# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

FAKULTA PROVOZNĚ EKONOMICKÁ

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ



# Elektronický podpis, certifikáty a elektronická komunikace ve státní správě a samosprávě

**Diplomová práce**

Praha 2012 ©


**Vedoucí práce:** RNDr. Dagmar Brechlerová, Ph.D.

**Autor práce:** Vladimír Fousek

# Prohlášení:

Prohlašuji, že jsem diplomovou práci na téma *Elektronický podpis, certifikáty a elektronická komunikace ve státní správě a samosprávě* zpracoval samostatně, pouze za odborného vedení vedoucí diplomové práce, paní RNDr. Dagmar Brechlerové, Ph.D.
Dále prohlašuji, že veškeré podklady, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury.

V Praze dne 31. března 2012

……
Vladimír Fousek

# Poděkování:

Tímto bych chtěl poděkovat vedoucí své diplomové práce paní RNDr. Dagmar Brechlerové, Ph.D. za cenné náměty a připomínky, odborné vedení a za trpělivost a ochotu.

# Elektronický podpis, certifikáty a elektronická komunikace ve státní správě a samosprávě

# The electronic signature, certificates and electronic communications in Public Administration

## Souhrn:

Tato diplomová práce se věnuje problematice elektronického podpisu, certifikátů a bezpečnosti jeho využívání. Práce se dělí na dvě části, část teoretická a část praktická.

Cílem teoretické části je uvést čtenáře do problematiky spojené s elektronickým podpisem. V teoretické části se práce zabývá základy kryptografie, teorií elektronického podpisu a časových razítek, certifikačními autoritami a legislativním rámcem elektronického podpisu.

Cílem praktické části je zaměřit se na bezpečnostní problematiku na straně poskytovatele certifikačních služeb a shrnutí legislativních požadavků na kvalifikované a akreditované poskytovatele certifikačních služeb. Součástí práce je také návrh dokumentu systémové bezpečnostní politiky kvalifikovaného poskytovatele, jakožto jednoho z povinných a stěžejních dokumentů, který musí být součástí bezpečnostní dokumentace.

## Klíčová slova:

Elektronický podpis, elektronická značka, časové razítko, certifikát, poskytovatel certifikačních služeb, symetrická kryptografie, asymetrická kryptografie, certifikační politika, informační bezpečnost, revokace certifikátu, seznam zneplatněných certifikátů.

## Summary:

This diploma thesis deals with the issue of electronic signature certificates and security of its use. The thesis is divided in two parts, the first is theoretical and the second is practical.

The goal of the theoretical part is to introduce readers to the questions associated with electronic signature. The theoretical part deals with the basics of cryptography, the theory of electronic signatures and time stamps, certification authority and the legislative framework of electronic signatures.

The goal of the practical part is to focus on security issues at the side of providers of certification services and requirements summarization for qualified and accredited certification services providers. This part also contents a draft of document called system security policy, which is one of the key document of security documentation required for qualified providers of certification authority.

**Key words:**

Electronic signature, electronic mark, time stamp, certificate, certification service provider, symmetric cryptography, asymmetric cryptography, certification policy, information security, certificate revocation, Certificate Revocation List.

# Obsah

# 1 Úvod

V době výběru tématu mé diplomové práce jsem již několikátým rokem pracoval ve společnosti poskytující certifikační služby a v rámci svých pracovních povinností jsem se podílel na zajištění interních auditů certifikačních služeb. Proto mi téma z oblasti elektronického podpisu a certifikačních služeb bylo velmi blízké a z toho důvodu jsem také uvítal možnost zpracovávat na toto téma svou diplomovou práci.

Problematika elektronického podepisování úzce souvisí s tématy bezpečné elektronické komunikace a informační bezpečnosti. S rostoucím významem informací, které jsou v současné době klíčovým aktivem většiny společností, roste i význam informačních systémů a komunikačních technologií podílejících se na přenosu, zpracování a uchování těchto informací a zvyšují se i nároky na jejich ochranu.

Některé informace, ať už uchovávané v informačním systému v různých podobách, nebo přenášené prostřednictvím elektronické komunikace, je třeba chránit a to zejména proti ztrátě důvěrnosti, dostupnosti nebo integrity.

**Důvěrnost** (Confidentiality) informací znamená, že k informacím mají přístup pouze autorizované subjekty a nikdo jiný.

**Dostupnost** (Availability) informací znamená, že informace je pro autorizovaného uživatele dostupná v okamžiku potřeby.

**Integrita** (Integrity) informací znamená zajištění správnosti a úplnosti informací.

Důvody, proč chránit data, může být zamezení následujících nežádoucích situací:

- porušení legislativy nebo předpisů
- porušení obchodního tajemství
- finančních ztrát
- náhrad penále

Problém uvedených v uvedených případech by mohl vzniknout např. umožněním přístupu k citlivým datům - osobním údajům klientů nebo zaměstnanců, což by bylo porušení legislativy resp. zákona o ochraně osobních údajů, nebo dalším příkladem může být ochrana informací vyplývající např. ze smluvního ujednání, nebo informací strategicky důležitých pro běh firmy a její výnosy, jejichž vyzrazením by firma ztratila konkurenceschopnost. Může se jednat o detaily smluv, informace o klientech apod.

Samozřejmě, že na různé informace jsou kladeny různé požadavky na jejich ochranu.

Například pro informace, které je ze zákona povinnost zveřejňovat v souvislosti s provozovanou činností, nebude asi požadavek na uchování důvěrnosti – informace jsou určené veřejnosti. Naopak bude kladen důraz na zachování dostupnosti a samozřejmě i jejich integrity. V jiném případě mohou být informace chráněné jako obchodní tajemství, tj. budou mít definovaný stupeň důvěrnosti, ale není vyžadována jejich trvalá dostupnost.

Informace, jak již bylo řečeno na začátku kapitoly, mohou být uloženy v nějaké podobě v informačním systému u vlastníka, nebo jejich správce, nebo mohou být přenášena prostřednictvím elektronické komunikace. Pokud je pro data vyžadován nějaký stupeň ochrany, ať už z pohledu důvěrnosti, integrity nebo dostupnosti dat, musí být chráněné nejen uložené informace, ale je potřeba je chránit i během přenosu prostřednictvím elektronické komunikace.

Ochrana informací se tedy dělí do dvou oblastí – ochrana uložených dat u majitele nebo správce dat a ochrana přenášených dat.

V prvním případě mohou být data pod výhradní kontrolou jednoho subjektu a tomu odpovídají i možnosti jejich zabezpečení. Mohou být kombinovány metody fyzické a organizační bezpečnosti, jako je kontrolovaný vstup do prostor, zabezpečení počítačů apod. s metodami logické ochrany dat s využitím kryptografických metod.

Ve druhém případě, kde se jedná o přenos dat, už není možné využít metod fyzické bezpečnosti a jedinou možností je využití možností logické ochrany – šifrování a elektronické podepisování dat.

V následujících kapitolách se práce věnuje zejména elektronickému podepisování, certifikátům a certifikačním autoritám, ale v prvních kapitolách jsou popsány i metody šifrování. Z pohledu tří základních požadavků na bezpečnost informací uvedených výše, řeší metody logické ochrany dvě – důvěrnost a integritu dat, přičemž šifrování dat zajišťuje bezpečnost z pohledu důvěrnosti a elektronické podepisování zajišťuje bezpečnosti dat z pohledu integrity, resp. nepopiratelnosti subjektu, který data podepsal.

# 2 Cíl práce a metodika

Problematika související s elektronickým podepisováním, certifikáty a jejich praktickým využíváním v elektronické komunikaci je velice rozsáhlá a díky tomu existuje mnoho možností zpracování tohoto tématu. Já jsem se rozhodl pojmout tuto práci z části jako teoretickou, která bude obsahovat ucelený pohled na danou problematiku a z části jako praktickou, která bude zaměřena na bezpečnostní problematiku na straně poskytovatele kvalifikovaných certifikačních služeb a bude shrnovat legislativní požadavky se zaměřením na vytvoření bezpečnostní dokumentace. Pro tvorbu diplomové práce jsem použil nástroj *MS Office Professional Edition 2003*.

Při psaní teoretické části diplomové práce jsem čerpal z uvedených zdrojů, z podnětů a připomínek vedoucí mé diplomové práce a částečně ze svých pracovních zkušeností. Výsledkem je ucelený pohled na problematiku elektronických podpisů, certifikátů a certifikačních autorit. Práce začíná popisem základních principů kryptografie, navazuje kapitola popisující elektronické podpisy, certifikáty, časová razítka a certifikační autority.

Pro názornost v textu těchto kapitol doplněny obrázky, které jsem vytvořil v nástroji, který jsem měl k dispozici – *Visio Standard 5.0 for MS Windows*. Při převodu obrázků z formátu *.vsd do formátu obrázku použitelného pro vložení v nástroji MS Office (použil jsem *.jpg) se vyskytl problém u některých českých znaků, proto jsem změnil problematické znaky české abecedy za písmena bez diakritiky.

Praktická část se zabývá problematikou na straně poskytovatele certifikačních služeb shrnutím podmínek pro kvalifikované poskytovatele certifikačních služeb vydávajících kvalifikované certifikáty, se zaměřením na bezpečnostní dokumentaci na straně poskytovatelů. Součástí praktické části je i návrh dokumentu systémová bezpečnostní politika. Při tomto návrhu jsem čerpal z legislativních norem a ze svých pracovních zkušeností.

# 3 Kryptografie

Téma kryptografie úzce souvisí s elektronickým podpisem, protože elektronický podpis je založen na asymetrických kryptografických algoritmech. Proto pro správné pochopení principů elektronického podpisu byla zařazena tato kapitola, která má čtenáře uvést do oblasti zvané kryptografie. Čtenář je seznámen se základy kryptografie a jejími základními pojmy a principy, které jsou technologickým rámcem pro používání elektronického podpisu a certifikátů.

Kryptografie je vědecká disciplína, která se zabývá ochranou dat prostřednictvím jejich šifrování. Úkolem šifrování je změnit data tak, aby je mohla přečíst pouze oprávněná osoba; prostřednictvím šifrování se tedy zajišťuje důvěrnost dat. Vstupem do šifrovacího procesu je otevřený čitelný text, který se během procesu transformuje na šifrovaný, nečitelný text. K tomu se dnes zpravidla využívá šifrovací klíč, symetrický nebo asymetrický viz. následující text. Opačný proces, který naopak z šifrovaného nečitelného textu udělá za pomoci dešifrovacího klíče čitelný text, se nazývá dešifrování. Dřívější označení těchto procesů bylo kryptování a dekryptování.

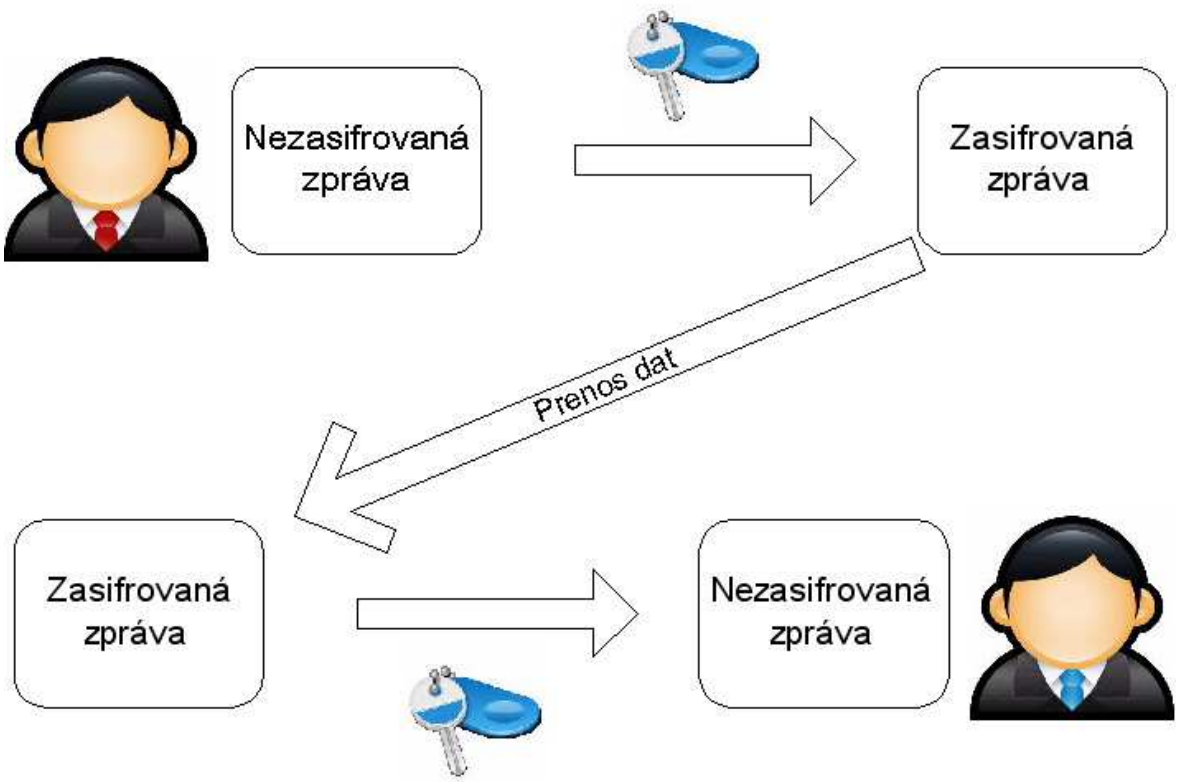
Šifrování a dešifrování může probíhat buď na základě společného tajemství, resp. jediného klíče, který je pak použitý pro oba dva procesy, nebo na základě klíčového páru, přičemž jeden je použitý pro šifrování a druhý pro dešifrování textu. Podle toho pak rozlišujeme symetrickou kryptografii a asymetrickou kryptografii.

Jiné možné rozdělení kryptografických algoritmů je podle množství dat, která jsou šifrována v jednom okamžiku. Algoritmy zpracovávající zprávu jako sekvenci bitů, tedy postupně po jednotlivých bitech, se nazývají proudové. Algoritmy, které zpracovávají text po blocích, se nazývají blokové. Tímto dělením se dále zabývat nebudeme.

## 3.1 Symetrická kryptografie

Metody symetrické kryptografie využívají pouze jeden šifrovací klíč (společné tajemství), který je společný pro oba procesy – šifrování i dešifrování.

Princip je znázorněn na následujícím obrázku:




**Obrázek 1: Princip symetrické kryptografie (vlastní zdroj)**

Symetrická kryptografie je založená na substitučních a transpozičních technikách.

V rámci substituční techniky probíhá nahrazování znaků otevřeného jinými znaky podle předem definovaného předpisu, který se nazývá substituční tabulka.

V rámci transpoziční techniky nedochází k záměně jednotlivých znaků, ale mění se jejich pořadí. Současné symetrické algoritmy (např. AES) pak kombinují obě popsané techniky. Současné používané symetrické algoritmy jsou například TRIPLEDES, IDEA a AES. Pro jednotlivé algoritmy je možné matematickými metodami spočítat náklady a čas potřebný na dešifrování zprávy i bez znalosti šifrovacího klíče. Ovlivnit tento čas je možné volbou délky klíče, resp. pokud je šifrovací klíč dostatečně dlouhý, může být šifra prakticky nedešifrovatelná.

## 3.2 Asymetrická kryptografie

Metody asymetrické kryptografie jsou založené na dvojici klíčů – soukromého klíče (Private Key) a veřejného klíče (Public Key). Ke generování klíčového páru existuje celá řada volně stažitelného SW, nebo lze klíčový pár vygenerovat prostředky operačního systému (např. v OS Unix/Linux příkazem SSH-KEYGEN s příslušnými parametry). Pro

generování klíčového páru musí být použitý takový algoritmus, který zajistí, že z veřejného klíče nebude možné zjistit v reálném čase soukromí klíč uživatele.

Asymetrická kryptografie je založená na ochraně soukromého klíče uživatele. Na rozdíl od symetrické kryptografie, kdy pro šifrování i dešifrování existoval pouze jeden klíč a obě strany tj. šifrující i dešifrující ho musely znát, u asymetrické kryptografie musí být soukromý klíč bezpečně uložen u jeho vlastníka a chráněn před jeho vyzrazením a naopak veřejný klíč musí být zveřejněn vhodným způsobem, aby byl dostupný ostatním subjektům, se kterými je potřeba komunikovat. Pro ochranu soukromého klíče existuje celá řada prostředků. Možnosti ochrany soukromých klíčů jsou zmíněny v podkapitole 3.6.

V současné době jsou nejpoužívanější asymetrické algoritmy RSA a DSA.

Princip asymerických kryptografických algoritmů tedy předpokládá existenci klíčového páru. Jedná se o takové dva klíče, že text, který je zašifrovaný jedním klíčem z páru, je možné v reálném čase dešifrovat pouze druhým klíčem z tohoto páru. Z uvedeného vyplývá, že text zašifrovaný jedním klíčem, není možné tím samým klíčem i dešifrovat.

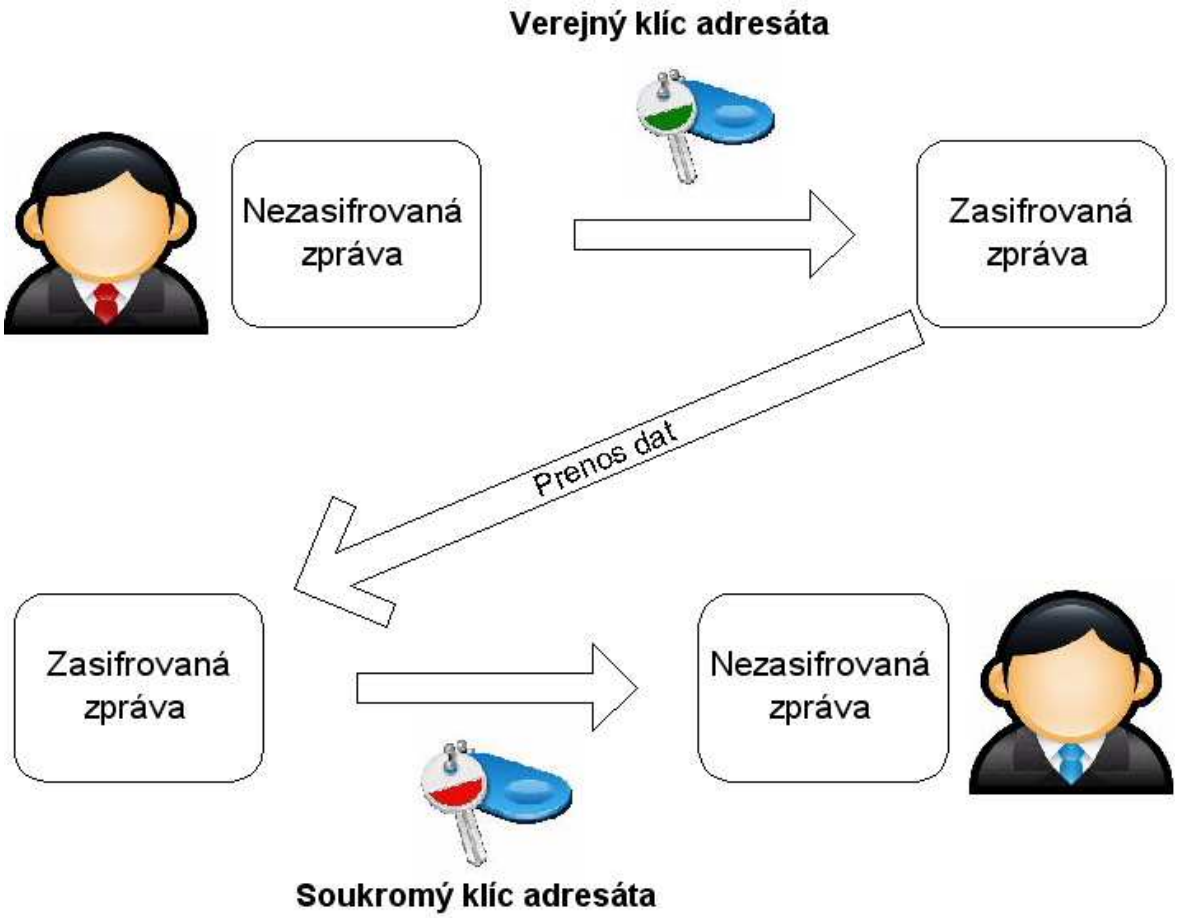
Z pohledu technologie šifrování a dešifrování je jedno, jestli byl text šifrován soukromým klíčem a dešifrován veřejným klíčem, nebo jestli to bylo obráceně.

Záleží na tom ale, jestli má být kryptografický algoritmus použitý pro zašifrování zprávy, resp. použití pro zajištění důvěrnosti textu, který je určen pouze určitému příjemci, nebo jestli má být algoritmus použitý pro autorizaci odesílatele, resp. zajištění nepopiratelnosti vytvoření a podepsání textu odesílatelem a integrity.

### 3.2.1 Šifrování textu

Pro zašifrování otevřeného textu, tj. zajištění jeho čitelnosti pouze pro autorizovaný subjekt, je možné použít veřejný klíč z páru, kde držitelem soukromého klíče je právě autorizovaná osoba. Použití veřejného klíče není problém, je volně dostupný komukoliv a proto každý může provést zašifrování zprávy. Vlastní zašifrování textu nic neříká o tom, kdo to provedl. Jak bylo již řečeno, k dešifrování textu je zapotřebí druhý z páru klíčů, tzn. že text bude moci rozšifrovat pouze autorizovaný subjekt, kterému je určen.

Princip šifrování je znázorněn na následujícím obrázku:

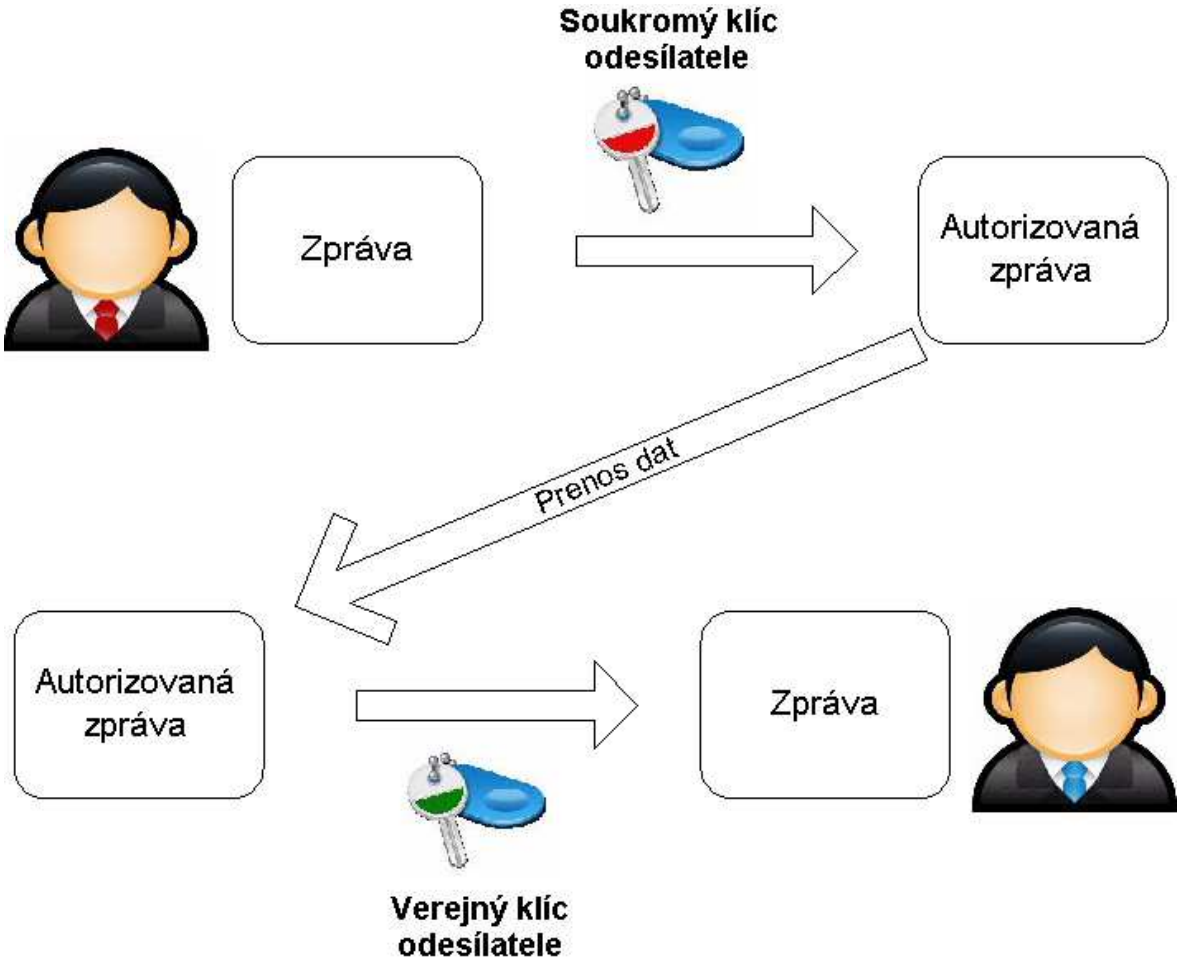



**Obrázek 2: Princip šifrování v asymetrické kryptografii (vlastní zdroj)**

### 3.2.2 Podepisování textu

Jiný způsob použití páru klíčů je určen pro podepsání zprávy nebo textu. Pro vytvoření elektronického podpisu zprávy použije podepisující subjekt svůj soukromý klíč. Zašifrovaný text soukromým klíčem odesílatele se nedá považovat za šifrovaný ve smyslu důvěrný. Kdokoliv může text dešifrovat, protože k dešifrování bude použit veřejný klíč odesílatele, který je k dispozici komukoliv. Jaký smysl tedy má šifrovat text soukromým klíčem? Příjemce, který dešifruje zprávu pomocí veřejného klíče odesílatele, má jistotu, že šifrování provedl právě odesílatel a nikdo jiný. V tomto případě hovoříme o tzv. nepopiratelnosti, resp. neodmítnutelnosti odpovědnosti ze strany odesílatele.

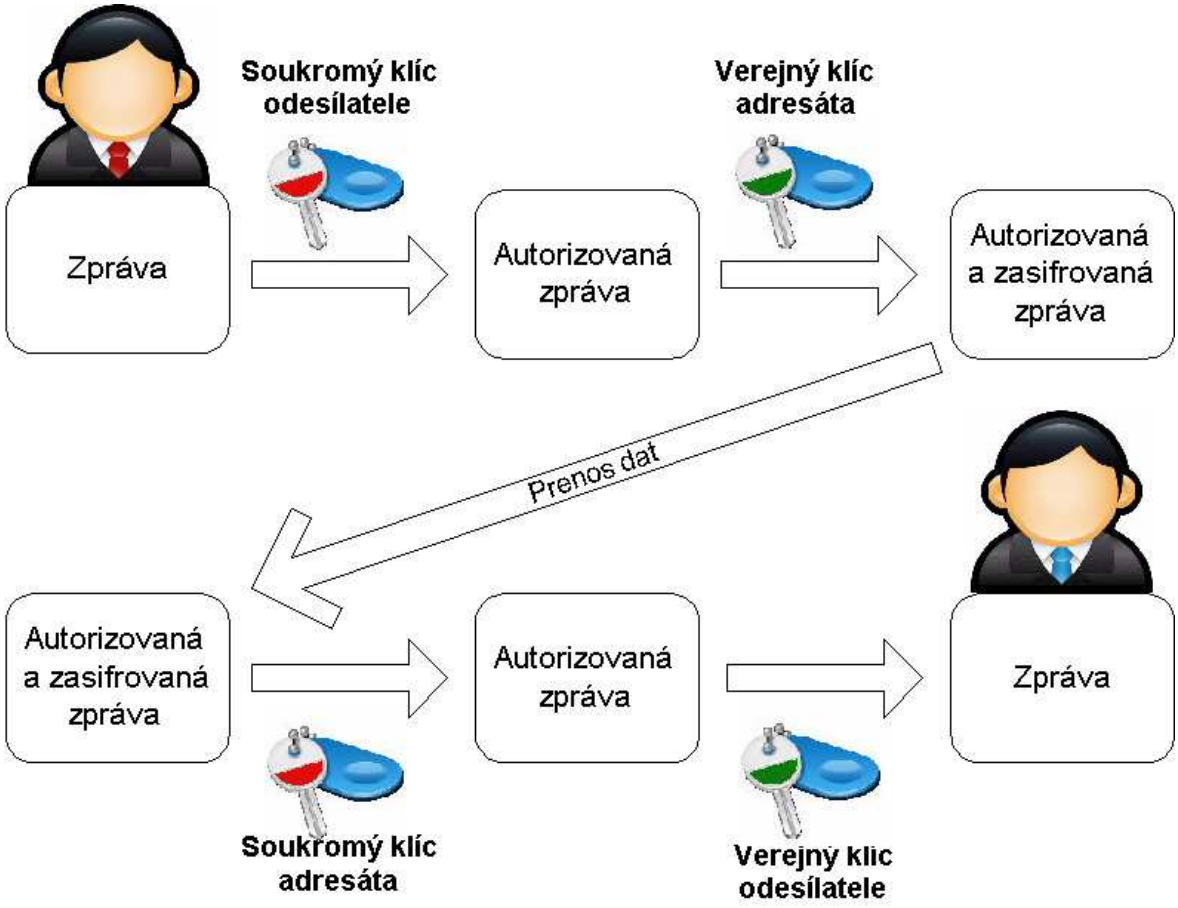
Princip je zobrazen na následujícím obrázku:




**Obrázek 3: Princip elektronického podepisování (vlastní zdroj)**

Na tomto principu je založený elektronický podpis, kterému je věnována samostatná kapitola č. 4.

V případě potřeby je samozřejmě možné oba dva způsoby zkombinovat tak, že vznikne zpráva elektronicky podepsaná i šifrovaná pouze pro konkrétního příjemce. Toho dosáhneme tak, že nejprve text zprávy zašifrujeme soukromým klíčem odesílatele a následně veřejným klíčem příjemce. Princip je znázorněn na následujícím obrázku:




**Obrázek 4: Princip kombinace podpisu a zašifrování zprávy (vlastní zdroj)**

## 3.3 Symetrická vs. asymetrická kryptografie - výhody a nevýhody

Algoritmy symetrické kryptografie mají před asymetrickými jednu výhodu – jejich výpočetní náročnost je mnohem menší, proto je jejich aplikace časově méně náročná, než je tomu v případě asymetrických algoritmů.

Nevýhod symetrických algoritmů vůči asymetrickým je několik. Největším problémem je patrně nutnost distribuce jednoho společného klíče mezi odesílatelem a příjemcem takovým způsobem, který zaručí důvěrnost klíče, resp. jeho nevyzrazení třetí straně. To je možné zajistit buď osobním předáním klíče nebo za použití další metody pro bezpečná přenos klíče. V praxi to může být velmi problematické nebo nemožné.

Další nevýhodou symetrických algoritmů oproti asymetrickým je potřeba velkého počtu klíčů, pro každou dvojici odesílatel – příjemce je potřeba jeden klíč. Například pro 50 lidí, kteří by spolu navzájem chtěli bezpečně komunikovat, by bylo potřeba 1225 samostatných klíčů (každý s každým, tj. kombinace dvou z 50ti vypočteno dle vzorce *n!/((n-k)! k!)* ) a

v případě použití asymetrické kryptografie by bylo použito pouze 50 klíčových párů. Počet klíčů s dalšími uživateli by rychle stoupal, například pro 1000 uživatelů by to bylo už 499500 klíčů.

## 3.4 Šifrovací algoritmus RSA

Algoritmus RSA byl pojmenován podle svých tvůrců Rivestu, Shamirovi a Alemanovi. Algoritmus je založen na složitosti faktorizace velkých prvočísel, stupeň bezpečnosti pak závisí na jejich velikosti, resp. na velikosti vygenerovaných klíčů. Princip fungování se zakládá na myšlence jednoduchosti vynásobit dvě vygenerované dlouhá prvočísla, ale přitom je prakticky nemožné z tohoto součinu provést rozklad na původní součinitele.
Algoritmus RSA při dostatečně velkém klíči je považován za prakticky neprolomitelný. V současné době se považuje za bezpečný algoritmus RSA s délkou klíče 2048 bitů. Tento algoritmus také využívají kvalifikované certifikační autority v rámci poskytování certifikačních služeb.

## 3.5 Hashovací funkce

Vzhledem k pomalosti asymetrické kryptografie, která je dána její matematickou složitostí, se pro vytváření elektronického podpisu zpráv nepoužívá šifrování celé zprávy, ale pouze jejího hashe. Vlastní podepsaná zpráva pak není zašifrovaná, zpráva je ve tvaru otevřeného textu. Pomocí soukromého klíče se zašifruje pouze hash, který se pak připojí v příloze ke zprávě.

Co je to hash?

Hash je hodnota (řetězec) předem dané velikosti, která představuje zhuštěnou hodnotu celé původní zprávy. Hash je počítán z původního textu prostřednictvím hashovací funkce, což je jednosměrná transformace umožňující z otevřeného textu libovolné velikosti získat jednoznačný digitální otisk této zprávy. Jednosměrnost transformace spočívá v tom, že není možný zpětný proces, tedy získání původního textu z hash hodnoty.
V praxi se nejčastěji používají hashovací funkce MD-5, SHA-1 a SHA-2.
Hashovací funkce musí plnit především tři základní funkce:

1) Odolnost vůči získání předlohy – nelze získat původní dokument
2) Odolnost vůči získání jiné předlohy – je prakticky nemožné najít takový dokument, který by měl stejnou hodnotu hash jako původní dokument.

3) odolnost proti nalezení kolize – není možné najít dva různé dokumenty se stejnou hash hodnotou.

Pro bezpečné fungování elektronického podpisu je nutné splnění všech uvedených požadavků na hashovací funkci. Doporučení pro používání konkrétních hashovacích funkcí je možné nalézt v dokumentu ETSI TS 102 176 - 1 [1]

## 3.6 Prostředky pro ochranu kryptografických klíčů

Bezpečné uchovávání informací o kryptografických klíčích používaných pro komunikaci s ostatními subjekty je nejslabším článkem celého procesu. Při použití symetrické kryptografie je potřeba uchovávat maximálně bezpečně společný klíč, používaný pro šifrování i dešifrování zpráv, zejména z pohledu zajištění důvěrnosti a integrity. Jeho vyzrazení nebo modifikace by znehodnotily celý proces šifrování.

V případě asymetrických algoritmů je potřeba maximálně chránit nejen soukromé klíče proti vyzrazení a modifikaci, ale i veřejné klíče všech komunikujících stran proti neoprávněné modifikaci.

Pro uložení kryptografických klíčů lze v zásadě použít jakýkoliv prostředek, nejedná se o nic jiného než o textový řetězec určité délky. Pro bezpečné ukládání je ale vhodné z výše uvedených důvodů využít zabezpečené úložiště.

### 3.6.1 Úložiště klíčů na pevném disku

Způsob ukládání na pevném disku počítače se liší, například podle operačního systému, používané aplikace apod.

V UNIXových systémech se zpravidla používá domácí adresář HOME uživatele, kde jsou uloženy nešifrovaně privátní klíče uživatele.

V operačním systémech Windows jsou klíče uloženy v úložišti klíčů v šifrované podobě, kde jsou k dispozici pouze pro uživatele, který je jejich vlastníkem. Zobrazit si existující klíče a certifikáty dostupné pro daného uživatele je možné přes MS management konzoli (MMC) – Certifikáty.

[1] http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf

### 3.6.2 Externí zařízení pro ukládání klíčů

Ukládání kryptografických klíčů na mobilní externí zařízení má oproti úložištím na pevném disku počítače nesporné výhody:

- mobilita, resp. možnost přenášet a používat kryptografické líče na různých počítačích, např. doma a v práci, případně na přenosném počítači.
- bezpečnost – kryptografické klíče nejsou uložené na pevném disku počítače, který není trvale pod dohledem vlastníka klíčů. Navíc dnes téměř každý počítač je trvale připojen, nebo alespoň se připojuje do datových sítí, ať už firemních, nebo přímo do internetu. Tyto skutečnosti s sebou nesou riziko útoku, tedy získání nebo modifikace klíčů neoprávněnou osobou.

Jako zařízení pro bezpečné uchovávání kryptografických klíčů se nejčastěji používají čipové karty, nebo dnes možná častěji USB Tokeny.

Zařízení musí podporovat potřebné algoritmy pro použití kryptografických klíčů – šifrování a dešifrování, resp. podepisování a ověřování podpisů. Bezpečnostní tokeny i karty již dnes většinou umožňují generovat privátní klíč přímo ve své paměti. Během používání klíč vůbec neopouští paměť zařízení.

Ochrana tokenů a karet před neoprávněným použitím je realizována přes PIN. Zpravidla lze využít čtyř až osmi místných bezpečnostních kódů, v případě několika po sobě jdoucích chybných zadání PIN se karta nebo token automaticky zablokuje.

# 4 Elektronický podpis

## 4.1 Vytvoření a ověření elektronického podpisu zprávy

Celý proces vytvoření a ověření elektronického podpisu se skládá z následujících kroků:

1) vytvoření podpisu zprávy na straně odesílatele
    - vytvoření hashe zasílané zprávy
    - zašifrování hodnoty hash
    - připojení elektronického podpisu ke zprávě
2) ověření podpisu zprávy na straně příjemce
    - spočítání hodnoty hash z otevřeného textu zprávy
    - dešifrování elektronického podpisu pomocí veřejného klíče odesílatele
    - porovnání obou hodnot hashe k určení pravosti podpisu

Prvním krokem v procesu vytvoření elektronického podpisu je výpočet hodnoty hash podepisované zprávy, tedy otisku zprávy z předem definovanou délkou. Délka otisku zprávy je zpravidla mnohem menší, než celá zasílaná zpráva.

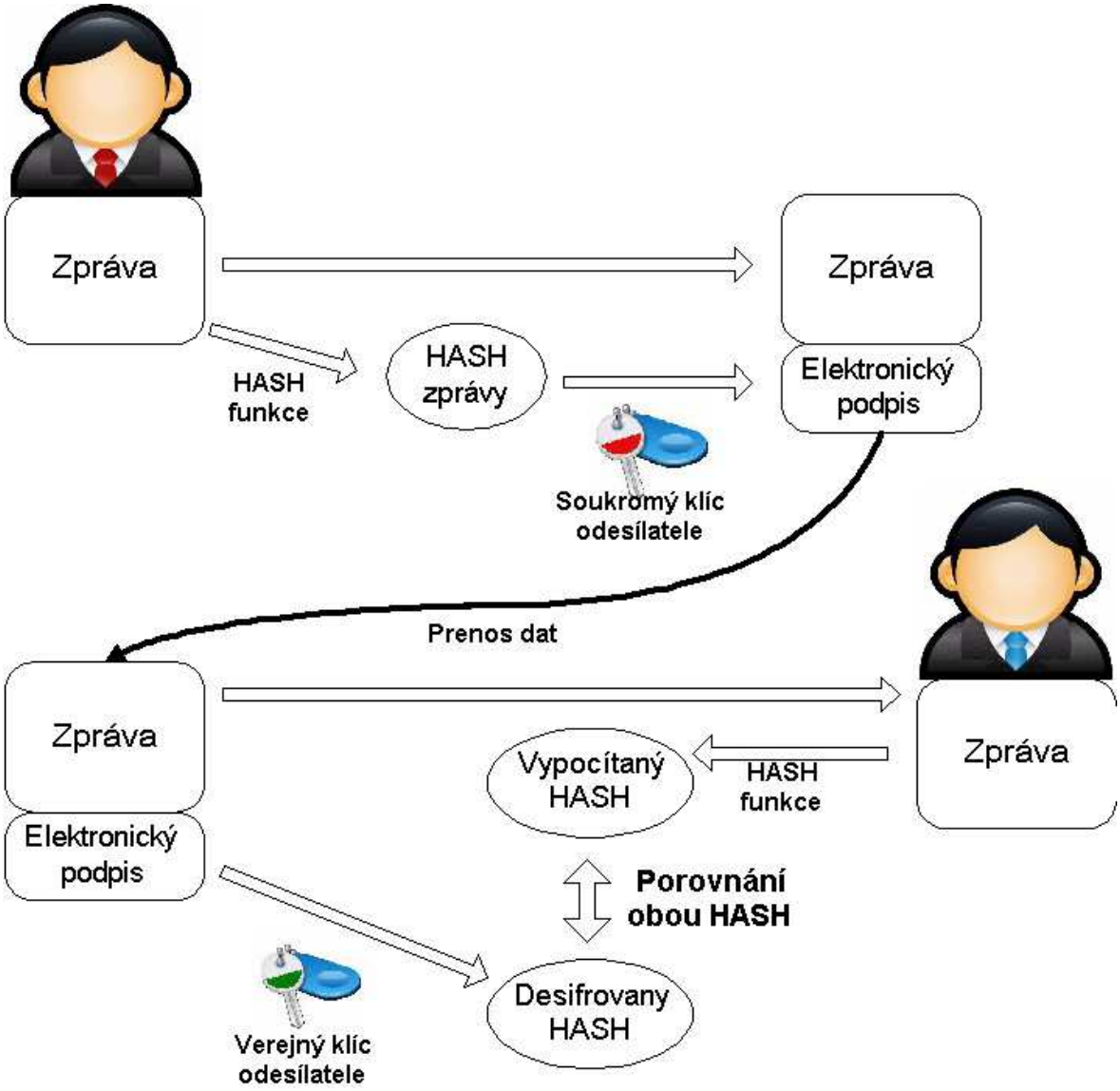
Hodnota hash se zašifruje pomocí některého asymetrického algoritmu. Díky malé velikosti hash je proces šifrování a dešifrování velmi rychlý, přestože se jedná o asymetrickou kryptografii. Pro zašifrování na straně podepisujícího se použije privátní klíč, jehož vlastníkem je podepisující subjekt. Výsledná zašifrovaná hash hodnota je elektronickým podpisem zprávy.

Elektronický podpis se připojí jako příloha k podepsanému textu. Zasílaný text zůstává ve formě otevřeného textu.

Po přijetí zprávy příjemcem se nejprve spočítá nová hodnota hash podle zaslaného otevřeného textu zprávy. Následně se podle veřejného klíče odesílatele předpokládaného odesílatele dešifruje elektronický podpis uložený v příloze. Tím vznikne hodnota hash vypočítaná na straně odesílatele.

Posledním krokem ověření podpisu je porovnání těchto dvou hodnot hashů, vypočítaného a dešifrovaného. Pokud jsou hodnoty totožné, považuje se elektronický podpis odesílatele za pravý.

Celý proces je popsán na následujícím obrázku.

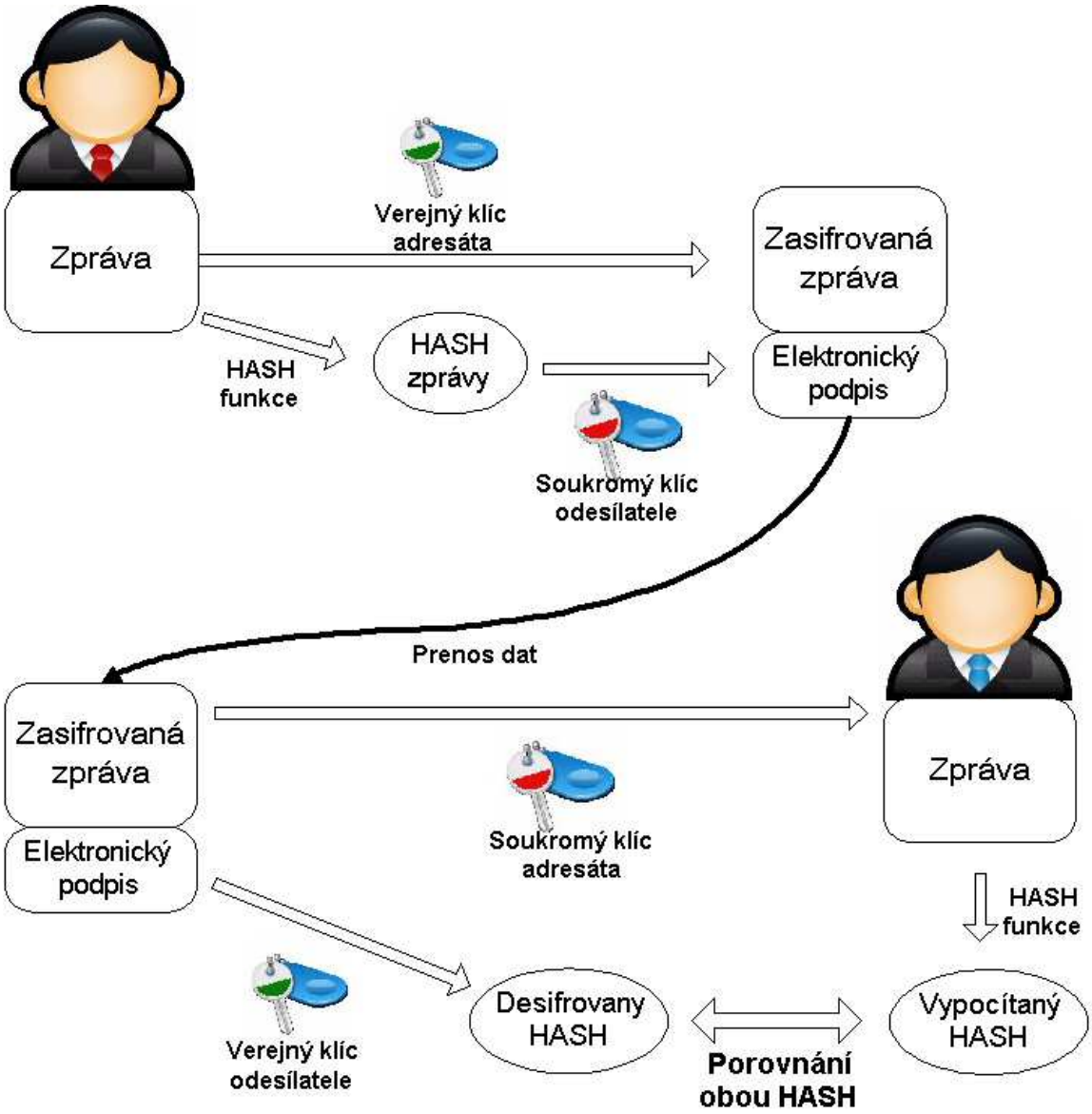



**Obrázek 5: Princip elektronického podepisování zprávy s využitím funkce hash (vlastní zdroj)**

Obsah elektronicky podepsané zprávy je navíc možné chránit šifrováním. V zásadě existují dva způsoby, jak to zajistit. V obou případech se nejdříve vytvoří elektronický podpis výše uvedeným způsobem, a až poté se šifruje vlastní text zprávy.

První případ je jednodušší, ale méně využívaný kvůli jeho pomalé rychlosti. Spočívá v tom, že otevřený text zprávy se zašifruje pomocí veřejného kryptografického klíče příjemce. Vzniklý šifrovaný text s připojeným elektronickým podpisem se odesílá příjemci.

Dešifrování a ověření elektronického podpisu se provádí v opačném pořadí, resp. adresát nejdříve použije svůj soukromý klíč pro dešifrování vlastní zprávy a následně ověří elektronický podpis výše uvedeným způsobem, viz následující obrázek.




**Obrázek 6: Princip elektronického podepisování zprávy s využitím funkce hash společně se zašifrováním zprávy (vlastní zdroj)**

Vzhledem k tomu, že zasílaná zpráva může být značně velká a v kombinaci s použitou asymetrickou kryptografií by šifrování zprávy trvalo neúměrně dlouho, je výhodnější a také častěji používaný druhý způsob s použitím asymetrického i symetrického klíče.

V tomto případě se před přenosem na straně odesílatele vygeneruje symetrický klíč, který se následně použije pro zašifrování celé zprávy. Symetrické šifrování velkých objemů dat je mnohem rychlejší, než asymetrické. Asymetrická kryptografie se pak použije pro zašifrování vygenerovaného symetrického klíče, použije se k tomu veřejný klíč příjemce.
Dešifrování a ověření elektronického podpisu se opět provádí opačným postupem, nejdříve se použije soukromý klíč adresáta pro dešifrování hodnoty symetrického klíče. Následně se aplikuje symetrický klíč na vlastní zašifrovanou zprávu a po dešifrování textu se ověří elektronický podpis výše uvedeným způsobem.

## 4.2 Certifikáty

Problém, který je v rámci asymetrické kryptografie potřeba řešit, je bezpečné uchovávání a distribuce kryptografických klíčů. Pro ukládání privátních kryptografických klíčů je situace jednodušší – klíče je potřeba mít uložené na bezpečném úložišti, kam bude mít přístup pouze vlastník těchto klíčů. Bezpečným úložištím pro ukládání kryptografických klíčů je věnována jiná kapitola. Jiné nároky jsou kladeny na práci s veřejnými klíči. K veřejným klíčům je potřeba navíc uchovávat jednoznačnou identifikaci vlastníků těchto klíčů. Navíc na rozdíl od soukromých klíčů, které je potřeba chránit a nikde nezveřejňovat, veřejné klíče musí mít protistrana k dispozici pro ověření podpisu nejpozději současně s vlastní zprávou, resp. pro zašifrování ještě před začátkem přenosu. Další problém je tedy s bezpečnou distribucí veřejných klíčů mezi komunikujícími stranami.
Problém uchovávání a distribuce veřejných klíčů se dá řešit prostřednictvím certifikátů veřejného klíče (dále budu zmiňovat zkráceně - certifikát)

### 4.2.1 Co je to certifikát

Zjednodušeně se dá říci, že certifikát veřejného klíče je datová zpráva, prostřednictvím které je jednoznačně spojena podepisující osoba se svým veřejným klíčem, který je potřeba pro ověřování jejího digitálního podpisu.
Ze své podstaty tedy certifikát musí obsahovat veřejný klíč vlastníka certifikátu a další údaje identifikující vlastníka certifikátu, jako jsou např. jméno a příjmení, firma, email, adresa.
Certifikát vydává určitý poskytovatel certifikačních služeb, v praxi také označovaný jako certifikační autorita. Certifikát tedy také musí obsahovat digitální podpis certifikační autority, která tak zaručuje, že daný veřejný klíč skutečně patří uvedené osobě.

Běžné certifikáty tedy obsahují:

- ID certifikátu – jednoznačná identifikace certifikátu
- Platnost od, platnost do - datum vydání certifikátu a datum platnosti
- Omezení certifikátu – vymezení účelu, ke kterému lze certifikát použít.
- ID certifikační autority – jednoznačná identifikace vydavatele certifikátu
- Algoritmus CA – algoritmus certifikační autority, který byl použit pro podepsání certifikátu
- Algoritmus PK – algoritmus, kterým byl vytvořen klíčový pár dané osoby, resp. algoritmus podepisovaného veřejného klíče.
- Veřejný klíč vlastníka – veřejný klíč, ke kterému se certifikát váže.
- ID vlastníka – informace o vlastníkovi certifikátu, se kterými je jednoznačně svázaný certifikát.
- Podpis CA – Certifikační autorita podepisuje certifikát, k tomu využívá již dříve popsaný způsob digitálního podpisu. Podpis je pak uložen v certifikátu.

Doporučená struktura certifikátu pro běžné použití je popsána v dokumentu RFC-3280 - "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"[2].

### 4.2.2 Třídy certifikátů

Z pohledu míry ověření identity vlastníka elektronického podpisu pro vydání certifikátu je možné rozdělit certifikáty do následujících čtyř tříd:

**1. třída** – Certifikační autorita při vydávání certifikátu ověří pouze unikátnost jména, se kterým má být veřejný klíč svázán, resp. že požadované jméno je volné. Tato třída se spíše hodí pro testování než pro skutečné používání.

**2. třída** – Při vydávání certifikátu se nemusí dostavit vlastník certifikátu osobně. Certifikační autorita vydá certifikát na základě ověření vlastníka třetí stranou, například na základě notářsky ověřené žádosti o vydání certifikátu.

**3. třída** – Pro vydání certifikátu musí žadatel o certifikát osobně navštívit certifikační autoritu, kde je ověřena jeho totožnost na základě předepsaných dokladů. Způsob ověření totožnosti žadatele je stanoven certifikační politikou. Certifikáty této třídy jsou vhodné pro většinu účelů. Certifikáty 3. třídy jsou také vyžadovány zákonem o elektronickém podpisu.

[2] http://tools.ietf.org/html/rfc3280

**4. třída** – Certifikáty této třídy musí splňovat stejné podmínky, které jsou stanoveny pro certifikáty 3. třídy, a navíc musí žadatel prokázat oprávněnost k určité činnosti.

### 4.2.3 Formáty certifikátu

Existuje několik formátů, ve kterých lze certifikáty uchovávat. Různé formáty se hodí pro různé využití certifikátů v závislosti na použité platformě, SW apod.

Struktura certifikátu je popsána prostřednictvím jazyka ASN.1 (Abstract Syntax Notation One). Jedná se o jednoznačnou klasifikaci certifikátu, jednotlivé objekty jsou zde popsány tak, že jsou srozumitelné pro člověka. Pro technologické zpracování však není potřeba zachovat čitelnou formu certifikátu pro člověka. Certifikáty se proto uchovávají ve formátu BER (Basic Encoding Rules), PEM – možnost zobrazení v některých textových editorech, DER (Distinguished Encoding Rules), TXT – zpětně transformovatelný do čitelné podoby.

Certifikační autority většinou umožňují klientům stažení certifikátu v různých formátech pro ulehčení jejich použití.

### 4.2.4 Typy certifikátů

Za důvěryhodnost certifikátu ručí vždy jeho vydavatel – certifikační autorita. Každý klientský certifikát je podepsaný elektronicky certifikační autoritou. Proto pro ověření, že daný certifikát vydala skutečně určitá certifikační autorita, je potřeba mít k dispozici certifikát této certifikační autority – jedná se o ověření elektronického podpisu CA na klientském certifikátu.

To ale vyvolává další problém, a to, jak ověřit elektronický podpis na certifikátu CA, aby byla zaručena důvěryhodnost tohoto certifikátu. Možnosti jsou dvě:

1) V prvním případě existuje nadřízená instituce, o jejíž důvěrnosti se již nepochybuje, která pak vydává certifikáty jednotlivým certifikačním autoritám. Tato instituce bývá zmocněna zvláštním zákonem. Tento způsob se využívá např. na Slovensku, kde vydává certifikát akreditovaným certifikačním autoritám Národní bezpečnostní úřad. Tak vzniká minimálně třístupňová certifikační cesta, která je tvořena klientským certifikátem, certifikátem vydavatele klientských certifikátů a nadřízenou institucí.
2) Ve druhém případě si certifikační autorita vydavatele klientských certifikátů vydá certifikát sama – vystavitel i vlastník certifikátu je stejný. Tento způsob je častěji využívaný, používá se i v České republice. Takový certifikát se označuje jako kořenový, samopodepsaný. Kořenový certifikát sám o sobě nezaručuje pravost a

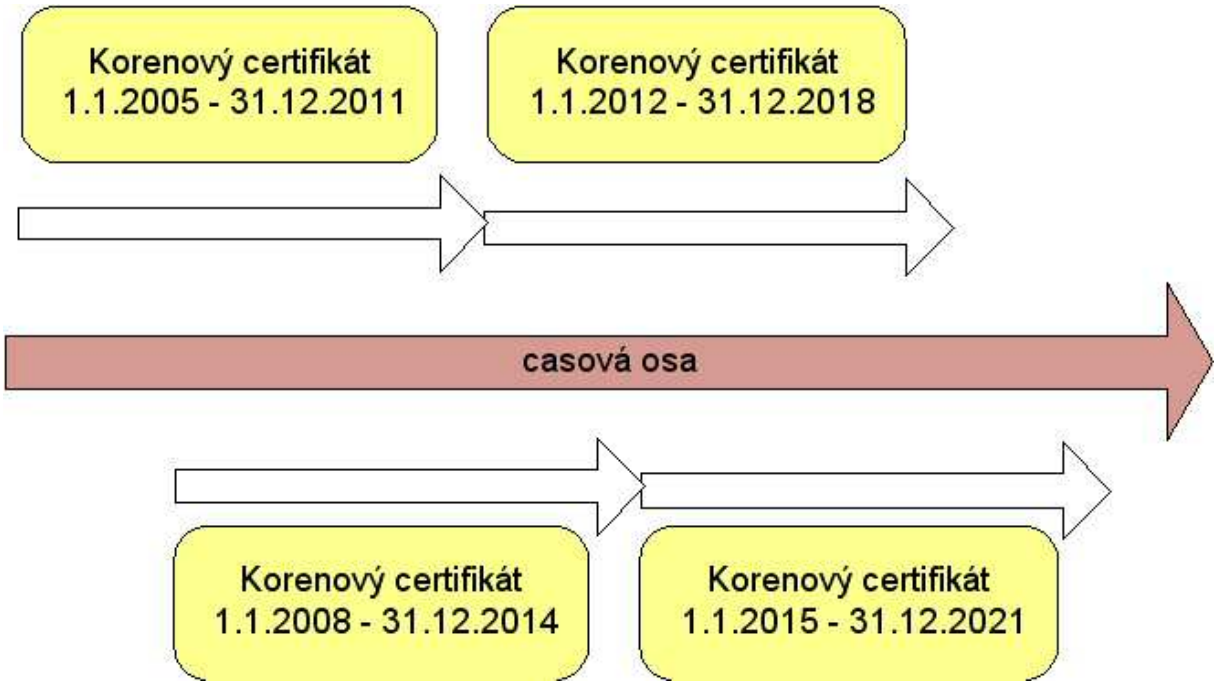
důvěrnost vydavatele certifikátu. Pro zaručení důvěrnosti se zde používá např. předání takového certifikátu komunikujícím stranám důvěryhodným způsobem nebo zveřejněním certifikátu prostřednictvím důvěryhodné třetí strany. V České republice se například zveřejňují certifikáty akreditovaných poskytovatelů CA prostřednictvím webových stránek Ministerstva vnitra ČR.

Popsané typy certifikátů jsou dnes akceptovány běžnými aplikacemi a operačními systémy. Jako příklad je možno uvést MS Windows, kde jsou certifikáty poskytovatelů certifikačních služeb rozděleny do kategorií:

- důvěryhodné kořenové certifikační úřady – CA, které systém Windows považuje za důvěryhodné při ověřování bezpečné komunikace. V systému jsou implicitně instalované certifikáty splňující podmínky společnosti Microsoft.
- zprostředkující certifikační úřady – sem spadají certifikáty vystavené podřízeným certifikačním autoritám.
- důvěryhodný vydavatel – sem patří certifikáty vydané CA, které jsou důvěryhodné v rámci zásad omezení použití nebo omezení SW.

### 4.2.5 Platnost certifikátů CA

Platnost certifikátů certifikačních autorit, které jsou použité pro vydávání klientských certifikátů, je také omezená, i když je výrazně delší než u klientských certifikátů (více než 5 let) . Protože se při ověřování podpisu klientského certifikátu ověřuje i platnost podpisu certifikační autority v tomto certifikátu, musí být zaručeno, že po celou dobu platnosti klientského certifikátu bude i platná certifikát vydavatele. Proto certifikační autorita nemůže používat svůj certifikát až do konce jeho platnosti, ale musí včas zajistit vydání nového certifikátu. V praxi se tento problém řeší tak, že certifikační autorita má souběžně platné dva certifikáty, jejichž platnosti se prolínají, viz následující obrázek.




**Obrázek 7: Překryv platností certifikátů CA (vlastní zdroj)**

Pro možnost ověření certifikátu protějšku, resp. ověření elektronického podpisu vydavatele na tomto certifikátu, je potřeba mít na počítači uložený certifikát CA a její zařazení mezi důvěryhodné certifikační autority. Co se týče českých akreditovaných poskytovatelů certifikačních služeb, certifikáty Postsignum a ICA jsou již zařazeny mezi příslušné složce (Důvěryhodné kořenové certifikační úřady) již po instalaci Windows (a příslušných aktualizacích).

V případě potřeby lze certifikát zpravidla získat na stránkách vydavatele certifikátů, v případě akreditovaných poskytovatelů je to povinnost daná legislativou. Na stránkách dané certifikační autority je tedy potřeba najít ten správný certifikát, protože jeden poskytovatel certifikačních služeb může nabízet více typů komerčních certifikátů. Například jedna certifikační autority může vydávat kvalifikované certifikáty používané pro zaručené podpisy elektronických dokumentů a zároveň komerční certifikáty pro šifrování komunikace. Pokud jsou v dané době platné paralelně dva certifikáty dané CA, je potřeba mít nainstalované oba.

Certifikáty bývají ke stažení v běžně dostupných formátech (PEM, DER, TXT).

Pravost certifikátu CA může být ověřena pomocí hash hodnoty certifikátu (fingerprintu) - hash staženého certifikátu lze porovnat s hashem zveřejněným prostřednictvím důvěryhodného zdroje nebo získaným na vyžádání od poskytovatele. V případě

akreditovaných poskytovatelů certifikačních služeb jsou hashe zveřejněny na stránkách Ministerstva vnitra.

Certifikát je třeba nainstalovat do správného úložiště (v případě ČR do složky Důvěryhodné kořenové certifikační úřady). Korektní uložení certifikátů lze ověřit na úložišti certifikátů systému. Ve Windows je možné použít k tomuto účelu Microsoft Management Consoli (MMC), modul certifikáty. Zde jsou také vidět všechny položky certifikátu včetně data platnosti nebo hashe.

Klient by si měl instalovat pouze certifikáty CA, kterým důvěřuje, v opačném případě by to mohlo znamenat ohrožení bezpečnosti elektronické komunikace.

### 4.2.6 Klientské certifikáty

Jak již bylo řečeno, klientské certifikáty vydávají certifikační autority jednotlivým osobám pro účely zabezpečení elektronické komunikace.

Existuje několik typů certifikátů nabízených CA:

- komerční certifikáty
- kvalifikované certifikáty
- testovací certifikáty

**Komerční certifikáty** nepodléhají zákonu o elektronickém podpisu, pro vydávání komerčních certifikátů není potřeba kvalifikované ani akreditované vydávající certifikační autority. Používání komerčních certifikátů je pouze na dohodě komunikujících stran, vydávání, zneplatňování a obnova certifikátů by se měla řídit certifikační politikou poskytovatele certifikačních služeb, které však nepodléhá znění zákona o elektronickém podpisu. Komerční certifikáty mají široké využití, například pro zabezpečení důvěrnosti přenášených dat šifrováním, pro elektronické podepisování datových zpráv, nebo pro zajištění autentizace uživatelů.

**Kvalifikované certifikáty** jsou vydávány v souladu se zákonem o elektronickém podpisu a jejich vydavatelé musí být kvalifikovanými poskytovateli certifikačních služeb. Tyto certifikáty je možné používat pouze pro elektronické podepisování, nelze je používat pro ostatní účely, ke kterým lze využít komerční certifikát. Toto omezení vychází ze současné legislativy v ČR, tj. zákona o elektronickém podpisu. Vhodné využití kvalifikovaných certifikátů je pro komunikaci občanů se státní správou, nebo pro komunikaci mezi jednotlivými složkami státní správy, kde naopak nelze využít komerční certifikáty.

V souvislosti s použitím kvalifikovaného certifikátu hovoříme kvalifikovaném elektronickém podpisu, nebo elektronické značce. Z technického pohledu není mezi elektronickým podpisem a značkou rozdíl. Rozdíl je ale v tom, s jakým typem subjektu je subjektu je podpis nebo značka spojena:

Elektronický podpis – *údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.* [ZAK227]

Zaručený elektronický podpis navíc musí splňovat:

- *Je jednoznačně spojen s podepisující osobou.*
- *Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.*
- *Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.*
- *Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.* [ZAK227]

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

- *Jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu.*
- *Byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou.*
- *Jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat* [ZAK227]

### 4.2.7 Testovací certifikáty

Tento typ certifikátu je určen pouze pro testování a většina CA ho vydává zdarma. Lze o něj požádat online prostřednictvím webových stránek poskytovatele, certifikát je vydán a např. zaslán mailem bez jakéhokoliv ověření žadatele.

### 4.2.8 Postup pro získání klientského certifikátu

**Výběr typu certifikátu**

S ohledem na účel vydávaného certifikátu si klient musí zvolit, jaký typ certifikátu potřebuje - musí zvolit mezi kvalifikovaným nebo komerčním certifikátem. Kvalifikovaný

certifikát je určený pro elektronické podepisování dokumentů zejména při komunikaci občanů a firem se státní správou, nebo pro komunikaci uvnitř státní správy. Kvalifikované certifikáty nelze využít pro šifrování dokumentů

Komerční certifikáty slouží pro elektronické podepisování dokumentů a pro šifrování. Omezením komerčních certifikátů je, že komunikující strany musí uznávat danou komerční certifikační autoritu. Pro komunikaci se státní správou nejsou komerční certifikáty určené.

**Výběr údajů uvedených v certifikátu**

Certifikát, podobně jako např. průkaz totožnosti, jednoznačně identifikuje vlastníka certifikátu. Žadatelem o vydání certifikátu elektronického podpisu je zpravidla fyzická osoba. Vlastníkem certifikátu však může být fyzická osoba, právnická osoba nebo úřad. V certifikátu může být uveden i vlastník, který je zároveň fyzickou osobou a zároveň zástupcem nějaké společnosti. Dle zamýšleného použití certifikátu je třeba zvolit údaje, které bude daný certifikát obsahovat. Například jestli mají být uvedeny pouze základní údaje o fyzické osobě, nebo má být uvedena i například role vlastníka certifikátu ve společnosti. Certifikační autority proto nabízejí certifikáty s různými typy údajů, resp. certifikáty pro fyzické a právnické osoby.

**Výběr certifikační autority**

Výběr certifikační autority závisí na požadovaném typu certifikátu. Při výběru komerční certifikační autority může být certifikační autorita jasně daná, např. při komunikaci s bankou může banka akceptovat pouze vlastní certifikáty.

Při výběru kvalifikované certifikační autority pro komunikaci se státní správou může klient vybírat z akreditovaných poskytovatelů certifikačních služeb. Výběrovými kriterii může být například cena, dostupnost v místě klienta, další přidaná hodnota (např. balíček obsahující navíc bezpečné úložiště pro certifikáty – token, případně akceptace dané CA dalšími subjekty nad rámec státní správy).

**Vytvoření žádosti o certifikát**

V tomto kroku klient vygeneruje klíčový pár pomocí dostupného softwarového vybavení, případně prostřednictvím nástrojů certifikační autority, a vytvoří žádost o certifikát v předepsaném formátu vybrané CA. Procedura generování páru klíčů a generování žádosti bývá zpravidla automatizovaná, stačí využít funkcionalit prostřednictvím webových

stránek vybrané certifikační autority. Generování páru klíčů je také možné realizovat prostřednictvím USB Tokenu, ve kterém zároveň zůstane privátní klíč bezpečně uložen. V takovém případě je potřeba využít software dodaný k Tokenu. Jak jsem zmínil výše, někteří poskytovatelé certifikačních služeb nabízejí balíček, jehož součástí je právě USB Token, potřebný SW a návod, jak vygenerovat klíče i žádost o certifikát.

Bez ohledu na zvolený způsob vytvoření žádosti musí žádost o certifikát obsahovat údaje, které mají být součástí certifikátu. Pro různé typy a určení certifikátu jsou různé vyplňované údaje, z nichž některé jsou pro daný typ povinné a některé volitelné. Mezi povinné položky patří zejména údaje potřebné pro identifikaci žadatele, např. celé jméno, stát, emailová adresa, v případě, že se jedná o zaměstnanecký certifikát, tak i organizace. Mezi nepovinné položky patří naopak ty údaje, které se ve vydávaném certifikátu nebudou vyskytovat, nebo mají informativní charakter, jako je poštovní adresa žadatele, akademický titul apod.

Vygenerovaná žádost o certifikát je standardním dokumentem. Existuje více formátů žádostí, v poslední době se však používá hlavně formát PKCS#10 (dle RFC-2314). Žádost o certifikát je podepsaná datová struktura, k jehož podepsání je použit právě vygenerovaný privátní klíč žadatele. Veřejný klíč je uložen je součástí žádosti.

Po vygenerování páru klíčů se doporučuje provést zálohu privátního klíče. Pokud je privátní klíč uložen na Windowsovém úložišti certifikátů, je pro zálohu možné využít manažera certifikátů – Windows aplikaci CERTMGR.MSC, samostatně spustitelnou z příkazového řádku, nebo např. přes MMC (Microsoft Management Consoli). Soukromý klíč se bezpečně zazálohuje pod heslem do souboru *.PFX.

**Předání žádosti o certifikát CA**

Žadatel předá žádost o vydání prostřednictvím kontaktního místa – registrační autority. Ty bývají oddělené od centrálního systému jednak z důvodu bezpečnosti a jednak z důvodu klientské dostupnosti - poskytovatelé certifikačních služeb mají více kontaktních míst po republice. Žadatel se musí dostavit osobně na registrační autoritu, aby doložil údaje uvedené v žádosti. U certifikačních autorit vyšší úrovně bezpečnosti (určitě platí pro kvalifikované) je potřeba doložit všechny údaje uvedené v žádosti.

K doložení údajů je před návštěvou registrační autority připravit všechny potřebné doklady. Způsob dokládání údajů pro jednotlivé typy certifikátů musí být uveden v konkrétní certifikační politice dané CA.

**Ověření informací na kontaktním místě**

Pracovníci registrační autority na kontaktním místě ověří pravdivost uvedených údajů v žádosti o certifikát oproti předloženým dokladům. K ověření můžou využít i informace z dostupných registrů a informačních zdrojů (např. obchodní rejstřík).Dále je možné ověřit i konzistenci šifrovacích klíčů a jejich jedinečnost v rámci dané certifikační autority.

**Vytvoření certifikátu**

Certifikační autorita vytvoří elektronický dokument definovaného formátu, který obsahuje údaje z žádosti o certifikát. Tento dokument pak elektronicky podepíše svým certifikátem.
Následně je certifikát předán žadateli. Certifikát může být nahrán žadateli na datový nosič přímo na kontaktním místě, nebo je zaslán prostřednictvím emailu nebo zveřejněn na stránkách certifikační autority. Zveřejňování certifikátů na stránkách certifikačních autorit přispívá k vyšší bezpečnosti, protože je možné kýmkoliv snadno ověřit existenci i platnost certifikátu. Žadatel však může zamezit zveřejnění certifikátu, pokud tak uvede v žádosti o certifikát.
Stejně jako záloha privátního klíče se doporučuje i záloha veřejného klíče a certifikátu.

**Vydávání následného certifikátu**

U vydávání následného certifikátu (před koncem platnosti předchozího) je celý proces zjednodušen, vygenerovanou žádost o certifikát může žadatel elektronicky podepsat platným certifikátem.
Zde je pouze potřeba včas odeslat žádost o následný certifikát, resp. ještě před ukončením platnosti předešlého. Po ukončení je potřeba žádat o následný certifikát standardní cestou.

### 4.2.9 Životní cyklus certifikátu

Každý certifikát má omezenou dobu platnosti v souladu s certifikační politikou. Důvodem pro omezování maximální doby platnosti je bezpečnost. Nejen se stoupajícím výkonem výpočetní techniky se zvyšuje riziko objevení nějakých mezer v používaných kryptografických algoritmech. V případě vydávání časově neomezených certifikátů by pak mohlo dojít k tomu, že certifikáty vydané s použitím zastaralých technologií by se staly nespolehlivé.
Běžně vydávané klientské certifikáty jsou vydávány na jeden rok. Prodloužení této doby by určitě uvítali klienti, protože by došlo ke zlevnění používání certifikátů i zvýšení

komfortu užívání certifikátů. Vyžadovalo by ale změnu technologie například zvýšení délky šifrovacích klíčů, což by mohlo způsobit problémy v aplikacích z důvodu jejich nepřipravenosti.

### 4.2.10 Zneplatnění certifikátu

Zneplatnění, nebo také revokaci certifikátu, je možné provést dříve, než vyprší délka jeho platnosti omezená certifikační autoritou. O zneplatnění certifikátu může požádat klient způsoby, které jsou definovány v certifikační politice. Důvodů pro zneplatnění může být několik, například obava z prozrazení soukromého klíče, ukončení pracovně právního vztahu se zaměstnancem v případě zaměstnaneckého certifikátu apod. Příkladem vyzrazení soukromého klíče může být krádež osobního počítače, nebo jen krádež dat.

Certifikační politika musí definovat takové způsoby žádání o zneplatnění certifikátů, aby nemohlo dojít ke zneužití této možnosti neoprávněnou osobou. Žádost o zneplatnění je určitě možné podat při osobní návštěvě pracoviště registrační autority. Žádost je ale také možné podat i v mimopracovních hodinách těchto pracovišť, nebo z místa, odkud je takové pracoviště nedostupné. V těchto případech je možné požádat o zneplatnění např. prostřednictvím emailu, webových stránek vydávající certifikační autority, nebo třeba i telefonicky.

Certifikační politika musí definovat způsob autentizace pro tyto případy. Je možné například email s žádostí o zneplatnění elektronicky podepsat zneplatňovaným certifikátem, nebo v případě jiných možností využít jednorázové heslo, které je pro tyto případy zpravidla definováno klientem už během procesu vydávání certifikátu.

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou:

- číslo certifikátu, což je jednoznačný identifikátor certifikátu v rámci dané certifikační autority – jeden klient může mít více platných certifikátů.
- Autentizace, tj. v případě použití prostředků elektronické komunikace například již zmíněný podpis nebo jednorázové heslo. V případě osobní návštěvy pracoviště registrační autority se může klient prokázat platným průkazem totožnosti akceptovaným certifikační autoritou.

Nepovinně je pak možné uvést důvod zneplatnění certifikátu.

Zneplatněný certifikát je pak zařazen do seznamu zneplatněných certifikátů CRL (Certificate Revocation List). CRL obsahuje všechny zneplatněné certifikáty, jejichž doba platnosti ještě neuplynula. Samo zařazení zneplatněného certifikátu do CRL nezamezuje

jeho zneužití, certifikační autorita pouze zveřejňuje tento dokument a je povinností každého, aby při využívání elektronického podpisu kontroloval tento CRL.

Vydané CRL jsou elektronicky podepsané vydávající certifikační autoritou, čímž je zaručena jejich integrita. CRL vydává každá certifikační autorita v pravidelných intervalech, které jsou definovány v certifikační politice a vycházejí z platné legislativy. Dokument CRL je zveřejňován prostřednictvím webových serverů certifikační autority. Adresy, kde je CRL zveřejňován, bývají uvedeny v rozšířených položkách certifikátů. Struktura CRL je definovaná normou X.509 (RFC3280)[3], stejně jako struktura certifikátů.

Vydaný CRL obsahuje položku Next Update, která obsahuje předpokládaný termín vydání další aktualizace CRL. O každém zneplatněném certifikátu je zde uvedeno jeho sériové číslo a časový okamžik (datum a čas) zneplatnění.

Vydané CRL jsou číslovány vzestupně (položka CRL Number) a certifikační autorita musí zajistit, aby číslování tvořilo souvislou číselnou řadu.

### 4.2.11 Obnova certifikátu

Vzhledem k omezené platnosti certifikátů je nutné certifikáty periodicky obnovovat. V případě kvalifikovaných klientských certifikátů je jejich platnost omezena na jeden rok. V případě že klient požaduje i nadále využívat zabezpečenou elektronickou komunikaci, je potřeba certifikáty obnovit. Obnova certifikátů je jednodušší proces, než bylo jejich vydávání, na jehož konci je vydání následných certifikátů klientovi. Pro vydání následného certifikátu zpravidla není potřeba osobní návštěva pracoviště registrační autority. Klient pouze musí vygenerovat žádost o vydání certifikátu, v rámci které se vygeneruje i nový pár klíčů. Veřejný klíč je pak připojen k žádosti o certifikát stejně jako u prvotního vydávání. Žádost je následně elektronicky podepsána předchozím certifikátem, což zajistí autentizaci a autorizaci klienta. Žádost je pak odeslána emailem na pracoviště registrační autority.

Takováto obnova má ale několik podmínek:

1) Od vydání předchozího certifikátu nedošlo ke změně osobních dat. Údaje předložené klientem pro vydání předchozího certifikátu musí být stále platné.
2) Žádost o vydání následného certifikátu musí být vytvořena ještě v době platnosti předchozího certifikátu, aby bylo možné předchozím certifikátem žádost podepsat. V praxi většinou certifikační autorita sama kontaktuje klienta určitou dobu před vypršením certifikátu většinou automatickým rozesíláním notifikačních mailů.

[3] http://tools.ietf.org/html/rfc3280

Pokud není některá z podmínek splněna, je nutná osobní návštěva klienta pracoviště registrační autority.

Další důvod, proč by mohl být problém v použití uvedeného postupu, je, pokud předchozí certifikát nebyl určen pro tvorbu a ověřování elektronického podpisu (ale např. pouze pro šifrování komunikace). V takovém případě by uvedený postup nemohl být použit. Tento případ se ale netýká kvalifikovaných certifikátů, které jsou vždy určeny pro elektronické podepisování.

# 5 Časové razítko

Časové razítko (Time Stamp) je stejně jako certifikát elektronický dokument. Může je vydávat poskytovatel certifikačních služeb, který zároveň poskytuje služby časové autority. Časové razítko se používá jako důkaz o tom, že konkrétní dokument, který je opatřen časovým razítkem, existoval již v době, která je uvedena v tomto razítku. Časovým razítkem je tedy datová zpráva, která důvěryhodným způsobem spojuje elektronický dokument s časovým okamžikem. Z toho pak vyplývá, že elektronický dokument existoval před daným časovým okamžikem uvedeným v razítku.

Časová razítka jsou zakotvena v české i evropské legislativě. V české legislativě jsou definována v zákonu o elektronickém podpisu, kde se hovoří o kvalifikovaném časovém razítku. Na rozdíl od elektronického podpisu, v případě časových razítek se mluví vždy o kvalifikovaném časovém razítku.

Hlavní rozdíl mezi certifikátem elektronického podpisu a časovým razítkem je ten, že certifikát je vázán na vlastníka certifikátu, tedy osobu – subjekt, certifikát definuje vazbu mezi fyzickou identitou a elektronickou identitou vlastníka. Kdežto časové razítko je vázáno na dokument, definuje vazbu mezi konkrétním dokumentem a časovým okamžikem.

Struktura časového razítka se řídí doporučením RFC3161[4]. Časové razítko obsahuje především následující položky:

- Verze protokolu (TSP), v současné době se využívá verze 1.
- Identifikátor politiky poskytovatele časových služeb (policy OID), podle které bylo časové razítko vydáno.
- Hash hodnota – jedná se o hash elektronického dokumentu, ke kterému se časové razítko vydává.
- Sériové číslo časového razítka – jedná se o jedinečné číslo, které každému časovému razítku přiděluje vydávající časová autorita a slouží pro jeho jednoznačnou identifikaci.
- Časová značka – identifikace časového okamžiku (datum + přesný čas na tisícinu sekundy + označení časového pásma).

[4] http://tools.ietf.org/html/rfc3161

- Hodnota Nonce – náhodné číslo, která do žádosti o časové razítko vložil žadatel a vydavatel ji pouze přenáší do výsledného časového razítka.
- Jednoznačná identifikace vydavatele časového razítka.

## 5.1 Autorita vydávající časová razítka

Postupy pro vydávání časových razítek, tj. práva a povinnosti časové autority a práva a povinnosti klientů, jsou popsány v dokumentu politika pro vydávání časových razítek. Pro poskytování této služby je klíčový přesný čas, který se do časového razítka vkládá. Časová autorita musí být schopná doložit přesnost a synchronizaci časového zdroje. Časový zdroj musí být v pravidelných intervalech synchronizován s důvěryhodným synchronizačním zařízením UTC (Universal Time Coordinated = koordinovaný světový čas). Pro synchronizaci údaje vkládaného do časových razítek bývá zpravidla využívána důvěryhodná synchronizační časová infrastruktura (TTI). Jedná se o bezpečnou synchronizační službu, která poskytuje platné a auditovatelné informace, které by byly použity v případě sporu mezi poskytovatelem časových služeb a klientem.

## 5.2 Vydání časového razítka

Časové razítko vydává poskytovatel online po obdržení žádosti od klienta. Postup vydání časového razítka se zcela liší od postupu vydávání certifikátu elektronického podpisu. Pro generování páru klíčů a žádosti o certifikát elektronického podpisu je možné využít standardní a běžně dostupný software, pro generování žádosti o časové razítko je zapotřebí specielní aplikace nebo knihovny, kterou zpravidla nabízí poskytovatel časových služeb. Získání časového razítka lze můžeme rozdělit do několika fází:

- Vytvoření žádosti o vydání časového razítka
- Odeslání žádosti na server časové autority
- Zpracování žádosti na straně poskytovatele a odeslání razítka
- Přijetí odpovědi od serveru časové autority a kontrola klientem

**Vytvoření žádosti o vydání časového razítka**

V podstatě jsou dva způsoby, jak se generují žádosti na straně klienta.

V prvním, častějším případě, jsou žádosti generovány v rámci používané aplikace zajišťující bezpečnou komunikaci. V takovém případě generuje žádosti o časová razítka

serverová část používané aplikace, která využívá poskytovatelem dodané aplikace např. Java aplet nebo knihovna.

Ve druhém, méně častém případě, může klient generovat žádost o časové razítko přímo ze svého počítače prostřednictvím instalované aplikace od poskytovatele.

Žádost o vydání časového razítka musí zejména obsahovat:

- Vygenerovanou hodnotu hash z dokumentu, který má být opatřen časovým razítkem (hash se generuje na straně klienta a poskytovateli se zasílá pouze tento hash. Poskytovatel nesmí zjišťovat zdrojový dokument).
- Volitelně může žádost obsahovat politiku, podle které má být razítko vydané.
- Hodnota Nonce – náhodná hodnota vytvořená na straně klienta, která je poskytovatelem přenesena do vydaného časového razítka a slouží pro spárování žádosti a obdrženého razítka na straně klienta (žadatele).

**Odeslání žádosti na server časové autority**

Vytvořená žádost se odesílá poskytovateli časových služeb prostřednictvím akceptovaného rozhraní, obvykle přes protokol https. Důvodem pro použití zabezpečeného protokolu je zpravidla ten, že se jedná o zpoplatněnou službu, a je tedy potřeba autentizace klienta k serveru poskytovatele. V opačném případě by bylo možné použít běžný http.

**Zpracování žádosti na straně poskytovatele a odeslání razítka**

Server poskytovatele po přijetí žádosti provede následující:

- validační kontroly formální správnosti žádosti a v případě chybné žádosti je vytvořen odpovídající chybový status, jehož formát je normalizovaný dle RFC3161
- pokud žádost prošla validačními kontrolami, je z důvěryhodného zdroje času získán časový údaj a ze zaslaných údajů a získaného časového údaje je vytvořeno časové razítko – výše popsaná datová struktura.
- Tato datová struktura je podepsána, resp. označena prostřednictvím elektronické značky serverem poskytovatele časových služeb, čímž je zaručena správnost údajů časového razítka.
- Časové razítko je odesláno klientovi a zároveň zaarchivováno na straně vydavatele. Některé autority poskytují klientům navíc i certifikát nadřízené časové autority

(TAC – Time Atribute Certificate). Tímto certifikátem se dokládá důvěryhodnost časového zdroje.

Celý tento proces je velice rychlý, zpracování žádosti a vydání časového razítka je provedeno ve zlomku vteřiny. Obvyklá kapacita vydavatele časových razítek jsou jednotky až desítky razítek za vteřinu.

**Přijetí odpovědi od serveru časové autority a kontrola klientem**

Aplikace na straně klienta přijme vygenerované časové razítko ve standardizovaném tvaru. Po přijetí provádí klientská aplikace kontrolu přijatých dat s časovým razítkem dle následujícího postupu:

1) Kontrola, jestli nebyl přijat chybový status, jako reakce na chybně zaslanou žádost.
2) Údaje ze žádosti odpovídají vygenerovanému časovému razítku. Zejména se jedná o hash elektronického dokumentu a použitý algoritmus, dále pak stejné párovací číslo Nonce.
3) V případě, že žádost obsahovala identifikátor politiky, podle kterého mělo být razítko vydáno, musí stejný identifikátor obsahovat i vygenerované časové razítko.
4) Časové razítko musí být označeno platnou elektronickou značkou vydavatele.
5) Musí být platný řetězec důvěry až k certifikátu certifikační autority, která vydala certifikát časové autority. Žádný z certifikátů v tomto řetězci nesmí být uveden na seznamu zneplatněných certifikátů (CRL).

Po úspěšně provedené kontrole získaného časového razítka na straně klienta je razítko uloženo pro další použití, jeho uplatnění je poměrně široké a nemusí být svázáno s konkrétní aplikací.

## 5.3 Využití časového razítka

Vydávání časových razítek není určeno výhradně pro žádný typ klientely, časová razítka mají své uplatnění ve firemní soukromé, i státní sféře.

Příklady využití:

- ochrana skenovaných dokumentů
- elektronická fakturace
- ochrana záznamů v sufitních souborech
- elektronické podatelny
- notářské služby – důvěryhodné archivy elektronických dokumentů

- elektronicky uzavírané smlouvy
- online obchodování

V současné době poskytují v ČR službu kvalifikovaného časového razítka všichni akreditovaní poskytovatelé certifikačních služeb, tj eidenty, První certifikační autorita i Postsignum České pošty.

# 6 Certifikační autority

Certifikační autority vystupují v rámci bezpečné elektronické komunikace jako třetí strany nezávislé na komunikujících stranách.

Funkce certifikačních autorit jsou následující:

- autentizace a registrace ostatních certifikačních autorit a uživatelů
- uložení a distribuce dat
- vydávání certifikátů
- notářské funkce

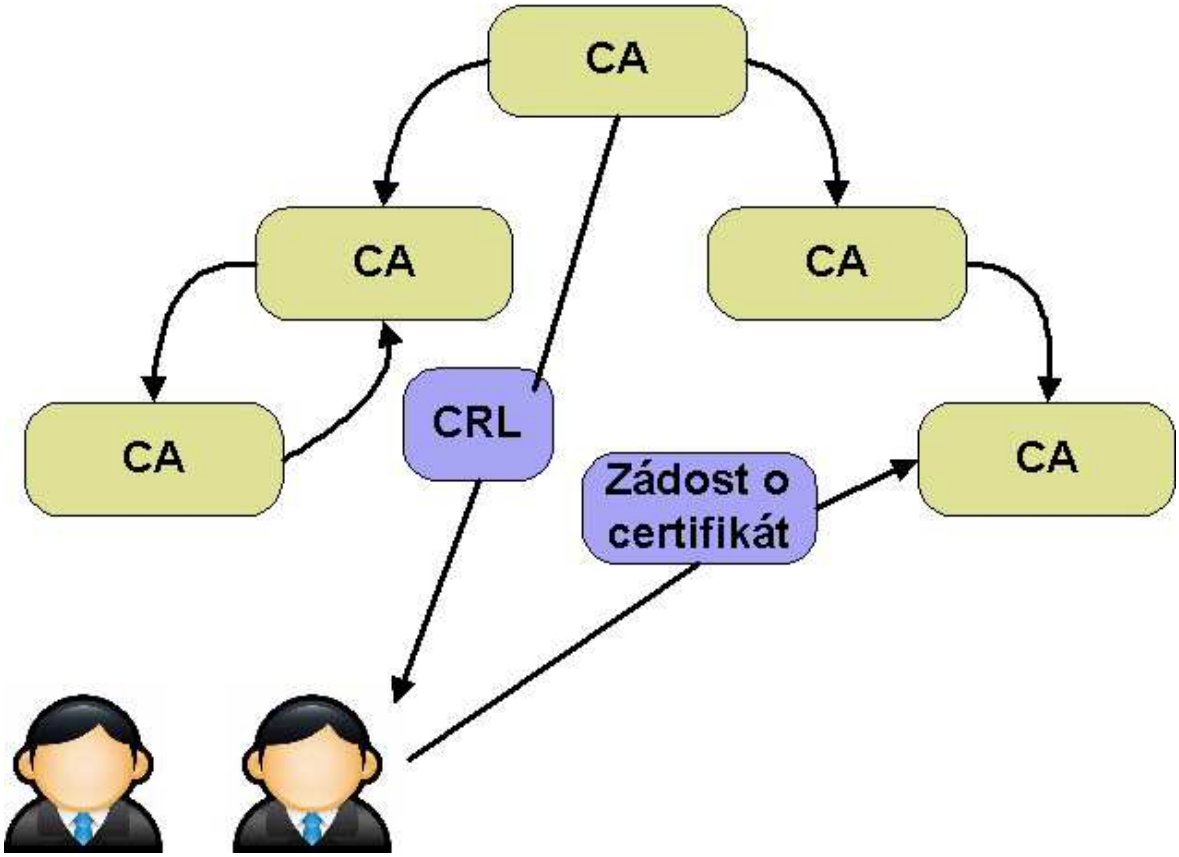
## 6.1 Autentizační funkce certifikačních autorit

Certifikační autorita nemusí existovat samostatně, ale může být součástí systému hiearchicky propojených certifikačních autorit. Teoreticky může existovat složitý řetězec propojených certifikačních autorit, což ale v praxi nebývá obvyklé. Hlavním důvodem je to, že pokud by měly být CA v rámci takového systému propojené, musely by mít stejné, nebo alespoň hodně podobné bezpečnostní politiky. To by asi bylo dost obtížné, protože se zpravidla jedná o různé podnikatelské subjekty, které si navíc často konkurují.

Běžně se ale toto propojení používá v rámci jednoho subjektu pro různé úrovně poskytování služeb nebo v rámci podřízenosti certifikační autority dané legislativou. Jako první příklad lze uvést vydávání certifikátů akreditovanými společnostmi, které jednak vydávají kvalifikované certifikáty a jednak komerční certifikáty. Pro druhý případ se nabízí příklad Slovenské republiky, kde je podřízenost kvalifikovaných certifikačních autorit daná zákonem.

### 6.1.1 Hiearchické propojení

Na následujícím obrázku je znázorněna stromová struktura certifikátu.




**Obrázek 8: Znázornění stromové struktury certifikátu (vlastní zdroj)**

Ve stromové struktuře existují vždy vazby mezi certifikačními autoritami, které jsou bezprostředně pod sebou. Vazby certifikačních autorit ve stromové struktuře fungují na principu, že nadřízená CA vydá certifikát podřízené CA, čímž jí projeví důvěru. Pokud se do existující struktury přidává nová certifikační autorita, pak tato nová CA musí vydat certifikát jí podřízené CA a naopak musí získat certifikát od jí nadřízené CA.

V některých případech se následně vydává certifikát i v opačném směru, čímž vzniká křížová certifikace. Křížová certifikace je ale spíš příklad rovnocenného vztahu dvou CA, než podřízenosti a nadřízenosti.

Ověřování podpisů komunikujících stran se pak provádí prostřednictvím certifikační cesty. Jedná se o řetězec certifikátů, který začíná klientským certifikátem podepisující strany a končí certifikátem, kterému důvěřuje ověřovatel.

Pokud je velká složitost certifikačního stromu, mohou být vydávány certifikáty i mezi CA různých větví. Zkrácení certifikační cesty výrazně zjednodušuje ověřování certifikátu.

### 6.1.2 Autentizace a registrace uživatelů

Úroveň ověřování identity uživatele vůči certifikační autoritě souvisí s mírou důvěry ve vydávané certifikáty této CA.

CA minimálně zajišťuje jedinečnost názvu subjektu, ale neověřuje jeho identitu. Vyšším stupněm je pak ověřování totožnosti podle osobních dokladů, které se provádí na místech registrační autority.

## 6.2 Uložení a distribuce dat

Během provozu certifikačních autorit vzniká velké množství dokumentů citlivé povahy, a tomu odpovídají i požadavky na způsob jejich zpracovávání a uchovávání.

Jedná se o dokumenty získané od klientů a dokumenty vytvořené certifikační autoritou.

Mezi dokumenty získané od klientů patří zejména žádosti o certifikát a s tím spojené dokumenty, jako jsou výpisy z obchodního rejstříku nebo fotokopie osobních dokladů klientů (týká se akreditovaných certifikačních autorit). Tyto dokumenty obsahují osobní údaje klientů a zacházení s nimi se řídí Zákonem o ochraně osobních údajů v aktuálním znění. Systémy zpracovávající tyto údaje proto musí odpovídat požadavkům pro zpracování osobních údajů. Souhlas klienta se zpracováním těchto údajů musí být součástí smlouvy o poskytování certifikačních služeb.

Mezi dokumenty vytvořené certifikační autoritou patří vydané certifikáty, seznamy zneplatněných certifikátů (CRL) a data pro zajištění jedinečnosti některých položek v certifikátech (DN, čísla certifikátů, .. ).

Doba pro uchování veškerých získaných nebo vytvořených dat je pro akreditované certifikační autority stanovena na 10 let. Tomu musí odpovídat nastavené procesy a technologické vybavení.

V souvislosti s technologií elektronického podpisu uchovávají certifikační autority i klienti privátní data sloužící k vlastnímu podepisování – soukromé klíče a certifikáty. Největší hodnotu mají soukromé klíče a certifikát kořenové certifikační autority. Tato data jsou nejvíce chráněnými daty v certifikační autoritě, zneužití nebo odcizení těchto dat by způsobilo ztrátu důvěrnosti všech vydaných certifikátů v rámci certifikační autority.

Způsobů ochrany důvěrných dat je několik, od uložení na disku v zašifrované podobě, uložení na externím nosiči, až po použití speciálního zařízení pro uchování těchto dat.

K uložení privátních dat na externím nosiči se využívá například čipová karta, nebo USB token. Tato zařízení bývají chráněna přístupovým PINem.

Důvěrná data, jako jsou již zmíněné soukromé klíče a certifikáty kořenových certifikačních autorit, bývají uchovávána ve speciálních zařízeních. Tato zařízení odolají logickým i fyzickým útokům a splňují vysoké nároky na rychlost prováděných kryptografických operací. Akreditovaní poskytovatelé vydávající kvalifikované certifikáty mohou používat pouze schválená zařízení.

### 6.2.1 Zveřejňování dat

V souvislosti s provozováním Certifikační autority zveřejňují některá data. Jedná se o zveřejnění dokumentů, jako jsou vydané certifikáty, seznamy zneplatněných certifikátů. V případě kvalifikovaných CA je povinnosti zveřejňovat tyto dokumenty zakotvena v zákonu o elektronickém podpisu včetně pravidelné aktualizace, na tyto dokumenty jsou proto kladeny požadavky na vysokou dostupnost. Zejména v případě seznamu zneplatněných certifikátů by ztráta dostupnosti mohla mít dopad na chod klíčových aplikací spoléhajících na certifikáty dané certifikační autority.

## 6.3 Vydávání certifikátů a další certifikačně správní funkce

Certifikační autorita pracuje z pohledu uživatele jako server služba poskytující definované služby:

- vydání klientského certifikátu – na základě žádosti o vydání klientského certifikátu, která obsahuje klientův veřejný klíč, je podepsaná jeho soukromým klíčem a obsahuje potřebné identifikační údaje v definovaném formátu, je ze strany CA vydán klientský certifikát. Samozřejmě až po proceduře ověření konkrétní osoby. Celý proces vydávání se řídí certifikační politikou, která je nedílnou součástí bezpečnostní politiky každé certifikační autority.
- Zneplatnění certifikátu – existuje několik způsobů jak podat žádost o zneplatnění certifikátu, všechny musí být definované v již zmíněné certifikační politice. Pokud CA vyhodnotí žádost jako oprávněnou, je certifikát zařazen na seznam zneplatněných certifikátů až do doby, kdy jeho platnost vyprší dle data platnosti certifikátu.

Jak již bylo zmíněno, certifikační autorita vydává v pravidelných intervalech seznamy zneplatněných certifikátů. Ke snížení rizika zneužití certifikátu v době od zneplatnění

certifikátu do vydání tohoto certifikátu na CRL je možné využít alternativu, tzv. Delta CRL.

Jedná se o přírůstkové CRL, které jsou vydávány v době mezi jednotlivými CRL a obsahují pouze certifikáty zneplatněné od posledního vydání CRL. V naší legislativě však vydávání Delta CRL není zakotveno a české certifikační autority jej nenabízejí.

Další možností ověření platnosti certifikátu je online ověření pomocí protokolu OCSP (Online Certificate Status Protocol). V tomto případě běží na serveru CA služba, která komunikuje prostřednictvím OCSP a na dotaz poskytuje informace o certifikátu, mimo jiné o jeho platnosti. Tato služba je již na pomezí certifikačních a notářských služeb.

## 6.4 Notářské funkce

Další možností uplatnění certifikačních autorit je v oblasti elektronických notářských služeb. Tato oblast přímo nesouvisí s vydáváním certifikátů, ale v tomto případě vystupuje CA ve vztahu k e svým klientům v roli elektronického arbitra. Certifikáty dané CA jsou v tomto případě pouze využity pro bezpečnou komunikaci, proto musí být oběma stranami akceptovány.

Elektronické notářské funkce souvisí s elektronickými dokumenty, průkaznost vzniku, existence, předávání, zpracování a případné archivace dokumentů. V dnešní době se jedná zejména o služby vydávání časových razítek, atributových certifikátů, potvrzování transakcí a služeb důvěryhodného archivu.

### 6.4.1 Časová razítka

Časovým razítkům je věnována kapitola 5.

### 6.4.2 Atributová autorita

Služby atributové autority nejsou zatím tak rozšířené, jako třeba časová razítka. Certifikáty vydávaná atributovou autoritou jsou jakési doplňky ke standardním klientským certifikátům, některé autority jej mohou vydávat jako doplněk k standardním certifikátům. Atributový certifikát na rozdíl od standardního nese informace o klientovi, které není možné uvádět do standardních certifikátů. Může se jednat o důvěrné informace, které se ale využívají pro autentizaci a autorizaci klienta v rámci bezpečných komunikačních systémů a na základě kterých je možné provádět některé úkony. Do atributového certifikátu lze uvádět libovolné údaje (atributy), jako například interní identifikaci uživatele, zařazení ve společnosti, skupina oprávnění uživatele apod.

Struktura atributového certifikátu vychází z RFC-3281. Atributový certifikát neobsahuje na rozdíl od standardních klientských certifikátů žádný klíč. Stěžejním prvkem certifikátu jsou atributy, které nesou důvěrné informace o vlastníkovi certifikátu.

### 6.4.3 Potvrzování elektronických transakcí

Tato služba umožňuje získat potvrzení o provedení určité elektronické transakce v určitou dobu, stejně jako např. při odesílání doporučeného dopisu je tato transakce potvrzena na přepážce oražením podacího lístku.

Pro potvrzování takových elektronických transakcí se využívá DVC (Data Validation Certificate). DVC jsou vydávány třetí nezávislou stranou, certifikační autoritou. Opět se jedná o podepsanou datovou strukturu, která nese informace vztahující se k dané transakci.

Příkladem použití DVC je potvrzení pravosti elektronického podpisu, což je použitelné zejména v delším časovém horizontu pro příjemce takového dokumentu. Po delší době od vytvoření elektronického podpisu dokumentu může být problém s ověřením jeho pravosti, vzhledem k omezené platnosti certifikátu. Z tohoto důvodu je výhodné přenést odpovědnost za toto ověření na důvěryhodnou autoritu vydávající DVC.

### 6.4.4 Bezpečnost certifikačních autorit

Všechny služby, které certifikační autority poskytují, se týkají bezpečné komunikace. Proto je tedy vlastní bezpečnost Certifikační autority klíčová pro poskytování všech těchto služeb. Vysoká bezpečnost je na jednu stranu žádoucí, na druhou však omezuje uživatele CA, proto je potřeba vždy hledat kompromis.

Každá certifikační autorita musí mít vytvořenou tzv. bezpečnostní dokumentaci, kde jsou implementována bezpečnostní pravidla. Pro kvalifikované certifikační autority, je definovaná povinná dokumentace v zákoně o elektronickém podpisu a dalších vyhláškách.

Mezi povinné dokumenty patří:

- certifikační politika
- prováděcí směrnice
- globální bezpečnostní politika
- systémová bezpečnostní politika
- krizový plán a plán obnovy

Ne všechny typy uvedených dokumentů jsou dostupné veřejnosti. Zveřejněny musí být dokumenty, které jsou nezbytné k posouzení klienta o vhodnosti dané certifikační autority

pro jeho účel. U každé certifikační autority musí být minimálně dostupná certifikační politika a v případě kvalifikovaných CA musí být dle zákona zveřejněna i tzv. Zpráva pro uživatele, která obsahuje zjednodušenou podobu certifikační politiky a usnadní klientům orientaci v postupech CA a nabízených službách.

Certifikační autority v ČR lze rozdělit na kvalifikované certifikační autority, akreditované certifikační autority a komerční certifikační autority.

**Kvalifikované certifikační autority** vydávající kvalifikované certifikáty se řídí legislativou ČR, zejména pak zákonem o elektronickém podpisu a dalšími zákony a vyhláškami. Jejich bezpečnost je kontrolována orgány státní správy.

**Akreditované certifikační** získaly akreditaci od Ministerstva vnitra a jimi vydané certifikáty jsou akceptované při komunikaci se státní správou.

**Komerční certifikační autority** jsou zpravidla určeny k zabezpečené komunikaci v rámci dané organizace nebo daného systému nebo aplikace. Příkladem může být komunikace klienta s bankovním systémem. Akceptování certifikátů komerčních certifikačních autorit je zpravidla omezeno na danou organizaci nebo systém.

# 7 E-GOVERNMENT

Tento pojem představuje elektronizaci státní správy a samosprávy. V ideálním případě by e-Government pokrýval kompletně všechny procesy a komunikaci v rámci výkonu veřejné moci včetně rozhodovacích procesů. K hlavním výhodám e-Governmentu patří:

- rychlost
- jednoduchost a uživatelská přívětivost
- neomezené úřední hodiny
- transparentnost a procesů a rozhodování
- efektivita procesů

Podmínkou pro zavedení e-Government je legislativní podpora - veškeré změny na úřadech, které v rámci e-Governmentu zavedou, musí mít oporu v platné legislativě.

## 7.1 Elektronické podatelny

Pojem elektronická podatelna je definován v zákonu o elektronickém podpisu a patří mezi klíčové pojmy e-Governmentu. Jedná se o pracoviště orgánu veřejné moci, které je jakýmsi styčným bodem pro zajištění komunikace mezi úřadem a občanem.

Zřízení elektronické podatelny také vyplývá z nařízení vlády č. 495/2004 Sb., které stanoví, že pokud má úřad povinnost přijímat a odesílat datové zprávy se zaručeným elektronickým podpisem, musí být k těmto účelům zřízena elektronická podatelna.

Funkce elektronické podatelny zahrnují:

- příjem a odesílání datových zpráv dálkovým přístupem i na technickém nosiči dat.
- kontrolu, zda jsou zprávy čitelné a schopné dalšího zpracování v orgánu veřejné moci, tj. jestli je elektronická zpráva v některém z akceptovaných formátů.
- ověření, že zpráva neobsahuje viry, červy, trojské koně apod.
- ověření platnosti certifikátu náležejícího k elektronickému podpisu,
- předání ověřeného podání k dalšímu řízení.

Vlastní funkci elektronické podatelny popisuje č. 496/2004 Sb. o elektronických podatelnách, které stanoví postupy pro přijímání a odesílání datových zpráv a definuje povinné údaje kvalifikovaného certifikátu, na základě kterých je možné podepisující osobu jednoznačně identifikovat.

Pokud podání má v uvedených bodech nedostatky, postupuje se podle předpisů upravujících odstraňování vad podání.

Pracoviště elektronické podatelny se také řídí standardy ISVS (informační systémy veřejné správy).

Názvy emailových adres elektronických podatelen jsou stanoveny ve standardu ISVS pro komunikaci informačních systémů 002/01.03. Elektronické podatelny musí mít název schránky ve formátu posta@<doména orgánu veřejné moci>.cz.

Pro provoz elektronické podatelny je potřeba mít zpracovaný bezpečnostní projekt podle Standardu ISPS 005/01.01. Součástí projektu musí být definování požadavků na personální a fyzickou bezpečnost, bezpečnost IS a režimové zabezpečení.

Technické vybavení podatelny musí být ve shodě se Standardem ISVS016/01.01.

## 7.2 Datové schránky

Zákon č. 300/2008 Sb., o elektronizaci některých procesních úkonů v oblasti orgánů veřejné moci upravuje elektronickou komunikaci mezi orgány veřejné moci navzájem a mezi orgány veřejné moci a právnickými osobami. V některých případech zákon stanoví povinné využití elektronické komunikace, k čemuž předepisuje použití tzv. datových schránek.

Datové schránky jsou obdobou fyzických poštovních schránek, do kterých jejich vlastníci přistupují bezpečným způsobem za použití průkazných autentizačních a autorizačních procedur. Pro autentizaci se v tomto případě využívá komerčních. Při komunikaci se dále využívá časových razítek, důležité úkony jako je odesílání zpráv, přístupy do vlastní schránky, vybírání schránky jsou doloženy kvalifikovanými časovými razítky. Datové schránky umožňují při odesílání zpráv využívání zaručeného elektronického podpisu. Vzhledem k použitým technologiím je srovnatelná důvěryhodnost a právní váha komunikace přes datové schránky s klasickým doručováním dokumentů do vlastních rukou.

# 8 Legislativní rámec

Pro úspěšné zavedení bezpečné komunikace s využitím elektronického podpisu je nutným předpokladem vytvoření jasných pravidel pro všechny zúčastněné strany.

Navíc pro možnost komerčního využití zabezpečené elektronické komunikace je potřeba nastavení takových pravidel, aby takto zabezpečená elektronická komunikace byla brána jako rovnocenná běžné papírové komunikaci. Proto je také nezbytné zakotvit tato pravidla a principy v závazných dokumentech a zákonech.

Na mezinárodní úrovni se stala průkopníkem standardizace elektronického podpisu komise OSN pro mezinárodní právo – UNCITRAL (United Nations Commission on International Trade Law). Tato komise aktuálně zahrnuje 60 členských států, za Českou republiku zastřešuje účast Ministerstvo průmyslu a obchodu. Významnými dokumenty vydanými komisí UNCITRAL pro oblast elektronické komunikace jsou:

- Doporučení týkající se právní závaznosti elektronických údajů
- Vzorový zákon o elektronickém obchodu
- Vzorový zákon o elektronickém podpisu
- Úmluva o užití elektronických sdělení v mezinárodním obchodě

Klíčovým dokumentem je právě vzorový zákon o elektronickém obchodu. V tomto dokumentu na stejnou úroveň postavena písemná i elektronická forma přenosu dat, což vytváří prostředí pro elektronické obchodování, přičemž vzorový zákon je nezávislý na konkrétním prostředí a technologii.

Po jeho schválení byl připraven a následně schválen i vzorový zákon o elektronickém podpisu., který obsahuje jednak terminologický základ, pojmy a definice a jednak průvodce pro ustanovení modelového zákona o elektronickém podpisu.

## 8.1 Směrnice EU

V EU vývoj směřoval k vytvoření prostředí, které bude akceptovat prostředky bezpečné elektronické komunikace jako rovnocennou alternativu k používání papírových dokumentů. V říjnu 1997 byla evropskému parlamentu předložena studie, která se zabývala zajištěním bezpečnosti a důvěryhodnosti elektronické komunikace a měla směřovat k evropským zásadám pro digitální podpisy a šifrování. Na základě této studie byla 13.12.1999 vydána směrnice Evropského parlamentu a Rady 1999/93/ES, která se

zabývá elektronickým podpisem a která je závazná dodnes. Směrnice se zabývá využitím elektronického podpisu pro účely autentizace a zaručeným elektronickým podpisem, který má být rovnocenný klasickému podpisu. Směrnice je zaměřena na aplikaci elektronického podpisu a právní validitu elektronického podepisování dokumentů. Dále jsou zde uvedeny požadavky pro všechny zúčastněné strany zapojené do procesu elektronického podepisování. Směrnice stanovuje nepopiratelnost u zaručených elektronických podpisů a je napsána na obecné úrovni, tzn., že neřeší technologickou úroveň a žádná schémata pro poskytovatele certifikačních služeb.

Směrnice předpokládá využití elektronického podpisu v mnoha oblastech, mimo jiné ve veřejném sektoru pro komunikaci mezi orgány státní správy a samosprávy a pro komunikaci těchto orgánů s občany. Podmínkou pro plnohodnotné využití elektronického podpisu je plná právní uznatelnost. Zřetel je také kladen na mezinárodní uznatelnost elektronického podpisu, aby se mohl využívat pro elektronickou obchodní komunikaci v mezinárodním obchodním styku.

Směrnice stanoví povinnost členských států EU poskytovat komisi EU a ostatním členským zemím informace o národním akreditačním schématu, národních institucích zodpovědných za akreditaci a dohled a jména a adresy poskytovatelů certifikačních služeb v dané zemi.

Směrnice dále zavádí společnou terminologii související s elektronickým podpisem. Ta je pak přebírána do legislativy jednotlivých členských zemí.

Směrnice předpokládá vznik samostatných zákonů v jednotlivých členských zemích s ustanovením vlastních akreditačních schémat. Dále je zde definována odpovědnost za dohled a kontrolu poskytování služeb elektronického podpisu na úrovni jednotlivých států.

Dle směrnice je právní účinnost elektronického podpisu ve vztahu k podepsanému elektronickému dokumentu stejná, jako v případě vlastnoručního podpisu na dokumentu. S tím souvisí i požadavek na akceptaci zaručeného elektronického podpisu jako důkazu v případě soudního řízení.

**Požadavky jednotlivých států na elektronický podpis**

Požadavky na elektronický podpis, který bude v dané zemi akceptován pro komunikaci se státní správou, lze rozdělit do následujících kategorií:

- užívání kvalifikovaného podpisu
- užívání kvalifikovaného certifikátu

- užívání nedefinovaného certifikátu
- užívání nedefinovaného podpisu
- užívání autentizačního mechanizmu

Kvalifikovaný podpis

Z uvedených kategorií je z kvalitativního hlediska nejpřísnější požadavek na užívání kvalifikovaného podpisu. V tomto případě musí být pro vytváření zaručeného elektronického podpisu využito bezpečné zařízení. (SSCD – Secure Signature Creation Device) a pro ověřování elektronického podpisu využito kvalifikovaného certifikátu. Za bezpečné zařízení SSCD se považuje čipová karta nebo např. USB Token, které splňují příslušné technologické a bezpečnostní standardy.

Podpis založený na kvalifikovaném certifikátu

Tato kategorie je méně přísnou a levnější variantou oproti kvalifikovanému podpisu, při zachování vysoké míry bezpečnosti. V tomto případě legislativa neřeší, jaký nástroj je využíván při vytváření elektronického podpisu. Požadováno je pouze využití párového klíče spojeného s kvalifikovaným certifikátem. Tato kategorie elektronických podpisů je využívána i v České republice.

Podpis bez kvalifikovaného certifikátu, nedefinovaný podpis

Do této kategorie patří využívání elektronického podpisu bez kvalifikovaného certifikátu, resp. bez jakéhokoliv certifikátu, což znamená, že nad využívanými elektronickými podpisy nemá stát žádnou možnost dohledu.

Autentizační mechanizmus

V této kategorii je komunikace zabezpečena pouze autentizací uživatele s použitím autentizačního tajemství, např. hesla, a komunikace za použití elektronického podpisu není vůbec vyžadována.

Implementace Směrnice EU do jednotlivých legislativ členských zemí byla provedena různými způsoby:

**Vydání samostatné právní normy**

Tento způsob je mezi členskými státy EU nejrozšířenější, touto cestou se vydala i Česká republika, kde tuto normu představuje Zákon o elektronickém podpisu.

**Zapracování dopadů direktivy do všech relevantních dokumentů**

V tomto případě se jedná nejen o vydání samostatné právní normy, ale i doplnění dopadů spojených s užíváním elektronického podpisu do všech relevantních dokumentů.

Pro úplnost uvádím dva méně využívané způsoby zapracování do lokální legislativy, a sice úprava právních norem v jednotlivých oblastech a úprava právních norem podle potřeby pro konkrétní aplikace elektronického podpisu.

## 8.2 Česká legislativa

České právní normy vztahující se k elektronickému podpisu a poskytovatelům certifikačních služeb z uvedené evropské směrnice. Jedná zejména o následující právní normy:

- Zákon č. 227/2000 Sb., o elektronickém podpisu.
- Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.
- Vyhláška ÚOOU č. 366/2001 Sb.
- Zákon č. 486/2004 Sb. (227/2000 Sb.)
- Vyhláška č. 496/2004 Sb., o elektronických podatelnách
- Nařízení vlády č. 495/2004 Sb., kterým se provádí Zákon č. 227/2000 Sb.
- Zákon č. 499/2004 Sb., o archivnictví a spisovné službě
- Zákon č. 101/2000 Sb., o ochraně osobních údajů

### 8.2.1 Zákon o elektronickém podpisu

V České republice je zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů klíčovým legislativním dokumentem. V duchu tohoto zákona zastává roli kontrolního a akreditačního orgánu v ČR Ministerstvo vnitra ČR (MVČR). Z toho pro MVČR vyplývají povinnosti, zejména dozor nad dodržováním zákona o elektronickém podpisu, udělování akreditací poskytovatelům certifikačních služeb a vyhodnocování shody nástrojů elektronického podpisu s požadavky stanovenými zákonem.

Další důležitou rolí Zákona o elektronickém podpisu je vymezení pojmů, které vychází a případně upřesňuje nebo rozšiřuje popis Směrnice EU.

**Elektronický podpis** – *údaje v elektronické podobě, které jsou připojené k datové zprávě, nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.*[ZAK227]

**Zaručený elektronický podpis** – *zaručeným elektronickým podpisem je elektronický podpis, který splňuje následující požadavky:*

1) *je jednoznačně spojen s podepisující osobou*
2) *umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě*
3) *byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou*
4) *je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat* [ZAK227]

**Povinnosti pro komunikující strany**

Ze zákona o elektronickém podpisu vyplývají povinnosti pro podepisující osoby i spoléhající osoby v rámci zabezpečené elektronické komunikace.

**Podepisující osoba** je osoba vytvářející elektronický podpis a je povinna:

- *Zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití.*
- *Uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu.* [ZAK227]

**Označující osoba** je osoba vytvářející elektronickou značku a platí zde obdobná pravidla jako pro osobu podepisující.

**Držitel certifikátu**

*Držitel certifikátu je povinen bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu a ve vztahu ke kvalifikovanému systémovému certifikátu.* [ZAK227]

**Spoléhající osoba** se podle zákona o elektronickém podpisu rozumí příjemce dokumentu opatřeného elektronickým podpisem. Spoléhající osoba je povinna si ověřit, že:zaručený elektronický podpis svázaný s dokumentem je platný, a zároveň certifikát podpisu je stále platný, tj. nevypršela mu platnost a nebyl zneplatněn.

**Ověření zaručeného elektronického podpisu**

Ověřování zaručeného elektronického podpisu nebo značky se provádí podle standardů asymetrických kryptografických algoritmů a hashovacích funkcí odpovídajících schématu

použitého při vytváření podpisu. Ověřování probíhá automatizovaně pomocí k tomu určené aplikace bez zásahu uživatele.

Používané standardy asymetrických algoritmů:

RSA, DSA, ECDSA-FP, ECDSA-F2M, ECGDSA-FP, ECGDSA-F2P.

Používané standardy hashovacích funkcí: SHA1, SHA2, RIPEND160

**Ověření platnosti certifikátu**

Ověřování se provádí pomocí aplikace bez zásahu uživatele a skládá se z následujících kroků.

1) Ověření, jestli v době doručení datové zprávy byl certifikát podepisující osoby v intervalu doby platnosti.
2) Ověření elektronické značky kvalifikovaného poskytovatele, kterou je označen kvalifikovaný certifikát podepisující osoby.
3) Ověření, jestli kvalifikovaný certifikát podepisující osoby nefiguruje v seznamu zneplatněných certifikátů (CRL), který předchází okamžiku doručení podepsané datové zprávy. Tento krok musí zpravidla provést ověřovatel ručně.
4) Ověření elektronické značky, kterou je podepsán seznam zneplatněných certifikátů.
5) Ověření certifikační cesty – pro ověření platnosti certifikátu podepisující nebo označující osoby se musí provést ověření všech certifikátů v certifikační cestě tak, jak je uvedeno v bodech 1) až 4).

   Certifikační cesta vzniká v případě, že kvalifikovaný systémový certifikát poskytovatele je opět založen na kvalifikovaném certifikátu nadřízené certifikační autority. Takovému zřetězení certifikátů se říká certifikační cesta.

**Ověření platnosti časového razítka**

To spočívá v ověření platnosti elektronické značky kvalifikovaného časového razítka a v ověření platnosti kvalifikovaného certifikátu, na kterém je založena elektronická značka. Postupy už jsou popsány v předchozích odstavcích.

**Povinnosti kvalifikovaných poskytovatelů certifikačních služeb**

Celý zákon o elektronickém podpisu je zaměřen zejména na kvalifikované certifikační autority poskytující certifikační služby v ČR, proto největší část zákona se také věnuje právě kvalifikovaným poskytovatelům certifikačních služeb. Zákon obsahuje

- požadavky na způsobilost poskytovatele certifikačních služeb

- povinnosti certifikačních autorit při vydávání kvalifikovaných certifikátů a kvalifikovaných razítek

Postupy poskytovatelů kvalifikovaných certifikačních služeb jsou dále upraveny vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Každý poskytovatel kvalifikovaných certifikačních služeb musí vést podrobnou dokumentaci o:

- veškerých poskytovaných službách
- veškerých užívaných postupech
- užívaných technologiích v rámci celé CA

Souhrnně se tato dokumentace nazývá Bezpečnostní dokumentace.

### 8.2.2 Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb.

Vyhláškou upravuje ministerstvo vnitra ČR postupy užívané poskytovateli kvalifikovaných certifikačních služeb, požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek.

### 8.2.3 Zákon č. 486/2004 Sb., úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

Jedná se o novelu zákona 227/2000 Sb. , o elektronickém podpisu, která řeší zásadní výtky původního znění zákona uvedeny níže:

- nekompatibilita zákona s ES
- zákon nepopisoval kvalifikovaná časová razítka
- zákon neumožňoval použití certifikátů elektronického podpisu, které byly vydána mimo Českou republiku, v rámci našeho zákona.
- V zákoně nebylo zahrnuto používání elektronických značek, tj. označování dokumentů automatizovaně systémem nebo aplikací bez přímého zásahu člověka.

Zákon touto novelizací zavádí nové pojmy:

- Časová razítka
- Elektronická značka
- Elektronické podatelny
- Zahraniční certifikáty

### 8.2.4 Nařízení vlády č. 495/2004 Sb., kterým se provádí Zákon č. 227/2000 Sb.

Tímto nařízením je orgánům veřejné moci ukládáno za povinnost zřídit vlastní elektronické podatelny, nebo v případě malého objemu elektronické komunikace zajistit elektronickou komunikaci prostřednictvím jiného úřadu. Se zřízením elektronické podatelny souvisí i povinnost, aby příslušní pracovníci podatelny kvalifikované certifikáty elektronického podpisu. Nařízení dále stanoví způsob ochrany zpracovávaných informací.

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

Tato vyhláška se zabývá postupy orgánů veřejné moci uplatňovanými při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny. Vyhláška dále stanoví strukturu údajů kvalifikovaného certifikátu, podle kterých je možné jednoznačně identifikovat podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny. Vyhláška navazuje na výše zmíněné nařízení vlády č. 495/2004 Sb.

### 8.2.6 Zákon č. 101/2000 Sb., o ochraně osobních údajů

Tento zákon upravuje práva a povinnosti při zpracování osobních údajů a definuje tzv. zpracovatele osobních údajů. Zákon slouží k naplnění práva na ochranu před neoprávněným zasahováním do soukromí. Zákon je v souladu s evropskými právy a mezinárodními smlouvami.

Vzhledem k povaze dat zpracovávaných poskytovateli certifikačních služeb jsou tito poskytovatelé z pohledu zákona o ochraně osobních údajů v roli zpracovatelů osobních údajů.

# 9 Praktická část – návrh vytvoření dokumentu

Cílem této kapitoly je vytvořit návrh jednoho z klíčových dokumentů pro poskytování kvalifikovaných certifikačních služeb - vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů - které by odpovídaly legislativním požadavkům na tyto dokumenty. V rámci tohoto návrhu je popsána možná struktura dokumentu Systémová bezpečnostní politika. V jednotlivých kapitolách je uvedeno, co by mělo být popsáno v textu těchto dokumentů.

Požadavky na kvalifikované a akreditované poskytovatele certifikačních služeb jsou obecně definovány v zákoně o elektronickém podpisu upřesněny ve vyhlášce o postupech kvalifikovaných poskytovatelů certifikovaných služeb.

**Zákon o elektronickém podpisu** definuje kvalifikovaného poskytovatele certifikačních služeb a akreditovaného poskytovatele certifikačních služeb:

*Kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6.* [ZAK227]. Podle § 6 je poskytovatel povinen oznámit Ministerstvu vnitra nejméně 30 dní před zahájením poskytování kvalifikovaných služeb.

*Akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona.* [ZAK227]

Rozdíl mezi kvalifikovaným poskytovatelem a akreditovaným poskytovatelem je ten, že:

*V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen "uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám* [ZAK227].

Zákon o elektronickém podpisu obecně definuje povinnosti kvalifikovaných a akreditovaných poskytovatelů, jako je:

- zveřejňování informací jako jsou informace o jeho identitě, o vydaných a zneplatněných certifikátech,
- zajištění kvalifikovaných pracovníků,

- používání bezpečných systémů a nástrojů elektronického podpisu a bezpečných postupů, které těchto systémů a nástrojů využívají,
- používání bezpečných systémů pro uchovávání kvalifikovaných certifikátů, případně kvalifikovaných časových razítek,
- povinnosti kvalifikovaného poskytovatele vůči klientům, tj. forma dokumentace potřebná pro vydání kvalifikovaného certifikátu, rozsah informování klienta před vydáním certifikátu, apod.

Dále se zde popisuje povinnost pro kvalifikovaného poskytovatele pro uchovávání dokumentace z provozování certifikačních služeb a její zajištění před ztrátou, zneužitím nebo poškozením a povinnost zachovávat mlčenlivost zaměstnanců kvalifikované certifikační autority.

Zákon kvalifikovanému poskytovateli také ukládá povinnosti spojené s vydáváním kvalifikovaných certifikátů a razítek:

- povinné náležitosti vydávaných certifikátů a časových razítek,
- přesnost, pravdivost a úplnost údajů v cetrifikátech,
- povinnost bezpečného ověření identity osoby před vydáním kvalifikovaného certifikátu,
- zajištění přesného časového údaje pro účely evidence časového okamžiku úkonů, jako je vydání certifikátu, zneplatnění certifikátu nebo vydání časového razítka,
- poskytování informací o podmínkách pro využívání certifikátů a časových razítek třetím stranám,
- povinnost neprodleného zneplatnění certifikátu na žádost držitele certifikátu a v dalších případech,
- neprodlené vydání časového razítka po přijetí žádosti o jeho vydání, apod.

**Vyhláška o postupech kvalifikovaných poskytovatelů certifikovaných služeb** rozvádí a upřesňuje požadavky definované na obecné úrovni zákonem o elektronickém podpisu.

Vyhláška stanoví:

- Zajištění informačních povinností vyplývajících ze zákona o elektronickém podpisu. Týká se informací o identitě poskytovatele, jeho kvalifikovaném systémovém certifikátu, seznamu zneplatněných certifikátů, informování osob o

podmínkách využívání kvalifikovaných certifikačních služeb ještě před uzavřením smlouvy o poskytování certifikačních služeb.

- Požadavky kvalifikovaný personál certifikační autority
- Požadavky na bezpečné systémy a nástroje certifikační autority včetně nástrojů pro bezpečné uchovávání kvalifikovaných certifikátů
- Způsoby uchovávání provozní dokumentace certifikačních autorit
- Zajištění bezpečnosti zveřejňovaných seznamů vydaných kvalifikovaných certifikátů (u certifikátů, k jejichž zveřejnění dal držitel souhlas) a seznamu zneplatněných certifikátů (CRL).
- Určení přesného časového okamžiku pro vydávání a zneplatňování kvalifikovaných certifikátů a pro vydávání kvalifikovaných časových razítek. V případě časových razítek i zajištění přesnosti času, aby odpovídal hodnotě koordinovaného světového času.
- Způsob poskytování informací třetím osobám o podmínkách využívání kvalifikovaných certifikátů i kvalifikovaných časových razítek a informace o akreditaci dané certifikační autority.
- Způsob zneplatnění certifikátů
- Náležitosti opatření proti padělání kvalifikovaných časových razítek
- Postupy pro bezpečné vytváření elektronických podpisů a značek.

Rozebírat všechny oblasti, které vyhláška upřesňuje, je nad rámec této diplomové práce. Tato praktická část se ale zaměřuje na vytvoření návrhu jednoho z klíčových dokumentů bezpečnostní dokumentace kvalifikoavného poskytovatele certifikačních služeb. V této vyhlášce je definováno, které konkrétní dokumenty spadají do bezpečnostní dokumentace certifikační autority. Jedná se o: [VYH378]

- *certifikační politika pro vydávání kvalifikovaných certifikátů, pokud poskytovatel tuto službu zajišťuje,*
- *certifikační politika pro vydávání kvalifikovaných systémových certifikátů, pokud poskytovatel tuto službu zajišťuje,*
- *politika pro vydávání kvalifikovaných časových razítek, pokud poskytovatel tuto službu zajišťuje,*
- *politika pro vydávání prostředků pro bezpečné vytváření elektronických podpisů, pokud poskytovatel tuto službu zajišťuje,*

- *certifikační politiky pro vydávání nadřízených kvalifikovaných systémových certifikátů,*
- *zprávy pro uživatele,*
- *certifikační prováděcí směrnice nebo jiné prováděcí směrnice k poskytovaným službám ,*
- *celková bezpečnostní politika,*
- *systémová bezpečnostní politika,*
- *plán pro zvládání krizových situací a plán obnovy.*

Z uvedeného seznamu dokumentů má certifikační autorita zpracované vždy jen ty, které se jí týkají (např. ne všichni poskytovatelé kvalifikovaných certifikačních služeb nabízejí i služby časové autority apod.).

Ne všechny dokumenty potřebné pro provozování certifikační autority jsou veřejné. Co ale určitě veřejné bude, jsou certifikační politiky a zpráva pro uživatele, někdy i části certifikační prováděcí směrnice.

Certifikační politiky jsou závazné dokumenty, které popisují zásady uplatňované při poskytování certifikačních služeb. Struktura těchto dokumentů vychází z RFC-3647[5], který je součástí vyhlášky č. 378/2006 Sb.

Certifikační prováděcí směrnice vychází ze stejného RFC jako certifikační politiky, ale na rozdíl od ní ze zabývá popisem interních postupů poskytovatele certifikačních služeb. To je také důvod, proč certifikační prováděcí směrnice nebývá veřejným dokumentem, nebo je pouze z části.

Celková bezpečnostní politika je neveřejný dokument, který stanoví cíle a popis způsobů zabezpečení důvěryhodných systémů CA a specifikuje zásady a předpisy řešící bezpečnost.

Systémová bezpečnostní politika bývá zpracována na základě analýzy rizik, kde jsou definována:

- aktiva těchto systémů
- hrozby, které na ně působí
- zranitelná místa
- pravděpodobnost výskytu hrozeb
- odhad následků hrozeb

Na základě těchto informací stanoví odpovídající bezpečnostní opatření.

[5] http://www.ietf.org/rfc/rfc3647.txt

Plán pro zvládání krizových situací je dokument obsahující popis postupů, které by byly uplatněny v případě výskytu mimořádné situace.

Splnění povinností kvalifikované certifikační autority stanovených zákonem o elektronickém podpisu a vyhláškou o postupech kvalifikovaných poskytovatelů certifikovaných služeb se zpravidla dokládá právě touto bezpečnostní dokumentací.

V následujícím textu se práce zaměřuje na návrh dokumentu Systémová bezpečnostní politika. Dle vyhlášky o postupech kvalifikovaných poskytovatelů certifikovaných služeb má tento dokument obsahovat následující body:

*a) stanovení cílů při ochraně informací,*

*b) stanovení způsobu zajištění bezpečnosti,*

*c) určení pravomocí a odpovědností při provozování důvěryhodných systémů,*

*d) pravidla a postupy konkrétně definující způsob správy a ochrany informačních technologií, aktiv informačních systémů a způsob distribuce informací v rámci důvěryhodných systémů a jiných systémů, které mají s důvěryhodnými systémy vazby,*

*e) způsoby uplatnění celkové bezpečnostní politiky ve vztahu k provozování důvěryhodných systémů,*

*f) popis důvěryhodných systémů, jejich vnitřních, vnějších a vzájemných vazeb,*

*g) vyhodnocení analýzy rizik a popis bezpečnostních opatření podle odstavce 5,*

*h) způsob šíření časového údaje v rámci důvěryhodných systémů, pokud poskytovatel poskytuje službu vydávání kvalifikovaných časových razítek.*[VYH378]

Zpracování dokumentu systémová bezpečnostní politika musí odpovídat požadavkům na české technické normy, které jsou uvedeny v příloze vyhlášky:

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

Vyhláška také definuje dokumenty z bezpečnostní dokumentace, které poskytovatel certifikačních služeb je povinen zveřejňit. Systémová bezpečnostní politika nepatří mezi zveřejňované dokumenty.

Následujících kapitoly obsahují návrh dokumentu systémová bezpečnostní politika kvalifikované certifikační autority.

## 9.1 Definice struktury dokumentu

V této kapitole je popsána struktura celého dokumentu Systémová bezpečnostní politika certifikační autority. V tomto případě je úvod dokumentu věnován formálnímu uvedení do problematiky a následně je dokument rozdělen do tří částí podle rozdělení pracovišť certifikační autority do třech typů: centrální pracoviště – datová centra, centrální pracoviště – klientské centrum a pracoviště registračních autorit. Na každý typ pracoviště jsou kladeny specifické požadavky, proto je toto rozdělení do samostatných kapitol nezbytné. Směrnici by bylo možné také rozdělit do třech samostatných směrnic.

## 9.2 Seznam použitých pojmů a zkratek

Každá organizace používá v rámci vlastní dokumentace řadu specifických pojmů a zkratek. V této kapitole je uveden seznam těch pojmů a zkratek, se kterými směrnice pracuje. Tyto pojmy už dále v textu nejsou vysvětlovány.

## 9.3 Organizačního zajištění

Organizační zajištění provozu certifikační autority bude vzhledem k rozsahu zřejmě popsáno v samostatném dokumentu, kde budou definovány jednotlivé role pro provozovanou certifikační autoritu. V této kapitole je tato dokumentace pouze zmíněna, protože tyto role se ve směrnici používají.

## 9.4 Úvodní ustanovení

### 9.4.1 Návaznosti na ostatní dokumenty

Tento dokument bude podřízeným dokumentem celkové bezpečnostní politiky v rámci společnosti, které certifikační autoritu provozuje. Případně může být součástí dokumentace, která obecně popisuje politiku bezpečnosti IT v rámci společnosti. Tyto vazby jsou v této kapitole definovány a musí být určeny návaznosti i případy, kdy by se jednotlivé dokumenty překrývaly. Mělo by platit, že oblasti, které nejsou rozpracovány v této směrnici, se řídí nařízenou směrnicí.

### 9.4.2 Správa dokumentu

Přiměřenost a aktuálnost ustanovení tohoto dokumentu musí být pravidelně kontrolována. V této kapitole bude uvedena požadovaná periodicita kontrol případně další požadavky na

mimořádné kontroly dokumentace. Příkladem může být požadavek na kontrolu minimálně jedenou za rok a při každé změně architektury certifikační autority nebo jiné významné změně na úrovni organizace s dopadem na CA. Dále zde bude uvedena odpovědnost konkrétní role za tyto kontroly a přípravu případných změn.

### 9.4.3 Rozsah platnosti

Po vydání dokumentu formou interní směrnice je dokument závazný jako součást pracovních předpisů pro pracovníky certifikační autority podílející se na provozu, správě, údržbě, rozvoji, kontrole a auditu. Bude zde definováno, jakých konkrétních pracovišť se dokument týká. Závaznost pro externí dodavatele musí být součástí příslušného smluvního vztahu.

## 9.5 Cíle dokumentu

### 9.5.1 Bezpečnostní cíle

Bezpečnostní opatření mají za cíl především zajistit bezpečnost CA v souladu s požadavky zákona č. 227/2000 Sb., v platném znění a navazujících předpisů, jako jsou:

- chránit důvěrnost soukromých klíčů CA (kořenové, podepisovací)
- odpovídající ověřování identit žadatelů před vydáváním certifikátů
- zabezpečení rychlé reakce na oprávněné žádosti o zneplatnění certifikátu a pravidelné vydávání CRL se zveřejněním v souladu s certifikační politikou
- zajištění odpovídající dostupnosti služeb certifikační autority dle certifikační politiky
- v souladu s legislativou zajištění bezpečného uložení všech dokumentů CA, mimo jiné v souladu se zákonem č. 101/2000 Sb., v platném znění.
- Zajistit auditovatelnost všech činností spojených s provozem CA

### 9.5.2 Vyhodnocení analýzy rizik

Tento dokument se navrhuje na základě předem provedené analýzy rizik, jejíž výsledky budou uvedeny v samostatném dokumentu a zde bude na dokument uveden odkaz.
Dále zde budou shrnuty výsledky této analýzy a vysvětlení těchto výsledků.

## 9.6 Obecné zásady bezpečnosti

### 9.6.1 Řízení

#### 9.6.1.1 Infrastruktura bezpečnosti IT

Zde bude uvedena odpovědnost jednotlivých rolí za dodržování ustanovení této bezpečnostní politiky. Odpovědnosti za jednotlivé činnosti mohou být také převzaty z nadřízeného dokumentu. Dále zde bude uvedena role odpovědná za implementaci zásad bezpečnostní politiky.

#### 9.6.1.2 Přístup třetích stran (outsourcing)

Outsourcing provozu CA, zajištění kontinuity provozu při mimořádných situacích a vývoji a údržby systémů CA, je převod odpovědnosti za uvedené činnosti na jiné osoby, než kmenové zaměstnance dané společnosti. Outsourcing nesmí snížit úroveň bezpečnosti CA, bezpečnostní požadavky musí být součástí smlouvy upravující tento vztah, která musí mimo jiné zajistit dodržování relevantních interních předpisů.

### 9.6.2 Klasifikace aktiv

Cílem je udržování přiměřené ochrany aktiv.

#### 9.6.2.1 Odpovědnost za aktiva

Zde bude uvedena odpovědnost konkrétních rolí za aktiva spojená s certifikační autoritou, tj. za informační aktiva, hmotná aktiva (HW) i programové vybavení (SW).

#### 9.6.2.2 Klasifikace informací

Klasifikace aktiv probíhá z pohledu:

- důvěrnosti
- integrity
- dostupnosti
- hodnoty

Klasifikovat by se měla všechna klíčová aktiva certifikační autority, zejména:

- soukromé klíče (kořenové, podepisující, pracovníků registračních autorit, ..)
- certifikáty veřejných klíčů (kořenové, podepisující, pracovníků registračních autorit, ..)
- CRL – seznam zneplatněných certifikátů

- certifikáty klientů
- datové toky mezi jednotlivými systémy v rámci organizace
- data uložená v jednotlivých aplikacích
- klientské smlouvy
- ostatní dokumenty a auditní záznamy vznikající v rámci provozu CA

### 9.6.3 Personální bezpečnost

Cílem personální bezpečnosti je zejména snížení rizika lidské chyby, krádeže nebo podvodu.

#### 9.6.3.1 Bezpečnost rolí

Všem zaměstnancům s přidělenou rolí v CA musí být věnována zvýšená pozornost z pohledu personální bezpečnosti, především dokumentování přidělování a odebírání rolí, prověřování uchazečů, dohodám o mlčenlivosti, pracovním náplním.
Pracovní smlouvy zaměstnanců a všechny smlouvy s externími pracovníky musí obsahovat ustanovení o ochraně důvěrnosti informací, zejména o osobních údajích, o datech pro vytváření elektronických podpisů a o bezpečnostních zařízeních. Tato ustanovení musí být platná i po skončení zaměstnaneckého vztahu nebo příslušných prací.
Procedury ukončení nebo změny pracovního poměru pracovníků v definovaných rolích CA musí zajistit ochranu informací nezávisle na součinnosti pracovníka, tzn. například odebrání veškerých přístupů do CA pro odcházejícího zaměstnance nezávisle na jeho vůli.
Musí být definované a následně dodržované zásady oddělení rolí. Definice může být součástí jiného dokumentu, například směrnice o organizačním zajištění CA.
Musí být vybudována zastupitelnost pro zajištění kritických činností CA
Obsazení rolí CA musí být pravidelně přezkoumáváno z pohledu oddělení rolí a zastupitelnosti, periodicita zde musí být uvedena.

#### 9.6.3.2 Zácvik a školení

Všichni pracovníci v roli CA musí být prokazatelně seznámeni s relevantními vnitřními předpisy včetně diferencovaně podle svých rolí.
Seznámení se provádí při nástupu nového pracovníka, při změnách v relevantních dokumentech, nebo periodicky v definovaných intervalech, které zde musí být uvedeny.

#### 9.6.3.3 Zastupitelnost

Požadavky na dosažitelnost rolí při běžném provozu i v případě řešení mimořádných situací musí být brány do úvahy při obsazování rolí, plánování dovolené, pracovních cest apod.
Speciální požadavky na zastupitelnost klíčových rolí budou uvedeny zde.

#### 9.6.3.4 Řešení bezpečnostních incidentů

Za řešení bezpečnostních incidentů zpravidla zodpovídá bezpečnostní administrátor. Pro řešení bezpečnostních incidentů v rámci certifikační autority nemusí být přidělená speciální role v CA, ale může řešit bezpečnostní administrátor, pokud tato role už ve společnosti existuje. V každém případě musí být vedeny záznamy o zjištění a řešení bezpečnostních incidentů, které se týkaly CA.

### 9.6.4 Soulad s požadavky na dokument

#### 9.6.4.1 Soulad s legislativou

V rámci certifikační autority musí být definovaná role, která sleduje změny legislativy, a v případě, že dojde ke změně legislativy s dopadem na vnitřní předpisy CA, iniciuje změnu předpisů.
Navíc soulad vnitřních předpisů s platnou legislativou musí být prověřován pravidelně. Periodicita musí být uvedena zde.

#### 9.6.4.2 Posouzení bezpečnostní politiky a technické shody

V pravidelných intervalech musí být ověřen soulad bezpečnostních postupů certifikační autority se zásadami uvedenými platnou bezpečnostní politikou.
Dále musí být pravidelně kontrolován soulad nastavení IS CA se zásadami bezpečnostní politiky a dalšími dokumenty, kde je popsáno jejich nastavení.

#### 9.6.4.3 Audit systému

Tato kapitola se týká zásad pro vytváření a uchovávání auditních záznamů, požadavků a zásad pro provádění kontrol a auditů a klasifikaci dokumenů které vznikají v souvislosti s auditem. Tyto zásady mohou být vyčleněny do samostatného dokumentu, pak by byl zde uveden odkaz.

Následující tři kapitoly řeší bezpečnostní požadavky na třech typech pracovišť certifikační autority. Struktura těchto kapitol, resp. struktura popisu bezpečnostních pravidel je na všech typech pracovišť téměř totožná, proto se v následujícím textu zaměřuji pouze na popis a příklady v kapitole zabývající se centrálními pracovišti – datovými centry.

## 9.7 Zásady bezpečnosti pro centrální pracoviště – datová centra

Tato kapitola popisuje požadavky na centrální datová centra, tj. hlavní datové centrum a záložní datové centrum certifikační autority.

### 9.7.1 Fyzická bezpečnost

#### 9.7.1.1 Bezpečnost prostor

V této kapitole musí být definováno fyzické zabezpečení prostor datových center, přičemž je možné se také odkázat na zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti v aktuálním znění – v tomto případě musí být uvedena kategorie objektu, kterou musí datová centra splňovat.
Popis bude zaměřen na:

- mechanické prostředky zabezpečení, jako jsou definice umístění center v budově, zabezpečení oken, dveří apod.
- elektronické zabezpečení, tj. požadavky na EZS (elektronický zabezpečovací systém), EPS (elektrinický protipožární systém), signalizace zatopení vodou
- přístupy do datových center, tj. které role mají mít přístup a za jakých podmínek, některé role mohou mít např. přístup pouze v doprovodu. Mělo by být řešeno i pro pracovníky vně certifikační autority, tj. technické pracovníky správy budov, úklidu apod. Dále pak bude popsáno vedení záznamů a těchto vstupech (automatický elektronický systém, evidence formou záznamů do deníku apod.)
- Dále zde bude uveden seznam dokumentace
    - bezpečnostní dokumentace (vyhodnocení rizik fyzické bezpečnosti, bezprčnostní projekt)
    - provozní řád datového centra
    - krizový plán pro případ vzniku mimořádných situací

#### 9.7.1.2 Bezpečnost technického vybavení

Tato část se týká technických prostředků datových center, jako jsou aplikační servery, datová úložiště, síťové prvky a bezpečnostní moduly.
Kapitola definuje umístění těchto zařízení a pravidla pro manipulaci s nimi, včetně předávání těchto zařízení do opravy a k likvidaci, kdy musí být definován způsob bezpečného smazání dat.

#### 9.7.1.3 Trezory

Pro ochranu informačních aktiv certifikační autority před zneužitím musí být v každém datovém centru (hlavním i záložním) instalován trezor. Kapitola definuje požadavky na ukládání dokumentace a dat do trezorů. Jedná se především o uložení podepisovacích klíčů, auditních záznamů a databázových záloh.
Dále zde bude uvedeno:

- požadavky na trezor, tj. jakou bezpečnostní třídu musí splňovat
- přístup do jednotlivých trezorů (které role v rámci certifikační autority)
- provádění kontrol v trezorech (které role v rámci certifikační autority provádějí kontrolu a které role u toho musí být přítomny)
- způsob vedení záznamů o přístupech do trezorů (např. provozní deníky)
- další bezpečnostní požadavky, jako např.
    - rozdělení záloh podepisovacích klíčů v různých lokalitách, aby pro rekonstrukci klíče byly potřeba zálohy alespoň ze dvou lokalit
    - redundance uložených záznamů – v případě poškození dat v jedné lokalitě musí být možné provést jejich rekonstrukci ze zbývajících záloh – z toho může vyplývat požadavek na další trezor uložený na bezpečném místě mimo datového centra a záložní lokality.
    - uložení databázových záloh v jiné lokalitě než je provozována databáze.

#### 9.7.1.4 Obecné požadavky

Zde bude popsán obecně popsán způsob ochrany dat a dokumentů souvisejících s provozem certifikační autority, zejména:

- požadavek na ukládání dokumentace a datových nosičů pod uzamčením, pokud nejsou zrovna používány a pod dohledem oprávněného pracovníka

- povinnosti pracovníků v rolích CA při přihlášení do aplikací CA – nesmí být ponechány bez dozoru apod.
- Pravidla pro ochranu autentizačního tajemství (hesla, čipové karty, USB Tokenu), které slouží pro přihlašování do apliakcí certifikační autority.

### 9.7.2 Provoz

#### 9.7.2.1 Provozní postupy a odpovědnosti

Tato kapitole se zabývá provozními postupy používanými při správě, údržbě a provozu systémů certifikační autority. Bude zde definováno:

- formální způsob dokumentace všech provozních postupů a požadavek na změnové řízení dokumentů
- definice dostupnosti dokumentů pracovníkům CA na obecné úrovni
- požadavek na pravidelné prověřování aktuálnosti provozních postupů, definice odpovědnosti a periodicity.
- způsob definování odpovědností v provozních postupech – za provedení konkrétních operací v rámci provozního postupu musí být odpovědný konkrétní role CA.
- Vedení auditních záznamů o provedených operací v rámci provozních postupů

#### 9.7.2.2 Řízení provozních změn

V této kapitole bude popsán způsob dokumentace o konfiguraci systému a nastavení jednotlivých částí. Popis by měl zachycovat požadavky na:

- řízení vývoje, údržby a změn v systémech CA, návaznost případných dalších interních předpisů popisujících tuto problematiku
- změnové řízení a schvalování všech změn v systémech certifikační autority
- hodnocení dopadů na bezpečnost v rámci změnových řízení
- testování před nasazením vývojových změn.
- způsob migrace programových změn
- odpovědnosti za výše uvedené požadavky

#### 9.7.2.3 Ochrana proti malware

Pokud je ve společnosti samostatný dokument řešící problematiku ochrana počítačů před škodlivým software, bude v této kapitole na ní uveden odkaz, případně budou doplněny další specifické požadavky. Na úrovni systémů CA se bude jednat především o pravidla pro kontrolu přenosových médií, které jsou potenciálním zdrojem škodlivého SW. Za tímto účelem bude pravděpodobně ve společnosti existovat antivirový scanner, který bude možné využívat i pro CA.

#### 9.7.2.4 Zálohování

Zálohování dat může být součástí samostatného dokumentu. Musí být definována obecná pravidla pro zálohování aplikačních dat i systémů a aplikací, aby byla možné rekonstrukce v případě havárie. Na úrovni systémové bezpečnostní politiky se jedná o nastavení pravidel a požadavků, které pak budou promítnuty do provozních postupů, havarijních plánů a plánů obnovy.

#### 9.7.2.5 Bezpečné nakládání s nosiči dat

Tato kapitola se částečně prolíná s kapitolou věnovanou trezorům. Jedná se o nastavení pravidel pro bezpečné uchovávání dokumentů a datových médií pod uzamčením. Dále je zde uveden způsob označování datových médií a jejich evidence v rámci certifikační autority. Na datových médiích by měla být klasifikována a označena podle typu informací, která jsou na ní uložena.

Dále by měl být definován způsob manipulace s archivními datovými médii a jejich skartace. Tyto zásady mohou být definovány v samostatném dokumentu a zde uveden pouze odkaz.

#### 9.7.2.6 Sledování provozu

Provoz datového centra bude monitorován pracovníky monitoringu – budou sledovány a vyhodnocovány definované parametry systémů v pravidelných intervalech, vzhledem k povaze aplikací bude pravděpodobně požadavek na monitoring v rozsahu 7x24. Pracovníci monitoringu misí mít k dispozici popis činností a seznam kontaktů pro řešení případných nestandardních situací.

Mimo nastavené sledování monitorovacího centra budou definovány pravidelné kontroly systémů a systémových zdrojů administrátorem. P těchto kontrolách bude proveden

záznam do provozní dokumentace. V případě zjištění nedostatků musí být definován způsob řešení.

#### 9.7.2.7 Bezpečnostní modul

Bezpečnostní modul je v rámci certifikační autority využíván pro zajištění kryptografických funkcí. V této kapitole musí být definován způsob používání a manipulace s ním:

- musí být zabezpečeno, aby s modulem bylo manipulováno pouze v zabezpečených prostorách a oprávněnými pracovníky v definovaných rolích CA. Resp. musí být přijata opatření, aby každá neoprávněná manipulace s modulem byla zjistitelná.
- Pokud není modul v zabezpečeném prostoru datového centra, nebo záložní lokality, musí z něj být vymazán veškerý kryptografický materiál včetně privátních klíčů.

### 9.7.3 Komunikace

#### 9.7.3.1 Sítě

V datových centrech musí být vybudována samostatná lokální síť, která bude s okolím propojená přes zabezpečený Firewall.

#### 9.7.3.2 Vzdálený přístup

V této kapitole bude definováno omezení vzdáleného přístupu na systémy certifikační autority umístěné v datových centrech. Nejedná se o přístup klientských aplikací operátorů registrační autority komunikujících se servery CA, ale o administrační přístupy přímo na servery. Nejvyšší bezpečnost se zajistí úplným omezením těchto přístupů, což je ale vyváženo určitou mírou nekomfortu při správě a kontrolách serverů.

#### 9.7.3.3 Šifrování

Šifrovány musí být veškeré přenosy mimo datová centra, ať už přenosy realizované prostřednictvím datové sítě, nebo data přenášená na datových médiích například v rámci zálohování (výjimkou mohou být přenosy v rámci monitorování systémů).
Způsob šifrování, tj. šifrovací mechanismy a minimální velikost šifrovacího klíče bude stanoven v tomto odstavci, včetně rolí, které to schvalují. Délka klíčů se bude lišit pro použití sysmetrické a asymetrické kryptografie.

### 9.7.4 Řízení přístupu do systémů CA

#### 9.7.4.1 Základní požadavky

Uživatelská práva jsou uživatelům v systémech CA (aplikacích, OS, DBMS) přidělována podle zařazení do rolí certifikační autority.

Rozsah práv odpovídající jednotlivým rolím CA může být uveden v dokumentacích k jednotlivým systémům. Pro přidělování práv musí platit zásada o přidělení minimálních nezbytných práv každému uživateli.

#### 9.7.4.2 Správa přístupu

Pro správu přístupových práv systémů certifikační autority musí existovat v rámci rolí certifikační autority i role administrátora přístupových práv. Pracovník jmenovaný do této role zajišťuje přidávání a odebírání práv dy systémů CA na základě požadavku kompetentní osoby. V této kapitole musí být definováno:

- kdo rozhoduje o přidělení a odebrání práv do systémů CA. Resp. která role v rámci CA.
- Způsob vedení záznamů o této činnosti – každá provozní aktivita musí být evidována formou auditního záznamu.
- nastavení procedury odebírání práv – musí existovat mechanismus odebírání práv uživatelům nezávislá na jejich vůli, která je propojena s ukončením procovního poměru nebo změnou zařazení pracovníka CA.
- Při být zabezpečeno, aby při odebírání uživatzelských práv nebyl účet uživatele ihned smazán, ale pouze uzamčen. Dále bude definovaná doba, po které je již možné účet smazat. Tento požadavek souvisí s požadavkem vedení auditních záznamů a případnou možností zpětného dohledání aktivity iživatele.
- V definovaných intervalech je nutné provádět přezkoumání přístupů a rozsahu oprávnění do systému CA.

#### 9.7.4.3 Identifikace a autentizace uživatelů

Zde budou uvedeny základní bezpečnostní požadavky pro identifikaci a autentizaci např.:

- požadavek na jednoznačnou identifikaci každého uživatele přistupujícího do aplikací certifikační autority – tzn., že není povolena žádná forma sdílení identifikace pro přístup.

- Požadavek na způsob autentizace, např. že operátoři se do aplikací CA autentizují výhradně prostředky asymetrické kriptografie a způsob uložení soukromého klíče uživatele, případně využití hesla a požadavky na jeho složitost apod..
- nastavení politiky přihlašování, jako je počet neúspěšných pokusů, po jejichž provedení se účet automaticky zamkne na určitou dobu a jaká je tato doba.
- Definice nastavení hlavních administrátorských účtů do systémů a do aplikací certifikační autority:
    - požadavek na prvotní změnu hesla a na následnou periodicitu změn
    - požadavky na složitost a délku hesla
    - požadavky na uložení hesel na bezpečném místě a jejich zajištění proti zneužití – musí být jasně zjistitelné použití hesla.
    - Vytvoření účtů pro konkrétní osoby, které budou sloužit pro běžnou práci uživatelů v systému. Hlavní administrátorské účty budou použity pouze v případě řešení nestandardní situace oprávněnou osobou.

#### 9.7.4.4 Odpovědnost uživatelů

Tato kapitola bude definovat práva a povinnosti uživatelů aplikací certifikační autority v souvislosti s používáním přístupů do aplikací. To se týká především ochrany autentizačního tajemství tj. i a zamezení sdílení svého přístupu s jiným uživatelem. Výjimky mohou tvořit případy, kdy není technologicky možné dodržet toto pravidlo (např. na UNIXových systémech použití superuživatele ROOT), nebo mimořádné situace, které jsou popsány v havarijních plánech. Uživatelé jsou dále povinni při podezření na prozrazení prostředku pro autentizaci podniknout kroky k zabránění zneužití prostředku, jako jsou změna hesla nebo PINu čipové karty).

#### 9.7.4.5 Způsoby autentizace

Jedná se o definici způsobů autentizace v rámci přihlašování k systémům a aplikacím certifikační autority. Může se jednat například:

- autentizaci heslem
    - definice požadavků na délku hesla
    - definice požadavků na komplexnost hesel
    - evidence změn uživatelských hesel administrátorem systému
    - požadavky na pravidelné změny hesla

- čipovou kartou
    - na čipové kartě je bezpečně uložen soukromí autentizační klíč uživatele
    - přístup na kartu musí být chráněn PINem
    - Dále by měly být uvedeny požadavky na PIN ve stejném rozsahu, jako se uvádějí pro hesla (délka, komplexicita, pravidelná změna).
    - Způsob předávání karty a PINu uživateli
    - způsob uchovávání karty, tj například požadavky na fyzickou bezpečnost, požadavek na neuchovávání PINu společně s kartou na jednom místě (byť pod zámkem)
    - měl by být uveden postup při ztrátě čipové karty, případně uvést odkazem na jinou dokumentaci (například revokace certifikátu)
    - Může zde být popsán i způsob evidence čipových karet

#### 9.7.4.6 Bezpečnostní modul

Na bezpečnostní modul jsou kladeny nejvyšší nároky, co se týče bezpečnosti, protože slouží pro manipulaci se soukromím klíčem certifikační autority. Tato kapitola musí přesně specifikovat bezpečnostní požadavky na toto zařízení. Popis bude patrně souviset konkrétním používaným zařízením. Obecně se dá říci, že:

- pro veškeré činnosti prováděné s modulem existuje definice, kdo (tj. které role certifikační autority) mohou tyto činnosti vykonávat.
- pro každou činnost se před jejím započetím musí pracovník v příslušné roli autentizovat pomocí přiděleného autentizačního tajemství, např. čipové karty, s uloženým bezpečnostním klíčem (chráněnou PINem).
- V rámci definovaných rolí certifikační autority jsou jmenováni do těchto rolí konkrétní pracovníci. Zařazování pracovníků do rolí musí být v souladu s již zmíněnou směrnicí zabývající se organizačním zajištěním certifikační autority, kde je mimo jiné definováno tabulkou separace rolí. Jedná se o to, že některé role nesmí být ze své povahy obsazeny jedním konkrétním člověkem z důvodu konfliktu zájmů.
- Technickými prostředky musí být zajištěno, že soukromý klíč certifikační autority je možné vyexportovat z modulu pouze zase na chráněné čipové karty.

### 9.7.5 BCP (Business continuity plan)

#### 9.7.5.1 Zajištění kontinuity provozu

Na některé informace a služby CA (především CRL a proces jeho vydávání) jsou kladeny značné nároky na dostupnost a těmto požadavkům také musí odpovídat úroveň všech opatření směřujících k zajištění nepřetržitosti provozu a obnovy po havárii. V této kapitole by měla být uvedena povinnost mít vytvořeny havarijní plány a zároveň v hrubých rysech specifikován obsah těchto plánů. Uvádím příklad požadavků, co by měl splňovat havarijní plán:

- Ochrana proti výpadku elektrického proudu
    - Napájení klíčových prvků (aktivních síťových prvků, serverů, bezpečnostních modulů) je zajištěno prostřednictvím chráněného okruhu napojeného na zdroje nepřetržitého napájení a zároveň zajištěné proti přepětí.
    - Případný výpadek elektrické energie bude signalizován dohledovému centru, kde pro tento případ budou existovat postupy pro.
- Existence havarijních plánů na pracovišti dohledového centra. Plány musí mimo jiné zahrnovat postupy při:
    - havárii sítě LAN nebo WAN v datovém nebo záložním centru
    - havárii serveru v datovém nebo záložním centru
    - požáru, zaplavení vodou nebo jinou živelnou pohromu v datovém centru nebo záložní lokalitě.
- Součástí plánů musí být popis činnosti v průběhu havárie a činností po havárii k rychlému obnovení provozu CA. Dále by měl být uveden seznam kontaktů .
- V každém havarijním plánu musí být uvedena osoba, která je odpovědná za pravidelnou kontrolu a aktualizaci.
- Proveditelnost každého havarijního plánu by měla být v rámci možností otestována.

#### 9.7.5.2 Opatření pro nestandardní situace

Tato kapitola definuje opatření pro případné řešení havarijních situací, jako jsou např.:

- Požadavek na existence redundantních klíčových zařízení, které by měly být definované době k dispozici pro případ havárie těchto zařízení v datovém centru.

- Požadavek na uložení autentizačních prostředků (hesla, čipové karty, ..) na bezpečném místě (v trezoru) pro případ řešení nestandardních situací.
- Požadavek na definici procedur pro přístup určených pracovníků do prostor datového nebo záložního centra i v mimopracovních hodinách pro případ řešení nestandardní situace.

## 9.8 Zásady bezpečnosti pro centrální pracoviště – klientská část

Tato kapitola popisuje bezpečnostní požadavky na klientskou část centrálního pracoviště, tj. centra, které zastřešuje veškerý kontakt s klientem prostřednictvím registračních autorit. Odpovědnosti klientské části centrálního pracoviště jsou:

- správa zákazníků a s nimi spojených žadatelů o certifikát. S tím souvisí:
    - vyřizování žádostí zasílaných oprávněnými osobami prostřednictvím emailu, například vydávání následných certifikátů.
    - zajišťování správy osobních údajů zákazníků a žadatelů
    - vedení dokumentace spojené s vydáváním certifikátů klientům (smlouvy o poskytování certifikačních služeb, žádosti o certifikáty, kopie osobních a jiných dokladů , ..)
- zajišťování podpory pracovišť registrační autority
    - vydávání autentizačních čipových karet s vygenerovaným certifikátem operátorům certifikační autority.
    - vedení registru čipových karet operátorů RA

## 9.9 Zásady bezpečnosti pro pracoviště registrační autority

Tato kapitola bude popisovat bezpečnostní požadavky na pracoviště registrační autority, tj. pracoviště, které slouží ke kontaktu s klientem. Kontaktní místo registrační autority zodpovídá zejména za následující činnosti:

- uzavírání smluv o poskytování certifikačních služeb s právnickými a fyzickými osobami zavádí je do Správy žadatelů
- vydávání certifikátů
- zneplatňování certifikátů

## 9.10 Vazby IS certifikační autority na ostatní IS ve společnosti

Systémy CA budou napojeny na další informační systémy ve společnosti, jako je ekonomický systém, databáze klientů, monitoring, .. Tyto vazby jsou popsány v této kapitole.

### 9.10.1 IS centra dohledu aplikací

Servery certifikační autority budou pravděpodobně napojeny na centrální monitoring, aby bylo možné soustavné sledování požadovaných parametrů pro rychlou detekci problémů za běhu systémů. V souvislosti se zákazem vzdáleného přístupu na servery CA umístěné v datovém a záložním centru, může být tento přístup řešen lokálními aplikacemi dohledu (agenty) které běží na serverech CA a v pravidelných intervalech odesílají posbírané informace do dohledového centra. Sledovány by měly být všechny služby a procesy nezbytné pro chod služeb CA.

### 9.10.2 Podnikový ekonomický systém

Důvodem pro napojení serverů certifikační autority může být například potřeba automatické fakturace za poskytování certifikačních služeb klientům. Aplikace CA může pravidelně předávat soubor s podklady pro fakturaci do ekonomického systému.

### 9.10.3 Databáze klientů

Pokud ve společnosti existuje centrální databáze klientů, má smysl napojit na ní i aplikace zajišťující provoz certifikační autority pro možnost sdílení informací o klientech.

## 9.11 Odkazy na související interní normy

V této kapitole by měl být uveden seznam interních norem, na které je v textu této směrnice odkazováno. Jedná s především o nadřízené dokumenty, tj. obecná systémová bezpečnostní politika, globální bezpečnostní politika společnosti a dále pak ostatní normy certifikační autority, jako je organizační zajištění, prováděcí směrnice, auditní a archivační politika, krizové a havarijní plány apod.

## 9.12 Závěrečná ustanovení

V této kapitole by mělo být definováno:

- okruh pracovníků, kteří musí být seznámeni s tímto dokumentem

- okruh rolí certifikační autority, jejichž členové musí být prokazatelně seznámeni se zněním této směrnice. Vzhledem k rozsahu platnosti průřezově celou certifikační autoritou se asi bude jednat o všechny role CA.
- odpovědná osoba (role) za výklad a aktualizaci této směrnice
- případný seznam interních směrnic, které dnem účinku této směrnice pozbývají platnost.
- den nabytí účinnosti této směrnice.

# 10 Zhodnocení výsledků a závěr

Zadáním pro tuto diplomovou práci bylo tématické zaměření na problematiku elektronického podpisu a certifikátů a jeho využívání v bezpečné elektronické komunikaci. Práce se v teoretické části zabývá problematikou elektronického podpisu jako celku. Jsou zde popsány základní principy kryptografie, jakožto technologického rámce pro elektronické podpisy. Dále se práce detailněji zabývá popisem elektronického podpisu a certifikátů, popisuje jednotlivé typy a třídy certifikátů a uvádí životní cyklus certifikátů i základní postupy související s vystavením, zneplatněním a obnovou certifikátů. V práci jsou zmíněny i další služby certifikačních autorit, jako je vydávání časových razítek nebo autentizační služby. Kvalifikované certifikační služby musí mít oporu v platné legislativě, proto je kapitola také věnována platným legislativním předpisům České republiky i Evropské unie, kdo jsou zmíněny zejména české právní normy související s elektronickým podpisem a kvalifikovanými certifikačními službami.
V praktické části se práce zabývá detailněji povinnostmi kvalifikovaných poskytovatelů certifikačních služeb v České republice s tím, že praktická část je zaměřena na vytvoření návrhu jednoho z povinných klíčových dokumentů, který musí být součástí bezpečnostní dokumentace každé kvalifikované certifikační autority, dle definice v zákonu o elektronickém podpisu a upřesnění ve vyhlášce o postupech kvalifikovaných poskytovatelů certifikačních služeb. V úvodu praktické části jsou blíže specifikovány tyto požadavky s uvedením relevantních citací jmenovaných právních norem. Následuje návrh zmíněného dokumentu systémové bezpečnostní politiky pro kvalifikovanou certifikační autoritu.

V České republice existuje legislativní rámec pro elektronické podpisy a poskytovatele certifikačních služeb, jehož klíčovou legislativní normou je zákon o elektronickém podpisu v platném znění. Fungují zde tři akreditované certifikační autority poskytující služby jak vydávání kvalifikovaných certifikátů elektronického podpisu , tak i další služby jako je vydávání kvalifikovaných časových razítek. Přesto můžeme očekávat další vývoj v oblasti technologie i legislativy související s elektronickými podpisy a certifikačními službami.
V oblasti technologie se v souvislosti s růstem výkonu výpočetní techniky dá očekávat, že aktuálně používané technologické standardy asymetrické kryptografie a hashovacích funkcí budou v budoucnu zdokonalovány a nahrazovány za bezpečnější.

Příkladem z oblasti budoucích legislativních změn může být vypořádání se s problémem ověření platnosti elektronického podpisu po delší době, tj. několika letech, desetiletích. Aktuální česká ani evropská legislativa toto neřeší a po ukončení platnosti podpisového certifikátu vzniká problém s ověřením elektronického podpisu.

Téma informační bezpečnosti je v dnešní době stále aktuální a vzhledem ke snaze elektronizovat stále více procesů poroste význam informační bezpečnosti i v budoucnu. Ať už se jedná o komunikaci občana s bankou (b2c), s orgány veřejné moci (g2c), nebo komunikaci mezi firmami (b2b), vždy se jedná o přenos citlivých informací, které by bylo možné zneužít třetí stranou a proto vždy bude potřeba tyto přenosy chránit.

# Použité zdroje

**Knižní zdroje:**

[BOS02] Bosáková, D. – Kučerová, A. – Peca, J. – Vondruška, P. Elektronický podpis. 1. vydání. Olomouc: ANAG, 2002. 141 s. ISBN 80-7263-125-X

[KNY10] Kný, M. – Požár, J. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. 1. vydání. Brno: Tribun EU, 2010. 128 s. ISBN 978-80-7399-067-1

[DOS04] Doseděl, T. Počítačová bezpečnost a ochrana dat. 1. vydání. Brno: Computer press, 2004. 190 s. ISBN 80-251-0106-1

[BAU08] Baudiš, P. Elektronický podpis a jeho aplikace v praxi. 1.vydání. Olomouc: ANAG, 2008. 153 s. ISBN 978-80-7263-465-1

[DOU08] Doucek, P. – Novák, L. – Svatá V. – Nedomová L. Řízení bezpečnosti informací. 1. vydání. Praha: Kamil Mařík – Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7

[ZEL03] ZELENKA J. – ČAPEK J. – FRANCEK J. – JANÁKOVÁ H. Ochrana dat. Kryptologie. 1. vydání. Hradec Králové: Gaudeamus, 2003. ISBN 80-7041-737-4

**Elektronické zdroje:**

[e-PET] Peterka, Jiří. e-archiv Jiřího Peterky: Elektronický podpis [online]. dostupné z: http://www.earchiv.cz/i_digsig.php3

**Legislativní normy:**

[ZAK227] Zákon č.227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů

[ZAK101] Zákon č. 101/2000 Sb. o ochraně osobních údajů

[VYH378] Vyhláška 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb

# Seznam obrázků

# Přílohy

## Příloha č. 1: Vymezení pojmů Zákonem o elektronickém podpisu [ZAK227]

*a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě,*

*b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky*

*1. je jednoznačně spojen s podepisující osobou,*

*2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,*

*3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,*

*4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,*

*c) elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky*

*1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,*

*2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,*

*3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat,*

*d) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,*

*e) podepisující osobou fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby,*

*f) označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou,*

*g) držitelem certifikátu fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán,*

*h) poskytovatelem certifikačních služeb fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,*

*i) kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,*

*j) akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,*

*k) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,*

*l) kvalifikovaným certifikátem certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,*

*m) kvalifikovaným systémovým certifikátem certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,*

*n) daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,*

*o) daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,*

*p) daty pro vytváření elektronických značek jedinečná data, která označující osoba používá k vytváření elektronických značek,*

*q) daty pro ověřování elektronických značek jedinečná data, která se používají pro ověření elektronických značek,*

*r) kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v*

*elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem,*

*s) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,*

*t) prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,*

*u) prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,*

*v) prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,*

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

*x) prostředkem pro vytváření elektronických značek zařízení, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem,*

*y) elektronickou podatelnou pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv,*

*z) akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.*