsledky a další související informace, které mají posilovat důvěru osob ve způsob provozování služeb daného poskytovatele certifikačních služeb.

(5) Obsahem celkové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění celkové bezpečnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

Komentář

Dokument celková bezpečnostní politika představuje široký soubor kritérií poskytovatele pro hodnocení bezpečnosti na úrovni vrcholového managementu. V tomto dokumentu jsou především deklarovány cíle a způsob zajištění bezpečnosti v rámci subjektu, který zajišťuje služby spojené s elektronickými podpisy. Stejně jako předcházející dokumenty je i v tomto případě na poskytovateli, zda a v jakém rozsahu zveřejní obsah tohoto dokumentu. Mělo by jít především o otevřenost a deklarování základních předpokladů pro naplnění všech cílů, které má poskytovatel prostřednictvím dokumentu celková bezpečnostní politika naplnit.

(6) Obsahem systémové bezpečnostní politiky je zejména stanovení cílů a popis způsobu zajištění bezpečnosti informačního systému, jehož prostřednictvím poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajišťuje služby spojené s elektronickými podpisy (dále jen „informační systém pro certifikační služby“). Systémová bezpečnostní politika obsahuje zejména

a) způsob uplatnění celkové bezpečnostní politiky ve vztahu k informačnímu systému pro certifikační služby,

b) popis vazeb mezi informačním systémem pro certifikační služby a jinými informačními systémy, které provozuje poskytovatel certifikačních služeb vydávající kvalifikované certifikáty,
c) způsob ochrany dat a jiných prvků informačního systému pro certifikační služby,
d) popis bezpečnostních opatření a
e) vyhodnocení analýzy rizik.

Komentář

Obsahem dokumentu systémová bezpečnostní politika je stanovení cílů a popis způsobu zajištění bezpečnosti konkrétního informačního systému, který poskytovatel k zajišťování služeb spojených s elektronickými podpisy používá nebo hodlá používat. Stěžejními obsahovými prvky dokumentu jsou především jeho vazby na celkovou bezpečnostní politiku, resp. způsob, jakým je uplatňována vzhledem k používanému informačnímu systému, popis již existujících vazeb mezi používaným informačním systémem a jinými obdobnými systémy provozovanými poskytovatelem, stanovení způsobu ochrany jednotlivých prvků tohoto informačního systému s akcentem na ochranu osobních dat, popis všech (základních) bezpečnostních opatření, která jsou uplatňována, a vyhodnocení analýzy možných rizik (znalostní databáze by měla být rozšířena o požadavky zákona o elektronickém podpisu), která je se stanovením základních bezpečnostních opatření úzce svázána. Účelem je stanovit bezpečnostní opatření tak, aby bylo možné vhodným způsobem čelit analýzou zjištěným rizikům.

(7) Požadavky na celkovou bezpečnostní politiku a systémovou bezpečnostní politiku Úřad zveřejňuje ve Věstníku Úřadu.

Komentář

Úřad na základě právní úpravy obsažené v § 35 odst. 2 a § 36 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, vydává Věstník, jehož účelem je mimo jiné zveřejňovat základní informace a požadavky, které mohou přispět k prosazení určitých záměrů a doporučení Úřadu v této oblasti. Proto je žádoucí, aby oba základní dokumenty bezpečnostní politiky, tj. celková a systémová, vycházely z těch předpokladů, které jsou obsaženy v požadavcích zákona o elektronickém podpisu, a deklarovaly tak jejich splnění a zabezpečení. Oba dokumenty celková bezpečnostní politika a systémová bezpečnostní politika musí být dále zpracovány tak, aby byly v souladu s požadavky, které jsou obsaženy v platných normách upravujících oblast informační bezpečnosti. V praxi se dnes považují za základní normy v této oblasti technické normy ISO 17799 a ČSN ISO/IEC TR 13335. Obě normy se navzájem

doplňují, a pokrývají tak plně oblast informační bezpečnosti. V listopadu 2001, tedy krátce po publikování vyhlášky, byla ISO 17799 převzata ČSNI do českého právního prostředí jako ČSN ISO 17799. Na základě shora uváděného zmocnění zveřejňuje Úřad požadavky na obsah těchto dokumentů ve Věstníku Úřadu. Úřad proto využil tuto zákonnou možnost a upřesnil požadavky na celkovou bezpečnostní politiku a požadavky na systémovou bezpečnostní politiku ve Věstníku Úřadu č.12/2001.

Zde publikovaný text zní:

Při zpracování dokumentů celková bezpečnostní politika a systémová bezpečnostní politika se postupuje dle požadavků těchto norem:

- *ISO 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti ,*
- *ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3.*

Aktuální informaci lze dále nalézt na webových stránkách Úřadu (http://www.uoou.cz).

(8) Obsahem plánu pro zvládání krizových situací je zejména stanovení postupů, které jsou uplatněny v případě mimořádné události. Mimořádnou událostí se pro účely této vyhlášky rozumí událost, která ohrožuje poskytování služeb spojených s elektronickými podpisy a která nastává zejména v důsledku selhání informačního systému nebo výskytu faktoru, který není pod kontrolou poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

Komentář

Dokument „plán pro zvládání krizových situací" je dalším ze základních dokumentů, kterými poskytovatel certifikačních služeb dokládá svou připravenost v této oblasti. Z hlediska zajištění bezpečnosti služeb spojených s elektronickými podpisy je nezbytné vždy předpokládat situace, které mohou nastat v důsledku vzniku mimořádných událostí (selhání funkčnosti informačního systému, živelní pohroma, selhání lidského faktoru aj.). Pro takové potenciální hrozby poskytovatel zpracovává plán postupů, které budou uplatněny v případě, že dojde k mimořádné situaci. Vyhláška v tomto ustanovení obsahuje i základní definici pojmu mimořádná událost pro účely vyhlášky. K tomu je třeba uvést, že autoři textu vyšli z dosavadních praktik a zkušeností, jak tyto mimořádné jevy hodnotit a zvládat je. Je třeba konstatovat, že nejde v žádném případě o taxativní výčet, ale je nezbytné očekávat i možnou existenci nových, dosud nepoznaných krizových situací. Základem pro aplikaci tohoto ustanovení je povinnost poskytovatele demonstrovat svou připravenost mobilizovat všechny dostupné síly a prostředky pro zvládnutí krizové situace a likvidace jejích následků.

(9) Obsahem plánu obnovy je zejména stanovení postupů pro obnovu řádné funkce informačního systému pro certifikační služby.

Komentář

Dokument „plán obnovy" musí velmi úzce navazovat na dokument „plán pro zvládání mimořádných situací". Pro poskytovatele totiž pouhé zvládnutí mimořádné situace není samo o sobě dostačující pro obnovení řádné funkce používaného informačního systému. Poskytovatel proto současně musí stanovit základní postupy, jejichž pomocí bude v případě likvidace mimořádné události obnovena řádná funkce informačního systému. Je nezbytné, aby jak mimořádná situace, tak i obnova funkce používaného informačního systému nebyly řešeny chaoticky až v okamžiku, kdy dojde k jejich vzniku, neboť tím by mohlo dojít k dalším škodám, ale je nezbytné, aby poskytovatel měl včas připraven plán obnovy informačního systému, který nastartuje ihned, jakmile to dovolí likvidace mimořádné události, která vedla k ohrožení používaného informačního systému.

Je nezbytné, aby se poskytovatel prostřednictvím tohoto dokumentu vyjádřil v tom směru, za jak dlouho je schopen plně obnovit poskytování svých služeb, které souvisí s jeho povinnostmi některé informace poskytovat nepřetržitě, popřípadě s jeho povinností vykonat některou činnost v pevně stanoveném termínu. Protože jde o zákonnou povinnost poskytovatele podléhající dozorové pravomoci Úřadu, bude zejména při posuzování připravenosti poskytovatele Úřad dbát na splnění všech deklarovaných závazků poskytovatele v tomto dokumentu.

(10) Při zajišťování služeb spojených s elektronickými podpisy poskytovatel certifikačních služeb vydávající kvalifikované certifikáty postupuje podle dokumentů uvedených v odstavci 1 písm. a) až f).

Komentář

Zásady, cíle a postupy, které poskytovatel uvádí v dokumentech uvedených v odstavci 1 písm. a) až f), jsou pro jeho činnost závazné, tj. deklarované zásady a postupy musí poskytovatel dodržovat vždy. Současně však musí být poskytovatelem zachován soulad obsahu a postupů uváděných v těchto dokumentech s fakticky vykonávanou činností. Vychází se v tomto případě zejména z ustanovení § 6 odst. 1 písm. j) zákona o elektronickém podpisu, které mimo jiné stanoví povinnost zajištění dostatečné bezpečnosti postupů. Tato skutečnost však současně nebrání poskytovateli, aby přijal a vydal (zveřejnil) ještě další možná opatření nebo postupy, kterými on sám hodlá dále ještě garantovat zabezpečení všech prováděných činností v oblasti elektronického podpisu.

Poskytovatel certifikačních služeb musí provádět nejméně jedenkrát za 12 měsíců kontrolu bezpečnostní shody (§ 6 písm. c) vyhlášky), jejímž výsledkem je písemný posudek. Povinnou součástí tohoto posudku je potvrzení, že používání informačního systému

pro certifikační služby je v souladu se způsoby zajištění bezpečnosti stanovenými v dokumentech poskytovatele vydávaných podle § 2 odst. 1 písm. c) a d) vyhlášky.

Dojde-li Úřad při výkonu své kontrolní působnosti k závěru, že akreditovaný poskytovatel certifikačních služeb nebo poskytovatel certifikačních služeb vydávající kvalifikované certifikáty porušuje povinnosti uložené mu zákonem, může mu za takové jednání uložit pokutu (§18 zákona o elektronickém podpisu). Tyto kontroly provádí Úřad podle plánu kontrol, který je schvalován vždy na určité časové období. Kontrola může být Úřadem provedena také na základě podnětu nebo podání jiného subjektu nebo poškozené osoby, která zjistí nebo má podezření, že poskytovatel porušil některou svou povinnost nebo že poskytovatel nepostupuje při zajišťování služeb spojených s elektronickými podpisy v souladu s dokumenty uvedenými v § 2 odst. 1 písm. c) a d) vyhlášky.

(11) Dostatečností finančních zdrojů je schopnost poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty finančně zabezpečit řádné provozování služeb spojených s elektronickými podpisy i s ohledem na riziko odpovědnosti za škody.

Komentář

V § 2 odst. 11 se upřesňuje obsah povinností poskytovatele podle § 6 odst. 1 písm. l) zákona o elektronickém podpisu, který určuje poskytovateli, aby v souladu s požadavky zákona o elektronickému podpisu a s ohledem na riziko odpovědnosti za škody „měl k dispozici dostatečné finanční zdroje na provoz".

Zde rozvedená dikce citovaného ustanovení zákona o elektronickém podpisu definuje povinnost poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, především jako jeho schopnost zabezpečit řádné provozování služeb spojených s elektronickými podpisy. To je velmi důležitá skutečnost, protože si nelze představit, že by mělo docházet k činnosti spojené s poskytováním certifikačních služeb, aniž by pro její provozování měl poskytovatel dostatečné finanční krytí. Zákonodárce současně předpokládá, že deklarované dostatečné finanční zdroje musí sloužit i pro krytí případné odpovědnosti poskytovatele za škodu vzniklou při provozování těchto služeb. Takto deklarované krytí je samozřejmě jen velmi obtížné odhadnout, neboť bude záležet vždy na četnosti vzniku mimořádných událostí a s tím související připravenosti poskytovatele na obnovu svých povinností. Protože zákonodárce začlenil do zákona o elektronickém podpisu jen velmi obecně formulovanou povinnost poskytovatele, nebylo možné v mezích zmocnění k vydání vyhlášky, aby Úřad stanovil přesnější požadavky na doklady nebo dokumenty, kterými by byla tato povinnost blíže upřesněna. Proto se v tomto ustanovení pouze blíže stanoví, co se rozumí pod pojmem dostatečností finančních zdrojů na provoz a s ohledem na riziko odpovědnosti za škody.

§ 3
Bezpečnost postupu při vydávání kvalifikovaných certifikátů a provozování seznamu kvalifikovaných certifikátů, které byly zneplatněny

(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje zaručeným elektronickým podpisem kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Tento zaručený elektronický podpis musí být založený na kvalifikovaném certifikátu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.

Komentář

Obsah tohoto ustanovení o podepisování vydávaných kvalifikovaných certifikátů a seznamů kvalifikovaných certifikátů, které byly zneplatněny, navazuje na § 6 odst. 1 písm. g) zákona o elektronickém podpisu, ve kterém je jako jedna z povinností poskytovatele obsažena povinnost zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny. Dále toto ustanovení navazuje na § 6 odst. 1 písm. k) zákona o elektronickém podpisu, podle kterého je poskytovatel povinen přijmout odpovídající opatření proti zneužití a padělání kvalifikovaných certifikátů. Podepisování zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu je ze strany poskytovatele základním prostředkem pro dosažení požadované bezpečnosti. Kvalifikovaný certifikát poskytovatele může být „selfsign" (podepsaný samotným poskytovatelem), nebo může být vydaný i jiným poskytovatelem. Kvalifikované certifikáty poskytovatele, který žádá Úřad o udělení akreditace, se podle § 10 odst. 7 zákona o elektronickém podpisu předkládají Úřadu k ověření. Ověření je součástí rozhodnutí Úřadu o udělení akreditace. Podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu Úřad pravidelně zveřejňuje přehled udělených akreditací, v němž budou též u každého poskytovatele uvedeny otisky jeho ověřených kvalifikovaných certifikátů. Tento přehled bude dostupný v elektronické podobě na webových stránkách Úřadu. Přehled i s otisky bude též zveřejňován ve Věstníku Úřadu.

(2) Nástroj elektronického podpisu používaný pro podepisování podle odstavce 1 nelze použít pro jiné účely.

Komentář

Podepisování zaručeným elektronickým podpisem podle odstavce 1 tohoto ustanovení je realizováno nástrojem elektronického podpisu. Bezpečnost tohoto postupu, kterou vyžaduje pro celý systém zejména § 6 odst. 1 písm. j) zákona o elektronickém podpisu, musí být zajištěna zejména tím, že tento nástroj nelze používat pro jiné účely, tj. pro podepisování jiných datových zpráv. Četnější používání stejného nástroje více osobami zvyšuje vý-

razně možnost jeho zneužití. V dosud přijatých dokumentech Evropských společenství[1)] se k tomuto postupu doporučuje tento nástroj používat jako vhodný nástroj i pro vydávání tzv. časových značek (time-stamping). Jiné účely jeho použití jsou však i zde vyloučeny, zejména pak není možné podpisovat prostřednictvím stejného nástroje „obyčejné" certifikáty a současně seznam „obyčejných" certifikátů, které byly zneplatněny.

1) Pokud je v komentářích odkazováno na dokumenty Evropských společenství, jsou tím míněny dokumenty, které navazují na Směrnici 1999/93/ES, o zásadách Společenství pro elektronické podpisy. Tyto dokumenty vznikají z iniciativy Evropské komise a vydávají je The European Telecommunications Standards Institute (ETSI), European Electronic Signature Standardization Initiative (EESSI) a European Committee for Standardization / Information Society Standardization Systém (CEN/ISSS). Dokumenty lze získat například na webových stránkách těchto subjektů.

(3) Uvedení do provozu a změna provozního režimu nástroje elektronického podpisu používaného pro podepisování podle odstavce 1 vyžadují, aby je prováděly současně nejméně dvě fyzické osoby, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty.

Komentář

Bezpečnost postupu poskytovatele při vydávání kvalifikovaných certifikátů a při plnění dalších v tomto ustanovení vyhlášky uváděných povinností musí být současně zajištěna tím, že aktivaci a deaktivaci (uvedení do provozu a změnu provozního režimu) uvedeného nástroje elektronického podpisu musí vykonávat současně nejméně dvě fyzické osoby poskytovatelem k tomu určené. Předpokládá se, že poskytovatel určí pro tuto činnost, která je z hlediska bezpečnosti velmi kritická, své vlastní zaměstnance, ovšem zákon i vyhláška současně uznávají, že není možné poskytovatele v jeho rozhodnutí, kdo bude tyto činnosti vykonávat, dále omezovat.

Samotný způsob realizace tohoto požadavku může, ale nemusí zajistit již příslušný nástroj elektronického podpisu. Tato skutečnost bude totiž jednou z otázek při vyhodnocení shody nástroje elektronického podpisu. Některé typy nástrojů totiž přímo umožňují generovat přístupové autentizační karty typu k z n (tj. musí být přítomno k osob z n možných osob, kde k musí být nejméně 2). Pokud tento postup nebude umožňovat poskytovatelem používaný nástroj elektronického podpisu, pak bude muset poskytovatel stanovit jiný způsob, jakým zajistí postup, který je v tomto odstavci předpokládán. Takovým možným náhradním způsobem může být například i takový postup, kdy autentizační kartu k nástroji bude mít k dispozici ještě jiná fyzická osoba než ta osoba, která bude zadávat příslušný PIN.

(4) V případě, že jsou data pro vytváření elektronického podpisu používána pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, nelze je použít pro jiné účely.

Komentář

V tomto ustanovení vyhlášky je vymezena zásada, která vychází z předpokladu, že bezpečnost postupu poskytovatele se dále posiluje požadavkem, aby data pro vytváření elektronického podpisu, která budou užívána pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, nebyla dále používána pro jiné účely, tj. pro podepisování jiných datových zpráv. Platí zde obdobně ty skutečnosti, které již byly uvedeny v komentáři k odstavci 2 tohoto ustanovení vyhlášky. Data pro vytváření elektronického podpisu poskytovatele, která se budou používat pro podpis kvalifikovaných certifikátů a pro podpis seznamu kvalifikovaných certifikátů, které byly zneplatněny, není možné používat nejen pro podpis „obyčejných" certifikátů nebo pro podpis seznamu „obyčejných" certifikátů, které byly zneplatněny, ale tato data nelze používat ani pro podpis vydávaných časových značek (pokud tuto službu poskytovatel provozuje).

(5) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí dostupnost svého kvalifikovaného certifikátu nejméně dvěma na sobě nezávislými způsoby.

Komentář

Komentované ustanovení vyhlášky navazuje na § 6 odst. 1 písm. e) zákona o elektronickém podpisu, který mimo jiné ukládá poskytovateli povinnost zajistit, aby se každý mohl ujistit o identitě poskytovatele certifikačních služeb a kvalifikovaném certifikátu poskytovatele. Poskytovateli se ukládá, aby dostupnost svého kvalifikovaného certifikátu zajistil nejméně dvěma na sobě nezávislými způsoby. Dva způsoby dostupnosti, které nesmí být na sobě závislé (např. na webových stránkách poskytovatele a v jeho sídle), tento zákonný požadavek splní. Nejedná se o kritickou činnost poskytovatele (z hlediska bezpečnosti), kvalifikovaný certifikát poskytovatele stačí získat důvěryhodným způsobem pouze jednou a lze jej používat po celou dobu jeho platnosti (zpravidla dva roky a více let). Není tedy třeba jej při každém ověření podpisu znovu „stahovat", implementovat a kontrolovat.

Zneplatnění certifikátu poskytovatele je však naprosto výjimečnou a odlišnou situací. Není sice nezbytná okamžitá dostupnost tohoto certifikátu, ale je však potřeba zajistit důvěryhodnou možnost ověření skutečnosti, že nainstalovaný kvalifikovaný certifikát patří příslušnému poskytovateli (ověření, že nebyl zaměněn). Zpravidla se pro tento postup využívá nejčastěji kontrola otisku (součást certifikátu) proti otisku získanému jiným způsobem. Tento otisk přitom může být zveřejněn např. v tištěné podobě, umístěn na www stránkách různých subjektů, zaslán na požádání poskytovatelem apod.

Proto se první předání a převzetí certifikátu poskytovatele doporučuje učinit osobně (například na CD, které poskytovatel distribuuje na různých akcích, v registračních místech apod.). V případě akreditovaných poskytovatelů je součástí rozhodnutí Úřadu o udělení akreditace i ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem (§ 10 odst. 7 zákona o elektronickém podpisu). Takto ověřené certifikáty a jejich jednoznačná identifikace (například otisk) budou pravidelně zveřejňovány ve Věstníku Úřadu a dále na jeho webových stránkách.

(6) Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné.

Komentář

Odstavec 6 v ustanovení § 3 vyhlášky navazuje na § 6 odst. 1 písm. g) zákona o elektronickém podpisu, kterým se stanoví povinnost poskytovatele k provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým způsobem. Obě dikce se sice poněkud odlišují v tom smyslu, že zákon o elektronickém podpisu stanoví povinnost „veřejně přístupného" seznamu, zatímco vyhláška obsahuje výraz „dálkový přístup", aniž by výslovně stanovila, že tento dálkový přístup musí být totožný s veřejným přístupem. Lze však usuzovat, že zákonodárce i autoři vyhlášky měli nepochybně na mysli právě obdobnou a nejčastěji využívanou formu zveřejnění těchto druhů informací; ve vyhlášce je však více zdůrazňována skutečnost, že tento přístup musí být zabezpečen nepřetržitě. Opět se v tomto případě předpokládá, že tento seznam bude poskytovatelem umístěn nejméně na dvě IP adresy. Adresy, na kterých budou tyto seznamy uloženy, musí být uvedeny jak v certifikační politice poskytovatele, tak také přímo v kvalifikovaném certifikátu vydávaném poskytovatelem, a to v položce CRL DP (CRL Distribution Point).

(7) Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin. Tento údaj obsahuje číslo kvalifikovaného certifikátu unikátní u poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, datum a čas s uvedením hodiny, minuty a sekundy, od kdy byl kvalifikovaný certifikát zneplatněn.

Komentář

Zákon o elektronickém podpisu ukládá v § 6 odst. 7 poskytovateli povinnost ukončit platnost kvalifikovaného certifikátu, pokud o to podepisující osoba požádá. Zároveň zákon o elektronickém podpisu stanoví v § 15 odst. 2 požadavek, aby poskytovatelem vytvářený

seznam kvalifikovaných certifikátů, které byly zneplatněny, obsahoval přesný časový údaj, odkdy byl certifikát zneplatněn. Přestože je zájem, aby doba mezi přijetím požadavku na ukončení platnosti kvalifikovaného certifikátu a zveřejněním informace o jeho zneplatnění byla co nekratší, nelze vždy zajistit, aby se tak stalo současně či s odstupem několika málo hodin. Vzhledem ke zcela specifickým požadavkům na bezpečnost podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, se děje tento proces vždy pravidelně po určité době za přesně stanovených podmínek a za účasti poskytovatelem určených osob. Z tohoto důvodu se nemůže vždy při ukončení platnosti některého kvalifikovaného certifikátu ihned současně vytvářet nový seznam, ale tento seznam je připravován, podepisován a zveřejňován poskytovatelem podle plánu přípravy nového seznamu kvalifikovaných certifikátů, které byly zneplatněny. Stanovení kratší doby, než je uvedených 12 hodin, která by se dotýkala všech vydaných kvalifikovaných certifikátů, by na straně poskytovatele znamenalo značný nárůst nákladů spojených se zajištěním tohoto procesu. To by se následně promítlo do ceny kvalifikovaných certifikátů, která by mohla být pro některé uživatele neakceptovatelná. Zároveň se ve vyhlášce tato doba stanoví jako maximální a předpokládá se tak současně, že poskytovatel u agend vyžadujících vysokou míru bezpečnosti stanoví ve své certifikační politice tuto dobu co nejkratším intervalem. Poskytovatel může současně nabídnout i jiné služby zveřejňování informací o platnosti certifikátu (tzv. statutu certifikátu). Patřit sem bude především protokol OCSP (Online Certificate Status Protocol), který umožňuje dotaz na aktuální statut certifikátu. Lze tak získat potřebnou informaci o platnosti certifikátu ještě dříve, než je zveřejněna v seznamu kvalifikovaných certifikátů, které byly poskytovatelem zneplatněny. Tyto programy však zatím nejsou příliš rozšířené a je zatím jen málo aplikací, které je používají. Poskytovatel může nabídnout i další služby související se zveřejněním informace o zneplatněných certifikátech. Patří sem i možnost rozesílání informace o ukončení platnosti certifikátu. Tato informace je poskytovatelem rozeslána „předplatitelům" této služby ihned po ukončení platnosti certifikátu. I v tomto případě je informace o ukončení platnosti certifikátu k dispozici dříve, než je zveřejněna poskytovatelem v seznamu kvalifikovaných certifikátů, které byly zneplatněny.

V praxi se však nejčastěji ke kontrole platnosti certifikátu stále používá především seznam kvalifikovaných certifikátů, které byly zneplatněny. Ve standardu ETSI ("Policy requirements for certification authorities issuing qualified certificates") se doporučuje, aby doba zveřejnění mezi dvěma takovými seznamy byla nejvýše 24 hodin. Úřad v návrhu vyhlášky prosazoval v souladu s tímto dokumentem periodické vydávání seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to v limitu do 24 hodin. V průběhu projednávání návrhu vyhlášky v komisích Legislativní rady vlády byl text příslušného paragrafu upraven. Doba zveřejnění je oproti původnímu návrhu kratší a je stanovena na maximálně 12 hodin. Doba je však vázána nikoliv na dobu posledního vydání seznamu kvalifikovaných certifikátů, které byly zneplatněny, ale na dobu mezi ukončením platnosti kvalifikovaného

certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, poskytovatelem.

Výsledná formulace je tak poněkud nešťastná. Při přesném dodržení znění tohoto paragrafu totiž nemusí být vždy zachována periodicita vydávání příslušného seznamu. Pokud totiž poskytovatel neobdrží žádnou žádost o ukončení platnosti, není nucen podle znění tohoto paragrafu vydat nový seznam zneplatněných certifikátů. V praxi se však periodicita vydávání tohoto seznamu důsledně zachovává (seznamy se číslují) a seznamy, certifikátů, které byly zneplatněny, se vydávají i v případě, že k žádné změně nedošlo. Ačkoliv se tedy poskytovateli přímo neukládá povinnost pravidelně zveřejňovat seznam kvalifikovaných certifikátů, které byly zneplatněny, a to i v případě, že nedošlo k žádné změně, předpokládá se, že poskytovatelé budou takto postupovat. Jedná se o vžitou praxi, a to jak v České republice, tak i v zahraničí.

V § 6 odst. 1 písm. h) zákona o elektronickém podpisu se ukládá poskytovateli zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám. Z tohoto důvodu se ukládá, aby tyto údaje byly uvedeny v seznamu kvalifikovaných certifikátů, které byly zneplatněny. Aby bylo možné kvalifikovaný certifikát v seznamu jednoznačně určit, je doplněn požadavek na uvedení čísla kvalifikovaného certifikátu. Podle § 12 odst. 1 písm. g) zákona o elektronickém podpisu musí být číslo kvalifikovaného certifikátu u daného poskytovatele unikátní. Určení používaného času a jeho kontrola se zpravidla uvádí v certifikační prováděcí směrnici.

§ 4
Bezpečnost informačního systému pro certifikační služby

(1) Používaný informační systém pro certifikační služby se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost a prokazatelnost jejich původu a pokud odpovídá požadavkům technické normy upravující oblast informační bezpečnosti.[1)]

[1)] ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

Komentář

V návaznosti na § 6 odst. 1 písm. j) zákona o elektronickém podpisu se upřesňují požadavky na používaný informační systém pro certifikační služby. Za splněné se považují v případě, že systém vyhovuje požadavkům, které stanoví technický předpis upravující oblast informační bezpečnosti. Tímto technickým předpisem je norma ČSN ISO 15408, která stanoví kritéria pro hodnocení bezpečnosti informačních technologií. Nevylučuje se ovšem ani použití dosud hojně používaných ITSEC, neboť existují převodní tabulky mezi stupni bezpečnosti stanovenými oběma uvedenými předpisy. Bezpečnostní profil úrovně zaručitelnosti bezpečnosti 4 (dále EAL 4) byl stanoven v souladu s předpisy Evropských společenství.

(2) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí zaznamenávání událostí při

a) vydání kvalifikovaných certifikátů,
b) ukončení platnosti kvalifikovaných certifikátů,
c) nakládání s daty pro vytváření elektronického podpisu a jim odpovídajícími daty pro ověřování elektronického podpisu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty (dále jen „párová data poskytovatele“), a to během jejich celého životního cyklu, a
d) nakládání s kvalifikovaným certifikátem poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, a to během celého životního cyklu tohoto certifikátu.

Komentář

Pro dokládání bezpečnosti postupů, které podporují požívané systémy a nástroje elektronického podpisu podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu, je poskytovatel povinen zajišťovat zaznamenávání událostí, které nastávají při činnostech uvedených pod písmeny a) až d) a které jsou z hlediska zajištění informační bezpečnosti služeb spojených s elektronickými podpisy nejvíce kritické. Konkrétní způsob, kterým by měli poskytovatelé provádět zaznamenávání výše uvedených událostí,není stanoven. Postup při zaznamenávání výše uvedených událostí je závislý na použitém informačním systému, bezpečnostní politice a možnostech poskytovatele. Způsob zaznamenávání událostí poskytovatel podrobně popisuje v certifikační prováděcí směrnici. V dokumentech předpisové základny, zpravidla v personální politice, popřípadě v bezpečnostní politice, bude také nezbytné stanovit, kteří zaměstnanci poskytovatele nebo jiné osoby budou provádět zaznamenávání událostí, kdo bude tuto činnost kontrolovat a kdo bude odpovědný za dodržení stanovených postupů.

(3) Záznamy o událostech podle odstavce 2 musí být pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, dostupnosti, integrity, časové autentičnosti a důvěrnosti těchto záznamů.

Komentář

Při pořizování záznamů o událostech podle odstavce 2 písm. a) až d) a při dalším nakládání s nimi musí být postupováno tak, aby byly věrohodné, v případě potřeby dostupné oprávněným osobám a aby byly neporušené a autentické z hlediska času. Konkrétní postup poskytovatele při plnění povinnosti podle odstavce 3 opět bezprostředně souvisí s použitým informačním systémem poskytovatele a postupy popsanými v certifikační prováděcí směrnici a popřípadě v dalších dokumentech předpisové základny. Lze předpokládat, že na tuto činnost se mimo jiné soustředí kontrolní činnost prováděná v rámci vnitřního auditu i v rámci kontroly podle § 6 písm. c) a také dozor prováděný Úřadem nad dodržováním zákona o elektronickém podpisu.

(4) Prostory, kde dochází k činnosti podle odstavců 1 až 3 a podle § 5 odst. 1, musí být zabezpečeny obdobně jako objekty kategorie „D“ podle zvláštního právního předpisu.[2)]

[2)] Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.

Komentář

Ve vyhlášce se odkazuje na zvláštní právní předpis, který upravuje objektovou bezpečnost. Vyhláška ovšem využívá pouze jednu kategorii, a to kategorii „D“, neboť požadavky na zabezpečení prostor poskytovatele, ve kterých bude docházet k činnosti podle § 4 odst. 1 až 3 a § 5 odst. 1, jsou obdobné. Vytvářet novou právní úpravu v případě, kdy lze využít již existující a vyhovující právní úpravu, by bylo nadbytečné. Technické prostředky obsahující obdobné požadavky, které stanoví vyhláška č. 339/1999 Sb., o objektové bezpečnosti, jsou prostředky volně dostupnými na trhu. Jejich předností je, že již jsou certifikovány jako způsobilé pro navrženou kategorii.

Technické předpisy upravující oblast informační bezpečnosti stanoví obecné požadavky na bezpečnost; požadavky na zabezpečení prostorů stanovené v těchto technických předpisech jsou obdobné jako požadavky na zabezpečení objektů kategorie „D“ stanovené vyhláškou č. 339/1999 Sb., o objektové bezpečnosti.

Začlenění prostorů poskytovatele, ve kterých se budou provádět tzv. „choulostivé operace“, do kategorie „D“, bylo určeno na základě obdobných požadavků pro tuto činnost. Konkrétně stanovená opatření ochrany prostoru z hlediska

- *a) fyzické ostrahy objektu,*
- *b) požadovaných technických prostředků a*
- *c) režimových opatření*

jsou vhodná i pro prostory, ve kterých se budou provádět tzv. „choulostivé operace“ Požadavky na kategorii „V“ lze vzhledem k určenému účelu považovat za příliš „slabé“ (například u objektů kategorie „V“ se fyzická ostraha objektu zajišťuje pouze v pracovní době). Požadavky na kategorii „T“ jsou nadbytečně přísné a neodpovídají stanovenému účelu.

Vždy se bude jednat o prostory, ve kterých bude poskytovatel provozovat informační systém pro certifikační služby. Oddělení prostorů, ve kterých bude docházet k činnosti podle § 4 odst. 1 až 3 a podle § 5 odst. 1, od ostatních prostorů (tzv. „demilitarizované zóny“) musí poskytovatel certifikačních služeb určit v systémové bezpečnostní politice. Obecně platí, že v odděleném prostoru se zpracovávají všechny z hlediska bezpečnosti důležité informace. Zejména se v odděleném prostoru bude uskutečňovat vytváření a podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které mají být zneplatněny, správa databáze informací o klientech a správa databáze všech vydaných kvalifikovaných certifikátů. Tato databáze se může replikovat do tzv. „demilitarizované zóny“ pro usnadnění přístupu například k informacím o statutu certifikátu.

(5) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) a k) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty pořizuje písemné záznamy o tom, že osoby jím určené k zajišťování služeb spojených s elektronickými podpisy jsou

a) seznamovány v potřebném rozsahu s dokumenty uvedenými v § 2 odst. 1 písm. a) až e) a
b) proškolovány tak, aby jejich odborné předpoklady odpovídaly vykonávané činnosti.

Komentář

Zákon o elektronickém podpisu stanoví v § 6 odst. 1 písm. j) povinnost používat bezpečné postupy, v § 6 odst. 1 písm. i) povinnost přijímat do pracovního nebo obdobného poměru osoby, které mají odborné znalosti, zkušenosti a kvalifikaci nezbytnou pro poskytovatele služby a které jsou obeznámeny s příslušnými bezpečnostními postupy, dále v § 6 odst. 1 písm. i) povinnost přijímat do pracovního nebo obdobného poměru osoby, které jsou obeznámeny s příslušnými bezpečnostními postupy. Personální bezpečnost se posiluje tím, že poskytovatel je povinen pořizovat písemné záznamy o tom, že osoby poskytovatelem určené k zajišťování služeb spojených s elektronickými podpisy jsou seznamovány se základními dokumenty poskytovatele uvedenými v § 2 odst. 1 písm. a) až e) v potřebném rozsahu a proškolovány tak, aby jejich odborné předpoklady odpovídaly činnosti, kterou vykonávají. Posiluje se tak tzv. „bezpečnostní vědomí“, tj. pochopení významu a důležitosti informační bezpečnosti a schopnost v rámci svěřené činnosti používat bezpečné postupy.

§ 5
Bezpečnost postupu při nakládání s párovými daty poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty

(1) Při vytváření, používání a uchovávání párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být jakákoliv manipulace s těmito daty prováděna

a) výhradně fyzickými osobami, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty,
b) podle postupů stanovených certifikační prováděcí směrnicí a
c) v souladu se systémovou bezpečnostní politikou.

Komentář

Nakládání s párovými daty poskytovatele je součástí bezpečných postupů podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu. Při nakládání s párovými daty poskytovatele musí být postupováno tak, aby jakoukoliv manipulaci s nimi mohly vykonávat pouze fyzické osoby určené poskytovatelem pro tuto činnost. Poskytovatel je povinen zabezpečit, aby vytváření, používání a uchovávání párových dat, což je z hlediska bezpečnosti považováno za činnosti kritické, prováděly výlučně fyzické osoby určené k tomu poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty, a to zpravidla jeho zaměstnanci, ovšem není možné jej v tomto směru omezovat. Jakákoliv manipulace s párovými daty nemůže probíhat náhodně ani u jednoho poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty rozdílně případ od případu, nýbrž podle postupů stanovených certifikační prováděcí směrnicí a v souladu se systémovou bezpečnostní politikou.

(2) Při vytváření párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být použity kryptografické algoritmy a jejich parametry, které jsou uvedeny v příloze č. 2 této vyhlášky.

Komentář

Párová data poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty mohou být vytvářena výhradně za použití kryptografických algoritmů, které splňují kryptografické parametry uvedené v příloze č. 2 vyhlášky, neboť pouze tyto jsou v členských státech Evropské unie považovány v současné době za bezpečné. Stanovení přípustných algoritmů a jejich parametrů je nezbytné nejen z hlediska kompatibility, ale i pro možnost uznávání elektronických podpisů a kvalifikovaných certifikátů v případech jejich používání i za hranice jednotlivých států.

(3) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty je povinen svá data pro vytváření elektronického podpisu zničit po ukončení jejich životního cyklu; o tom pořizuje zápis, který obsahuje

a) popis způsobu zničení dat,
b) datum zničení dat,
c) datum pořízení zápisu a
d) jméno, příjmení a podpis osoby určené poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty k tomu, aby zničení dat zajistila.

Komentář

Součástí požadavků na bezpečnost postupů je požadavek na zničení dat pro vytváření elektronického podpisu poskytovatele poté, kdy skončil jejich životní cyklus, tj. kdy poskytovatel rozhodl, že tato data nebudou dále používána. O zničení dat je nutno pořídit zápis, který musí obsahovat náležitosti podle odstavce 3. Z důvodu bezpečnosti nelze data pro vytváření elektronického podpisu, u nichž skončil jejich životní cyklus, považovat za součást informací a dokumentů, které je poskytovatel povinen podle § 6 odst. 1 písm. m) zákona o elektronickém podpisu uchovávat po dobu nejméně 10 let.

(4) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty v případě neoprávněného použití nebo vzniku důvodné obavy ze zneužití svých dat pro vytváření elektronického podpisu užívaných pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, je bezodkladně povinen

a) ukončit platnost svého kvalifikovaného certifikátu, který byl k těmto datům vydán,
b) ukončit platnost kvalifikovaných certifikátů, které byly těmito daty podepsány,
c) zpřístupnit informaci o ukončení platnosti svého kvalifikovaného certifikátu s uvedením důvodu ukončení platnosti, a to nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné, a
d) informovat osoby, které byly dotčeny ukončením platnosti kvalifikovaného certifikátu podle písmene a) o ukončení platnosti jejich kvalifikovaných certifikátů vydaných tímto poskytovatelem certifikačních služeb. V informaci musí být uveden důvod ukončení platnosti kvalifikovaného certifikátu podle písmene a).

Komentář

Ustanovení upřesňuje povinnosti poskytovatele v případě, kdy je ohrožena bezpečnost jeho dat pro vytváření elektronického podpisu, která jsou užívána pro podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny. Aby se předešlo možnosti jejich zneužití, ukládá se poskytovateli, jakým způsobem je poskytovatel certifikačních služeb vydávající kvalifikované certifikáty povinen postupovat v případě neoprávněného použití nebo vzniku důvodné obavy ze zneužití svých dat a co je v takové situaci povinen bezodkladně učinit.

Zneužití dat pro vytváření elektronického podpisu poskytovatele je situací, která by v praxi neměla nastat. Jsou-li dodržena všechna vyžadovaná opatření – používání hodnoceného nástroje, používání nástroje jen pro vymezené úkoly, rozdělení autentizace k nástroji elektronického podpisu, záznamy všech kritických operací, stanovená personální a fyzická bezpečnost – je téměř vyloučeno, aby mohla být tato data zneužita.

§ 6
Ověření bezpečnosti používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují

Požadavek na bezpečnost používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují, se považuje za splněný, pokud je doložen

a) dokumenty uvedenými v § 2 odst. 1 písm. a) až e),

Komentář

Ustanovení navazuje na § 6 odst. 1 písm. j) zákona o elektronickém podpisu. Především se stanoví okruh dokumentů, kterými se dokládá splnění povinností stanovených v § 6 zákona o elektronickém podpisu. Tyto dokumenty jsou specifikovány v § 2 odst. 1 vyhlášky.

b) výsledkem hodnocení, podle něhož jsou splněny požadavky technické normy upravující oblast informační bezpečnosti,[1)] a

[1)] ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

Komentář

Předložit je nutné rovněž dokument o hodnocení dokládajícím splnění požadavků technických předpisů upravujících oblast informační bezpečnosti. Kritéria pro hodnocení bezpečnosti informačních technologií stanoví ČSN ISO 15408. Bezpečnostní profil úrovně zaručitelnosti bezpečnosti 4 (EAL 4) je stanoven v souladu s dokumenty Evropských společenství. Poskytovatel musí prokázat, že jeho systém byl navržen a vyvíjen v souladu s požadavky technických předpisů upravujících oblast informační bezpečnosti. Systém poskytovatele nemusí být hodnocen v testovací laboratoři a poskytovatel není povinen získat výsledek hodnocení, tj. stvrzení, že systém splňuje příslušnou úroveň zaručitelnosti bezpečnosti. Poskytovatel však musí být schopen předložit všechny dokumenty, které se vyžadují před zahájením vlastního procesu hodnocení. Zejména jde o těchto 24 dokumentů: „Configuration management documentation, Delivery documentation, Administrator guidance, Installation, generation, and start-up security procedures, Functional specification, User guidance, High-level design, Low-level design, Subset of the implementation representation, Correspondence analysis between the TOE summary specification and the functional specification, Correspondence analysis between the functional specification and the high-level design, Correspondence analysis between the high-level design and the low-level design, Correspondence analysis between the low-level design and the subset of the implementation representation, TOE security policy model, Life-cycle definition documentation, Vulnerability analysis, Misuse analysis of the guidance, Development security documentation, Development tool documentation, Test documentation, Test coverage analysis, Depth of testing analysis, Strength of function claims analysis, Current information regarding obvious vulnerabilities".

Informační systém se považuje za hodnotitelný na stupeň EAL 4, jestliže ten, kdo systém plánoval a vyvíjel, postupoval s odbornou péčí a bylo dosaženo takové technické úrovně, že systém může být předán do příslušné laboratoře k hodnocení. V případě, že systém může být předán do příslušné laboratoře k hodnocení, má se za to, že systém splňuje všechny stanovené požadavky a poskytovatel je v takovém případě schopen prokázat splnění všech stanovených požadavků, a to především provedení všech předepsaných úkonů během vývoje tohoto systému.

Tento způsob prokázání splnění požadavků podle § 6 odst. 1 písm j) zákona o elektronickém podpisu byl přijat zejména proto, že v současnosti v České republice neexistuje žádná technická nebo obdobná testovací laboratoř, která by prováděla testování podle ČSN ISO 15408 a která by byla schopna provést příslušná hodnocení. Poskytovatel takto není omezován v rozhodnutí ve věci výběru odborníka nebo pracoviště, které připraví podklady k hodnocení a které popřípadě hodnocení provede.

c) písemným posudkem, jehož součástí je potvrzení, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy upravující oblast informační bezpečnosti,[3)] je používání informačního systému pro certifikační služby v souladu se způsoby zajištění bezpečnosti stanovenými v dokumentech uvedených v § 2 odst. 1 písm. c) a d). Kontrola

bezpečnostní shody musí být prováděna opakovaně, a to vždy nejpozději do 12 měsíců od provedení poslední kontroly bezpečnostní shody.

[3] ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1 – 3.

Komentář

Vyžaduje se písemný posudek, který obsahuje potvrzení o provádění kontroly bezpečnostní shody provedené podle ČSN ISO/IEC TR 13335 (Informační technologie – Směrnice pro řízení bezpečnosti IT 1 – 3). Podle této normy se postupuje při výběru subjektu, který kontrolu provádí (auditor), a vytváří se dokumentace o kontrole. Předmětem kontroly bezpečnostní shody je úroveň celkové bezpečnostní politiky a systémové bezpečnostní politiky. Tato kontrola musí být prováděna periodicky, a to nejméně jedenkrát ročně. Kontroluje se soulad způsobů zajištění bezpečnosti stanovených v dokumentech, uvedených v § 2 odst. 1 písm. c) a d), a vlastního používání informačního systému pro certifikační služby.

§ 7
Prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

Komentář

Zákon o elektronickém podpisu nestanoví žádnému subjektu povinnost používat zaručený elektronický podpis. Záleží pouze na rozhodnutí podepisující osoby nebo osoby, která se spoléhá na pravost podpisu, zda takový prostředek bude (nebo nebude) používat, například z důvodu vyšší bezpečnosti, a tedy i vyšší právní jistoty Podle § 3 odst. 2 zákona o elektronickém podpisu 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.

V dokumentech Evropských společenství se pro zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření elektronického podpisu používá zkrácené označení „kvalifikovaný podpis“.

Osoba, která se spoléhá na kvalifikovaný podpis, musí mít velkou důvěru ve spolehlivost používaných prostředků elektronické komunikace. Nemůže však z podpisu přímo zjistit, zda se jedná o kvalifikovaný, nebo nekvalifikovaný podpis (přesněji, zda při vytváření podpisu byl, nebo nebyl použit prostředek pro bezpečné vytváření elektronického podpisu). Navrhuje se tedy, aby osoba, která vlastní prostředek pro bezpečné vytváření elektronického podpisu, si tuto informaci nechala zapsat do svého kvalifikovaného certifikátu.

Pokud by vytvořila podpis založený na tomto certifikátu bez použití prostředku pro bezpečné vytváření elektronického podpisu, musí o tom druhou komunikující stranu informovat, a to například v podepsaném textu.

V dokumentech Evropských společenství se doporučuje pro tento typ podpisu dosáhnout v právních předpisech jednotlivých členských států Evropské unie stejnou právní akceptovatelnost jako u podpisu vlastnoručního. V této souvislosti je nutné poznamenat, že v současnosti pouhá skutečnost, že určitá písemnost byla opatřena kvalifikovaným (bezpečným) elektronickým podpisem, nestačí k tomu, aby byl takový podpis právně akceptovatelný tam, kde se jinak musí používat vlastnoruční podpis.

V členských státech Evropské unie v současnosti stále ještě neexistují kompletní normy a standardy, které jsou nutné pro hodnověrné určení bezpečnosti používaného prostředku. Základní problém bezpečnosti se často shrnuje do jediné věty: „What You See is What You Sign“. Zajištění toho, aby podepisující osoba měla jistotu, že skutečně podepsala to, co vidí (a vyjádřila tak svoji vůli), je technicky nesmírně náročné a vede k odborným diskusím, zda je vůbec možné tento požadavek splnit při použití běžného počítače vybaveného komerčním systémem. Obecně lze konstatovat, že v členských státech Evropské unie se (tak jako v České republice) požaduje provádět hodnocení používaných prostředků podle ISO 15408 na úroveň EAL 4. V současné době se dokončují návrhy metodiky pro postup při takovém hodnocení, příslušné bezpečnostní profily (PP-Protecion Profiles) a administrativní záležitosti kolem vzájemného uznávání hodnocení provedených v jednotlivých členských státech Evropské unie. Zvláštní význam se klade na vytvoření definice tzv. „lidského rozhraní“. Předpokládá se rovněž vývoj a výroba speciálních bezpečných klávesnic, „monitorů“, speciálních čipových karet atd.

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

a) byla informována, že používá tento prostředek, a
b) zadala přístupové heslo nebo byl uplatněn jiný obdobný autentizační mechanismus.

Komentář

Vyžaduje se, aby prostředek pro bezpečné vytváření zaručeného elektronického podpisu měl implementovány takové funkce, které zajistí, že podepisující osoba si bude vědoma, že určitý prostředek právě používá a že je tento prostředek chráněn proti běžným způsobům zneužití. Předpokládá se využití čipové karty nebo jiného tokenu, nutnost zadat PIN, nebo dokonce využití biometrické autentizace (například otisku prstu).

(2) Prostředek pro bezpečné vytváření zaručeného elektronického podpisu musí používat kryptografické algoritmy a jejich parametry, které jsou uvedeny v příloze č. 2 této vyhlášky.

Komentář

Stanovují se kryptografické algoritmy a jejich parametry, které se v současné době považují za bezpečné vzhledem k požadavkům na bezpečné podepisování. Tyto algoritmy a parametry byly vybrány na základě doporučení EESSI (European Electronic Signature Standardization Initiative), které bylo publikováno dne 4. 5. 2001 v dokumentu Algorithms and Parameters for Secure Electronic Signatures (draft, V 1.44).

(3) Prostředek pro bezpečné vytváření zaručeného elektronického podpisu vyžaduje dostatečnou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek odpovídá požadavkům technické normy upravující oblast informační bezpečnosti.[1)]

[1)] ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.

Komentář

Bezpečnost při vytváření zaručeného elektronického podpisu se považuje za dostatečně zaručenou, pokud prostředek odpovídá požadavkům technických předpisů v oblasti informační bezpečnosti. Norma ČSN ISO 15408 stanoví kritéria pro hodnocení bezpečnosti informačních technologií a v souvislosti s nimi i úroveň zaručitelnosti bezpečnosti. Pojem „úroveň zaručitelnosti bezpečnosti" je použit v publikaci Hanáček, P. – Staudek, J.: Bezpečnost informačních systémů. Praha, Úřad pro státní informační systém, červenec 2000. Bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4 (EAL 4) byl stanoven na základě dokumentu CEN/ISSS WS/E-SIGN N 136, který definuje bezpečnostní požadavky pro prostředky pro bezpečné vytváření elektronického podpisu v souladu se Směrnicí 1999/93/ES.

Standardy a normy Evropské unie pro tuto oblast připravuje CEN/ISSS. V oblasti podpory legislativního procesu je činná pracovní skupina pro elektronický podpis (E-SIGN Workshop).

V současné době (leden 2002) se problematikou prostředků pro bezpečné vytváření a ověřování elektronických podpisů zabývají následující dokumenty, z nichž některé se nacházejí teprve ve fázi schvalování:

1 N123	*Terminology for EESSI documents*
3 D1-N161	*Security Requirements for Trustworthy System Managing Certificates for Electronic Signatures*

4 D2-N178	*Cryptographic Module for CSP Signing Operations Protection Profile*
5 F-N137	*Secure Signature – Creation Device*
6 F-N177	*Memorandum: CC-Evaluation of WS/E sign CWA Area F*
7 G1-N141	*Security Requirements for Signature Creation Applications*
8 G2-N140	*Procedures for electronic signature verification*
9 V-N112	*Minimum criteria to be taken into account by Member Conformity Assessment Guidance*
10 V-N143	*Part 1 – General*
11 V-N144	*Part 2 – Certification Authority services and processes*
12 V-N164	*Part 3 – Trustworthy systems managing certificates for electronic signatures*
13 V-N165	*Part 4 – Signature creation applications and procedures for electronic signature verification*
14 V-N166	*Part 5- Secure signature creation devices*
15 D2- N0191	*Cryptographic Module for CSP Key Generation Services – PP*
16 AA1 N-0183	*Guidelines for the implementation of Secure Signature-Creation Devices*
17 AA2 N-0192	*General Requirements for Electronic Signatures*

(4) Splnění požadavků na prostředek pro bezpečné vytváření zaručeného elektronického podpisu stanovených v § 17 zákona o elektronickém podpisu se dokládá

a) výsledkem hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu a seznamem technických norem upravujících oblast informační bezpečnosti, podle kterých byl hodnocen, a
b) podrobným popisem funkce a technickou dokumentací prostředku pro bezpečné vytváření zaručeného elektronického podpisu.

Komentář

Na základě dokumentů uvedených v odstavci 4 lze rozhodnout o tom, zda prostředky splňují požadavky stanovené v § 17 zákona o elektronickém podpisu. Dokumenty uvedené v odstavci 4 se Úřadu předkládají zejména při výkonu dozoru.

Právní úprava výslovně nestanoví, který subjekt je oprávněn provést hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu. V současnosti se předpokládá, že hodnocení budou provádět laboratoře, které vyvíjejí činnost v členských státech Evropské unie. Je pravděpodobné, že i v České republice vznikne příslušné řádně vybavené hodnotitelské pracoviště. Aby hodnocení provedené takovým pracovištěm mohlo být uznáváno i v členských státech Evropské unie, bude nutné jeho zapojení do evropského akreditačního schématu. Některé prvky této koncepce jsou obsaženy již ve Směrnici 1999/93/ES, o zásadách Společenství pro elektronické podpisy.

(5) Požadavky uvedené v odstavcích 2 až 4 musí splňovat rovněž prostředek pro bezpečné ověřování zaručeného elektronického podpisu.

Komentář

Požadavky, které jsou stanoveny v odstavcích 2 až 4 pro prostředky pro bezpečné vytváření zaručeného elektronického podpisu, se v plném rozsahu vztahují rovněž na prostředky pro bezpečné ověřování zaručeného elektronického podpisu.

§ 8
Náležitosti postupu a způsobu vyhodnocování shody nástrojů elektronického podpisu

(1) Úřad vyhodnocuje na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

Komentář

Zajišťovat vyhodnocování shody nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů ukládá Úřadu § 9 odst. 2 písm. e) zákona o elektronickém podpisu. Úřad zahájí vyhodnocování shody na základě obdržené písemné žádosti. Předpokládá se, že žadateli budou především poskytovatelé, ale mohou jimi být i jiné subjekty, například výrobci, dovozci a prodejci příslušného nástroje elektronického podpisu.

(2) Žádost podle odstavce 1 musí obsahovat

a) podrobný popis funkce a technickou dokumentaci nástroje elektronického podpisu podle odstavce 1 a
b) výsledek hodnocení kryptografických funkcí, které používá nástroj elektronického podpisu podle odstavce 1 a které musí odpovídat požadavkům Úřadu na kryptografické moduly. Tyto požadavky Úřad zveřejňuje ve Věstníku Úřadu. Toto hodnocení zajišťuje zpravidla dodavatel příslušného nástroje elektronického podpisu.

Komentář

V žádosti o vyhodnocení shody musí být obsaženy takové informace, které umožní Úřadu řádně provést příslušná vyhodnocení. Úřad zveřejňuje požadavky na bezpečnost příslušných kryptografických modulů ve Věstníku Úřadu. Tento způsob stanovení a zveřejňování požadavků na kryptografické moduly byl zvolen především s ohledem na skutečnost, že

standard FIPS 140-1 je v současné době nahrazován standardem FIPS 140-2, a dále s ohledem na skutečnost, že orgány Evropských společenství v současné době (únor 2002) vyvíjejí jim ekvivalentní standard.

Ve Věstníku Úřadu č.12/2001 a na svých webových stránkách Úřad zveřejnil požadavek na kryptografické funkce: nástroj elektronického podpisu musí splňovat požadavky na Security Level 3 podle Standardu pro hodnocení bezpečnosti kryptografických modulů vydaného National institute of standards and technology v USA – FIPS PUB 140.

Kromě povinných součástí žádosti (podrobný popis funkce, technická dokumentace, výsledek hodnocení kryptografických funkcí) se doporučuje v zájmu rychlejšího a bezproblémového vyřízení žádosti o vyhodnocení shody současně s podáním žádosti předložit Úřadu také následující dokumenty:

- *přesná identifikace nástroje;*
- *obecné informace k dovozu, výrobě a prodeji nástroje;*
- *manuál (v českém jazyce, popřípadě v anglickém jazyce);*
- *seznam a parametry kryptografických funkcí a jejich přesnou identifikaci ve vztahu k algoritmům a parametrům uvedeným v příloze č. 2 vyhlášky, a to včetně*
  - *podpisových schémat,*
  - *algoritmů pro generování klíčů,*
  - *popisu metod použitých pro generování náhodných čísel*
  - *popisu použitého generátoru náhodných čísel;*
- *popis, jak lze při použití nástroje zajistit splnění požadavků podle § 3 odst. 3 vyhlášky.*

Pokud na základě například nedostatečně podrobně zpracovaných předložených dokumentů nebude Úřad moci rozhodnout o vyhodnocení shody, může požadovat potřebné doplnění předložených dokumentů, popřípadě doplnění informací či prokázání dalších skutečností důležitých pro rozhodnutí.

Požadavek na výsledek hodnocení kryptografických funkcí se považuje za splněný, pokud byl nástroj hodnocen podle Standardu pro hodnocení bezpečnosti kryptografických modulů vydaného National institute of standards and technology v USA – FIPS PUB 140, Security Level 3 a pokud je provedené hodnocení doloženo příslušným úředně ověřeným certifikátem a je k němu rovněž připojen úřední překlad tohoto certifikátu do českého jazyka.

K žádosti je nezbytné připojit doklad o zaplacení správního poplatku stanoveného pro podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky. Tento správní poplatek činí 10 000 Kč. Číslo příslušného účtu je zveřejněno ve Věstníku Úřadu č. 12/2001 a na webových stránkách Úřadu.

(3) Pokud nástroj elektronického podpisu podle odstavce 1 splňuje požadavky stanovené zákonem o elektronickém podpisu a Úřad vysloví shodu,

je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, zveřejňuje Úřad ve Věstníku Úřadu.

Komentář

Pokud Úřad u nástroje vysloví shodu, zveřejní informaci o tom ve Věstníku Úřadu a na svých webových stránkách. Pokud poskytovatel hodlá používat nástroj, který je typově shodný s nástrojem, u nějž již byla Úřadem vyslovena shoda, není zapotřebí opakovaně provádět vyhodnocení shody také u tohoto typově shodného nástroje.

Do 1. 2. 2002 byla vyslovena shoda pro tyto dva nástroje:

I. nCipher Corporation Ltd, ***nShield F3 SCSI,*** *Firmware 5.0, Hardware verze nC4032W-150, pracující ve FIPS módu*

II. Eracom Technologies Australia, Pty. Ltd., ***CSA8000,*** *Hardware Revision: G, Firmware Version 1.1, pracující ve FIPS módu*

§ 9
Účinnost

Tato vyhláška nabývá účinnosti dnem vyhlášení.*)

**) Red. pozn.: tj. 10. října 2001.*

Komentář

Vyhláška byla podepsána předsedou Úřadu dne 3. října. 2001. Publikována byla ve Sbírce zákonů částka 138.

Vyhláška nabyla platnosti a účinnosti dnem jejího vyhlášení. Tímto dnem je 10. říjen 2001, kdy byla rozeslána příslušná částka Sbírky zákonů.

Příloha č. 1 k vyhlášce č. 366/2001 Sb.

Kryptografické algoritmy a jejich parametry pro data pro vytváření elektronického podpisu a jim odpovídající data pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu, a k nimž má být vydán kvalifikovaný certifikát

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	emsa-pss	SHA1
003	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	–	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	–	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	–	SHA1
008	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	MD5
009	RSA	MinModLen=1020	emsa-pss	MD5

Komentář k příloze č. 1

Na přílohu č. 1 se odkazuje v § 2 odst 2 písm. b) vyhlášky. Příloha obsahuje údaje, které určují požadavky na vlastnosti dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být poskytovatelem vydán kvalifikovaný certifikát. Příloha obsahuje konkrétní kryptografické algoritmy a jejich parametry, které musí být pro tato data použity. Ve všech případech se jedná se o standardní asymetrické algoritmy RSA, DSA a ECDSA. Z důvodu bezpečnosti se stanoví minimální parametry pro klíče (modul) těchto funkcí. K dosažení kvality těchto parametrů je nutné nainstalovat podporu pro tzv. silnou kryptografii. Jako hašovací funkce se povolují SHA-1, RIPEMD-160 a dnes již méně používaná MD5. Lze předpokládat, že hašovací funkce MD5 se v příštích letech přestane zcela používat a při případné novelizaci vyhlášky již bude vypuštěna.

Příloha č. 2 k vyhlášce č. 366/2001 Sb.

Kryptografické algoritmy a jejich parametry pro vytváření párových dat poskytovatele a pro prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

Podpisová schémata

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus pro generování klíčů	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	–	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	–	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	–	SHA1

Algoritmy pro generování klíčů

Označení generátoru klíčů	Používané označení	Asymetrický algoritmus	Metoda generování náhodných čísel	Parametry náhodného generátoru
4.01	rsagen1	RSA	trueran	EntropyBits≥128
4.02	dsagen1	DSA	trueran nebo pseuran (FIPS 186-2)	EntropyBits≥128 nebo SeedLen≥128
4.03	ecgen1	ECDSA-F_p nebo ECDSA-$F2^m$	trueran nebo pseuran	EntropyBits≥128 nebo SeedLen≥128

Metody generování náhodných čísel

Označení náhodného generátoru	Používané jméno	Parametry náhodného generátoru
5.01	trueran	EntropyBits
5.02	pseuran	SeedLen
5.03	FIPS 186-2-31	SeedLen
5.04	FIPS 186-2-32	SeedLen

Komentář k příloze č. 2

Na přílohu č. 2 vyhláška odkazuje na dvou místech textu. Poprvé je na ni odkazováno v § 5 odst. 2 vyhlášky v souvislosti s vytvářením párových dat poskytovatele a podruhé v § 7 odst. 2 vyhlášky v souvislosti s kryptografickými algoritmy prostředku pro bezpečné vytváření elektronického podpisu. Tato příloha byla vytvořena na základě publikovaného doporučení EESSI. Toto doporučení – dokument Algorithms and Parameters for Secure Electronic Signatures – v době přípravy vyhlášky existovalo pouze v návrhu (draft V 1.44, ze 4.5.2001). Předpokládá se, že pro elektronické podepisování budou uvedené algoritmy používány nejméně do konce roku 2005 a pro ověřování elektronického podpisu nejméně do konce roku 2006. Předpokládá se, že poté bude nutné provést jejich nové hodnocení. V říjnu 2001 byl tento dokument nahrazen verzí 2.1. Oproti verzi 1.44 došlo jen k nepatrným změnám. Byly doplněny algoritmy pro speciální verzi asymetrických šifer – německou verzi ECDSA nazývanou ECGDSA (Elliptic Curve German Digital Signature Algorithm). Byl rovněž upraven požadavek na generátor klíčů pro RSA. Kromě používání „trueran" generátoru (fyzikální generátor) bylo povoleno používat i „pseuran" (pseudo-náhodný generátor). Zatímco první změna je z hlediska právní úpravy přijaté v České republice nepodstatná, druhá změna znamená, že posuzování generátorů se v České republice uskutečňuje podle „přísnějších" požadavků, než je tomu v členských státech Evropské unie. Lze předpokládat, že v případě novelizace vyhlášky budou požadavky pro posuzování generátorů odpovídat požadavkům, podle nichž se při hodnocení postupuje v členských státech Evropské unie.

V případě nejasnosti ve výkladu některých ve vyhlášce uvedených pojmů se doporučuje prostudovat dokument Algorithms and Parameters for Secure Electronic Signatures, kde jsou jednotlivé pojmy přesně a vysvětleny.

5. ABECEDA ELEKTRONICKÉHO PODPISU

A.

Alena se rozhodla, že bude elektronicky podepisovat datové zprávy, které předává Petrovi.

B.

Petr může být její kolega, přítel, ale může být i osobou, která provozuje elektronický obchod, kam chce Alena zasílat objednávky zboží, které tento obchod nabízí. Petr může zastupovat banku, se kterou chce Alena tímto způsobem komunikovat. A konečně Petr může být pracovníkem úřadu, kterému chce Alena takto zasílat například svá daňová přiznání. V každém případě Alenino rozhodnutí, jakým způsobem se bude elektronicky podepisovat, závisí na tom, jaký elektronický podpis Petr akceptuje, resp. jaký považuje za důvěryhodný s ohledem na závažnost obsahu zasílaných zpráv.

C.

Pokud je Petr Alenin kolega nebo přítel, patrně postačí, když Alena nebude nic měnit na tom, jak se podepisuje do této doby. To znamená, že i nadále bude pod text zprávy, kterou napíše, uvádět své jméno (napíše jej z klávesnice). Petr má vždy možnost si osobně nebo telefonicky ověřit, že zprávu skutečně napsala Alena a že ji odeslala v tom znění, ve kterém Petrovi došla.

D.

Pokud se Alena s Petrem osobně neznají, může vzniknout problém. Někdo se může za Alenu vydávat a poslat Petrovi zprávu podepsanou „Alena“, nebo může zprávu, kterou Alena Petrovi poslala, pozměnit. Za této situace nemůže Petr považovat takový podpis za důvěryhodný. Alena tedy musí použít takový elektronický podpis, který uvedené pochybnosti neumožní.

E.

Alena bude používat **elektronický podpis založený na certifikátu**[1]**.** Elektronický podpis je v takovém případě pro každou podepsanou zprávu jiný

a odvozuje se od této zprávy[2]. Zároveň je závislý na něčem, co je tajemstvím Aleny a co nemůže pro vytvoření Alenina podpisu použít nikdo jiný.

[1] Certifikát není nezbytnou podmínkou pro používání digitálního podpisu (např. PGP). Uvedená varianta je popisována s ohledem na zákon o elektronickém podpisu, který upravuje používání certifikátu, resp. kvalifikovaného certifikátu.

[2] Tento typ podpisu nazývá zákon o elektronickém podpisu „zaručený elektronický podpis“. V praxi se používá spíše zkrácený název „elektronický podpis“, případně „digitální podpis“ – viz poznámka [6].

F.

Certifikát získá Alena od poskytovatele certifikačních služeb (též certifikační autorita). Nabídku jejich služeb je možné vyhledat na Internetu. Než si bude Alena vybírat poskytovatele, zjistí, jaký certifikát považuje Petr za důvěryhodný, případně jestli za důvěryhodné certifikáty považuje certifikáty vydané pouze některými poskytovateli. Například banka může považovat za důvěryhodné pouze ty certifikáty, které sama vydá. Jiný subjekt může považovat za důvěryhodné pouze kvalifikované certifikáty[3], případně kvalifikované certifikáty vydané akreditovanými poskytovateli[4]. To je pro Alenu první hledisko pro výběr poskytovatele – zda vydává ty certifikáty, které Petr akceptuje.

[3] Je míněn kvalifikovaný certifikát ve smyslu zákona o elektronickém podpisu (viz § 12). Podle zákona o elektronickém podpisu se mohou poskytovatelé rozhodnout, že požádají Úřad pro ochranu osobních údajů o udělení akreditace. Získání akreditace však není podmínkou pro poskytování certifikačních služeb. Kvalifikované certifikáty vydané akreditovanými poskytovateli jsou vyžadovány v „oblasti veřejné moci“ – viz § 11 zákona o elektronickém podpisu.

[4] Praxe u jednotlivých poskytovatelů může být odlišná. Zde je popsán jeden z užívaných postupů. Vlastní postup uvádí každý poskytovatel ve své certifikační politice.

G.

Dalšími hledisky pro výběr poskytovatele je rozsah služeb, které nabízí, a jejich cena. Pokud Petr akceptuje pouze certifikát, který poskytovatel Aleně vydá na základě ověření její totožnosti, kdy se Alena musí prokázat příslušnými doklady, bude pro Alenu důležité i místo, kde poskytovatel své služby nabízí. Aby byli poskytovatelé svým zákazníkům co nejblíže, zřizují často v řadě míst tzv. **registrační autority,** které přijímají žádosti o vydání certifikátu.

H.

Než Alena poskytovatele navštíví, měla by se seznámit s jeho certifikační politikou. Jedná se o dokument, který je určený jak pro osoby, kterým poskytovatel vydává certifikáty (Alena), tak pro osoby, které se na tyto certifikáty spoléhají (Petr). Obsahuje nabídku služeb konkrétního poskytovatele a podmínky, za kterých tyto služby poskytuje. Poskytovatelé zveřejňují certifikační politiky zpravidla na svých webových stránkách.

I.

Když si Alena vybere určitého poskytovatele, najde si na jeho webových stránkách **žádost o vydání certifikátu**[5] a tu vyplní. Zároveň jí tak poskytovatel umožní vytvoření dvojice dat, kterou tvoří data pro vytváření elektronického podpisu a data pro ověřování elektronického podpisu[6]. Data pro vytváření podpisu si Alena ponechá a zůstávají jejím tajemstvím. Data pro ověřování podpisu jsou součástí vytvořené žádosti o vydání certifikátu a není důvod je utajovat, naopak jsou určena ke zveřejnění. Následně Alena celou žádost odnese k poskytovateli. Poskytovatel ověří totožnost Aleny a uzavře s ní smlouvu o vydání certifikátu.

[5] Praxe u jednotlivých poskytovatelů může být odlišná. Zde je popsán jeden z užívaných postupů. Vlastní postup uvádí každý poskytovatel ve své certifikační politice.

[6] Při použití technologie digitálního podpisu, v současné době jediné realizované technologie tzv. zaručeného elektronického podpisu, se užívá pro data pro vytváření elektronického podpisu pojem „soukromý klíč“ a pro data pro ověřování elektronického podpisu pojem „veřejný klíč“.

J.

Zpravidla si Alena vydaný certifikát od poskytovatele hned neodnese. Poskytovatel jej Aleně zašle na zvoleném nosiči poštou a tak si ověří, zda se Alena zdržuje na adrese, kterou má uvedenou v dokladech, které poskytovateli předložila, resp. zda se neprokázala doklady jiné osoby. Poskytovatel může certifikát zaslat i e-mailem a tak si ověřit správnost a platnost elektronické adresy, kterou Alena v žádosti uvedla. Zároveň poskytovatel Alenu vyzve, aby zkontrolovala, zda údaje uvedené v certifikátu jsou správné, a aby tuto správnost potvrdila elektronicky podepsanou zprávou, kterou e-mailem zašle poskytovateli. Tak si poskytovatel ověří, že Alena má data pro vytváření podpisu.

K.

Alena může mít data pro vytváření podpisu uložená na pevném disku svého počítače, na disketě, na čipové kartě nebo v nějakém jiném přenosném bezpečnostním modulu (souhrnně se takové nosiče nazývají „tokeny“). Tato data bude Alena používat, jak napovídá jejich název, pro vytváření svého elektronického podpisu. Alena je musí pečlivě střežit, aby je nemohl nikdo zneužít. Pokud tomu Alena nezabrání, může se ten, kdo se dat zmocní, podepisovat jako Alena, tj. „falšovat“ její podpis. V tomto případě ovšem grafolog nepomůže, na základě posouzení elektronického podpisu nelze rozlišit, kdo data pro podpis použil.

L.

Data pro vytváření podpisu tvoří s daty pro ověřování podpisu pevnou dvojici. Nelze nahradit, vyměnit nebo podvrhnout žádnou jejich část, aniž by tím nebyla narušena jejich vazba.

M.

Data pro ověřování podpisu jsou uvedena v certifikátu, který poskytovatel Aleně vydal. Certifikát může obsahovat i další údaje – obchodní jméno poskytovatele, který certifikát vydal, Alenino jméno a příjmení (případně její pseudonym), údaj o počátku a konci platnosti certifikátu[7], informaci o tom, že Alena je oprávněna se podpisovat jménem určitého subjektu (firmy, úřadu), údaj o omezení použití certifikátu na „nefinanční“ transakce, nebo omezení výše finančních transakcí – to vše podle účelu, ke kterému bude Alena certifikát používat. Alena si může nechat vystavit více certifikátů – každý pro jiný účel. Poskytovatel opatří vydávaný certifikát svým elektronickým podpisem. Tak jej chrání proti možnosti podvrhnutí jiného certifikátu a proti pozměnění údajů, které jsou v něm uvedeny. Současně tím poskytovatel stvrzuje, že údaje uvedené v certifikátu před vydáním certifikátu ověřil.

[7] Certifikáty se z důvodu bezpečnosti vydávají na omezenou dobu, zpravidla v rozsahu 6 měsíců až dvou, max. pěti let.

N.

Certifikát je vydán ve formě datové zprávy. Pokud by byl listinou, mohla by obsahovat následující text: „Já, níže podepsaný poskytovatel X.Y., vydávám Aleně tento certifikát k jejím datům pro ověřování podpisu. Ověřil jsem to-

tožnost Aleny a dále jsem ověřil, že Alena má data pro vytváření podpisu a jim odpovídající data pro ověřování podpisu. Tento certifikát vydávám na dobu 6 měsíců. Dále prohlašuji, že Alena předložila doklady, podle nichž je jednatelkou firmy AB a je oprávněna se jejím jménem podepisovat. Na základě Aleniny žádosti omezuji použití tohoto certifikátu na finanční transakce v max. výši 200 000 Kč“.

O.

Proč jsou Alenina data pro ověřování podpisu uvedena v certifikátu? Protože právě prostřednictvím certifikátu se dostanou bezpečnou a důvěryhodnou cestou k Petrovi a s jejich pomocí Petr ověří Alenin podpis. A kde Petr certifikát získá? Dostane jej zároveň s elektronicky podepsanou zprávou[8)].

8) To platí pro většinu běžně užívaných aplikací. Pokud Petr nedostane certifikát zároveň se zprávou, musí Alena Petrovi sdělit, kde může její certifikát získat, resp. kde je dostupný (například na tzv. klíčových serverech, na její webové stránce atd.).

P.

Nyní může Alena elektronicky podepsat zprávu, kterou napsala. Jak to provede? Zadá příkaz (klikne na příslušnou ikonu), aby zpráva byla elektronicky podepsána jejími daty pro vytváření elektronického podpisu. To, co se děje po zadání tohoto příkazu, Alena na svém monitoru nevidí ani se tohoto procesu nijak neúčastní[9)]. Výsledkem je elektronický podpis, který je ke zprávě přiložen. Elektronický podpis tak závisí na zprávě, ke které je přiložen, a na datech pro vytváření elektronického podpisu podepsané osoby, tj. Aleny.

9) Není nezbytné, aby Alena následující postup znala (stejně tak jako pravděpodobně neví, jaké procesy se odehrávají v motoru jejího auta, když nastartuje). Z napsané zprávy se pomocí hašovací funkce vytvoří tzv. otisk. Ať je na vstupu této funkce jakkoliv dlouhá zpráva, na jejím výstupu je otisk, který má pevnou délku (128, 160 bitů nebo více). Pokud by následně došlo ve zprávě k jakékoliv změně, otisk by byl odlišný. Pořízený otisk se dále šifruje pomocí zvoleného asymetrického algoritmu a pomocí Alenиných dat pro vytváření elektronického podpisu.

Q.

Pokud Alena dostatečně chrání svá data pro vytváření podpisu, nikdo jiný než ona takový podpis nevytvoří. Útočník se nemůže podepsat jako Alena.

Útočník sice může podvrhnout jinou zprávu či změnit obsah původní zprávy, ovšem Petr tuto změnu při ověřování podpisu zjistí.

R.

Petr dostane otevřený text zprávy, elektronický podpis Aleny a certifikát Aleny. Tak jako se Alena přímo nepodílela na procesu vytváření podpisu, stejně tak Petr nezasahuje do procesu ověřování Alenina podpisu[10)]. Většina aplikací sama ohlásí, že úspěšně ověřila podpis.

10) K otevřenému textu se vypočte otisk, který označíme jako otisk č. 1. Z Alenina elektronického podpisu se získá pomocí Aleniných dat pro ověřování elektronického podpisu otisk č. 2. Pokud se oba otisky rovnají, pak je zajištěno, že zpráva nebyla od okamžiku podepsání změněna a podpis byl vytvořen pomocí Aleniných dat pro vytváření elektronického podpisu. Následně se zkontroluje platnost Alenina certifikátu, a to z hlediska doby jeho platnosti (zda neuplynula doba platnosti, která je uvedena v certifikátu) a z hlediska toho, zda nebyl Alenin certifikát změněn.

S.

Petr musí zjistit ještě jednu okolnost, a to jestli je Alenin certifikát skutečně platný. Alena sice má v certifikátu uvedenu dobu, dokdy certifikát platí, ale před uplynutím této doby se mohla rozhodnout, že poskytovatele požádá, aby předčasně ukončil jeho platnost. Za jaké situace? Například tehdy, když ztratí svá data pro vytváření podpisu a má obavu, že se jejím jménem bude moci podepisovat někdo jiný. Vzhledem k tomu, že nelze měnit obsah vydaného certifikátu, není možné údaj o předčasném ukončení jeho platnosti do něj dodatečně zapsat.

T.

Poskytovatel pravidelně vydává seznam certifikátů, u nichž byla předčasně ukončena platnost[11)]. Do tohoto seznamu musí Petr nahlédnout a ujistit se, že Alenin certifikát v něm není uveden[12)].

11) Podle zákona o elektronickém podpisu se jedná o seznam certifikátů, které byly zneplatněny. Poskytovatelé vydávají tyto seznamy zpravidla na svých webových stránkách pod zkratkou CRL (certificate revocation list).

12) Toto zjištění většina běžných aplikací zatím automaticky neprovádí. Pokud si Petr „stahuje“ seznam do svého počítače, nesmí zapomenout na jeho pravidelnou aktualizaci („stahování“ aktuálního seznamu). Existují i tzv. on-line protokoly (OCSP), které umožňují přímý přístup k informacím o těchto certifikátech. Pokud Petrův software umí využít příslušný protokol, nemusí Petr provádět aktualizaci stahovaných seznamů. Potřebné informace poskytne každý poskytovatel.

U.

Pokud chce mít Petr skutečně jistotu, že Alenin certifikát byl platný v době, kdy Alena zprávu elektronicky podepsala, nahlédne do seznamu, který byl vydán až poté, kdy přijal Alenou podepsanou zprávu. Poskytovatelé vydávají tyto seznamy v pravidelných intervalech, například po 6 hodinách (tj. v 6, 12, 24 hodin). Může tedy nastat situace, kdy Alena v 7 hodin zjistí ztrátu svých dat pro vytváření podpisu, v 8 hodin požádá poskytovatele, aby ukončil platnost jejího certifikátu. Útočník v 9 hodin podepíše zprávu Aleninými daty. V 10 hodin Petr ověřuje Alenin podpis. Předpokládejme, že daný poskytovatel vydává seznam v 6, 12, 18 a ve 24 hodin. Petr tedy v 10 hodin nahlédne do seznamu, který byl vydán v 6 hodin. V něm pochopitelně informace, která nastala o několik hodin později, není. Proto musí Petr nahlédnout do seznamu, který bude vydán ve 12 hodin.

V.

Alena může elektronicky podepisovat nejen textové zprávy, ale vše, co existuje v elektronické podobě, např. obrázek, program, databázový soubor, makro apod.

W.

Alena může elektronicky podepsat i datové zprávy, které nemá v úmyslu nikomu předávat, ale chce je uchovat v elektronické podobě. Kdykoliv v budoucnu bude mít Alena při otevření těchto zpráv jistotu, že jejich obsah nebyl od okamžiku podepsání změněn.

X.

Pokud Alena bude chtít zachovat důvěrnost svých sdělení, musí je vhodným programem zašifrovat. Samotný elektronický podpis zprávu nešifruje a ponechává ji v otevřené podobě.

Y.

Není důvod se obávat toho, že je používání elektronického podpisu složité. Není o nic složitější, než je práce s e-mailovou poštou.

Z.

Objevují se pochybnosti, zda je možné se na elektronický podpis spoléhat. V běžném životě se spoléháme velmi často na podpis, který vypadá jako pouhý „klikyhák“ a kterému důvěřujeme, aniž máme příslušný podpisový vzor nebo daný podpis známe. Zaručený elektronický podpis nám poskytuje mnohem vyšší míru bezpečí, navíc z certifikátu získáme řadu důvěryhodně předaných informací.

6. TYPY ELEKTRONICKÝCH PODPISŮ

6.1 ÚVODNÍ POJMY

Celý systém elektronického podepisování dokumentů ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), je založen na několika základních pojmech. Definice těchto primitivů jsou uvedeny v § 2 tohoto zákona. Patří sem především:

- elektronický podpis,
- zaručený elektronický podpis,
- datová zpráva,
- podepisující osoba,
- poskytovatel certifikačních služeb,
- akreditovaný poskytovatel certifikačních služeb,
- certifikát,
- kvalifikovaný certifikát,
- data pro vytváření elektronických podpisů,
- data pro ověřování elektronických podpisů,
- prostředek pro vytváření elektronických podpisů,
- prostředek pro ověřování elektronických podpisů,
- prostředek pro bezpečné vytváření elektronických podpisů,
- prostředek pro bezpečné ověřování elektronických podpisů,
- nástroj elektronického podpisu,
- akreditace.

Pomocí těchto pojmů vymezíme různé typy elektronických podpisů, tedy různých typů podpisů, o kterých přímo nebo nepřímo hovoří zákon o elektronickém podpisu.

K vymezení jednotlivých typů použijeme následující kategorie: politika kvalifikovaného certifikátu (zpravidla uvedena v certifikační politice), formát elektronického podpisu, formát kvalifikovaného certifikátu, časové razítko, požadavek na bezpečný systém, požadavek na prostředek pro bezpečné vytváření elektronického podpisu (PBVP). Podle konkrétních požadavků na tyto kategorie pak definujeme typický profil pro následující typy elektronických podpisů:

- elektronický podpis,

- zaručený elektronický podpis,
- zaručený elektronický podpis založený na kvalifikovaném certifikátu,
- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb,
- kvalifikovaný podpis,
- kvalifikovaný podpis určený pro podepisování dokumentů, u nichž se předpokládá určitá doba archivace.

Takto definované podpisy se vyskytují v různých souvislostech ve Směrnici 1999/93/ES (dále jen „Směrnice“) a ve standardech ETSI (European Telecommunication Standards Institute) a CEN/ISSS (European Committee for Standardization/Information Society Standardization System).

6.2 ELEKTRONICKÝ PODPIS (GENERAL ELECTRONIC SIGNATURE)

Vyjdeme z vymezení, které je obsaženo v § 2 písm. a) zákona o elektronickém podpisu:

„elektronickým podpisem (se rozumí pro účely tohoto zákona) 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“.

Definice uvedená v článku 2 odst. 1 Směrnice zní:

"Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."

Překlad:

„Elektronickým podpisem se rozumí data v elektronické podobě, která jsou připojena k jiným elektronickým datům nebo jsou s nimi logicky spojena a která slouží jako metoda autentizace.“

Požadavky na námi definované a sledované kategorie jsou tedy zcela minimální. Nepožaduje se časové razítko, není definován žádný konkrétní formát nebo standard, který by popisoval tvar vytvořených nebo předávaných dat. Není použit certifikát nebo jiný způsob zveřejnění pomocných dat (např. dat pro ověřování podpisu, osobních dat podepisující osoby, informace o systému použitém při podpisu apod.) ani tato data nejsou definována.

Nejsou kladeny žádné specifické požadavky na použitý podpisový systém nebo na prostředek pro vytváření, případně pro ověřování elektronického podpisu.

Uvedené požadavky sestavíme do následující tabulky – tabulku se stejnou strukturou použijeme následně k definici všech dále uvedených typů elektronických podpisů.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	**Nezveřejnění nebo přímé poskytování politiky**	Zveřejnění politiky	Zveřejnění užívání PBVP
Formát elektronického podpisu	Elektronický podpis	Elektronický podpis + testování dat	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	Profil kvalifikovaného certifikátu		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	**Nižší úroveň**	Kvalifikovaná úroveň	
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Tento typ podpisu nemá pro příjemce příliš velkou vypovídací hodnotu a důvěra v něj je minimální. Slouží spíše pro informaci příjemce. Příkladem může být „podpis“ vložený pod klasický e-mail, ale i např. jméno autora uvedené v záhlaví článku (v elektronické podobě, dokument v MS Word apod.).

Skutečnost, že i tento podpis je podpisem ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu, vyplývá z § 3 odst. 1:

„Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem“.

6.3 ZARUČENÝ ELEKTRONICKÝ PODPIS (ADVANCED ELECTRONIC SIGNATURE)

Začněme opět definicemi. Porovnáním definice uvedené v zákoně o elektronickém podpisu, § 2 písm. b) a definice ve Směrnici, článek 2 odst. 2 zjistíme, že tento pojem je zaveden obdobným způsobem a nemůže dojít k zásadně odlišnému chápání.

Zákon o elektronickém podpisu, § 2 písm. b):

„zaručeným elektronickým podpisem (se rozumí pro účely tohoto zákona) elektronický podpis, který splňuje následující požadavky:
- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.“

Směrnice, článek 2 odst. 2:

" 'advanced electronic signature' means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control;
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."

Překlad:

„vylepšeným elektronickým podpisem“ se rozumí elektronický podpis, který splňuje tyto požadavky:
a) je jednoznačně spojen s podepisující osobou;
b) umožňuje identifikovat podepisující osobu;
c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou;
d) je spojen s daty, ke kterým se vztahuje, tak, aby bylo možno zjistit jakoukoliv následnou změnu těchto dat.

Požadavky na námi definované a sledované kategorie se vzhledem k předchozí definici mění. Stále se ještě nevyžaduje časové razítko, nevyžaduje se použití certifikátu ke zveřejnění dat pro ověření podpisu. Nově se zavádí přesné formáty pro vytváření a přenos elektronických podpisů. To je nutné především z hlediska kompatibility a interoperability. Základním dokumentem v této oblasti je Electronic Signature Formats (ETSI TS 101 733 V1.2.2, 2000-12).

Nově se zavádí požadavek na důvěryhodnost operačního systému, ve kterém se dokument podepisuje. Nejsou kladeny žádné specifické požadavky na podpisový prostředek nebo ověřovací prostředek. Bezpečnost těchto prostředků (použití, zabezpečení, ochrana) se zcela nechává na podepisující osobě (případně na osobě, která se spoléhá na podpis).

Uvedené požadavky opět sestavíme do tabulky:

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	**Nezveřejnění nebo přímé poskytování politiky**	Zveřejnění politiky	Zveřejnění užívání PBVP
Formát elektronického podpisu	**Elektronický podpis**	Elektronický podpis + testování dat	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	Profil kvalifikovaného certifikátu		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň		**Kvalifikovaná úroveň**
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Tento typ podpisu nemá pro příjemce příliš velkou vypovídací hodnotu a důvěra v něj je minimální. Slouží spíše pro informaci příjemce. Příkladem může být „podpis" vložený pod klasický e-mail, ale i např. jméno autora uvedené v záhlaví článku (v elektronické podobě, dokument v MS Word apod.).

Skutečnost, že i tento podpis je podpisem ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu, vyplývá z § 3 odst. 1:

„Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem".

6.4 ZARUČENÝ ELEKTRONICKÝ PODPIS ZALOŽENÝ NA KVALIFIKOVANÉM CERTIFIKÁTU (ADVANCED ELECTRONIC SIGNATURE USING QUALIFIED CERTIFICATE)

Začněme opět definicemi. K použití tohoto typu podpisu se zavádějí pojmy certifikát, kvalifikovaný certifikát a pojem poskytovatel certifikačních služeb. Připomeňme, že poskytovatelé certifikačních služeb se dělí na poskytovatele, kteří vydávají certifikáty, na poskytovatele, kteří vydávají kvalifikované certifikáty a na akreditované poskytovatele.

Definice typů certifikátů jsou uvedeny v § 2 písm. g) a h) zákona o elektronickém podpisu:

„g) certifikátem (se rozumí pro účely tohoto zákona) datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost",

„h) kvalifikovaným certifikátem (se rozumí pro účely tohoto zákona) certifikát, který má náležitosti stanovené tímto zákonem (viz § 12) a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty (viz § 6)".

Definice poskytovatelů certifikačních služeb jsou uvedeny v § 2 písm. e) a f) zákona o elektronickém podpisu:

„e) poskytovatelem certifikačních služeb (se rozumí pro účely tohoto zákona) subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy",

„f) akreditovaným poskytovatelem certifikačních služeb (se rozumí pro účely tohoto zákona) poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona".

Povinnosti poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, jsou obsaženy v § 6 zákona o elektronickém podpisu a jsou dále upřesněny v prováděcí vyhlášce č. 366/2001 Sb.

Každý poskytovatel certifikačních služeb může požádat Úřad pro ochranu osobních údajů o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Podmínky udělení akreditace jsou uvedeny v § 10 zákona o elektronickém podpisu. Ve Směrnici se požaduje, aby se jednalo o dobrovolný akt. Akreditovaný poskytovatel certifikačních služeb

by měl být chápán jako důvěryhodný poskytovatel těchto služeb. V zákoně o elektronickém podpisu je však ustanovení, které je z hlediska požadavku Směrnice problematické. Jedná se o § 11, který stanoví, že v oblasti veřejné moci se smí používat pouze kvalifikované certifikáty vydané akreditovaným poskytovatelem. Ten, kdo chce své certifikační služby nabízet pro využití v oblasti veřejné moci, musí tedy nejdříve získat akreditaci a dobrovolnost požadovaná Směrnicí pro poskytovatele certifikačních služeb v oblasti veřejné moci se stává nutností.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	**Zveřejnění politiky**	Zveřejnění užívání PBVP
Formát elektronického podpisu	Elektronický podpis	**Elektronický podpis + testování dat**	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň		**Kvalifikovaná úroveň**
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Vrátíme se k popisu jednotlivých typů podpisů. Požadavky na námi sledované kategorie se vzhledem k předchozímu typu dále rozšiřují. Stále se ještě nevyžaduje časové razítko. Zpřísňují se požadavky na přesné formáty pro vytváření a přenos elektronických podpisů. Používání formátů se rozšiřuje o stanovení požadavků na formáty kvalifikovaných certifikátů a o další související formáty (např. žádost o vydání certifikátu apod.). To je upraveno například dokumentem ETSI Qualified Certificates Profile (ETSI TS 101 862 V1.1.1, 2000–12). Požadavek na důvěryhodnost operačního systému, ve kterém se datová zpráva podepisuje, je stejný jako u předchozího typu. Požadavky na poskytovatele certifikačních služeb vydávající kvalifikované certifikáty upřesňuje vyhláška č. 366/2001 Sb. V Evropské unii řeší tuto otázku dokument Policy Requirements for CSPs Issuing Qualified Certificates (ETSI TS 101 456 V1.1.1, 2000–12).

Ani u tohoto typu podpisu není součástí profilu povinný požadavek na používání bezpečného podpisového nebo ověřovacího prostředku.

Tento typ podpisu je základním typem elektronického podpisu, kterým se zabývá zákon o elektronickém podpisu. Tento typ podpisu má pro příjemce vysokou vypovídací hodnotu a důvěra v něj je vysoká; je také podpořena právními aspekty, které vyplývají z použití takovéhoto podpisu a které plynou ze zákona o elektronickém podpisu. Slouží pro styk příjemce a jiného subjektu, který vlastní kvalifikovaný certifikát. Příjemce podepsanou osobu nemusí osobně znát, data pro ověřování elektronického podpisu získá příjemce z kvalifikovaného certifikátu. Právní jistota v souvislosti s tímto způsobem komunikace vyplývá ze zákona o elektronickém podpisu, nemusí se tedy na rozdíl od předchozího případu uzavírat speciální smlouvy pro právní podporu této komunikace. Důvěra v obsah certifikátu je podmíněna důvěrou v poskytovatele certifikačních služeb, který certifikát vydal. Tato důvěra vyplývá i ze skutečnosti, že zákon o elektronickém podpisu stanoví poskytovatelům vydávajícím kvalifikované certifikáty celou řadu povinností.

Podpisu může být použit i k „anonymnímu“ styku (místo jména podepisující osoby může být v kvalifikovaném certifikátu uveden pseudonym, ovšem s označením, že se jedná o pseudonym). V případě právního sporu může být „anonymní“ držitel certifikátu dohledán prostřednictvím údajů, které má k dispozici poskytovatel certifikačních služeb. Uvedený typ podpisu lze použít všude tam, kde se v zákoně o elektronickém podpisu umožňuje použít elektronický podpis. Tento typ podpisu je přímo vyžadován v § 11, který stanoví způsob komunikace v oblasti veřejné moci. Tento profil je, jak jsme se již zmínili, zpřísněn – nestačí, aby byl kvalifikovaný certifikát vydán poskytovatelem, který vydává kvalifikované certifikáty, ale poskytovatelem, který byl akreditován Úřadem pro ochranu osobních údajů.

Obecně se považuje tento typ za vhodný pro přímou komunikaci mezi subjekty. Není vhodný k archivaci dat a tam, kde je nutné zpětně prokazovat, kdy přesně byl dokument podepsán.

6.5 KVALIFIKOVANÝ PODPIS (QUALIFIED ELECTRONIC SIGNATURE)

Dostáváme se k velice důležitému pojmu kvalifikovaný podpis. Tento termín není v zákoně o elektronickém podpisu přímo použit. Přesto je na několika místech zmíněn, vždy však jen opisem. Poprvé se s ním můžeme setkat v § 3 odst. 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."

Od předchozího typu se tento typ liší požadavkem na použití prostředku pro bezpečné vytváření podpisu. Požadavky na tento prostředek jsou uvedeny v § 17 zákona o elektronickém podpisu. V členských zemích Evropské unie se otázkou bezpečných prostředků zabývá celá řada dokumentů. Řada otázek však v době psaní tohoto příspěvku ještě nebyla dořešena. Příkladem těchto dokumentů mohou být následující dokumenty CEN/ISSS :

- Secure Signature-Creation Devices (EAL 4 and EAL 4+), (CWA Draft on Area F),
- Security Requirements for Signature Creation Systems (CWA Draft on Area G1),
- Procedures for Electronic Signature Verification V1.0.3 (2001-01-25, CWA Draft on Area G2),
- EESSI Conformity Assessment Guidance; Version 2.0 (2001-01-22, CWA Draft on Area V).

Pojmy prostředek pro bezpečné vytváření podpisu a prostředek pro bezpečné ověřování podpisu patří k nejproblematičtějším v celém systému elektronického podepisování. Přesné požadavky na tyto prostředky nebyly dosud zcela zformulovány. Obecně se tyto požadavky dají rozdělit do tří oblastí: požadavky technicko-kryptografické, požadavky na začlenění těchto prostředků do informačního systému a legislativně právní požadavky. Nejsou dořešeny ani otázky související s hodnocením bezpečnosti takových prostředků. Přísnější kritéria se uplatňují při jejich hodnocení v Německu a Rakousku. Zde se hodnotí i aplikace, ve které je prostředek používán. V jiných členských státech Evropské unie se hodnocení soustřeďuje pouze na prostředek a hodnocení spočívá pouze v hodnocení z pohledu technicko-kryptografického. V řadě členských států Evropské unie se ještě k hodnocení prostředků nepřistoupilo. Celá problematika je natolik komplexní a složitá, že si zaslouží samostatné podrobné odborné zhodnocení.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	Zveřejnění politiky	**Zveřejnění užívání PBVP**
Formát elektronického podpisu	Elektronický podpis	**Elektronický podpis + testování dat**	Elektronický podpis + testování dat + časová razítka
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň		**Kvalifikovaná úroveň**
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	Nižší úroveň	**Kvalifikovaná úroveň**	Vyšší úroveň

Kvalifikovaný podpis se považuje z hlediska důvěry za nejvhodnější. Tento podpis má pro příjemce vysokou vypovídací hodnotu. V dokumentech EU se uvažuje, že by mohl být používán v těch situacích, kde se v písemné podobě vyžaduje vlastnoruční podpis. V české legislativě by jeho využití namísto vlastnoručního podpisu však patrně znamenalo změnu (novelu) příslušných právních předpisů, a to například vložením věty „ ...toto musí být podepsáno vlastnoručně nebo pomocí kvalifikovaného podpisu... " do textu příslušných právních předpisů.

6.6 „VYLEPŠENÝ" ELEKTRONICKÝ PODPIS (ENHANCED ELECTRONIC SIGNATURE)

Tento typ je obecně použitelný s libovolným předchozím typem. Liší se přidáním některého z dalších požadavků na podpis, který není součástí zaručeného elektronického podpisu ani nesouvisí s předchozími typy (např. časová značka, rozšířené požadavky na verifikaci, rozšířené požadavky na podpisový prostředek, rozšířená ochrana proti určitému druhu útoků).

6.7 KVALIFIKOVANÝ PODPIS URČENÝ PRO ARCHIVACI DAT (QUALIFIED ELECTRONIC SIGNATURE WITH LONG-TERM VALIDITY)

Nejdůležitějším typem, který vznikl jako vylepšený elektronický podpis z kvalifikovaného podpisu, je kvalifikovaný podpis určený pro archivaci dat.

Tento podpis je blíže představen ve standardu ETSI Policy requirements for CSPs issuing trusted time stamps, ve kterém jsou zformulovány minimální požadavky v oblasti bezpečnosti a kvality zabezpečení důvěryhodného poskytování služeb určených k vydávání časových razítek. Časová razítka jsou specifikována v dokumentu ETSI Time Stamping Profile (draft ETSI TS 101 861 V.1.1.4). Vzhledem k tomu, že musí být zajištěna odolnost proti útokům po celou dobu archivace, je v kategorii prostředek pro bezpečné vytváření podpisu vznesen požadavek zvýšené bezpečnosti.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	Zveřejnění politiky	**Zveřejnění užívání PBVP**
Formát elektronického podpisu	Elektronický podpis	Elektronický podpis + testování dat	**Elektronický podpis + testování dat + časová razítka**
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	**Použití protokolu pro časová razítka**		
Požadavek na bezpečný systém	Nižší úroveň		**Kvalifikovaná úroveň**
Požadavek na prostředek pro bezpečné vytváření elektronického podpisu	Nižší úroveň	Kvalifikovaná úroveň	**Vyšší úroveň**

Vzhledem ke specifickým požadavkům je využití zřejmé – dlouhodobá archivace elektronicky podepsaných dokumentů v elektronické formě. V této souvislosti se připomíná, že pokud tuto službu zajišťuje poskytovatel certifikačních služeb, měl by zajistit i uchování příslušného software, který umožní otevření a zobrazení podepsaných dat i v době, kdy tento software již není běžně používán.

Literatura:

[1] Matejka, J.,Vondruska, P.: The basic terms and legal aspects of the ESA from the practical use and security points of view, sborník mezinárodní konference IDET, Brno 2001

[2] Vondruška, P.: Typy elektronických podpisů, sborník konference Bezpečnosť dát 2001, Bratislava

[3] Vondruška, P.: Bezpečnostní požadavky na jednotlivé typy EP a PCS, Elektronický podpis a antivirová ochrana komunikačních systémů, Vojenská akademie Brno, 2001

[4] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures, http://www.ict.etsi.org/eessi/e-sign_directive.pdf

[5] ETSI, European Telecommunication Standards Institute, http://www.etsi.org/sec/el-sign.htm

[6] CEN/ISSS, European Committee for Standardization/Information Society Standardization System, http://www.ni.din.de, http://www.cenorm.be/isss/worksho/e-sign

7. PROSTŘEDEK PRO BEZPEČNÉ VYTVÁŘENÍ ELEKTRONICKÉHO PODPISU A NÁSTROJ ELEKTRONICKÉHO PODPISU

Tato kapitola je věnována vysvětlení pojmu prostředek pro bezpečné vytváření a ověřování elektronického podpisu (§ 7 vyhlášky), nástroj elektronického podpisu (§ 8 vyhlášky) a vztahu mezi nimi, dále postupu při vyslovení shody nástroje s požadavky stanovenými v zákoně o elektronickém podpisu a vysvětlení rozdílu v chápání obsahu těchto pojmů v dokumentech Evropské unie a v zákoně o elektronickém podpisu.

7.1 PROSTŘEDEK PRO BEZPEČNÉ VYTVÁŘENÍ A OVĚŘOVÁNÍ ZARUČENÝCH ELEKTRONICKÝCH PODPISŮ

Začněme informací k překladu těchto pojmů z anglicky psaných materiálů Evropské unie. Je potřeba vědět, že v těchto materiálech se používá v souvislosti s pojmem nástroj elektronického podpisu termín „product“ („electronic-signature product“ – nástroj elektronického podpisu), zatímco termín „device“ je určen pro český termín prostředek (srovnej např. secure signatur-creation device – prostředek pro bezpečné vytváření elektronických podpisů).

Požadavky na prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů jsou uvedeny v § 17 zákona o elektronickém podpisu. Požadavky na tyto prostředky vycházejí z obdobných obecných požadavků Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy, tak, jak jsou uvedeny v příloze č. III této Směrnice.

Tyto požadavky mají především zajistit, aby prostředek pro bezpečné vytváření podpisu za pomoci odpovídajících technických a programových prostředků a postupů zaručil, že data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno, že 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. Tento prostředek musí dále zajistit, aby data pro vytváření podpisu mohla být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou. 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.

Obdobné jsou i bezpečnostní a procesní požadavky na prostředek pro bezpečné ověřování podpisu. Nově se zde zavádějí požadavky související se zobrazením výsledku ověření, případně se spolehlivým zobrazením dat uvedených v certifikátu. Jedná se zejména o tyto požadavky:

- podpis musí být spolehlivě ověřen a výsledek tohoto ověření musí být řádně zobrazen,
- ověřující osoba musí mít možnost spolehlivě zjistit obsah podepsaných dat,
- spolehlivě musí být zjištěna pravost a platnost certifikátu při ověřování podpisu,
- výsledek ověření a případné použití pseudonymu musí být řádně zobrazeno.

Uvedené požadavky jsou upřesněny v § 7 prováděcí vyhlášky k zákonu o elektronickém podpisu. Konkretizují se zde alespoň některé z požadavků, např. se vyžaduje, aby podepisující osoba byla informována, že používá tento prostředek, a musela před jeho použitím zadat přístupové heslo nebo použít jiný obdobný autentizační mechanismus. Upřesněny jsou i požadavky na kryptografické algoritmy a jejich parametry. Tyto požadavky jsou uvedeny v příloze č. 2 vyhlášky. Příloha byla zpracována podle obdobného dokumentu Evropské unie, a to dokumentu Algorithms and Parameters for Secure Electronic Signatures, který vydala EESSI (The European Electronic Signature Standardization Initiative). V tomto dokumentu se stanoví asymetrické kryptografické algoritmy včetně algoritmů založených na eliptických křivkách, které budou pro účely bezpečných elektronických podpisů považovány po dobu 5 let (od začátku roku 2001) za bezpečné. V tomto dokumentu jsou dále stanoveny i parametry klíčů, způsob generování klíčů a další technické detaily.

Vyhláška dále vyžaduje pro prostředek pro bezpečné vytváření zaručeného elektronického podpisu dostatečnou technickou a kryptografickou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek odpovídá požadavkům technické normy upravující oblast informační bezpečnosti. Touto normou je ČSN ISO 15408 a příslušná úroveň záruky je EAL 4. Požadavek byl stanoven v souladu s dokumenty standardizační komise CEN/ISSS (European Committee for Standardization/Information Society Standardization System) N137-Secure Signature – Creation Device a N141--Security Requirements for Signature Creation Applications.

Splnění požadavků na prostředek pro bezpečné vytváření zaručeného elektronického podpisu stanovených v § 17 zákona o elektronickém podpisu se dokládá výsledkem hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu a seznamem technických norem upravujících oblast informační bezpečnosti, podle kterých byl hodnocen. Poskytovatel není omezen ve volbě subjektu, který takové potřebné hodnocení může provést. Předpokládá se přebírání hodnocení z laboratoří v členských státech Evropské unie. Časem pravděpodobně vznikne hodnotitelské pracoviště i v České republice. Aby bylo uznáno hodnocení tohoto pracoviště i v členských státech Evropské unie, je nutné zapojení tohoto pracoviště do evropského akreditačního systému. Ve Směrnici 1999/93/ES se k hodnocení prostředků pro elektronické podpisy uvádí pouze toto:

„Příslušné veřejnoprávní či soukromé subjekty pověřené členskými státy stanoví shodu prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III. V souladu s postupem uvedeným v článku 9 stanoví Komise kritéria, podle nichž členské státy stanoví, zda může být daný subjekt pověřen."

V současné době ještě v členských státech Evropské unie není zcela shoda v tom, jak bude toto ustanovení Směrnice realizováno.

Zákon o elektronickém podpisu nestanoví žádnému subjektu povinné používání prostředku pro bezpečné vytváření a ověřování elektronického podpisu. Je pouze na podepisující osobě nebo na osobě, která se spoléhá na podpis, zda takový prostředek (např. z důvodu vyšší bezpečnosti, a tedy i právní jistoty) používá nebo ne. Poněkud deklarativně se o tomto podpisu mluví pouze v paragrafu 3 odst. 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."

Shrnutí

1. V zákoně o elektronickém podpisu není stanovena žádnému subjektu povinnost používat prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů.
2. Používáním těchto prostředků se zvyšuje důvěra v tento způsob komunikace.

3. Kvalifikovaný podpis je zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření elektronického podpisu.
4. Prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů musí splňovat bezpečnostní požadavky podle ISO 15408, na úroveň záruky EAL 4; v České republice je toto hodnocení uznáváno z kterékoliv testovací laboratoře, která je schopna tyto testy provádět.

7.2 NÁSTROJ ELEKTRONICKÉHO PODPISU

Pojem nástroj elektronického podpisu je širší než pojem prostředek pro bezpečné vytváření a ověřování elektronického podpisu.

V zákoně o elektronickém podpisu je pojem nástroj elektronického podpisu vymezen v § 2 písm. o) takto:

„Pro účely tohoto zákona se rozumí nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů".

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje svým zaručeným elektronickým podpisem vydávané kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Nástroj elektronického podpisu používaný pro toto podepisování nelze z důvodu vyšší bezpečnosti použít pro jiné než tyto účely!

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty musí používat bezpečný nástroj elektronického podpisu a tato skutečnost musí být ověřena Úřadem pro ochranu osobních údajů.

Úřad pro ochranu osobních údajů vyhodnocuje na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

Pokud nástroj elektronického podpisu splnil požadavky stanovené zákonem o elektronickém podpisu a Úřad vyslovil shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, zveřejňuje Úřad ve Věstníku Úřadu a na svých webových stránkách (http://www.uoou.cz/ep_nastroje.php3).

Jiné subjekty, například podepisující osoba, elektronická podatelna, poskytovatel certifikačních služeb, který nevydává kvalifikované certifikáty, nemají povinnost takový nástroj používat. Jeho cena je vysoká a pohybuje se v tisících USD.

Za podání žádosti o vyhodnocení shody nástroje elektronického podpisu se platí správní poplatek 10 000 Kč.

Shrnutí

1. Nástroj elektronického podpisu je prostředek pro vytváření elektronického podpisu, který lze používat k podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny.
2. Poskytovatelé certifikačních služeb, kteří vydávají kvalifkované certifikáty, musí takový nástroj elektronického podpisu používat.
3. Shodu nástroje s požadavky zákona o elektronickém podpisu vyslovuje v České republice Úřad pro ochranu osobních údajů.

7.3 EVROPSKÁ UNIE

Ve Směrnici 1999/93/ES se rozlišují prostředky pro bezpečné vytváření elektronického podpisu (SSCD – secure signature electronic device) a nástroje elektronického podpisu (electronic signature product). Požadavky na prostředky pro bezpečné vytváření elektronického podpisu jsou uvedeny v příloze III Směrnice. Shoda prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III Směrnice má být posouzena k tomu členskými státy určenými odpovídajícími veřejnoprávními či soukromými organizacemi. Ve Směrnici není stanoveno, zda má být také hodnocen nástroj elektronického podpisu.

Na základě výše uvedených skutečností lze předpokládat, že vymezení pojmů nástroje a prostředku elektronického podpisu v zákoně o elektronickém podpisu a v prováděcí vyhlášce jsou v zásadě v souladu s obsahem Směrnice 1999/93/ES.

Shrnutí

1. Prostředky pro bezpečné vytváření elektronického podpisu musí být hodnoceny podle stejných kritérii v členských státech Evropské unie i České republice. Vzhledem k tomu, že v České republice chybí specializované hodnotitelské pracoviště, hodnocení je možné převzít ze zahraničí.

2. Nástroje elektronického podpisu nemusí být v současné době hodnoceny ve všech členských státech Evropské unie, povinné je jejich hodnocení např. v Německu a Rakousku. V České republice musí být hodnoceny pouze nástroje, které používá poskytovatel vydávající kvalifikované certifikáty, a to jen ty nástroje, které používá k podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny. Shodu se stanovenými požadavky vyslovuje Úřad pro ochranu osobních údajů.

Literatura:

[1] Matejka, J., Vondruska, P.: The basic terms and legal aspects of the ESA from the practical use and security points of view, sborník mezinárodní konference IDET, Brno 2001

[2] Vondruška, P.: Typy elektronických podpisů, sborník konference Bezpečnosť dát 2001, Bratislava

[3] Vondruška, P.: Bezpečnostní aspekty elektronického podpisu, sborník konference Security 2001, Praha

[4] Vondruška, P.: Anatomie prováděcí vyhlášky ÚOOÚ k zákonu o elektronickém podpisu č. 227/2000 Sb., sborník, konference Současnost a budoucnost krizového managementu, Praha 2001

[5] Vondruška, P.: Elektronický podpis, Řízení místních orgánů 2002, RAABE, Praha 2002

[6] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures, http://www.ict.etsi.org/eessi/e-sign_directive.pdf

[7] CEN/ISSS, European Committee for Standardization/Information Society Standardization System, http://www.ni.din.de, http://www.cenorm.be/isss/worksho/e-sign

[8] EESSI, European Electronic Signature Standardization Initiative http://www.ict.etsi.org/eessi/EESSI-homepage.htm

[9] Zákon č. 227/2001 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), http://www.mvcr.cz/sbirka/2000/sb068-00.pdf

[10] Vyhláška č. 366/2001 Sb. (k zákonu o elektronickém podpisu), http://www.mvcr.cz/sbirka/2001/sb138-01.pdf

8. VYSVĚTLENÍ ZÁKLADNÍCH POJMŮ

Pojmy jsou vysvětleny pouze ve vztahu k elektronickém podpisu, zejména k zákonu o elektronickém podpisu. Jejich případné další významy nejsou uvedeny.

Akreditace

Viz též ***Poskytovatel certifikačních služeb***

Akreditace ve smyslu zákona o elektronickém podpisu je osvědčení vydávané Úřadem pro ochranu osobních údajů (dále jen Úřad) poskytovatelům certifikačních služeb. Požádat o udělení akreditace pro výkon činnosti akreditovaného poskytovatele může každý poskytovatel. V žádosti o akreditaci musí doložit skutečnosti podle § 10 odst. 2 zákona. Akreditovaný poskytovatel musí mít sídlo na území České republiky. Kromě činností uvedených v zákoně o elektronickém podpisu může akreditovaný poskytovatel certifikačních služeb bez souhlasu Úřadu působit jen jako advokát, notář nebo znalec. Nad činností akreditovaných poskytovatelů vykonává Úřad dozor.

Působení akreditovaných poskytovatelů je nezbytné v oblasti orgánů veřejné moci, neboť podle **§ 11 zákona:**
V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb.

§ 2 písm. p) zákona
akreditací (se rozumí) osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

Certificate Revocation List (CRL)

Viz též ***Seznam kvalifikovaných certifikátů, které byly zneplatněny***

Při vydávání certifikátu je stanoveno a přímo v certifikátu uvedeno, na jaké časové údobí se vydává, resp. do jakého data bude platný. Mohou však nastat okolnosti, kdy je nezbytné ukončit platnost certifikátu dříve, než bylo při jeho vydání stanoveno. Může se jednat o změnu jména osoby, které byl certifikát vydán, nebo obecně o změnu některého z údajů uvedených v certifikátu, vyzrazení nebo hrozbu vyzrazení dat pro vytváření elektronického podpisu. Za těchto okolností poskytovatel ukončí platnost certifikátu. Poskytovatel vydává strukturovaný dokument, s předem stanovenou periodicitou vydávání, který se nazývá Certificate Revocation List (CRL – viz Certificate Revocation List). CRL obsahuje přesný časový údaj, kdy byl vydán, a identifikuje certifikáty, které byly zneplatněny. CRL je podepsán elektronickým podpisem poskytovatele a je veřejně přístupný, zpravidla na webových stránkách poskytovatele. Každý zneplatněný certifikát je v CRL identifikován svým unikátním číslem (jedinečným u daného poskytovatele). Toto číslo je certifikátu přiděleno už při jeho vydání. Osoba, která se na podpis spoléhá, do CRL nahlíží, aby zjistila, zda v něm není uvedeno číslo certifikátu, jehož platnost právě ověřuje.

Kdy osoba spoléhající se na podpis zpravidla používá CRL? Při přijetí elektronicky podepsané zprávy aplikace nejprve zkontroluje platnost certifikátu podepisující osoby, a to z hlediska doby jeho platnosti (zda neuplynula doba platnosti, která je v něm uvedena) a z hlediska toho, zda nebyl tento certifikát změněn – toto zjistí ověřením elektronického podpisu poskytovatele. Osoba spoléhající se na podpis se musí následně ujistit, zda platnost certifikátu nebyla ukončena předčasně (zpravidla nevykoná aplikace sama). Osoba spoléhající se na podpis „nahlédne“ do CRL, který zveřejnil poskytovatel, který podepisující osobě certifikát vydal. Není ovšem nezbytné prohlížet jednotlivé položky CRL, ale lze jej „stáhnout“ do svého počítače a implementovat do aplikace, která v rámci ověření zjišťuje, zda certifikát není v CRL uveden. Osoba spoléhající se na podpis by měla CRL pravidelně aktualizovat („stahovat“ aktuální CRL), neboť starší aplikace toto zpravidla sama neučiní ani nerozpozná, že CRL není aktuální.

Zákon o elektronickém podpisu používá pojem „seznam certifikátů, které byly zneplatněny“. Vztahují se k němu zejména tato ustanovení:

§ 5 odst. 2 zákona
Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. 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 odst. 1 zákona
poskytovatel vydávající kvalifikované certifikáty je povinen

písm. g)
zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem

písm. 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

§ 15 odst. 2 zákona

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.

Certifikační autorita

Viz též ***Poskytovatel certifikačních služeb***

Poskytovatel certifikačních služeb je autorita, která je důvěryhodná pro uživatele certifikačních služeb, tj. je důvěryhodná jak pro podepisující osoby, kterým vydává certifikáty, tak pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny. Certifikační autorita zejména vydává certifikáty, za stanovených podmínek je zneplatňuje a vydává CRL (viz Certificate Revocation List). Vydané certifikáty a CRL podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci, a je identifikovatelná jako subjekt, který je vydal.

Certifikační autorita může některé činnosti zajišťovat prostřednictvím jiných subjektů, např. služby registračních autorit (viz Registrační autorita), vždy však na ní zůstává odpovědnost za poskytované služby. Certifikační autorita může prostřednictvím jiných subjektů zajišťovat i vydávání certifikátů, vždy však data pro vytváření elektronického podpisu (soukromý klíč), kterým jsou tyto certifikáty podepisovány, musí být identifikovatelná jako náležející certifikační autoritě a certifikační autorita je odpovědná za náležité zacházení s nimi.

Certifikační autoritou se rozumí „certification-service-provider“ ve smyslu Směrnice 1999/93/ES o zásadách společenství pro elektronické podpisy a „poskytovatel certifikačních služeb“ ve smyslu zákona o elektronickém podpisu (viz Poskytovatel certifikačních služeb). Někdy je pod pojmem „certifikační autorita“ chápán pouze HW a SW, s jejichž pomocí jsou certifikáty vydávány.

Certifikační politika

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty je povinen vydat certifikační politiku a umožnit k ní trvalý dálkový přístup. Tento dokument je z hlediska jeho zákazníků – tedy žadatelů o certifikát – velice důležitý. Obsahuje informace o poskytovateli, o jeho službách a jejich cenách. Na základě tohoto dokumentu může žadatel posoudit kvalitu nabízených služeb, dále například zjistit, zda je poskytovatel pojištěn nebo jak postupuje v krizových situacích. Certifikační politika slouží pro výběr vhodného poskytovatele. Doporučená struktura tohoto dokumentu je obsažena v RFC 2527.

K předepsanému obsahu certifikační politiky se vztahuje **§ 2 odst. 2** vyhlášky č. 366/2001 Sb.

Obsahem certifikační politiky je zejména:

a) stanovení zásad, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy a

b) popis vlastností dat pro vytváření elektronického podpisu a jim odpovídajících dat pro ověřování elektronického podpisu, která si vytváří osoba žádající o vydání kvalifikovaného certifikátu a k nimž má být vydán kvalifikovaný certifikát; kryptografické algoritmy a jejich parametry, které musí být pro tato data použity, jsou uvedeny v příloze č. 1 této vyhlášky.

Certifikát

Viz též ***Kvalifikovaný certifikát***

Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby. Jedná se o datovou zprávu, která je vydána poskytovatelem certifikačních služeb a která spojuje data pro ověřování podpisu (viz Data pro vytváření a data pro ověřování elektronického podpisu) s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují.

Vydáním certifikátu poskytovatel stvrzuje, že data pro ověřování elektronického podpisu patřící určité osobě a že ve spojení s daty pro vytváření elektronického podpisu podepisující osoby vykonávají požadované funkce.

Certifikát tedy představuje spojení mezi daty pro ověřování elektronického podpisu a identitou určité osoby (ve smyslu: „tato data patří osobě X.Y.“). Identitu podepisující osoby podle typu certifikátu může poskytovatel zjišťovat různými způsoby, v některých případech postačí e-mailová adresa, v jiných je nutné osobně prokázat totožnost příslušnými doklady.

Zákon o elektronickém podpisu neupravuje jiné předávání dat pro ověřování elektronického podpisu než prostřednictvím kvalifikovaných certifikátů (viz Kvalifikovaný certifikát). V praxi jsou používány i jiné způsoby nebo certifikáty, které nejsou kvalifikované ve smyslu zákona o elektronickém podpisu. Certifikáty jako standardní způsob předávání dat pro ověřování elektronického podpisu používá například Microsoft Outlook nebo Outlook Express. Data pro ověřování elektronického podpisu lze také vystavit v inter-

netové síti veřejných klíčů (např. u PGP) či na jakémkoliv jiném vhodném místě, kde se s nimi mohou seznámit ti, se kterými má podepisující osoba v úmyslu komunikovat. Pro ověření „pravosti“ dat pro vytváření elektronického podpisu se používá rovněž jejich podepisování jinou osobou, osobní předání jejich otisku (jednoznačné identifikace, angl. hash) například na vizitce nebo zaslání otisku e-mailem a následným ověřením telefonicky, pokud má ověřující jistotu, že danou osobu pozná po hlase.

V souvislosti s vydáváním certifikátů se lze setkat s pojmy „rekey“, „renewal“ a „update“. Ty souvisejí s vydáním nového certifikátu osobě, která má dosud platný certifikát vydaný tímto poskytovatelem. V této souvislosti mohou nastat následující situace, případně jejich modifikace:

- Nový certifikát je ve srovnání s dosud platným certifikátem vydán s jinými daty pro ověřování podpisu podepisující osoby, s jiným unikátním číslem a případně s uvedením jiné doby platnosti. Další údaje zůstávají nezměněny. Dosud platný certifikát může zůstat dále v platnosti, a to až do uplynutí doby platnosti v certifikátu uvedené, je však nepřípustné v tomto certifikátu jakékoliv údaje dále měnit, a to včetně dat pro ověřování podpisu podepisující osoby a doby platnosti certifikátu (zpravidla angl. rekey).
- Vydáním nového certifikátu je prodloužena platnost dat uvedených v dosud platném certifikátu. V novém certifikátu se ve srovnání s dosud platným certifikátem mění pouze doba platnosti a unikátní číslo. Další údaje, včetně dat pro ověřování podpisu podepisující osoby, zůstávají v novém certifikátu stejné jako v dosud platném certifikátu (zpravidla angl. renewal).
- Nový certifikát je vydán z důvodu, že došlo k tak zásadním změnám v údajích uvedených v dosud platném certifikátu, že je nutné tento certifikát zrušit (zpravidla angl. update).

Zákon o elektronickém podpisu neobsahuje odpovídající pojmy pro rekey, renewal a up-date ani speciálně neupravuje výše uvedené situace.

K vydávání a následné správě kvalifikovaných certifikátů se vztahují celá ustanovení zákona o elektronickém podpisu, uveďme alespoň následující:

§ 2 písm. g) zákona

certifikátem (se rozumí) datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost

§ 6 odst. 1 zákona

Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen

písm. a)

zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti kvalifikovaných certifikátů stanovené tímto zákonem

písm. b)

zajistit, aby údaje uvedené v kvalifikovaných certifikátech byly přesné, pravdivé a úplné

písm. 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

písm. 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,

písm. 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.

CRL

viz ***Certification Revocation List***

Časové razítko

Časové razítko je údaj, který lze přidat k elektronicky podepsané datové zprávě a který stvrzuje, že datová zpráva existovala dříve, než k ní bylo toto razítko přidáno. Takové stvrzení musí učinit někdo důvěryhodný a nezávislý na podepisující osobě a příjemci zprávy. Může se jednat o jednu ze služeb, které poskytuje poskytovatel, nebo ji může nabízet jiný subjekt.

U datových zpráv, u kterých se předpokládá dlouhodobé uchování, je možné např. díky použití časového razítka prokázat, že datová zpráva byla podepsána v době platnosti příslušného certifikátu.

Vzhledem k tomu, že jiný způsob prokázání času, kdy byla datová zpráva elektronicky podepsána, je velmi problematický, je možné předpokládat rozvoj služeb časových razítek.

Zákon o elektronickém podpisu používání časových razítek neupravuje.

Data pro vytváření a data pro ověřování elektronického podpisu

Viz též ***Podepisující osoba, Digitální podpis***

Data pro vytváření elektronického podpisu slouží, jak název napovídá, pro jeho vytvoření. Nestačí však zprávu elektronicky podepsat, je nutné ještě zajistit, aby mohlo být ověřeno, kdo zprávu podepsal. K tomu slouží data pro ověřování elektronického podpisu, která musí být odpovídající datům pro vytváření, tj. obojí data musí být taková, aby ve spojení zajišťovala požadované funkce. Data pro ověřování elektronického podpisu se při použití technologie digitálního podpisu nazývají „veřejný klíč" a data pro vytváření elektronického podpisu „soukromý klíč". Tato data si každý zájemce generuje prostřednictvím aplikace pro generování klíčů. Data pro vytváření podpisu musí podepisující osoba uchovat v tajnosti, data pro ověřování podpisu jsou naopak určena ke zveřejnění. Data pro ověřování podpisu je nutné bezpečně předávat mezi podepisující osobou a osobou, která se na podpis spoléhá – zpravidla příjemce elektronicky podepsané zprávy. K tomuto bezpečnému předání může sloužit certifikát (viz příslušné heslo), což je datová zpráva, která spojuje data pro ověřování podpisu s osobou, které byl vydán (tj. s podepisující osobou) a umožňuje ověřit její totožnost.

Poskytovatelé nabízejí možnost vygenerovat data ve spolupráci s nimi, resp. umožňují jejich vygenerování. To však zpravidla neznamená, že poskytovatel data sám vygeneruje. V takovém případě by hrozilo nebezpečí, že pokud bude poskytovatel nedůvěryhodný a bude znát data pro vytváření elektronického podpisu osoby, které vydává certifikát, může je zneužít jako kdokoliv jiný.

Někteří poskytovatelé, zejména v zahraničí, nabízejí službu generování dat pro vytváření elektronického podpisu. Pokud by tuto službu měl v úmyslu nabídnout poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty podle zákona o elektronickém podpisu, musí mít na zřeteli ustanovení § 6 odst. 3 zákona, podle kterého „nesmí uchovávat a kopírovat data pro vytváření zaručeného elektronického podpisu osob, kterým poskytuje své certifikační služby".

Úmysl získat certifikát se vyjádří vyplněním žádosti o vystavení certifikátu a jejím odesláním (předáním) poskytovateli. Součástí procesu vyplňování žádosti je generování dvojice dat pro vytváření a ověřování elektronického podpisu (asymetrických šifrovacích klíčů) v prostředí počítače žadatele o certifikát. Data pro vytváření elektronického podpisu zůstávají uložena u žadatele, data pro ověřování elektronického podpisu se stávají součástí žádosti o vydání certifikátu.

Data pro vytváření elektronického podpisu mohou být uložena na pevném disku počítače, na disketě, na čipové kartě nebo v přenosném bezpečnostním modulu (souhrnně „tokeny"). Je vhodné, aby přístup k těmto datům byl chráněn přístupovým heslem, frází, PINem apod., které zná jen jejich vlastník. Volba nosiče by měla odpovídat účelu, pro který bude elektronický podpisu používán.

§ 2 písm. i) zákona
daty pro vytváření elektronických podpisů (se rozumí) jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu

§ 2 písm. j) zákona
daty pro ověřování elektronických podpisů (se rozumí) jedinečná data, která se používají pro ověření elektronického podpisu

Datová zpráva

S pojmem „datová zpráva" se lze v souvislosti s elektronickým podpisem setkat především ve dvou významech – datovou zprávou je to, co je podepisováno, datovou zprávou je i certifikát (viz příslušné heslo).

Elektronicky je možné podepsat jakoukoliv datovou zprávu, tedy vše, co existuje v elektronické (binární) podobě. Může to být e-mailová zpráva, obrázek, program, databázový soubor, makro atd.

§ 2 písm. c) zákona
datovou zprávou (se rozumí) elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou

Digitální podpis

Viz též ***Elektronický podpis, Zaručený elektronický podpis, Data pro vytváření a data pro ověřování elektronického podpisu***

Technologie digitálních podpisů umožňuje vytváření zaručených elektronických podpisů podle zákona o elektronickém podpisu. K objasnění pojmu digitální podpis je nutné vysvětlit několik matematických a kryptografických technik. Na straně podepisující osoby se z napsané zprávy pomocí hašovací funkce vytvoří tzv. otisk zprávy (anglicky „message digest") – označme jej HASH 1. Na vstupu hašovací funkce může být libovolná a libovolně dlouhá datová zpráva, na jejím výstupu je otisk, který má pevnou délku 128 nebo 160 bitů (první údaj platí pro hašovací funkci MD5, druhý pro SHA-1, předpokládá se, že v krátké budoucnosti se začnou používat i hašovací funkce

s otiskem s vyšším počtem bitů). Pokud by následně bylo ve zprávě změněno jediné písmeno, mezera mezi slovy nebo čárka ve větě, získá se na výstupu zcela jiný otisk. Výpočetně je prakticky nemožné vytvořit ke zprávě jinou zprávu, která má stejný otisk. Vytvořený otisk napsané zprávy se šifruje za pomoci zvoleného asymetrického algoritmu a pomocí dat pro vytváření elektronického podpisu osoby, která se podepisuje. Získaný výsledek je digitálním podpisem, který je ke zprávě připojen.

Na straně příjemce zprávy se k otevřenému textu vypočte hash - tentokráte jej označme HASH 2. Z digitálního podpisu se pomocí dat pro ověřování elektronického podpisu osoby, která zprávu podepsala, získá hodnota, která by se měla rovnat hodnotě HASH 1. Pokud jsou hodnoty HASH 1 a HASH 2 shodné, má osoba, která se na podpis spoléhá, jistotu, že zpráva nebyla cestou změněna a že zprávu podepsala osoba, které přísluší data pro vytváření elektronického podpisu, neboť jen ta mohla z HASH 1 vytvořit digitální podpis.

Uvedené postupy na svém monitoru nevidí ani podepisující osoba, ani příjemce zprávy. Proces podepsání je spuštěn zadáním pokynu „digitálně (elektronicky) podepsat“ nebo např. „ověřit podpis“.

Za předpokladu použití bezpečného podpisového schématu nelze odvodit či vypočítat z elektronického podpisu nebo z dat pro ověřování elektronického podpisu data pro jeho vytváření.

Zákon o elektronickém podpisu neužívá pojem digitální podpis, nýbrž zaručený elektronický podpis. Přebírá tak princip Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy, tj. stanoví pojmy bez ohledu na technologii, která je v současné době používána. Předpokládá se, že v budoucnu budou využity například biometrické metody.

Elektronická podatelna

Elektronická podatelna je definována v nařízení vlády č. 304/2001 Sb. jako pracoviště pro příjem a odesílání datových zpráv. Povinnost zřídit jedno či více takových pracovišť je uložena tímto nařízením orgánům veřejné moci, pokud pro ně ze zvláštních předpisů, které jsou v tomto nařízení citovány pod čarou, vyplývá povinnost přijmout podání učiněné v elektronické podobě, podepsané elektronicky, anebo stanoví-li zvláštní právní předpis právo těchto orgánů činit úkony v elektronické podobě. Tato povinnost se vztahuje rovněž na územní samosprávné celky provádějící výkon státní správy v rámci přenesené působnosti.

Elektronické podatelny musí být vybaveny potřebnými zařízeními připojenými k veřejné datové síti, popřípadě jiným sítím. Tato zařízení musí splňovat požadavky na technické a programové vybavení podle standardů vydaných Úřadem pro veřejné informační systémy. Zařízení musí umožňovat používání zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Elektronický podpis

*Viz též **Digitální podpis, Zaručený elektronický podpis***

Elektronický podpis je zpravidla chápán jako číslo, které vytváří podepisující osoba pomocí svých dat pro vytváření elektronického podpisu a pomocí zprávy, kterou podepisuje. Elektronický podpis je jiný pro dvě odlišné zprávy, závisí na podepisované zprávě, nelze jej tedy koupit ani jinak obdobně získat. Přísně vzato by se pod pojem „elektronický podpis“ vešel i podpis, který je napsán z klávesnice PC. Takový podpis příliš velkou důvěru nevzbuzuje – je těžké identifikovat a prokázat, kdo jej skutečně napsal. Elektronickým podpisem je tedy v praxi zpravidla míněn zaručený elektronický podpis. Ten umožňuje vytvářet technologie digitálních podpisů.

V případě, že zpráva byla podepsána zaručeným elektronickým podpisem:

1. fyzická osoba (podepisující osoba), která zprávu podepsala, nemůže popřít, že je původcem této zprávy (nepopiratelnost původu – anglicky „non-repudiation“),
2. je možné zjistit, zda zpráva nebyla změněna poté, co byla podepsána (zachování integrity zprávy, tj. její celistvosti),
3. je možné zjistit identitu podepsané osoby,
4. je zajištěna právní akceptovatelnost podpisu.

Uvedených vlastností zaručeného elektronického podpisu nemusí využít pouze příjemce zprávy, ale obecně kdokoliv, kdo se na daný podpis spoléhá. Příjemcem zprávy může být například příslušný finanční úřad jako příjemce daňového přiznání. Dalším, kdo se na daný zaručený elektronický podpis spoléhá, může být příslušný správce daně.

Na rozdíl od vlastnoručního podpisu, který je, resp. ideálně by měl být pokaždé stejný, a to bez ohledu na to, co se podepisuje, je zaručený elektronický podpis pokaždé jiný. Závisí na textu, ke kterému je připojen, a na použitých datech pro vytváření elektronického podpisu. To je důvodem, proč není možné mít podpisové vzory zaručených elektronických podpisů. Stej-

ně tak nelze elektronicky podepsat zprávu dříve, než byla napsána („in bianco“), tj. zaručený elektronický podpis nemůže existovat sám o osobě, bez zprávy, která jím má být podepsána.

§ 2 písm. a) zákona

elektronickým podpisem (se rozumí) 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

§ 2 písm. b) zákona

zaručeným elektronickým podpisem (se rozumí) 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*

Kvalifikovaný certifikát

Viz též ***Certifikát***

Kvalifikovaný certifikát je certifikát, jehož obsah je stanoven zákonem o elektronickém podpisu (viz dále).

§ 2 písm. h) zákona

kvalifikovaným certifikátem (se rozumí) certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty

§ 12 zákona

(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,
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.

Kvalifikovaný (elektronický) podpis

Pojem kvalifikovaný podpis, resp. kvalifikovaný elektronický podpis neobsahuje ani zákon o elektronickém podpisu, ani Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy. Poprvé se objevil v dokumentech, které vznikají z iniciativy Evropské komise a na Směrnici navazují. Kvalifikovaným podpisem je míněn zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí použití prostředku pro bezpečné vytváření elektronického podpisu (viz Prostředek pro vytváření elektronických podpisů a prostředek pro ověřování elektronických podpisů). Tento „opis“ kvalifikovaného podpisu obsahuje zákon o elektronickém podpisu:

§ 3 odst. 2 zákona

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.

Zákon ani vyhláška neupravují, v jakých případech má být kvalifikovaný podpis používán.

Nástroj elektronického podpisu

Pojem nástroj elektronického podpisu se poprvé objevil v zákoně o elektronickém podpisu a byl převzat ze Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy (angl. electronic-signature product). Z nástrojů elektronického podpisu, jak jsou definovány v zákoně o elektronickém podpisum (viz dále), jsou ve středu pozornosti nástroje používané poskytovatelem pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny. Tyto nástroje nesmí

poskytovatel používat pro jiné účely než jakými může být podepisování vydávaných certifikátů, které nejsou kvalifikovanými certifikáty podle zákona o elektronickém podpisu, podepisování jiných datových zpráv apod. Nástroje musí odpovídat požadavkům stanoveným zákonem o elektronickém podpisu a upřesněným vyhláškou k tomuto zákonu. Nástroj, který poskytovatel hodlá pro uvedené účely používat, musí projít hodnocením Úřadu (viz § 8 vyhlášky č.366/2001 Sb. a příslušný komentář). Pokud poskytovatel hodlá používat nástroj, u nějž Úřad již shodu dříve vyslovil, není nutné nástroj opětovně hodnotit. Seznam nástrojů, u nichž byla vyslovena shoda, je zveřejňován ve Věstníku Úřadu a na webových stránkách Úřadu. Předpokládá se, a dosavadní krátká praxe tomu nasvědčuje, že o vyslovení shody budou žádat především dovozci či prodejci nástrojů, nikoliv sami poskytovatelé.

§ 2 písm. o) zákona

nástrojem elektronického podpisu (se rozumí) technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů

Osoba spoléhající se na podpis

Osobou spoléhající se na podpis může být příjemce elektronicky podepsané zprávy i osoba, která není přímým příjemcem zprávy od podepisující osoby, ale s elektroniky podepsanou zprávou pracuje a potřebuje se na podpis spoléhat (např. správce daně, auditor, soud apod.).

Osoba spoléhající se na podpis může využít skutečnosti, že většina běžně užívaných aplikací zasílá certifikát zároveň s elektronicky podepsanou zprávou. Pokud tomu tak není, musí podepisující osoba oznámit, kde je její certifikát dostupný, nebo musí být z použitého systému (nebo protokolu) zřejmé, kde se úložiště takového certifikátu nachází. Zpravidla se jedná o server poskytovatele, který certifikát vydal, nebo webovou stránku podepisující osoby. Nelze počítat s tím, že z certifikátu je možné obecně získat příliš mnoho informací o osobě, které byl vydán, tj. o podepisující osobě. To ostatně není účelem certifikátu. Účelem je důvěryhodným způsobem předat data pro ověřování elektronického podpisu podepisující osoby.

Osoba spoléhající se na podpis spoléhá na to, že poskytovatel před vydáním certifikátu ověřil totožnost osoby, které certifikát vydává. Při vydávání certifikátů nižších úrovní se neověřuje totožnost, ale například platnost a existence e-mailové adresy. Tento postup však nelze uplatnit v případě, že je vydáván kvalifikovaný certifikát podle zákona o elektronickém podpisu,

kdy se jednoznačně požaduje ověření totožnosti žadatele o vydání kvalifikovaného certifikátu a pořízení kopie jeho průkazů totožnosti.

Je třeba připomenout, že poskytovatel certifikačních služeb nemůže jiné osobě, tedy ani osobě spoléhající se na podpis, sdělit údaje, které osoba, která žádá o vystavení certifikátu, tomuto poskytovateli sdělila (například poštovní adresa, telefonní číslo) a které nejsou uvedeny v certifikátu. Výjimku představují situace, kdy dotčená osoba vysloví se sdělením těchto údajů souhlas nebo pokud tak stanoví zákon (například v případě soudního řízení apod.).

Zákon o elektronickém podpisu neobsahuje pojem „osoba spoléhající se na podpis“ ani jiný obdobný pojem. K jejímu jednání, případně povinnostem se vztahuje zejména následující ustanovení:

§ 5 odst. 2 zákona

Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. 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.

Ověření platnosti certifikátu

Pro ověření platnosti certifikátu podepisující osoby je nutným předpokladem důvěra v poskytovatele, který jej vydal. Pokud osoba spoléhající se na podpis tuto důvěru má, nainstaluje do svého software certifikát poskytovatele (je nutné odlišit certifikát poskytovatele a certifikát podepisující osoby).

Pokud osoba spoléhající se na podpis obdrží elektronicky podepsanou zprávu a zároveň certifikát podepisující osoby (případně získá certifikát jiným způsobem), následně ověří, zda certifikát podepisující osoby vydal poskytovatel uvedený v certifikátu a zda tento certifikát nebyl od okamžiku jeho vydání změněn. Toto ověření zajistí sama aplikace, a to ověřením elektronického podpisu poskytovatele, který je na certifikátu podepisující osoby.

Následně se zjišťuje, zda byl certifikát podepisující osoby platný v době, kdy byla zpráva podepsána. Přímo v certifikátu je uveden počátek a konec doby platnosti certifikátu (platnost od – do). V průběhu této doby však mohla být ukončena platnost certifikátu. Zda se tak nestalo, je nutné ověřit u poskytovatele v seznamu certifikátů, které byly zneplatněny (zveřejňován obvykle pod zkratkou CRL – Certification Revocation List – *viz příslušné heslo*).

Vždy je nutné počítat s určitým prodlením, které nastane mezi dobou, kdy držitel certifikátu požádá o ukončení platnosti svého certifikátu, a do-

bou, kdy je informace o zneplatnění certifikátu zveřejněna v CRL, resp. je vydán nový, aktualizovaný seznam zneplatněných certifikátů. Z technického i organizačního hlediska je velmi obtížné, aby mezi těmito dvěma akcemi nebyla určitá časová prodleva. Jak dlouhá tato prodleva je, lze zjistit v certifikační politice příslušného poskytovatele. Podle obsahu elektronicky podepsané zprávy je nutné zvážit, zda akceptovat obsah zprávy až poté, kdy uplyne doba, kterou poskytovatel potřebuje ke zveřejnění nového seznamu certifikátů, které byly zneplatněny. Například pokud osoba spoléhající se na podpis obdrží zprávu se závažným obsahem (zavazuje se, že uhradí 10 milionů Kč) a ví, že poskytovatel vydává nový seznam certifikátů, které byly zneplatněny (CRL), každých 12 hodin, je vhodné, aby s platbou vyčkala, než si ověří v CRL, které bylo vydáno 12 hodin po podepsání dokumentu (nebo pokud není schopna prokázat, kdy byl dokument podepsán, 12 hodin po přijetí dokumentu) , že certifikát je stále platný.

Je-li ověřována platnost kvalifikovaného certifikátu, je nutné pamatovat na následující ustanovení:

§ 5 odst. 2 zákona

Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. 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.

Podepisující osoba

Podepisující osobou ve smyslu zákona č. 227/2000 Sb. může být pouze fyzická osoba. Stejně jako v případě vlastnoručního podpisu není přípustné, aby se elektronicky podepisovala právnická osoba, byť v případě elektronického podpisu by z technického hlediska teoreticky taková možnost byla. Stejně jako jsou v organizaci (firmě apod.) určeni pracovníci, kteří jsou oprávněni svým podpisem opatřovat listinné dokumenty a jednat tak jménem právnické osoby, je potřeba analogicky postupovat i při elektronickém podepisování. V certifikátu v položce „účel“ lze konstatovat oprávnění fyzické osoby k podepisování jménem osoby právnické. Fyzická osoba se tak může elektronicky podepisovat jménem právnické osoby a osoba spoléhající se na podpis v certifikátu „vidí“, že tato osoba je k tomu oprávněna.

Podepisující osoba musí mít prostředek pro vytváření elektronického podpisu (viz Prostředek pro vytváření a prostředek pro ověřování elektronic-

kých podpisů) a data pro vytváření elektronického podpisu (viz Data pro vytváření a data pro ověřování elektronického podpisu).

Bezpečnost elektronického podepisování je do značné míry závislá na chování podepisující osoby, zejména na její schopnosti uchovat v tajnosti svá data pro vytváření elektronického podpisu (soukromý klíč). Pokud hrozí nebezpečí zneužití jejích dat pro vytváření elektronického podpisu, je podepisující osoba o této skutečnosti povinna uvědomit poskytovatele, který jí kvalifikovaný certifikát vydal. Další povinností podepisující osoby je podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu. I když zákon stanoví uvedené povinnosti pouze v případě, že je vydán certifikát s označením „kvalifikovaný“ a jedná se o kvalifikovaný certifikát podle zákona, je žádoucí, aby se takto podepisující osoba chovala i v případě, že jí byl vydán jakýkoliv certifikát.

Fyzická osoba může mít libovolný počet certifikátů. Jiné certifikáty může akceptovat banka, jiné úřad. S „univerzálními“ certifikáty, které by akceptovali všichni potenciální příjemci elektronicky podepsaných zpráv (všechny osoby spoléhající se na podpis), se v současné době ani v ČR ani zahraničí nepočítá. Je to obdobná situace, jako když osoba využívá služeb více bank a od každé má jednu platební kartu.

§ 2 písm. d) zákona

podepisující osobou (se rozumí) fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby

§ 5 odst. 1 zákona

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.

Poskytovatel certifikačních služeb

Viz též ***Certifikační autorita***

Poskytovatel certifikačních služeb je subjekt, který vydává certifikáty a vede jejich správu. Zejména zveřejňuje seznamy vydaných certifikátů a se-

znamy certifikátů, které byly zneplatněny (CRL viz Certificate Revocation List). Přijímá a realizuje žádosti o ukončení platnosti certifikátů.

V České republice působí těchto poskytovatelů několik a s nabídkou jejich služeb a s praktickými návody jejich využití je možné se seznámit na jejich webových stránkách. Někteří z těchto poskytovatelů vydávají certifikáty již několik let. Předmětem jejich služeb není poskytování elektronických podpisů, jak se někdy mylně uvádí, ale vydávání certifikátů a další výše uvedené činnosti. Certifikáty jsou vydávány zpravidla na dobu šesti měsíců a za cenu několika stokorun.

Ti poskytovatelé certifikačních služeb, kteří se rozhodnou, že budou vydávat kvalifikované certifikáty podle zákona o elektronickém podpisu (viz Kvalifikovaný certifikát), se musí řídit příslušnými ustanoveními tohoto zákona.

Poskytovatelé se mohou rozhodnout, že požádají Úřad (viz Úřad pro ochranu osobních údajů) o udělení akreditace (viz Akreditace). Činnost akreditovaných poskytovatelů je podle příslušného ustanovení zákona o elektronickém podpis nezbytná v „oblasti orgánů veřejné moci“, kde „je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb“.

Nad činností akreditovaných poskytovatelů a poskytovatelů vydávajících kvalifikované certifikáty vykonává Úřad dozor.

To neznamená, že všichni poskytovatelé musí vydávat kvalifikované certifikáty, případně žádat o akreditaci, a všichni občané, kteří se chtějí elektronicky podepisovat, musí mít kvalifikované certifikáty. V soukromoprávní oblasti, například při komunikaci dvou firem, komerčních bank s jejich klienty apod., je na komunikujících subjektech, zda budou vyžadovat používání kvalifikovaných certifikátů ve smyslu zákona o elektronickém podpisu.

Při výběru poskytovatele jsou základními hledisky zpravidla:

- jeho důvěryhodnost,
- účel, pro který bude elektronický podpis používán,
- služby, které poskytovatel nabízí,
- kompatibilita s aplikacemi, které žadatel o certifikát používá,
- cena poskytovaných služeb.

Pro některé účely může plně postačit certifikát, při jehož vydání žadatel komunikuje s poskytovatelem pouze e-mailem. Vydání takového certifikátu nabízejí jak zahraniční, tak tuzemští poskytovatelé na svých webových stránkách. Vydávání těchto certifikátů je zpravidla zdarma.

Pro jiné účely, např. pro styk s bankou nebo úřadem, bývá vymezen okruh poskytovatelů, jejichž certifikáty daný subjekt (banka, úřad) uznává. Například banky uznávají většinou pouze ty certifikáty, které samy vydaly. Získání certifikátu, který má poskytnout vyšší míru záruky a který je určen pro komunikaci v závažných věcech (finanční operace, podání, smluvní závazky apod.), a to včetně kvalifikovaného certifikátu podle zákona, je spojeno s ověřováním totožnosti osoby, které má být certifikát vydán. Je tedy nezbytné poskytovatele s příslušnými osobními doklady osobně navštívit. V případě vydání kvalifikovaného certifikátu je poskytovatel navíc povinen pořídit a uchovat kopie dokladů, kterými se totožnost prokazuje.

Poskytovatelé velmi často nabízejí zdarma vydávání testovacích certifikátů. K jejich vydání není nutná osobní návštěva poskytovatele.

Zákon o elektronickém podpisu podrobně a v mnoha ustanoveních upravuje povinnosti poskytovatelů, kteří vydávají kvalifikované certifikáty, resp. akreditovaných poskytovatelů. Připomeňme alespoň příslušné definice:

§ 2 písm e) zákona
poskytovatelem certifikačních služeb (se rozumí) subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy

§ 2 písm. f) zákona
akreditovaným poskytovatelem certifikačních služeb (se rozumí) poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona

Prostředek pro vytváření elektronických podpisů a prostředek pro ověřování elektronických podpisů

Uvedené pojmy se poprvé objevily v zákoně o elektronickém podpisu a byly převzaty ze Směrnice 1999/93/ES, o zásadách Společenství pro elektronické podpisy (angl. signature-creation device, signature-verification device). Souhrnně se jedná o hardware a software, které jsou užívané pro vytváření, resp. ověřování elektronických podpisů. Náležitosti a způsob používání těchto prostředků zákon o elektronickém podpisu neupravuje.

Z hlediska bezpečnosti lze za prostředky vyšší kategorie označit prostředky pro bezpečné vytváření elektronických podpisů a prostředky pro bezpečné ověřování elektronických podpisů (oproti výše uvedeným pojmům je vloženo slovo „bezpečné“, angl. secure-signature-creation device, pro prostředek pro bezpečné ověřování Směrnice odpovídající pojem neobsahuje, pouze v příloze IV uvádí doporučení pro bezpečné ověření podpisu). Požadavky

na tyto prostředky jsou stanoveny v § 17 zákona a upřesněny v § 7 vyhlášky. Povinnost používat tyto prostředky zákon ani vyhláška nestanoví. Více k tomuto tématu viz komentář k § 7 vyhlášky.

§ 2 písm k) zákona
prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů

§ 2 písm. l) zákona
prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů

§ 2 písm. m) zákona
prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem

§ 2 písm. n) zákona
prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem

Příjemce datové zprávy

viz ***Osoba spoléhající se na podpis***

Registrační autorita

Vykonává regitrační služby, tj. zejména ověřuje totožnost osob, které žádají o vydání certifikátu, případně zjišťuje specifické znaky těchto osob. Tato služba předchází vydání certifikátu. Může zahrnovat rovněž ověření, zda žadatel o vydání certifikátu má data pro vytváření podpisu. Registrační autorita je místem, kde se uzavírá s žadateli smlouva o vydání certifikátu a kde je dostupná certifikační politika (viz certifikační politika) a certifikát poskytovatele Pro zajišťování činnosti registračních autorit certifikační autority často využívají služeb jiných subjektů, tj. děje se tak na základě smluvních vztahů mezi certifikační autoritou a registrační autoritou. Viz též certifikační autorita.

Zákon o elektronickém podpisu neupravuje výslovně činnost registračních autorit, ale povinnosti, které se na činnosti, které zpravidla zajišťují, vztahují, jsou obsaženy v povinnostech poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty (zejména § 6 zákona).

Seznam certifikátů, které byly zneplatněny

viz ***Certification Revocation List (CRL)***

Šifrování

Šifrování datové zprávy je samostatný úkon, který nevyplývá z funkce elektronického podpisu. Elektronicky podepsaná zpráva může být šifrována, ale toto šifrování nezajišťuje elektronický podpis. Pokud tedy elektronicky podepsaná datová zpráva není šifrována, je předávána v otevřené podobě a osoba, která ji získá, se může seznámit s jejím obsahem.

Zákon o elektronickém podpisu šifrování elektronicky podepsaných datových zpráv neupravuje.

Time stamping

viz ***Časové razítko***

Úřad pro ochranu osobních údajů (ÚOOÚ)

Informace o Úřadu pro ochranu osobních údajů lze získat na Internetové adrese http://www.uoou.cz.

Povinnosti, příp. kompetence Úřadu v oblasti elektronického podpisu stanoví celkem tři právní předpisy: zákon o ochraně osobních údajů, zákon o elektronickém podpisu a vyhláška k tomuto zákonu. Základními povinnostmi Úřadu jsou udělování (a případné odnímání) akreditací, dozor nad činností akreditovaných poskytovatelů a poskytovatelů vydávajících kvalifikované certifikáty, vyhodnocování shody nástrojů elektronického podpisu a vydávání vyhlášek podle § 20 zákona o elektronickém podpisu. Úřad naopak nekoordinuje používání elektronického podpisu v ČR, a to ani v případě elektronické komunikaci mezi občanem a státem.

§ 2 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů
Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a pro oblast elektronického podpisu v rozsahu stanoveném zvláštním právním předpisem (pozn. tj. zákonem o elektronickém podpisu)

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

§ 9 odst. 2 zákona

Úřad

písm. a)

uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb subjektům působícím na území České republiky

písm. 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 (atd.)

písm. e)

vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou (atd.)

Zaručený elektronický podpis

Více viz ***Elektronický podpis***

Vytváření zaručených elektronických podpisů umožňuje technologie digitálních podpisů (viz Digitální podpis).

Zaručený elektronický podpis, pro který se v praxi ne zcela přesně často používá zkrácený název elektronický podpis, definuje zákon o elektronickém podpisu následovně:

§ 2 písm. b)

zaručeným elektronickým podpisem (se rozumí) 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.*

ELEKTRONICKÝ PODPIS

přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů

Mgr. Dagmar Bosáková, JUDr. Alena Kučerová, JUDr. Jaroslav Peca, Mgr. Pavel Vondruška

Vydalo: Nakladatelství ANAG
Tisk a vazba:
Autorská uzávěrka: Prosíme doplnit
ISBN 80-7263-125-X

ANAG, spol. s r. o.
Kollárovo nám. 7, 779 11 Olomouc
Tel.: 068/57 57 411, fax: 068/54 18 867
www.anag.cz, e-mail: obchod@anag.cz