ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

FAKULTA PROVOZNĚ EKONOMICKÁ

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

DISERTAČNÍ PRÁCE NA TÉMA:

METODIKA PRO KVALIFIKOVANÉ POSKYTOVATELE CERTIFIKAČNÍCH SLUŽEB

Školitel:

Doc. PhDr. Ivana Švarcová, CSc.

Autor:

Ing. Lenka Vašáková

2007

PODĚKOVÁNÍ

Děkuji touto cestou Doc. PhDr. Ivana Švarcové, CSc., vedoucí disertační práce, za odborné vedení, cenné rady a připomínky a za ochotnou pomoc při vypracování této disertační práce.

Děkuji též Mgr. Dagmar Bosákové z Ministerstva informatiky za odborné informace, které jsem díky ní získala a podporu, kterou mi při vypracování této práce poskytla.

SHRNUTÍ

Disertační práce se zabývá problematikou poskytování certifikačních služeb. Nejprve popisuje základní principy kryptografie, ukazuje matematický princip asymetrické kryptografie, vysvětluje fungování hashovacích funkcí. Dále se věnuje certifikátům veřejného klíče, infrastruktuře veřejných klíčů, certifikačním autoritám a jejich vzájemným vazbám. Poté jsou popsány profily certifikátu, seznamu zneplatněných certifikátů a profil časového razítka. V další části se téma zužuje na kvalifikované certifikační služby vymezené směrnicí EU 1999/93/EC. Jsou vysvětleny principy zákona o elektronickém podpisu, vyhlášky a norem upravujících postupy poskytovatelů certifikačních služeb. Jádrem této práce je vytvoření metodiky pro implementaci požadavků těchto dokumentů poskytovatelem certifikačních služeb. Poslední část je věnována návrhu metrik, které lze využít pro posouzení úrovně splnění některých požadavků poskytovatelem certifikačních služeb.

SUMMARY

The dissertation addresses the certification service provisioning problematic. At first it describes basic principles of cryptography, it shows mathematical principles of asymmetric cryptography, and it shows hash function operation. Further it deals with public key certificates, public key infrastructure, certification authorities and its interconnections. Then certificate, certificate revocation list and time-stamp token profiles are described. In the next part, the theme narrows to qualified certificate services as specified in the EU Directive 1999/93/EC. Principles of electronic signature act; ordinance and rules governing certification service provider policies are described. Core of this work is methodic on how to implement these rules in certification service provider practice. The last part is devoted to concept of metrics for measurement of quality of some activities of certification service provider.

KLÍČOVÁ SLOVA

asymetrická kryptografie
hashovací funkce
certifikát veřejného klíče
časové razítko
certifikační autorita
poskytovatel certifikačních služeb
digitální podpis
kvalifikovaný certifikát
akreditovaný poskytovatel certifikačních služeb
systém managementu bezpečnosti informací

KEYWORDS

asymmetric cryptography
hash function
public key certificate
time-stamp token
certification authority
certification service provider
digital signature
qualified certificate
accredited certification services provider
information security management system

Obsah

Seznam obrázků

1 ÚVOD

Disertační práce se zabývá problematikou poskytování kvalifikovaných certifikačních služeb v rámci zákona č. 227/2000 Sb. o elektronickém podpisu a porovnává přístup legislativy ČR po novelizaci tohoto zákona s předchozími podmínkami. Definuje metodiku pro poskytovatele certifikačních služeb, která vychází z právního rámce, mezinárodních standardů, norem a de-facto standardů.

V úvodu je obecně pojednáno o problematice poskytování certifikačních služeb, infrastruktuře veřejných klíčů, principech certifikátů, seznamech zneplatněných certifikátů. Poté je vysvětlen smysl zákonné úpravy elektronických podpisů, zejména s přihlédnutím k naposledy novelizovaným ustanovením. Dále je problematika zúžena na kvalifikované certifikační služby, jejichž poskytování se řídí zákonem, vyhláškou a normami vyžadovanými vyhláškou. Je vytvořena metodika, podle které by poskytovatel certifikačních služeb měl postupovat, aby jeho činnost byla v souladu s vyhláškou (na jejíž přípravě se autorka podílela) a novelizovaným zákonem o elektronickém podpisu. V závěrečné části autorka navrhuje metriky, na jejichž základě je možné provést posouzení, zda poskytovatel certifikačních služeb má předpoklady pro poskytování kvalifikovaných certifikačních služeb.

Poskytovatelé certifikačních služeb mají velkou odpovědnost a mezi jejich povinnosti patří, aby byly služby, které poskytují, důvěryhodné pro jejich uživatele a spoléhající se strany. Činnost poskytovatelů certifikačních služeb by měla být na porovnatelné úrovni, a to i v rámci Evropské unie. Proto je vhodné se řídit normami a předpisy, které byly vytvořeny zejména na základě předchozích zkušeností a mohou tak pomoci předejít mnohým problémům. Proto může být přehled vytvořený touto prací užitečný pro ujasnění vztahů mezi zákony, vyhláškami, normami a de-facto standardy pro poskytovatele certifikačních služeb.

2 CÍL

Cílem práce je vytvoření metodiky, podle které bude možné postupovat při poskytování tzv. kvalifikovaných certifikačních služeb ve smyslu zákona o elektronickém podpisu. Práce vychází z literární rešerše, která byla důkladnou analýzou oblasti poskytování certifikačních služeb. Cílem vytvořené metodiky je její využití při provádění auditu a dalších kontrol, při dochází k posouzení, zda kvalifikovaný poskytovatel certifikačních služeb (dále též poskytovatel) postupuje v souladu s právními předpisy a odpovídajícími normami. Metodiku budou moci využít i poskytovatelé, kteří mají postupovat v souladu s požadavky, které v ní jsou popsány. Autorka také zohlední prostředí v Evropské unii, protože je vhodné, aby bylo dosaženo porovnatelné úrovně vzhledem k vzájemnému uznávání kvalifikovaných certifikátů, které tito poskytovatelé vydávají.

Cílem této práce je rovněž navržení metrik, jejichž využití umožní přehledně posoudit činnost poskytovatelů jim samým, jejich auditorům, subjektům provádějícím akreditaci a kontrolním orgánům.

3 METODIKA ZPRACOVÁNÍ PRÁCE

Tato práce je vytvářena na základě analýzy literatury z oblasti infrastruktury veřejných klíčů, či konkrétněji z oblasti poskytování certifikačních služeb spojených s vydáváním certifikátů veřejného klíče, na jejichž základě se ověřuje digitální podpis. Zejména se jedná o mezinárodní a evropské normy, právní předpisy, směrnice Evropské unie a internetové de facto standardy (request for comments).

Nejprve jsou vysvětleny základní principy poskytovaných služeb po matematické i technické stránce. Následně autorka znázorňuje celkový pohled na poskytování certifikačních služeb, popisuje všechny typy těchto služeb a schematicky znázorňuje jejich souvislosti. Dále konkrétně specifikuje jednotlivé služby, včetně charakteristik jednotlivých produktů. Poté se zaměřuje na popis prostředí a služeb konkrétněji, pouze na kvalifikované certifikační služby, vymezené směrnicí Evropské unie [3] a zákonem o elektronickém podpisu [1]. Následně je popsána nejvyšší nadstavba, a to způsob, jak je nutné bezpečně řídit organizaci poskytující certifikační služby – samotná technologie nemůže zajistit dostatečnou důvěryhodnost, k tomu je nutná efektivní organizace s efektivním řízením, a to zejména řízením bezpečnosti.

Pro subjekty, které by potenciálně mohly využít tuto metodiku, jsou dále navrženy metriky pro posouzení úrovně splnění některých požadavků zákona [1]. Autorka při navrhování těchto metrik vycházela ze skript Měření a hodnocení jakosti informačních systémů [57], z metodiky COBIT [58] a doporučení NIST Security Metrics Guide for Information Technology Systems [59] a Security Systems Self-Assessment Guide for Information Technology Systems [60].

Práce postupuje od obecných principů přes jejich uplatnění v technických normách až po jejich nasazení a případná omezení v prostředí kvalifikovaných certifikačních služeb. Následně jsou vymezeny požadavky na řízení bezpečnosti u poskytovatelů těchto služeb.

Zároveň je porovnáno prostředí v České republice a Evropské unii, a to zejména na základě vlastních zkušeností autorky a získaných dokumentů – autorka poskytuje v této oblasti konzultace na Ministerstvu informatiky a je zástupkyní ČR ve fóru FESA (European Forum of Supervisory Authorities), kde jsou zástupci institucí odpovědných za provádění dozoru u poskytovatelů z jednotlivých zemí (nejedná se pouze o země EU, ale např. i o Turecko či Izrael). Vzhledem k tomu, že je poměrně velký tlak na to, aby spolu dokázali občané, soukromé společnosti a státní instituce v jednotlivých zemích sdílet stejný systém důvěry v prostředí Internetu, je velmi důležité, aby byl model poskytování certifikačních služeb v jednotlivých zemích EU velmi podobný.

Vzhledem k tomu, že se autorka podílela i na tvorbě nové vyhlášky pro poskytovatele certifikačních služeb, vychází při vytváření disertační práce ze znalostí, zkušeností a z vlastních představ o zavádění postupů poskytovatelů certifikačních služeb, které při vytváření této vyhlášky měla.

4 ZÁKLADNÍ PRINCIPY PKI A JEJICH OBJASNĚNÍ

Dnešní společnost postupně směřuje k převádění některých svých činností do počítačového světa. Jednou z funkcí, která tuto činnost podporuje, je i možnost podepisování. Vzhledem k tomu, že z právního hlediska se jedná o funkci poměrně závažnou, jsou na ni kladeny vysoké bezpečnostní nároky. Často jsou dokonce nároky kladené na podpis vytvořený elektronickými prostředky větší než na ten vlastnoruční (to je však často dáno tím, že se elektronický podpis, resp. certifikáty, na nichž je založen, používají k dalším účelům, ke kterým původně nebyly určeny). Evropská unie kvůli tomu přijala směrnici [3], která členským zemím říká, jakým způsobem mají tuto funkci zajišťovat. Ani Evropská unie však nevytvářela originální řešení a postavila základní funkcionalitu na běžných normách definujících algoritmy pro elektronický podpis a infrastrukturu veřejných klíčů. Některé oblasti však upraveny nebyly, takže vznikly nové normy, aby v jednotlivých státech byly poskytovány obdobné služby obdobným způsobem. Z těchto norem pak ve svých legislativních úpravách vycházejí nejen státy EU, ale i asijské, americké, či africké státy – stejně jako evropské normy vycházejí z norem amerických. Vzhledem k tomu, že se technologie dynamicky vyvíjejí, snažila se EU ve směrnici o obecné definice, které by mohly v budoucnu umožňovat použití nových technologií, které budou naplňovat daná kriteria. V současnosti se pro tento účel využívá asymetrická kryptografie.

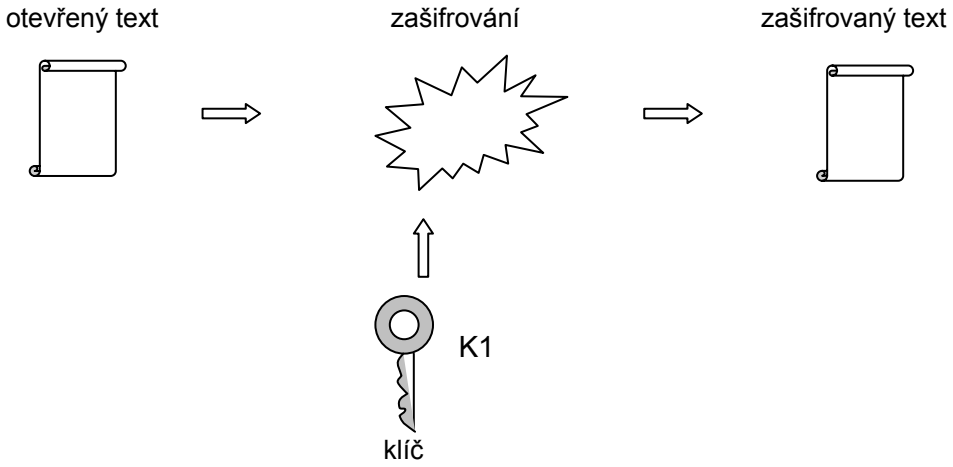
4.1 Kryptografie

Kryptografie používá pro zamezení čitelnosti (utajení obsahu) zprávy šifrovací algoritmus. Šifrování je založeno na kryptografickém (šifrovacím) algoritmu a klíči. Pomocí šifrování lze zabezpečit utajení zprávy, autentizaci a ověření integrity.

Utajení zprávy je skrytí obsahu zprávy před všemi kromě odesílatele a příjemce zprávy. Autentizace je možnost ověření, že prokazující strana (strana posílající zprávu) je ta, za kterou se vydává. Integrita je celistvost, to znamená,

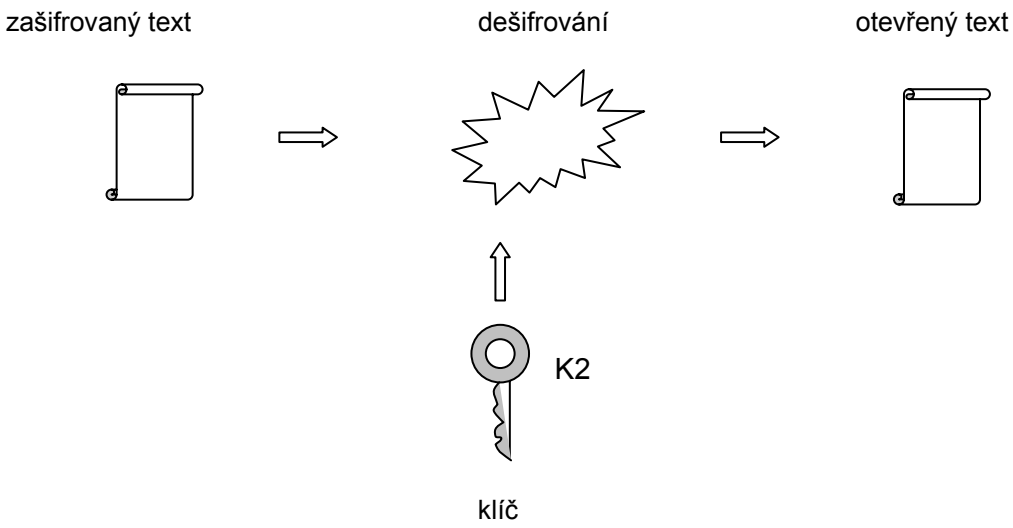
že pokud kryptografie zajišťuje ověření integrity, lze určit, jestli došla daná zpráva v nezměněné podobě.

Utajení zprávy může být zabezpečeno šifrováním, tedy kryptografickým algoritmem, který převádí srozumitelný (otevřený, plain) text do nesrozumitelné formy, zvané zašifrovaný text (cipher text). Vstupem do šifrovacího algoritmu je klíč, který má pro šifrování kritický význam.



Obrázek 1 – Zašifrování

Dešifrování je převod zašifrovaného textu pomocí klíče do původní podoby, srozumitelného (otevřeného) textu. Klíč pro zašifrování se může, ale nemusí shodovat s klíčem pro dešifrování. Pomocí této vlastnosti lze zaručit autentizaci (ne každé šifrování však autentizaci zaručuje).



Obrázek 2 – Dešifrování

Otevřeným (srozumitelným) textem zde nerozumíme jen text jako takový, ale i spustitelné programy, hudbu, obrázky, video, aj. Jde o jakákoliv data, která chceme zašifrovat.

Ověření integrity se dnes provádí pomocí tzv. hashovacích funkcí, které provádějí kontrolní součet, otisk zprávy. Integritu lze ověřovat i pomocí symetrických šifer.

4.1.1 Klíč

Při využití jednoho určitého klíče získáme transformací pro určitý otevřený text jediný konkrétní zašifrovaný text. Abychom dostali původní text, musíme použít odpovídající klíč, kterým dešifrujeme zašifrovaný text. Pokud je možných klíčů dostatečné množství, zajistíme, aby byl útok hrubou silou (zkoušení všech možností) v přijatelném čase nemožný. Výběr z množiny klíčů by měl být náhodný a pravděpodobnost výběru libovolného klíče má být pro všechny klíče stejná. Délka klíče je počet bitů jednotlivého klíče.

Šifry, které se používají v dnešní době, lze rozdělit na dvě skupiny: symetrické (s tajným klíčem) a asymetrické (s veřejným klíčem).

4.1.2 Symetrické šifry

Symetrické šifry používají stejný klíč pro zašifrování jako pro dešifrování. Z toho je zřejmé, že pokud má být zašifrovaný text utajený, musí zůstat třetí straně utajen klíč, kterým byl text zašifrován. Problémem je doručení tajného klíče příjemci tak, aby nebyl prozrazen. Klíč je také nutné často vyměňovat a generování klíče musí být co nejvíce náhodné (čísla z generátorů náhodných čísel nikdy nejsou skutečně náhodná, algoritmus na generování náhodných čísel lze vždy prolomit). Kromě toho, že je problémem klíče distribuovat, dalším problémem symetrického šifrování je velký počet těchto klíčů, které si musí každý s každým předat a poté uchovávat. Výhodou symetrického šifrování je jeho podstatně vyšší rychlost proti asymetrickému šifrování a potřeba kratšího klíče.

Příkladem používaných symetrických šifer je Triple DES, IDEA, BLOWFISH, AES.

4.1.3 Asymetrické šifry

Asymetrické šifry používají vždy dva klíče, z nichž jeden je soukromý a druhý veřejný. Přenáší se pouze veřejný klíč, který je dostupný všem. Veřejné klíče musí být přiřazeny danému uživateli důvěryhodným způsobem (aby nebylo možné vydávat se za někoho jiného a následně dešifrovat zprávu určenou jinému příjemci). Soukromé klíče se nikdy nikam nepřenáší a nejsou s nikým sdíleny. Každému uživateli potom stačí jeden soukromý klíč, jeho veřejný klíč a veřejné klíče těch, se kterými si chce vyměňovat zašifrované zprávy. Aby byl systém důvěryhodný, musí existovat důvěryhodná třetí strana (TTP – trusted third party), která potvrdí, že je osoba tou, za kterou se vydává. Vzhledem k tomu, že klíče v asymetrické kryptografii jsou generovány z prvočísel, musí být mnohem delší než v symetrické kryptografii (pokud by byly kratší, byly by snadno uhodnutelné a šifra napadnutelná hrubou silou). Samotné generování prvočísel je velkým problémem, který se matematika snaží již staletí vyřešit.

Asymetrická kryptografie využívá to, že je výpočetně velmi obtížné z veřejného klíče určit klíč soukromý.

Pro objasnění asymetrického šifrování uvádím známé příklady šifrovaného dopisování Alice a Boba [4]:

Zašifrování:

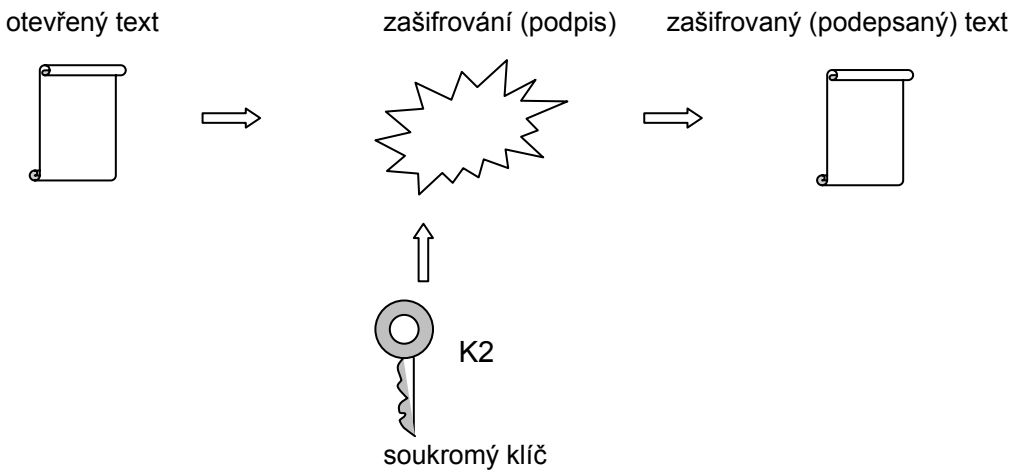
Alice chce poslat tajnou zprávu Bobovi. Zašifruje ji tedy Bobovým veřejným klíčem. Bob zprávu po obdržení dešifruje svým soukromým klíčem a přečte si ji. Nikdo jiný si Bobovu zprávu nemůže přečíst, protože jen on má svůj soukromý klíč.

Podpis a zašifrování:

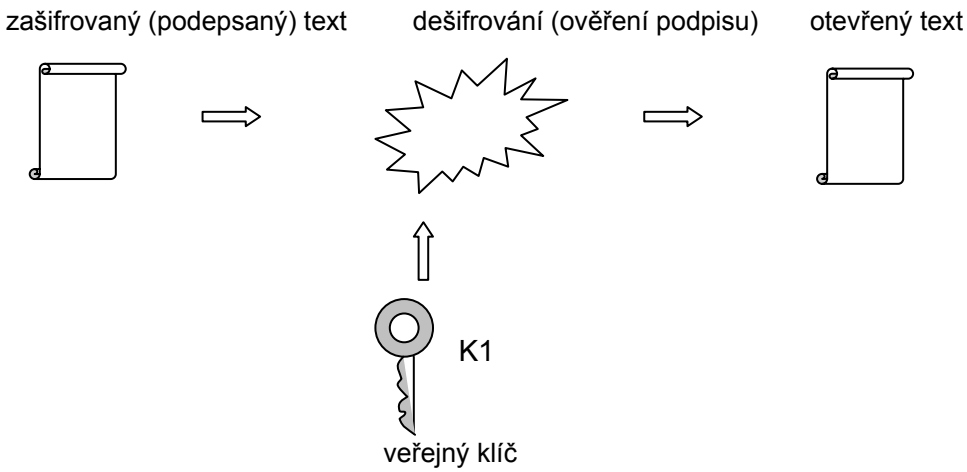
Alice chce poslat Bobovi zašifrovanou zprávu a chce, aby Bob věděl, že je jedině od ní. Alice tedy zprávu nejprve zašifruje svým soukromým klíčem (ten nikdo jiný nemá) a potom ji zašifruje Bobovým veřejným klíčem (nikdo jiný než Bob si zprávu nebude moci přečíst). Bob doručenou zprávu nejprve dešifruje svým soukromým klíčem, a potom ji dešifruje veřejným klíčem Alice. Pak je jisté, že zprávu poslala jedině Alice.

Podpis:

Kdyby Alice nechtěla zprávu utajit, ale jen podepsat, zašifrovala by ji pouze svým soukromým klíčem, a potom by si ji mohl přečíst kdokoliv, kdo má její veřejný klíč.[5]



Obrázek 3 – Digitální podpis – vytvoření



Obrázek 4 – Digitální podpis – ověření

4.1.4 Matematické vyjádření asymetrické kryptografie – RSA

V asymetrické kryptografii je velmi důležité nejprve vypočítat správně klíče. Obecně je postup při generování soukromého a veřejného klíče u schématu RSA dle [6] verze 2.1 (verze 2.1 je verzí se zdokonaleným zabezpečením, která se zatím v praxi běžně nepoužívá, proto je v popisu algoritmu zabudováno i běžně využívané schéma RSA podle dřívějších verzí standardu PKCS #1) následující:

- Zvolíme *u* prvočísel r_i; *i=1,2,..,u*, která jsou různá

- Spočítáme součin $N=\prod_{i=1}^{u} r_i$

- Spočítáme $\lambda(N) = \prod_{i=1}^{u} (r_i - 1)$

- Pokud $u=2$, první dva prvky r_1, r_2 se nazývají p, q

- Zvolíme nezáporné celé číslo e takové, že $3 < e < N-1$ a e a $\lambda(N)$ jsou nesoudělná

- Veřejný klíč je tvořen dvojicí (N, e), kde e je tzv. veřejný exponent RSA.

- Spočítáme nezáporné celé číslo d takové, že $0 < d < N$ a $e \cdot d \equiv 1 \bmod \lambda(N)$, používá se rozšířený Euklidův algoritmus

- Pak je soukromý klíč tvořen dvojicí (N, d), kde d je tzv. privátní exponent RSA a je nutno ošetřit integritu d a N.

- Soukromý klíč může být tvořen i pěticí (p, q, dP, dQ, $qInv$), případně, pokud je $u>2$, pro každé další prvočíslo použité pro vytvoření soukromého klíče je vytvořena trojice (r_i, d_i, t_i), $i = 3, \ldots, u$. Prvky takového soukromého klíče jsou určeny následovně:

- p a q jsou výše uvedená prvočísla r_1 a r_2

- exponenty dP a dQ jsou kladná celá čísla menší než p, resp. q pro která platí:

$$e \cdot dP \equiv 1 \pmod{(p-1)}$$

$$e \cdot dQ \equiv 1 \pmod{(q-1)}$$

- koeficient $qInv$ je kladné celé číslo menší než p, pro které platí:

$$q \cdot qInv \equiv 1 \pmod{p}.$$

Pokud je $u>2$:

- r_i , $i=3,..,u$; je další prvočíslo, které patří do součinu N, exponenty d_i , $i=3,..,u$; jsou kladná celá čísla, pro která platí:

$$e \cdot d_i \equiv 1 \pmod{(r_i - 1)}$$

- koeficienty t_i, $i=3,..,u$; jsou kladná celá čísla menší než r_i, pro která platí:

$$R_i \cdot t_i \equiv 1 \pmod{r_i},$$

kde $R_i = r_1 \cdot r_2 \cdot \ldots \cdot r_{i-1}$.

Poté je již možné využít klíče pro šifrování nebo digitální podpis.

Před provedením operace šifrování nebo digitálního podpisu je nutné provést úpravu vstupních dat, ta je však nad rámec tohoto textu. U digitálního podpisu je součástí úpravy vstupních dat výpočet otisku zprávy s využitím hashovací funkce, čímž je úprava vstupních dat velmi zjednodušena.

Šifrování proběhne výpočtem $c = m^e \mod N$, kde m je text určený k zašifrování a c tedy bude zašifrovaná zpráva, kterou si může přečíst pouze vlastník soukromého klíče (N, d) odpovídajícího veřejnému klíči (N, e). Text určený k zašifrování musí být před použitím zformátován, velikost vstupu musí být v rozmezí $0 \le m \le N - 1$.

Dešifrování může vlastník odpovídajícího soukromého klíče poté provést výpočtem $m = c^d \mod N$.

V případě použití druhého typu soukromého klíče bude dešifrování probíhat jako výpočet:

$m_1 = c^{dP} \bmod p$

$m_2 = c^{dQ} \bmod q$

jestliže $u > 2$, $m_i = c^{d_i} \bmod r_i$, $i = 3, \ldots, u$

$h = (m_1 - m_2) \cdot qInv \bmod p$

$m = m_2 + q \cdot h$

jestliže $u > 2$, $R = r_1$

pro všechna $i = 3, ..., u$

$R = R \cdot r_{i-1}$

$h = (m_i - m) \cdot t_i \ (mod\ r_i)$

$m = m + R \cdot h$.

Získané m je v případě, že byl použit správný klíč, původní zpráva.

Digitální podpis je možno vytvořit výpočtem $s = m^d \ mod\ N$, kde m je text určený k podpisu a s je vytvořený podpis, který si může ověřit každý, kdo má k dispozici veřejný klíč *(N,e)* odpovídající soukromému klíči *(N,d)*, který byl vstupem pro funkci vytvoření podpisu.

V případě, že byl použit soukromý klíč tvořený pěticí údajů (p, q, dP, dQ, $qInv$) a trojicí (r_i, d_i, t_i), $i = 3, \ldots, u$, bude výpočet následující:

$s_1 = m^{dP} \bmod p$

$s_2 = m^{dQ} \bmod q$

jestliže $u > 2$, $s_i = m^{d_i} \bmod r_i$, $i = 3, \ldots, u$

$h = (s_1 - s_2) \cdot qInv \bmod p$

$s = s_2 + q \cdot h$

jestliže $u > 2$, $R = r_1$

pro všechna $i = 3, ..., u$

$R = R \cdot r_{i-1}$

$h = (s_i - s) \cdot t_i \ (mod\ r_i)$

$s = s + R \cdot h.$

Ověření digitálního podpisu je pak možno provést výpočtem $m = s^e \ mod\ N$, což je v podstatě dešifrování. [6] Problematika asymetrické kryptografie je mnohem obsáhlejší, jistě by bylo zajímavé se zaobírat i kryptoanalýzou symetrických i asymetrických algoritmů, ale to již není předmětem této práce.

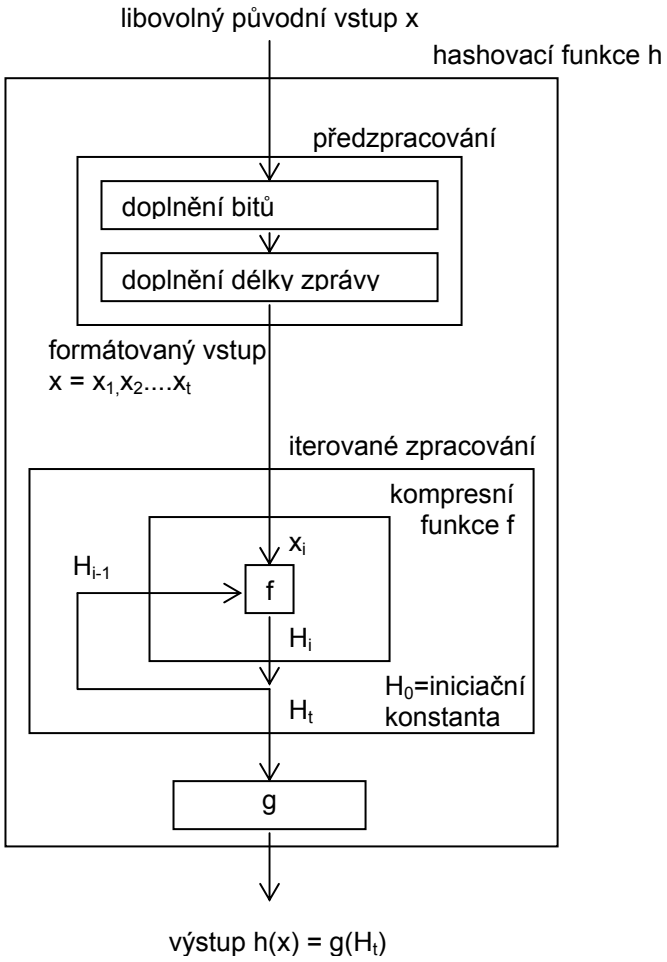
4.1.5 Hashovací funkce

Pro ideální hashovací funkci je z výpočetního hlediska nemožné najít dvě různé zprávy se stejnou hodnotou hashe. Tato vlastnost se nazývá bezkoliznost. Z hodnoty hashe již není možné odvodit obsah původní zprávy,

protože hashovací funkce je jednocestná, tzn. že v jednom směru lze snadno vypočítat, ale určit inverzní hodnotu je velmi obtížné.

Hashovací funkce je obecně zobrazení *h*, které přiřazuje zprávě jako vstupu výstup označovaný slovem hash (někdy též otisk), resp. je to zobrazení, které řetězci libovolné délky přiřazuje řetězec pevné délky. Z tohoto obecného principu je zřejmé, že kolize v praxi musí existovat, protože možných řetězců pevné délky existuje méně než všech možných řetězců libovolné délky. Cílem tvůrců hashovacích funkcí je tedy to, aby zprávy, které se liší pouze ve velmi málo bitech, nemohly mít stejný otisk a aby výstup z hashovacích funkcí měl co nejvíce náhodný charakter.

Znázornění hashovací funkce je uvedeno na následujícím schématu:



Obrázek 5 – Hashovací funkce [7]

Nejprve je provedeno předzpracování vstupních dat (*x*). Data se rozdělí na bloky definované délky ($x = x_1,x_2,....x_t$). Pokud je v daném bloku méně bitů, jsou doplněny tak, aby nemohly existovat dvě různé zprávy, které budou po provedení doplnění identické. Součástí doplňku je i údaj o délce zprávy. Poté již je vstup připraven ke zpracování. Do kompresní funkce postupně vstupují jednotlivé části zformátovaného vstupu (x_i, $i=1,2,..,t$) a výsledky předchozího průchodu dat kompresní funkcí (H_{i-1}). V první iteraci je místo vstupu z předchozí iterace použita na vstupu iniciační konstanta (H_0). Po průchodu všech částí zformátovaného vstupu hashovací funkcí je vrácena jako výstup poslední hodnota (H_t) získaná průchodem kompresní funkcí f, resp. její zobrazení *g* –

většinou se však používá identické zobrazení, tj. vstup do funkce *g* je zároveň výstup. Tato hodnota má pevnou délku.[7],[36]

Výše popsané schéma s využitím iterovaného zpracování pevně dané délky bloku kompresní funkcí *f* se používá v současných hashovacích funkcích nejčastěji.[8] Jako kompresní funkce se obvykle používají symetrické šifrovací algoritmy ve vhodném režimu[1].

4.1.6 Využití kryptografie

Asymetrická kryptografie je řádově tisíckrát pomalejší než symetrická. Výhodou asymetrické kryptografie je, že při vyšším počtu uživatelů, kteří ji využívají, stačí pro šifrovanou komunikaci méně klíčů, než by bylo nutné vyměnit při symetrické kryptografii. Asymetrickou kryptografii lze využít nejen pro utajení zprávy, ale i pro autentizaci. Příkladem asymetrických šifer je výše popsaný algoritmus RSA nebo algoritmy s využitím eliptických křivek.

V kryptografických systémech se často využívá kombinace symetrické a asymetrické kryptografie, někdy také v kombinaci s hashovací funkcí (např. SHA-1, RIPEMD-160, funkce třídy SHA-2). Příkladem může být systém, kde se předání tajných klíčů pro komunikaci provede pomocí asymetrické kryptografie a další komunikace už je šifrována symetricky.

Jiným příkladem využití kombinace šifrovacích algoritmů může být digitální podpis, jehož princip byl již vysvětlen a bude dále rozvinut.

4.1.7 Kryptoanalýza

Při kryptoanalýze se kryptoanalytik snaží určit sílu šifrovacího algoritmu, případně se pokouší proniknout do šifrovacího systému. V této kapitole bude kryptoanalýza pojata pouze z pohledu praktického uplatnění v oblasti digitálního podpisu.

---

[1] Takové využití symetrických algoritmů se začíná jevit jako největší slabina současných hashovacích funkcí; na tento problém upozorňují i kryptologové v ČR a snaží se navrhnout a umožnit praktické využití funkcí konstruovaných speciálně pro využití v hashovacích funkcích [56].

Síla algoritmu je za předpokladu, že je algoritmus dobře navržen, dána zejména délkou použitého klíče, jak je uvedeno výše. U symetrické kryptografie je klíč náhodné číslo, které je jen velmi málo omezeno, zatímco u asymetrické kryptografie je klíč tvořen na základě prvočísel. U asymetrické kryptografie je tedy nutné používat řádově delší klíče než u symetrické.

Nízká délka klíče byla také důvodem, proč bylo nutné v oblasti symetrické kryptografie nahradit algoritmus DES (64 bitový, resp. 56 bitový klíč, vzhledem k osmi paritním bitům, šifruje bloky o délce 64 bitů) novým algoritmem AES (128, 192 nebo 256 bitový klíč, šifruje bloky o délce 128 bitů). Ačkoliv bylo popsáno několik teoretických útoků na samotný algoritmus DES, vždy byl na reálné prolomení použit útok hrubou silou – zatím bylo třeba spojit výpočetní síly na Internetu, ale technologický vývoj jde velmi rychle kupředu. U asymetrické kryptografie se v současnosti doporučuje používat algoritmy s délkou klíče 1024 bitů, v lepším případě 2048 bitů (v současnosti probíhá postupný přechod k této délce klíče).

Oblast kryptoanalýzy se v současnosti nejvíce projevila u hashovacích funkcí. Jak je výše uvedeno, hashovací funkce má být jednocestná a bezkolizní funkce. Kolize je definována jako situace, kdy je možné najít dvě zprávy se stejným otiskem. Je zřejmé, že když v hashovací funkci dojde k vytvoření otisku pevné délky z libovolně dlouhého a libovolné znaky obsahujícího textu, musí nějaké kolize vždy existovat. Síla hashovací funkce se tedy odvíjí od délky výstupu, tedy otisku zprávy. [5]

V současnosti se zejména čínským matematikům [9],[10] daří nalézat u algoritmů MD5, RIPEMD, nebo SHA-0 texty, které mají stejný otisk. Dokonce je již možné u algoritmu MD5 z libovolného textu vytvořit jiný smysluplný kolizní text (samozřejmě díky úpravám, které se pro běžného uživatele nezobrazí). Proto již skutečně není vhodné používat algoritmus MD5, ačkoliv se tak stále děje.

Nalezení kolize k libovolnému textu se podařilo [9],[10] u algoritmu SHA-1 zredukovat ze složitosti 2^{80} na 2^{69}. To je stále ještě velká technologická náročnost, v současnosti obtížně realizovatelná (navíc je velmi málo

pravděpodobné, že by byl nalezený text smysluplný). Vzhledem k této skutečnosti se však nedoporučuje (např. Národní bezpečnostní úřad na svých webových stránkách) využívat hashovací algoritmy, které vytvářejí otisk o délce menší než 160 bitů. Nejčastěji využívanou hashovací funkcí je v současnosti SHA-1, která zatím náporu útoků odolává (kromě útoků na redukované formy, které se nepoužívají, a zmiňovaného útoku, který je výpočetně náročný).

V současnosti (do roku 2010) dochází k přesunu od funkce SHA-1 k funkcím třídy SHA-2 (tedy SHA-224, SHA-256, SHA-384 a SHA-512). Problémem však nadále zůstávají pochybnosti o samotném způsobu konstruování těchto hashovacích funkcí, jak je popsáno v poznámce ke kapitole věnované hashovacím funkcím.

4.2 Digitální podpis

Digitální podpis má zaručit autentičnost zprávy (zprávu podepsala právě daná osoba), umožnit zjištění, zda nedošlo k narušení integrity zprávy (lze poznat, jestli nedošlo ke změně) a zaručit nepopiratelnost odpovědnosti (pokud uživatel podepíše zprávu, nemůže tvrdit, že ji nepodepsal). Pro vytvoření digitálního podpisu je možné použít různá schémata, dále je popsáno v současnosti nejčastěji používané.

Digitální podpis v tomto schématu vzniká asymetrickým zašifrováním otisku zprávy, které se provádí se soukromým klíčem podepisující osoby. Pro výpočet otisku se použije hashovací funkce. Pokud je splněna podmínka unikátnosti soukromého klíče, která je nutná pro fungování asymetrických kryptografických algoritmů, je zpráva čitelná pro všechny, kteří mají k dispozici veřejný klíč, a všichni mají možnost se přesvědčit o tom, že zprávu tímto způsobem podepsala jen jediná možná osoba, a to ta, která má příslušný soukromý klíč. K přenosu veřejného klíče a údajů o podepisující osobě se používá struktura zvaná certifikát veřejného klíče (dále certifikát). Profil certifikátu ve formátu X.509 v3 je popsán ve standardu RFC 3280 [11]. Vzhledem k tomu, že je v zájmu všech používat certifikáty se stejnou strukturou, používá se převážně tento standardní profil. I zde však existuje určitá míra

volnosti, takže například údaj o e-mailové adrese může být uveden na dvou různých místech. Dalším populárním formátem certifikátů je formát PGP, který používají produkty postavené na systému PGP (Pretty Good Privacy)[12].

4.3 Důvěra v certifikáty

Spolehlivost informace o tom, jestli je osoba tou, za kterou se vydává, závisí ale na způsobu předání veřejného klíče, nebo certifikátu, který jej obsahuje – pokud nebude existovat spolehlivý kanál, kterým jej lze získat, není možné se na autentičnost původu zprávy spolehnout. Z toho důvodu musí existovat někdo, kdo stvrdí, že certifikát, který daná osoba má, obsahuje skutečně údaje této osoby. Stvrzení se provádí podepsáním certifikátu.

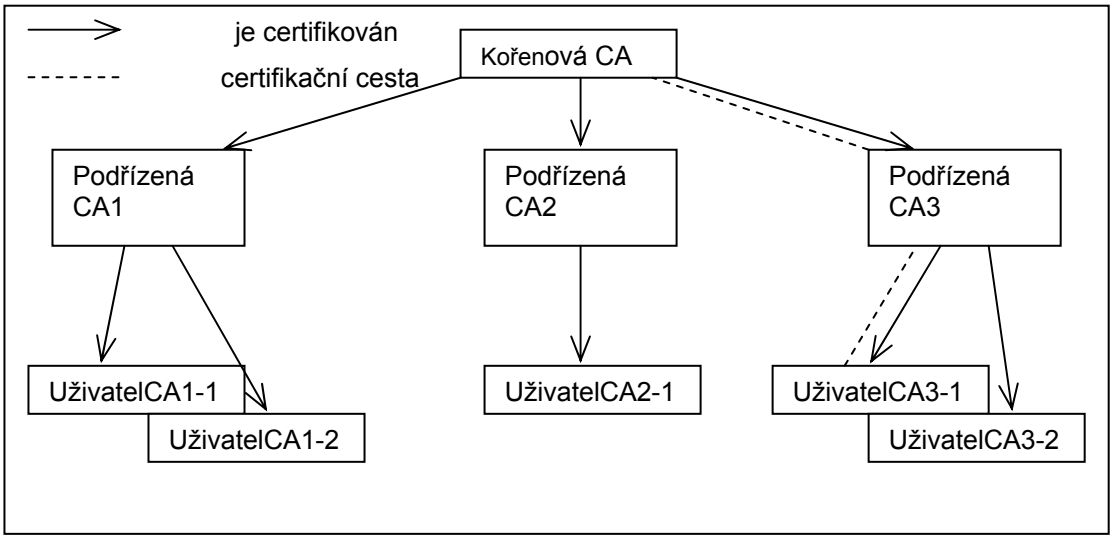
Například v PGP vzniká tzv. „pavučina důvěry“ [13], ve které si uživatelé vzájemně podepisují své certifikáty a přenos důvěry funguje na principu – tuto osobu znám, důvěřuji jí, proto budu důvěřovat i údajům v certifikátech, jejichž pravost potvrdila. Tento systém však nemá dostačující důvěryhodnost např. pro podpis smluv. Z toho důvodu se používají služby důvěryhodných třetích stran, jako jsou certifikační autority (dále též CA). Důvěryhodná třetí strana má odpovědnost za ověření osob (samozřejmě v závislosti na tom, jaké záruky si definuje a jak bude fungování jejích služeb probíhat). Po ověření stvrdí správnost údajů v certifikátu svým podpisem. Aby bylo možné platnost tohoto podpisu ověřit, má i certifikační autorita svůj certifikát, ze kterého lze získat veřejný klíč.

Certifikační autority mohou tvořit hierarchickou strukturu – mohou potvrzovat důvěryhodnost certifikačních autorit na nižším stupni hierarchie podpisem certifikátu tzv. podřízené certifikační autority. Certifikát certifikační autority, která je umístěna nejvýše v tzv. certifikační cestě, je podepsán sám sebou, bývá také označován jako kořenový certifikát. V hierarchické struktuře certifikačních autorit je důležitým prvkem skutečnost, že každá certifikační autorita má svá pravidla, tzv. politiky, na základě kterých postupuje při vydávání certifikátu podřízeným certifikačním autoritám nebo koncovým uživatelům.

Pokud uživatelé důvěřují kořenové certifikační autoritě, lze snadno stanovit pravidla pro certifikační cesty.[14]

Certifikační cesta je tedy seznam certifikátů, počínaje od samopodepsaného kořenového certifikátu, přes certifikáty jemu podřízené certifikační autority, až po certifikát odesilatele podepsané zprávy, v rámci dané hierarchické struktury. Díky tomu může uživatel, který chce ověřit platnost podpisu a certifikátu, který obdržel od druhého uživatele, ověřit platnost certifikátů od kořenového certifikátu přes certifikáty podřízených certifikačních autorit až po certifikát certifikační autority, která mu certifikát vydala. Pro ověření použije vždy veřejný klíč z certifikátu, který je nadřízený certifikátu, jehož platnost ověřuje. Kromě již zmiňovaného kořenového certifikátu, který je samopodepsaný. V případě kořenového certifikátu je pouze na uživateli, aby se na základě certifikační politiky rozhodl, zdali této certifikační autoritě bude důvěřovat[2]. Pokud má uživatel určité pochybnosti o pravosti kořenového certifikátu, je možné jej (resp. jeho otisk) porovnat s kořenovým certifikátem umístěným u dalšího subjektu (např. u kvalifikovaných poskytovatelů certifikačních služeb zveřejňuje kořenové certifikáty i Ministerstvo informatiky).

[2] V praxi to však není tak snadné, vzhledem k finančním zájmům některých soukromých společností dochází k tomu, že např. při instalaci internetového prohlížeče je uživateli dopředu nastaveno několik certifikačních autorit, jejichž certifikátům díky tomuto opatření nevědomky důvěřuje. Proto se doporučuje nejprve úložiště s důvěryhodnými certifikačními autoritami v operačním systému vyprázdnit.



Obrázek 6 – Infrastruktura certifikačních autorit – hierarchie

Kromě těchto vztahů mezi certifikačními autoritami existují ještě další způsoby, jak lze upravovat důvěru, a to pomocí cross-certifikace a bridgeových certifikačních autorit.

4.4 Cross-certifikace

Cross-certifikace je postup, kdy jedna certifikační autorita podepíše veřejný klíč druhé certifikační autority a dá tak najevo, že důvěřuje této certifikační autoritě. Tento proces může být jednocestný nebo vzájemný. Když nadřízená certifikační autorita podepisuje certifikát podřízené certifikační autority, jedná se také o cross-certifikaci. Většinou je však tímto pojmem míněno vzájemné podepsání veřejných klíčů dvou různých subjektů. Pokud k němu dojde, struktura bude opět mít spíše rysy „pavučiny důvěry“, hierarchie se tímto způsobem „rozbije“.

Tak je dosaženo toho, že uživatelé mohou důvěřovat jen jedné z těchto certifikačních autorit a automaticky důvěřují i certifikátům vydaným tou druhou.

V tomto smyslu však cross-certifikace není v praxi příliš obvyklá, protože tak může dojít k problémům s přenosem odpovědnosti, kdy má v podstatě první

certifikační autorita odpovědnost i za certifikáty vydané druhou certifikační autoritou – obě strany by si tedy musely velmi důvěřovat, aby se vzájemně nepodezřívaly, že certifikáty té druhé nemohou být dostatečně důvěryhodné, aby za ně daná CA mohla nést odpovědnost.

4.5 Bridgeové certifikační autority

Existuje i další způsob, jak dosáhnout toho, aby si uživatelé mohli vzájemně uznávat certifikáty vydané různými certifikačními autoritami, které nejsou v jedné hierarchické struktuře. Jedná se o bridgeovou certifikační autoritu. To je další subjekt, který má své vlastní certifikáty a který tvoří jakési jádro, ve kterém jsou dostupné certifikáty certifikačních autorit, které mají podobné politiky. Pro zařazení certifikační autority do bridge se používá např. cross-certifikace (zde však existuje zmiňovaný problém s odpovědností), nebo, jako je to v případě Evropské bridgeové/gatewayové certifikační autority (dále EBGCA), tzv. trust-service status list (dále jen TSL), případně jiný systém využívající „trust listy“ [3].

4.6 EBGCA

Pro projekt EBGCA byl vybrán standard ETSI TS 102 231 [15].

Tento standard definuje způsob, jak udržet informaci o důvěryhodných službách na jednom místě. Jedná se o strukturu (buď XML strukturu, nebo strukturu zapsanou v ASN.1 notaci), která jednak obsahuje informace o svém vydavateli, URL, kde je možno nalézt politiky, pořadí daného seznamu TSL, datum vydání TSL a datum vydání příštího TSL – to jsou tzv. údaje o schématu. Dále obsahuje údaje (název, URL) o jednotlivých poskytovatelích, jejichž důvěryhodné služby jsou na seznamu.

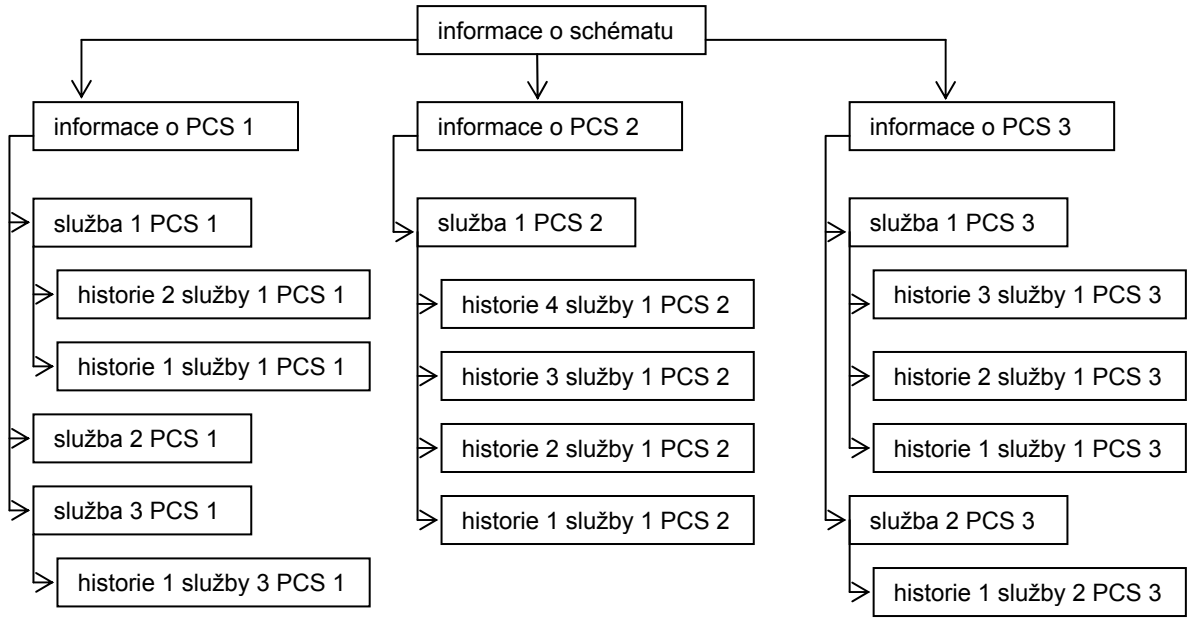
---

[3] Podobný model založený na Trust listech je použit například v Itálii. Vzhledem k tomu, že tam působí velmi mnoho certifikačních autorit, resp. kvalifikovaných poskytovatelů certifikačních služeb, bylo nutné tímto způsobem zpřehlednit situaci.

V hierarchickém členění jsou poté uvedeny informace o jejich službách, tj. identifikace služby u poskytovatele, jednoznačná identifikace typu služby v daném schématu, název služby, certifikát certifikační autority, případně URL odkaz na bližší informace o službě a zejména informace o stavu dané služby (tj. zda je služba v souladu s požadavky schématu).

Vzhledem k tomu, jak mají být informace z TSL použity, TSL musí obsahovat i informace historické – pokud došlo v průběhu času k tomu, že některá služba byla ze seznamu odstraněna, je nutné, aby bylo zřejmé, kdy se tak stalo (jinak nelze určit, jestli byla operace provedená s certifikátem vydaným poskytovatelem certifikačních služeb uvedeným na TSL v dané době platná či nikoliv). Proto je mezi informacemi o službě uveden i údaj o tom, jestli existuje o dané službě nějaký historický záznam. V případě, že ano, je k dané službě přičleněna posloupnost záznamů o historii, v sestupném pořadí – záznam obsahuje opět identifikátor služby a dále informaci o předchozím stavu a dobu, kdy došlo ke změně. TSL musí samozřejmě obsahovat i elektronický podpis, a díky tomu je vhodná i existence certifikátu s odpovídajícím veřejným klíčem (případně je možné využít i jiný způsob předání veřejného klíče).

Pokud se uživatel na základě politiky EBGCA rozhodne důvěřovat poskytovatelům a jejich službám uvedeným na TSL, musí nejprve „nainstalovat“ kořenový certifikát EBGCA, poté certifikát, který obsahuje veřejný klíč odpovídající soukromému klíči použitému pro podpis TSL. Poté, v případě, že dojde k realizaci projektu tak, jak byl otestován v rámci pilotního projektu, bude použita aplikace (jednalo se o Javovskou aplikaci) sloužící k zobrazení TSL v uživatelsky přívětivé podobě. Uživatel následně na základě svého rozhodnutí nainstaluje všechny certifikáty na TSL. Když mu poté např. bude doručena zpráva elektronicky podepsaná na základě certifikátu vydaného v rámci služby poskytovatele uvedené na TSL, bude pro něj tento certifikát při ověřování elektronického podpisu také důvěryhodný.



Obrázek 7 – Schéma TSL

I zde samozřejmě dochází k problémům s odpovědností, protože je nutné, aby EBGCA odkazovala na certifikační autority s podobnými zárukami a aby bylo zřejmé, kdo za tyto informace ručí.

V případě EBGCA je tato skutečnost velmi problematická. V Evropské směrnici 1999/93/EC [3] o elektronických podpisech je členským státům uloženo, aby kvalifikované certifikáty vydané v ostatních zemích byly akceptovány jako kvalifikované i v jejich zemi. Zatím však neexistuje nástroj, jak jednoduše zjistit, které certifikační autority v jednotlivých zemích vydávají kvalifikované certifikáty. Prohledávat stránky, většinou v národních jazycích jednotlivých zemí a pátrat po informaci o poskytovatelích vydávajících kvalifikované certifikáty, je uživatelsky nepřívětivé. Dalším důležitým aspektem je skutečnost, že takto je upravena pouze oblast kvalifikovaných certifikátů, které jsou určeny pro elektronický podpis, zatímco oblast šifrování, autentizace, časových razítek, případně další oblasti, kde jsou využívány certifikační služby, takto upraveny nejsou. V ostatních oblastech je ještě komplikovanější se shodnout na tom, kdo a na základě jakých předpokladů bude důvěryhodným

subjektem, jehož služby budou uvedeny v seznamu důvěryhodných služeb v rámci Evropské unie. Navíc dokumentace poskytovatelů je většinou pouze v národních jazycích, takže není snadné se přesvědčit o důvěryhodnosti jejich služeb.

Vzhledem k stále častější komunikaci v rámci privátního i veřejného sektoru je však nutná existence platformy, která umožní orientaci uživatelů v důvěryhodných elektronických službách a jejich poskytovatelích. Je totiž nutné – v zájmu co největšího rozšíření jejich používání – aby bylo používání certifikátů co nejjednodušší. Přehlednost informací o poskytovatelích a jejich službách k tomu nezbytně patří.

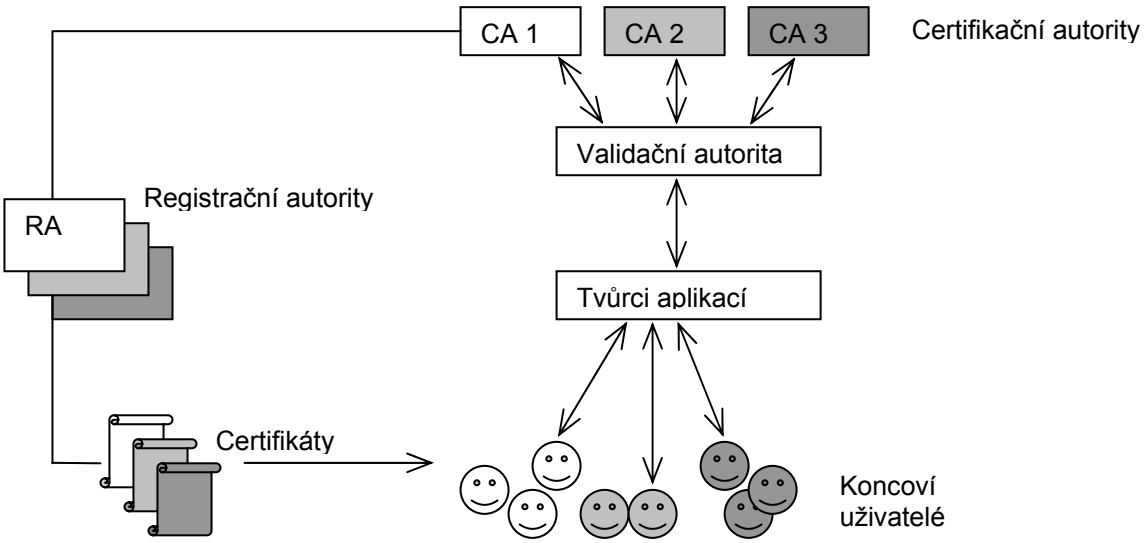
4.7 Služby validačních autorit (validation authority)

V dnešní době začínají některé společnosti nabízet služby tzv. validační autority. Výše uvedené postupy pro určení důvěryhodnosti bývají považovány z různých důvodů za obtížně použitelné, a to ať díky přenosu odpovědnosti, nebo kvůli technické náročnosti. Proto některé organizace nabízejí, že na základě informací o jednotlivých poskytovatelích certifikačních služeb určí, jaké jsou jejich záruky a pro jaké účely je tedy možno certifikáty dané organizace použít. Hlavním smyslem je určení, zda je možno se na certifikát vydaný určitou společností a použitý za určitým účelem spolehnout. Spoléhající se strana poté obdrží pouze informaci o tom, zda se může spolehnout, nemusí číst certifikační politiky poskytovatelů (nehledě na to, že z certifikačních politik se stejně nemůže spolehlivě přesvědčit, zda poskytovatel skutečně provádí to, co v nich proklamuje).

Validační autorita klasifikuje služby poskytovatelů certifikačních služeb. Tvůrce aplikací, v nichž se mají certifikáty používat (resp. spoléhající se strana), si musí určit, jaké požadavky na certifikát má. Poté využije některou z forem, v jakých validační autorita umožňuje ověřit vhodnost použitého certifikátu. V některých případech validační autorita nabízí i samotné ověření platnosti podpisu či další služby. Odpovědnost za klasifikaci nese validační autorita, která musí zvážit případné riziko. Zařazení certifikační autority pak může

například podmiňovat prováděním auditů podle některých norem. Pro tvůrce aplikací, ve kterých se mají certifikáty používat, je tento systém nejjednodušší, pouze se spolehne na validační autoritu. Tyto služby jsou zpoplatněné, proto tento model bude vhodný spíše pro organizace nebo instituce, které provádějí ověřování velmi často (např. poskytovatele webových služeb).

Schematicky lze znázornit validační autoritu následovně:



Obrázek 8 – Schéma využití validační autority [16]

4.8 Infrastruktura veřejných klíčů

Vše, co bylo výše uvedeno, včetně subjektů, které používají a spoléhají se na certifikáty, se souhrnně nazývá infrastruktura veřejných klíčů. Účelem této infrastruktury je správa klíčů, a to zejména veřejných. V některých případech je možné poskytovat služby, které se týkají správy klíčů soukromých, mohou to však být spíše klíče pro šifrování, pro digitální podpis tento postup není doporučován. Pokud dojde ke ztrátě soukromého klíče určeného pro podpis, bude si uživatel pouze muset pořídit nový certifikát (a ověření jeho dříve vytvořeného podpisu nebude problematické). Pokud dojde ke ztrátě soukromého klíče určeného pro šifrování (resp. dešifrování), nebude možné

zjistit obsah žádné zprávy zašifrované odpovídajícím veřejným klíčem. Proto je v některých případech možné využít službu uchování soukromého klíče nezávislou třetí stranou. Tento krok však obecně nelze vzhledem k možným rizikům doporučit[4].

Infrastruktura veřejných klíčů (Public key infrastructure, zkráceně PKI) je infrastruktura tvořená všemi, kteří disponují veřejným klíčem. Vzhledem k různým možnostem, jak může taková infrastruktura vypadat, dále bude tato práce zaměřena na schéma definované doporučením ITU-T X.509 [18] – tato specifikace je dotvářena de-facto standardy RFC (např. [11], [19], [20], [21], [22], [23]), určenými pro internetovou infrastrukturu veřejných klíčů. Na této specifikaci je založeno pojetí PKI pro služby spojené s poskytováním kvalifikovaných certifikátů v Evropské unii i v České republice (přestože to je nad rámec této práce, je vhodné zmínit, že stejné pojetí PKI je uplatňováno v legislativě i praxi na celém světě – v USA, v asijských, afrických i latinskoamerických zemích).

Cílem při vytváření internetové infrastruktury veřejných klíčů bylo vyhovět potřebám zajistit deterministickou, automatizovanou identifikaci, autentizaci, důvěrnost, řízení přístupu a autorizační funkce. Podpora těchto služeb ovlivňuje atributy obsažené v certifikátu, stejně jako pomocné kontrolní informace v certifikátu, jako jsou údaje o politikách a omezení certifikační cesty.[11]

Ve vztahu k uživatelům bylo záměrem dosažení co nejjednoduššího použití certifikátů na různých platformách při posílání e-mailů a při internetové komunikaci. Lze přivítat, že takové specifikace existují, většinou jsou dostupné zdarma, dokonce je možné dávat podněty k jejich změnám, ale praxe stále není uspokojivá – např. v běžných produktech společnosti Microsoft není

[4] Přestože je využíván čím dál častěji, například organizacemi, jejichž zaměstnanci používají pro svou práci notebooky, jejichž disky z bezpečnostních důvodů šifrují. V případě, že by k soukromému klíči měl přístup pouze příslušný zaměstnanec, přišla by organizace v případě jeho odchodu i o všechna data na pevném disku jeho notebooku. Proto si důvěryhodným způsobem uchovává příslušné soukromé klíče i organizace. Existují pak ovšem dvě místa, odkud může tajná informace o klíči uniknout.

v současnosti možné správně zobrazit všechny informace v certifikátu obsažené. Na druhou stranu vyjadřuje společnost Microsoft ochotu poskytovat služby, které budou v souladu se směrnicí Evropské unie o elektronických podpisech [3], která vychází z dokumentů pro Infrastrukturu veřejných klíčů podle specifikace X.509 (dále PKIX). Proto snad v budoucnu bude uživatelských problémů s certifikáty ubývat.

Zjednodušený model architektury podle specifikace PKIX je znázorněn na níže uvedeném schématu. Prvky tohoto modelu tvoří:

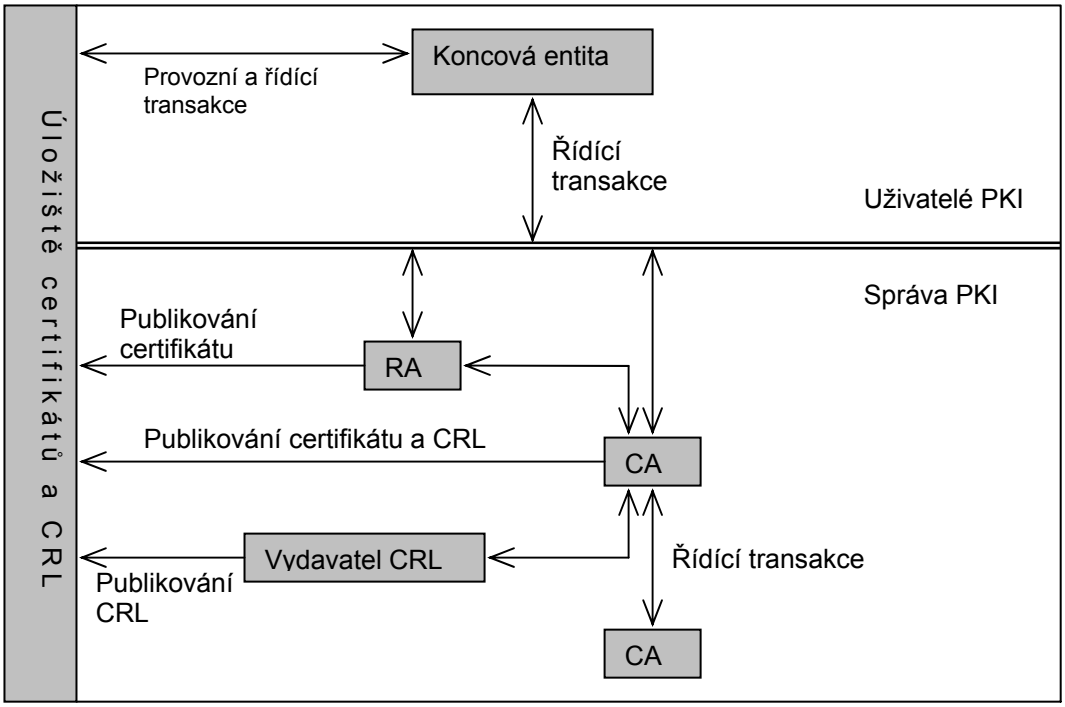
Koncová entita: uživatel nebo systém, který může být uveden v předmětu certifikátu. Může se jednat i o spoléhající se stranu.

Certifikační autorita (CA): subjekt vydávající certifikáty.

Registrační autorita (RA): místo, kde probíhá registrace uživatelů (tuto službu může zajišťovat stejný subjekt jako CA nebo jiný subjekt).

Vydavatel seznamu zneplatněných certifikátů (dále CRL): subjekt, který pro certifikační autoritu publikuje seznam zneplatněných certifikátů (tuto službu může zajišťovat stejný subjekt jako CA nebo jiný subjekt).

Úložiště: servery, na kterých jsou uložena data a odpovídajícím způsobem chráněna (tuto službu může zajišťovat stejný subjekt jako CA nebo jiný subjekt).



Obrázek 9 – Schéma PKIX [11]

4.9 Poskytovatel certifikačních služeb

Mezi důvěryhodné služby poskytovatelů certifikačních služeb (dále PCS) patří nezbytně:

- Služba registrační autority
- Služba generování certifikátů
- Služba vydávání a publikování certifikátů
- Služba zneplatňování certifikátů
- Služba publikování seznamu zneplatněných certifikátů

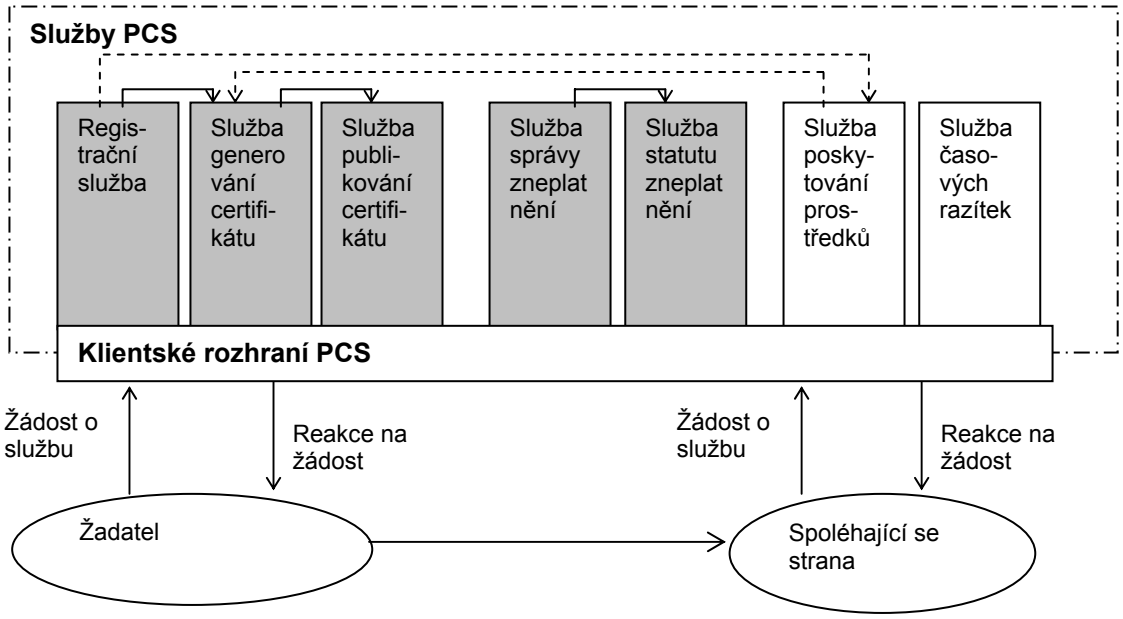
Mezi další možné důvěryhodné služby poskytovatelů certifikačních služeb patří:

- Služba autority časových razítek
- Služba poskytování prostředků pro vytváření podpisu

Všechny uvedené služby mohou být poskytovány jiným subjektem než je PCS, a to na základě smluv, např. formou outsourcingu. Odpovědnost vůči

spoléhající se straně, držiteli certifikátu a podepisující osobě však má samotný PCS.

Jejich vazby ve vztahu k subjektům, které vlastní a používají certifikáty, znázorňuje schéma převzaté z [17].



Obrázek 10 – Schéma služeb poskytovatele a vazeb [17]

4.10 Certifikát veřejného klíče

PKI tedy spočívá v poskytování služeb spojených s certifikáty veřejného klíče. Kromě toho, že certifikát obsahuje veřejný klíč, jsou v něm ještě další údaje. Pro zápis položek, které může certifikát obsahovat, se většinou používá notace ASN.1, definovaná v [24], [25]. Doporučení pro tvorbu profilu certifikátu je uvedeno v RFC 3280. V současné době se používají certifikáty ve formátu X.509 verze 3. Díky potřebě použití těchto certifikátů v prostředí Internetu byl jejich profil specifikován právě zmiňovaným RFC 3280 [11].

Základní syntaxe polí v certifikátu v ASN.1 notaci [11]:

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }
```

```
TBSCertificate  ::=  SEQUENCE  {
     version         [0]  EXPLICIT Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     extensions      [3]  EXPLICIT Extensions OPTIONAL
                          -- If present, version MUST be v3
     }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
     notBefore      Time,
     notAfter       Time }

Time ::= CHOICE {
     utcTime        UTCTime,
     generalTime    GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     subjectPublicKey     BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension  ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING  }
```

Certifikát obsahuje tři základní části – `tbsCertificate`, což je nejrozsáhlejší část, obsahující základní údaje, jako je jméno majitele certifikátu a jeho vystavitele či veřejný klíč. Další částí je `signatureAlgorithm`, který obsahuje identifikátor algoritmu podpisu (jak je výše uvedeno, certifikát musí být digitálně podepsán), pro identifikaci se používá OID (OBJECT IDENTIFIER [26]). Třetí část je samotný podpis certifikátu (resp. digitální podpis části `tbsCertificate`), `signatureValue`.

V části `tbsCertificate` je údaj o verzi certifikátu podle specifikace X.509. Pokud není uveden, předpokládá se verze 1, pokud má být certifikát v souladu s profilem v RFC 3280, musí jít o verzi 3, tzn. položka musí mít hodnotu 2. Dalším údajem je sériové číslo certifikátu unikátní u dané certifikační autority. Dalším údajem je `signature`, který opět obsahuje identifikátor algoritmu podpisu, který musí být stejný jako `signatureAlgorithm` v základní části certifikátu, protože se jedná opět o algoritmus, kterým CA podepisuje vydané certifikáty.

Dalším údajem v certifikátu je `issuer`, tedy CA, která vydala certifikát. V této položce je uveden název této CA. Tato položka může obsahovat více atributů, které jsou stejné jako atributy v poli `Subject`. Příkladem těchto atributů je název organizace, která certifikát vydala, případně její organizační jednotky, údaj o státu, ve kterém je poskytovatel usazen, případně další údaje.

Velmi důležitým údajem je položka `validity`, která se skládá z údajů o době od které je certifikát platný a do které je certifikát platný. Čas je udáván v UTC, tedy koordinovaném světovém času (při zobrazení certifikátu je čas převáděn na místní čas). Údaje mohou být udávány v jednom ze dvou typů zápisu, které se liší počtem míst pro uvedení roku, oba údaje musí být uvedeny ve stejném typu zápisu.

Dalším údajem je `subject`, položka která obsahuje název subjektu, který certifikát používá. Tato položka může mít další atributy stejného typu jako položka `issuer`. Většinou se do této položky uvádí jméno, příjmení, tituly, název organizace a její IČ a případně i adresa.

Další položka je `SubjectPublicKeyInfo`. V této položce je identifikátor algoritmu, který bude sloužit pro šifrování nebo podpis, a samotný veřejný klíč.

Dále jsou v certifikátu dva nepovinné údaje - unikátní identifikátor CA, která vydala certifikát, a unikátní identifikátor subjektu, který certifikát používá.

4.10.1 Rozšíření v certifikátu

Dalším důležitým údajem (resp. posloupností údajů) jsou rozšíření v certifikátu. Těchto rozšíření je více, autorka zmiňuje jen ta nejpodstatnější.

Některá rozšíření jsou povinná pro certifikáty X.509 v3, některá jsou pouze doporučena. Rozšíření tvoří posloupnost jednotlivých rozšíření v certifikátu. Pokud je rozšíření použito, je v certifikátu uvedeno OID daného rozšíření (v poli `extnID`) a ASN.1 zápis hodnoty tohoto rozšíření (v poli `extnValue`). U rozšíření musí být dále uvedeno, zda je kritické nebo není kritické (systém, který používá daný certifikát, musí certifikát odmítnout v případě, že nerozpoznává jeho rozšíření, které je označeno jako kritické; pokud nerozpoznává rozšíření, které kritické není, certifikát lze použít, přestože je v něm takové rozšíření použito).

Identifikátor klíče certifikační autority - na základě tohoto údaje je možné přiřadit veřejný klíč odpovídající soukromému klíči, kterým byl certifikát podepsán. Například pokud certifikační autorita mění kořenový certifikát, budou po určitou dobu platné dva kořenové certifikáty s různými veřejnými klíči. Aby bylo možné určit, který klíč je nutné pro ověření platnosti podpisu použít, je možné využít právě tuto položku.

Identifikátor klíče subjektu – tento údaj slouží k rozlišení certifikátů, které se liší pouze ve veřejném klíči.

Použití klíče (`keyUsage`) je rozšíření, které umožňuje omezit použití klíče v certifikátu, například pouze na šifrování, podpis, nepopiratelnost odpovědnosti, podpis CRL.

Zápis rozšíření použití klíče v ASN.1 notaci:

```
id-ce-keyUsage OBJECT IDENTIFIER ::=  { id-ce 15 }

KeyUsage ::= BIT STRING {
     digitalSignature        (0),
     nonRepudiation          (1),
     keyEncipherment         (2),
     dataEncipherment        (3),
     keyAgreement            (4),
     keyCertSign             (5),
     cRLSign                 (6),
     encipherOnly            (7),
     decipherOnly            (8) }
```

V certifikátu je v případě, že je pro daný účel možno certifikát použít, nastaven příslušný bit odpovídající specifikaci X.509 verze 3. Například

v certifikátu, jemuž odpovídající klíč je určen pro podpis a nepopiratelnost odpovědnosti, bude položka použití klíče nastavena (`110000000`). Aplikace, ve které je certifikát použit, pak nesmí umožnit takto nastavený certifikát použít například pro šifrování (musí tedy tento údaj kontrolovat).

Doporučení pro možné nastavení položky použití klíče vztažmo k algoritmům, které jsou při práci s klíčem použity, je uvedeno v [27]. Kombinace nastavení použití klíče nejsou jinak omezeny (u digitálního podpisu v případě, že se jedná o kvalifikovaný certifikát, je v CWA 14 167-1 [17] doporučeno exkluzivní nastavení bitu `nonRepudiation` – běžné aplikace však použití certifikátu s takovým nastavením neumožňují, takže se v praxi toto doporučení v ČR nepoužívá[5]).

Dalším velmi důležitým rozšířením jsou certifikační politiky (certificate policies). V certifikátu koncového uživatele je to stručná informace o certifikační politice, podle které byl certifikát vydán a podle které je certifikát používán. U nadřízených certifikátů vymezuje použití všech podřízených certifikátů v certifikační cestě. Informace slouží především spoléhající se straně, aby mohla snadno zjistit, jak je možné s certifikátem nakládat, resp. zda se může na certifikát spolehnout. Většinou zde je přímo URL odkaz na certifikační politiku, případně na certifikační prováděcí směrnici, příp. její část, kterou je možné zveřejnit, nebo na zprávu pro uživatele.

Dalším rozšířením je údaj alternativní název subjektu (`subject alternative name`). Tuto položku je možné využít například pro uvedení e-mailové adresy subjektu (tento údaj může být i přímo v položce `subject`, což není zrovna ideální a poskytovatelé skutečně e-mailovou adresu uživatelů uvádějí v certifikátech nejednotně – aplikace jsou však na tuto skutečnost většinou připraveny). Do této položky je možné vkládat takřka libovolné údaje,

[5] Například v Itálii kvalifikované certifikáty mají nastaven exkluzivně pouze bit non-repudiation a uživatelé nemohou při vytváření kvalifikovaného elektronického podpisu (v Itálii používají standardně prostředek pro bezpečné vytváření podpisu) používat standardní e-mailové klienty a používají speciálně vyvinuté aplikace.

je třeba pouze si pro tento účel zřídit nové OID. Běžné aplikace však zobrazí pouze obsah této položky, ale pokud bude tato položka nést obsah, který vyžaduje nějakou funkcionalitu pro své zobrazení, běžné aplikace ji nebudou schopny reprezentovat (může jít např. i o problémy s diakritikou, nebo zobrazením biometrického údaje v podobě fotografie).

Dalším velmi důležitým údajem je CRL distribution points. Zde jsou uvedena místa (internetové adresy), kde si může spoléhající se strana stáhnout seznam zneplatněných certifikátů (CRL). Pro přístup k CRL se nejčastěji používá HTTP protokol, nebo protokol LDAP. Proti tomuto seznamu je nutné provést kontrolu vždy při ověřování platnosti podpisu. Pokud se certifikát na tomto seznamu nachází, nelze se na něj spoléhat.

V certifikátu se ještě mohou objevit rozšíření pro použití na Internetu (Internet certificate extensions). Tato rozšíření se používají pro uvedení informací o přístupu k dalším informacím o poskytovateli, který vydal certifikát, případně o subjektu certifikátu. Pokud například poskytovatel umožňuje přístup k informacím o zneplatnění certifikátů přes OCSP protokol (online certificate status protocol), uveřejní v tomto rozšíření internetovou adresu.

Informace o subjektu certifikátu by měly být v certifikátu uvedeny zejména tehdy, pokud je subjekt certifikátu zároveň certifikační autoritou. V takovém případě zde může být uvedena adresa, kde jsou k dispozici úložiště veřejných certifikátů a CRL. Pokud je subjektem autorita časových razítek, je zde uvedena internetová adresa (URI v případě přístupu přes HTTP nebo FTP, e-mailová adresa /zapsaná ve formátu rfc822Name/ v případě přístupu prostřednictvím elektronické pošty).

4.11 Seznam zneplatněných certifikátů

V případě, že dojde ke kompromitaci soukromého klíče, nebo k nějakému jinému důvodu pro ukončení platnosti certifikátu, je nutné jej nechat u poskytovatele certifikačních služeb zneplatnit. Poskytovatel musí co nejdříve tuto informaci přidat na seznam zneplatněných certifikátů. Tento seznam poté pravidelně vydává na místech, která jsou uvedena v certifikátu. Tento seznam

musí být digitálně podepsán svým vystavitelem. Nejčastěji jím je přímo certifikační autorita, která vydala příslušný certifikát, ale je možné tuto odpovědnost delegovat na jinou důvěryhodnou třetí stranu.

Spoléhající se strana má povinnost při ověřování platnosti podpisu zkontrolovat, jestli se certifikát podepisující osoby nenachází na seznamu zneplatněných certifikátů.

4.11.1 Profil CRL

V současné době má poslední verze profilu CRL dle X.509 číslo 2.

Zápis profilu základních položek CRL v ASN.1 notaci [11]:

```
CertificateList  ::=  SEQUENCE  {
  tbsCertList          TBSCertList,
  signatureAlgorithm   AlgorithmIdentifier,
  signatureValue       BIT STRING  }

       TBSCertList  ::=  SEQUENCE  {
       version                 Version OPTIONAL,
                                    -- if present, MUST be v2
       signature               AlgorithmIdentifier,
       issuer                  Name,
       thisUpdate              Time,
       nextUpdate              Time OPTIONAL,
       revokedCertificates     SEQUENCE OF SEQUENCE  {
            userCertificate         CertificateSerialNumber,
            revocationDate          Time,
            crlEntryExtensions      Extensions OPTIONAL
                                          -- if present, MUST be v2
                                  }  OPTIONAL,
       crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                          -- if present, MUST be v2
                                  }
```

CRL obsahuje stejně jako certifikát tři základní části – `TBSCertList`, `SignatureAlgorithm` a `SignatureValue`. Položka `SignatureAlgorithm` obsahuje identifikátor algoritmu, který byl použit pro podpis CRL, resp. části `TBSCertList` (TBS znamená „to be signed“ – indikuje tedy určení této části k podpisu). Tento identifikátor algoritmu musí být stejný jako identifikátor algoritmu v poli `signature` přímo v posloupnosti `TBSCertList`. Položka `SignatureValue` pak obsahuje samotnou hodnotu vypočteného podpisu.

Nejobsáhlejší součást CRL je posloupnost `TBSCertList`. V poli `version` je uvedena verze, pokud má být CRL v souladu s [11], musí to být verze 2. Dalším polem je již zmiňovaný `signature`, obsahující identifikátor algoritmu, který byl použit pro podpis CRL a který musí být totožný s algoritmem uvedeným v `SignatureAlgorithm`.

`TBSCertList` dále obsahuje položku `issuer`, která musí odpovídat pravidlům definovaným pro položku `issuer` v certifikátu. Účelem této položky je identifikace vydavatele CRL.

Další položkou je `ThisUpdate`, ve které je uvedena doba, kdy byl daný seznam zneplatněných certifikátů vydán. Formát zápisu času je `UTCTime`, případně `GeneralizedTime`, pokud se počítá s dobou po roce 2049 [6] (aplikace poskytovatele na tuto okolnost může být připravena). Dalším údajem je `NextUpdate`, což je doba, kdy bude vydán následující seznam zneplatněných certifikátů. CRL může být vydáno před touto dobou, ale nesmí být vydáno později než v uvedené době. Formát zápisu je stejný jako u `ThisUpdate`.

Nejdůležitější součástí `TBSCertList` je samotný seznam certifikátů, které jsou reprezentovány sériovým číslem. Kromě sériového čísla musí být na seznamu uvedena doba, kdy nastalo zneplatnění, a mohou zde být uvedeny rozšiřující položky pro vstup na CRL – `CRLEntryExtensions`. Nejpodstatnějším rozšířením tohoto druhu je `reasonCode`, kterým je uveden důvod zneplatnění. Může nabývat následujících hodnot:

```
id-ce-cRLReason OBJECT IDENTIFIER ::= { id-ce 21 }

-- reasonCode ::= { CRLReason }

CRLReason ::= ENUMERATED {
     unspecified             (0),
     keyCompromise           (1),
     cACompromise            (2),
     affiliationChanged      (3),
     superseded              (4),
     cessationOfOperation    (5),
```

[6] Formát `UTCTime` obsahuje pouze dvě čísla pro vyjádření roku. Proto se pro data před rokem 1950 a po roce 2049 používá formát `GeneralizedTime`.

```
certificateHold          (6),
removeFromCRL            (8),
privilegeWithdrawn       (9),
aACompromise            (10) }
```

Dalším údajem v `CRLEntryExtensions` je `invalidityDate`, ve kterém je možné uvést dobu, kdy byl certifikát již neplatný (například kdy došlo, nebo lze předpokládat, že došlo, ke kompromitaci soukromého klíče). Tato doba může předcházet době, kdy nastalo zneplatnění uvedené přímo na CRL (tam je uvedena doba, kdy poskytovatel provedl zneplatnění).

Samotný `TBSCertList` může obsahovat vlastní rozšíření, která slouží k přičlenění dalších atributů k CRL. Nejdůležitějšími rozšířeními, která jsou v případě, že má být profil CRL v souladu se specifikací v [11], povinná, jsou `AuthorityKeyIdentifier` a `CRLNumber`. `AuthorityKeyIdentifier` slouží k určení správného klíče, kterým byl seznam zneplatněných certifikátů podepsán – to je důležité zejména pokud má poskytovatel klíčů více. `CRLNumber` slouží k snadnější orientaci uživatelů, protože se jedná o rostoucí posloupnost celých čísel, ze které lze snadno určit, jestli již byl vydán nový seznam zneplatněných certifikátů.

4.12 Časová razítka

Poskytovatel certifikačních služeb může kromě „klasických“ certifikačních služeb poskytovat i službu časových razítek. Principielně je časové razítko obdobou certifikátu, kde je však nejpodstatnější informací datum, čas a jednoznačná reprezentace dat, k nimž bylo razítko časové vydáno. Kromě toho, narozdíl od certifikátů veřejného klíče, není povoleno, aby poskytovatel ověřoval, kdo o časové razítko požádal.

Časové razítko (time-stamp token, TST) slouží k tomu, aby bylo možné ověřit, zda určitá data existovala před určitým časovým okamžikem. Toho lze využít například i pro ověření, zda byl digitální podpis dokumentu vytvořen před určitým okamžikem (například před tím, než došlo ke zneplatnění certifikátu, na němž byl digitální podpis založen).

Časové razítko se vytváří tak, že nejprve uživatel – žadatel o časové razítko – vytvoří hash (automaticky vytvořený pomocí hashovací funkce) dat, u nichž bude chtít potvrdit existenci v čase. Tento otisk dat zašle poskytovateli k „orazítkování“. Poskytovatel poté z důvěryhodného zdroje času přiřadí k otisku strukturovanou formou čas a své vlastní identifikátory. Tuto strukturu opatří svým digitálním podpisem – tak vznikne samotné časové razítko. Sám si u sebe uloží tzv. time mark – časovou značku, což je v podstatě auditní log. Dále vypočte otisk posloupnosti časových razítek (záleží na tom, jak dlouhou posloupnost si zvolil) a tu taktéž uloží – toto opatření zamezí případnému pokusu o falšování (není pak možné podstrčit časové razítko, které bude obsahovat čas mezi dvěma skutečně existujícími razítky). Časové razítko pošle zpět uživateli.

Autorita časových razítek je dle RFC 3161 [22] definována jako TTP (Trusted Third Party - důvěryhodná třetí strana), která vytváří časová razítka pro důkaz existence dat v daném časovém okamžiku.

4.12.1 Požadavky na autoritu časových razítek

Na autoritu časových razítek, která bude postupovat v souladu s RFC 3161 [22] jsou kladeny následující požadavky:

- používat důvěryhodný zdroj času,
- vkládat důvěryhodnou časovou hodnotu do každého časového razítka,
- každé nové časové razítko generovat s jedinečným sériovým číslem,
- vytvářet časové razítko pro každou korektní žádost,
- do každého časového razítka vložit identifikaci bezpečnostní politiky,
- označovat časovým razítkem pouze otisk dat,
- kontrolovat, že délka hashe odpovídá definované délce jednocestné hashovací funkce identifikované pomocí OID,
- netestovat jiným způsobem korektnost OID,
- nezahrnovat identifikaci žadatele do časového razítka,
- podepisovat každé časové razítko klíčem a certifikátem využívaným výhradně pro tyto účely,

- odpovídat chybovým hlášením, pokud jsou požadovány doplňkové informace, které autorita časových razítek neposkytuje. [28],[22]

4.12.2 Žádost o časové razítko

Profil žádosti o časové razítko definovaný v RFC 3161 [22] zapsaný v ASN.1 notaci je následující:

```
TimeStampReq ::= SEQUENCE  {
   version                      INTEGER  { v1(1) },
   messageImprint               MessageImprint,
     --a hash algorithm OID and the hash value of the data to be
     time-stamped
   reqPolicy             TSAPolicyId              OPTIONAL,
   nonce                 INTEGER                  OPTIONAL,
   certReq               BOOLEAN                  DEFAULT FALSE,
   extensions            [0] IMPLICIT Extensions  OPTIONAL  }

MessageImprint ::= SEQUENCE  {
        hashAlgorithm                AlgorithmIdentifier,
        hashedMessage                OCTET STRING  }
```

Žádost obsahuje informaci o verzi, ze které lze určit, podle jakých pravidel je žádost vytvořena. Dalším údajem je zmíněný otisk dat, která mají být „orazítkována“ – ten je rozdělen na dvě části, jednak musí být uvedeno OID hashovací funkce, která byla pro vytvoření otisku použita, a dále zde je uveden samotný otisk.

Pole `reqPolicy` obsahuje OID politiky, podle které bylo časové razítko vytvořeno. V časovém razítku může být uvedeno náhodné číslo (`nonce`), které žadatel vytvoří, a autorita časových razítek jej musí poslat ve své odpovědi (pokud je v žádosti uvedeno). Důvodem zahrnutí tohoto údaje je zvýšení bezpečnosti – pro útočníka je obtížnější zahrnout při útoku typu „man-in-the-middle“ do podvrženého časového razítka i tento údaj.

Další položkou je `certReq`. Tato položka slouží k určení, jestli chce žadatel v odpovědi zahrnout certifikát veřejného klíče, kterým bylo časové razítko podepsáno.

Žádost neobsahuje identifikaci žadatele – tato informace není součástí protokolu a autorita časových razítek tuto informaci nesmí ověřovat. Pokud tuto

informaci chce použít, musí pro identifikaci a autentizaci žadatele použít jiné prostředky[7].

4.12.3 Odpověď na žádost o časové razítko

Syntaxe odpovědi autority časových razítek je v ASN.1 definována [22]:

```
TimeStampResp ::= SEQUENCE  {
      status                  PKIStatusInfo,
      timeStampToken          TimeStampToken     OPTIONAL  }
```

Odpověď obsahuje dvě základní části – `PKIStatusInfo` a `TimeStampToken`. Pokud má `PKIStatusInfo` hodnotu `Status` 0 nebo 1, musí být v odpovědi obsaženo časové razítko (`TimeStampToken`). V případě, že má jakoukoliv jinou hodnotu, nesmí být obsaženo.

```
PKIStatusInfo ::= SEQUENCE {
      status        PKIStatus,
      statusString  PKIFreeText     OPTIONAL,
      failInfo      PKIFailureInfo  OPTIONAL  }
```

`status` musí nabývat jednu z hodnot:

```
PKIStatus ::= INTEGER {
      granted                (0),
      -- when the PKIStatus contains the value zero a TimeStampToken,
       -- as requested, is present.
      grantedWithMods        (1),
       -- when the PKIStatus contains the value one a TimeStampToken,
       -- with modifications, is present.
      rejection              (2),
      waiting                (3),
      revocationWarning      (4),
       -- this message contains a warning that a revocation is
       -- imminent
      revocationNotification (5)
       -- notification that a revocation has occurred  }
```

Položka `statusString` z `PKIStatusInfo` může obsahovat slovní odůvodnění, proč nebylo v odpovědi zahrnuto časové razítko.

[7] Poskytovatel tuto informaci samozřejmě potřebuje za účelem plateb – poskytovatel však identifikaci a autentizaci provádí nezávisle na službě vydávání TST.

V případě, že v odpovědi není časové razítko (hodnota `TimeStampToken`), musí být v položce `failInfo` indikován důvod. Tato položka může nabývat následujících hodnot:

```
PKIFailureInfo ::= BIT STRING {
   badAlg               (0),
     -- unrecognized or unsupported Algorithm Identifier
   badRequest           (2),
     -- transaction not permitted or supported
   badDataFormat        (5),
     -- the data submitted has the wrong format
   timeNotAvailable    (14),
     -- the TSA's time source is not available
   unacceptedPolicy    (15),
     -- the requested TSA policy is not supported by the TSA
   unacceptedExtension (16),
     -- the requested extension is not supported by the TSA
    addInfoNotAvailable (17)
      -- the additional information requested could not be understood
      -- or is not available
    systemFailure       (25)
      -- the request cannot be handled due to system failure  }
```

Dále může být v odpovědi v případě korektního stavu (tedy hodnoty `status` 0 nebo 1) samotné časové razítko. Časové razítko obsahuje OID, které jednoznačně určuje typ obsahu (`contentType`) a samotný obsah (`content`). Obě položky jsou naplňovány v souladu s RFC 2630 [21], které popisuje syntaxi kryptografických zpráv.

```
TimeStampToken ::= ContentInfo
     -- contentType is id-signedData ([21])
     -- content is SignedData ([21])
     -- eContentType within SignedData is id-ct-TSTInfo
     -- eContent within SignedData is TSTInfo
```

V obsahu v položce `SignedData` je obsažen identifikátor (OID) určující typ obsahu uvnitř položky obsahu a sekvence `TSTInfo`, která obsahuje následující prvky:

```
TSTInfo ::= SEQUENCE  {
   version                      INTEGER  { v1(1) },
   policy                       TSAPolicyId,
   messageImprint               MessageImprint,
     -- MUST have the same value as the similar field in
```

```
  -- TimeStampReq
serialNumber                 INTEGER,
 -- Time-Stamping users MUST be ready to accommodate integers
 -- up to 160 bits.
genTime                      GeneralizedTime,
accuracy                     Accuracy                 OPTIONAL,
ordering                     BOOLEAN              DEFAULT FALSE,
nonce                        INTEGER                  OPTIONAL,
  -- MUST be present if the similar field was present
  -- in TimeStampReq.  In that case it MUST have the same value.
tsa                          [0] GeneralName          OPTIONAL,
extensions                   [1] IMPLICIT Extensions   OPTIONAL  }
```

Verze obsahuje číslo vyjadřující verzi časového razítka. Pole `policy` musí obsahovat identifikátor politiky, podle které bylo časové razítko vydáno. Pokud se neshoduje s identifikátorem umístěným v žádosti, musí žadateli vrátit chybové hlášení (`PKIFailureInfo` bude mít hodnotu 15, `unacceptedPolicy`).

Pole `messageImprint` obsahuje otisk dat, k nimž je přiřazeno dané časové razítko. Tento otisk se musí shodovat s otiskem zaslaným žadatelem o časové razítko.

Sériové číslo (`serialNumber`) je kladné celé číslo přiřazené poskytovatelem ke každému vydanému časovému razítku. Toto číslo musí být unikátní u dané autority časových razítek a tato vlastnost musí být zaručena i v případě přerušení služby.

Časový údaj uvedený v časovém razítku v položce `genTime` reprezentuje moment vytvoření razítka autoritou časových razítek. Údaj je podle RFC 3161 [22] a TS 102 023 [29] vyjádřen jako čas UTC (Coordinated Universal Time).

Pole `accuracy` udává přesnost, jakou má uváděný čas. Jedná se o následující posloupnost:

```
Accuracy ::= SEQUENCE {
        seconds        INTEGER              OPTIONAL,
        millis     [0] INTEGER  (1..999)    OPTIONAL,
        micros     [1] INTEGER  (1..999)    OPTIONAL  }
```

Přičtením k časovému údaji získáme horní hranici, kdy mohlo být nejpozději vytvořeno časové razítko. Odečtením přesnosti od času vytvoření časového razítka získáme údaj, kdy nejdříve mohlo být časové razítko

vytvořeno. Pokud pole `accuracy` není v časovém razítku obsaženo, je nutné, aby byl uveden v nějaké jiné veřejně dostupné dokumentaci, například v politice pro vydávání časových razítek.

Pole `ordering` indikuje, jestli autorita časových razítek zaručuje, že všechna časová razítka bude možné seřadit podle údaje v poli `genTime` nezávisle na přesnosti v poli `accuracy`. V opačném případě (tedy pokud hodnota v poli `ordering` není uvedena nebo je nastavena na FALSE) je možné seřadit dvě časová razítka od jedné nebo různých autorit časových razítek pouze pokud interval mezi vydáním prvního a druhého časového razítka je větší než součet přesností u obou těchto razítek.

Pole `nonce` musí být obsaženo pouze v případě, že bylo obsaženo v žádosti, a pak musí mít stejnou hodnotu, jako mělo v dané žádosti.

Pole `tsa` je v časovém razítku obsaženo proto, aby v něm mohl být uveden název vydávající autority časových razítek. Toto jméno má být shodné se jménem uvedeným v poli `subject` certifikátu, na základě kterého má být ověřena platnost časového razítka. V praxi se však pro tento účel používá identifikátor certifikátu `ESSCertID` v položce `SigningCertificate`, která je součástí položky `signerInfo`.

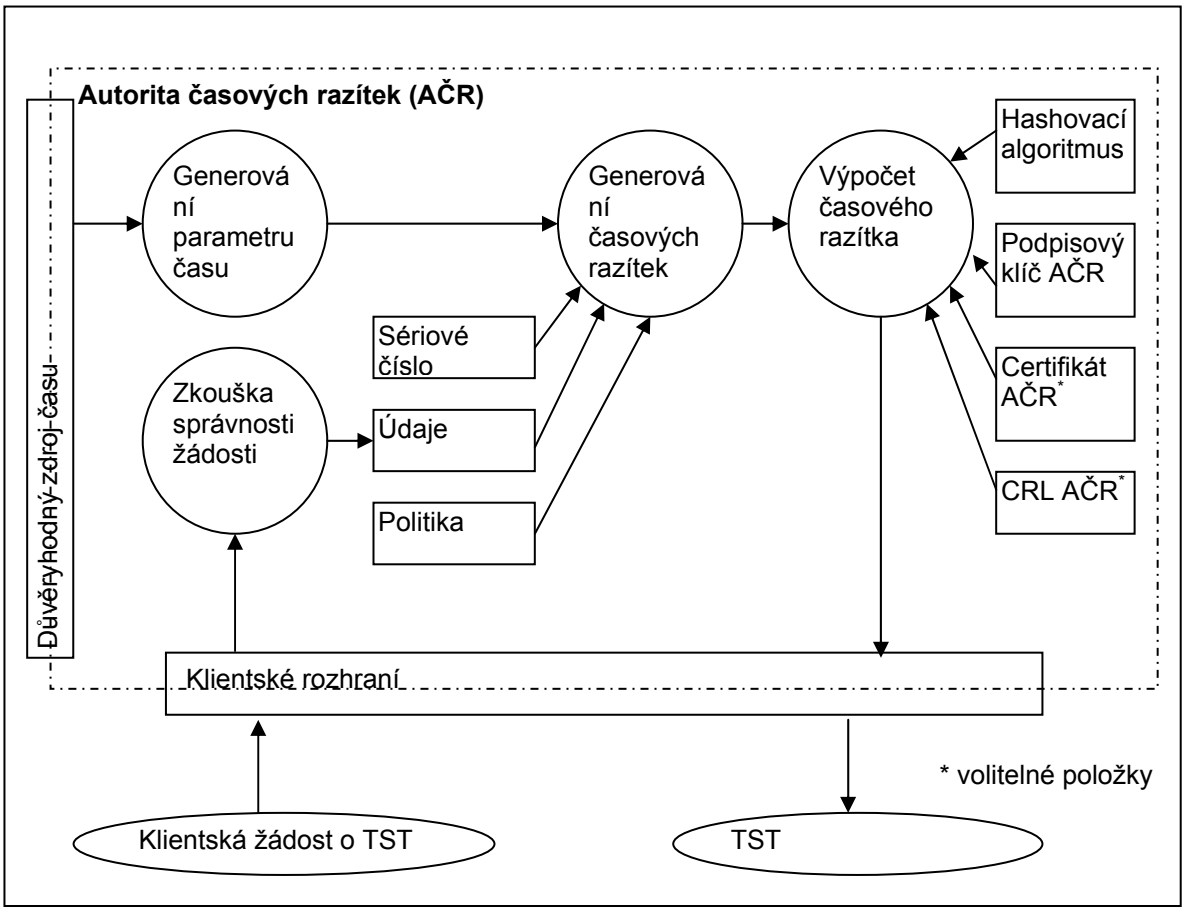
Pole `extensions` může sloužit k případným budoucím rozšířením, která se ukážou jako vhodná pro použití v časovém razítku.

4.12.4 Ověření platnosti časového razítka

Uživatel, případně jiná osoba, která se chce přesvědčit o pravosti časového razítka, po přijetí zprávy s časovým razítkem nejprve ověří digitální podpis časového razítka (použije veřejný klíč z veřejně dostupného certifikátu autority časových razítek poskytovatele certifikačních služeb, jehož platnost nejprve ověří), poté vypočte otisk ze zprávy a porovná jej s otiskem uvedeným ve struktuře časového razítka. Pokud jsou otisky shodné, je razítko v pořádku.

Pokud by i přesto osoba, která se chce přesvědčit o pravosti časového razítka, resp. o skutečnosti, zda data existovala před určitým časovým okamžikem, nedůvěřovala – případně by chtěla ověřit platnost časového razítka

po dlouhé době, je možné si u poskytovatele certifikačních služeb vyžádat doložení existence dat na základě časových značek u něj uložených.



Obrázek 11 – Schéma poskytování časových razítek

4.13 Bezpečné kryptografické prostředky

Soukromý klíč, jak je uvedeno výše, může být uložen na různých médiích. Nejjednodušší způsob je jeho uložení na pevném disku počítače. Tento způsob však není ideální z bezpečnostního hlediska. Z bezpečnostního hlediska žádný skutečně ideální způsob neexistuje, ale úroveň záruk v tomto případě může být i vyšší. Toho lze docílit použitím média, které může podepisující osoba držet o něco více pod svou výhradní kontrolou. Takovým médiem může být například čipová karta nebo USB token.

Samotná čipová karta však není zárukou bezpečnosti, důležité jsou její parametry, jejichž ověření může být doloženo například nějakým certifikátem nebo jiným uznávaným hodnocením (nejčastěji se využívá hodnocení podle Common Criteria [33] na potřebnou úroveň záruk - EAL). Čipovou kartu v podstatě tvoří jak samotný hardware, tak vlastní operační systém a další programové vybavení, které se používá při provádění kryptografických funkcí a při generování náhodných čísel použitých pro vytvoření soukromých a veřejných klíčů – hodnoceno by tedy v ideálním případě mělo být oboje.

Je vhodné si v případě, že uživatel chce mít soukromý klíč uložený na čipové kartě, obstarat čipovou kartu přímo od poskytovatele, od kterého získal i certifikát. Tím je zaručena kompatibilita. Pokud uživatel důvěřuje danému poskytovateli, což dává najevo koupí certifikátu, může mu důvěřovat i v případě získání čipové karty.

Použití čipové karty má i svá úskalí – čipová karta musí být při použití ve čtečce čipových karet, a to v kompatibilní čtečce. Může se tak teoreticky stát, že ke každé čipové kartě potřebuje uživatel jinou čtečku, což je uživatelsky nepřívětivé (a pokud je čtečka stejná, musí čipové karty pro jednotlivé operace postupně vyměňovat).

Na druhou stranu existuje značné riziko, že uživatel přijde o svůj soukromý klíč uložený v úložišti certifikátů svého operačního systému ve svém počítači, například při havárii pevného disku. Proto je vhodné soukromý klíč exportovat na disketu nebo jiné vhodné médium (které musí být bezpečně uloženo), což je pro uživatele opět náročné – uživatelská přívětivost je tedy v jednotlivých případech na individuálním zvážení.

Problematice bezpečných prostředků se autorka věnuje dále v textu, vzhledem k tomu, že je to téma poměrně obsáhlé a nesouvisí přímo s obsahem této práce, bude se tomuto tématu věnovat pouze okrajově.

5 OBLAST KVALIFIKOVANÝCH CERTIFIKAČNÍCH SLUŽEB

Až dosud se autorka věnovala obecnému a spíše teoretickému popisu jednotlivých možných služeb poskytovatele certifikačních služeb a ukázala návaznosti mezi těmito službami v rámci infrastruktury veřejných klíčů. Zabývala se vysvětlením základních principů, které jsou obecně platné, protože jsou zejména technického a technologického rázu. Dále bude téma zúženo a tato práce se bude věnovat pouze úzce vymezené oblasti, kterou je oblast tzv. kvalifikovaných certifikačních služeb, která je v České republice vymezena zákonem o elektronickém podpisu, prováděcími předpisy k tomuto zákonu a souvisejícími normami.

5.1 Zákon o elektronickém podpisu č. 227/2000 Sb.

5.1.1 Historie zákona o elektronickém podpisu

V roce 2000 byl připraven Úřadem na ochranu osobních údajů zákon o elektronickém podpisu [2]. Smyslem zákona bylo umožnit použití digitálního podpisu v rámci elektronické komunikace jako ekvivalent podpisu vlastnoručního při běžné listinné formě komunikace.

V této oblasti od roku 1999 existuje směrnice Evropské unie [3], na základě které byl zákon vytvořen – prostředí v České republice by mělo být zejména v oblasti informačních a komunikačních technologií v souladu s prostředím v zemích EU, aby byla snazší vzájemná komunikace. Směrnice EU však nebyla příliš striktní, takže ač všechny země mají legislativu v souladu s touto směrnicí, dosažení interoperability není vůbec jednoduché právě kvůli různým zvoleným modelům.

Zřejmě nejvýrazněji se projevila věta „*Členské státy mohou používání elektronických podpisů ve veřejnoprávním sektoru podmínit případnými doplňujícími požadavky*.“ [3]. Díky ní většina států v souladu se směrnicí vytvořila dobrovolné akreditační schéma pro poskytovatele certifikačních služeb. Zákonem pak podmínila použití digitálního podpisu při komunikaci

v rámci veřejného sektoru použitím elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Protože však směrnice nenařizuje vzájemné uznávání akreditací, a akreditační schéma je navíc dobrovolné, takže jej některé státy nemají, vzájemné uznávání kvalifikovaných certifikátů je sice hypotetickou možností, ale není takřka vůbec využíváno. Přesto existují snahy (nejsou však většinou dostatečně podporovány) umožnit spoléhající se straně alespoň rozeznat, zda se jedná o kvalifikovaný certifikát. Příkladem může být výše popsaný projekt EBGCA. Dokud nebude toto ověření prakticky možné, státy nemají tendenci v této oblasti vyvíjet žádné aktivity.

V roce 2001 byla k zákonu [2] vydána vyhláška č. 366/2001 Sb. [34] upravující oblast poskytovatelů certifikačních služeb. Tato vyhláška je svědectvím své doby, ve které ještě nebyly v Evropské unii vytvořeny normy konkretizující oblast PKI. Tvůrci vyhlášky byli nuceni si některé podmínky určit sami. Obdobná situace byla i v jiných zemích, což vedlo jednak k tomu, že poskytovatelé v jednotlivých zemích mají různé podmínky, a dále k tomu, že v České republice, ale i v dalších státech, jsou některé požadavky přísnější či jiné, než jaké ukládají v současné době existující normy Evropské unie pro tuto oblast.

Zákon byl novelizován v roce 2002, a to dokonce dvakrát. Nejprve byl zákonem č. 226/2002 Sb. přidán odstavec o nutnosti identifikovat z certifikátu podepisující osobu. Novelizace zákonem č. 517/2002 Sb. zákon upravovala pouze kvůli přechodu kompetencí v oblasti elektronického podpisu z Úřadu na ochranu osobních údajů na Ministerstvo informatiky. Zásadnější novelizace proběhla v roce 2004, a to zákonem č. 440/2004 Sb., o té viz níže. Kvůli této rozsáhlé novelizaci bylo vydáno úplné znění zákona (ve Sbírce zákonů má číslo 486/2004 [1]). Je velmi pravděpodobné, že v brzké době proběhne další novelizace zákona o elektronickém podpisu, která bude převádět kompetence z Ministerstva informatiky na Ministerstvo vnitra.

V roce 2006 byla vydána nová vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích a nástroje

elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek [53]. Tato vyhláška zrušila vyhlášku č. 366/2001 Sb.[34] a upravila postupy kvalifikovaných poskytovatelů certifikačních služeb, přičemž vychází z norem ETSI a CEN, které jsou využívány ve státech EU.

V roce 2002 byla udělena akreditace prvnímu poskytovateli certifikačních služeb v České republice. V roce 2005 byla udělena akreditace dalším dvěma poskytovatelům certifikačních služeb (pro poskytování kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů). V roce 2006 rozšířil první akreditovaný poskytovatel své služby o poskytování kvalifikovaných časových razítek a kvalifikovaných systémových certifikátů. Vzhledem k velikosti trhu[8] v České republice nelze očekávat v dohledné době další žádosti o akreditaci.

5.1.2 Základní principy zákona o elektronickém podpisu

Vzhledem ke skutečnosti, že zákon existuje v prostředí právního řádu ČR a svým způsobem i EU, používá v některých případech odlišné pojmy, které odpovídají některým pojmům „technického světa“ popsaným výše. Proto budou na tomto místě vysvětleny základní pojmy, které bude nutné používat v následujícím textu.

Elektronický podpis ve smyslu zákona o elektronickém podpisu představuje pouze data spojená se zprávou a umožňující identifikaci osoby. To znamená, že elektronickým podpisem ve smyslu zákona o elektronickém podpisu je zpráva, na konci které je napsáno jméno a příjmení dané osoby (případně další údaj umožňující její jednoznačnou identifikaci, např. pokud je podepsán Pavel Novák). Tyto požadavky jsou minimální, rozhodně nemají postačující úroveň, aby je bylo možno považovat za ekvivalent vlastnoručnímu podpisu.

Proto je v zákoně zaveden pojem zaručený elektronický podpis, který již ve své definici obsahuje podmínky, které je v současnosti možné naplnit využitím asymetrické kryptografie, hashovacích funkcí a organizačně-

[8] V České republice je zatím přibližně 40 000 platných kvalifikovaných certifikátů, tj. přibližně 40 000 klientů, kteří využívají služby poskytovatelů certifikačních služeb.

technických opatření umožňujících se spoléhat na údaje v certifikátu. Technologicky tedy podmínky splňuje digitální podpis.

V novele zákona byl zaveden další pojem - uznávaný elektronický podpis. Jedná se v podstatě o zkratku pro zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. Kvalifikovaným certifikátem je míněn certifikát veřejného klíče, na který, resp. na jehož vydání, jsou kladeny zákonné požadavky. Kvalifikovaný certifikát umožňuje identifikovat podepisující osobu, a touto osobou musí být osoba fyzická. Poskytovatel certifikačních služeb, který požádá Ministerstvo informatiky o akreditaci a je mu vydáno osvědčení o akreditaci, je akreditovaným poskytovatelem. Po získání akreditace může být u akreditovaných poskytovatelů prováděna kontrola[9]. Tato kontrola se provádí podle zákona o státní kontrole [37]. Vzhledem k tomu, o jakou jde odpovědnost (poskytovatel spravuje systém, na základě kterého vytvářejí občané podpisy, které jsou na úrovni vlastnoručních podpisů), je to velmi důležitý mechanismus, který je zaveden, aby zaručil dostatečnou důvěryhodnost.

Elektronická značka je pojem, který byl nově zaveden při poslední novelizaci zákona. Zaveden byl zejména proto, že byl velký zájem ze strany úřadů i soukromých společností, aby bylo možné mít podpis „na firmu“ nebo „na úřad“ a provádět podepisování automatizovaně. Například vydávání výpisů z různých evidencí je ze strany veřejnosti velmi žádané a úřady se bránily právě argumentem, že pokud musí výpisy stejně podepisovat pracovník, je to neefektivní a příliš ekonomicky náročné. Pojmem elektronická značka se označuje digitální podpis, který je vytvořen na základě certifikátu, který může být vydán i právnické osobě (nemusí v něm být uvedeno konkrétní jméno fyzické osoby), a tento digitální podpis může být vytvářen automatizovaně. Certifikát, na základě kterého lze elektronicky označit data, se nazývá kvalifikovaný systémový certifikát.

---

[9] Kontrola se provádí i u kvalifikovaných poskytovatelů, kteří splní oznamovací povinnost – oznámí ministerstvu informatiky, že budou vydávat kvalifikované certifikáty.

Vzhledem k tomu, že je problematické vyjádřit vazbu mezi certifikátem a podpisem, resp. elektronickou značkou (daty obsaženými v certifikátu lze podpis ověřit, ale ne vytvořit), je v zákoně použita konstrukce „elektronický podpis založený na kvalifikovaném certifikátu“ – tím je míněn elektronický podpis vytvořený s využitím soukromého klíče, který odpovídá veřejnému klíči z kvalifikovaného certifikátu.

Soukromý klíč je v zákoně označován jako data pro vytváření elektronického podpisu a veřejný klíč jako data pro ověřování elektronického podpisu.

Kvalifikované časové razítko bylo také zavedeno až novelizací zákona v roce 2004. Důvodem byla opět poptávka ze strany soukromoprávní a veřejnoprávní. Objevovaly se výklady, které naznačovaly, že dokument bez důvěryhodného časového razítka nemusí být uznán jako důkaz u soudu. Použití časových razítek je potřebné zejména pro elektronickou archivaci. U soudu se však dosud žádný spor v této oblasti neprojednával a úprava archivace dokumentů v elektronické podobě v naší zemi zatím spíše nevnímá existenci elektronických dokumentů [38]. Kvalifikované časové razítko je svou strukturou totožné s časovým razítkem, podmínky pro jeho poskytování jsou omezeny tím, že jeho poskytovatel musí být kvalifikovaným nebo akreditovaným poskytovatelem certifikačních služeb. Další podmínky jsou obsaženy ve vyhlášce, které je věnována následující kapitola.

Zákon o elektronickém podpisu nejprve určuje požadavky na zaručený elektronický podpis a elektronické značky – tyto požadavky byly naformulovány tak, aby nebyla upřednostňována jedna určitá technologie (tedy asymetrická kryptografie) a v případě potřeby by mohla být nahrazena jinou[10].

Dále se definují základní povinnosti podepisující a označující osoby a povinnosti držitele certifikátu. Držitelem certifikátu je míněn ten, kdo jej koupil

[10] Popravdě řečeno se jedná do určité míry o alibismus, který vyplývá již ze směrnice EU, protože v zákoně se muselo vycházet z určitých reálných předpokladů, tedy z konkrétní použité technologie a s ní spojených postupů. V případě, že by byla technologie digitálního podpisu prolomena a nahrazena jiným postupem, jistě by muselo ke změně zákona dojít.

a má jej ve svém majetku. Podepisující, resp. označující osoba nemusí být vždy držitelem certifikátu – například pokud zaměstnavatel vybaví své zaměstnance kvalifikovanými certifikáty, je držitelem certifikátu zaměstnavatel a podepisující osobou je příslušný zaměstnanec. Je důležité vědět, že z vlastnictví soukromého klíče vyplývá určitá povinnost se o něj náležitě starat – to je totiž oblast, kde ani sebedokonalejší technologie nepomůže, protože závisí zejména na lidském faktoru.

Dále jsou v zákoně uvedeny povinnosti kvalifikovaného poskytovatele certifikačních služeb, jejichž realizace je dále upravena prováděcí vyhláškou. Povinnosti kvalifikovaného poskytovatele jsou dále rozvedeny pro oblast vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek.

Zákonem je dále upravena odpovědnost za porušení povinností daných zákonem. Veškerou odpovědnost za škodu má poskytovatel certifikačních služeb. Pouze v případě, kdy se spoléhající se strana spolehne na certifikát, jehož použití je omezeno, v oblasti, pro kterou není certifikát určen, nese odpovědnost tato spoléhající se strana.

Další paragrafy se zabývají akreditacemi a výkonem dozoru. Poskytovatel certifikačních služeb se může stát kvalifikovaným poskytovatelem certifikačních služeb tak, že skutečnost, že bude poskytovat kvalifikované služby, oznámí Ministerstvu informatiky.

Pokud chce poskytovatel certifikačních služeb získat akreditaci, může o ni požádat Ministerstvo informatiky. To na základě předložené dokumentace posoudí, jestli má předpoklady pro poskytování kvalifikovaných certifikačních služeb. Pokud jsou předpoklady splněny, akreditaci mu udělí. Proces akreditace především spočívá ve spolupráci s poskytovatelem certifikačních služeb, který v průběhu řízení upravuje svou dokumentaci a postupy na základě požadavků ministerstva tak, aby naplnil všechny zákonné požadavky.

U kvalifikovaných i akreditovaných poskytovatelů provádí Ministerstvo informatiky dozor, při kterém postupuje podle zákona o státní kontrole [37]. Protože není proces akreditace ani dozoru systematicky rozpracován

do podoby metrik, autorka dále definuje metriky pro některé základní požadavky zákona na postupy poskytovatele certifikačních služeb.

Akreditovaní poskytovatelé mohou rozšířit poskytování kvalifikovaných certifikačních služeb, a to tak, že tuto skutečnost oznámí ministerstvu a předloží dokumentaci dokládající předpoklady, že je schopen danou službu poskytovat. Ministerstvo informatiky může poskytovateli rozšíření zakázat, pokud nebudou předpoklady doloženy.

Další paragraf se zabývá využíváním kvalifikovaných certifikačních služeb v oblasti orgánů veřejné moci. Je zde uvedeno, že za účelem podpisu je v této oblasti možno používat jen zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb. V rámci poslední novelizace bylo přidáno ustanovení o tom, že elektronické dokumenty orgánů veřejné moci opatřené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu nebo zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb mají stejné právní účinky jako veřejné listiny. Dále je zde uvedeno, že pro komunikaci s orgány veřejné moci slouží tzv. elektronická podatelna. Více k tomuto tématu lze nalézt v dokumentech [39],[40],[41], není však předmětem této práce.

Dále se zákon zabývá obsahem kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka. Poskytovatelé vycházejí z norem a de-facto standardů zmiňovaných v kapitolách tohoto dokumentu objasňujících základní principy PKI, ale je nutné, aby byly uvedeny alespoň zcela základní údaje, které v kvalifikovaných certifikátech (resp. kvalifikovaných systémových certifikátech a kvalifikovaných časových razítcích) musí bezpodmínečně být, a naopak, že jiné osobní údaje mohou být v certifikátu uvedeny jen se souhlasem podepisující osoby. Někdy se může jednat o údaje, které jsou podle uvedených norem nepovinné. Další podmínkou je, že pokud je použití těchto produktů nějakým způsobem omezeno, musí to být zjevné spoléhající se straně – vzhledem k tomu, že z opomenutí těchto omezení plyne spoléhající se straně odpovědnost, je toto

opatření nutné. Na druhou stranu je obvyklé, že běžně dostupné aplikace mnohdy položky certifikátů zobrazují neúplně, případně nekorektně, takže pokud chce poskytovatel vložit do certifikátu nějaký „neobvyklý“ údaj, je vhodné, aby vytvořil i vlastní prohlížeč certifikátů, který bude vše zobrazovat korektně[11].

Další ustanovení se zaobírají povinností poskytovatele vyplývající z ukončení jeho činnosti. Vzhledem k dozorové činnosti Ministerstva informatiky je dále uvedeno, jaká mohou být uložena nápravná opatření.

Zajímavým paragrafem je §16, který se zabývá uznáváním kvalifikovaných certifikátů vydaných zahraničními poskytovateli certifikačních služeb. Pokud byl certifikát vydán jako kvalifikovaný v některé ze zemí EU (případně v dalších státech splňujících podmínky dané zákonem), je automaticky kvalifikovaný i na našem území [1]. Vzhledem k tomu, že hlavní oblast využití kvalifikovaných certifikátů je oblast veřejné správy, a v této oblasti je nutné, aby měl poskytovatel akreditaci v dané zemi, cíl Evropské unie – dosáhnout jednoduché vzájemné komunikace mezi jejími zeměmi s využitím kvalifikovaných certifikátů – nebyl naplněn. Touto problematikou a jejím technickým řešením se zabývá zejména kapitola tohoto dokumentu věnovaná EBGCA.

Další paragraf zákona o elektronickém podpisu se zabývá prostředky pro bezpečné vytváření a ověřování elektronických podpisů.

Prostředky pro vytváření elektronických podpisů jsou v Evropské unii omezeny velmi výrazně. Požadavky v CWA 14167-1 [17] upřesňují, že prostředky pro bezpečné vytváření elektronického podpisu musí být hodnoceny podle Common Criteria [33] na úroveň záruk EAL 4+. Například v České republice v současné době neexistuje subjekt, který by hodnocení mohl provádět. I proto jsou tyto prostředky příliš drahé a nikdo je na našem území nenabízí. Například v Německu je však situace jiná a skutečnost, že použití

[11] Příkladem problematického údaje v certifikátech je údaj s OID 1.3.6.1.5.5.7.1.3, které je zaregistrováno pro „QC Statement“, tedy prohlášení, že se jedná o kvalifikovaný certifikát – dané prohlášení není zobrazeno v běžných aplikacích, takže je pro uživatele náročné s tímto údajem pracovat.

bezpečného prostředku při vytváření elektronického podpisu (tzv. kvalifikovaný elektronický podpis) je povinné takřka při jakémkoliv úkonu, blokuje rozvíjení využívání kvalifikovaných certifikačních služeb a vzbuzuje nevoli u některých uživatelů. V České republice zatím není použití kvalifikovaného elektronického podpisu, tj. zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vytvořeného prostřednictvím prostředku pro bezpečné vytváření elektronických podpisů, vyžadováno žádným právním předpisem.

Další paragraf se zabývá prostředkem pro vytváření elektronických značek. Vzhledem k jinému režimu používání kvalifikovaných systémových certifikátů (je možné vytvářet elektronické značky automatizovaně a není nutné pokaždé kontrolovat, co je označováno) je vhodné upravit správu příslušného soukromého klíče a vytváření elektronických značek striktněji. Vyhláška se zabývá prostředky pro vytváření elektronických značek v oblasti orgánů veřejné moci. Je poskytnut návod, jak s daty pro vytváření elektronických značek nakládat a jak elektronické značky vytvářet.

Další ustanovení se zaobírají udělováním pokut a přestupky. Použité formulace jsou velmi konkrétní, aby bylo jasné, za jaké konání musí být udělena pokuta a za jaké nikoliv.

Zmocňovací ustanovení zmocňují Ministerstvo informatiky k vydání vyhlášek upravujících jak oblast elektronických podatelen (vyhláška č. 496/2004 Sb.[40] a s ní související nařízení vlády č. 495/2004 Sb.[39]), tak oblast kvalifikovaných certifikačních služeb. Vyhlášce č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb [53], která upravuje tuto oblast, bude věnována následující kapitola.

5.2 Vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb

Jak již bylo zmíněno, k předchozí verzi zákona o elektronickém podpisu byla vydána vyhláška č. 366/2001 Sb. [34]. Tato vyhláška byla tvořena v době, kdy ještě neexistovaly mnohé z dokumentů, které jsou citovány v této práci,

jako jsou ETSI standardy TS a dokumenty CEN nazývané CWA. Některé byly jen ve stavu návrhu. Proto nebylo jasné, jak upravit některé oblasti, aby byly v souladu s EU. V zájmu vyšší kompatibility s Evropskou unií byl novelizován zákon o elektronickém podpisu a ještě více se tento faktor projevil na nové vyhlášce. Kromě toho bylo u nového zákona o elektronickém podpisu odlišné zmocňovací ustanovení, takže by ani technicky nemohl vzniknout totožný prováděcí předpis.

Základními principy, které byly použity při psaní vyhlášky [53], jsou následující. Pokud danou oblast upravuje nějaký dokument[12], který úspěšně používá mnoho organizací, není důvod, proč by měl být postup v České republice jiný. Nehledě na zmiňované podmínky dané směrnicí [3], ze kterých je zřejmé, že mají být poskytovatelé posuzováni na podobné úrovni, aby byly porovnatelné jejich služby, na které se mají spoléhat i občané a instituce z ostatních států.

Velmi podstatné je určení hranice, kdy je úroveň služeb daného poskytovatele dostatečná a kdy již nikoliv, a její definování takovým způsobem, aby nebylo ani pro poskytovatele, ani pro kontrolující stranu (kontrolní orgán dle zákona o státní kontrole [37]), pochyb, kdy je chování nutno napravit pouze uložením nápravného opatření, kdy je nutné udělit pokutu a kdy již je porušení tak závažné, že je nutné odebrat akreditaci. Vždy však bude existovat určitá míra volnosti, ve které se lze pohybovat – kvalifikovaný poskytovatel certifikačních služeb (dále též poskytovatel) jistě může nabídnout i kvalitativně lepší zajištění svých služeb, než je minimum stanovené zákonem a vyhláškou,

[12] Protože je v našem právním řádu možno odkázat na dokumenty, které jsou odcitovány v úředním věstníku Evropské unie, využívá tuto možnost vyhláška – dokumentem, který je nejčastěji použit, CWA 14167-1 [17]. Ve vyhlášce lze použít již existující normu, která upravuje danou oblast, a to v případě, že tato norma byla vydána jako ČSN. To je např. ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro management bezpečnosti informací [43], ČSN EN BS 7799-2 Systém managementu bezpečnosti informací - Specifikace s návodem pro použití [44] a ČSN ISO/IEC TR 13335 Informační technologie - Směrnice pro řízení bezpečnosti IT 1-3 [45].

stejně jako se může pohybovat na hranici únosnosti a s notnou podporou právníků se snažit některým podmínkám vyhýbat. Poskytovatelem certifikačních služeb mohou být velké společnosti stejně jako společnosti malé, s naprosto odlišným způsobem řízení. Vzhledem k tomu, jak malý trh je na území České republiky, není zde ani dostatek zkušeností na to, abychom mohli určovat podmínky individuálně. Proto je v co největší míře využito norem, které vznikly za účasti zkušených odborníků na tuto problematiku ve světě, a zejména v Evropské unii.

5.2.1 Bezpečné systémy a postupy poskytovatele

V první části vyhlášky je zrekapitulováno, co vyhláška upravuje, a jsou zde zavedeny pojmy. Další část již obsahuje velmi důležitá ustanovení, která se týkají systémů a postupů poskytovatelů certifikačních služeb. V předchozí vyhlášce [34] byl zaveden pojem informační systém pro certifikační služby, protože ještě neexistovaly evropské dokumenty, které by se blíže zabývaly informačními systémy poskytovatelů certifikačních služeb. Evropské dokumenty ale přinášejí pojem „důvěryhodné systémy“, který byl touto vyhláškou přejat. Poskytovatelé tedy musí své systémy provozovat v souladu s CWA 14 167-1 [17]. Přístup k provozu a managementu poskytovatele upravuje technická specifikace TS 101 456 [46], resp. TS 102 023 [29] pro poskytovatele časových razítek. I tyto normy musí být poskytovatelem implementovány, samozřejmě v závislosti na tom, které služby poskytuje.

Další oblast omezená ve vyhlášce je oblast fyzické (nebo objektové) bezpečnosti. Vzhledem k tomu, že tato oblast je obecně upravena vyhláškou Národního bezpečnostního úřadu č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků [55], je pro vyjmenované účely (vytváření kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, prostředků pro vytváření elektronických podpisů, zneplatňování kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů a vytváření seznamů zneplatněných certifikátů) použita kategorie „Důvěrné“ podle tohoto předpisu.

Tento princip byl ponechán stejný jako v předchozí vyhlášce [34], protože jej evropské dokumenty konkrétně neupravují.

Další požadavek se týká vedení bezpečnostní dokumentace (její součásti a jejich obsah je popsán níže), která má upravovat postupy poskytovatele. Následně je vyžadováno dodržování postupů uvedených v této dokumentaci, které je spolu s dodržováním norem posuzováno při kontrole bezpečnostní shody a při provádění auditu systému managementu bezpečnosti informací (dále audit ISMS).

V předchozí vyhlášce bylo vyžadováno hodnocení informačního systému pro certifikační služby na úroveň zaručitelnosti bezpečnosti (EAL) 4 podle Common Criteria [33]. Tento přístup se však neosvědčil, protože výsledkem bylo nepřiměřené omezení poskytovatelů certifikačních služeb, vzhledem k náročnosti této normy. Hodnocení je náročné po časové i finanční stránce, neprovádí jej žádný subjekt v České republice. Ani výsledky získané z tohoto hodnocení neodpovídaly představám autorů vyhlášky [34]. Pokud jsou některé části důvěryhodných systémů poskytovatele hodnoceny podle Common Criteria na EAL 4, není u nich nutné následně provádět kontrolu bezpečnostní shody, ale kromě níže uvedených případů při zajišťování kritických činností není toto hodnocení již povinně vyžadováno vůbec. Tento postup je v souladu s evropskými dokumenty. Informační systémy poskytovatele certifikačních služeb se musí v čase vyvíjet, takže jednorázové hodnocení není ideálním řešením – vhodné je ponechat provádění pravidelných kontrol bezpečnostní shody a přidání mechanismu provádění auditů ISMS.

5.2.2 Bezpečnostní dokumentace

V nové vyhlášce je uveden výčet bezpečnostní dokumentace poskytovatele. Jak již bylo zmíněno, dokument, který slouží ke zveřejnění informací o poskytovaných službách pro podepisující osoby a spoléhající se strany, se nazývá certifikační politika. Vzhledem k tomu, že tento typ dokumentů má být přehledný a srozumitelný, patří k požadavkům vyhlášky nutnost vést pro každou službu odlišnou certifikační politiku. V případě, že

poskytovatel vydává kvalifikovaná časová razítka, je součástí jeho bezpečnostní dokumentace i dokument nazvaný politika pro vydávání časových razítek. Pokud poskytovatel vydává prostředky pro bezpečné vytváření podpisu, musí mít ve své bezpečnostní dokumentaci i dokument politika pro vydávání prostředků pro bezpečné vytváření podpisu. Protože není vhodné slučovat vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů koncovým uživatelům s vydáváním certifikátu kořenového, případně dalších certifikátů v mezistupních v hierarchii certifikačních autorit (tj. nikoliv kořenových, ale dalších certifikátů určených pro označování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů nebo kvalifikovaných časových razítek), je vhodné pro každý takový certifikát mít zvláštní politiku. Důvodem je skutečnost, že každá taková služba může mít jiné bezpečnostní nároky. Navíc je nutné, aby tento typ dokumentů byl přehledný. Politiky pro vydávání certifikátů, které slouží pouze poskytovateli, nejsou obvykle veřejné.

Certifikační a další politiky určené pro veřejnost mají spíše proklamativní charakter. Konstatují, že poskytovatel danou činnost zajišťuje, ale již neobsahují konkrétní způsob, jak toho poskytovatel dosahuje. Konkrétní naplnění se vztahuje například na samotný obsah certifikátu a způsob dokládání údajů, které v něm mají být uvedeny – protože na základě certifikační politiky má budoucí podepisující osoba vygenerovat žádost o certifikát a doložit údaje správnými dokumenty.

Další důležitý dokument, který již obsahuje konkrétní údaje o způsobu naplnění činností spojených s poskytováním certifikačních služeb, se nazývá certifikační prováděcí směrnice. Tento dokument se obvykle nezveřejňuje (je možné zveřejnit některé části, které neohrožují bezpečnost důvěryhodných systémů poskytovatele).

Struktura certifikačních politik a certifikačních prováděcích směrnic, která je uvedena v příloze nové vyhlášky, vychází z dokumentu RFC 3647 [23], a to zejména kvůli snadné porovnatelnosti jimi poskytovaných služeb.

Nově zavedeným dokumentem, který má poskytovatel vést, a který je určen ke zveřejnění, je „Zpráva pro uživatele“. Tento dokument má být výrazně stručnější než certifikační politiky a má být vytvořen zvlášť pro každou certifikační službu poskytovanou koncovým uživatelům. Slouží ke zveřejnění identifikačních údajů poskytovatele a základnímu přehledu o dané kvalifikované certifikační službě a možnostech jejího využívání.

Další dokumenty patří k základním dokumentům organizace poskytovatele jako celku. Jsou to dokumenty, které musí být prosazovány na úrovni managementu organizace – jedná se o celkovou bezpečnostní politiku a systémovou bezpečnostní politiku. Tyto dokumenty musí vycházet z analýzy rizik (stejně jako všechny postupy v důvěryhodných systémech poskytovatele certifikačních služeb).

Celková bezpečnostní politika obsahuje bezpečnostní cíle organizace a dále zásady, jaké si organizace poskytovatele stanoví, aby tak cíle mohla naplnit. Velmi důležité je vymezení odpovědností v tomto dokumentu.

Systémová bezpečnostní politika pak rozpracovává naplnění cílů stanovených bezpečnostní politikou v oblasti správy a ochrany informačních technologií a aktiv informačních systémů. Stanovuje způsob řešení bezpečnosti, určuje pravomoci a odpovědnosti při provozování důvěryhodných systémů. Protože se jedná o poskytovatele certifikačních služeb, je důležité, aby v systémové bezpečnostní politice byly popsány vazby mezi důvěryhodnými systémy, vazby uvnitř těchto systémů a vnější vazby z důvěryhodných systémů poskytovatele.

Celková bezpečnostní politika a systémová bezpečnostní politika mají být zpracovány v souladu s normami [43] a [45]. Důvodem, proč se ve vyhlášce objevují požadavky na postup v souladu s normami, je stanovení jasných pravidel, na základě kterých je možné si vytvořit představu o podmínkách, které je nutné splnit jako kvalifikovaný či akreditovaný poskytovatel certifikačních služeb. Vzhledem k tomu, že tyto normy již prošly svým vývojem a jsou v praxi často využívány, bylo jejich využití smysluplnější než vytváření vlastních pravidel.

Další dokumenty, které poskytovatel musí mít, a jejichž obsahem se musí řídit, jsou plán pro zvládání krizových situací, plán obnovy a případně další dokumenty, na které poskytovatel odkazuje ze svojí dokumentace a kterými dokládá splnění požadavků zákona [1] – tedy jak zajišťuje bezpečnost svých systémů.

Plán pro zvládání krizových situací musí popsat postupy, které budou provedeny v případě, že dojde k výskytu mimořádné události. Mimořádnou událostí je míněna situace, kdy dojde k ohrožení poskytování certifikačních služeb, zejména v souvislosti se selháním informačního systému nebo technického vybavení.

Plán obnovy má sloužit k rozpracování zásad, které vedou k co nejrychlejší obnově fungování důvěryhodných systémů. Zejména je důležité co nejrychleji uvést systém do stavu, kdy bude provádět kritické činnosti, jako je zneplatňování certifikátů.

5.2.3 Kontrola bezpečnostní shody a audit ISMS

Akreditovaný poskytovatel certifikačních služeb má v rukou systém, jehož narušení může způsobit závažné následky. V podstatě se na něj spoléhá celý náš „stát“, který důvěřuje, že informace v certifikátech byly správně ověřeny a že podepisující osoba je tou, za kterou se vydává. Proto má poskytovatel povinnost provádět kontroly a audity, jejichž výsledky předkládá Ministerstvu informatiky, a na jejichž základě je možné se přesvědčit, zdali poskytovatel dostává svých závazků. Je i v zájmu poskytovatele ověřovat si, zda je jeho činnost taková, jako si představuje. Zvláště u velkých organizací, kde management nemá možnost věnovat se jednotlivým detailům poskytování služeb, jsou tyto audity velmi podstatnou zpětnou vazbou.

Protože v dnešní době je v EU v oblasti informační bezpečnosti velmi populární dvoudílná norma BS 7799 [43], [44] (resp. normy z ní vycházející, BS 7799-1 nahradila ISO 17799 a BS 7799-2 nyní nahradila ISO 27001 [54]), je její model přijat i u nás. Tato norma ve svém prvním dílu (nyní ISO 17799, které má být nahrazeno ISO 27002) obsahuje postupy pro management bezpečnosti

informací a ve svém druhém dílu (nyní ISO 27001) specifikuje systém managementu bezpečnosti informací (Information Security Management System, ISMS). Poskytovatelé certifikačních služeb musí mít zavedený ISMS, což v zásadě znamená, že si jejich vedení uvědomuje význam ochrany svých aktiv a náležitě ji prosazuje. Musí mít tedy dobře definované procesy, které v organizaci probíhají, musí mít zaveden efektivní způsob provádění změn. Bezpečnost musí být prosazována na úrovni nejvyššího vedení, všechny incidenty musí být oznámeny příslušným odpovědným osobám, není přípustné problémy „tutlat".

Zavedení ISMS je možné doložit platným certifikátem na shodu s ČSN BS 7799-2, resp. ČSN ISO/IEC 27001[13], a pak není třeba provádět audit ISMS ve smyslu nové vyhlášky. Pokud poskytovatel takový certifikát nemá, musí si od nezávislého auditora nechat provést audit ISMS (tedy audit posuzující, že je zaveden ISMS podle normy ČSN BS 7799-2 [44], resp. ČSN ISO/IEC 27001 [54]), který bude auditor provádět v souladu s normou ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu[14].

Certifikace na shodu s ČSN BS 7799-2 je nákladnější než samotné provedení auditu, proto byl zvolen tento přístup – zatím jsou příjmy z poskytování certifikačních služeb velmi nízké, takže by podmínka certifikace byla příliš zatěžující. V nové vyhlášce je dále uvedeno, jaké náležitosti má mít zpráva o auditu ISMS, aby bylo pro všechny zúčastněné strany zřetelné, co se od nich očekává. Součástí zprávy o auditu je i prohlášení o výsledku auditu, které má poskytovatel povinnost zveřejnit ve zprávě pro uživatele. Audit ISMS

[13] V době, kdy byla vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb vydána, byla platná norma ČSN BS 7799-2, která byla v listopadu 2006 nahrazena normou ČSN ISO/IEC 27001.

[14] Ačkoliv tato norma není formulována přímo pro audit systému řízení bezpečnosti informací, její obsah je dostatečně obecný, aby bylo možné podle ní postupovat při jakémkoliv auditu podle procesních norem. V řadě ISO/IEC 27000 by však mělo pod číslem 27007 vyjít doporučení pro audit ISMS, které bude pravděpodobně vycházet i z normy ISO 19011.

je podle nové vyhlášky nutné provádět opakovaně, nejméně jednou za dva roky, a je nutné jej provést před zahájením poskytování kvalifikovaných certifikačních služeb.

Jeden z požadavků, jejichž plnění auditor musí v rámci auditu ISMS ověřit, je plnění povinností stanovených legislativou. Jednou z těchto povinností je i pravidelné provádění kontroly bezpečnostní shody – poskytovatel proto předkládá auditorovi i výsledky provedení kontroly bezpečnostní shody (pokud již kvalifikovanou certifikační službu poskytuje). Kontrolu bezpečnostní shody může pro poskytovatele provést i jeho zaměstnanec, může se tedy jednat o interní kontrolu.

Kontrola bezpečnostní shody je posouzením, zda poskytovatel provozuje důvěryhodné systémy v souladu s požadavky zákona a vyhlášky. Tím je míněno, že pokud má poskytovatel povinnost postupovat podle své bezpečnostní dokumentace nebo se v určité oblasti řídit určitou normou, musí ověřit při kontrole bezpečnostní shody, jestli postupuje v souladu se všemi zmíněnými dokumenty. Vyhláška je koncipována tak, že pokud je daná oblast upravena mezinárodní nebo evropskou normou, uvádí se pouze odkaz a jen pokud daná oblast není upravena, je úprava uvedena přímo ve vyhlášce. Proto je při provádění kontroly bezpečnostní shody nutné posoudit shodu postupů poskytovatele ve všech oblastech s dostatečnou podrobností, tedy včetně kontroly plnění požadavků norem, na které je odkázáno.

Vzhledem k předchozím zkušenostem z provádění dozoru ze strany Ministerstva informatiky je zvlášť stanoveno, že je nutné ověřit i shodu provádění změnového řízení s popisem postupu změnového řízení v bezpečnostní dokumentaci. Zkušenost je taková, že poskytovatelé mají tendenci při - z jejich pohledu - „malých změnách“ změnit údaj v některém dokumentu, což často vede k nekonzistentnosti dokumentace, která se stává pro osoby, které nemají historické informace, protože jsou například nově přijati,

nesrozumitelnou[15]. Dále je nutné posoudit rizika, která taková změna může přinést, zhodnotit efektivitu opatření, a teprve v případě, že je opatření schváleno odpovědnými osobami v organizaci, je možné ji realizovat a promítnout do související dokumentace.

Kontrola bezpečnostní shody se provádí podle normy TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3 [45]. Tento postup je osvědčený již z dob předchozí vyhlášky [34]. Norma TR 13335 [45] je obecně platná pro oblast informační bezpečnosti. Protože byly vypracovány dokumenty „conformity assessment guidance“ [47], které mají sloužit jako návod pro vyhodnocování shody s některými z uvedených norem, jako například CWA 14167-1 [17], TS 101 456 [46], TS 102 023 [29], je doporučeno tyto postupy použít při provádění kontroly bezpečnostní shody. Poskytovatel však musí vždy své kroky při provádění kontroly bezpečnostní shody popsat, aby nebylo pochyb o správnosti jeho postupu. Lze též doporučit, aby se postup při provádění jednotlivých kontrol bezpečnostní shody příliš nelišil, aby výstupy z provedení těchto kontrol byly porovnatelné a mohlo dojít k měřitelnému zlepšování. Z toho důvodu je také vhodné, aby byl audit spíše zaměřen na zjištění a podchycení reálné situace než na konstatování „splněno bez výhrad“ u všech kritérií.

Při provedení kontroly bezpečnostní shody je třeba vypracovat zprávu, ve které musí být kromě jiného uveden výsledek provedení kontroly bezpečnostní shody. Kontrola se provádí pravidelně nejpozději po 12 měsících, přičemž je možné ji provádět pouze ve vztahu k provedeným změnám. Celý systém musí být posuzován alespoň jednou za 4 roky. Zpráva o kontrole bezpečnostní shody se předkládá Ministerstvu informatiky, protože to je základní informace, na jejímž základě je možné si vytvořit představu o důvěryhodnosti činností a služeb poskytovatele.

[15] Příkladem „malé změny“ může být změna ve fakturačním systému. Může vypadat jako nesouvisející s důvěryhodnými systémy, a tudíž může vyvolat představu, že nemusí být dále posuzována. Taková změna se však promítne i do činnosti registračních autorit, což může mít vliv na dokumentaci poskytovatele.

5.2.4 Bezpečný kryptografický modul

Poskytovatel musí pro vytvoření, uložení a veškerou manipulaci se svým soukromým klíčem, který slouží pro označování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a seznamů zneplatněných certifikátů nebo pro vytvoření, uložení a veškerou manipulaci se soukromým klíčem, který slouží pro označování vydaných kvalifikovaných časových razítek, použít bezpečný kryptografický modul. Poskytovatel musí mít jiný soukromý klíč pro označování kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů, než pro označování kvalifikovaných časových razítek. Při vydávání časových razítek je jiný režim než při vydávání certifikátů, takže je nutné tyto činnosti oddělit i v té nejcitlivější oblasti, tj. samotnými klíči. Toto omezení je dáno i mezinárodními normami upravujícími tuto oblast [17].

Kryptografický modul je zařízení, které musí splňovat přísné bezpečnostní požadavky. V souladu s CWA 14167-1 [17] se v České republice uznávají moduly, které jsou certifikovány podle profilu ochrany definovaného v CWA 14167-2 [48] nebo CWA 14167-4 [49]. Rozdíl mezi profily ochrany popsanými v těchto dokumentech spočívá pouze v tom, že [48] popisuje ochranu modulu, který zabezpečuje i funkci zálohování klíčů a dat s nastavením modulu, kterou dle [17] kryptografický modul může umožňovat. Profil ochrany popsaný v [49] bude použit pro hodnocení kryptografického modulu, který zálohu klíčů a zmíněných dat neumožňuje.

Tento profil ochrany odpovídá EAL 4 podle Common Criteria [33], ale na některé hodnocené charakteristiky jsou kladeny vyšší nároky. Díky tomu nelze uznat certifikát (v tomto případě se nejedná o certifikát veřejného klíče, ale o certifikát dokládající splnění požadavků určité normy), který je vystaven pouze na EAL 4, což v praxi znamená, že správný certifikát podle [48], [49] lze získat jedině v některé z evropských zemí (v současnosti zejména Německo, případně Itálie). Vzhledem k tomu, jak malý trh s těmito moduly v Evropě, i přes zdejší „hrdost“ jsou moduly nejčastěji hodnoceny americkým NIST a mají certifikát na FIPS 140-1 nebo 2 [50] na úroveň 3 nebo vyšší. Tento způsob již není v [17] explicitně uveden, přestože v minulých verzích tohoto dokumentu

uveden býval. Protože je v [17] ponechána věta, že „modul musí být hodnocen podle [48], [49], nebo podle jiné použitelné specifikace na srovnatelné úrovni hodnocení“, je i v České republice tento postup (tedy s certifikátem FIPS 140-1 nebo 2 úroveň 3 [50] a doložením dokumentů prokazujících, že modul splňuje všechny požadavky CWA 14 167-1 [17]) považován za dostačující.

V České republice se takové moduly (zejména kvůli velikosti trhu v této oblasti) nevyrábějí, není zde ani žádná specializovaná laboratoř, která by taková zařízení testovala. Případné další testování zařízení by značně zvyšovalo finanční náročnost a bylo by v podstatě nadbytečné. Proto dochází jen k formálnímu posouzení, zda je dokumentace k zařízení v pořádku, zda kryptografický modul podporuje některá z kryptografických schémat, která budou uvedena na úřední desce Ministerstva informatiky[16]. Bude posouzeno, zda nástroj lze do provozu nasadit tak, jak to vyžadují normy upravující oblast kryptografických modulů. Pokud modul splňuje stanovené požadavky, bude uveden na seznamu vyhodnocených nástrojů.

Protože se zde spoléháme na hodnocení jiného subjektu, a tento subjekt může z určitých důvodů certifikát odvolat, dochází k problému, co s takovou událostí. Pokud by poskytovatel dále nemohl nástroj používat, musel by mít v rezervě další modul, který by v takovém případě mohl okamžitě začít používat. Přechod na nový modul však trvá nejméně jeden rok, tj. dobu platnosti certifikátů označených soukromým klíčem uloženým v původním kryptografickém modulu. Jinak by musely být všechny tyto certifikáty zneplatněny. Proto je ve vyhlášce uvedeno, že poskytovatel může na svou odpovědnost modul používat, i když je ze seznamu vyškrtnut, ale musí uplatnit všechna opatření, aby byla bezpečnost takového modulu dostatečná (stanovení těchto opatření vyplývá z analýzy rizik), musí být schopen uplatnění těchto opatření a korektní fungování kryptografického modulu prokázat a musí kontrolovat provádění těchto opatření.

[16] Kryptografická schémata a algoritmy jsou na úřední desce zveřejněny na základě dokumentů ALGO-paper [35] a na základě doporučení odborníků na tuto oblast v naší zemi.

Kryptografický modul je umístěn a používán v prostorech, které jsou zabezpečeny jako objekty kategorie „Důvěrné“ podle vyhlášky Národního bezpečnostního úřadu č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků [55]. Samozřejmě musí být modul nasazen a používán v souladu s technickou dokumentací.

Podle předchozí vyhlášky [34] si hodnocení nástroje objednal některý ze zástupců výrobce v České republice, dostal příslušné rozhodnutí, ale jiný výrobce se mohl pouze odkázat na informaci zveřejněnou ve věstníku ministerstva nebo na jeho webových stránkách – proto je nově zavedeno poskytování výpisů ze seznamu vyhodnocených nástrojů pro všechny zájemce.

Poskytovatelé nemusí použít nástroj, který je hodnocen Ministerstvem informatiky, stačí, pokud mají příslušný certifikát – tedy certifikát dokladující soulad s CWA 14167-2 [48] nebo CWA 14167-4 [49]. Vzhledem ke zkušenostem s tím, že i banky, jejichž certifikační autority působí mimo rámec zákona o elektronickém podpisu [1], [2], považují za konkurenční výhodu vyhodnocení kryptografického modulu ministerstvem, lze očekávat, že zájem o hodnocení nástrojů bude trvat.

5.2.5 Další obecné požadavky na poskytovatele

Vzhledem k zákonnému zmocnění obsahuje vyhláška několik odstavců, které obsahují spíše samozřejmé požadavky, které zde budou jen velmi stručně shrnuty.

Poskytovatel má povinnost v dokumentech, které jsou zveřejněny, uvést identifikační údaje o sobě, o tom, že je akreditován, podmínky pro využívání kvalifikovaných certifikačních služeb a další informace o svých službách. Nadřízené kvalifikované systémové certifikáty poskytovatele musí být zveřejněny nejméně dvěma na sobě nezávislými způsoby.

Dále je popsáno, co musí poskytovatel učinit v případě odejmutí akreditace, například se jedná o zveřejnění této informace v celostátně distribuovaném deníku a oznámení této informace všem osobám, které mají platné certifikáty.

Vyhláška dále požaduje, aby poskytovatel stanovil, jak zajistí dostatečnou kvalifikaci pracovníků, kteří budou vykonávat role při provádění činností spojených s poskytováním kvalifikovaných certifikačních služeb. Samozřejmě je zde i požadavek na obeznámení pracovníků s bezpečnostní dokumentací v rozsahu odpovídajícím svěřené činnosti.

Důležité ustanovení obsahuje paragraf zabývající se uchováváním informací a dokumentace poskytovatele. Poskytovatel musí uchovávat seznamy zneplatněných certifikátů, záznamy o událostech spojených s poskytováním kvalifikovaných certifikačních služeb a bezpečnostní dokumentaci se zachováním prokazatelnosti původu, dostupnosti, integrity, časové autentičnosti a důvěrnosti. Způsob, jak bude tyto informace a dokumentaci uchovávat tak, aby vyhověl požadavkům vyhlášky, stanoví ve své bezpečnostní dokumentaci. Poskytovatel uchovává tyto informace a dokumentaci po dobu 10 let.

Další oblastí, kterou nová vyhláška upravuje, je oblast opatření proti zneužití a padělání certifikátů. Poskytovatel má především povinnost chránit svá data pro označování (tedy soukromý klíč) vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a seznamů zneplatněných certifikátů. Tato data smí být použita jen pro zmíněné účely. Pro označování, uchovávání a manipulaci se soukromým klíčem poskytovatele se používá bezpečný kryptografický modul popsaný výše.

Dále je upraveno, jaké činnosti musí poskytovatel minimálně provést v případě, že zjistil, že došlo ke zneužití jeho soukromého klíče, nebo má podezření, že by ke zneužití mohlo dojít. Ve vyhlášce [53] je uvedeno, že má poskytovatel zneplatnit všechny certifikáty v certifikační cestě, které jsou podřízené certifikátu, jehož veřejný klíč odpovídá zkompromitovanému soukromému klíči.

Poskytovatel dále uvede ve své bezpečnostní dokumentaci, jakým způsobem zajišťuje ochranu seznamů vydaných certifikátů a seznamů zneplatněných certifikátů.

Další úprava se vztahuje ke způsobu určení data a času, který je obsažen ve vydaných certifikátech jako údaj o počátku a konci jejich platnosti,

dále v seznamu zneplatněných certifikátů, kde je údajem o době zneplatnění daného certifikátu a o době vydání daného seznamu zneplatněných certifikátů.

Vyhláška dále obsahuje ustanovení o ochraně dat (soukromých klíčů) vytvářených pro uživatele. Poskytovatel má povinnost postupovat v souladu s CWA 14 167-1 [17] a své postupy popíše v dokumentaci. Poskytovatel má přímo ze zákona povinnost zajistit, aby se soukromé klíče uživatelů nemohly dostat do nepovolaných rukou. Skutečnost je však taková, že je problematické s dostatečnou jistotou zaručit, že se k soukromým klíčům uživatelů nikdo kromě uživatelů samotných nedostane, takže tento typ služeb žádný poskytovatel nenabízí a je málo pravděpodobné, že by je nabízel. Z pohledu uživatele se takový způsob získání dat, která musí držet pod svou výhradní kontrolou, nemůže jevit jako vhodný. V současnosti se stále najde mnoho odpůrců používání elektronického podpisu právě z toho důvodu, že nemohou mít pod výhradní kontrolou zařízení a aplikaci vytvářející soukromý klíč nebo elektronický podpis – proto se odmítají na něj spoléhat. Svěřit přímo vytváření soukromého klíče poskytovateli je pak dalším krokem k pocitu, že můžeme být snadno sledováni a naše identita zneužita. Přesto je tato možnost ponechána v evropských normách, a proto musí být umožněno tento typ služby poskytovat – budoucnost ukáže, jestli budou jednou lidé ochotni vytvoření takto citlivých dat svěřit jinému subjektu.

Vyhláška dále upravuje, jak musí poskytovatel postupovat při zneplatňování certifikátů – musí v certifikačních politikách stanovit, jakým způsobem bude možné požádat o zneplatnění certifikátu, musí zajistit nepřetržitý příjem žádostí o zneplatnění certifikátů a musí postupovat i v této oblasti v souladu s CWA 14 167-1 [17].

5.2.6 Kvalifikovaná časová razítka

Narozdíl od kvalifikovaných systémových certifikátů, u nichž jsou obdobné požadavky jako na kvalifikované certifikáty, je problematika kvalifikovaných časových razítek řešena ve vyhlášce [53] zvlášť.

Jak již bylo uvedeno v kapitole o kryptografických modulech, kvalifikovaná časová razítka mohou být označována jen soukromým klíčem, který slouží výhradně pro tento účel. Podmínky pro nakládání s tímto klíčem dané vyhláškou jsou ale obdobné jako pro klíč využívaný pro označování kvalifikovaných a kvalifikovaných systémových certifikátů. Proto musí poskytovatel, který již vydává kvalifikované certifikáty, použít pro vydávání kvalifikovaných časových razítek další kryptografický modul.

Poskytovatel zajišťuje, aby data, která jsou obsažena v kvalifikovaném časovém razítku, odpovídala datům v žádosti o kvalifikované časové razítko. Dále zajistí, aby byl správně synchronizován čas a aby bylo vydávání kvalifikovaných časových razítek korektní. Postup, jak budou zajišťovat splnění těchto požadavků, je blíže upraven v dokumentech [17] a [29].

Další požadavek na poskytovatele se týká toho nejdůležitějšího, co v časovém razítku je uvedeno, a to je časový údaj. Poskytovatel musí mít své vlastní měřidlo času, které musí odpovídat požadavkům naší legislativy, zejména zákonu č. 505/1990 Sb., o metrologii. Měřidlo času musí být kalibrováno právě podle tohoto zákona, jinak nemůže být zdrojem přesného času v prostředí České republiky. Měřidlo se nesmí použít v případě, že dojde ke změně jeho metrologických vlastností. Měřidlo času musí pracovat s nejistotou časové informace menší než 1 sekunda a poskytovatel uvede tento údaj v politice pro vydávání časových razítek.

Splnění uvedeného požadavku se v praxi ukázalo jako velmi problematické, protože v současnosti neexistuje způsob, jak kalibraci provést, když je časový údaj získáván z „black-boxu“ modulu pro vydávání časových razítek, který je vysoce zabezpečený a u něhož je problematické se dostat k tak nízké úrovni reprezentace času, že není pochyb o tom, že je zdroj času skutečně přesný. Nakonec se Ústavu fotoniky a elektroniky podařilo provést takové měření, na jehož základě bylo možné potvrdit, že nejistota časové informace daného zdroje času je nižší než 1 sekunda – kalibrace v pravém slova smyslu však zatím provedena nebyla.

Pokud poskytovatel zjistí, že došlo k výskytu události, která má vliv na bezpečnost vydání kvalifikovaného časového razítka nebo na přesnost časové informace, musí ihned přerušit vydávání časových razítek, dokud neobnoví řádný stav v souladu s postupy stanovenými v plánu zvládání krizových situací a v plánu obnovy. Informaci o této události dále zveřejní na svých webových stránkách, informuje o ní dotčené subjekty a Ministerstvo informatiky. Pokud má tato situace vliv na již vydaná kvalifikovaná časová razítka, informaci zveřejní i v celostátně distribuovaném deníku, a to tak, aby bylo možné zjistit, na která časová razítka se nelze spoléhat.

Měřidlo času musí být stejně jako kryptografický modul umístěno v prostorech kategorie „Důvěrné“ podle vyhlášky Národního bezpečnostního úřadu č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků [55].

5.2.7 Prostředky pro bezpečné vytváření elektronických podpisů

O bezpečných kryptografických prostředcích již bylo obecně pojednáno výše, nyní tedy konkrétněji k prostředkům pro bezpečné vytváření elektronických podpisů (dále „SSCD“ – secure signature-creation device). Požadavky na prostředky pro bezpečné vytváření elektronických podpisů, které je nutné využít při vytváření kvalifikovaného elektronického podpisu dle směrnice [3][17], jsou obecně popsány v [17]. Tento dokument stanoví, jakým způsobem má být prostředek inicializován a jak má být připraven k předání uživateli. Dodržení těchto postupů je vyžadováno novou vyhláškou. Požadavky jsou konkretizovány v dokumentu CWA [51], který obsahuje profily ochrany vytvořené v souladu s Common Criteria [33] na úroveň zaručitelnosti bezpečnosti EAL 4+.

[17] Soukromý klíč však může být uložen i na „obyčejné“ aktivní čipové kartě, která nesplňuje tak náročné požadavky, ale i přesto může zaručit vyšší úroveň bezpečnosti než pevný disk počítače. Pak se však nejedná o bezpečný prostředek pro vytváření elektronického podpisu ve smyslu směrnice [3] nebo zákona o elektronickém podpisu [1].

Uvedená norma CWA [51] rozlišuje tři typy SSCD. První typ SSCD je určený jen pro vytváření dat pro vytváření elektronických podpisů a dat pro ověřování elektronických podpisů (tedy vytváření soukromého a veřejného klíče). Druhý typ SSCD dle [51] je prostředek určený výhradně pro vytváření elektronických podpisů a uložení dat pro vytváření elektronických podpisů; tato data je možné získat důvěryhodným kanálem z prostředku prvního typu. Třetí typ SSCD je kombinací typu prvního a druhého, je možné jej využít jak pro vytváření dat pro vytváření a ověřování podpisu, tak pro samotné vytváření podpisu daty pro vytváření podpisu vytvořenými uvnitř prostředku (tedy vytváření soukromého a veřejného klíče a vytváření podpisu s využitím soukromého klíče). Rozdíl mezi těmito typy SSCD je zachycen na následujících schématech [51].

Vysvětlení pojmů ze schémat:

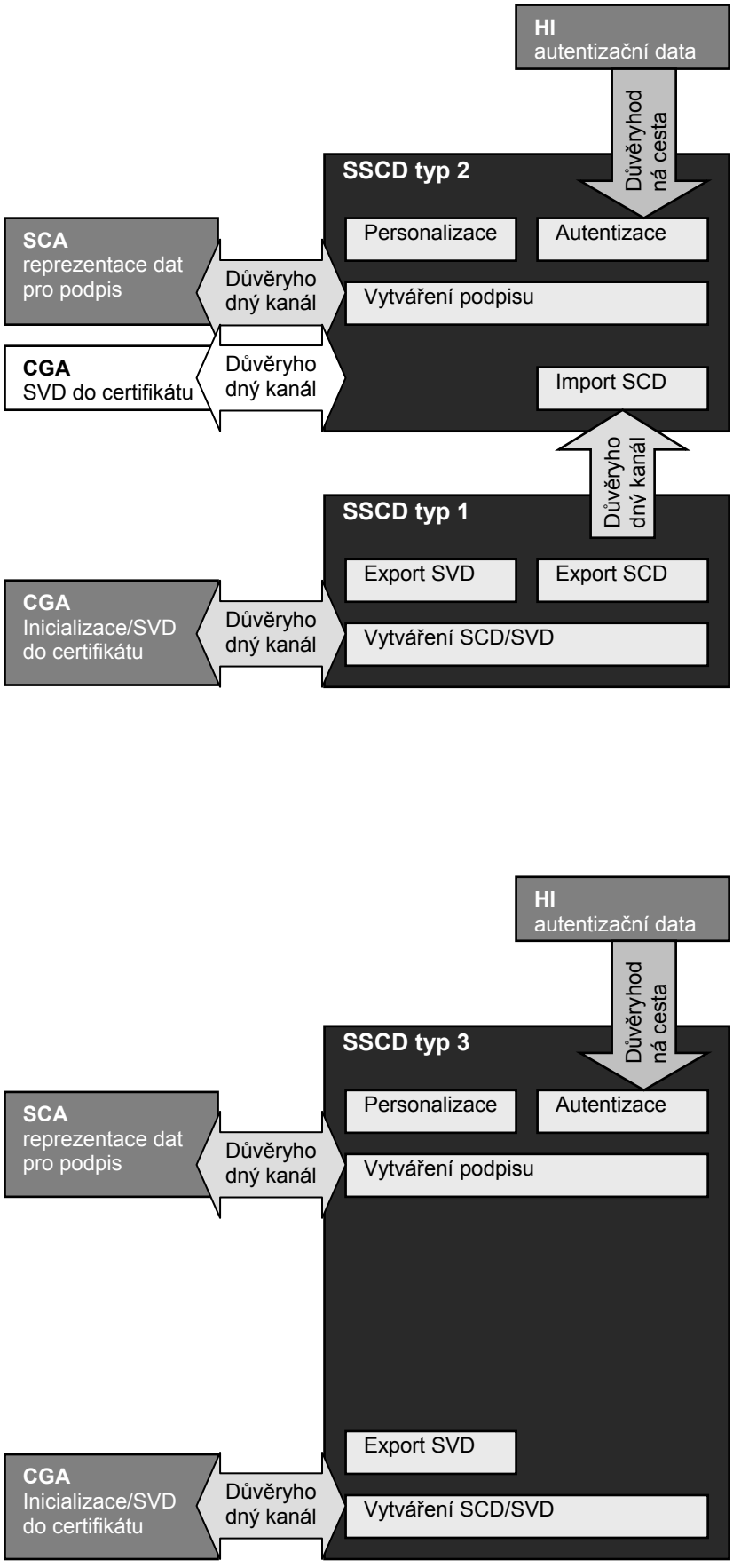
SCD – signature creation data, data pro vytváření podpisu, soukromý klíč. Nesmí opustit SSCD.

SVD – signature verification data, data pro ověřování podpisu, veřejný klíč.

CGA – certification generation application, aplikace pro vytváření certifikátu, certifikát může být vytvořen ve všech typech SSCD. Veřejný klíč se musí dostat do této aplikace důvěryhodným kanálem. Pokud je CGA v SSCD prvního nebo třetího typu, slouží i pro inicializaci vytváření SCD/SVD.

SCA – signature creation application, aplikace pro vytváření podpisu. Přes tuto aplikaci se do SSCD dostane důvěryhodným kanálem jednoznačná reprezentace dat určených k podpisu (např. hash nebo samotná data). Po provedení operace se podpis zašle důvěryhodným kanálem do aplikace.

HI – human interface, rozhraní pro komunikaci s člověkem – pokud není součástí SSCD, musí být zprostředkováno zaslání autentizačních dat důvěryhodnou cestou. V některých případech je vyžadováno, aby při hodnocení SSCD byla hodnocena úroveň bezpečnosti SSCD i včetně tohoto rozhraní a aplikace použité při komunikaci uživatele s SSCD.



Obrázek 12 – Schémata jednotlivých typů SSCD

U SSCD, stejně jako u kryptografických modulů, může dojít k tomu, že certifikát potvrzující hodnocení daného typu SSCD může být stažen. Například protože produkt již není dostatečně podporován výrobcem. Proto má Ministerstvo informatiky možnost SSCD vyškrtnout ze seznamu vyhodnocených prostředků. Vzhledem k tomu, že tento typ karet má omezenou platnost, např. na 3 roky, a certifikáty, které jsou na ně uloženy, mívají platnost 1 rok, a ani cena není tak vysoká, jako je tomu u kryptografických modulů, nebude možné SSCD, které není na seznamu, používat.

5.2.8 Ochrana dat pro vytváření elektronických značek

Nová vyhláška se kromě poskytovatelů certifikačních služeb zabývá i ochranou soukromých klíčů pro vytváření elektronických značek, které používají orgány veřejné moci. Vzhledem k tomu, že na elektronické značky jsou stanoveny mírnější podmínky a funguje u nich odpovědnost právnické osoby, která je vždy problematičtější než odpovědnost osoby fyzické (hlavně z hlediska „uvědomění si“ této odpovědnosti), je vhodné na tuto problematiku ve vyhlášce upozornit, aby bylo jasné, že se s takovými prostředky má zacházet velmi obezřetně. Proto je povinné, aby byly zmíněné soukromé klíče uloženy a používány na externím médiu, jako je čipová karta, kryptografický token nebo kryptografický modul. Protože nakládání se soukromými klíči orgánů veřejné moci není tématem této práce, dále zde nebude probíráno.

Akreditovaní poskytovatelé certifikačních služeb mají jeden rok na to, aby se přizpůsobili podmínkám nové vyhlášky – tato doba je dostačující vzhledem ke skutečnosti, že již došlo ke změně zákona, který zavádí všechny povinnosti, jejichž provedení je v nové vyhlášce konkretizováno. Samozřejmě způsobů naplnění podmínek daných zákonem bylo často více – ale podpora evropských norem byla deklarována dopředu, takže podmínky upřesněné novou vyhláškou, které poskytovatelé mohli jen obtížně předvídat, se týkají spíše oblastí, které nejsou evropskými dokumenty jednoznačně upraveny a jejich naplnění by nemělo být příliš náročné.

5.3 Management poskytovatele certifikačních služeb

Nová vyhláška odkazuje v celé řadě oblastí na evropské a mezinárodní normy. Bylo by tedy vhodné více odkrýt, co je v těchto normách uvedeno, a to zejména v těch, které se zabývají organizací, řízením činností poskytovatele, zejména řízením bezpečnosti aktiv, a vysvětlit, co uvedené požadavky pro činnost poskytovatele skutečně znamenají (tedy jakým způsobem je mohou implementovat). Autorka vytvořila metodiku, která poskytovateli ukazuje, jakým způsobem má postupovat při implementaci obecných norem pro oblast řízení bezpečnosti informací ve svém prostředí.

5.3.1 Aplikace BS 7799

Za základní normu upravující oblast řízení bezpečnosti informací lze považovat dokument BS 7799 [43], [44], resp. [54]. Tato norma má dvě části. První část [43] je „best practice“a obsahuje doporučení pro řízení bezpečnosti informací. Druhá část [44], resp. [54] je formulována jako požadavky na systém řízení bezpečnosti informací – nejedná se tedy o „měkká“ doporučení, ale o „tvrdé“ požadavky. První část spíše vysvětluje, jak naplnit požadavky druhé části. V případě provádění auditu je nutné splnit všechny požadavky druhé části. Tato norma má význam zejména pro vytvoření uceleného systému, který by i díky zpětnovazebním mechanismům měl zaručit, že budou zvládána rizika ohrožující řízení bezpečnosti informací v organizaci.

5.3.2 Aplikace první části BS 7799, resp. ISO/IEC 17799, u poskytovatelů certifikačních služeb

První věcná kapitola první části [43] se zabývá jednou z nejpodstatnějších součástí řízení bezpečnosti – hodnocením rizik. Z hlediska poskytovatele certifikačních služeb je velmi důležité precizně provést tuto analýzu, vzhledem ke škodám, které mohou vzniknout v případě podcenění některých rizik. U poskytovatele navíc kromě obvyklých problémů může v případě některých událostí dojít k udělení pokuty Ministerstvem informatiky –

pokud dojde k porušení zákona o elektronickém podpisu. Poskytovatel certifikačních služeb má podle vyhlášky [53] tuto analýzu provést v souladu s normou TR 13335 [45], resp. její třetí částí, která podrobně vysvětluje možné přístupy k provádění analýzy rizik. Pro provedení analýzy rizik poskytovatelé certifikačních služeb obvykle používají některou z dostupných metod – nejčastěji je využívána metoda CRAMM.

Na základě provedení analýzy rizik je nutné, aby si poskytovatel certifikačních služeb určil, jak bude s jednotlivými riziky pracovat – některá lze akceptovat (např. nebude se uplatňovat protiopatření vzhledem k malé pravděpodobnosti, že může riziko nastat, nebo jsou náklady na protiopatření neúměrně vysoké). Na ostatní rizika je nutné vybrat vhodná protiopatření, případně přestat vykonávat činnost, která riziko způsobuje, či přenést riziko na jiný subjekt (např. pojišťovnu[18] nebo dodavatele).

Další, velmi podstatnou kapitolou, je „bezpečnostní politika“, kde je zvláště upozorněno na to, že tento dokument (resp. bezpečnost informací) má být podporován ze strany vedení a jeho obsah má být dostupný všem zaměstnancům organizace, a to ve formě, která je jim přístupná a srozumitelná. Poskytovatel certifikačních služeb musí vytvořit bezpečnostní politiku nejen v souladu s touto normou, ale i s požadavky vyhlášky [53]. Požadavky vyhlášky však vycházejí přímo z norem, takže není obtížné je implementovat zároveň. Kromě vytváření samotného obsahu bezpečnostní politiky je podstatný i postup při revizích a vyhodnocování efektivity bezpečnostní politiky.

Další kapitola se zabývá organizací bezpečnosti, tedy samotným řízením bezpečnosti informací v organizaci. Jsou zde doporučení jak vybudovat a udržovat infrastrukturu bezpečnosti informací, dále jak zajistit bezpečnost při přístupu třetích stran a jak přistupovat k outsourcingu. Z hlediska poskytovatelů certifikačních služeb je kromě vlastního vnitřního uspořádání, které má zajistit

[18] Ze zkušenosti vyplývá, že pojišťovny nemají mnoho informací, podle kterých by mohly určit pravděpodobnost, že dojde k pojistné události – proto jsou podmínky pojištění v oblasti poskytování certifikačních služeb relativně nevýhodné.

bezpečnost, podstatná i oblast externí bezpečnosti. Některé činnosti totiž nechávají zajistit smluvními stranami (což předpokládají i normy, které se poskytováním certifikačních služeb zabývají). V případě, že poskytovatel certifikačních služeb svěří třetí straně některou z činností, při kterých může dojít k velkým škodám, nemůže se tím zbavit své odpovědnosti – proto je nutné, aby měl velmi kvalitně zpracované smlouvy, kterými zajistí, aby byly služby třetí strany bezpečné a aby tato strana nemohla zneužít informace, k nimž se při své činnosti dostane.

Další kapitola se zabývá řízením aktiv a klasifikací informací – tedy tím, že si poskytovatel má identifikovat svá aktiva, jejich hodnotu a důležitost pro organizaci. Podle těchto informací poskytovatel určí opatření, díky kterým budou daná aktiva přiměřeně chráněna, a uvede je ve svých interních směrnicích.

Je důležité, aby bylo popsáno, jakým způsobem se s aktivy nakládá a jak jsou označována. Pokud je například určité aktivum poskytovatele certifikačních služeb považováno za důvěrné, je nutné, aby bylo v interních směrnicích popsáno, jak bude toto aktivum označeno (například uvedením písmena „D“ na titulní straně tištěného dokumentu, uvedením písmena „D“ na CD-ROM), jaké jsou další náležitosti aktiva (např. číslování stran, verzování) a pak také jak s daným typem aktiva lze nakládat (a kdo s daným typem aktiva může nakládat).

Aktiva nejsou jen informace, ale i aplikace, technické vybavení, lidé. Zacházení a odpovědnost ve vztahu ke každému typu aktiva a způsobu jeho využívání je nutné v dokumentaci vymezit. Rozhodnutí o tom, jaká aktiva mají důležitost pro poskytovatele, záleží na konkrétní situaci. Poskytovatel musí dbát na ochranu osobních údajů, které získává od žadatelů o certifikát, o svůj soukromý klíč, který používá pro označování vydaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a časových razítek, o kryptografický modul a o znalosti a schopnosti osob, které mají přístup k těmto velmi důležitým aktivům. Poskytovatel také musí zajišťovat, aby určité informace a služby byly vždy dostupné.

Další kapitola se zabývá personální bezpečností (bezpečností z hlediska lidských zdrojů). V této oblasti je základní již první fáze – přijímací řízení, které má zamezit případným lidským chybám – to se týká zejména pracovníků na citlivých pozicích. U poskytovatele certifikačních služeb je to role bezpečnostního správce, správce systému, bezpečnostního auditora. Nejprve je nutné vymezit požadavky na kvalifikaci a další vlastnosti přijímaného pracovníka – to je již přímo požadavkem vyhlášky [53]. Je vhodné si prověřit informace, které o sobě uchazeč o zaměstnání uvede. Důležitá je též kvalitní pracovní smlouva.

V průběhu pracovního vztahu jsou důležitou součástí personální bezpečnosti školení zaměstnanců vedoucí k tomu, aby si uvědomovali bezpečnostní hrozby a aby byli připraveni se podílet na dodržování zásad bezpečnostní politiky v průběhu své běžné pracovní činnosti. V dokumentu [43] je dále uvedeno, že v oblasti personální bezpečnosti má být dbáno na minimalizaci škod způsobených bezpečnostními incidenty a chybami, jejich sledování a následné poučení z těchto chyb – tedy oblast reakcí na bezpečnostní incidenty a chyby. Pravidla pro přístup k chybám a incidentům musí být formalizovaná, pracovníci poskytovatele musí vědět, kam mají takové události hlásit, aby se dostaly okamžitě na místo, kde je možné na ně prakticky reagovat. Vzhledem k tomu, že může být zaměstnanci hlášení bezpečnostních incidentů považováno za zbytečné, protože se podle jejich zkušenosti „většinou nic nestane“, je vhodné formalizovat i postup v případě, že zaměstnanec poruší bezpečnostní politiku nebo jiné bezpečnostní směrnice.

Další důležitou součástí personální bezpečnosti je vytvoření pravidel pro ukončení pracovního poměru. Zejména jde o neopomenutí odebrání přístupových práv do všech citlivých součástí systému. Na tuto oblast je nutné se zaměřit i v případě změny pracovní pozice – i v takové situaci je nutné identifikovat, zda nemá dojít k odebrání některých práv a přidělení jiných. Pravidla definovaná pro pracovníky poskytovatele se nemusí vztahovat pouze na zaměstnance organizace poskytovatele, ale i na zaměstnance smluvních partnerů – i u nich je nutné stanovená pravidla dodržovat a dodržování

kontrolovat. Personální bezpečnost je jednou z nejnáročnějších a nejzásadnějších složek řízení bezpečnosti, protože lidský faktor je často nejslabším článkem.

Další kapitola normy ISO 17799 [43] se zabývá fyzickou bezpečností (někde také objektovou bezpečností) a bezpečností prostředí. Poskytovatel certifikačních služeb musí vymezit tzv. fyzický bezpečnostní perimetr, a to pro všechny fyzické oblasti, ve kterých se nakládá s citlivými aktivy a kde se provádějí kritické operace z hlediska bezpečnosti důvěryhodného systému poskytovatele. U poskytovatele se zejména jedná o umístění hardwarového kryptografického modulu, který využívá pro vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Poskytovatel certifikačních služeb musí prostory, ve kterých je kryptografický modul fyzicky umístěn, zabezpečit obdobně jako zabezpečené oblasti kategorie „Důvěrné“ podle vyhlášky Národního bezpečnostního úřadu [55].

V oblasti fyzické bezpečnosti je nutné dbát na kontroly vstupu osob do zabezpečených prostor a zabezpečení objektů obecně. Je nutné myslet na bezpečnost zařízení, jeho umístění, zabezpečení dodávky energie, bezpečnost kabeláže, údržbu zařízení a bezpečnost těch zařízení, která jsou umístěna mimo objekt, který vlastní organizace. Další oblast, na kterou je třeba dbát, je postup při likvidaci nebo opakovaném použití zařízení – běžné mazání nelze považovat za způsob, jak zamezit dostupnosti dat na paměťových médiích.

Další kapitola [43] se zabývá řízením komunikací a řízením provozu. V první části, věnované provozním postupům a odpovědnostem, se zabývá zajištěním správného a bezpečného provozu prostředků pro zpracování informací. Všechny provozní postupy mají být zdokumentovány přesným návodem v provozní dokumentaci.

Poskytovatel certifikačních služeb by se měl zaměřit na řízení provozních změn. Další důležitý požadavek se vztahuje na oddělení povinností – poskytovatel certifikačních služeb musí oddělit činnosti, které mohou vést k neautorizované modifikaci nebo zneužití jeho dat (zejména jeho vlastních

soukromých klíčů) či služeb. U poskytovatele certifikačních služeb je pro provedení některých operací (generování párových dat poskytovatele a další operace s hardwarovým kryptografickým modulem) nutná přítomnost více osob, aby nemohlo dojít k podvrhu. Je důležité, aby byl prováděn nezávislý bezpečnostní audit – v případě poskytovatele musí být prováděny jednak interní bezpečnostní audity (kontrola bezpečnostní shody) a dále audity třetí stranou (audit systému řízení bezpečnosti informací).

Další požadavek normy ISO 17799 se vztahuje na oddělení vývoje, testování a provozu. Při tvorbě programů musí být nejprve vytvořena verze, která je následně otestována, avšak jinými osobami než vývojáři. Teprve po úspěšném otestování může být programové vybavení nasazeno v provozu. V případě (který je u poskytovatelů poměrně častý), kdy je software získáván od dodavatele, je nutné otestovat produkt nejen u dodavatele, ale i v reálném prostředí poskytovatele před nasazením do ostrého provozu.

Důležitým mechanismem pro zajištění bezpečnosti je plánování a akceptace systému. Před vytvářením nového systému je nutné vytvořit plán kapacit na provoz, kterému má být následně přizpůsobena tvorba systému. Před uvedením systému do provozu je třeba ověřit testováním, že jsou splněna akceptační kriteria. Akceptační kriteria je nutné vždy dopředu přesně vymezit. Pokud je systém pořizován od dodavatele, je nutné akceptační kriteria vymezit ve smlouvě. Z hlediska poskytovatele certifikačních služeb je zásadní, aby nasazením nové verze systému nedošlo k přerušení výkonu jeho kritických činností (např. vydávání CRL).

Poskytovatel musí mít implementovánu efektivní ochranou proti škodlivým programům, a to včetně opatření umožňujících detekovat přítomnost škodlivého kódu. Poskytovatel musí dbát na to, aby nebyla poškozena jeho pověst, takže je nutné chránit nejen kritickou infrastrukturu, ale např. i webové stránky, které jsou dostupné veřejnosti.

Poskytovatel musí zálohovat některá data. Při zálohování není důležité pouze samotné zálohování, ale i pravidelné testování, zda jsou zálohy čitelné a použitelné. Poskytovatel musí zajistit udržení integrity a dostupnosti informací

a prostředků pro jejich zpracování. U záloh je také nutné si stanovit dobu, po kterou jsou zálohy uchovávány. Kvalifikovaný poskytovatel má povinnost některá data (data, která souvisejí s vydáním certifikátu) uchovávat po dobu deseti let. Pro dlouhodobé uchování těchto dat je nutné ověřovat, zda jsou data stále čitelná, a vhodně zvolit média pro uchovávání těchto dat, aby existovaly záruky, že tato média mají životnost po stanovenou dobu.

Další část kapitoly o řízení komunikací a provozu se zabývá správou bezpečnosti sítě. Cílem bezpečnostních opatření v této oblasti je zajištění ochrany informací v počítačových sítích a ochrany síťové infrastruktury. Kromě pravidel pro síťové služby a přenosy dat je pro poskytovatele zásadní monitorování a zaznamenávání všech událostí, které ovlivňují bezpečnost.

Tato kapitola se zabývá i bezpečností při zacházení s médii, a to zejména nakládáním s vyměnitelnými médii, likvidací datových nosičů, postupy pro manipulaci s informacemi a bezpečností systémové dokumentace. Média mají být označována, má být zaznamenán každý přístup k datům a postup pro manipulaci s médii musí být popsán. U poskytovatele je zásadní obsah systémové dokumentace, která může obsahovat citlivé informace o důvěryhodném systému, takže je nutné ji (resp. její části obsahující citlivé informace) bezpečně uložit a dávat ji k dispozici jen oprávněným osobám.

Další část této kapitoly obsahuje požadavky na výměnu informací a programů mezi organizacemi. Poskytovatel certifikačních služeb je povinen v souladu s právními předpisy zpřístupňovat některé informace svým klientům, spoléhajícím se stranám a Ministerstvu informatiky. Některé z těchto informací jsou zásadního rázu, jedná se zejména o zveřejňování seznamu zneplatněných certifikátů, který musí být přístupný nepřetržitě. Mezi další informace, které poskytovatel musí povinně zveřejnit, patří seznam vydaných certifikátů, certifikační politika, informace o tom, že je kvalifikovaným poskytovatelem certifikačních služeb, případně informace o odnětí akreditace. Zejména v případě certifikační politiky je třeba dbát na to, aby informace, které jsou v ní obsažené, nemohly být pro poskytovatele bezpečnostním rizikem. Některé informace poskytovatel zasílá prostřednictvím e-mailové komunikace – i v tomto

případě je třeba dbát na případná rizika, která mohou ohrozit nejen samotného poskytovatele, ale i jeho klienty.

Další část kapitoly o řízení komunikací a provozu se věnuje elektronickému obchodu – tato kapitola však ve vztahu k poskytovatelům certifikačních služeb není relevantní, protože elektronický obchod není standardní součástí služeb důvěryhodných systémů poskytovatele. Tato kapitola se zabývá i bezpečnostními požadavky na zveřejňované informace, zejména jde o zamezení modifikace zveřejňovaných dat – tyto požadavky naopak jsou pro poskytovatele certifikačních služeb relevantní; zejména u dat určených spoléhajícím se stranám je nutné používat digitální podpis pro určení integrity a zajištění autenticity těchto informací.

Zvláštní požadavek normy ISO 17799 se týká monitorování, resp. pořizování a vyhodnocování auditních záznamů (neboli záznamů o událostech). Ačkoliv je tento požadavek uveden již v části věnované správě sítě, vzhledem k zásadnímu dopadu tohoto bezpečnostního opatření je mu věnována celá část kapitoly. Poskytovatel certifikačních služeb musí stanovit, jaké události bude zaznamenávat a sledovat, aby eliminoval riziko neoprávněného získání či modifikace informací. Poskytovatel má pravidelně vyhodnocovat incidenty, ke kterým došlo, a na jejich základě přijmout případná další opatření.

Další kapitola se zabývá řízením přístupu. Její první část obsahuje požadavky na řízení přístupu. Zde je zásadní identifikace všech informací, stanovení rizik, kterým jsou informace vystaveny, a následné stanovení pravidel pro šíření těchto informací. Tyto kroky jsou součástí provedení hodnocení rizik. Poskytovatel má stanovit politiku pro řízení přístupu, která bude vymezovat provozní požadavky na řízení přístupu a určovat pravidla řízení přístupu.

Druhá část se zabývá řízením přístupu uživatelů. Pro poskytovatele je zásadní popis pravidel pro získání oprávnění pro přístup do systému a následné odebrání tohoto oprávnění. Poskytovatelé používají pro přístup do systému obvykle čipové karty s autentizačními a šifrovacími certifikáty namísto běžného jména a hesla (použití jména a hesla má z hlediska bezpečnosti nižší úroveň), protože případné škody způsobené uživatelem

v systému mohou být vysoké. Poskytovatel má provádět školení uživatelů svých informačních systémů pro práci s čipovými kartami a přistupování do systému. Je vhodné provádět pravidelnou kontrolu, zda mají uživatelé oprávnění, která jim skutečně náleží.

Třetí část této kapitoly se zabývá odpovědnostmi uživatelů (jedná se zejména o uživatele z řad zaměstnanců poskytovatele). Uživatelé musí znát své odpovědnosti, aby se zamezilo zneužívání uživatelského přístupu. Poskytovatel má dbát na to, aby nemohlo dojít ke zneužití počítačů, které jsou bez obsluhy. Je vhodné přijmout pravidlo prázdného stolu a prázdné obrazovky monitoru. To je důležité zejména u pracovníků registračních autorit, kteří jsou v přímém kontaktu se zákazníkem, ale i ostatní uživatelé informačního systému mají dodržovat bezpečnostní opatření, která poskytovatel stanovil. I tato oblast má být předmětem školení.

Čtvrtá část obsahuje požadavky na řízení přístupu k síti. Poskytovatel má vymezit pravidla, která jsou uplatňována při přístupu uživatele k síťovým službám. Poskytovatel má upravit způsob autentizace uživatele externího připojení, způsob autentizace uzlů v síti, ochranu portů pro vzdálenou diagnostiku, oddělení vnitřních síťových domén organizace a vnějších síťových domén, řízení síťových spojení (např. prostřednictvím firewallů), řízení směrování sítě a bezpečnost síťových služeb.

Pátá část se zabývá řízením přístupu k operačnímu systému, které má zamezit neautorizovanému přístupu do operačního systému. Poskytovatel certifikačních služeb má uvést, jakým způsobem je zajištěno řízení přístupu do operačního systému a s příslušnými pravidly seznámit uživatele. Je možné využít možnost indikace přihlášení uživatele pod nátlakem; v takovém případě musí být stanoven i postup, jak bude na zjištění takové události reagováno. V některých případech je vhodné, aby byl přístup uživatele po určitém čase, kdy není aktivní, zablokován.

Šestá část upravuje oblast řízení přístupu k aplikacím a informacím. Navrhuje bezpečnostní prostředky, které mohou být použity k omezení přístupu k aplikacím tak, aby byly přístupné pouze pro oprávněné uživatele. Velmi citlivé

aplikace, což je u poskytovatele certifikačních služeb minimálně prostředí hardwarového kryptografického modulu, mají být v umístěny v izolovaném počítačovém prostředí (samozřejmě izolované prostředí je relativní pojem a i úroveň této izolovanosti je nutné vymezit).

Sedmá část kapitoly o řízení přístupu se zabývá velmi důležitou a v současné době poměrně opomíjenou oblastí, a to oblastí mobilních výpočetních prostředků a práce na dálku. Tyto prostředky mají specifické vlastnosti, takže je nutné jim věnovat zvláštní pozornost a definovat bezpečnostní pravidla pro nakládání s nimi. Pro získání dostatečného povědomí o rizicích, která jsou spojena s používáním mobilních prostředků, je vhodné organizovat pro uživatele mobilních zařízení školení a zavést kontroly dodržování pravidel, která jsou pro používání mobilních výpočetních prostředků stanovena. Někteří poskytovatelé certifikačních služeb nabízejí službu mobilních registračních autorit – v tomto případě je nutné věnovat zvýšenou pozornost těmto bezpečnostním pravidlům při proškolení pracovníků, kteří tyto služby zajišťují.

Další kapitola se zabývá akvizicí, vývojem a údržbou systémů. Cílem je zajištění bezpečnosti již ve fázi pořizování systému. Pokud je do systému implementována bezpečnostní funkce, je nutné, aby ostatní funkcionality neporušily její bezpečnost. Proto je důležité, aby byl řízený celý proces vývoje systému. Poskytovatel musí již při specifikaci požadavků na vytvoření či nákup nového systému, případně na provedení změn stávajícího systému, definovat odpovídající bezpečnostní požadavky a opatření. Některé z těchto požadavků mohou vyplývat i ze zákonných povinností poskytovatele, případně z požadavků norem.

Ve druhé části této kapitoly je popsáno správné zpracování dat v aplikacích, ochrana dat proti ztrátě, neoprávněné modifikaci nebo jejich zneužití. Konkrétně obsahuje požadavky na validaci vstupních dat, na kontrolu vnitřního zpracování dat, na integritu dat a na validaci výstupních dat.

Ve třetí části jsou uvedena kryptografická opatření, která lze použít pro zajištění důvěrnosti, autentičnosti a integrity dat. Pokud je některý

mechanismus (šifrování, digitální podpis) použit, je třeba určit, jaké mají být jeho parametry. Pro poskytovatele je vhodné využít parametry definované v dokumentu ALGO-paper [35]. Poskytovatel musí mít popsaný systém správy klíčů, a to od fáze generování, přes ukládání a používání, až po ničení soukromých klíčů (a naopak dlouhodobé uchování veřejných klíčů a certifikátů, ve kterých byly veřejné klíče obsaženy). V některých případech je použití kryptografických mechanismů požadováno zákonem [1] či vyhláškou [53].

Ve čtvrté části této kapitoly je řešena problematika bezpečnosti systémových souborů. Systémové soubory a aplikace mají být zabezpečeny tak, aby u nich byla udržena integrita. Odpovědnost za implementaci programového vybavení do operačního systému má být definována. Provozní programové vybavení má být implementováno tak, aby nenarušilo operační systém a naopak. Testovací data mají být chráněna a kontrolována. Ke knihovnám zdrojových kódů má být zavedeno řízení přístupu.

Pátá část se zabývá bezpečností procesů vývoje a podpory. Uvedená bezpečnostní opatření jsou uplatňována při vývoji a v průběhu podpory aplikací za účelem udržení bezpečnosti programů a informací v aplikacích. Prvním opatřením je definování postupů změnového řízení. Změny musí být před provedením odsouhlaseny, čemuž musí předcházet určení veškerého programového vybavení, informací, databázových systémů, uživatelů, systémové a bezpečnostní dokumentace, které budou změnami ovlivněny. Pokud dojde ke změnám v operačním systému, což je poměrně častá situace (např. instalace bezpečnostních záplat), je též vhodné zkontrolovat, jestli změny nemají negativní vliv na funkčnost nebo bezpečnost.

Dále je zmíněna modifikace programových balíků poskytovatelem, ke které by mělo docházet pokud možno minimálně. Je nutné zvážit riziko, protože za chyby způsobené takto modifikovanými balíky ručí sám poskytovatel a nikoliv výrobce programového balíku. Další oblast, která je v této kapitole popsána, se zabývá skrytými kanály a trojskými koni, proti kterým je nutné se odpovídajícím způsobem chránit.

Dále je uvedeno, jakými problematickými oblastmi je vhodné se zabývat při získávání programového vybavení vyvíjeného externím dodavatelem. Změnové řízení je jedním ze základních mechanismů, jehož kvalitní nastavení je bezpodmínečně nutné pro správné zajištění služeb poskytovatele. Vzhledem k tomu, že většina používaného programového vybavení je získávána od dodavatele, je nutné dbát na kvalitní smlouvy (v současnosti se používá tzv. SLA – service level agreement, tj. smluv, které se vyznačují stanovením měřitelných parametrů a akceptovatelných hodnot těchto parametrů) a pečlivou kontrolu dodaného software při jeho akceptaci.

Poslední součástí této kapitoly je řízení technických zranitelností. Pokud existuje jakákoliv zranitelnost v systému, je nutné ji zaznamenat, vyhodnotit její dopad a v případě rizika, které nelze akceptovat, přijmout odpovídající bezpečnostní opatření. V rámci správy zranitelností je nutné sledovat vhodné zdroje informací – jedná se jednak o informace od subjektů, od nichž byl systém pořízen, a dále o informace od subjektů, které poskytují specializované služby pro informování o existujících zranitelnostech (za tímto účelem se využívají tzv. CERT – computer emergency response team).

Další oblast, kterou se poskytovatel má zabývat, je zvládání bezpečnostních incidentů. V případě, že dojde k bezpečnostní události nebo je zaměstnanci identifikována slabina v důvěryhodném systému poskytovatele, je nutné tuto informaci nahlásit. Poskytovatel musí zdokumentovat, jaké události mají zaměstnanci hlásit a jaký je postup tohoto hlášení. Poskytovatel musí vymezit činnost zaměstnanců, kteří se mají bezpečnostními incidenty a slabinami zabývat. Zaměstnanci mají být dobře proškoleni, protože je důležité, aby nedošlo k tomu, že některé důležité události nenahlásí, protože jim nepřipadají důležité, nebo naopak k tomu, že zaměstnanci nahlásí i velmi nepodstatné události, a pak skutečným bezpečnostním incidentům není věnována dostatečná pozornost.

V případě, že dojde k bezpečnostnímu incidentu, je nutné co nejrychleji provést kroky pro obnovu řádné funkce důvěryhodného systému. Postup v těchto případech musí podle vyhlášky [53] poskytovatel popsat v plánu

obnovy. Důležité je také, aby po úspěšné obnově po bezpečnostním incidentu došlo k vyhodnocení incidentu a případné úpravě postupů, aby se daný incident nemohl opakovat. Pokud vznikla bezpečnostním incidentem škoda, je nutné zajistit důkazy v dostatečné kvalitě pro případné soudní řízení.

Další kapitola je věnována řízení kontinuity činností organizace. Smyslem je popsat, jakým způsobem je možné bránit přerušení činností organizace a díky tomu chránit kritické procesy organizace před následky závažných chyb a katastrof. V organizaci má být vytvořen řízený proces pro vytvoření a udržování kontinuity podnikatelských činností. Při zajišťování kontinuity podnikatelských činností mají být zaznamenávány události, které mohou způsobit narušení procesů, a mají být analyzovány dopady. Tyto události mají být podchyceny v analýze rizik, a následně má být vytvořen plán pro zvládnutí těchto událostí – ve vyhlášce [53] je uveden jako plán zvládání krizových situací. Tento plán má být implementován v souladu s postupy v něm uvedenými.

Pro poskytovatele je zásadní službou, která musí být vždy k dispozici, služba zneplatňování certifikátů a zveřejňování seznamu zneplatněných certifikátů. Tyto služby musí být v případě závažného selhání důvěryhodného systému obnoveny nejdříve. Poskytovatel by měl testovat, zda budou tyto kritické činnosti v případě havárie skutečně rychle obnoveny.

Má existovat jednotný systém plánů kontinuity podnikatelských činností, aby v případě vzniku nových požadavků byly příslušné plány doplněny. Plány kontinuity mají být testovány, udržovány a přehodnocovány, aby byly co nejaktuálnější, tzn. co nejúčinnější v případě problémů. Postupy uvedené v plánech kontinuity mají být zahrnuty do postupů při řízení změn v organizaci, aby tato problematika nebyla při změnách opomíjena.

Poslední kapitola [43] se zabývá dalšími požadavky, se kterými musí být organizace v souladu, aby zaručila správným způsobem bezpečnost informací. Jedná se o soulad s právními normami a o soulad s bezpečnostní politikou organizace a s technickými normami.

U právních požadavků je nutné nejprve určit, jaké jsou relevantní právní předpisy – obecně se může jednat o zákony na ochranu duševního vlastnictví, ochranu dokladů organizace, ochranu osobních údajů a soukromí. Kvalifikovaný poskytovatel certifikačních služeb se musí řídit i specifickými zákony upravujícími oblast jeho působnosti. Jedná se zejména o zákon o elektronickém podpisu [2] a vyhlášku o postupech kvalifikovaných poskytovatelů certifikačních služeb [53], ale i o zákon o archivnictví [38] či vyhlášku o fyzické bezpečnosti [55].

Další legislativní omezení se mohou vztahovat na prevenci zneužití prostředků pro zpracování informací – v některých zemích může být neoprávněné využití prostředků pro zpracování informací považováno za trestný čin. Další oblastí, na kterou je třeba dbát, je oblast použití kryptografických prostředků – některé země mají omezení pro import nebo export hardware nebo software podporující kryptografické funkce. Naopak v některých případech může být využití kryptografie při určitých formách komunikace vyžadováno, a v takovém případě je nutné se přizpůsobit případným omezením použitých kryptografických prostředků (např. algoritmy, délky klíčů). Poskytovatelé mají podle vyhlášky používat algoritmy zveřejněné na úřední desce Ministerstva informatiky – v současnosti je na této úřední desce odkaz na evropskou normu ALGO-paper [35].

Pro poskytovatele je zásadní, aby postupoval v souladu se svými bezpečnostními politikami a normami, k jejichž plnění se přihlásil. U poskytovatele dochází k situaci, kdy je požadavek na postupování v souladu s bezpečnostními politikami a některými normami zároveň požadavkem právního předpisu.

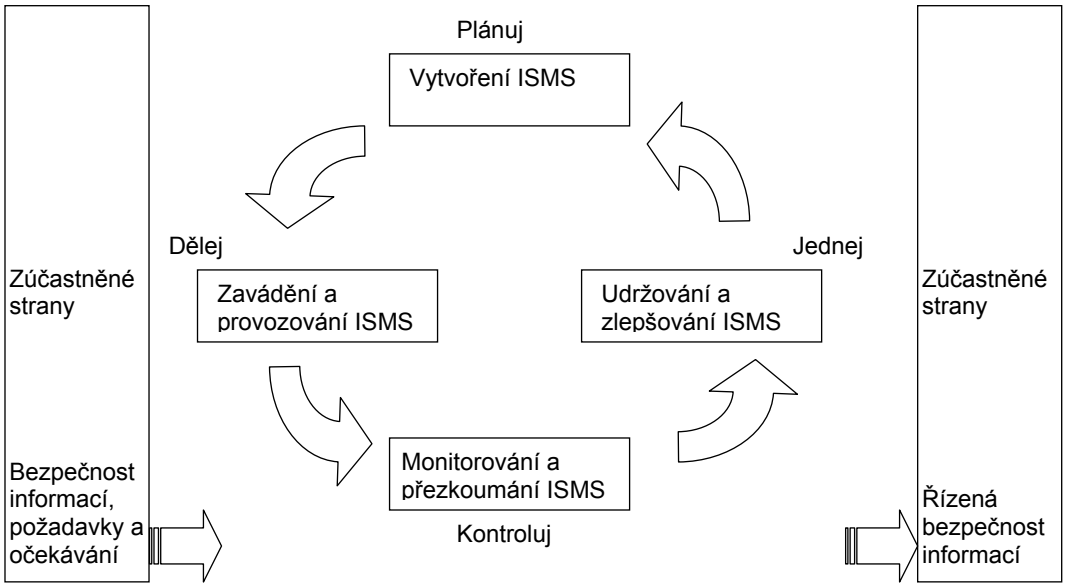
Za účelem ověření, zda skutečně existuje soulad se stanovenými požadavky, probíhá kontrola technické shody. Poskytovatel musí zajistit, aby všechny bezpečnostní postupy, za které má odpovědnost, byly předmětem pravidelného ověření. Při provádění těchto kontrol je důležité, aby bylo možné porovnat jejich výsledky. Poskytovatel certifikačních služeb má povinnost

provádět tyto kontroly (ve vyhlášce [53] je tento typ kontrol nazýván kontrolou bezpečnostní shody).

Poskytovatel má při provádění auditu či kontroly postupovat tak, aby zjistil všechny nedostatky co nejefektivněji, aniž by tím narušil svou běžnou činnost. V žádném případě nesmí při auditu dojít k ohrožení bezpečnosti důvěryhodných služeb poskytovatele. Samotné nástroje pro provádění auditu systému (programy, datové soubory) mají být chráněny.

5.3.3 Aplikace druhé části BS 7799, resp. ISO/IEC 27001, u poskytovatelů certifikačních služeb

Druhá část BS 7799 [44], naposledy vydaná jako ISO/IEC 27001:2005, obsahuje návod na implementaci a správu systému managementu bezpečnosti informací. Specifikuje požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentovaného systému managementu bezpečnosti informací. Norma může být uplatněna u všech typů organizací. V případě, že nemohou být využity některé požadavky této normy [44], je možné uvažovat o jejich vyřazení. Takové vyřazení však nesmí ovlivnit schopnost nebo odpovědnost organizace zajistit bezpečnost informací a musí být v souladu s bezpečnostními požadavky stanovenými na základě analýzy rizik a se zákonnými požadavky. Opodstatněnost vyřazení musí být doložena rozhodnutím odpovědných osob. Poskytovatel má vytvořit prohlášení o aplikovatelnosti, v němž uvede, které požadavky a opatření byly implementovány v jeho systému řízení bezpečnosti informací, a naopak které požadavky a opatření nebyly v jeho systému řízení bezpečnosti použity a zdůvodnění jejich vyřazení.



ISMS - systém managementu bezpečnosti informací

Obrázek 13 – Model PDCA aplikovaný na procesy ISMS [44]

Norma [44] nejprve vysvětluje všeobecné požadavky na systém managementu bezpečnosti informací. Zavádí model Plan-Do-Check-Act (PDCA, Plánuj-Dělej-Kontroluj-Jednej) a prosazuje procesní přístup pro vybudování, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti systému managementu bezpečnosti informací v organizaci. Dále jsou vymezeny požadavky na dokumentaci, konkrétně jaké dokumenty musí být minimálně součástí dokumentace systému managementu bezpečnosti informací, jak musí být dokumentace řízena a jak musí být řízeny záznamy o událostech.

Norma obsahuje požadavek na odpovědnost vedení organizace za vybudování, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti systému managementu bezpečnosti informací v organizaci. Mezi tyto požadavky patří nutnost zajištění potřebných zdrojů, udržování bezpečnostního povědomí prostřednictvím školení a správná personální politika.

Požadavek na vedení organizace se vztahuje i k přezkoumávání systému managementu bezpečnosti informací. Je upřesněno, jaké mají být vstupy a výstupy z přezkoumání, dále je uvedeno, že mají v plánovaných intervalech probíhat interní audity systému managementu bezpečnosti informací. Jak již bylo uvedeno výše, poskytovateli certifikačních služeb je vyhláškou [53] uložena povinnost provádět audity a kontroly.

Velmi podstatnou kapitolou je kapitola věnovaná zlepšování systému managementu bezpečnosti informací. Organizace musí neustále zlepšovat efektivnost systému managementu bezpečnosti informací. Jakékoliv zjištěné nedostatky v provozování systému managementu bezpečnosti informací musí být odstraněny a postup této činnosti má být zdokumentován. Dále je nutné určit předem opatření, která slouží jako prevence proti opakovanému výskytu nehod – většinou je finančně efektivnější stanovit a uplatnit preventivní opatření než opatření nápravné [44].

Příloha A normy [44] obsahuje normativní požadavky, které sestávají z cílů jednotlivých opatření, a samotná bezpečnostní opatření – opatření uvedená v příloze A odpovídají opatřením, která jsou uvedena v první části BS 7799 (resp. v ISO/IEC 17799). V průběhu vytváření systému managementu bezpečnosti informací musí být určena opatření, která budou v organizaci uplatněna a uvedena v prohlášení o aplikovatelnosti, jak je již uvedeno výše.

5.3.4 TS 101 456

Dokument TS 101 456 [46] specifikuje požadavky na postupy certifikačních autorit poskytujících kvalifikované certifikáty. Rozlišuje oblast s použitím bezpečných prostředků pro vytváření elektronického podpisu a oblast, kde tyto prostředky nejsou použity. V České republice se zatím bezpečné prostředky pro vytváření elektronického podpisu nepoužívají, takže v současnosti jsou pro poskytovatele relevantní pouze požadavky na poskytování služeb bez těchto bezpečných prostředků.

Dokument může sloužit jako podklad pro nezávislé hodnotitele posuzující splnění požadavků na vydávání kvalifikovaných certifikátů – jako návod pro hodnocení lze použít dokument CWA 14 172 [47].

Dokument nejprve vymezuje základní pojetí certifikačních autorit, certifikačních služeb, vztahů mezi certifikační politikou a certifikační prováděcí směrnicí, význam pojmu držitel certifikátu nebo podepisující osoba. Dále se zabývá samotným obsahem certifikační politiky. Obsahuje vymezení povinností a odpovědností jednotlivých subjektů – poskytovatele, držitele certifikátu, podepisující osoby, spoléhající se strany.

Dále jsou uvedeny požadavky na postupy poskytovatelů certifikačních služeb – jaké informace mají být uvedeny v certifikační prováděcí směrnici, požadavky na správu infrastruktury veřejných klíčů, zejména klíčů poskytovatele certifikačních služeb, kryptografického modulu, ve kterém je soukromý klíč poskytovatele certifikačních služeb vytvořen, uložen a používán. Dále požadavky na přípravu prostředků pro bezpečné vytváření podpisu pro koncové uživatele.

V následující kapitole jsou uvedeny požadavky na životní cyklus při správě certifikátů. Jsou to požadavky na registraci, vydání následného certifikátu, generování certifikátu pro nové uživatele, informování uživatele o podmínkách poskytovaných služeb, vydání certifikátu, zneplatnění certifikátu.

Dále jsou uvedeny požadavky na řízení a provoz poskytovatele certifikačních služeb. Patří sem konkrétní požadavky na řízení bezpečnosti, klasifikaci a řízení aktiv, personální bezpečnost, fyzickou bezpečnost a bezpečnost prostředí, provozní řízení, řízení přístupu do systému, vývoj důvěryhodných systémů, řízení kontinuity podnikatelských činností a postup v případě bezpečnostních incidentů, ukončení činnosti certifikační autority, shodu s právními požadavky a záznamy související s poskytováním kvalifikovaných certifikátů. Obecně lze jako návod pro řízení bezpečnosti použít normu BS 7799 [43] a [44], na kterou je z dokumentu odkazováno.

Poslední kapitola hlavního dokumentu obsahuje rámec pro správu politik poskytovatele a pro nakládání s ostatními politikami poskytovatele obecně.

Dále jsou v dokumentu přílohy, z nichž nejzajímavější je struktura zprávy pro uživatele a tabulka s propojením na RFC 3647 [23].

Dokument [46] je zásadním dokumentem poukazujícím na potenciální problematické oblasti při poskytování certifikačních služeb v návaznosti na řízení bezpečnosti podle normy BS 7799. Přestože při podrobném čtení lze narazit na jisté rozpory, či spíše nejednoznačnosti, mezi dokumentem CWA 14 167-1 [17] a tímto dokumentem [46], je tento dokument vzhledem ke své orientaci na postupy nezbytným doplněním a vysvětlením, jak naplnit požadavky CWA 14 167-1.

5.3.5 TS 102 023

Dokument TS 102 023 [29] obsahuje požadavky na postupy autorit časových razítek. Tyto požadavky na provoz a management autorit časových razítek slouží k tomu, aby daly návod, jak zajistit, aby se uživatelé a spoléhající se strany mohly na poskytované služby spolehnout.

Dokument vysvětluje, jaký je vztah mezi politikou pro vydávání časových razítek a prováděcí směrnicí pro vydávání časových razítek. Obsahuje výčet základních povinností a odpovědností jednotlivých subjektů PKI v oblasti poskytování časových razítek.

Nejrozsáhlejší kapitola se zabývá samotnými postupy poskytovatele časových razítek. Tyto postupy mají být obsaženy v prováděcí směrnici poskytovatele a některé, ve strukturované podobě, ve zprávě pro uživatele. Konkrétní požadavky jsou pak blíže rozvedeny pro správu klíčů poskytovatele časových razítek. Soukromý klíč použitý pro podepisování vydávaných časových razítek smí být použit jen pro tento účel a musí být uložen v bezpečném kryptografickém modulu. Dále jsou obsaženy požadavky na činnosti spojené s veřejným klíčem.

Poté je upraveno samotné vydání časového razítka – musí v něm být přesný čas, identifikace politiky, podle které bylo vydáno apod. Dále je upřesněna informace o způsobu získávání přesného času.

Samozřejmě je v této kapitole obsažena i informace o tom, jak má poskytovatel postupovat – jsou zde uvedeny specifické požadavky na řízení bezpečnosti, klasifikaci a řízení aktiv, personální bezpečnost, fyzickou bezpečnost a bezpečnost prostředí, provozní řízení, řízení přístupu do systému, vývoj důvěryhodných systémů, na postupy v případě kompromitace služeb autority časových razítek, ukončení činnosti autority časových razítek, shodu s právními požadavky a požadavky na záznamy související s provozováním autority časových razítek. Požadavky, které nejsou specifické, ale jejichž splnění je nutné při poskytování důvěryhodných služeb, mohou být stejně jako v případě poskytování certifikátů zajištěny podle BS 7799 [43] a [44].

Další požadavek se vztahuje na provoz autority časových razítek, který musí být dostatečně spolehlivý. Jsou vyjmenovány konkrétní charakteristiky, na které je třeba zejména dbát.

6 METRIKY PRO POSOUZENÍ DŮVĚRYHODNÝCH SYSTÉMŮ POSKYTOVATELE CERTIFIKAČNÍCH SLUŽEB

Poskytovatel certifikačních služeb musí při provozování svých důvěryhodných systémů získávat zpětnou vazbu, aby mohl zefektivňovat kvalitu svých služeb. Rovněž akreditační a kontrolní orgán potřebuje získat informace o tom, v jakém jsou stavu důvěryhodné systémy poskytovatele. Proto autorka této práce navrhuje metriky, které umožní měření vybraných atributů jakosti, na základě kterých je možno posoudit předpoklady pro provozování důvěryhodných systémů.

Metriky autorka definuje pro jednotlivé atributy, které autorka určila na základě požadavků, které jsou zákonem o elektronickém podpisu [2] kladeny na poskytovatele certifikačních služeb. Smyslem hodnocení, pro která jsou tyto míry definovány, je určení úrovně, s jakou poskytovatel certifikačních služeb, resp. důvěryhodné systémy, které provozuje, splňují požadavky, které jsou na tyto systémy a poskytovatele kladeny.

Autorka se zaměřuje na posouzení splnění požadavků na kvalifikované poskytovatele certifikačních služeb, které se provádí při všech zmiňovaných ověřováních činnosti těchto poskytovatelů (tzn. akreditace, dozor, kontrola bezpečnostní shody a audit systému managementu bezpečnosti informací).

Provedení měření má být rychlé a jednoduché, nesmí narušit běžný chod organizace. Měření jsou navržena tak, aby bylo možné je provádět opakovaně a výsledky měření porovnávat. Některá měření je možné provádět automatizovaně s využitím vhodné aplikace.

Celý systém metrik má význam pouze v případě, že zjištěné nedostatky jsou postupovány dále k odpovědným zaměstnancům poskytovatele, kteří se zasadí o realizaci odpovídajících opatření. Je vhodné, aby se tito zaměstnanci zapojili i do procesu definování požadavků, jejichž plnění má být měřeno. Na nejvyšší úrovni budou jistě figurovat i požadavky na ekonomickou efektivnost poskytování služeb, které je také třeba měřit (ale návrh metrik pro tuto oblast není předmětem práce). Vedení organizace v konkurenčním prostředí se jistě

zaměří na sledování kvality služeb poskytovaných uživatelům, kteří kupují jejich produkty – tedy certifikáty a časová razítka.

Požadavky by samozřejmě měly v tomto případě definovat všechny subjekty, kterých se bezpečnost v organizaci týká – ředitel, bezpečnostní ředitel, správce ICT, ekonomický ředitel, personální ředitel – samozřejmě názvy pozic se v organizacích mohou lišit, ale podstatné je vymezení odpovědnosti za jednotlivé oblasti činnosti poskytovatele.

Kromě legislativních požadavků a požadavků norem má poskytovatel vyhodnocovat i plnění požadavků své vlastní dokumentace, což je nad rámec tohoto dokumentu.

Základní požadavky na kvalifikovaného poskytovatele certifikačních služeb vyplývají ze zákona o elektronickém podpisu. Požadavky vyhlášky a norem již pouze rozšiřují a konkretizují základní zákonné požadavky, definují způsob jejich splnění. Pokud poskytovatel nedodrží povinnosti stanovené zákonem, může mu být uložena pokuta do výše 10 000 000 Kč, což je pokuta „likvidační“. I z toho důvodu autorka definuje metriky pro některé požadavky zákona. Požadavky zákona, které jsou použity jako měřené atributy, byly vybrány s ohledem na jejich měřitelnost.

Metriky autorka navrhuje tak, že v nich zohledňuje nejen požadavky zákona, ale i vyhlášky a norem, které vysvětlují, jakým způsobem má být požadavek naplněn – na základě těchto požadavků je měřena většina atributů.

6.1 Kvalifikační požadavky

Poskytovatel musí zajistit, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnou pro poskytování kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy.

Požadavek – měřený atribut	Personální zajištění poskytovaných kvalifikovaných certifikačních služeb na dostatečné úrovni znalostí.
Účel míry	Je výkon poskytovaných služeb zajištěn vhodně kvalifikovanými osobami? Probíhá pravidelné školení těchto osob? Jsou zdokumentovány odpovídající postupy?
Činnosti, které je nutné provádět pro splnění požadavku	Při přijímání osob je nutné určit přesné požadavky na odbornost a kvalifikaci uchazečů a ověřit jejich odborné znalosti. Je nutné provádět pravidelné školení osob, aby znaly bezpečnostní postupy, které mají dodržovat Je nutné, aby se v případě změny bezpečnostního postupu všechny zainteresované osoby o této změně včas dozvěděly.
Metoda měření	Procento osob odpovědných za bezpečnost, které mají odpovídající kvalifikaci a prošly odborným školením ze všech osob odpovědných za bezpečnost.
Vzorec pro výpočet	Počet osob z otázky 5/počet osob z otázky 9 x 100%
Na základě čeho je posuzováno	1. Jsou definovány role, které odpovídají za bezpečnost? 2. Jsou dokumentovány kvalifikační požadavky na osoby v těchto rolích? 3. Dochází při přijímání osob k ověření jejich odborných znalostí v oblasti bezpečnosti? 4. Mají osoby odpovědné za bezpečnost přístup k bezpečnostní dokumentaci? 5. Kolik je osob, které jsou odpovědné za bezpečnost u poskytovatele? 6. Existují záznamy o kvalifikaci osob, které jsou odpovědné za bezpečnost?

	7. Existují záznamy o tom, jaké osoby prošly bezpečnostním školením? 8. Je v dokumentaci poskytovatele požadavek na provádění pravidelných školení u osob odpovědných za bezpečnost? 9. Kolik osob z těch, které jsou odpovědné za bezpečnost, má odpovídající kvalifikaci a zároveň absolvovalo v dokumentací požadovaném termínu odpovídající školení?
Zdroje dat pro určení míry	Záznamy o školeních, bezpečnostní dokumentace, personální evidence.
Interpretace míry	Pokud by poskytovatel neměl vymezeno, jaké osoby odpovídají za bezpečnost, jaké má na tyto osoby kvalifikační požadavky a jaká školení musí tyto osoby pravidelně absolvovat, a následně by nedokumentoval, jestli tyto požadavky jsou splněny, nebylo by možné toto měření korektně provést. V takovém případě je nutné zavést postupy, které povedou k možnosti určit míru splnění tohoto zákonného požadavku. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.2 Bezpečné systémy

Poskytovatel musí používat bezpečné systémy a bezpečné nástroje elektronického podpisu, zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují, a zajistit dostatečnou kryptografickou bezpečnost těchto nástrojů; systémy a nástroje jsou považovány za bezpečné, pokud odpovídají požadavkům stanoveným zákonem a prováděcí vyhláškou, nebo pokud splňují požadavky technických norem uvedených v rozhodnutí Komise vydaném na základě článku 3 (5) směrnice 1999/93/ES.

Požadavek – měřený atribut	Používání bezpečných systémů a nástrojů elektronického podpisu a zajištění bezpečných postupů.
Účel míry	Používá poskytovatel bezpečné systémy? Používá poskytovatel bezpečné nástroje elektronického podpisu? Zajišťuje poskytovatel bezpečné postupy? Zajišťuje poskytovatel kryptografickou bezpečnost ve svých důvěryhodných systémech?
Činnosti, které je nutné provádět pro splnění požadavku	Poskytovatel v případě, že nakupuje nebo vytváří důvěryhodné systémy, jejichž součástí jsou i nástroje elektronického podpisu, musí pořizovat ty, které jsou v souladu s požadavky zákona, vyhlášky a norem (a nebo je v souladu s těmito požadavky vytvářet). Poskytovatel musí sledovat požadavky zákona, vyhlášek a norem, které se na jeho činnost vztahují, a kontrolovat jejich dodržování. Zejména se to týká použitého kryptografického modulu, který musí být na seznamu vyhodnocených nástrojů e-podpisu. Poskytovatel musí být připraven na situaci, kdy kryptografický modul bude nutné vyměnit. Použití kryptografického modulu a důvěryhodných systémů musí být upraveno v dokumentaci a postupy s tím spojené musí respektovat požadavky vyhlášky a norem. Poskytovatel musí sledovat aktuální vývoj v oblasti kryptografie a mít nástroje, které uplatní v případě nutnosti nahrazení kryptografických algoritmů kvůli jejich prolomení.

Metoda měření	Procento požadavků zákona, vyhlášky a norem na důvěryhodné systémy, jejichž způsob naplnění je implementován, ze všech těchto požadavků.
Vzorec pro výpočet	Počet kladně zodpovězených otázek/5*100%
Na základě čeho je posuzováno	1. Používá poskytovatel kryptografický modul uvedený na seznamu vyhodnocených nástrojů elektronického podpisu? 2. Je výsledek poslední kontroly bezpečnostní shody v oblasti uplatňování požadavků normy CWA 14167-1 kladný? 3. Je výsledek poslední provedené kontroly bezpečnostní shody v oblasti uplatňování požadavků vyhlášky o postupech kvalifikovaných poskytovatelů certifikačních služeb kladný? 4. Dochází k pravidelnému (s frekvencí, která je v souladu s vyhláškou a dokumentací poskytovatele) ověřování uplatňování postupů pro splnění požadavků? 5. Dochází k přijímání nápravných opatření v případě zjištění nedostatků (v případě, že nebyly nedostatky zjištěny, je odpověď též kladná)?
Zdroje dat pro určení míry	Bezpečnostní dokumentace, dokumentace z kontroly bezpečnostní shody, případně kontrola na místě.
Interpretace míry	Pokud poskytovatel nebude používat vyhodnocený kryptografický modul, nemá další hodnocení význam, vzhledem k porušení základního bezpečnostního požadavku. K této situaci by však nemělo docházet a pokud je kryptografický modul certifikován odpovídajícím způsobem, je možné jej dodatečně vyhodnotit a v případě splnění požadavků zákona, vyhlášky a norem by byl tento problém odstraněn.

	Kladný výsledek kontroly bezpečnostní shody je i výsledek s výhradou – z toho vyplývá 5. otázka, která směřuje k odstraňování případných zjištěných nedostatků. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě je roven 100.

Uvedený požadavek je ve skutečnosti velmi široký - odkazuje na další požadavky uvedené v zákoně, ve vyhlášce a v dokumentu CWA 14 167-1 [17]. Tyto dokumenty odkazují na další normy, které je nutné dodržet. Splnění jednotlivých požadavků těchto norem musí poskytovatel vyhodnocovat při kontrole bezpečnostní shody. Vzhledem k množství těchto požadavků je definování odpovídajících metrik nad rámec tohoto dokumentu. V této oblasti je dle autorky největší prostor pro rozšíření disertační práce.

6.3 Uchovávání údajů

Poskytovatel má podle zákona povinnost uchovávat určité údaje. Jedná se o údaje o certifikátech a časových razítcích, která vydal a údaje s jejich vydáním související. Je nutné, aby způsob uchování těchto údajů byl spolehlivý.

6.3.1 Systémy pro uchovávání certifikátů a časových razítek

Poskytovatel musí používat bezpečné systémy pro uchovávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů nebo kvalifikovaných časových razítek 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.

Požadavek – měřený atribut	Změny záznamů a uchovávané záznamy o certifikátech a časových razítcích mohou provádět pouze pověřené osoby, lze kontrolovat správnost záznamů a je zjevné, pokud dojde k porušení bezpečnostních požadavků.
Účel míry	Nakládá poskytovatel certifikačních služeb se záznamy důvěryhodně?
Činnosti, které je nutné provádět pro splnění požadavku	Do důvěryhodného systému existuje pouze řízený přístup. Všechny události, které se týkají změn a přidávání záznamů o certifikátech, jsou zaznamenávány. Záznamy jsou uchovávány a jejich správnost je možné kontrolovat. Systém umožňuje detekci porušení bezpečnostních požadavků.
Metoda měření	Procento důvěryhodných systémů, ve kterých jsou zaznamenávány události (v dostatečném rozsahu) ze všech důvěryhodných systémů poskytovatele.
Vzorec pro výpočet	Počet důvěryhodných systémů, u nichž byla na otázky 3 a 4 kladná odpověď / počet všech důvěryhodných systémů z otázky č. 1 x 100%
Na základě čeho je posuzováno	1. Kolik má poskytovatel důvěryhodných systémů? Pro každý důvěryhodný systém: 2. Je možný pouze řízený přístup do systému? 3. Jsou zaznamenávány všechny události? 4. Je u každé události zaznamenán jednoznačný identifikátor uživatele, datum a čas, typ události a příkaz, který byl zadán? 5. Je možné zpětně ověřovat integritu záznamů o událostech?

	6. Je možné zjistit, zda došlo v systému k porušení bezpečnostních opatření?
Zdroje dat pro určení míry	Záznamy o událostech, dokumentace důvěryhodných systémů, zprávy z auditu.
Interpretace míry	Požadavek na zaznamenávání událostí musí být splněn uplatněním opatření, která jsou rozvedena výše. Je vhodné, aby poskytovatele systém varoval v případě, že dojde k podezřelému jednání uživatelů. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.3.2 Uchovávání souvisejících údajů

Kvalifikovaný poskytovatel certifikačních služeb dále uchovává informace a dokumentaci související s poskytovanými kvalifikovanými certifikačními službami podle tohoto zákona, zejména

a) smlouvu o poskytování kvalifikované certifikační služby, včetně žádosti o poskytování služby,

b) vydaný kvalifikovaný certifikát, vydaný kvalifikovaný systémový certifikát nebo vydané kvalifikované časové razítko,

c) kopie předložených osobních dokladů podepisující osoby nebo dokladů, na jejichž základě byla ověřena identita označující osoby,

d) potvrzení o převzetí kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu držitelem, případně jeho souhlas se zveřejněním kvalifikovaného certifikátu v seznamu vydaných kvalifikovaných certifikátů,

e) prohlášení držitele certifikátu o tom, že mu byly poskytnuty informace o přesných podmínkách pro využívání kvalifikovaných certifikačních služeb,

f) dokumenty a záznamy související s životním cyklem vydaného kvalifikovaného nebo kvalifikovaného systémového certifikátu.

Požadavek – měřený atribut	Uchovávání informací a dokumentace související s poskytovanými kvalifikovanými certifikačními službami.
Účel míry	Uchovává poskytovatel všechny požadované informace a dokumentaci?
Činnosti, které je nutné provádět pro splnění požadavku	Při každém vydání kvalifikovaného certifikátu dochází k vytvoření příslušné dokumentace, případně ji předá žadatel registrační autoritě, nebo je jen ověřeno, zda již taková dokumentace existuje. Dokumentace je zkontrolována registrační autoritou a následně vhodným způsobem uložena.
Metoda měření	Procento kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek, která byla vydána, a poskytovatel k nim má odpovídající dokumentaci, a to ze všech vydaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek za sledované období (např. 1 měsíc).
Vzorec pro výpočet	Počet kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek, u kterých jsou uchovány všechny požadované údaje (na otázky 1-4 a 6 a 7 v případě kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů je odpověď kladná, a na otázku 5 je kladná odpověď v případě, že je certifikát určen ke zveřejnění. V případě kvalifikovaných časových razítek jsou kladné odpovědi na otázky 1 a 2) ve sledovaném období / počet všech vydaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek dle otázky 8 x 100%

Na základě čeho je posuzováno	Pro každý vydaný kvalifikovaný certifikát, kvalifikovaný systémový certifikát a kvalifikované časové razítko ve sledovaném období: 1. Je uchována smlouva o poskytování kvalifikované certifikační služby a žádost o ni? 2. Je uchován vydaný kvalifikovaný certifikát, kvalifikovaný systémový certifikát a kvalifikované časové razítko? 3. Jsou uchovány kopie dokladů, kterými žadatel o kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát prokázal identitu? 4. Je uchováno potvrzení o převzetí kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu? 5. Je v případě, že byl vydán certifikát, u kterého dal jeho držitel souhlas se zveřejněním, uchován doklad o tomto souhlasu? 6. Je uchováno prohlášení držitele certifikátu, že byl seznámen s přesnými podmínkami pro využívání kvalifikovaných certifikačních služeb? 7. Jsou uchovány dokumenty související s životním cyklem daného certifikátu? 8. Kolik bylo ve sledovaném období vydáno kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek?
Zdroje dat pro určení míry	Seznam kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů, úložiště vydaných kvalifikovaných časových razítek, dokumentace o kvalifikovaných certifikačních službách na registrační autoritě a v úložištích, kde se tato dokumentace uchovává.

Interpretace míry	Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.4 Spolehlivost údajů v certifikátech

Poskytovatel certifikačních služeb musí zajistit, aby údaje uvedené v kvalifikovaných certifikátech a kvalifikovaných systémových certifikátech jím vydaných byly přesné, pravdivé a úplné.

Požadavek – měřený atribut	Je zajištěno, aby byly údaje uvedené ve vydaných certifikátech byly přesné, pravdivé a úplné.
Účel míry	Je u vydaných kvalifikovaných a kvalifikovaných systémových certifikátů zajištěna přesnost, pravdivost a úplnost údajů v nich uvedených?
Činnosti, které je nutné provádět pro splnění požadavku	Pracovník registrační autority a pracovník certifikační autority ověřuje, zda v údajích není překlep, případně jiná chyba. Pracovník registrační autority ověřuje, zda se údaje v žádosti shodují s údaji v předložených dokumentech a následně i v certifikátu.
Metoda měření	Procento certifikátů, u kterých se při následné kontrole zjistí nesoulad s údaji v kopiích/originálech dokumentů, na jejichž základě byl certifikát vydán. Měření se provede na vzorku certifikátů ve zvoleném intervalu.
Vzorec pro výpočet	Počet certifikátů, u nichž byla na otázku 2 kladná odpověď / počet všech certifikátů x 100%
Na základě čeho je posuzováno	Pro každý certifikát: 1. Podařilo se vyhledat dokumenty, na jejichž základě byl certifikát vydán? 2. Jsou údaje v certifikátu shodné s údaji v dokumentech?

Zdroje dat pro určení míry	Dokumenty, na jejichž základě jsou vydávány certifikáty, seznam a úložiště certifikátů.
Interpretace míry	Podmínkou pro vyhodnocení je dostupnost dokumentů, na jejichž základě byl certifikát vydán – posouzení, zda je splněn požadavek zákona na uchování dokumentace, je tedy v podstatě prováděno i při tomto měření. Při měření je nutné uvažovat i velmi pravděpodobnou situaci, ke které dojde v případě, že by byl certifikát vydán s nepřesnými údaji – s největší pravděpodobností dojde k jeho zneplatnění. Pokud došlo ke zneplatnění v krátké době, např. na základě následné kontroly pracovníka registrační autority, je nutné vydání takového certifikátu považovat za méně závažné než v případě existence certifikátu s chybnými údaji, který v krátké době zneplatněn nebyl. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.5 Provozování seznamů

Poskytovatel musí provozovat a zveřejňovat seznamy související s jeho službami. Jdná se o seznam vydaných certifikátů a seznam zneplatněných certifikátů. Tyto údaje jsou potřebné pro zajištění důvěry pro spoléhající se stranu.

6.5.1 Seznam certifikátů

Poskytovatel musí zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných a kvalifikovaných systémových certifikátů, k jejichž zveřejnění dal držitel certifikátu souhlas, a zajistit dostupnost tohoto seznamu i dálkovým přístupem a údaje v seznamu obsažené při každé změně bez zbytečného odkladu aktualizovat.

Tento požadavek je v zákoně o elektronickém podpisu nepřesně formulován a v podstatě se jedná o nesoulad se směrnicí EU o elektronických podpisech – ta totiž požaduje, aby byly certifikáty veřejně přístupné pro vyhledávání, nikoliv aby existoval jejich úplný seznam (zákon vlastně ani neříká, že mají být k dispozici certifikáty, jak to požaduje směrnice EU). Obvyklá praxe také není zveřejnění úplného seznamu certifikátů, protože by jej některé subjekty mohly zneužívat pro svůj obchodní zájem.

Tento požadavek zákona tedy v praxi není poskytovateli striktně dodržován, s ohledem na to, že požadavek směrnice EU o elektronických podpisech zní odlišně – metrika je tedy navržena pro posouzení dostupnosti certifikátů a nikoliv jejich seznamu.

Požadavek – měřený atribut	Je zajištěna dostupnost vydaných kvalifikovaných a kvalifikovaných systémových certifikátů, s jejichž zveřejněním dal držitel certifikátu souhlas.
Účel míry	Je u vydaných kvalifikovaných a kvalifikovaných systémových certifikátů, které mají být zveřejněny, zajištěna dostupnost?
Činnosti, které je nutné provádět pro splnění požadavku	Poskytovatel vytvořil mechanismus, jak vyhledat certifikát, který byl vydán a s jehož zveřejněním dal jeho držitel souhlas. Poskytovatel zajišťuje dostupnost tohoto mechanismu na webových stránkách. Po vyhledání je možné certifikát zobrazit. Poskytovatel zajišťuje dostupnost certifikátů, které lze vyhledat.

Metoda měření	Procento certifikátů, které se podařilo vyhledat a zobrazit, ze všech hledaných certifikátů, v průběhu měření (přičemž nesmí být započítány případy, kdy došlo k chybě na serveru u toho, kdo se snaží certifikát vyhledat)
Vzorec pro výpočet	Počet certifikátů, u nichž byla na otázky 3 a 4 kladná odpověď / počet všech hledaných certifikátů x 100%
Na základě čeho je posuzováno	Pro každý hledaný certifikát: 1. Existuje vyhledávací funkce? 2. Lze zobrazit vyhledaný certifikát? 3. Podařilo se certifikát vyhledat? 4. Podařilo se certifikát zobrazit?
Zdroje dat pro určení míry	Záznamy o událostech v průběhu měření.
Interpretace míry	Požadavek na vyhledání certifikátů může být splněn pouze tehdy, pokud existuje vyhledávací funkce, tato funkce je dostupná a bezporuchová, a pokud existuje databáze obsahující certifikáty, které je možné na základě vyhledání zobrazit. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.5.2 Seznam zneplatněných certifikátů

V zákoně dále následuje požadavek na zajištění provozování bezpečného a veřejně přístupného seznamu kvalifikovaných a kvalifikovaných systémových certifikátů, které byly zneplatněny, a to i dálkovým přístupem. Nesplnění tohoto požadavku by bylo závažným problémem – protože na seznam zneplatněných certifikátů se spoléhá ověřující osoba, a pokud není dostupný, nemůže se dostatečně přesvědčit o platnosti certifikátu. To by mohlo

být nepříjemné i pro poskytovatele, který by nesl odpovědnost za to, že svým nedůsledným jednáním způsobil škodu.

Požadavek – měřený atribut	Je zajištěna dostupnost seznamu zneplatněných certifikátů dálkovým způsobem?
Účel míry	Je u seznamu zneplatněných certifikátů zajištěna dostupnost?
Činnosti, které je nutné provádět pro splnění požadavku	Pokud dojde ke zneplatnění certifikátu, je nutné, aby bylo sériové číslo tohoto certifikátu uvedeno v seznamu zneplatněných certifikátů. Seznam zneplatněných certifikátů musí být dostupný v elektronické formě, a to na místě uvedeném v daném certifikátu. Je zajištěna nepřetržitá dostupnost seznamu zneplatněných certifikátů. Seznam zneplatněných certifikátů má být dostupný i „neelektronickou“ cestou – poskytovatel certifikačních služeb si ve své certifikační politice určuje, jakým způsobem dává seznam zneplatněných certifikátů k dispozici – většinou je ho možné získat na registračních autoritách na disketě.
Metoda měření	Procento případů, kdy byl seznam zneplatněných certifikátů dostupný, a to ze všech pokusů o získání seznamu zneplatněných certifikátů za určitý časový úsek (přičemž nesmí být započítány případy, kdy došlo k chybě na serveru u toho, kdo se snaží seznam zneplatněných certifikátů získat)
Vzorec pro výpočet	Počet případů, ve kterých byla na otázku 2 kladná odpověď / počet všech pokusů o získání seznamu zneplatněných certifikátů x 100%

Na základě čeho je posuzováno	Pro každý pokus o získání seznamu zneplatněných certifikátů: 1. Je v certifikátu uvedena adresa, na které je dostupný seznam zneplatněných certifikátů? 2. Lze získat seznam zneplatněných certifikátů? 3. Pokud seznam zneplatněných certifikátů nelze získat, je v certifikátu uvedena další adresa, na které má být dostupný seznam zneplatněných certifikátů? (pokud ano → bod 2)
Zdroje dat pro určení míry	Záznamy o událostech v průběhu měření.
Interpretace míry	Požadavek na dostupnost seznamu zneplatněných certifikátů (CRL) lze splnit pouze tehdy, pokud je v certifikátu uveden údaj o tom, kde lze CRL získat. V současnosti poskytovatelé v ČR umožňují přístup k CRL přes protokol HTTP, alternativou je přístup přes protokol adresářové služby LDAP. V certifikátu může být uvedeno víc adres, na nichž je CRL k dispozici – v takovém případě je nutné, pokud z jedné z uvedených adres nebylo možné CRL získat, vyzkoušet i případné další adresy. Podstatné je, aby bylo CRL daného poskytovatele dostupné alespoň na jednom z míst uvedených v certifikátu. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.6 Určení data a času

Poskytovatel má zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný nebo kvalifikovaný systémový certifikát vydán nebo zneplatněn, mohly být přesně určeny.

Požadavek – měřený atribut	Je zajištěno, aby bylo možné přesně určit datum a čas, kdy byl certifikát vydán nebo zneplatněn.
Účel míry	Je vždy možné přesně určit datum a čas, kdy byl certifikát vydán nebo zneplatněn?
Činnosti, které je nutné provádět pro splnění požadavku	Poskytovatel certifikačních služeb musí zajistit, aby měl k dispozici zdroj přesného času. Pokud dojde k vydání certifikátu, musí poskytovatel zaznamenat přesný čas, kdy byl certifikát vydán. Pokud dojde ke zneplatnění certifikátu, musí poskytovatel zaznamenat přesný čas, kdy k tomuto zneplatnění došlo, a uvést tento údaj na seznamu zneplatněných certifikátů[19].
Metoda měření	Procento případů, kdy je u certifikátu možné zjistit přesný údaj o datu a času jeho vydání a případně zneplatnění.
Vzorec pro výpočet	Počet případů, ve kterých byla na otázku 2 kladná odpověď / počet všech pokusů o získání přesného data a času vydání nebo zneplatnění certifikátu x 100%
Na základě čeho je posuzováno	1. Je v certifikační politice uvedeno, jak/kde je možné zjistit přesné datum a čas vydání a zneplatnění certifikátu? Pro každý pokus o získání údaje o datu a času vydání nebo zneplatnění certifikátu:

[19] Požadavek na určení přesného času vydání certifikátu je zaveden směrnicí o elektronických podpisech [3]. V praxi je však podstatným údajem pro spoléhající se stranu datum a čas, odkdy je certifikát platný, což je údaj, který se s časem vydání nemusí shodovat – proto poskytovatel údaj o okamžiku vydání certifikátu zaznamenává a dává k dispozici, ale v certifikátu tento údaj uveden není (není pro něj vyhrazená položka). Problém zjevně vznikl díky tomu, že v době vytváření směrnice o elektronických podpisech neměli její tvůrci dostatek praktických zkušeností s touto problematikou.

	2. Lze zjistit datum a čas vydání nebo zneplatnění certifikátu (čas vydání musí být možné získat vždy, čas zneplatnění pouze pokud ke zneplatnění došlo, takže u zneplatněného certifikátu musí být k dispozici oba údaje, aby byla odpověď kladná)?
Zdroje dat pro určení míry	Záznamy o událostech v průběhu měření. Seznamy zneplatněných certifikátů. Seznam vydaných certifikátů.
Interpretace míry	Předpokladem pro vyhledání údaje je jeho zpřístupnění poskytovatelem – to může být v případě údaje o datu a času vydání certifikátu problematické. Pokud došlo ke zneplatnění certifikátu, seznam zneplatněných certifikátů obsahuje datum a čas zneplatnění jako povinnou položku. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.7 Poskytování informací o certifikačních službách

Poskytovatel musí poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných a kvalifikovaných systémových certifikátů, včetně omezení pro jejich použití, a informace o tom, zda je či není akreditován Ministerstvem informatiky; tyto informace lze poskytovat elektronicky.

Požadavek – měřený atribut	Poskytovatel poskytuje na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných a kvalifikovaných systémových certifikátů, včetně omezení pro jejich použití, a informace o tom, zda je či není akreditován Ministerstvem informatiky.

Účel míry	Je vždy možné získat informace o podmínkách poskytování certifikačních služeb?
Činnosti, které je nutné provádět pro splnění požadavku	Poskytovatel musí poskytovat uvedené informace – to je možné realizovat na registračních autoritách nebo prostřednictvím telefonní služby či Internetu. Musí být dostupná informace o tom, na jakém místě je možné tyto informace získat.
Metoda měření	Procento případů, kdy bylo možné získat požadované informace.
Vzorec pro výpočet	Počet případů, ve kterých byla na otázku 2 kladná odpověď / počet všech pokusů o získání požadované informace x 100%
Na základě čeho je posuzováno	1. Je v certifikační politice nebo v jiném dostupném dokumentu uvedeno, jak/kde je možné získat údaje o podmínkách poskytování certifikačních služeb? Pro každý pokus o získání informace o podmínkách pro využívání kvalifikovaných a kvalifikovaných systémových certifikátů, nebo informace o omezení pro jejich použití, nebo informace o tom, zda je či není akreditován ministerstvem: 2. Lze získat požadovanou informaci?
Zdroje dat pro určení míry	Záznamy o událostech v průběhu měření. Pokud informace není dostupná na Internetu, je nutné zahrnout i údaje získané od poskytovatele certifikačních služeb telefonicky či v provozovně.

Interpretace míry	Předpokladem pro získání informace je zjištění, na jakém místě je možné ji získat. Je v zájmu poskytovatele, aby poskytoval informace o jím poskytovaných službách, a to v nejlepším případě automatizovaným způsobem, tj. na Internetu. Jinak bude mít vysoké náklady spojené s plněním této povinnosti. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100.

6.8 Zneplatňování certifikátů

Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované nebo kvalifikované systémové certifikáty, musí neprodleně zneplatnit certifikát, pokud o to držitel, podepisující osoba nebo označující osoba požádá, nebo pokud ho uvědomí, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů nebo elektronických značek, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů. Podle vyhlášky [53] musí poskytovatel umožnit požádat o zneplatnění nejméně dvěma na sobě nezávislými způsoby. Podle CWA 14167-1 [17] nesmí doba od přijetí žádosti o zneplatnění do změny statutu certifikátu na seznamu zneplatněných certifikátů překročit 24 hodin.

Požadavek – měřený atribut	Zneplatňuje poskytovatel v uvedených případech neprodleně certifikát?
Účel míry	Je možné vždy zneplatnit certifikát, a to dostatečně rychle?
Činnosti, které je nutné provádět pro splnění požadavku	Poskytovatel musí stanovit minimálně 2 způsoby, jak je možné požádat o zneplatnění certifikátu. Poté, co obdrží poskytovatel žádost o zneplatnění a ověří identitu žadatele a jeho oprávnění k provedení

	zneplatnění, musí tuto událost zaznamenat a předat sériové číslo certifikátu a přesný čas, kdy má ke zneplatnění dojít, na místo, kde dochází k vydávání seznamu zneplatněných certifikátů (tato činnost může být prováděna i automatizovaně na základě zaslání elektronicky podepsané žádosti o zneplatnění). Poté, co je informace na toto místo předána, musí být daný certifikát zařazen na nejbližší seznam zneplatněných certifikátů s přesným časem, kdy žadatel požádal o zneplatnění.
Metoda měření	Procento případů, kdy se podařilo oprávněné osobě požádat o zneplatnění certifikátu a certifikát byl zařazen včas na správný seznam zneplatněných certifikátů.
Vzorec pro výpočet	Počet případů, ve kterých byla na otázku 2 kladná odpověď & (na otázku 3 záporná odpověď nebo (na otázku 3 kladná odpověď & na otázku 4 kladná odpověď & na otázku 5 kladná odpověď)) / počet všech pokusů o zneplatnění certifikátu x 100%
Na základě čeho je posuzováno	1. Je v certifikační politice nebo v jiném dokumentu dostupném podepisující osobě a držiteli certifikátu uvedeno, jakými dvěma způsoby je možné požádat o zneplatnění certifikátu? Pro každý pokus (přičemž je nutné vyzkoušet oba způsoby žádání o zneplatnění) o zneplatnění certifikátu: 2. Bylo správně posouzeno oprávnění žadatele o zneplatnění certifikátu? 3. Pokud ano, byla osoba oprávněna certifikát zneplatnit?

	4. Pokud ano, byl certifikát zneplatněn (tj. jeho sériové číslo je uvedeno na seznamu zneplatněných certifikátů) do 24 hodin? 5. Odpovídá čas zneplatnění době podání žádosti o zneplatnění?
Zdroje dat pro určení míry	Záznamy o událostech v průběhu měření. Seznamy zneplatněných certifikátů.
Interpretace míry	Předpokladem pro provedení zneplatnění je zjištění, jakým způsobem je možné o něj požádat. Poskytovatel musí tyto informace poskytnout jako jednu ze základních informací o poskytování jeho služeb. Poskytovatel nesmí umožnit zneplatnit certifikát osobě, která k tomu není oprávněna. Pokud se však prokazatelně dozví, že má certifikát zneplatnit (přijde mu žádost o zneplatnění), musí operaci zneplatnění provést ihned – důvodem pro zneplatnění může být skutečnost, že podepisující osoba nemá soukromý klíč pod svou výhradní kontrolou. V takovém případě by mohlo mít otálení dramatické důsledky. Výsledek může být z intervalu $0 \leq X \leq 100$, v ideálním případě by byl roven 100. Tato metrika by mohla být doplněna tak, aby zohledňovala dobu, jaká maximálně uplyne od žádosti o zneplatnění po zařazení na seznam zneplatněných certifikátů. Kvalita služeb poskytovatele se pak zkracováním této doby může ještě více zlepšovat.

6.9 Vydávání časových razítek

Poslední metrika je navržena pro stanovení úrovně plnění zákonné povinnosti kvalifikovaného poskytovatele certifikačních služeb, pokud vydává

kvalifikovaná časová razítka. Kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

Je problematické určit obsah pojmu „neprodleně“. Obecně v právních předpisech výraz neprodleně znamená, že od chvíle, kdy se ten, kdo má konat neprodleně, dozví o tom, že má danou činnost vykonat, nemá provádět nic jiného, než právě tuto činnost. Protože však obvykle časová razítka vydává server, je navržena hodnota půl hodiny jako maximální možná. Problémem může být nevydání časového razítka v delším časovém horizontu, případně skutečnost, že časové razítko nebylo vydáno vůbec.

Samozřejmě je nutné počítat v rámci měření i s tím, že místo časového razítka může být vráceno chybové hlášení a časové razítko nemusí být získáno – to je standardní postup (může k němu dojít např. i v případě chybného formátu zaslané žádosti o časové razítko) a v takovém případě je při provádění měření nutné tuto variantu posuzovat podobně, jako kdyby bylo vydáno časové razítko.

Požadavek – měřený atribut	Poskytovatel vydává kvalifikovaná časová razítka neprodleně po přijetí žádosti o jeho vydání.
Účel míry	Vydává poskytovatel časová razítka v dostatečně krátké době od zaslání žádosti?
Činnosti, které je nutné provádět pro splnění požadavku	Poskytovatel musí neprodleně po přijetí žádosti o časové razítko zajistit jeho vydání. Většinou se za tímto účelem využívá server, který provádí všechny potřebné události automatizovaně. Z toho důvodu je nutné, aby uplatnil poskytovatel dostatečná bezpečnostní opatření, aby byl tento server dostupný a mohl časová razítka v co nejkratší době vydat. Z hlediska následné kontroly je vhodné zaznamenávat události související s činnostmi od okamžiku přijetí žádosti po vydání časového razítka.

Metoda měření	Počet časových razítek za sledované období, která byla vydána za delší dobu než 30 minut.
Vzorec pro výpočet	Počet případů, ve kterých byla na otázku 2 kladná odpověď
Na základě čeho je posuzováno	Pro každý pokus o získání časového razítka: 1. Bylo vydáno časové razítko nebo odesláno chybové hlášení? 2. Trvalo vydání časového razítka (nebo zaslání chybového hlášení) déle než 30 minut?
Zdroje dat pro určení míry	Záznamy o událostech v průběhu měření.
Interpretace míry	Výsledek může být z intervalu $0 \leq X \leq n$ (přičemž n je počet pokusů o získání časového razítka), v ideálním případě by byl roven 0. Pokud dojde k tomu, že razítko (nebo chybové hlášení) vůbec nebylo zasláno, jedná se o vážný problém. Otázka stanovení „hranice akceptovatelnosti“ je dána zejména politikou poskytovatele, který si může stanovit, jaká je maximální doba, do které musí časové razítko vydat. V případě, že by bylo problematické si stanovit maximální dobu, kterou nemá doba od přijetí žádosti po vydání časového razítka přesáhnout, je možné pouze určit maximální dobu, která uplynula od přijetí žádosti po vydání časového razítka.

Poskytovatel certifikačních služeb disponuje velmi komplexním systémem, jehož velmi podstatným a nejzranitelnějším místem jsou lidé. Postihnout činnost osob obecně (které nemusí být zaměstnanci poskytovatele, naopak se předpokládá využití služeb zajišťovaných jinými subjekty, např. formou outsourcingu) lze obtížně, vzhledem k tomu, že je každý člověk

individualita (narozdíl od počítačového programu). Navrhované metriky tedy spíše postihují základní a spíše technologické prvky důvěryhodných systémů a jejich základní vlastnosti.

Samotným zredukováním komplexního systému do tabulky dojde k jistému zkreslení situace. Protože zde byly navrženy metriky pro základní charakteristiky důvěryhodných systémů, není možné, aby některý požadavek nebyl splněn. Jde tedy spíše o to, do jaké míry jsou požadavky plněny. Následně by tyto metriky měly napomoci porovnávání úrovně kvality měřených atributů.

Problematika důvěryhodných systémů kvalifikovaných poskytovatelů certifikačních služeb je velmi komplexní, proto by bylo možno nalézt velmi mnoho metrik – avšak jejich vypovídací hodnota pro toho, kdo posuzuje splnění předpokladů pro poskytování kvalifikovaných certifikačních služeb, by byla nízká – proto je nutné metriku vytvořit pouze pro kriteria, jejichž nesplnění by indikovalo nedodržení požadavků zákona. Poskytovatel by měl mít zpracovánu hlubší strukturu, díky které může indikovat potenciální problémy ve svém systému – proto musí provádět kontrolu bezpečnostní shody a zajistit provedení auditu systému managementu bezpečnosti informací.

Nebezpečím těchto zjednodušených „přehledů reality“ je opomenutí podstatné vlastnosti, na kterou při vytváření metrik nebylo pamatováno – například právě díky formalizované struktuře, která je všem známa. Proto je nutné (stejně jako u všech ostatních exaktních disciplin aplikovaných na reálný život) provést i subjektivní hodnocení globálního fungování důvěryhodných systémů poskytovatele. Především je nutné zabránit tomu, aby nevhodnou implementací požadavku nedošlo k výraznému snížení celkové efektivity činností poskytovatele.

Toto základní posouzení nejdůležitějších požadavků zákona je vhodné provést při větších změnách v důvěryhodných systémech poskytovatele jako minimalistickou kontrolu – navržené metriky slouží ke stanovení úrovně plnění zákonných požadavků, jejichž nesplnění může vést k fatálním důsledkům.

7 ZÁVĚR

7.1 Zhodnocení dosažení cílů práce

Cílem práce bylo vytvoření metodiky, podle níž je možné postupovat při poskytování kvalifikovaných certifikačních služeb.

Tato disertační práce vytváří ucelenou představu o problematice poskytování certifikačních služeb, a to zejména kvalifikovaných certifikačních služeb, na základě studia literatury a konzultací s odborníky na danou problematiku. Tento dokument obsahuje metodiku pro poskytovatele certifikačních služeb, kteří chtějí být akreditovanými poskytovateli certifikačních služeb v souladu se zákonem o elektronickém podpisu a vyhláškou [53].

Disertační práce postupuje od matematické teorie přes jednotlivé technické prvky, požadavky zákona o elektronickém podpisu, až po nejvyšší organizačně – řídící nadstavbu nutnou pro poskytování důvěryhodných certifikačních služeb. Analyzuje všechny související normy a předpisy upravující poskytování certifikačních služeb, bezpečné postupy poskytovatelů certifikačních služeb a bezpečnost informací. Je zohledněna situace v České republice, ale i v Evropské unii, v jejímž prostoru se pohybujeme a se kterým je nutné být v souladu. Na základě analýzy je vytvořena metodika pro poskytování certifikačních služeb.

Disertační práce v souladu se svým cílem navrhuje metriky, které jsou určeny auditorům nebo dalším subjektům vykonávajícím akreditaci, kontroly či dozor, při posuzování plnění základních požadavků kladených na poskytovatele certifikačních služeb. Vzhledem ke komplexnosti důvěryhodných systémů, které mají poskytovatelé certifikačních služeb, byly navrženy pouze metriky pro zákonné požadavky na kvalifikované poskytovatele certifikačních služeb.

7.2 Přínosy práce pro vědu a praxi

Disertační práce obsahuje unikátní ucelený přehled o poskytování certifikačních služeb. Jedná se o rozsáhlou analýzu požadavků na poskytování certifikačních služeb, jejich souvislostí a postupů, kterými lze požadavky naplnit.

Informace obsažené v této práci nevycházejí pouze z teorie, ale uplatňují se v ní i praktické zkušenosti s navrženými postupy.

Protože se autorka této práce podílela na tvorbě vyhlášky, jejíž požadavky jsou v práci dále rozvedeny, je pro praxi užitečné, že existuje metodika, která vysvětluje, jak všechny požadavky vyhlášky implementovat a ověřit jejich plnění. Metodika je vytvořena na základě praktických zkušeností s poskytovateli certifikačních služeb a na základě informací získaných při komunikaci s odborníky na tuto problematiku z členských států EU. Principy metodiky byly ověřeny i v praxi, a to právě díky zmíněné vyhlášce a zpětné vazbě ze strany poskytovatelů.

Oblastí poskytování certifikačních služeb se zabývá pouze omezená skupina subjektů, proto je metodika unikátním zdrojem informací pro všechny další návrhy na zdokonalování v této oblasti. Vzhledem k rychlému rozvoji ve využívání informačních technologií a Internetu lze očekávat tlak na změny a vytváření dalších možností využívání certifikačních služeb. Jistě se bude jednat o širší využití certifikátů pro autentizaci či šifrování při komunikaci s veřejnou správou. Přestože dosud neexistují v České republice ani v Evropské unii pravidla pro tuto oblast, jistě by měla vycházet z údajů obsažených v této práci.

Přínosem této práce je i návrh metrik, díky nimž je možné porovnávat úroveň splnění požadavků kladených na poskytovatele certifikačních služeb. V průběhu tvorby této práce již došlo k praktickému uplatnění některých navržených metrik při provádění státní kontroly u akreditovaného poskytovatele certifikačních služeb. Za tímto účelem bude možné využívat i další metriky v závislosti na zaměření kontrol či auditů.

7.3 Náměty pro další zkoumání

Metodiku je možné rozšiřovat v závislosti na potřebách poskytovatelů a auditorů. Je vhodné ji průběžně aktualizovat na základě zkušeností s jejím využitím.

Metriky jsou navrženy pro atributy, které vycházejí ze zákonných požadavků, proto je možné navrhnout další metriky pro požadavky vyhlášky a norem, které jsou v podstatě podrobnějším rozkladem a zpřesněním zákonných požadavků. Použití navržených metrik je též vhodné dále ověřit v praxi.

Poskytování kvalifikovaných certifikačních služeb je jednou z oblastí, jejíž existence je nutná pro usnadnění komunikace prostřednictvím Internetu, protože umožňuje provádět některé z činností běžného světa, které ve světě počítačů není snadné zajistit. Vnáší do anonymního světa prvek důvěryhodného ověření identity a podpisu – tedy projevu vůle. Zprostředkování těchto služeb však musí být svěřeno do kompetentních rukou, které musí mít vnitřní mechanismy pro zlepšování vlastní činnosti. Lze očekávat, že v budoucnu se budou digitálně podepisovat smlouvy na velmi vysoké částky nebo zdravotnické záznamy. Pak je důvěryhodná činnost poskytovatelů certifikačních služeb zásadní. Disertační práce slouží jako model efektivních postupů kvalifikovaných poskytovatelů certifikačních služeb.

8 SEZNAM LITERATURY

[1] Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb. *Sbírka zákonů Česká republika. Částka 167.* Tiskárna Ministerstva vnitra, 2004. 16 s.

[2] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). *Sbírka zákonů Česká republika. Částka 68.* Tiskárna Ministerstva vnitra, 2000. 16 s.

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[4] PINKAVA, Jaroslav
Úvod do kryptologie [online]. květen 1998, poslední změna: 24.7.2000 [cit. 2001-12-15]. URL: http://www.aec.cz/aecweb2.zip.

[5] NEZDAROVÁ, Lenka
Nové trendy v symetrickém šifrování: diplomová práce. Praha: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2002. 77 s.

[6] PKCS #1
RSA Cryptography Standard. v2.1, Bedford: RSA Laboratories. June 14, 2002 [cit. 2005-15-06]. 62 s.
URL: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html.

[7] MAZZOCCHI, Daniele
Chapter 9: hash function [online]. 01-Feb-2002 [cit. 2005-06-08].
URL: http://sconce.ics.uci.edu/seminar/slides/chap9new.ppt.

[8] PINKAVA, Jaroslav
Hashovací funkce v roce 2004 [online]. říjen 2004 [cit. 2005-05-08].
URL: http://crypto-world.info/pinkava/clanky/hash_2004.pdf.

[9] SCHNEIER, Bruce
A free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography [serial online]. Counterpane, Inc., 1998- [cit. 2005-07-30].
URL: http://www.counterpane.com/crypto-gram.html.

[10] XIAOYUN, Wang [1]; DENGGUO, Feng [2]; XUEJIA, Lai [3]; HONGBO, Yu [1]
Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD [online], The School of Mathematics and System Science, Shandong University, Jinan250100, China [1]; Institute of Software, Chinese Academy of Sciences, Beijing100080, China [2]; Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, China [3]; rump session, Crypto 2004, 2004, revised on August 17, 2004 [cit. 2005-08-05].
URL: http://eprint.iacr.org/2004/199.pdf.

[11] HOUSLEY, R.; POLK W.; FORD, W.; SOLO, D
IETF RFC 3280, *Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile* [online], April 2002 [cit. 2005-06-11].
URL: http://www.rfc.net/rfc3280.html.

[12] *How PGP works* [online]. [cit. 2005-06-15]
URL: http://www.pgpi.org/doc/pgpintro/.

[13] PETERKA, Jiří
eArchiv Jiřího Peterky: Bezpečnost na Internetu: Strom důvěry, nebo pavučina důvěry? [online]. [cit. 2005-07-25].
URL: http://www.earchiv.cz/b01/b0100016.php3.

[14] CHADWICK, David W.
Security and Protection of Information: Introduction to PKIs, Brno, 3.-5. května 2005.

[15] ETSI TS 102 231
Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information [online], v.1.1.1., Sophia Antipolis Cedex: ETSI, 2003-10 [cit. 2005-07-08]. 59 s.
URL: http://portal.etsi.org/docbox/esi/Open/ts_102231v010101p.pdf.

[16] BUENE, Leif; ØLNES Jon; ØVERLAND Trond
Validation Authority Services: PKI interoperability by an independent trusted Validation Authority. Oslo: DNV, 21.6.2005. 21 s.

[17] CWA 14167-1:2003
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. Brussels: EUROPEAN COMMITTEE FOR STANDARDIZATION, June 2003. 47 s.

[18] ITU-T Recommendation X.509 (1997 E) | ISO/IEC 9594-8
Information Technology - Open Systems Interconnection – The Directory: Authentication Framework. Geneva: International Telecommunication Union, June 1997.

[19] ADAMS, C.; FARRELL, S.
IETF RFC 2510 (1999). *Internet X.509 Public Key Infrastructure Certificate Management Protocols* [online], March 1999 [cit. 2005-06-21].
URL: http://www.rfc.net/rfc2510.html.

[20] MYERS , M.; ADAMS, C.; SOLO, D.; KEMP, D.
IETF RFC 2511 (1999). *Internet X.509 Certificate Request Message Format* [online], March 1999 [cit. 2005-06-21].
URL: http://www.rfc.net/rfc2511.html.

[21] HOUSLEY, R.
IETF RFC 2630 (1999). *Cryptographic Message Syntax* [online], June 1999 [cit. 2005-06-21].
URL: http://www.rfc.net/rfc2630.html.

[22] ADAMS, C.; CAIN, P.; PINKAS, D.; ZUCCHERATO, R.
IETF RFC 3161 (2001). *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)* [online], August 2001 [cit. 2005-06-21].
URL: http://www.rfc.net/rfc3161.html.

[23] CHOKHANI, S.; FORD, W.; SABETT, R.; MERRILL, C.; WU, S.
IETF RFC 3647 (2003). *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Internet X.509 Certificate Request Message Format* [online], November 2003 [cit. 2005-06-21].
URL: http://www.rfc.net/rfc3647.html.

[24] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002
Information Technology — Abstract Syntax Notation One (ASN.1): Specification of Basic Notation. Geneva: International Telecommunication Union, July 2002.

[25] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002
Information Technology — ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER). Geneva: International Telecommunication Union, July 2002.

[26] *Object identifier tree* [online]. Paris: France Telecom, aktualizováno Thu Jul 21 2005 [cit. 2005-07-12]
URL: http://asn1.elibel.tm.fr/en/oid/.

[27] POLK, W.; HOUSLEY, R.; BASSHAM, L.
IETF RFC 3279 (2002). *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [online], April 2002 [cit. 2005-06-21].
URL: http://www.rfc.net/rfc3279.html.

[28] HRAD, Miroslav; RÁČEK, Jaroslav
ČASOVÁ HLEDISKA ELEKTRONICKÉHO PODEPISOVÁNÍ [online], Brno: Masarykova univerzita, Fakulta informatiky, [cit. 2005-08-10].
URL: http://honor.fi.muni.cz/tsw/2003/039.pdf.

[29] ETSI TS 102 023
Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities v.1.2.1., Sophia Antipolis Cedex: ETSI, 2003-01-14. 32 s.

[30] ETSI TS 101 861
Time stamping profile, v.1.2.1., Sophia Antipolis Cedex: ETSI, 2003-01. 32s.

[31] ETSI TS 102 158
Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates, v.1.1.1. Sophia Antipolis Cedex: ETSI, 2003-10. 42 s.

[32] HOBZA, Jan
Elektronický podpis v právní úpravě a praxi: diplomová práce. Praha: Česká zemědělská univerzita, Provozně ekonomická fakulta, 23. dubna 2003. 143 s.

[33] ČSN ISO/IEC 15408
Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT (část 1 až 3). Praha : Český normalizační institut, 2002.

[34] Vyhláška č. 366/2001 Sb. o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu. *Sbírka zákonů Česká republika. Částka 138.* Tiskárna Ministerstva vnitra, 2001. 8 s.

[35] ETSI TS 102 176
Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures, v.1.2.1. Sophia Antipolis Cedex: ETSI, 2005-07-12.

[36] Eastlake, D., Jones, P.
IETF RFC 3174 (2001). *US Secure Hash Algorithm 1 (SHA1)* [online], September 2001 [cit. 2005-07-20].
URL: http://www.rfc.net/rfc3174.html.

[37] Zákon č. 552/1991 Sb., o státní kontrole. *Sbírka zákonů Česká republika. Částka 104.* Tiskárna ministerstva vnitra, 1991. 40 s.

[38] Zákon č. 499/2004 Sb.o archivnictví a spisové službě a o změně některých zákonů. *Sbírka zákonů Česká republika. Částka 173.* Tiskárna ministerstva vnitra, 2004. 40 s.

[39] Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) ve znění pozdějších předpisů. *Sbírka zákonů Česká republika. Částka 171.* Tiskárna ministerstva vnitra, 2004. 8 s.

[40] Vyhláška č. 496/2004 Sb., o elektronických podatelnách. *Sbírka zákonů Česká republika. Částka 171.* Tiskárna ministerstva vnitra, 2004. 8 s.

[41] MINISTERSTVO INFORMATIKY
Zpracovala Nezdarová, L. a kol., *Best practice: Jak vyřizovat elektronickou poštu* [online], verze 2.0. Praha. 2004 [cit. 2005-08-20]. 25 s.
URL: http://www.micr.cz/files/1923/BPvyrizovani-posty.pdf.

[42] Commission decision; 2003/511/EC
Commission Decision 2003/511/EC on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council. Brussels. 14 July 2003. 2 s.

[43] ČSN ISO/IEC 17799
Informační technologie – Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací. Praha: Český normalizační institut, Srpen 2006. 102 s.

[44] ČSN ISO/IEC 27001
Informační technologie – Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, Říjen 2006. 36 s.

[45] ČSN ISO/IEC TR 13335
Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1-3. Praha: Český normalizační institut, 2000. 96 s.

[46] ETSI TS 101 456
Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, v. 1.3.1, Sophia Antipolis Cedex: ETSI, 2005-05. 50s.

[47] CWA 14172
EESSI Conformity Assessment Guidance. Brussels: EUROPEAN COMMITTEE FOR STANDARDIZATION, March 2004. 107 s.

[48] CWA 14167-2
Cryptographic module for CSP signing operations with backup – Protection profile - CMCSOB PP. Brussels: EUROPEAN COMMITTEE FOR STANDARDIZATION, May 2004. 89 s.

[49] CWA 14167-4
Cryptographic module for CSP signing operations – Protection profile - CMCSO PP. Brussels: EUROPEAN COMMITTEE FOR STANDARDIZATION, May 2004. 83 s.

[50] FIPS PUB 140-2
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION; SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES. Gaithersburg: Information Technology Laboratory; National Institute of Standards and Technology, May 25, 2001. 69 s.
URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[51] CWA 14 169
Secure signature-creation devices "EAL 4+". Brussels: EUROPEAN COMMITTEE FOR STANDARDIZATION, May 2004. 219 s.

[52] Národní bezpečnostní úřad
Aktuality; Připojení České republiky k CCRA [online]. Praha, [cit. 2005-08-28].
URL: http://www.nbu.cz/aktualita12.php.

[53] Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích a nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb). *Sbírka zákonů Česká republika. Částka 120.* Tiskárna ministerstva vnitra, 2006. 88 s.

[54] ČSN ISO/IEC 27001
Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2006. 38 s.

[55] Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. *Sbírka zákonů Česká republika. Částka 179.* Tiskárna ministerstva vnitra, 2005. 208 s.

[56] KLÍMA, Vlastimil
Stranka venovana specialni blokove sifre DN, hasovaci funkci HDN a konstrukci SNMAC. [online]. Praha, [cit. 2007-03-28].
URL: http://cryptography.hyperlink.cz/SNMAC/SNMAC_CZ.html.

[57] VANÍČEK, Jiří
Měření a hodnocení jakosti informačních systémů. Praha: Česká zemědělská univerzita, 2000. 211 s.

[58] IT Governance Institute
COBIT 4.; Control Objectives, Management Guidelines, Maturity Models [online]. Rolling Meadows, USA, [cit. 2006-11-18].

[59] SP 800-55

NIST Special Publication 800-55; Security Metrics Guide for Information Technology Systems [online]. Gaithersburg: Information Technology Laboratory; National Institute of Standards and Technology. July 2003.
URL: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf.

[60] SP 800-26

NIST Special Publication 800- 26; Security Self-Assessment Guide for Information Technology Systems [online]. Gaithersburg: Information Technology Laboratory; National Institute of Standards and Technology. November 2001.
URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf.