Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Obor Veřejná správa a regionální rozvoj

Katedra informačních technologií

Diplomová práce

na téma

Zaručený elektronický podpis a jeho praktické využití na Městském úřadu s rozšířenou působností

Vedoucí diplomové práce: **Ing. Eva Kánská**

Autor diplomové práce: **Bc. Jiří Schumann**

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Schumann Jiří

Veřejná správa a regionální rozvoj nav.- Most

Název práce

Zaručený elektronický podpis a jeho praktické využití na Městském úřadě s rozšířenou působností

Anglický název

Advanced electronic signature and its practical use at the Municipal Office with extended

---

Cíle práce

Diplomová práce je zaměřena na problematiku využívání elektronického podpisu na obecním úřadu s rozšířenou působnosti. Hlavním cílem práce je zanalyzovat vybranou problematiku a navrhnout optimalizaci z pohledu občana a zaměstnance. Dílčím cíle práce je vytvoření přehledné řešené problematiky a analýza využití vybrané aplikace s použitím elektronického podpisu.

Metodika

Metodika řešení problematiky této diplomové práce je založena na analýze odborné literatury a platné legislativy v dané problematice. Na základě syntézy ziskaných zkušeností a výsledků vlastního šetření budou formulovány závěry diplomové práce.

Harmonogram zpracování

12/2010 - 04/2011: Studium literatury, sběr informací
05/2011 - 08/2011: Zpracování a analýza získaných informací,
09/2011 - 12/2011: Zhodnocení výsledků práce
01/2012 - 12/2012: Tvorba finálního dokumentu diplomové práce
03/2012 Odevzdání diplomové práce

Rozsah textové části

60 - 80 stran

Klíčová slova

zaručený elektronický podpis, certifikát, certifikační autorita, kryptografie, zaručená konverze dokumentů, CzechPoint, e-Governent, Informační systém datových schránek, Zákon o elektronickém podpisu

---

Doporučené zdroje informací

Dostálek Libor, Vohnoutová Marta, Velký průvodce infrastrukturou PKI a technologií elektronického podpisu, Nakladatelství Computer press a.s. Praha 2007, ISBN 80-251-0828-7

Budiš Petr, Elektronický podpis a jeho aplikace v praxi, nakladatelství ANAG, Olomouc 2008, ISBN 978-80-7263-465-1

Dagmar Bosáková, Alena Kučerová, Jaroslav Peca, Pavel Vondruška. Elektronický podpis, nakladatelství ANAG, Olomouc 2002, ISBN 80-7263-125-X

Lidinský Vít, Švarcová Ivana, Budiš Petr, Loebl Zbyněk, Procházková Barbora, eGovernment bezpečně Nakladatelství: GRADA Publishing, a.s 2008 ISBN: 978-80-247-2462-1

Jiří Peterka, Báječný svět elektronického podpisu,Nakladatelství CZ.NIC, z. s. p. o. Praha 2011 ISBN: 978-80-904248-3-8

Vedoucí práce

Kánská Eva, Ing.

Termín odevzdání

březen 2012

---

doc. Ing. Zdeněk Havlíček, CSc.

Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr.h.c.

Děkan fakulty

V Praze dne 29.10.2011

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma „Zaručený elektronický podpis a jeho praktické využití na Městském úřadu s rozšířenou působností“ vypracoval samostatně za pomoci odborných konzultací s vedoucím diplomové práce Ing. Evou Kánskou a s využitím uvedených informačních zdrojů.

……

Bc. Jiří Schumann

V Rakovníku 28. 3. 2012

Poděkování

Touto cestou bych chtěl především poděkovat vedoucí diplomové práce Ing. Evě Kánské za odborné vedení, připomínky a cenné rady, které mi poskytovala v průběhu zpracování této diplomové práce a také mé manželce Dagmar Schumannové za trpělivost a oporu během mého studia.

Zadání

Zaručený elektronický podpis a jeho praktické využití na městském úřadu s rozšířenou působností

Souhrn:

Diplomová práce je zaměřena na popis technologií používaných při využívání zaručeného elektronického podpisu a praktické využití zaručeného elektronického podpisu ve veřejné správě, a to na Městském úřadu s rozšířenou působností. Práce se nejprve zabývá teoretickými poznatky z oblastí, které se dotýkají elektronických podpisů. Jedná se hlavně o legislativu a technologie používané při práci se zaručenými elektronickými podpisy. Obecně popisuje používané šifrovací algoritmy, kryptografické metody, ověřování pravosti dokumentů, bezpečnost používání zaručených elektronických podpisů, význam a typy elektronických podpisů. V diplomové práci je dále popisována problematika týkající se certifikátů a certifikačních autorit, Czechpointu, systému datových schránek, archivace elektronických dokumentů. Dále je na praktických příkladech ukázáno reálné používání zaručeného elektronického podpisu při práci úředníků městského úřadu s rozšířenou působností, a to od tvorby podpisu, přes jejich správu, až do jeho využití v komunikaci s veřejností i s ostatními orgány Veřejné správy. Závěr práce popisuje výhody a nevýhody využívání zaručeného elektronického podpisu a zamýšlí se nad jeho budoucností.

Klíčová slova:

Zaručený elektronický podpis, certifikát, certifikační autorita, kryptografie, zaručená konverze dokumentů, CzechPoint, e-Governent, Informační systém datových schránek, Zákon o elektronickém podpisu

Advanced electronic signature and its practical use at the Municipal Office with Extended

Summary:

This thesis is focused on the description of technologies used in apply of advanced electronic signature and the practical application of advanced electronic signatures in public administration, namely the municipality with extended competence. The first part of this essay contains the theoretical knowledge that includes also electronic signatures. It concerns mainly legislation and technologies used to work with advanced electronic signatures. Generally this part describes the used cryptographic algorithms, cryptographic methods, document authentication, the security usage of advanced electronic signatures, meaning and types of electronic signatures. In the following parts of this thesis are described the matters concerning the certificates and certification authorities, CzechPOINT, the system of electronic data boxes, archiving of electronic documents. The practical part of this thesis illustrates the examples of using real advanced electronic signature in the work of officials in the municipality with extended competence that means from the signature creation, through its management, to its use in communication with the public or with other authorities of public administration. The conclusion of this essay describes the advantages and disadvantages of using advanced electronic signature and speculates about its future.

Key words:

Guaranteed electronic signature, certificate, certificate authority, cryptography, secure document conversion, CzechPoint, e-Government, the systém of eletronic data boxes, electronic signature act

Obsah

1 Úvod

V první řadě si je nutné, abychom si ujasnli, co je vlastně elektronický podpis. V žádném případě to není vlastnoruční podpis člověka, jakoukoliv formou převedený do elektronické nebo digitální podoby. Není to ani podpis připojovaný automaticky aplikacemi k dokumentům, například v emailu, tzv. vizitka. Elektronický podpis, a zvláště pak zaručený elektronický podpis musí splňovat mnohá kritéria, která si vysvětlíme později.

Autor práce je zaměstnán od roku 2005 na Městském úřadu v Rakovníku jako správce informačních technologií. Náplní práce autora je také zavádění eGovernmentu do praxe, to znamená i technologií vyžadujících použití zaručeného elektronického podpisu. Z tohoto důvodu si autor vybral zaručený elektronický podpis jako téma své Diplomové práce. Vzhledem ke svým praktickým zkušenostem ze zavádění eGovernmentu do praxe se autor zaměřuje především na problematiku elektronického podpisu ve veřejné správě, konkrétně na praktické využívání zaručeného elektronického podpisu na městském úřadu s rozšířenou působností.

Elektronické podpisy využívané jako zaručené jsou výsledkem dlouholetých zkušeností mnoha vědců z oblasti výpočetní techniky a především pak z oblasti kryptografie. Elektronických podpisů vznikla celá řada a mají různé vlastnosti a slouží k různým účelům. Pro nahrazení vlastnoručního podpisu na elektronických dokumentech a datových správách se využívá právě zaručený elektronický podpis založený na kvalifikovaném certifikátu. Pokud se v dalším textu budu zmiňovat o elektronickém nebo digitálním podpisu, tak je míněn vždy tento zaručený elektronický podpis, pokud není řečeno jinak.

Hned v úvodu bude provedeno srovnání zaručeného elektronického podpisu s běžným vlastnoručním podpisem. Pokud kdokoli připojí svůj vlastnoruční podpis na běžný papírový dokument, tak se v souladu se zákonem předpokládá, že je s dokumentem obeznámen, že s ním souhlasí a že ručí za jeho obsah. Z této

premisy pak vychází i příjemce dokumentu a považuje dokument za důvěryhodný. Každý jednotlivec má svůj má svůj charakteristický rukopis a proto vlastnoruční podpis zcela jednoznačně identifikuje osobu, která podpis vytvořila. V případě, že potřebujeme důvěryhodnost vlastnoručního podpisu ještě zvýšit, tak můžeme vlastní akt podpisu provést před státem určenou autoritou, která skutečnost, že podpis provádí ta osoba, která je uvedena na dokumentu ověří podle předložených osobních dokumentů a provede o tom úřední zápis do knihy ověřování a vyznačí tento akt i na ověřeném dokumentu. Toto ověřování provádí například matriční úřady nebo notářské kanceláře. V případě že je požadováno do budoucna zabránit i pozměnění papírového dokumentu, tak bude vytvořen ve více vyhotoveních. Všechna tato vyhotovení dokumentu pak budou opatřena vlastnoručními podpisy a popřípadě i s jejich úředním ověřením, Tato vyhotovení si pak ponechají zúčastněné strany a případnou změnu jednoho dokumentu lze pak velmi snadno prokázat porovnáním s dokumentem protistrany.

V případě že se jedná o dokument v jakékoliv elektronické podobě, tak je situace složitější. Lze sice provést podepsání dokumentu jménem, nebo vytvořit elektronický obraz podepsaného papírového dokumentu, ale důvěryhodnost tohoto aktu je zcela nulová. Vlastnoruční podpis sice lze napodobit, ale případný grafologický rozbor by zřejmě zfalšovaný podpis prokázal, a pokud se jedná o úředně ověřený podpis, tak je téměř nemožné dokument zfalšovat. Ovšem v případě elektronického textu je tomu přesně naopak. Připojit k dokumentu cizí jméno může v podstatě kdokoliv a neexistuje způsob, jak takový podvrh prokázat. Navíc je velmi snadné elektronický dokument pozměnit, aniž by kdokoliv tuto změnu dokázal zjistit. Většina uživatelů dnešních moderních komunikačních technologií si tyto skutečnosti vůbec neuvědomuje, a je pro ně velkým překvapením, že téměř všechna elektronická data a dokumenty v prostředí internetu jsou nezabezpečena proti přečtení, modifikaci a případnému zneužití. Z tohoto důvodu bylo nutné najít technologií, která by dokázala zcela jednoznačně identifikovat osobu podepisující dokument a zároveň zaručila jeho nepozměnitelnost, a případně aby byla znemožněna čitelnost dokumentu pro někoho jiného než pro odesílatele a příjemce dokumentu Tyto požadavky lze shrnout pod tři slova, a to **autentičnost** (původ dokumentu, identita autora), **integrita** (neporušenost a nepozměněnost dat)

a **nepopiratelnost** (podepsaná strana nemůže později popřít, že daný dokument podepsala). Dále je třeba u některých dokumentů zajistit i utajení obsahu, takže se k prvním třem požadavkům přidává ještě požadavek na **utajení obsahu** dokumentu před neoprávněnými osobami. Všechny tyto požadavky splňuje využívání zaručených elektronických podpisů založených na technologiích vycházejících z tzv. Asymetrické kryptografie.

Elektronická komunikace v dnešní době začíná nahrazovat komunikaci pomocí papírových dokumentů, a proto je třeba zajistit, aby bylo možno provádět úkony odpovídající vlastnoručnímu podpisu co nejjednodušeji, a aby byly zachovány všechny aspekty jako u podpisu vlastnoručního. Touto myšlenkou se v oblasti veřejní správy zabývá dnes tak často zmiňovaný e-Government.

Vlastní používání elektronických podpisů se díky implementaci technologií asymetrické kryptografie do standardně používaných programů do značné míry zautomatizovalo, a jejich použití stalo velmi jednoduchým. V mnoha případech vlastník elektronického podpisu ani neví, že jeho podpis byl k nějakému dokumentu připojen.

I když jsou elektronické podpisy využívány v naší republice, ve veřejné správě více než pět let a legislativa je staví na úroveň s podpisy vlastnoručními, tak veřejnost a někdy i úředníci veřejné správy si neuvědomují jejich právní sílu, neznají podmínky využití a elektronické podpisy proto podceňují a bagatelizují jejich význam.

2 Cíl práce a metodika

Cílem diplomové práce je, provést analýzu využívání kvalifikovaných elektronických podpisů na obecním úřadu s rozšířenou působností. Úvodní část práce se zabývá teorií elektronického podpisu a obsahuje definice pojmů používaných v této problematice. Další kapitola popisuje legislativní zakotvení elektronického podpisu v českém právním řádu včetně historie a je zde i naznačen vztah k legislativě Evropské unie. V přílohách je potom uvedeno plné znění zákona 227/2000 Sb., o elektronickém podpisu v aktualizovaném znění.

V teoretické části práce jsou popsány různé druhy elektronických podpisů. Je zde ukázáno jejich dělení podle technických i legislativních kritérií a podle praktického využití a je zde ukázána i část problematiky související s poskytovateli certifikačních služeb, jako zajišťovatelů důvěry v elektronický podpis, na které je postavena celá tato problematika. Dále je uveden seznam akreditovaných certifikačních autorit, které jediné mohou vydávat zaručené elektronické podpisy, které jsou podle zákona nezbytné pro komunikaci s institucemi veřejné správy.

Dalším cílem diplomové práce je zanalyzovat vybranou problematiku, a pokud budou nalezeny nedostatky, tak navrhnout opatření, která by vedla k jejich nápravě.

Metodika řešení problematiky této diplomové práce je založena na analýze odborné literatury a platné legislativy v dané problematice. Na základě syntézy získaných zkušeností a výsledků vlastního šetření budou formulovány závěry diplomové práce

3 Základní pojmy

V dalších částech diplomové práce budou využívány některé pojmy, které se pojí se specifickými technologiemi, nebo nejsou příliš známé široké veřejnosti. Pro vysvětlení proto většina z nich bude uvedena v této kapitole.

3.1.1 Akreditace

Akreditací zákon o elektronickém podpisu rozumí osvědčení, vydávané Úřadem pro ochranu osobních údajů poskytovatelům certifikačních služeb. Toto osvědčení stvrzuje, že poskytovatel splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Působení akreditovaných poskytovatelů je nezbytné pro komunikaci v oblasti orgánů veřejné moci, neboť v této oblasti je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb. [6]

3.1.2 Akreditovaný poskytovatel certifikačních služeb

Akreditovaný poskytovatel certifikačních služeb ve smyslu zákona o elektronickém podpisu je poskytovatel, který získal akreditaci podle tohoto zákona [6]

3.1.3 Asymetrická kryptografie

Asymetrická kryptografie neboli kryptografie veřejného klíče, je oblast kryptografie založená na následující myšlence: Každý subjekt systému má vlastní dvojici klíčů – soukromý klíč, který musí udržet v tajnosti, a veřejný klíč, který je naopak určen ke zveřejnění. Oba klíče jsou spolu spojeny jednoznačnou vazbou odpovídající zvolenému kryptografickému algoritmu, přičemž musí být prakticky nemožné ze znalosti veřejného klíče vypočítat klíč soukromý. Šifrování mezi dvěma subjekty potom probíhá následovně. Odesílatel, který chce druhé straně zaslat utajenou zprávu, zašifruje tuto zprávu pomocí veřejného klíče příjemce. Zašifrovaný text může poté poslat veřejně přístupným kanálem, protože odšifrovat jej lze jedině pomocí

příslušného soukromého klíče, který vlastní pouze příjemce. Myšlenku asymetrické kryptografie lze využít i při podepisování zpráv. Brzy po zveřejnění teoretického schématu asymetrické kryptografie (1978) se objevuje první šifrový systém založený na této myšlence. Vžil se pro něj název RSA (zkratka z prvních písmen tvůrců systému Rivest, Shamir a Adleman). Tento systém se po malých úpravách (především prodloužení bitové délky klíče a stanovení jistých pravidel, která musí klíče splňovat) používá dodnes.[6]

3.1.4 Atest

Atest je podle zákona o informačních systémech veřejné správy osvědčení vydané jedním z atestačních středisek, které potvrzuje shodu daného produktu (např. technického vybavení elektronické podatelny) se standardy ISVS, a tedy i jeho způsobilost pro použití v informačních systémech veřejné správy.[6]

3.1.5 Atestace

Atestací se rozumí v souladu se zákonem o informačních systémech veřejné správy proces posuzování daného produktu (např. technického vybavení elektronické podatelny), jehož cílem je určení způsobilosti jeho použití v informačních systémech státní správy. Atestace probíhá podle příslušných standardů ISVS a metodik atestačních středisek. [6]

3.1.6 Atestační středisko

Atestační středisko ve smyslu zákona o informačních systémech veřejné správy je nezávislý subjekt, který je pověřen Úřadem pro veřejné informační systémy k provádění atestací a udělování atestů [6]

3.1.7 Autentizace

Autentizace je proces, který slouží k ověření prohlášené identity daného subjektu (uživatele). Používané metody pro autentizaci jsou: co znám (heslo), co mám (čipová karta), jaký jsem (biometrické metody). [6]

3.1.8 Certificate revocation list (CRL)

Anglický výraz se překládá jako seznam zneplatněných (odvolaných) certifikátů. CRL vydává poskytovatel v pravidelných, předem stanovených intervalech. Každý zneplatněný certifikát je v CRL identifikován svým unikátním číslem, které je certifikátu přiděleno při jeho vydání a které je jedinečné u daného poskytovatele. Každý vydaný CRL obsahuje přesný časový údaj svého vydání a je podepsán elektronickým podpisem poskytovatele. je veřejně přístupný, zpravidla na webových stránkách poskytovatele. Osoba, která se na podpis spoléhá, do CRL nahlíží, aby zjistila, zda v něm není uvedeno číslo certifikátu, jehož platnost právě ověřuje. Osoba spoléhající se na podpis by měla CRL pravidelně aktualizovat („stahovat“ aktuální CRL), neboť starší aplikace toto zpravidla sama neučiní, ani nerozpozná, že CRL není aktuální. Zákon o elektronickém podpisu používá pojem „seznam kvalifikovaných certifikátů, které byly zneplatněny”. Ukládá poskytovateli povinnost „zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem”. [6]

3.1.9 Certifikační autorita

Certifikační autorita je subjekt, který je důvěryhodný pro uživatele certifikačních služeb, tj. pro podepisující osoby, kterým vydává certifikáty, a pro osoby, které se spoléhají na podpisy, s nimiž jsou tyto certifikáty spojeny. Certifikační autorita zejména vydává certifikáty a zajišťuje jejich správu, včetně vydávání CRL. Vydané certifikáty a CRL podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci a je identifikovatelná jako subjekt, který je vydal.

Certifikační autorita může některé činnosti zajišťovat prostřednictvím jiných subjektů, např. služby registračních autorit, vždy však zůstává odpovědná za poskytované služby. Certifikační autorita může prostřednictvím jiných subjektů

zajišťovat i vydávání certifikátů; data pro vytváření elektronického podpisu (soukromý klíč), kterými jsou tyto certifikáty podepisovány, však musí být vždy identifikovatelná jako náležející certifikační autoritě a certifikační autorita je odpovědná za náležité zacházení s nimi.

Certifikační autoritou se rozumí „certification-service-provider" ve smyslu směrnice o elektronických podpisech a „poskytovatel certifikačních služeb" ve smyslu zákona o elektronickém podpisu. Někdy je pod pojmem „certifikační autorita" chápán pouze příslušné aplikační softwarové a technické vybavení, s jehož pomocí jsou certifikáty vydávány.[6]

3.1.10 Certifikační politika

Zákonu o elektronickém podpisu definuje certifikační politiku jako dokument, který vydává poskytovatel a který obsahuje informace o poskytovateli, jeho službách a jejich cenách. Certifikační politika je velmi důležitým dokumentem pro uživatele služeb poskytovatele. Na jejím základě je možné posoudit kvalitu nabízených služeb, dále například zjistit, zda je poskytovatel pojištěn, jak postupuje v krizových situacích nebo zda při vlastní činnosti postupuje v souladu se zásadami stanovenými v tomto dokumentu. Doporučená struktura tohoto dokumentu je obsažena v RFC 2527. Certifikační politika odpovídá na otázku „co poskytovatel dělá", certifikační prováděcí směrnice na otázku „jak poskytovatel dělá to, co deklaroval v certifikační politice".

Podle zákona o elektronickém podpisu je poskytovatel vydávající kvalifikované certifikáty povinen vydat certifikační politiku a umožnit k ní trvalý dálkový přístup. [6]

3.1.11 Certifikát veřejného klíče

Certifikát veřejného klíče je datová zpráva, vydaná poskytovatelem, která slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby a tuto osobu identifikuje. Spojuje data pro ověřování podpisu s podepisující osobou a umožňuje s dostatečnou spolehlivostí a věrohodností ověřit, ke které fyzické osobě se data pro ověřování elektronického podpisu vztahují.

Vydáním certifikátu poskytovatel stvrzuje, že data pro ověřování elektronického podpisu patřící určité osobě a že ve spojení s daty pro vytváření elektronického podpisu podepisující osoby vykonávají požadované funkce. Certifikát tedy představuje spojení mezi daty pro ověřování elektronického podpisu a identitou určité osoby (ve smyslu „tato data patří osobě X.Y.“). Identitu podepisující osoby podle typu certifikátu může poskytovatel zjišťovat různými způsoby, v některých případech postačí e-mailová adresa, v jiných je nutné osobně prokázat totožnost příslušnými doklady.[6]

3.1.12 Czech POINT

CzechPOINT je český státní projekt, v jehož rámci obecní úřady s rozšířenou působností, krajské úřady, notáři a další právnické osoby (např. provozovny České pošty a.s. a lokální pracoviště Hospodářské komory ČR s příslušným oprávněním) mohou lidem vydávat výpisy z katastru nemovitostí, z rejstříku trestů či živnostenského rejstříku. Vznikl 22. června 2005 a jeho propagátorem byl poslanec Ivan Langer, který byl od roku 2006 ministr vnitra v Topolánkově vládě. Síť byla naplno spuštěna 28. ledna 2008. Na Czech POINTech lidé získávají veškeré údaje, opisy a výpisy, které jsou vedeny v centrálních veřejných evidencích a registrech o jejich osobě, majetku a právech. Odpadává tak další obíhání po úřadech dle hesla „nemá obíhat občan, ale dokument“.[7]

3.1.13 Časová značka

Časová značka je auditovatelný záznam uchovávaný v bezpečném prostředí třetí důvěryhodnou stranou, která spojuje zasílaná data s hodnotou času při jejich přijetí do archivu.[6]

3.1.14 Časové razítko

Časové razítko je časový záznam digitálně podepsaný důvěryhodnou třetí stranou. Obecně můžeme říci, že časové razítko poskytuje důkaz existence v čase, tedy důkaz, že daná data existovala před uvedeným časem. Časové razítko je tedy rozhodným

nástrojem pro určování, zda elektronický dokument, a tedy i samotný elektronický podpis, byl vytvořen v okamžiku platnosti jeho certifikátu. Žadatel (jakákoli osoba, která má zájem o získání časového razítka pro svoje data) nejdříve zašle autoritě časových razítek (AČR) žádost o časové razítko. Její součástí jsou především předmětná data, resp. jejich otisk. Přesný formát žádosti specifikuje dokument RFC 3161 (viz RFC). Autorita časových razítek po přijetí žádosti zkontroluje její správnost a postoupí ji do generátoru časových razítek. Zde se vytváří časové razítko jako datová položka, jejíž součástí je hodnota času, sériové číslo razítka, identifikátor politiky autority a datum. Časové razítko se pak připojí k zaslanému otisku a tato dvojice se podepíše soukromým klíčem autority časových razítek. Tím vzniká tzv. časový token (TST), který se zasílá žadateli běžně ve formátu DER či PEM.[6]

3.1.15 Data pro vytváření elektronického podpisu

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

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

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

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

Data pro vytváření elektronického podpisu mohou být uložena na pevném disku počítače, na disketě, na čipové kartě nebo v přenosném bezpečnostním modulu (souhrnně „tokeny"). je vhodné, aby přístup k těmto datům byl chráněn přístupovým heslem, frází, PINem apod., které zná jen jejich vlastník. Volba nosiče by měla odpovídat účelu, pro který bude elektronický podpis používán.[6]

3.1.16 Datová schránka

Datová schránka je v českém právním řádu od roku 2009 definována jako elektronické úložiště speciálního typu zřízené podle příslušného zákona, které je určeno k doručování elektronických dokumentů od orgánů veřejné moci a k provádění úkonů vůči orgánům veřejné moci. Novela zákona doplnila ještě s účinností od 1. ledna 2010 dodávání dokumentů fyzických i právnických osob mezi sebou. V obecném významu

však původně toto sousloví označovalo jakékoliv úložiště dat, zpravidla v elektronické podobě, například e-mailovou schránku. Ze zákona musí být datová schránka zřízena každému orgánu veřejné moci, každé podnikající fyzické nebo právnické osobě a některým dalším typům subjektů. Ostatní fyzické a právnické osoby mají právo nechat si datovou schránku bezplatně zřídit. Orgány veřejné moci jsou povinny posílat dokumenty adresátům přednostně do datové schránky, mají-li ji zřízenu, a vzhledem k právní fikci doručení tak mají subjekty, jimž schránka byla zřízena, de facto povinnost si z ní dokumenty vyzvedávat. Česká republika je údajně prvním státem na světě, kde je používání datové schránky pro orgány veřejné moci a podnikající subjekty takto povinné.[7]

3.1.17 Elektronická podatelna

Elektronická podatelna ve smyslu nařízení vlády k zákonu o elektronickém podpisu je místo pro příjem a odesílání datových zpráv, které musí zřídit orgány veřejné moci k přijímání elektronicky podepsaných zpráv. Elektronická podatelna je informačním systémem veřejné správy a proto se na ni vztahují standardy ISVS.[6]

3.1.18 Elektronický podpis

Elektronický podpis jsou, pro účely zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů, data v elektronické podobě, která jsou připojena k datové zprávě nebo jsou s ní logicky spojena, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. V tomto pojetí se může elektronickým podpisem rozumět i podpis v textu e-mailové zprávy. Zákon o elektronickém podpisu upravuje především náležitosti zaručeného elektronického podpisu a elektronickým podpisem ve smyslu předchozí definice se dále nezabývá, je v zákoně použit pouze podpůrně. Z toho důvodu se v praxi pod pojmem elektronický podpis většinou rozumí zaručený elektronický podpis.[6]

3.1.19 Hashovací funkce

Hashovací funkce je obecně matematická funkce, jejímž vstupem je libovolně velký datový blok a výstupem je datový řetězec pevné délky. V oblasti digitálních podpisů se hashovací funkce obvykle používají k výpočtu tzv. otisku podepisované zprávy. Namísto původní zprávy tak podepisujeme její podstatně „kratší" otisk (délky např. 128 nebo 160 bitů). Vlastnosti takových hashovacích funkcí navíc zaručují, že je prakticky nemožné vytvořit k libovolné zprávě jinou zprávu, která by měla stejný otisk. Pokud tedy ve zprávě změníme byť i jediné písmeno, otisk na výstupu bude zcela odlišný. Hashovací funkce jsou veřejně známé a kdokoli si může vypočítat otisk libovolného datového souboru. Mezi nejznámější a nejpoužívanější hashovací funkce patří MD5 (Message Digest, otisk délky 128 bitů) a SHA-1 (Secure Hash Algorithm, otisk délky 160 bitů).[6]

3.1.20 Identifikace

Identifikací rozumíme proces, při kterém se subjekt prohlašuje za určitou entitu informačního systému. Při zasílání elektronicky podepsaných zpráv se identifikace podepisující osoby může provádět například prohlášením v textu zprávy, odesláním zprávy z e-mailového účtu známého příjemci. V souladu se zásadami PKI se identifikace provádí pomocí certifikátu. Po identifikaci podepisující osoby musí následovat její autentizace.[6]

3.1.21 Integrita (neporušenost)

U dokumentů podepisovaných elektronicky je potřeba zajistit podobné vlastnosti, které zajišťuje podpis na klasickém dokumentu. Především se vyžaduje, aby u již podepsaného dokumentu bylo možno zjistit, zda nebyl následně změněn. Tato vlastnost se nazývá integrita nebo-li neporušenost.[6]

3.1.22 Kořenová certifikační autorita (root CA)

Kořenová certifikační autorita je certifikační autorita, která je pro podřízené certifikační autority důvěryhodným ověřovatelem jejich certifikátů. Kořenová

certifikační autorita si sama vydává a podepisuje svůj certifikát kořenové autority a podepisuje certifikáty podřízených certifikačních autorit. Kořenová certifikační autorita většinu svého života zůstává ve stavu „spánku", neboť její úkoly jsou jedinečné. Je důležité uchovat její podepisovací klíče na mimořádně bezpečném místě, neboť se jedná o vrchol důvěry v celé PKI .[6]

3.1.23 Kořenový certifikát

Kořenový certifikát je certifikát kořenové certifikační autority. Tento certifikát je „self-signed" (samopodepsaný) a zpravidla se vydává s velmi dlouhou dobou platnosti (např. 10 nebo 50 let). Při jeho generování jsou použity parametry, které by měly obstát i zkoušku časem (dlouhé asymetrické klíče a bezpečné hashovací funkce). Seznam zneplatněných certifikátů se k tomu certifikátu vydává pouze jednou. Jelikož je kořenový certifikát „self-signed", důvěra v něj se neopírá o další důvěryhodnou stranu. To znamená, že teoreticky všichni uživatelé daného PKI (podepisující osoby, podřízené CA, spoléhající strany apod.) důvěřují této certifikační autoritě.[6]

3.1.24 Kvalifikovaný certifikát

Kvalifikovaný certifikát je certifikát vydaný podle zákona o elektronickém podpisu a obsahuje položky podle § 12 tohoto zákona. Oprávnění vydávat kvalifikované certifikáty má pouze „poskytovatel certifikačních služeb vydávající kvalifikované certifikáty", jehož povinnosti stanoví především § 6 zákona o elektronickém podpisu a upřesňuje vyhláška k tomuto zákonu. Při komunikaci v oblasti orgánů veřejné moci je možné používat pouze kvalifikované certifikáty vydané akreditovaným poskytovatelem.[6]

3.1.25 Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis je zaručený elektronický podpis, který byl vytvořen pomocí prostředku pro bezpečné vytváření elektronického podpisu

a je založený na kvalifikovaném certifikátu. Směrnice o elektronických podpisech vyžaduje, aby kvalifikovanému elektronickému podpisu byly přiznány stejné právní účinky vůči podepisovaným datům v elektronické podobě, jako má vlastnoruční podpis vůči listině.[6]

3.1.26 Neodmítnutelnost též nepopiratelnost nebo neodvolatelnost

Jedná se o jednu ze čtyř vyžadovaných vlastností elektronického podpisu (zachování integrity, možnost identifikace, nepopiratelnost vytvoření podpisu, právní akceptovatelnost). Elektronický podpis musí zajistit, aby osoba, která se podepsala, nemohla později popřít, že tento úkon vykonala. Jedná se tedy o nemožnost odmítnutí odpovědnosti za jeho použití k právním úkonům elektronicky podepsaným tímto klíčem. je to však nejen právní pojem, ale i technický výraz. V tomto případě se tím chápe určení, pro jaký účel se soukromý klíč používá. Všechny možnosti použití klíče jsou stanoveny v certifikátu v položce „použití klíče" (Key Usage).[6]

3.1.27 Osoba spoléhající na podpis

Osoba spoléhající na podpis je zpravidla příjemce elektronicky podepsané zprávy. Může se však jednat i o osobu, která není přímým příjemcem zprávy, ale s elektronicky podepsanou zprávou pracuje a potřebuje se na podpis spoléhat (např. správce daně, auditor, soud apod.).

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

osoby, které certifikát vydává. Při vydávání certifikátů nižších úrovní se neověřuje totožnost, ale například platnost a existence e-mailové adresy. Tento postup však nelze uplatnit v případě, že je vydáván kvalifikovaný certifikát podle zákona o elektronickém podpisu, kdy se jednoznačně požaduje ověření totožnosti žadatele o vydání kvalifikovaného certifikátu a pořízení kopie jeho průkazů totožnosti.

Osoba spoléhající na podpis bývá někdy označována jako „třetí strana".[6]

3.1.28 PKI (Public Key Infrastructure)

PKI je v kryptografii označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy bez nutnosti jejich individuální kontroly.

Infrastrukturu PKI lze spravovat dvěma základními způsoby vytváření vztahů důvěry:

- certifikační autorita – přísně hierarchická struktura,
- síť důvěry – distribuovaný systém.

PKI zahrnuje celou řadu různých komponentů, např.:

- digitální certifikáty,
- šifrovací klíče,
- asymetrická kryptografie,
- certifikační autorita,
- bezpečností architektura sítě,
- způsob bezpečného vydávání certifikátů,
- nástroje pro správu, obnovu a rušení certifikátů. [7]

3.1.29 Soukromý klíč

Soukromý klíč slouží k vytváření elektronických podpisů nebo k dešifrování dat. Musí být uchováván v tajnosti a jeho znalost přísluší pouze jeho vlastníku. To, co zašifrujeme privátním klíčem, lze dešifrovat pouze odpovídajícím veřejným klíčem. [6]

3.1.30 Veřejný klíč

Veřejný klíč se používá jako párové heslo k soukromému klíči. Veřejný klíč umožní dešifrování zprávy nebo ověření identity osoby podepsané elektronickým podpisem. [6]

3.1.31 Podepisující osoba

Ve smyslu zákona č. 227/2000 Sb.,o elektronickém podpisu může být podepisující osobou pouze fyzická osoba. Stejně jako v případě vlastnoručního podpisu není přípustné, aby se elektronicky podepisovala právnická osoba. Jako jsou v organizaci určeni pracovníci, kteří jsou oprávněni svým podpisem opatřovat listinné dokumenty a jednat tak jménem právnické osoby, je stejným způsobem postupováno i u elektronického podepisování. [6]

4 Legislativní rámec elektronického podpisu

Z legislativního hlediska je podpisem stvrzen právní úkon provedený v listinné formě. Podepisující osoba tímto svým podpisem vyjadřuje, že je s dokumentem seznámena, souhlasí s jeho obsahem a potvrzuje svou ochotu dodržet závazky z dokumentu vyplývající. Pro zvýšení autenticity psaného podpisu se používá jeho ověření autoritou, která tento akt stvrdí a ověření zapíše do evidence. Zaručený elektronický podpis dnešní legislativa staví na úroveň takto ověřeného vlastnoručního podpisu.

Prvním zákonem, který upravoval použití elektronického podpisu, byl americký zákon „UTAH Digital Signature Act“ z roku 1995. V Evropě začaly jednotlivé státy řešit tuto problematiku lokálně. Evropská unie však pochopila nutnost jednotného řešení této problematiky včas, a to hlavně proto, že mezi jednotlivými státy unie probíhá čilý obchodní ruch a je potřeba řešit situaci i na poli stále se rozšiřujícího elektronického obchodování. Proto byla v říjnu 1997 předložena studie „O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování“. Na základě této studie vznikla Směrnice Evropského parlamentu a Rady 199/93/ES ze dne 13. Prosince 1999, která je závazná pro všechny státy Evropské unie.

Česká republika transformovala tuto směrnici do samostatné právní normy. Touto normou je Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, který byl vydán dne 1. října roku 2000. Česká republika se tím stala třetí zemí, která upravila používání elektronických podpisů právní normou. Tento základní právní předpis zrovnoprávňuje dokumenty v elektronické podobě s dosavadními klasickými dokumenty v listinné formě. Dalším významným mezníkem v uvádění elektronických podpisů do praxe bylo vydání Nařízení vlády č. 495/2004 Sb. stanovující povinnost orgánům veřejné moci zřídit elektronické podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu). Toto nařízení vlády stanovuje povinnost orgánům veřejné moci přijímat

podání od občanů a od dalších právnických a fyzických osob elektronicky, pokud jsou splněny podmínky stanovené tímto nařízením. Z tohoto důvodu musely orgány veřejné moci vybavit své příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem zpracování a ochranu informací. Toto nařízení nabylo účinnosti k 1. lednu 2005. Dalším legislativním dokumentem upravujícím používání elektronických podpisů byla Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, která byla vydána 2. srpna 2006. První část vyhlášky je určena poskytovatelům certifikačních služeb a obsahuje požadavky na jejich postupy při vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Druhá část se vztahuje na označující osoby, zejména na orgány veřejné moci – obsahuje požadavky na ochranu soukromých klíčů, které se používají při vytváření elektronických značek. První část vyhlášky nabývá účinnosti 17.8.2006, druhá část nabývá účinnosti 1.11.2006. [10]

Dalším legislativním předpisem, který ovlivnil používání elektronických podpisů v České republice, je například Zákon č. 365/2000 Sb. o informačních systémech veřejné správy, zejména pak jeho novela z 20. Června 2007, kterou se realizuje takzvaný projekt Czech POINT (Český podací ověřovací informační národní terminál), který je součástí strategie vlády v oblasti eGovernmentu. Podle této novely byla vytvořena síť CzechPOINTů, tedy míst kontaktu veřejnosti s veřejnou správou.

Dalším milníkem v rozvoji českého eGovernmentu je zprovoznění Datových schránek neboli ISDS (Informační Systém Datových Schránek). V souladu novelou zákona 300/2008 Sb. a prováděcími vyhláškami byl ISDS uveden do provozu 1.7.2009, a vlastní provoz byl zahájen 1.11.2009, kdy systém v souladu se zákonem automaticky aktivoval dosud nezprovozněné schránky.

5 Technologický rámec digitálního podpisu

K lepšímu pochopení principů a technologií digitálního podpisu, musíme nyní krátce odbočit a povědět si něco o šifrování dokumentů, které s digitálním podpisem úzce souvisí. Šifrování zpráv se používá již velmi dlouho a jeho cílem je zabránit odposlouchávání zpráv na jejich cestě od odesilatele k příjemci. S nějakou jednodušší šifrou se zřejmě potkal každý: pomocí nějakého klíče zprávu zakódujeme (například nahradíme písmena jinými symboly), odešleme ji, a příjemce ji pomocí stejného klíče dekóduje do původní čitelné podoby. [11]

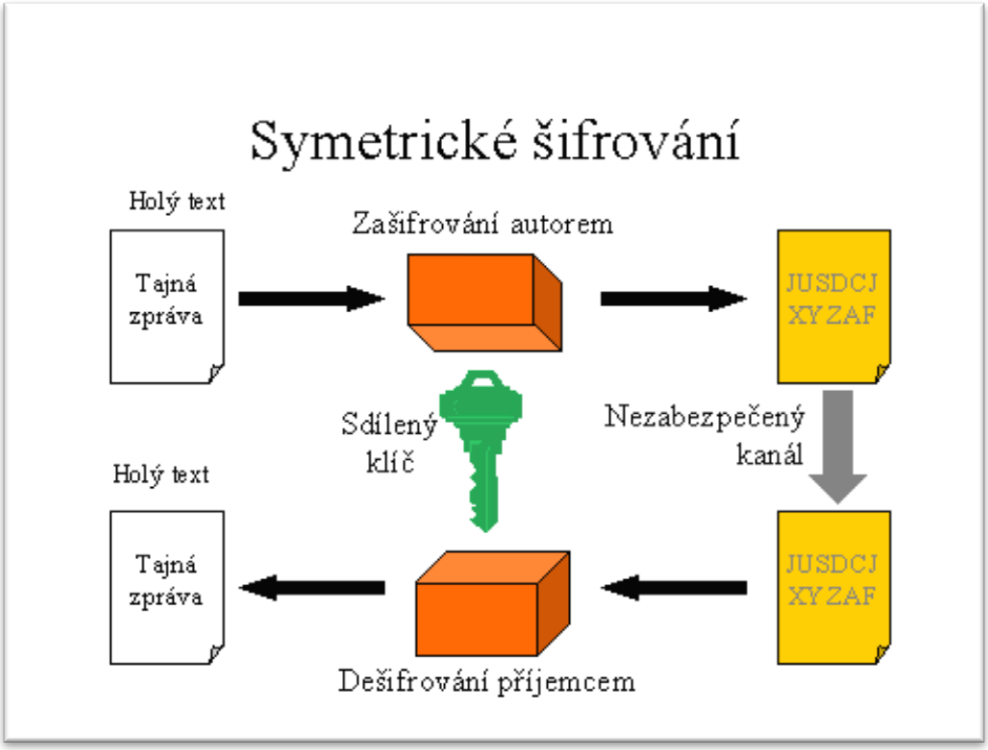
5.1 Algoritmy použité při tvorbě elektronických podpisů

Šifrovací algoritmus je postup, při kterém se libovolná data v obecné podobě převedou na data zašifrovaná, tedy běžným způsobem nečitelná, a zároveň je to i postup pro jejich následné dešifrování, což je jejich převod zpět do původní podoby. Při této činnosti bývá zpravidla použit jeden nebo více šifrovacích klíčů. Tyto klíče se používají pro šifrování a pro dešifrování dat. Podle jejich použití rozlišujeme takzvané symetrické a asymetrické šifrovací algoritmy

5.1.1 Symetrické šifrovací algoritmy

Symetrické šifrovací algoritmy se používají převážně tam, kde je zapotřebí šifrovat velké objemy dat. je to dáno hlavně tím, že pro zašifrování není potřeba tak velkého výpočetního výkonu jako u šifrování asymetrického. Pro šifrování i dešifrování se používá jen jeden klíč. Z této skutečnosti vyplívá potřeba, aby tento klíč byl držen v tajnosti (někdy se používá i název Tajný nebo Sdílený klíč), Proto se tato technologie používá převážně pro šifrování ukládaných dat, nikoliv pro šifrování zpráv. Je totiž problematické udržet šifrovací klíče v tajnosti, pokud se procesu účastní větší množství

osob. Neoprávněná osoba, která se dostane k uloženým zašifrovaným datům, má v případě prozrazení jediného klíč plný přístup k původním informacím.



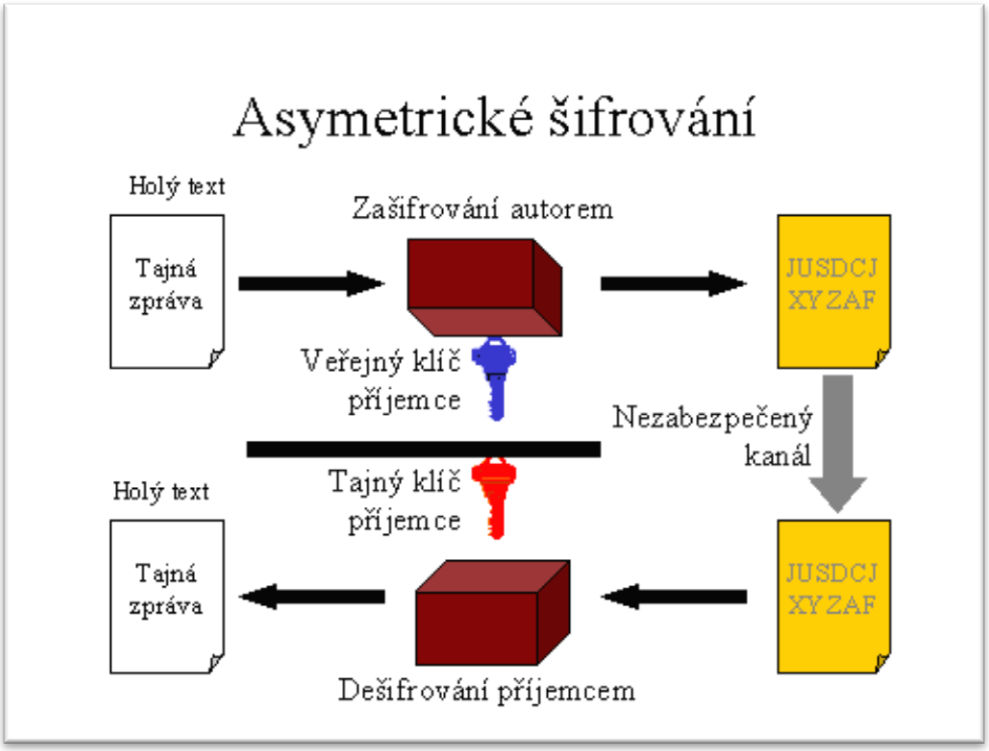
Obrázek 1 - symetrické šifrování (zdroj: http://sandbox.cz/~varvara/El_podpis/ index.html

Symetrické šifrování je velmi jednoduché, rychlé a nenáročné na hardware, ale má bohužel velkou nevýhodu, pro kterou se nedá použít pro přenos datových zpráv ve větším měřítku, Tím je nutnost předat příjemci tajný klíč, aby mohl doručenou datovou zprávu dešifrovat. Tento nedostatek odstraňuje takzvané asymetrické šifrování, které využívá dvojici různých klíčů.

5.1.2 Asymetrické šifrovací algoritmy

Dnes používané asymetrické šifrovací algoritmy vycházejí převážně ze systému RSA. RSA jsou první písmena jmen vědců – kryptografů, kteří tento systém vymysleli. Byli to pánové Rivest, Shamir a Adelmann. Princip asymetrického šifrování vychází z toho, že pro zašifrování a dešifrování zprávy existují dva, od sebe různé, klíče, které

jsou ovšem logicky spojeny. (proto asymetrická kryptografie). Tyto klíče jsou vytvořeny podle metody RSA a první u nich, takzvaný veřejný klíč, se používá k zašifrování datové zprávy a druhý, takzvaný soukromý klíč, se použije pro dešifrování datové zprávy. Tyto klíče se převážně vydávají ve vztahu k jednotlivé osobě a veřejný klíč této osoby je opravdu zcela veřejný, a je dokonce velmi žádoucí aby byl k dispozici komukoliv. To ovšem neplatí o soukromém klíči, který si musí osoba pro kterou byl vytvořen, držet pod svou výhradní kontrolou a tím zabránit jeho kompromitaci. Veřejným klíčem se data dají pouze zašifrovat, soukromým klíčem se dají takto zašifrovaná data dešifrovat. Z této situace vyplívá, že data může veřejným klíčem osoby zašifrovat kdokoliv, a jen osoba, pro kterou byla dvojice klíčů vygenerována, může takto zašifrovaná data dešifrovat a přečíst jejich obsah. Párová dvojice klíčů je vytvořena tak, že z klíče veřejného není možné žádným způsobem odvodit ani spočítat klíč soukromý. To zaručuje, že pouze držitel soukromého klíče může zašifrovanou zprávu dešifrovat a získat její obsah.



Obrázek 2 - Asymetrické šifrováni (zdroj: http://sandbox.cz/~varvara/El_podpis/ index.html)

V praxi vypadá šifrovaná komunikace mezi odesílatelem a příjemcem následovně: odesílatel si zjistí veřejný klíč příjemce, a tímto klíčem zašifruje data, která chce odeslat a poté je odešle na adresu příjemce; příjemce pomocí svého privátního klíče zprávu rozšifruje. V případě, že adresát chce stejným způsobem odpovědět, tak šifruje zprávu veřejným klíčem původního odesílatele, a ten svým privátním klíčem zprávu dešifruje. Je tedy nutno, aby obě strany měly vygenerován svůj asymetrický pár klíčů.

Jediným problémem pro odesílatele může být zjištění veřejného klíče adresáta. V praxi jsou veřejné klíče zveřejňovány na webových serverech certifikačních autorit, nebo stačí, že před započetím šifrované komunikace si odesílatel a adresát navzájem zašlou elektronicky podepsané zprávy, které obsahují veřejnou část asymetrického páru klíčů.

5.2 Zaručený elektronický podpis založený na technologii RSA

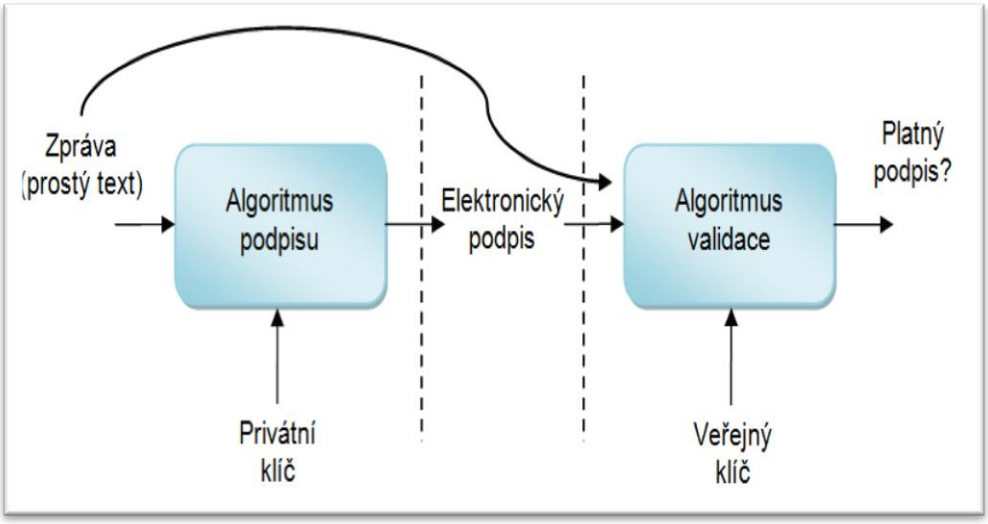
Zaručený elektronický podpis je založen na technologii asymetrického šifrování, konkrétně na systému RSA. Každá fyzická osoba, jíž je elektronický podpis vydán se stává vlastníkem asymetrického páru klíčů stejně jako při asymetrickém šifrování. Připojení tohoto podpisu k datové správě nebo k dokumentu je zcela identické jako podpis autora vlastní rukou na dokumentu v listinné podobě. je ovšem rozdíl v typech elektronických podpisů a v jejich použití, Ne každý certifikát je možno použít jako podpis, a různé podpisy mají různou právní váhu. Viz kapitola Druhy elektronických podpisů. Elektronický podpis připojený k datové zprávě nebo k dokumentu by měl zajistit již dříve zmíněné atributy. Jsou to:

- Autentičnost – autor je jednoznačně identifikovatelný
- Nepopiratelnost – autor nemůže popřít, že byl s dokumentem seznámen, že s ním souhlasí a že jej podepsal vědomě.

- Integrita – pokud je připojený podpis ověřen certifikační autoritou, tak to znamená, že od doby podpisu nebyl změněn a je pravý

5.2.1 Principy elektronického podpisu

Elektronický podpis může být použit pro distribuci zprávy ve formátu prostého textu v případech, kdy příjemce musí identifikovat a ověřit odesílatele zprávy. Podepsání zprávy nemění vlastní zprávu, ale vytvoří řetězec znaků elektronického podpisu. Tento řetězec znaků může být následně připojen ke zprávě, nebo může být odeslán nezávisle. Formát předání zprávy a elektronického podpisu se řídí definovanými pravidly (standardy), kterých existuje celá řada, a hraje důležitou roli v celém procesu. Elektronický podpis reprezentuje malý objem dat, která jsou zašifrována privátním klíčem odesílatele. Při rozšifrovaní dat se použije veřejný klíč odesílatele, který zaručí, že data byla zašifrována odesílatelem popř. někým, kdo má přístup k privátnímu klíči odesílatele. Elektronický podpis je vytvářen s využitím veřejně dostupných algoritmů a privátního klíče a je ověřován odpovídajícím veřejným klíčem. Tento proces je zobrazen na následujícím obrázku.

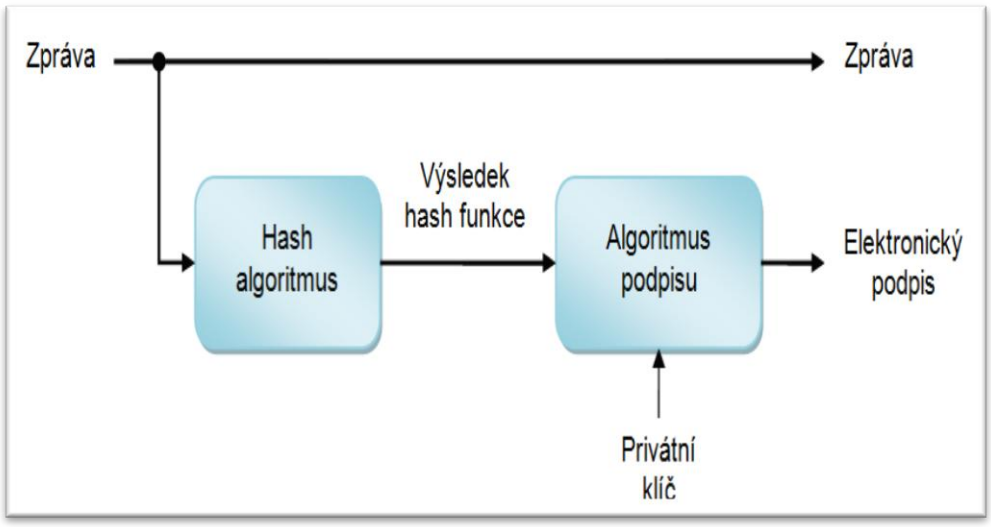


Obrázek 3 - Proces vytváření a ověřování elektronického podpisu

V průběhu vytváření elektronického podpisu vstupují do hry dva základní kroky. V prvním kroku je z vlastní zprávy vytvářena hodnota funkce hash (známá také jako

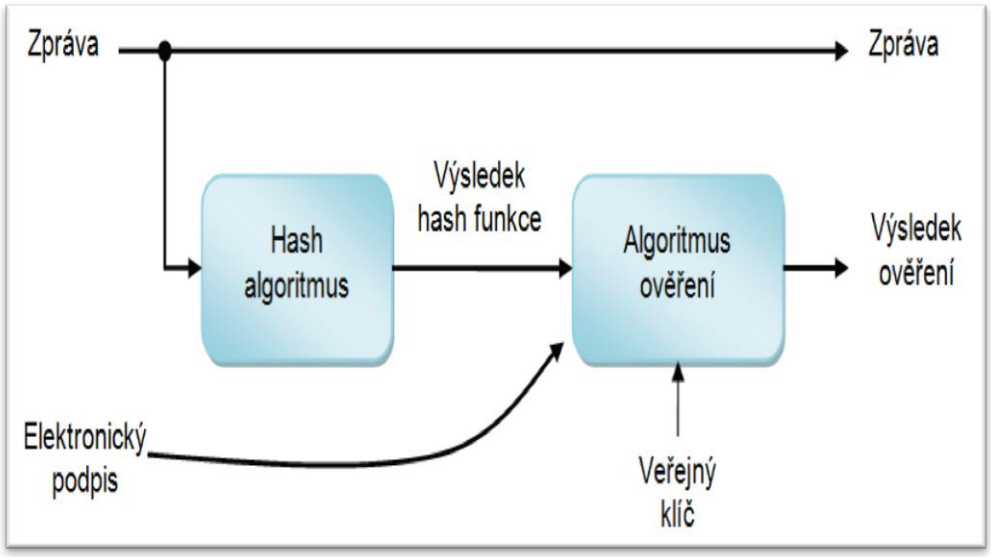
message digest). Tato výsledná hodnota je následně v dalším kroku podepsána s využitím privátního klíče odesílatele. Proces podepsání ve skutečnosti znamená zašifrování hodnoty hash privátním klíčem.

Následující obrázek je ilustrací dvou kroků použitých při vytváření elektronického podpisu.



Obrázek 4 - Proces vytváření elektronického podpisu

Pro vlastní kontrolu podpisu je nezbytné mít k dispozici vlastní zprávu a elektronický podpis. Za prvé se ze zprávy vytvoří hodnota funkce hash stejným postupem, jaký byl použit při vytváření elektronického podpisu. Veřejným klíčem odesílatele se rozšifruje hodnota funkce hash v elektronickém podpisu (ta byla vytvořena při podepisování). V případě, že se první hodnota funkce hash shoduje s rozšifrovanou hodnotou, je prokázáno, že zpráva je ta, kterou odesílatel podepsal, a že nebyla změněna. Následující obrázek ilustruje proces ověření elektronického podpisu.



Obrázek 5 - Proces ověřování elektronického podpisu

Hodnota funkce hash je složena z malého množství binárních dat, definované délky podle zvoleného hash algoritmu. Např. délka pro SHA-1 je 160 bitů a pro SHA-256 je výstupní délka 256 bitů. Všechny výsledné hodnoty funkce hash sdílejí stejné vlastnosti bez ohledu na použitý algoritmus.

Délka hodnoty hash je dána typem použitého hash algoritmu, a tato délka se nemění v závislosti na délce vlastní zprávy. Přechod na algoritmy rodiny SHA-2 znamená, že se zvětšuje délka hodnoty hash ze 160 bitů u algoritmu SHA-1 na příslušnou délku nového algoritmu SHA-2.

Každá dvojice neidentických zpráv vede na totálně rozdílnou hodnotu hash, dokonce i v případě, že se dvě zprávy liší pouze v jediném bitu. I pro splnění této podmínky se přechází na hash algoritmy s větší délkou výstupní hodnoty.

Pokaždé, když je počítána hodnota hash z příslušné zprávy za použití toho samého algoritmu, je vytvořena stejná hodnota funkce hash.

Hash algoritmus je jednosměrná funkce. Z dané výsledné hodnoty hash funkce není možné obnovit původní zprávu. [12]

5.3 Certifikát

Pokud je požadováno, aby byl elektronický podpis opravdu důvěryhodný, je nutné prokázat, že privátní klíč, pomocí kterého byl podpis vytvořen, skutečně patří podepisující osobě. K tomu slouží takzvaný certifikát, což je vlastně dokument vydaný třetí důvěryhodnou stranou, která stvrzuje, že podepisující osoba je vlastníkem daného páru klíčů. Tento certifikát je potom připojen k vlastnímu podpisu. [11]

Certifikát je tedy pro příjemce jakýmsi potvrzením o tom, že odesílatel je opravdu tím kdo je uveden v certifikátu, a že je vlastníkem páru asymetrických klíčů. Tato skutečnost je tak důvěryhodná, jak je důvěryhodná certifikační autorita, která podepisující osobě vydala certifikát.

5.4 Ověření platnosti elektronického podpisu

Dalším důležitým krokem v používání elektronického podpisu je ověření jeho platnosti. Toto ověření se skládá z několika úkonů:

- Ověření neporušenosti integrity podepsané zprávy nebo dokumentu. V případě, že je integrita porušena, tak je podpis automaticky považován za neplatný.
- Ověřuje se platnost certifikátu v konkrétním okamžiku. Tento okamžik musíme ovšem podle dvou hledisek, a to zda je řádně platný podle data v něm uvedeném, a zda nebyl revokován.

- V případě, že jde o certifikát, který je již v době ověřování neplatný, a je-li připojeno časové razítko, které je platné, tak se posuzuje, zda byl certifikát platný v době připojení časového razítka.
- Dále se stejným způsobem kontroluje platnost nadřízených, takzvaných kořenových certifikátů certifikační autority, která certifikát vydala.

V případě, že jakákoliv z výše uvedených podmínek není splněna, tak musíme zprávu nebo dokument považovat za nedůvěryhodnou.

5.5 Bezpečnost při používání elektronického podpisu

Při podmínce využívání elektronického podpisu jako plnohodnotné náhrady vlastnoručního podpisu je třeba, aby technologie elektronického podpisu byla považována za bezpečnou. Vzhledem k tomu, že elektronický podpis je pouze řetězec dat, který je zkonstruován na základě nějakých pravidel, a je vytvořen softwarem, který je k tomuto účelu naprogramován. Parametry pro vytvoření do software zadává uživatel. Tato vstupní data a hardware musí být pod jeho výhradní kontrolou. Veškerá bezpečnost je tedy založena na složitosti a bezpečnosti algoritmu, podle kterého jsou vytvořeny klíče podpisu, a na jejich ochraně ze strany uživatele

5.5.1 Základní podmínky bezpečnosti

Existují tři základní podmínky bezpečnosti elektronického podpisu, které musejí být vždy splněny, aby elektronický podpis mohl být považován za pravý, neporušený a bezpečný. Tyto tři podmínky musí být splněny vždy společně.

- Algoritmus, podle kterého byl elektronický podpis vytvořen, nebyl prolomen a ani nebyla zpochybněna hashovací funkce
- Pravost elektronického podpisu byla ověřena bezpečnou certifikační autoritou – veřejná část klíče je pravá a platná

- Privátní část klíče je pod výhradní kontrolou držitele

Tyto tři podmínky se vztahují hlavně k zaručenému elektronickému podpisu, který je založen na kvalifikovaném certifikátu. Jedině tento elektronický podpis je ze zákona akceptovatelný v elektronické komunikaci s veřejnou správou. Existují samozřejmě i elektronické podpisy s nižším zabezpečením, ale ty mají jiné použití a nižší požadavky na bezpečnost.

Nejproblematičtější z pohledu příjemce podepsané zprávy se jeví hlavně třetí podmínka, a to proto, že její splnění nelze technickými prostředky kontrolovat a proto je založena hlavně na důvěře v odesílatele.

5.5.2 Bezpečnostní rizika

Největší rizika jsou:

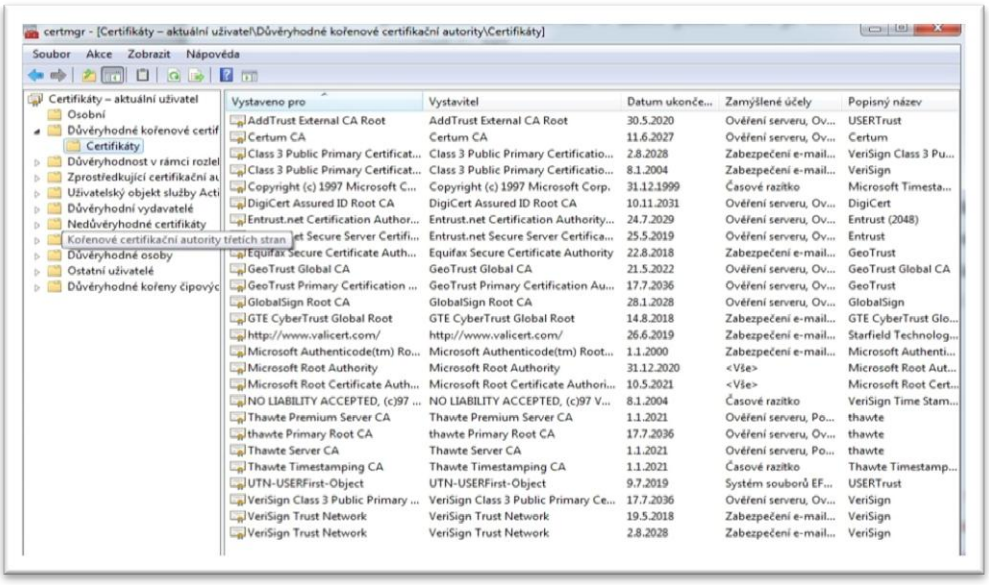
- Uživatel nemá privátní klíč pod výhradní kontrolou – odcizení privátního klíče, nebo jeho zneužití vydavatelem
- Podvržení padělaného privátního klíče
- Narušení algoritmu, podle kterého byly klíče generovány.

5.5.3 Bezpečné uchování soukromého klíče

Pro splnění třetí bezpečnostní podmínky je nutné, aby soukromý klíč byl jeho uživatelem bezpečně uložen a chráněn proti zneužití. K tomuto účelu slouží úložiště klíčů přímo v počítači uživatele, nebo různá mobilní zařízení. Tato úložiště a mobilní zařízeni se liší stupněm ochrany soukromého klíče proti zneužití. V případě, že by došlo k prolomení ochrany úložiště nebo mobilního zařízení, tak by se mohl, ten kdo získá nad nimi kontrolu, vydávat za vlastníka elektronického podpisu a jeho vlastním jménem mu způsobit nemalé škody.

5.5.3.1 Úložiště systému Microsoft Windows

Systém Microsoft Windows obsahuje modul úložiště certifikátů, který je součástí Microsoft management console. V tomto úložišti jsou uloženy všechny certifikáty. Jedná se o certifikáty osobní – elektronické podpisy, certifikáty kořenových autorit, certifikáty třetích stran, elektronické značky technologické komponenty a další. Elektronické podpisy uložené v tomto úložišti je možno zabezpečit proti zneužití heslem. V případě této ochrany je třeba při každém použití elektronického podpisu zadat heslo, které je známo pouze majiteli klíče.



Obrázek 6 - Úložiště systému Microsoft Windows 7

5.5.3.2 Čipové karty

Bezpečné uložení certifikátů nabízí čipové karty. Jedná se o plastové karty o rozměrech běžné bankovní karty s paměťovým nebo mikroprocesorovým čipem. Mohou být s kontakty, nebo i bezkontaktní. V čipu jsou uloženy certifikáty, a to jak certifikáty uživatele, tak i kořenové certifikáty autority která zaručený elektronický podpis vydala a případně i další doplňkový obsah. Certifikáty na těchto kartách jsou chráněny osobním pinem, který je vyžadován vždy, pokud je třeba ho použit pro

elektronický podpis dokumentu nebo zprávy. Používání těchto čipových karet vyžaduje zvláštní hardwarovou výbavu počítače – čtečku čipových karet a speciální obslužný software, který se používá pro nahrávání certifikátů na čipové karty a integruje do počítače možnosti jejich použití. Problémem tohoto řešení je ovšem kompatibilita čteček s čipovými kartami a to, že jen málo uživatelů zvládne složitost instalace čtečky a ovládacího software. Proto se toto řešení využívá nejčastěji v bankovním sektoru pro zabezpečení komunikace mezi peněžním ústavem a jeho klientem. Banky toto řešení dodávají jako kompletní službu ke svým produktům, a vzhledem ke složitosti k této službě poskytují i servis.

Obrázek 7 - Příklady čteček a čipových karet

Velkou výhodou čipových karet je možnost integrace funkcí, kdy jedna karta v sobě může integrovat například přístupový klíč do budovy, elektronickou peněženku, kreditní nebo debetní bankovní kartu, identifikační průkaz, úložiště elektronického podpisu, biometrické údaje uživatele a mnoho dalších. Zde se skrývá velký potenciál pro zefektivňování vnitrofiremních procesů nebo pro veřejnou správu v práci s občany. Příkladem tohoto řešení je i kontroverzní projekt elektronického občanského průkazu.

5.5.3.3 Tokeny

Dalším hardwarovým úložištěm elektronického podpisu je USB token. Jeho použití je podstatně jednodušší než u čipové karty. USB token je zařízení které v sobě

integruje USB rozhraní pro připojení k počítači a čip pro uložení certifikátů. Jeho použití je stejné jako u čipové karty. Jeho použití je vázáno na osobní pin, nebo u moderních zařízení i na biometrickou autentifikaci uživatele – otisk prstu. Připojuje se přímo na port USB, který je součástí každého osobního počítače. I v tokenu je možno integrovat funkce, takže je možné jej používat například jako úložiště dat. USB token je oproti čipové kartě jednodušeji použitelným bezpečnostním řešením, pro které není třeba další čtecí zařízení. V některých případech je nutné však instalovat obslužný software

obrázek 8 – USB token a USB token s biometrickým zabezpečením

5.5.4 Uživatelé

Výše uvedené způsoby ochrany zaručeného elektronického podpisu jsou technologického charakteru, a bez odpovědného přístupu jejich uživatelů jsou zcela neúčinné. Při používání elektronického podpisu je proto nutné zachovávat jistá pravidla, aby nedošlo k vyzrazení osobních identifikačních údajů umožňujících použití elektronického klíče. Nebo aby nedošlo dokonce k odcizení privátního klíče. V případě, že k takové situaci dojde, měl by uživatel okamžitě zneužitý nebo zcizený elektronický podpis zneplatnit.

6 Elektronické podpisy

6.1 Druhy elektronických podpisů

V praktickém životě se můžeme setkat s různými druhy elektronických podpisů. Elektronické podpisy dělí na tyto kategorie:

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

K vymezení jednotlivých typů podpisů použijeme následující kategorie:

- politika kvalifikovaného certifikátu (zpravidla uvedena v certifikační politice),
- formát elektronického podpisu,
- formát kvalifikovaného certifikátu,
- časové razítko,
- požadavek na bezpečný systém,
- požadavek na prostředek pro bezpečné vytváření elektronického podpisu [1]

6.1.1 Elektronický podpis

Vyjdeme z vymezení, které je obsaženo v § 2 písm. a) zákona o elektronickém podpisu: elektronickým podpisem (se rozumí pro účely tohoto zákona) údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky

spojené, a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

Požadavky na sledované kategorie jsou zcela minimální. Nepožaduje se časové razítko, není definován žádný konkrétní formát nebo standard, který popisoval tvar vytvořených nebo předávaných dat. Není použit certifikát nebo jiný způsob zveřejnění pomocných dat. Nejsou kladeny žádné specifické požadavky na použitý podpisový systém, na prostředek pro vytváření elektronického podpisu.

Tento typ podpisu nemá pro příjemce příliš velkou vypovídací hodnotu. Slouží spíše pro informaci příjemce. Příkladem může být klasický podpis pod e – mailovou zprávou nebo identifikace autora v záhlaví článku. [1]

6.1.2 Zaručený elektronický podpis

Začněme opět definicemi. Porovnáním definice uvedené v zákoně o elektronickém podpisu, § 2 písm. b) a definice ve Směrnici, článek 2 odst. 2 zjistíme, že tento pojem je zaveden obdobným způsobem a nemůže dojít k zásadně odlišnému chápání. Zákon o elektronickém podpisu, § 2 písm. b): zaručeným elektronickým podpisem se rozumí pro účely tohoto zákona elektronický podpis, který splňuje následující požadavky:

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

- je jednoznačně spojen s podepisující osobou
- umožňuje identifikovat podepisující osobu;

- je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou;
- je spojen s daty, ke kterým se vztahuje, tak, aby bylo možno zjistit jakoukoliv následnou změnu těchto dat.

Takovýto podpis má pro příjemce již vyšší vypovídací hodnotu. Důvěra v takto vytvořený podpis je tedy podstatně vyšší než v případě elektronického podpisu. Slouží pro styk příjemce a odesílatele, kteří se na takovéto komunikaci předem dohodnou. Příjemce musí od podepisující se osoby získat důvěryhodným způsobem její data sloužící k ověření zaručeného elektronického podpisu. Příkladem komunikace, ke které muže být tento druh podpisu využit, muže být (s pomocí dohodnutého protokolu) komunikace klient - banka či obchodník - zákazník. [1]

6.1.3 Zaručený elektronický podpis založený na kvalifikovaném certifikátu

Tento elektronický podpis využívá k ověření kvalifikovaný certifikát vydaný akreditovanou certifikační autoritou.

Zákon č.227/2000 Sb., o elektronickém podpisu v § 2 písm. k) definuje, že „certifikátem je 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“. Kvalifikovaný certifikát je pak „certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanoveném tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty“. [8]

6.1.4 Zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb

Tento elektronický podpis se shoduje s podpisem uvedeným v předchozí podkapitole, je však o stupeň důvěryhodnější, a to proto, že kvalifikovaný certifikát pro tento elektronický podpis vydala akreditovaná certifikační autorita.

V § 11 písm. a) zákona č.227/2000 Sb., o elektronickém podpisu je uvedeno „V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb“.[8] Tím je stanoveno, že pouze elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb je ve veřejné správě uznáván a ostatní elektronické podpisy nejsou prokazatelné pro svoji nízkou výpovědní hodnotu a zabezpečení.

Poskytovatelé certifikačních služeb se dělí na poskytovatele, kteří vydávají certifikáty, na poskytovatele, kteří vydávají kvalifikované certifikáty a na akreditované poskytovatele. Akreditovaným poskytovatelem certifikačních služeb se rozumí poskytovatel, jemuž byla udělena akreditace podle zákona. Každý poskytovatel může požádat Úřad pro ochranu osobních údajů o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. V oblasti veřejné moci se smí používat pouze kvalifikované certifikáty vydané akreditovaným poskytovatelem.

Tento typ podpisu je základním typem elektronického podpisu, kterým se zabývá zákon o elektronickém podpisu. Pro příjemce má vysokou vypovídací hodnotu a důvěra v něj je také vysoká. je totiž podpořena právními aspekty, které vyplývají z použití takovéhoto podpisu a které plynou ze zákona. Příjemce podepsanou osobu nemusí osobně znát, data pro ověřování elektronického podpisu získá přímo z kvalifikovaného certifikátu. na rozdíl od předchozího případu se nemusí tedy uzavírat speciální smlouvy pro právní podporu této komunikace. Důvěra v obsah certifikátu je podmíněna důvěrou v poskytovatele certifikačních služeb, který certifikát vydal. Tato důvěra vyplývá

i ze skutečnosti, že zákon o elektronickém podpisu stanoví poskytovatelům vydávajícím kvalifikované certifikáty celou řadu povinností. Obecně se považuje tento typ za vhodný pro přímou komunikaci mezi subjekty. Není vhodný k archivaci dat a tam, kde je nutné zpětně prokazovat, kdy přesně byl dokument podepsán. [1]

6.1.5 Kvalifikovaný podpis

Tento termín není v zákoně o elektronickém podpisu přímo použit. Přesto je na několika místech zmíněn, vždy však jen opisem. Poprvé se s ním můžeme setkat v § 3 odst. 2: „Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.“ Od předchozího typu se liší požadavkem na použití prostředku pro bezpečné vytváření podpisu. Požadavky na tento prostředek jsou uvedeny v § 17 zákona o elektronickém podpisu. Právě ale pojmy „prostředek pro bezpečné vytváření podpisu“ a „prostředek pro bezpečné ověřování podpisu“ patří k nejproblematičtějším v celém systému elektronického podepisování. Kvalifikovaný podpis se považuje z hlediska důvěry za nejvhodnější. Pro příjemce má velmi vysokou vypovídací hodnotu. V dokumentech Evropské unie se uvažuje, že by mohl být používán v těch situacích, kde se v písemné formě vyžaduje vlastnoruční podpis. [1]

6.1.6 „Vylepšený“ elektronický podpis

Tento typ je obecně použitelný s libovolným předchozím typem. Liší se přidáním některého z dalších požadavků na podpis (např. časová značka, rozšířené požadavky na verifikaci, rozšířená ochrana proti určitému druhu útoků). [1]

6.1.7 Kvalifikovaný podpis určený pro archivaci dat

Nejdůležitějším typem, který vznikl jako vylepšený elektronický podpis z kvalifikovaného podpisu. Vzhledem ke specifickým požadavkům je využití zřejmé – dlouhodobá archivace elektronicky podepsaných dokumentů v elektronické formě. V této souvislosti se připomíná, že pokud tuto službu zajišťuje poskytovatel certifikačních služeb, měl by zajistit i uchování příslušného software, který umožní otevření a zobrazení podepsaných dat i v době, kdy tento software již není běžně používán. Vzhledem k tomu, že musí být zajištěna odolnost proti útoku po celou dobu archivace, je v kategorii prostředek pro bezpečné vytváření podpisu vznesen požadavek zvýšené bezpečnosti. [1]

6.1.8 Časové razítko

Elektronický podpis sice obsahuje nějaký údaj o čase, ale na ten se nemůžeme spoléhat. Takže je to vlastně stejné, jako kdyby tam vůbec nebyl. A to znamená, že vlastně nikdy nevíme (dostatečně spolehlivě), kdy přesně ten který elektronický podpis vznikl. Problém s nedůvěryhodností časového údaje „uvnitř“ elektronického podpisu je samozřejmě řešitelný: údaj o čase si necháme poskytnout od nějaké dostatečně důvěryhodné třetí strany. Od někoho, kdo má přímo povinnost mít správně seřízené hodinky, a bude také ručit za správnost poskytnutého časového údaje.

Proto se zde hovoří o časovém razítku, místo o elektronickém podpisu či značce. A to i v zákonech, kde je časové razítko definováno a má skutečně úplně jiné postavení, než elektronický podpis: pouze osvědčuje, že to, co je časovým razítkem opatřeno, již existovalo v době vzniku časového razítka. Přesněji, abychom dodrželi dikci zákona: existovalo před okamžikem, uvedeným na časovém razítku.

V praxi tedy budeme časové razítko používat k tomu, abychom „zafixovali“ dobu vzniku elektronického podpisu: když budeme mít elektronický dokument, opatřený

elektronickým podpisem, přidáme k němu ještě časové razítko. Tím stvrdíme to, že elektronický podpis na dokumentu již existoval v okamžiku, uvedeném na časovém razítku, a tudíž musel vzniknout někdy dříve.

Zdůrazněme si, že časové razítko neříká, jak dlouho již existuje to, co je časovým razítkem právě opatřováno. Pro „správný efekt“ časového razítka je také nutné respektovat správné pořadí: má-li časové razítko stvrzovat existenci elektronického podpisu v čase, musí být k dokumentu připojeno až po elektronickém podpisu. Nikoli obráceně. [5]

6.1.9 Elektronická značka

Všechny výše uvedené druhy elektronických podpisů měli společnou jednu zásadní vlastnost – elektronický podpis může vlastnit pouze fyzická osoba. Elektronická značka je obdobou elektronického podpisu, ovšem s tím rozdílem, že je vázána na technický prostředek, nikoliv na fyzickou osobu. Z toho pak vyplývá i možnost že elektronickou značku může vlastnit osoba právnická.

Elektronické značky se používají hlavně tam, kde elektronický podpis vytváří nějaký stroj nebo software bez přímé účasti člověka. Například u různých výstupů z informačních systémů, které jsou generovány zcela automaticky a v takovém počtu, že by zde přímé zapojení člověka nepřipadalo v úvahu. [5]

6.2 Certifikační autority

Obecně řečeno, certifikační autorita je subjekt, který vydává digitální certifikáty a potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. na základě principu přenosu důvěry tak můžeme důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že důvěřujeme samotné certifikační autoritě.

Ve vyhlášce Úřadu pro ochranu osobních údajů č. 366/2001 Sb., o upřesnění podmínek § 6 Zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů a § 17, který definuje prostředky pro vytváření a ověřování zaručených elektronických podpisů jsou definovány povinnosti certifikačních autorit, které vytvářejí zaručené elektronické podpisy založené na kvalifikovaném certifikátu. Podle této vyhlášky certifikační autority zpracovávají osobní údaje uživatelů za účelem poskytování služeb, ochrany zájmů uživatele, předávání osobních údajů třetím stranám, pokud je to nezbytně nutné pro poskytování služeb, a v případě poskytnutí souhlasu uživatele za marketingovými účely poskytovatele. Osobní data jsou zabezpečována na nejvyšší možné úrovni. Certifikační autorita se při zpracování dat řídí zákonem č. 101/2000 Sb., o ochraně osobních údajů. Údaje o certifikační autoritě, která je vydavatelem elektronického podpisu jsou obsaženy přímo v elektronickém certifikátu.

6.2.1 Akreditovaná certifikační autorita

Certifikační autority, které vydávají zaručené elektronické podpisy založené na kvalifikovaném certifikátu podléhají schvalování Ministerstva vnitra České republiky, (dříve Ministerstva informatiky České republiky), tzv, akreditaci a jejich seznam je zveřejněn na webu MVČR. (http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx).

Akreditovaná certifikační autorita vydává zpoplatněné kvalifikované certifikáty, což jsou standardní digitální certifikáty, které však jsou výše zmíněným zákonem uznávány v rámci komunikace se státními institucemi České republiky.

V současné době mají akreditaci vydanou jen tři certifikační autority.

6.2.1.1 První certifikační autorita, a. s.

První certifikační autorita, a.s. (I.CA), je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice a na Slovensku. Hlavní náplní společnosti je zajišťování činností bezprostředně souvisejících s poskytováním služeb certifikační autority a časové autority.

Tato certifikační autorita působí v české republice již od 15.3.2002 a v současnosti disponuje 20. Registračními místy v různých částech České republiky.

I.CA získala jako první v České republice osvědčení pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. V roce 2006 získala akreditaci také pro vydávání kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Rovněž v roce 2006 získala společnost akreditaci pro vydávání kvalifikovaných certifikátů a pro poskytování služby časové autority na Slovensku.

6.2.1.2 Česká pošta, s. p.

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb dne 3.8.2005 na základě akreditace udělené Ministerstvem informatiky ČR. Certifikační autorita Postsignum poskytuje služby vydávání kvalifikovaných, komerčních certifikátů a poskytování kvalifikovaného časového razítka.

Služby certifikační autority Postsignum lze využít na každé poště v celé České republice

6.2.1.3 eIdentity a. s.,

Společnost eIdentity a.s. získala akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb v září 2005.

Společnost nabízí služby, které jsou založeny na vysokém stupni důvěry všech účastníků, a proto jsou realizovány jen v kvalitně připraveném a provozovaném prostředí. Společnost eIdentity a.s. chce aktivně napomáhat rozvoji využívání

moderních bezpečnostních technologií v oblasti prolínání elektronického i našeho lidského světa.

Společnost eIdentity disponuje pouze čtyřmi kontaktními místy v Hlavním městě Praze.

7 Zaručený elektronický podpis a jeho význam

V případě podpisu na papírovém dokumentu jsou už z povahy tohoto aktu zřejmé jisté atributy. Jsou to především tyto: osoba, která podepisuje, musí být přítomna, předpokládá se, že se s podepisovaným dokumentem seznámila a že s ním souhlasí. Tyto atributy jsou pro ostatní zúčastněné strany jistou zárukou pro splnění závazků vyplývajících z obsahu dokumentu. Z tohoto důvodu se dokumenty podepisují ve více kopiích, a případně se ještě opatřují ověřovací doložkou.

Elektronický podpis by měl všechny tyto atributy nahradit na dokumentu elektronickém.

7.1 Požadované vlastnosti zaručeného elektronického podpisu

Zaručený elektronický podpis pro to, aby zaručil výše uvedené atributy musí poskytovat podle Peterky tyto záruky: - **Integrita dokumentu**. Tedy jeho neporušenost, ve smyslu celistvosti, neměnnosti.

Zaručený elektronický podpis nám také pomáhá identifikovat „toho, komu podpis patří“. Tedy tzv. podepsanou či podepisující osobu, jak říkají zákony a vyhlášky. Poskytne nám určité údaje o identitě této osoby (například její jméno a příjmení), obecně se tomu říká **identifikace.** Tak nastupuje ještě **autentizace**, neboli ověření identity, resp. odpověď na otázku: „jsem skutečně tím, za koho se vydávám?“ V nejjednodušším případě může být autentizace provedena zadáním (správného) hesla. Sofistikovanější metody autentizace pak mohou využívat i techniky elektronického podpisu. Zaručený elektronický podpis slouží i k poskytování důležité záruky, které se říká **nepopiratelnost** (někdy též: **neodmítnutelnost**): podepsaná osoba nemůže popřít,

že podpis vytvořila ona (resp. Nemůže odmítnout důsledky svého podpisu). To ovšem jen za podmínky, že tento zaručený elektronický podpis je dostatečně „kvalitní“, v tom smyslu, že se můžeme spolehnout na to, co nám říká ohledně identity podepsané osoby.[5]

K těmto zárukám, které podpis zaručený elektronický podpis poskytuje se muže ještě v některých případech přidat požadavek na utajení zprávy. Jde konkrétně o zajištění tzv. **důvěrnosti** (anglicky: privacy). Tím se rozumí zajištění toho, aby se s daným obsahem (v našem případě s obsahem dokumentu) nemohl seznámit nikdo nepovolaný. Zdůrazněme si, že požadavek na zajištění důvěrnosti neznamená, že se předmětný obsah nesmí dostat do rukou někoho nepovolaného. To by byl podstatně silnější požadavek, který by se v běžné praxi – například v prostředí dnešního Internetu – dal realizovat jen velmi obtížně. Proto se u důvěrnosti netrvá na tom, aby se předmětný obsah nemohl dostat do nepovolaných rukou - ale trvá se na tom, aby v takovém případě to oněm „nepovolaným rukám“ bylo k ničemu a nemohly se seznámit s tím, co má zůstat důvěrné. V praxi se důvěrnosti dosahuje vhodným zašifrováním příslušného obsahu. Jde o „něco jiného“ než je elektronický podpis: ten důvěrnost nezajišťuje. [5]

8 Využití certifikátů ve veřejné správě

Využití certifikátů ve veřejné správě je v dnešní době již v mnoha oblastech. Tou nejvíce viditelnou a diskutovanou je komunikace mezi veřejnou správou a občanem. Dále je to autentifikace úředníků k různým službám, autentifikace aplikací při komunikaci mezi sebou, podepisování elektronických dokumentů při konverzi listinných dokumentů do elektronické podoby, komunikace právnických osob pomocí Informačního systému datových schránek, šifrování komunikace, archivace elektronických dat a další.

8.1 Všeobecné použití podle typu certifikátu

K různým účelům jsou určeny příslušné typy certifikátů a elektronických podpisů. Toto použití je podrobně popsáno v tzv. certifikačních politikách, které pro každý typ certifikátu vydávají příslušné certifikační autority.

8.1.1 Komerční serverové certifikáty

Tyto certifikáty jsou elektronickou značkou a autentizují se jimi jednotlivé servery, respektive programy na nich běžící vůči jiným obdobným službám. Tato autentifikace probíhá převážně pomocí SSL (Secure Sockets Layer) a v rámci této elektronické komunikace dochází i k jejímu šifrování. Pro uživatele je tato část komunikace neviditelná, probíhá na pozadí a uživatel ji nemůže ovlivnit.

8.1.2 Komerční osobní certifikáty

Tato skupina certifikátů je určena pro šifrování datových zpráv a pro autentizaci uživatele a ověření elektronického podpisu

8.1.3 Komerční šifrovací certifikáty

Tyto certifikáty lze použít pouze pro šifrování dat [10]

8.1.4 Kvalifikované osobní certifikáty

Slouží pro ověření elektronického podpisu podepisující osoby v souladu se zákonem o elektronickém podpisu. [10]

8.1.5 Kvalifikované systémové certifikáty

Mohou být použity pouze pro ověření elektronické značky označující osoby v souladu se zákonem o elektronickém podpisu. [10]

8.1.6 Časová razítka

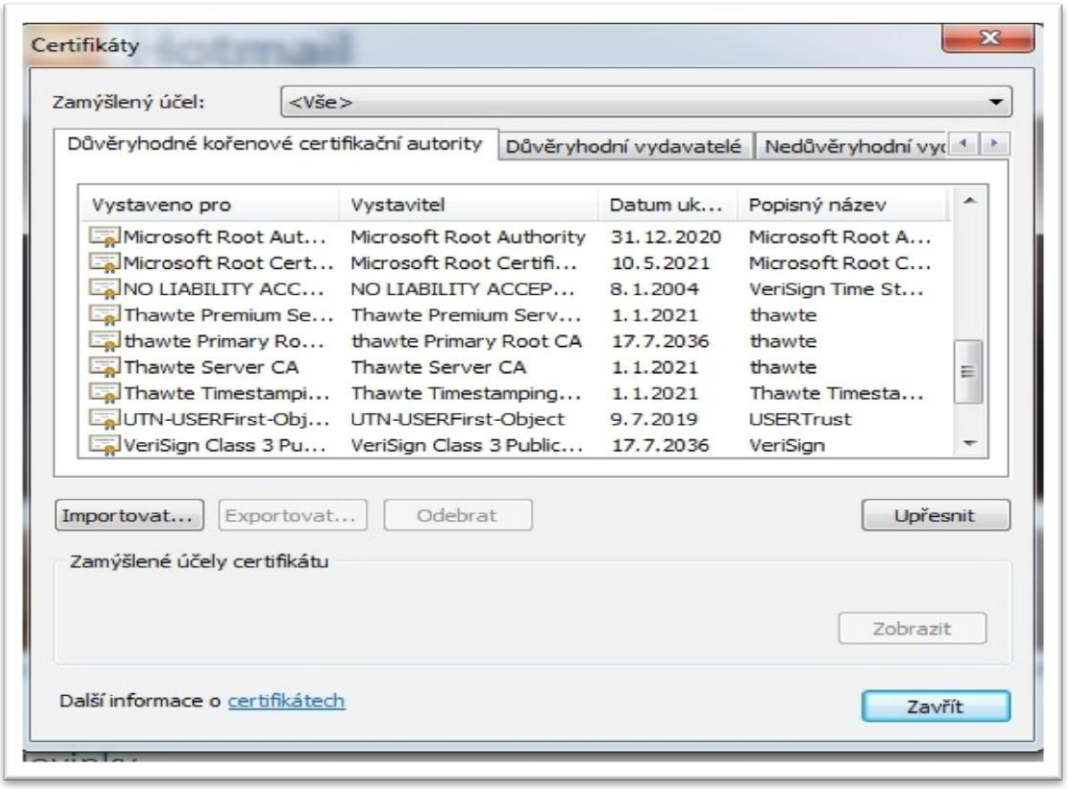
Toto elektronické označení, které připojujeme k elektronickému dokumentu, důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala v daný časový okamžik. Časové razítko důvěryhodným způsobem "razítkuje" elektronický dokument v daném čase a je tedy vhodným doplňkem k elektronickému podpisu.

S pomocí časových razítek lze u elektronických transakcí, formulářů, archivovaných dat, elektronických podpisů apod. prokázat jejich existenci v určitém čase. Časové razítko potvrzuje, že označená data existovala před uvedeným časovým okamžikem. [10]

8.1.7 Kořenové certifikáty certifikačních autorit

Kořenový certifikát certifikační autority je ve své podstatě také elektronický podpis, a každý uživatel si jeho nahráním do svého operačního systému může určit, zda

certifikační autoritě uvedené v kořenovém certifikátu důvěřuje, nebo ne.



Obrázek 9 - Úložiště kořenových certifikátů v systému MS W7

8.2 Ověření platnosti certifikátu

Přítomnost výše zmíněných kořenových certifikátů certifikačních autorit v systému má však ještě další účel, a to ověření zda v daný okamžik je elektronický podpis, respektive jeho certifikát platný nebo zda nebyl revokován. Toto ověření provede aplikace porovnáním proti takzvanému CRL listu.

9 Legislativní zakotvení použití elektronického podpisu ve veřejné správě

9.1 Podání podle zákona č. 500/2004 Sb., Správní řád

Podání je možno učinit písemně nebo ústně do protokolu anebo v elektronické podobě podepsané zaručeným elektronickým podpisem. Za podmínky, že podání je do 5 dnů potvrzeno, popřípadě doplněno způsobem uvedeným ve větě první, je možno je učinit pomocí jiných technických prostředků, zejména prostřednictvím dálnopisu, telefaxu nebo veřejné datové sítě bez použití zaručeného elektronického podpisu. Ten, kdo činí podání v elektronické podobě, uvede současně poskytovatele certifikačních služeb, který jeho certifikát vydal a vede jeho evidenci, nebo certifikát připojí k podání. [9]

V případě, že správní orgán nedisponuje prostředky, které by mu umožňovaly příjem podání opatřených elektronickým podpisem tak je povinen uzavřít veřejnoprávní smlouvu na poskytování této služby, například obec s obcí s rozšířenou působností.

9.2 Stížnosti podle zákona č. 500/2004 Sb., Správní řád

Stížnost je ve své podstatě také podáním a při jejím podání se postupuje zcela analogicky jako v předchozím případě.

9.3 Žádost o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

V případě žádosti o poskytnutí informací, zákon nespecifikuje požadavky na její náležitosti. Z toho vyplývá, že tato žádost nemusí být elektronicky podepsána. Ovšem v zákoně je uvedeno, že musí být doručena na podatelnu úřadu, z čehož vyplývá, že její elektronická forma musí být adresována na elektronickou podatelnu úřadu.

9.4 Běžná komunikace občan – obecní úřad

V případě, že nejde o podání a stížnost ve smyslu zákona č. 500/2004 Sb., Správní řád tak jde jen o běžnou komunikaci a u té není žádným předpisem nařízena náležitost elektronického podepisování.

10 Využívání kvalifikovaných elektronických podpisů v reálných situacích na MÚ Rakovník

10.1 Tvorba Kvalifikovaného elektronického podpisu

Zaměstnanci městského úřadu, kterým zákony nebo povaha práce nařizuje použití kvalifikovaných podpisů, mají podle vnitřních předpisů města povinnost mít kvalifikovaný elektronický podpis a také o něj odpovídajícím způsobem pečovat. Jedná se hlavně o bezpečnostní zásady při vyzrazení soukromého klíče, ale také o povinnost vytváření, zálohování a obnovy kvalifikovaných elektronických podpisů. Oddělení ICT poskytuje při práci s elektronickými podpisy a s certifikáty pouze metodickou pomoc. Toto opatření je vytvořeno hlavně proto, že veškeré údaje o kvalifikovaném elektronickém podpisu smí znát jen jeho majitel a nikdo jiný.

10.1.1 Cerifikační autorita

Městský úřad Rakovník má uzavřenou smlouvu o poskytování služeb certifikační autority s Českou poštou, respektive s Certifikační autoritou České pošty - Postsignum. Tato certifikační autorita byla vybrána hlavně z důvodu dostupnosti kontaktního místa na místní poště.

Ke komunikaci s certifikační autoritou je určena oprávněná osoba, pracovník ICT oddělení, která současně vede seznamy vydaných elektronických podpisů.

10.1.2 Vytváření kvalifikovaného elektronického podpisu

Na žádost vedoucího pracovníka se pracovník, který má mít elektronický podpis, zavede do tzv. seznamu oprávněných žadatelů o certifikát, který je veden u certifikační autority. Jedná se o seznam pracovníků, kteří na základě smlouvy mohou mít kvalifikovaný osobní podpis s identifikátorem městského úřadu. Tento zápis provede

oprávněná osoba buď písemnou formou na stanoveném formuláři, nebo elektronicky na zabezpečeném portálu certifikační autority.

Pracovník si po oznámení, že je zaveden v seznamu oprávněných žadatelů o certifikát na stránce https://www.postsignum.cz/online_generovani_zadosti.html vygeneruje pár certifikátů a žádost o vystavení kvalifikovaného elektronického podpisu. Soukromý klíč k elektronickému podpisu se uloží v počítači, na kterém generování probíhá a veřejný klíč zůstane na serveru. Po tomto kroku přijdou na emailovou adresu uvedenou při vytváření instrukce k ověření totožnosti žadatele o kvalifikovaný certifikát.

Obrázek 10 - Generování žádosti o certifikát

V těchto instrukcích je uvedeno číslo žádosti, se kterým se pracovník musí dostavit na kontaktní místo certifikační autority. Pracovník certifikační autority

na kontaktním místě, na základě čísla žádosti o kvalifikovaný certifikát, provede ověření identity žadatele a překontroluje správnost uvedených údajů. Tento krok je základním kamenem pro stanovení důvěry v certifikační autoritu, a nelze jej nijak obejít.

V dalším kroku opět přijde pracovníkovi emailová zpráva, ve které je odkaz na stažení veřejného klíče ke kvalifikovanému podpisu a ke stažení protokolů o vytvoření kvalifikovaného elektronického podpisu. Po stažení veřejného klíče kvalifikovaného elektronického podpisu jej pracovník spojí s v úložišti uloženým soukromým klíčem, čímž dojde k vytvoření kompletního elektronického podpisu.

10.2 Práce s dokumenty ve spisové službě

Městský úřad pro zpracování dokumentů používá spisovou službu Ginis, jejímž výrobcem je firma Gordic. Jedná se o databázový produkt nad databází ORACLE. Každý pracovník úřadu má ve svém počítači nainstalovanou aplikační část spisové služby, která mu umožňuje práci s dokumenty, které mu přísluší nebo které mu jsou postoupeny k vyřízení.

Struktura spisové služby se skládá z elektronické podatelny a z tzv. spisových uzlů. Jednotlivé spisové uzly obsluhují pověření pracovníci. Aplikační část spisové služby jednotlivých pracovníků úřadu je vždy součástí jednoho nebo více z těchto spisových uzlů. Toto propojení je dáno zařazením jednotlivých pracovníků ve struktuře úřadu. Jednotlivé spisové uzly odpovídají víceméně členění úřadu na jednotlivé odbory. Součástí je i modul spisovna a archiv, kam jsou předávány dokumenty k založení a k archivaci.

Vstupním bodem spisové služby pro komunikaci s veřejností je elektronická podatelna. Práce s veškerými dokumenty se řídí Spisovým a skartačním řádem úřadu, který vychází ze zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně

některých zákonů a z vyhlášky č. 646/2004 Sb., o podrobnostech výkonu spisové služby.

Všechny dokumenty, které jsou přijaty úřadem, musí být zaevidovány podatelnou úřadu a teprve poté jsou postoupeny jednotlivým pracovníkům k vyřízení.

Všechna korespondence pracovníků úřadu s veřejností a s ostatními úřady je opět vedena přes podatelnu.

Jedná se o dokumenty v papírové podobě, které jsou pouze evidovány spisovou službou, a případně mohou být do elektronické podoby převedeny a dokumenty v elektronické podobě, které jsou vedeny ve spisové službě v elektronické formě.

Instrukce k podáním pro občany jsou uvedeny na webové prezentaci města na webové adrese http://www.mesto-rakovnik.cz/servis-pro-obcany/e-podatelna/

10.2.1 Příjem podání podatelnou

Občan zašle na adresu úřadu dopis, nebo donese podání osobně na podatelnu, a tam pracovnice toto podání zaeviduje do spisové služby a postoupí jej na příslušný spisový uzel. Papírové podání je postoupeno tamtéž.

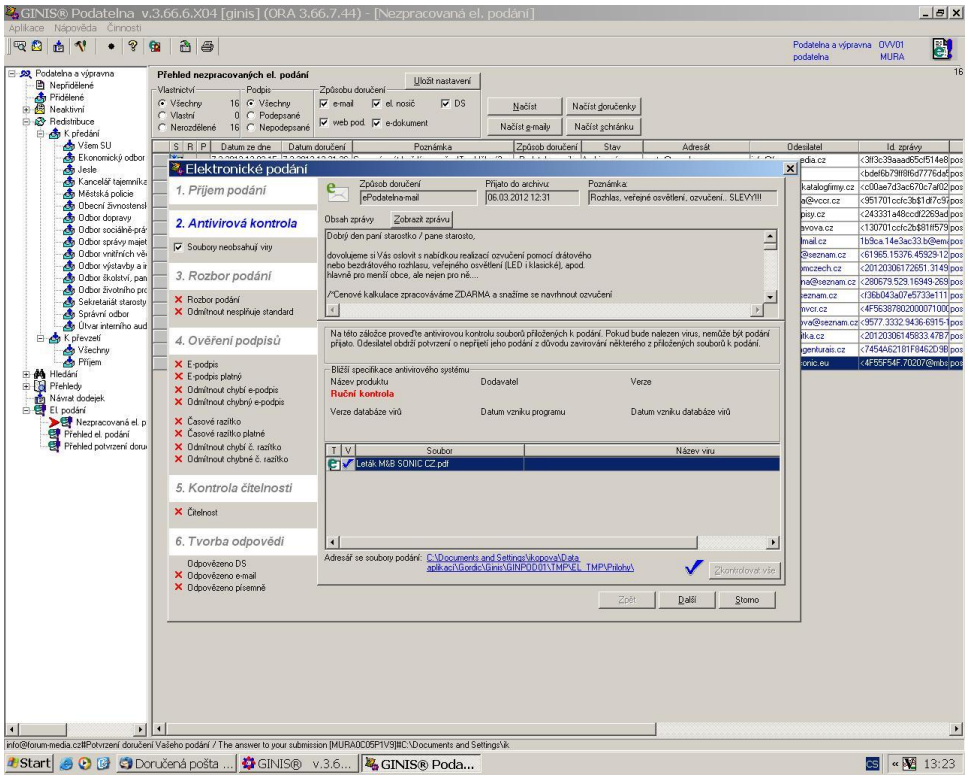
Modul spisové služby elektronická podatelna Ginis umožňuje nejen příjem podání v papírové podobě, ale i elektronicky.

10.2.2 Příjem elektronicky podepsané zprávy elektronickou podatelnou

Elektronická podatelna Ginis je schopna přijmout datové zprávy z různých zdrojů. Hlavně jsou to: emailová komunikace, datové zprávy z ISDS, datové nosiče a je možno i provést převedení papírového dokumentu do elektronické podoby pomocí autorizované konverze.

10.2.2.1 Příjem emailové zprávy

V případě, že na elektronickou adresu úřadu dorazí emailová zpráva, tak je tato zpráva přijata elektronickou podatelnou k vyhodnocení zda se jedná o elektronické podání či nikoliv. Toto vyhodnocení provádí pracovnice podatelny ve spolupráci s modulem spisové služby Elektronická podatelna Ginis.



Obrázek 11 - Vyhodnocení emailové zprávy ePodatelnou

Kontroluje se, zda zpráva obsahuje všechny náležitosti podání ve smyslu zákona č. 500/2004 Sb., Správní řád, dále se kontroluje, zda datová zpráva neobsahuje viry. Tato kontrola probíhá v aplikačním rozhraní ePodatelna Ginis. Tento software vyhodnotí přítomnost elektronického podpisu v datové zprávě, zkontroluje jeho platnost, a zda nebyl odvolán oproti aktuálnímu CRL seznamu, který je denně stahován od všech akreditovaných certifikačních autorit. Obsluha podatelny na základě informací o datové zprávě provede hodnocení. Pokud zpráva splní náležitosti podání, tak je zaevidována do spisové služby a zpráva je předána pracovnicí podatelny na příslušný spisový uzel k dalšímu zpracování. V případě že zpráva některou z podmínek nesplní,

tak je s ní nakládáno jako s obyčejným emailem a je předána na email vedoucímu příslušného odboru k vyřízení. Jsou-li k takové datové zprávě doplněny náležitosti podání do 5-ti dnů, tak se s ní dále nakládá jako s podáním dle Správního řádu.

O tom jakým způsobem bylo s datovou zprávou naloženo je její odesílatel automaticky informován přednastavenou zprávou. Vzory informačních zpráv odesílaných z ePodatelny je možno najít na www.mesto-rakovnik.cz

10.2.2.2 Příjem zprávy pomocí ISDS

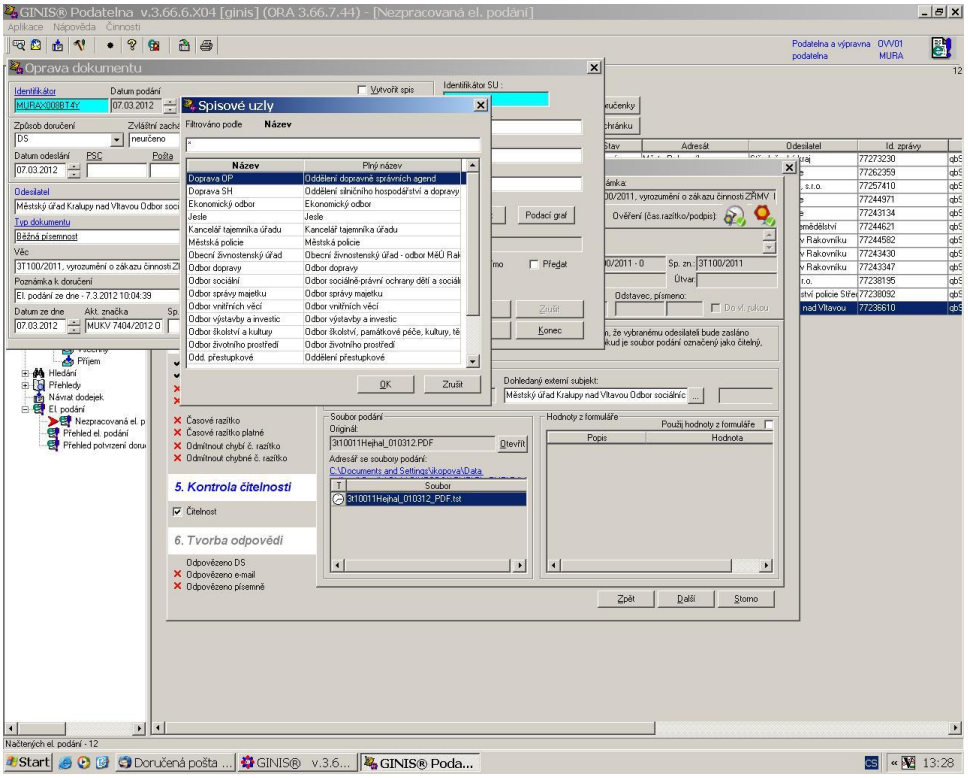
Modul spisové služby Elektronická podatelna Ginis dokáže automaticky uskutečnit přijetí datových zpráv ze systému ISDS. Spisová služba disponuje rozhraním pro připojení k systému ISDS. Zprávy jsou při přijetí automaticky přijaty. Vzhledem k povaze datových zpráv přenášených pomocí ISDS jsou tyto vždy považovány za podání ve smyslu zákona č. 500/2004 Sb., Správní řád. Po přijetí datové zprávy do elektronické podatelny je této zprávě přiděleno spisové evidenční číslo a zpráva je předána pracovnicí podatelny na příslušný spisový uzel k dalšímu zpracování.

Příjem zpráv je po technické stránce zajištěn automatizovaným připojením k rozhraní systému ISDS pomocí autentifikace elektronickým podpisem. V internetovém rozhraní ISDS je možnost zadat otisk certifikátu elektronického podpisu, který bude pro autentifikaci použit, a v administraci spisové služby je možno tento elektronický podpis načíst do systému Ginis, který jej pak používá pro autentizaci vůči ISDS.

10.2.2.3 Příjem podání na nosiči dat

Další možností jak učinit podání vůči úřadu je donést datovou zprávu nahranou na nosiči dat přímo do podatelny úřadu. Pracovnice podatelny ověří, zda takto doručená datová zpráva obsahuje všechny náležitosti a zda obsahuje platný zaručený elektronický

podpis, poté ji zaeviduje do spisové služby úřadu a zpráva je předána na příslušný spisový uzel k dalšímu zpracování.

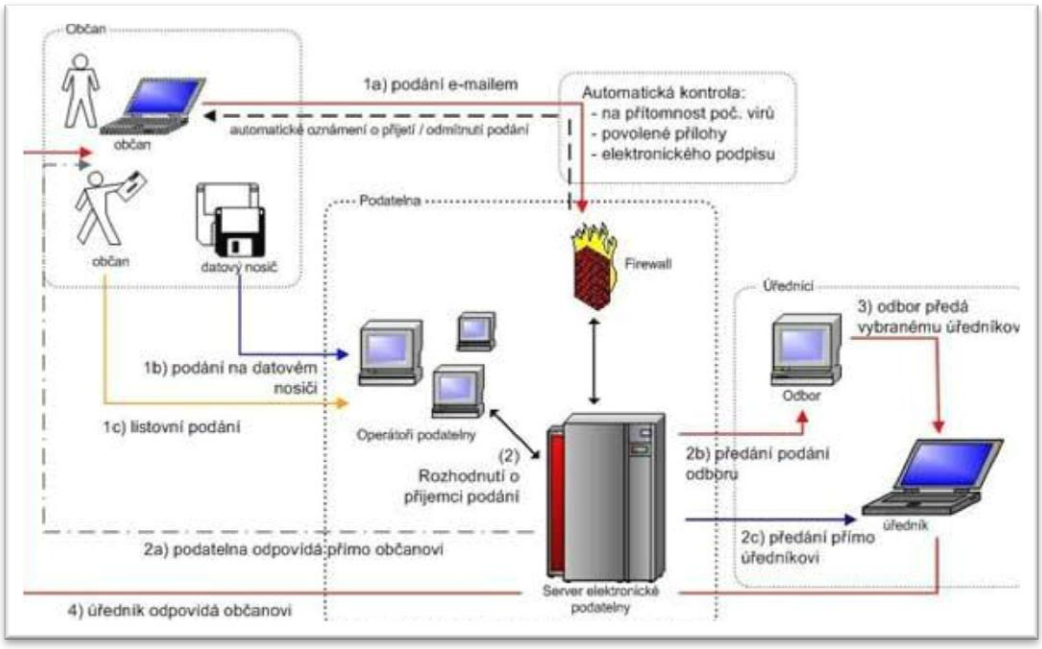


Obrázek 12 - Předání zprávy na příslušný spisový uzel

10.2.3 Odesílání zpráv elektronickou podatelnou

Jestliže pracovníci úřadu potřebují zaslat jakoukoliv informaci občanovi nebo jinému úřadu, tak to provádějí pomocí spisové služby. V aplikační části spisové služby úřadu vytvoří zprávu, opatří jí adresou nebo identifikátorem Datové schránky, do které má být doručena a podle jejího charakteru jí buď vytisknou, nebo opatří elektronickým podpisem. Takto vytvořená zpráva se v systému spisové služby odešle k vypravení na podatelnu úřadu. V případě že jde o písemnost, tak se s elektronickou verzí dodá na podatelnu i příslušný dopis.

Pracovnice podatelny zkontroluje u odesílaných zpráv veškeré náležitosti a poté je předá k doručení systému ISDS a nebo, příslušně ofrankované, České poště.



Obrázek 13 - Všeobecné schéma elektronické podatelny (zdroj: www.cvis.cz)

10.3 Podepsání dokumentu a archivace dokumentů

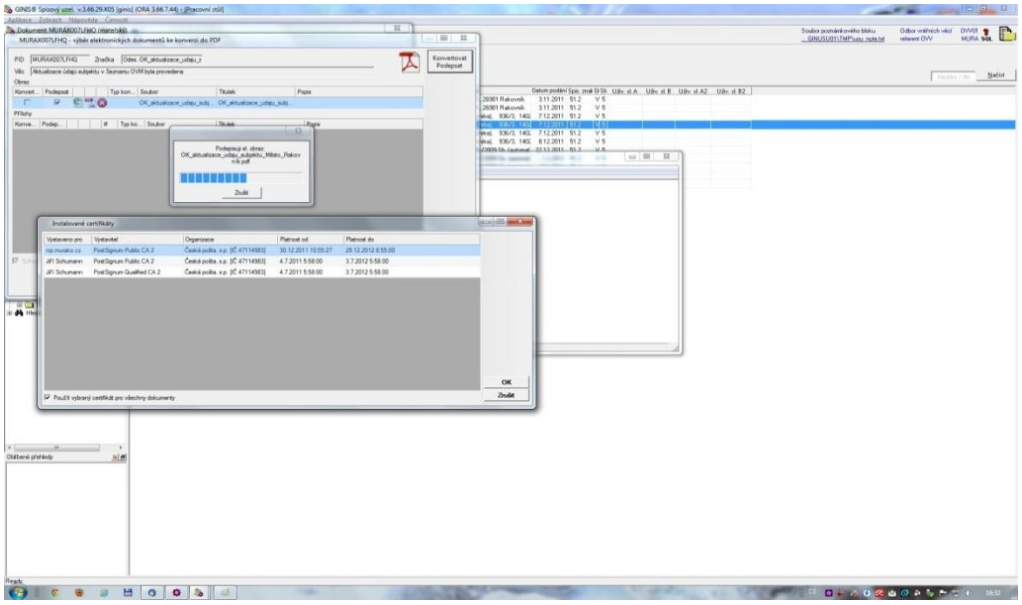
Dokument, aby splnil náležitosti podání podle Správního řádu, musí obsahovat elektronický podpis. To lze učinit dvěma způsoby. První, kdy k dokumentu připojíme elektronický podpis jako druhý soubor i s údaji které je logicky spojí, se téměř nepoužívá. Druhým způsobem je, že příslušné aplikační vybavení je schopno elektronický podpis začlenit přímo do dokumentu a také poté při novém otevření tohoto podepsaného dokumentu dokáže ověřit platnost tohoto podpisu.

Ve veřejné správě se stal standardem pro elektronicky podepsané dokumenty formát PDF a PDF/A a další odvozené. Jedná se o formáty, které vynalezla firma Adobe a které splňují náročné požadavky norem ISO pro vytváření, ukládání a archivaci (PDF/A) dokumentů. Tyto formáty jsou proto nejvíce preferovány, a v případě archivování elektronických dokumentů je formát PDF/A v současnosti asi jediný, který je používán ve větší míře.

Z výše uvedených důvodů jsou na Městském úřadu v Rakovníku všechny dokumenty, které jsou podepisovány zaručeným elektronickým podpisem, konvertovány před vlastním podpisem do formátu PDF/A. Tuto konverzi zajišťuje spisová služba Ginis. V případě, že by šlo o archivaci dokumentů do elektronického archivu, tak je třeba dokumenty v době platnosti kvalifikovaného elektronického podpisu označit kvalifikovaným časovým razítkem, a v době platnosti tohoto razítka provést přeznačení dalším časovým razítkem. Tento postup je třeba opakovat po celou dobu, po kterou je třeba elektronický dokument archivovat. O tento postup se postará zcela automaticky modul spisové služby eArchiv na základě připojeného skartačního znaku, který ve spisové službě dokumentu přidělí pracovník, který je vlastníkem dokumentu.

10.3.1 Spisová služba Ginis

V případě, že je zapotřebí elektronicky podepsat dokument, tak úředník, který jej podepisuje, tuto činnost provede v aplikačním rozhraní spisové služby. Dokument, který je v počítači úředníka, je vložen do spisové služby, do již existujícího elektronického spisu nebo je veden ve spisové službě jen jako dokument. Vždy je mu přidělen identifikační údaj. Existuje také možnost vytvořit dokument přímo ve spisové službě z šablony. Při podpisu dokumentu je provedena konverze dokumentu do formát PDF/A a poté je vyvolán dialog, ve kterém je možné vybrat příslušný elektronický podpis, viz obrázek 12. Podepsání dokumentu provede aplikační software na pozadí a podepsaný dokument uloží do úložiště dokumentů k dalšímu použití, případně je předán do spisovny k archivaci



Obrázek 14 – Konverze dokumentu a aplikace elektronického podpisu ve spisové službě Ginis

.

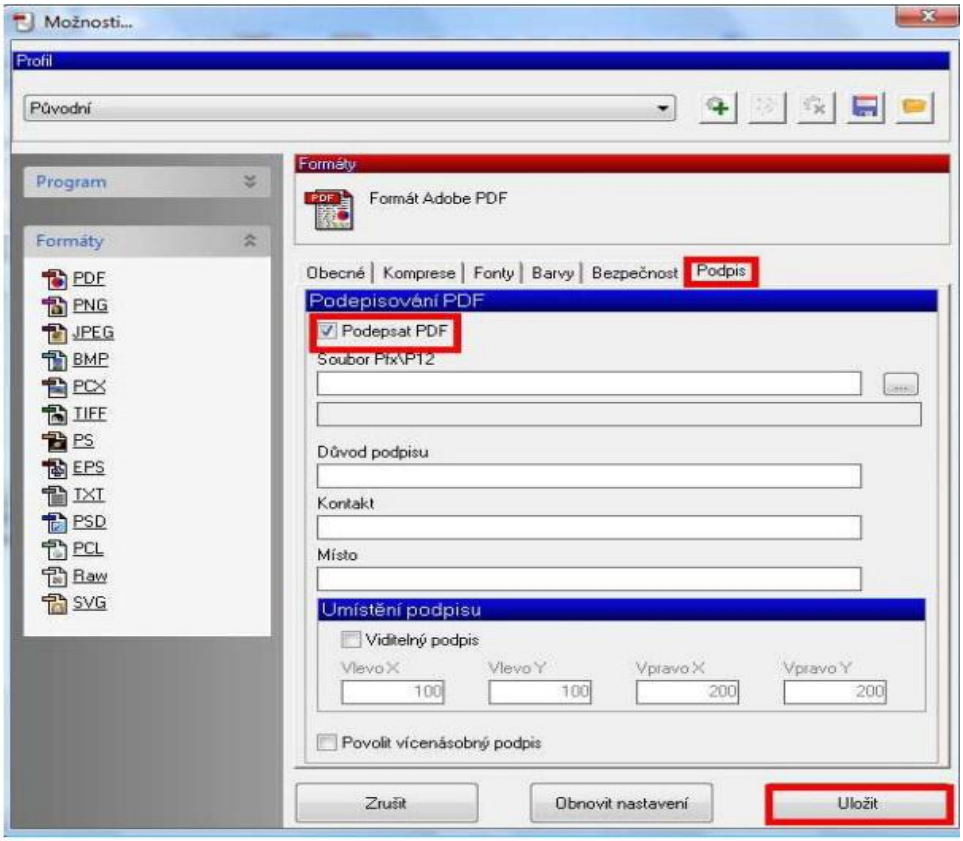
10.3.2 MS office 2010

Kancelářský balík firmy Microsoft pro práci s dokumenty Office 2010, který je standardně užíván pracovníky úřadu pro práci s dokumenty umožňuje připojit elektronický podpis k dokumentu a kontrolovat jeho platnost a neporušenost dokumentu. je v něm možno i uložit dokument po dokončení jako PDF/A. Bohužel není možné uložit dokument jako PDF/A a takovýto dokument i elektronicky podepsat. Z tohoto důvodu, se software MS Office používá pouze pro editaci dokumentů a konverzi a podpis zajišťuje spisová služba.

10.3.3 PDF creator

V případě, že je zapotřebí provést podpis dokumentu, který je umístěn mimo spisovou službu, tak k tomu slouží software PDF creator. Tento software je autorem šířen jako bezplatný, a je možné ho použít pro převod mnoha formátů souborů do formátu PDF. Současně s převodem umožňuje i připojení elektronického podpisu k dokumentu. Software se pro uživatele chová jako virtuální tiskárna, která pomocí

funkce tisk uloží pdf soubor do předem definovaného umístění. V nastavení virtuální tiskárny je možno nastavit i připojení elektronického podpisu ze souboru ve formátu pfx a nebo p12 (jedná se o formáty v kterých se ukládají elektronické podpisy do souboru).



Obrázek 15 - Vložení elektronického podpisu v PDF creatoru

Pdf Creator je používán i jako software který zajišťuje konverzi a podepisování souborů pro jiné aplikace na pozadí, aniž by o tom uživatel věděl.

10.4 Emailová komunikace

Při emailové komunikaci se úředníky používá elektronický podpis dvěma způsoby. Jestliže je zapotřebí předat dokument, který má jistou důležitost, která je reprezentována připojeným kvalifikovaným elektronickým podpisem, pak je takovýto

dokument připojen k emailové zprávě jako příloha, a sama zpráva pak již není podepsána. Druhou využívanou možností je podpis vlastní emailové zprávy. Tato možnost je využívána v případě, že je zapotřebí, aby byl autor zprávy jednoznačně identifikován příjemcem.

10.5 Autentizace uživatele v systémech veřejné správy

Další využití kvalifikovaných elektronických podpisů je v oblasti autentifikace uživatelů v různých systémech veřejné zprávy. Ministerstvo pro místní rozvoj provozuje rejstřík živnostenských podnikatelů, do kterého přistupují pracovníci Živnostenského úřadu. Autentifikace jednotlivých pracovníků je zajištěna pomocí ověření kvalifikovaným certifikátem umístěným na čipové kartě a jištěna použitím PINu. Bohužel, zde se často stává, že pracovníci jsou odvoláni od pracovní stanice, a od aplikace se neodhlásí a čipovou kartu ponechají ve čtečce. Zde by byla na místě cílená osvěta z kompetentních míst. Viz závěr této práce.

Pracovníci, kteří obsluhují pracoviště Czechpointu používají k autentizaci k systému kvalifikovaný komerční certifikát. Na základě autentifikace pomocí tohoto certifikátu mohou provádět výdej dokumentů ze systému a autorizovanou konverzi dokumentů. Správnost dokumentů je po jejich kontrole pracovníkem stvrzena tak, že pracovník k nim připojí svůj osobní kvalifikovaný elektronický podpis. Podrobně je práce na pracovišti Czechpoint popsána v následující kapitole.

Autentifikaci pomocí kvalifikovaného systémového certifikátu probíhá i mezi jednotlivými systémy, které jsou na Městském úřadu používány a to jak při komunikaci mezi sebou, tak při komunikaci se systémy provozovanými externě. Jedná se například o komunikaci spisové služby s Integrovaným Systémem Datových Schránek a předávání údajů systému Registru živnostenského podnikání do spisové služby Ministerstva pro místní rozvoj. Tyto procesy probíhají na pozadí činnosti uživatelů systému, na základě přednastavených parametrů ve vzájemně komunikujících

aplikacích. Potvrzování těchto transakcí se neprovádí, vzájemná důvěra komunikujících systémů je deklarována ověřením kvalifikovaných systémových certifikátů obou stran.

10.6 Autorizovaná konverze dokumentů a Czechpoint

Konverze dokumentu je podle zákona č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky, nebo úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky. Dokument, který provedením konverze vznikl, má stejné právní účinky jako originál nebo ověřená kopie dokumentu, jehož převedením výstup vznikl.

Zaručenou konverzi dokumentů na žádost provádí dle zákona č.300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, kontaktní místa veřejné správy uvedená v Zákoně č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. Jedná se především o pracoviště Czech Point.

Ještě existuje takzvaná konverze z moci úřední. Tu provádějí orgány veřejné moci pouze pro výkon své působnosti a není zpoplatněna

Při konverzi z dokumentu v elektronické podobě do dokumentu v listinné podobě subjekt provádějící konverzi ověří platnost všech certifikátů a časových značek, které jsou k elektronickému dokumentu připojeny a současně ověří, zda nebyly před okamžikem uvedeným v kvalifikovaném časovém razítku zneplatněny. V případě splnění všech zákonných náležitostí provede vlastní konverzi. Součástí konverze je kontrola obsahové shody dokumentů. O celém procesu se vydá takzvaná ověřovací doložka. Ověřovací doložka obsahuje všechny údaje o původním elektronickém dokumentu.

Při konverzi z dokumentu v listinné podobě do dokumentu v elektronické podobě subjekt provádějící konverzi postupuje tak, že na technickém zařízení provede převod

dokumentu do elektronické podoby a zkontroluje obsahovou shodu obou dokumentů. Ke vzniklému elektronickému dokumentu následně připojí svou uznávanou elektronickou značkou nebo uznávaný elektronický podpis osoby, která konverzi provedla, a zajistí, aby byl výstup opatřen kvalifikovaným časovým razítkem. O proběhlém procesu se vydá ověřovací doložka, která je k elektronickému dokumentu neoddělitelně připojena. Ověřovací doložka obsahuje všechny údaje o původním listinném dokumentu. Subjektům provádějícím konverzi je zákonem nařízeno o všech provedených konverzích vést evidenci. [11]

10.7 Přehled vydaných certifikátů pro MěÚ Rakovník v letech 2008 – 2012

Z níže uvedené tabulky je patrné, že hlavním impulzem pro používání osobních kvalifikovaných certifikátů úředníky Městského úřadu bylo zprovoznění Informačního Systému Datových Schránek v roce 2009. Do té doby byly zprávy odesílané podepisovány pouze pracovnicemi podatelny a komerčním certifikátem elektronické podatelny firmy AEC, která byla v té době na MěÚ v provozu. Tato epodatelna byla nahrazena s nákupem spisové služby epodatelnou firmy Ginis, která je popsána výše. Vypovídací hodnota této tabulky je bohužel nízká, protože certifikační autorita začala tyto údaje shromažďovat až na konci roku 2008. Situace od roku 2005 do roku 2008 je součástí autorovy Bakalářské práce Elektronický podpis a jeho využití ve veřejné správě © 2010 ČZU v Praze.

Výpis certifikátů | Městský úřad Rakovník				
Rok	**Vydávající autorita**	**Typ certifikátu**	**Druh certifikátu**	**Počet**
2008	PostSignum Public CA	Systémový	Šifrovací certifikáty	**1**
	PostSignum Public CA	Systémový	Komerční serverové certifikáty	**1**
2009	PostSignum Qualified CA	Osobní	Kvalifikované osobní certifikáty	**76**
	PostSignum Public CA	Systémový	Šifrovací certifikáty	**3**
	PostSignum Public CA	Systémový	Komerční serverové certifikáty	**4**
	PostSignum Public CA	Osobní	Komerční osobní certifikáty	**13**
	PostSignum Qualified CA	Systémový	Kvalifikované systémové certifikáty	**1**
2010	PostSignum Qualified CA	Osobní	Kvalifikované osobní certifikáty	**124**
	PostSignum Public CA	Osobní	Komerční osobní certifikáty	**24**
	PostSignum Public CA 2	Systémový	Šifrovací certifikáty	**1**
	PostSignum Public CA	Systémový	Komerční serverové certifikáty - SHA1	**1**
	PostSignum Public CA 2	Systémový	Komerční serverové certifikáty	**1**
	PostSignum Qualified CA 2	Systémový	Kvalifikované systémové certifikáty	**1**
2011	PostSignum Public CA 2	Systémový	Komerční serverové certifikáty	**3**
	PostSignum Qualified CA 2	Osobní	Kvalifikované osobní certifikáty	**112**
	PostSignum Public CA 2	Osobní	Komerční osobní certifikáty	**29**
	PostSignum Qualified CA 2	Systémový	Kvalifikované systémové certifikáty	**1**
2012	PostSignum Qualified CA 2	Osobní	Kvalifikované osobní certifikáty	**9**
	PostSignum Public CA 2	Osobní	Komerční osobní certifikáty	**1**

Obrázek 16 - Přehled vydaných certifikátů pro MěÚ Rakovník za roky 2008 - 2012 (zdroj: www.postsignum.cz/zakaznicky_portal)

11 Výhody a nedostatky v použití kvalifikovaného elektronického podpisu

Kvalifikovaný elektronický podpis ve veřejné správě by měl zlevnit, zrychlit a zjednodušit vyřizování veškerých věcí mezi příjemci a poskytovateli veřejné správy. V budoucnu se předpokládá, že komunikace pomocí papírových dokumentů by měla téměř zcela zaniknout. Ovšem tato myšlenka není zatím realizovatelná. Hlavní překážkou je mentalita lidí a nízká počítačová gramotnost, menšími překážkami jsou některé dílčí nedokonalosti v sladění legislativy a technických možností.

Zkušenost autora práce je taková, že ač má úředník možnost odeslat dokument občanovi nebo úřadu elektronicky, tak jej v mnoha případech vytiskne a odešle jako dopis pomocí České pošty, a to někdy i v případě že druhá strana má datovou schránku v systému ISDS. Stejně tak v případě, že úředník dostane elektronicky podepsaný dokument, tak jej vytiskne a založí do spisu, který vede duplicitně se spisem v elektronické podobě. Stejně tak podatelna v mnoha případech elektronicky přijaté dokumenty tiskne, poté eviduje do podacího deníku a dále s nimi nakládá jako s papírovými. Tyto situace jsou způsobeny neznalostí legislativy, která se týká použití kvalifikovaných elektronických podpisů ve veřejné správě, a konzervativním myšlením, které způsobuje nechuť používat nové postupy v práci a nové technologie.

Další nedostatky ve využití kvalifikovaného elektronického podpisu pro elektronickou komunikaci autor spatřuje v nedokonalosti elektronické komunikace ve veřejné správě pomocí emailů. Podle zá zákona č. 500/2004 Sb. Správní řád, si může účastník řízení zvolit adresu pro komunikaci. Pokud zvolí pro komunikaci emailovou schránku, pak mu musí být přednostně doručováno do ní. Ovšem podle § 19, odst. 8 a 9 Správního řádu musí účastník do následujícího dne potvrdit doručení datové zprávy do své schránky, podepsanou emailovou datovou zprávou. Bez tohoto potvrzení se datová zpráva považuje za nedoručenou a je nutno ji vypravit znovu na běžnou adresu účastníka. Bohužel není definováno, jaké má mít tato potvrzovací zpráva

náležitosti, a proto ji nelze automaticky přiřadit ve spisové službě jako doručenku. Z tohoto důvodu emailová komunikace s účastníky řízení je považována za neefektivní, a je na Městském úřadu v Rakovníku používána pouze na výslovnou žádost účastníka řízení. Vzhledem k povaze emailové komunikace, autor doporučuje, aby ze zákona byla vypuštěna možnost komunikovat emailem v případech, kdy je třeba zajistit ověřitelné doručení. Pro tyto účely je zřízen ISDS, který tyto problémy nemá.

Problémem je i to, že pracovnice podatelny ověřuje platnost elektronického podpisu na dokumentu nebo na datové zprávě v okamžiku přijetí do elektronické podatelny. V tomto okamžiku se ověřuje i skutečnost zda certifikát nebyl revokován. To se provádí oproti CRL listu, který je generován akreditovaným poskytovatelem certifikačních služeb a je zveřejněn na přesně definovaném místě, které je uvedeno v kvalifikovaném certifikátu. CRL listy jsou zveřejňovány v časových intervalech, (12 až 24h) a po tuto dobu není jisté, zda elektronický podpis je platný. Jestliže tedy pracovnice podatelny přijme elektronicky podepsaný email jako podání do spisové služby okamžitě po doručení, tak ještě po dobu 24 hodin existuje jisté riziko, že kvalifikovaný elektronický podpis, který byl ke zprávě připojen, je neplatný. V případě, že by byla datová zpráva zdržena podatelnou po dobu 24h pro kontrolní ověření odvolání podpisu, tak by sice byla jistota ohledně platnosti elektronického podpisu, ale již by vypršel jeden den ze zákonné lhůty, která je zákony stanovena pro vyřízení podání. Tento problém, je již technologicky vyřešen tím, že je možné kontrolu platnosti podpisu provést u certifikační autority online. Jde ovšem o nadstandardní službu, která je zpoplatněna. Je proto využívána jen tam, kde je tento problém klíčový.

Největší nebezpečí autor spatřuje v tom, že uživatelé kvalifikovaného elektronického podpisu, a to občané i úředníci, si stále ještě po dvanácti letech platnosti zákona č. 227/2000 Sb., o elektronickém podpisu neuvědomují, že právní dopady dokumentu podepsaného kvalifikovaným elektronickým podpisem jsou stejné jako dokumentu podepsaného před notářem nebo patřičným statním úředníkem. Toto nebezpečí ovšem není nedostatkem technologie, ale jejích uživatelů.

Pokud nedojde ve zlomu v přemýšlení o této problematice na všech úrovních, to jak u občanů, tak u úředníků a i centrálních a zákonodárných orgánů, tak bude muset minimálně jedna až dvě generace občanů vymřít a na jejich místo se dostanou dnešní třicátníci, kteří již v éře elektronizace vyrůstají a svět elektronické komunikace a elektronických podpisů je jejich přirozeností a druhou gramotností. Teprve pak bude myšlenka eGovernmentu realizována v plné šíři a úřady se zbaví dokumentů v papírové podobě.

Kladným efektem a velkou výhodou elektronické komunikace jsou i ekologické dopady. Jedná se například o snížení znečištění, které vzniká pří výrobě celulózy, omezení vzniku nebezpečného odpadu, kterým jsou tonery z tiskáren a i snížení výroby papíru a tím i nižší spotřeba dřeva a zachování lesních porostů.

12 Závěr

Elektronický podpis se v elektronické komunikaci používá po dobu více jak deseti let. Za tu dobu doznal po technologické stránce mnohá vylepšení a překonal dětské nemoci, kterými trpí všechny nové technologie. Používané programové vybavení pro práci s elektronickým podpisem je v dnešní době většině uživatelů srozumitelné a jeho obsluha je snadná. Legislativní zakotvení elektronického podpisu v českém právním řádu, je také dostatečné.

Autor předpokládá, že budoucnost komunikace občanů s veřejnou správou je opravdu v eGovernmentu a v elektronizaci veřejné správy a to včetně všech, v ní vznikajících, dokumentů. Je ovšem nutné vyřešit výše naznačené problémy. Česká republika vkládá do projektu eGovernmentu nemalé úsilí a prostředky. Jedná se například o tyto celostátní projekty: Czechpoint, ISDS - Datové schránky, Základní registry veřejné správy. Tyto projekty jsou klíčovými prvky eGovernmentu a elektronizace veřejné správy, ale z pohledu autora práce, který je realizátorem těchto projektů na obci s rozšířenou působností, se jedná o projekty legislativně nedotažené a

málo propagované Je v nich ponechána velká volnost pro alternativy. Elektronizace veřejné správy musí být centrálně řízena Vládou a Ministerstvem vnitra, a zákony musí být jednoznačné a nepřipouštět výjimky.

Autor se domnívá, že v rámci legislativy by měla být stanovena povinnost pro všechny právnické i fyzické osoby a i pro občany zřídit si datovou schránku a to proto, aby bylo s každým možno komunikovat elektronicky a zabezpečenou formou. V současnosti je tato povinnost pouze pro právnické osoby a některé další vyjmenované subjekty. To je nedostačující. Pošta by těm, kdo nemají možnost připojení k internetu, na jejich žádost doručila oznámení o doručené datové zprávě a datová zpráva by byla vydána občanovi na kontaktním místě Czechpointu, proti kontrole totožnosti, v konvertované podobě, analogicky s převzetím dopisu s doručenkou na poště.

Zákony, např. zákon č. 499/2004 Sb., o archivnictví a spisové službě, které se týkají dokumentů, jsou již zastaralé a jsou napsány primárně pro dokumenty v papírové podobě, proto by je měl stát novelizovat tak, aby primárním dokumentem ve veřejné správě byl vždy jen dokument elektronický, a papírový dokument by měl jen doplňkovou roli a jen ve zdůvodnitelných případech.

Jak je již uvedeno výše, tak problémem je i nedostatek odbornosti úředníků veřejné správy a personálu, který obsluhuje technologie, využívající elektronický podpis. Tento problém by mohl být vyřešen tak, že by v rámci povinného vzdělávání zaměstnanců veřejné správy byly proškoleny základní vědomosti z ICT minimálně v úrovni EDCL 2 (European Computer Driving Licence) a u nově přijímaných pracovníků by tyto znalosti byly součástí kvalifikačních požadavků. Tato problematika by měla být zahrnuta i do osnov pro Zvláštní odbornou způsobilost, která je definována zákonem č.312/2002 Sb. o úřednících územních samosprávných celků a zákonem č. 262/2006 Sb. zákoník práce.

Řešením pro odstranění počítačové negramotnosti veřejnosti by mohla být kampaň na podporu eGovernmentu, jejíž částí by byly i informace o elektronických

podpisech. Jako vzor by mohla posloužit televizní kampaň BESIP o silničním provozu, jen by v ní nebyly nebezpečné situace na silnici, ale vtipně zpracované životní situace občanů a jejich řešení pomocí elektronických komunikací. Tato kampaň by měla být financována státem a vysílána na veřejnoprávních médiích.

Technologie elektronického podpisu má v sobě velký potenciál pro zjednodušení komunikace mezi veřejností a úřady, mezi úřady navzájem a i mezi samotnými občany. Pokud dojde k tomu, že se většina komunikace, která nyní probíhá pomocí papíru, přesune do elektronické roviny, tak to bude mít i nezanedbatelný kladný ekonomický a ekologický dopad. Autor věří, že nastoupená cesta elektronizace veřejné správy je správná, a že by tento trend měl pokračovat a zintenzivnit. Zaručený elektronický podpis založený na kvalifikovaném certifikátu má v tomto procesu klíčovou roli, a je nezastupitelný.

13 Seznam použitých informačních zdrojů

[1] Bosáková D., Kučerová A., Peca J., Vondruška P., **Elektronický podpis**, nakladatelství ANAG, Olomouc, 2002, ISBN: 80-7263-125-X

[2] Dostálek, L., Vohnoutová M., **Velký průvodce infrastrukturou PKI a technologií elektronického podpisu**, nakladatelství Computer press, Praha, 2006, ISBN: 80-251-0828-7

[3] Budiš,P., **Elektronický podpis a jeho aplikace v praxi**, nakladatelství ANAG, Olomouc, 2008,ISBN: 978-80-7263-465-1

[4] Lidinský V., Švarcová I., Budiš P., Loebl Z., Procházková B., **eGovernment bezpečně,** nakladatelství GRADA Publishing,a.s 2008, ISBN: 978-80-247-2462-1

[5] Peterka J., **Báječný svět elektronického podpisu**, nakladatelství CZ.NIC, z. s. p. o., Praha 2011, ISBN: 978-80-904248-3-8

[6] http://web.mvcr.cz/archiv2008/casopisy/s/2002/0040/pril.html [17.3.2011]

[7] http://cs.wikipedia.org [10.5.2011]

[8] Zákon o elektronickém podpisu č.227/2000 Sb. a jeho novely

[9] Zákon č. 500/2004 Sb. - Správní řád

[10] http://www.postsignum.cz [19.3.2012]

[11] Jiří Schumann, Bakalářská práce - Elektronický podpis a jeho využití ve veřejné správě © 2010 ČZU v Praze

14 Seznam obrázků

15 Seznam příloh

ZÁKON č. 227/2000 Sb.,

o elektronickém podpisu a o změně některých dalších zákonů

(zákon o elektronickém podpisu)

ve znění zákona č. 226/2002 Sb., zákona č. 517/2002 Sb., zákona č. 440/2004 Sb. (úplné znění č. 486/2004 Sb.), zákona č. 635/2004 Sb., zákona č. 501/2004 Sb., zákona č. 444/2005 Sb., zákona č. 110/2007 Sb., zákona č. 124/2008 Sb., zákona č. 190/2009 Sb., zákona č. 223/2009 Sb., zákona č. 227/2009 Sb. a zákona č. 281/2009 Sb.

Parlament se usnesl na tomto zákoně České republiky:

Část první

ELEKTRONICKÝ PODPIS

§ 1

Účel zákona

Tento zákon upravuje v souladu s právem Evropských společenství1) používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

§ 2

Vymezení některých pojmů

Pro účely tohoto zákona se rozumí

a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které 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.

§ 3

Soulad s požadavky na podpis

(1) Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.

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

§ 3a

(1) Použití elektronické značky založené na kvalifikovaném systémovém certifikátu a vytvořené pomocí prostředku pro vytváření elektronických značek umožňuje ověřit, že datovou zprávu označila touto elektronickou značkou označující osoba.

(2) Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli.

§ 4

Soulad s originálem

Použití zaručeného elektronického podpisu nebo elektronické značky zaručuje, že dojdeli k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit.

§ 5

Povinnosti podepisující osoby

(1) Podepisující osoba je povinna

a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu.

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

§ 5a

Povinnosti označující osoby

(1) Označující osoba je povinna

a) zacházet s prostředkem, jakož i s daty pro vytváření elektronických značek s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný systémový certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření elektronických značek.

(2) Označující osoba je povinna zajistit, aby prostředek pro vytváření elektronických značek, který používá, splňoval požadavky stanovené tímto zákonem.

(3) Za škodu způsobenou porušením povinnosti podle odstavce 1 odpovídá označující osoba, i když škodu nezavinila, podle zvláštních právních předpisů,1a) odpovědnost za vady podle zvláštních předpisů tím není dotčena.1a) Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony

potřebné k tomu, aby si ověřil, že elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn.

§ 5b

Povinnosti držitele 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.

§ 6

Kvalifikovaný poskytovatel certifikačních služeb

(1) Kvalifikovaný poskytovatel certifikačních služeb je povinen

a) zajistit, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu, na jehož základě označuje vydané kvalifikované certifikáty nebo kvalifikované systémové certifikáty a seznamy certifikátů, které byly zneplatněny, nebo kvalifikovaná časová razítka,

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

c) používat bezpečné systémy a bezpečné nástroje elektronického podpisu, zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují, a zajistit dostatečnou kryptografickou bezpečnost těchto nástrojů; systémy a nástroje jsou považovány za bezpečné, pokud odpovídají požadavkům stanoveným tímto zákonem a prováděcí vyhláškou, nebo pokud splňují požadavky technických norem uvedených v rozhodnutí Komise vydaném na základě článku 3 (5) směrnice 99/93/ES,

d) používat bezpečné systémy pro uchovávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů nebo kvalifikovaných časových razítek v ověřitelné podobě takovým způsobem, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny porušující tyto bezpečnostní požadavky byly zjevné,

e) mít po celou dobu své činnosti k dispozici dostatečné finanční zdroje nebo jiné finanční zajištění na provoz v souladu s požadavky uvedenými v tomto zákoně a s ohledem na riziko vzniku odpovědnosti za škodu,

f) před uzavřením smlouvy o poskytování kvalifikovaných certifikačních služeb s osobou, která žádá o poskytování služeb podle tohoto zákona, informovat tuto osobu písemně o přesných podmínkách pro využívání kvalifikovaných certifikačních služeb, včetně případných omezení pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je, či není akreditován Ministerstvem vnitra (dále jen „ministerstvo“) podle § 10; tyto informace lze předat elektronicky.

(2) Neníli poskytovatel certifikačních služeb akreditován ministerstvem, je povinen ohlásit ministerstvu nejméně 30 dnů před zahájením poskytování kvalifikované certifikační služby, že ji bude poskytovat, a okamžik, kdy její poskytování zahájí. Zároveň předá ministerstvu k ověření svůj kvalifikovaný systémový certifikát uvedený v odstavci 1 písm. a).

(3) Pokud byla kvalifikovanému poskytovateli certifikačních služeb, který získal akreditaci podle § 10 tohoto zákona, akreditace ministerstvem odňata, je povinen bez prodlení informovat o této skutečnosti subjekty, kterým poskytuje své kvalifikované certifikační služby, a další dotčené osoby.

(4) Kvalifikovaný poskytovatel certifikačních služeb poskytuje služby podle tohoto zákona na základě smlouvy. Smlouva musí být písemná.

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

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

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

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

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

e) prohlášení držitele certifikátu o tom, že mu byly poskytnuty informace podle odstavce 1 písm. f),

f) dokumenty a záznamy související s životním cyklem vydaného kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, jejichž náležitosti upřesní prováděcí vyhláška.

(6) Veškeré informace a dokumentaci o poskytovaných službách podle tohoto zákona uchovává kvalifikovaný poskytovatel certifikačních služeb po dobu 10 let; po jejím uplynutí předá bez zbytečného odkladu ministerstvu seznam certifikátů vydaných jako kvalifikované, které byly zneplatněny. Kvalifikovaný poskytovatel je povinen zajistit uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením za podmínek, které upřesní prováděcí vyhláška. Informace a dokumentaci podle věty první může kvalifikovaný poskytovatel certifikačních služeb pořizovat a uchovávat v elektronické podobě. Pokud tento zákon nestanoví jinak, postupuje se při nakládání s informacemi a dokumentací podle zvláštního právního předpisu.2)

(7) Zaměstnanci kvalifikovaného poskytovatele certifikačních služeb, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji a daty pro vytváření elektronických podpisů podepisujících osob a elektronických značek označujících osob, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací; uvedené osoby může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

§ 6a

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů

(1) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty (dále jen „certifikáty vydané jako kvalifikované“), je povinen

a) zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) zajistit, aby údaje uvedené v certifikátech jím vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) před vydáním certifikátu jako kvalifikovaného bezpečně ověřit odpovídajícími prostředky identitu podepisující osoby nebo identitu označující osoby, případně i její zvláštní znaky, vyžadujeli to účel takového certifikátu,

d) zjistit, zda v okamžiku podání žádosti o vydání certifikátu jako kvalifikovaného měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo označující osoba data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek, která obsahuje žádost o vydání certifikátu,

e) zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, k jejichž zveřejnění dal držitel certifikátu souhlas v souladu s § 6 odst. 5 písm. d), a zajistit dostupnost tohoto seznamu i dálkovým přístupem a údaje v seznamu obsažené při každé změně bez zbytečného odkladu aktualizovat,

f) zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) přijmout odpovídající opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované,

i) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání certifikátů vydaných jako kvalifikované, včetně omezení pro jejich použití, a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

(2) Pokud kvalifikovaný poskytovatel certifikačních služeb, který vydává certifikáty jako kvalifikované, vytváří pro podepisující osobu data pro vytváření elektronických podpisů nebo pro označující osobu data pro vytváření elektronických značek,

a) musí zajistit utajení těchto dat před jejich předáním, nesmí tato data kopírovat a uchovávat je déle, než je nezbytné,

b) musí zaručit, že tato data odpovídají datům pro ověřování elektronických podpisů nebo datům pro ověřování elektronických značek.

(3) Kvalifikovaný poskytovatel certifikačních služeb, který vydává certifikáty jako kvalifikované, musí neprodleně zneplatnit certifikát, pokud o to držitel, podepisující osoba nebo označující osoba požádá, nebo pokud ho uvědomí, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů nebo elektronických značek, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.

(4) Kvalifikovaný poskytovatel certifikačních služeb musí rovněž neprodleně zneplatnit certifikát vydaný jako kvalifikovaný, dozvíli se prokazatelně, že podepisující nebo označující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, 2a) nebo pokud údaje, na jejichž základě byl certifikát vydán, pozbyly pravdivosti.

§ 6b

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných časových razítek

(1) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, je povinen

a) zajistit, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené tímto zákonem,

b) zajistit, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek,

e) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

(2) Kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

§ 7

Odpovědnost za škodu

(1) Za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá kvalifikovaný poskytovatel certifikačních služeb podle zvláštních právních předpisů.1a)

(2) Kvalifikovaný poskytovatel certifikačních služeb neodpovídá za škodu vyplývající z použití certifikátu vydaného jako kvalifikovaný, která vznikla v důsledku nedodržení omezení pro jeho použití podle § 12 odst. 1 písm. i) a j) a § 12a písm. h).

§ 8

Ochrana osobních údajů

Ochrana osobních údajů se řídí zvláštním právním předpisem.3)

§ 9

Akreditace a dozor

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

(2) Ministerstvo

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

b) vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a kvalifikovaných poskytovatelů certifikačních služeb, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona,

c) vede evidenci udělených akreditací a jejich změn a evidenci kvalifikovaných poskytovatelů certifikačních služeb,

d) vede evidenci vydaných kvalifikovaných systémových certifikátů, které používá kvalifikovaný poskytovatel certifikačních služeb podle § 6 odst. 1 písm. a) a které byly podle § 6 odst. 2 ověřeny ministerstvem,

e) průběžně uveřejňuje přehled udělených akreditací, přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb a kvalifikované systémové certifikáty podle písmena d), a to i způsobem umožňujícím dálkový přístup,

f) vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou,

g) plní další povinnosti stanovené tímto zákonem.

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

(4) Neníli tímto zákonem stanoveno jinak, postupuje ministerstvo při výkonu dozoru podle zvláštního právního předpisu. 4)

(5) Kvalifikovanému poskytovateli certifikačních služeb, který nesplnil povinnost součinnosti podle odstavce 3, lze uložit pořádkovou pokutu do výše 1 000 000 Kč.

§ 10

Podmínky udělení akreditace pro poskytování certifikačních služeb

(1) Každý poskytovatel certifikačních služeb může požádat ministerstvo o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

(2) V žádosti o akreditaci podle odstavce 1 musí žadatel doložit

a) v případě právnické osoby obchodní firmu nebo název, sídlo, popřípadě adresu organizační složky zahraniční osoby na území České republiky, a identifikační číslo žadatele, byloli přiděleno; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, místo usazení, místo podnikání, pokud je odlišné od místa usazení, a identifikační číslo žadatele, byloli přiděleno,

[→ Dnem 1. července 2010 se za slova „identifikační číslo“ vkládá slovo „osoby“.]

b) doklad o oprávnění k podnikatelské činnosti a u osoby zapsané do obchodního rejstříku také výpis z obchodního rejstříku ne starší než 3 měsíce,

c) věcné, personální a organizační předpoklady pro činnost kvalifikovaného poskytovatele certifikačních služeb podle § 6, 6a a 6b tohoto zákona,

d) údaj o tom, které kvalifikované certifikační služby hodlá žadatel poskytovat.

(3) Jestliže žádost neobsahuje všechny požadované údaje, ministerstvo řízení přeruší a vyzve žadatele, aby ji ve stanovené lhůtě doplnil. Jestliže tak žadatel v této lhůtě neučiní, ministerstvo řízení zastaví.

(4) Splňujeli žadatel všechny podmínky předepsané tímto zákonem pro udělení akreditace, vydá ministerstvo rozhodnutí, jímž mu akreditaci udělí. V opačném případě žádost o udělení akreditace zamítne. Akreditace poskytovatele certifikačních služeb vzniká též marným uplynutím lhůty a způsobem podle § 28 až 30 zákona o volném pohybu služeb.

§ 10a

Podmínky pro rozšíření služeb akreditovaného poskytovatele certifikačních služeb

(1) Akreditovaný poskytovatel certifikačních služeb může rozšířit poskytování kvalifikovaných certifikačních služeb o vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, kvalifikovaných časových razítek nebo o vydávání prostředků pro bezpečné vytváření elektronických podpisů podle tohoto zákona (dále jen „rozšiřované služby“).

(2) Akreditovaný poskytovatel certifikačních služeb je povinen rozšíření podle odstavce 1 oznámit ministerstvu tak, aby ministerstvo oznámení obdrželo alespoň 4 měsíce před zahájením poskytování služby.

(3) V oznámení musí akreditovaný poskytovatel certifikačních služeb doložit věcné, personální a organizační předpoklady pro zajištění rozšiřovaných služeb.

(4) Nedoložíli akreditovaný poskytovatel certifikačních služeb skutečnosti podle odstavce 3, anebo jsouli tyto skutečnosti neúplné nebo nepřesné, ministerstvo na to akreditovaného poskytovatele certifikačních služeb upozorní s tím, že nebudouli tyto vady ve lhůtě, kterou k tomu určí, odstraněny, rozhodnutím rozšiřování služeb zakáže.

(5) Ministerstvo oznámené rozšíření zakáže, pokud akreditovaný poskytovatel certifikačních služeb nesplnil všechny podmínky předepsané tímto zákonem pro poskytování rozšiřovaných služeb.

(6) O zákazu rozšíření poskytování kvalifikovaných certifikačních služeb vydá ministerstvo rozhodnutí nejpozději do 90 dnů od okamžiku, kdy obdrželo oznámení.

§ 11

(1) 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. Pokud je uznávaný

elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, stanoví ministerstvo prováděcím právním předpisem.

(2) Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

(3) Orgán veřejné moci přijímá a odesílá datové zprávy podle odstavce 1 prostřednictvím elektronické podatelny.

§ 12

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,

b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,

d) zvláštní znaky podepisující osoby, vyžadujeli to účel kvalifikovaného certifikátu,

e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,

f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám.

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

§ 12a

Náležitosti kvalifikovaného systémového certifikátu

Kvalifikovaný systémový certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona,

b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek,

d) data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby,

e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává,

f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,

g) počátek a konec platnosti kvalifikovaného systémového certifikátu,

h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.

§ 12b

Náležitosti kvalifikovaného časového razítka

Kvalifikované časové razítko musí obsahovat

a) číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,

b) označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,

c) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

d) hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,

e) data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno,

f) elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

§ 13

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při ukončení činnosti

(1) Kvalifikovaný poskytovatel certifikačních služeb musí záměr ukončit svou činnost ohlásit ministerstvu nejméně 3 měsíce před plánovaným datem ukončení činnosti a musí vynaložit veškeré možné úsilí k tomu, aby evidence vedená podle § 6 odst. 5 byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb. Kvalifikovaný poskytovatel certifikačních služeb dále musí prokazatelně informovat každou podepisující osobu, označující osobu a držitele, kterým poskytuje své certifikační služby, o svém záměru ukončit svoji činnost nejméně 2 měsíce před plánovaným datem ukončení činnosti.

(2) Nemůželi kvalifikovaný poskytovatel certifikačních služeb zajistit, aby evidenci vedenou podle § 6 odst. 5 převzal jiný kvalifikovaný poskytovatel certifikačních služeb, je povinen to nejpozději 30 dnů před plánovaným datem ukončení činnosti ministerstvu ohlásit. V takovém případě ministerstvo převezme evidenci a oznámí to dotčeným subjektům.

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

§ 14

Opatření k nápravě

(1) Zjistíli ministerstvo, že akreditovaný poskytovatel certifikačních služeb nebo kvalifikovaný poskytovatel certifikačních služeb porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě sjednal nápravu, a případně určí, jaká opatření k odstranění nedostatků je tento poskytovatel certifikačních služeb povinen přijmout.

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

(3) Rozhodneli ministerstvo o odnětí akreditace, může současně rozhodnout o zneplatnění certifikátů vydaných jako kvalifikované poskytovatelem certifikačních služeb v době platnosti akreditace.

§ 15

Zrušení kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu

Ministerstvo může nařídit kvalifikovanému poskytovateli certifikačních služeb jako předběžné opatření7) zneplatnění certifikátu vydaného jako kvalifikovaný, pokud existuje důvodné podezření, že certifikát byl padělán, nebo pokud byl vydán na základě nepravdivých údajů. Rozhodnutí o zneplatnění certifikátu vydaného jako kvalifikovaný může být vydáno také v případě, kdy bylo zjištěno, že podepisující nebo označující osoba používá prostředek pro vytváření podpisu nebo prostředek pro vytváření elektronických značek, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo elektronických značek nebo změnu podepisovaných nebo označovaných údajů.

§ 16

Uznávání zahraničních kvalifikovaných certifikátů

(1) Certifikát, který je vydán poskytovatelem certifikačních služeb usazeným v některém z členských států Evropské unie jako kvalifikovaný, je kvalifikovaným certifikátem ve smyslu tohoto zákona.

(2) Certifikát, který je vydán jako kvalifikovaný ve smyslu tohoto zákona v jiném než členském státu Evropské unie, je kvalifikovaným certifikátem ve smyslu tohoto zákona, pokud

a) poskytovatel certifikačních služeb splňuje podmínky práva Evropských společenství1) a byl akreditován k působení jako akreditovaný poskytovatel certifikačních služeb v některém z členských států Evropské unie,

b) poskytovatel certifikačních služeb usazený v některém z členských států Evropské unie, který splňuje podmínky práva Evropských společenství, 1) převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů, nebo

c) to vyplývá z mezinárodní smlouvy.

§ 17

Prostředky pro bezpečné vytváření a ověřování elektronických podpisů

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

a) data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno,

b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie,

c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou.

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

(3) Prostředky pro bezpečné vytváření elektronických podpisů musí být před svým použitím bezpečným způsobem vydány a data pro vytváření elektronických podpisů musí být důvěryhodným způsobem v těchto prostředcích vytvořena nebo do nich přidána.

(4) Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby

a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,

b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,

c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,

d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,

e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,

f) bylo jasně uvedeno použití pseudonymu,

g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§ 17a

Prostředky pro vytváření elektronických značek

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

a) data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,

b) označující osoba je informována, že zahajuje používání tohoto prostředku.

(2) Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí.

(3) Prostředek pro vytváření elektronických značek musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.

§ 18

Správní delikty právnických osob

(1) Kvalifikovanému poskytovateli certifikačních služeb, který

a) nezajistí, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu podle § 6 odst. 1 písm. a),

b) nezajistí, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnými pro poskytované kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) nezajištěním dostatečné bezpečnosti používaných systémů a nástrojů elektronického podpisu a postupů, které tyto systémy a nástroje podporují podle § 6 odst. 1 písm. c) a d), ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

d) nedisponuje dostatečnými finančními zdroji nebo jiným finančním zajištěním na provoz podle § 6 odst. 1 písm. e), a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6 odst. 1 písm. f), § 6 odst. 3 nebo § 13 odst. 1,

f) nesplní ohlašovací povinnost podle § 6 odst. 2, včetně předání kvalifikovaného systémového certifikátu k ověření nebo podle § 13 odst. 1 nebo 2,

g) poskytne certifikační služby na základě jiné než písemné smlouvy,

h) neuchovává informace a dokumentaci podle § 6 odst. 5,

i) neuchovává veškeré informace a dokumentaci podle § 6 odst. 6 po dobu nejméně 10 let, nebo

j) nezajistí uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením podle § 6 odst. 6,

se uloží pokuta do výše 10 000 000 Kč.

(2) Kvalifikovanému poskytovateli certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty a který

a) nezajistí, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) nezajistí, aby údaje uvedené v certifikátech vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) neověří identitu osoby podle § 6a odst. 1 písm. c),

d) nezajistí soulad dat podle § 6a odst. 1 písm. d),

e) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované a nezajistí jeho dostupnost a aktualizaci podle § 6a odst. 1 písm. e),

f) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) nezajistí, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) nepřijetím odpovídajících opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

i) nesplní informační povinnost podle § 6a odst. 1 písm. i),

j) nezajistí soulad a utajení dat podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří,

k) kopíruje a uchovává data podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří, nebo

l) nezneplatní certifikát podle § 6a odst. 3 a 4,

se uloží pokuta do výše 10 000 000 Kč.

(3) Kvalifikovanému poskytovateli certifikačních služeb, který vydává kvalifikovaná časová razítka a který

a) nezajistí, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené v § 12b,

b) nezajistí, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) nezajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) nepřijme odpovídající opatření proti padělání kvalifikovaných časových razítek, a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6b odst. 1 písm. e), nebo

f) nevydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání,

se uloží pokuta do výše 10 000 000 Kč.

(4) Kvalifikovanému poskytovateli certifikačních služeb, který vydává prostředky pro bezpečné vytváření elektronických podpisů a který

a) nevydá prostředky pro bezpečné vytváření elektronických podpisů bezpečně podle § 17 odst. 3, nebo

b) nevytvoří v těchto prostředcích nebo nepřidá do těchto prostředků data pro vytváření elektronických podpisů důvěryhodným způsobem podle § 17 odst. 3,

se uloží pokuta do výše 10 000 000 Kč.

(5) Akreditovanému poskytovateli certifikačních služeb, který nesplní oznamovací povinnost podle § 10a odst. 2, se uloží pokuta do výše 10 000 000 Kč.

(6) Akreditovanému poskytovateli certifikačních služeb, který poruší zákaz vydaný ministerstvem podle § 10a odst. 5, se uloží pokuta do výše 10 000 000 Kč.

§ 18a

Přestupky

(1) Kvalifikovaný poskytovatel certifikačních služeb se dopustí přestupku tím, že

a) nezajistí, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu podle § 6 odst. 1 písm. a),

b) nezajistí, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnými pro poskytované kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) nezajištěním dostatečné bezpečnosti používaných systémů a nástrojů elektronického podpisu a postupů, které tyto systémy a nástroje podporují podle § 6 odst. 1 písm. c) a písm. d), ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

d) nedisponuje dostatečnými finančními zdroji nebo jiným finančním zajištěním na provoz podle § 6 odst. 1 písm. e), a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6 odst. 1 písm. f), § 6 odst. 3 nebo § 13 odst. 1,

f) nesplní ohlašovací povinnost podle § 6 odst. 2, včetně předání kvalifikovaného systémového certifikátu k ověření nebo podle § 13 odst. 1 nebo 2,

g) poskytne certifikační služby na základě jiné než písemné smlouvy,

h) neuchovává informace a dokumentaci podle § 6 odst. 5,

i) neuchovává veškeré informace a dokumentaci podle § 6 odst. 6 po dobu nejméně 10 let, nebo

j) nezajistí uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením podle § 6 odst. 6.

(2) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty, se dopustí přestupku tím, že

a) nezajistí, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) nezajistí, aby údaje uvedené v certifikátech vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) neověří identitu osoby podle § 6a odst. 1 písm. c),

d) nezajistí soulad dat podle § 6a odst. 1 písm. d),

e) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované a nezajistí jeho dostupnost a aktualizaci podle § 6a odst. 1 písm. e),

f) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) nezajistí, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) nepřijetím odpovídajících opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

i) nesplní informační povinnost podle § 6a odst. 1 písm. i),

j) nezajistí soulad a utajení dat podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří,

k) kopíruje a uchovává data podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří, nebo

l) nezneplatní certifikát podle § 6a odst. 3 a 4.

(3) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, se dopustí přestupku tím, že

a) nezajistí, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené v § 12b,

b) nezajistí, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) nezajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) nepřijme odpovídající opatření proti padělání kvalifikovaných časových razítek, a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6b odst. 1 písm. e), nebo

f) nevydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

(4) Kvalifikovaný poskytovatel certifikačních služeb, který vydává prostředky pro bezpečné vytváření elektronických podpisů, se dopustí přestupku tím, že

a) nevydá prostředky pro bezpečné vytváření elektronických podpisů bezpečně podle § 17 odst. 3, nebo

b) nevytvoří v těchto prostředcích nebo nepřidá do těchto prostředků data pro vytváření elektronických podpisů důvěryhodným způsobem podle § 17 odst. 3.

(5) Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti podle § 6 odst. 7.

(6) Za přestupky podle odstavců 1 až 4 lze uložit pokutu do výše 10 000 000 Kč.

(7) Za přestupek podle odstavce 5 lze uložit pokutu do výše 250 000 Kč.

§ 19

Společná ustanovení

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při určení výměry pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž bylo spácháno.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Správní delikty podle tohoto zákona v prvním stupni projednává ministerstvo.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby8) nebo v přímé souvislosti s ním, se vztahují ustanovení zákona o odpovědnosti a postihu právnické osoby.

(6) Pokuty vybírá a vymáhá místně příslušný celní úřad. Výnos z pokut je příjmem státního rozpočtu.

[→ Dnem 1. ledna 2011 se v § 19 odst. 6 věta první zrušuje.]

§ 20

Zmocňovací ustanovení

(1) Ministerstvo stanoví prováděcím právním předpisem způsob splnění informační povinnosti podle § 6 odst. 1 písm. a) a f) a odst. 3, kvalifikační požadavky podle § 6 odst. 1 písm. b), požadavky na bezpečné systémy a bezpečné nástroje podle § 6 odst. 1 písm. c) a d), způsob uchovávání informací a dokumentace podle § 6 odst. 5 a 6 a způsob, jakým se splnění těchto požadavků dokládá.

(2) Ministerstvo stanoví prováděcím právním předpisem způsob ověření souladu dat podle § 6a odst. 1 písm. d), způsob zajištění bezpečnosti seznamů podle § 6a odst. 1 písm. e) a f), určení data a času podle § 6a odst. 1 písm. g), náležitosti opatření podle § 6a odst. 1 písm. h), způsob splnění informační povinnosti podle § 6a odst. 1 písm. i), způsob ochrany a zajištění souladu dat podle § 6a odst. 2, způsob zneplatnění certifikátů podle § 6a odst. 3 a 4 a způsob, jakým se splnění těchto požadavků dokládá.

(3) Ministerstvo stanoví prováděcím právním předpisem způsob zajištění přesnosti času při vytváření kvalifikovaného časového razítka podle § 6b odst. 1 písm. b), způsob zajištění souladu dat podle § 6b odst. 1 písm. c), náležitosti opatření podle § 6b odst. 1 písm. d), způsob splnění informační povinnosti podle § 6b odst. 1 písm. e) a způsob, jakým se splnění těchto požadavků dokládá.

(4) Ministerstvo stanoví prováděcím právním předpisem strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, a postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny podle § 11 odst. 3.

(5) Ministerstvo stanoví prováděcím právním předpisem způsob zajištění postupů, které musí podporovat prostředky pro bezpečné vytváření a ověřování elektronických podpisů při ochraně dat pro vytváření elektronických podpisů podle § 17 a prostředky pro vytváření elektronických značek při ochraně dat pro vytváření elektronických značek podle § 17a, a způsob, jakým se splnění těchto požadavků dokládá.

Část druhá

Změna občanského zákoníku

§ 21

Část třetí

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

§ 22

[→ Dnem 1. ledna 2011 se část třetí zrušuje.]

Část čtvrtá

Změna správního řádu

§ 24

zrušen

Část pátá

Změna občanského soudního řádu

§ 24

Část šestá

Změna trestního řádu

§ 25

Část sedmá

Změna zákona o ochraně osobních údajů

§ 26

Část osmá

Změna zákona o správních poplatcích

§ 27

Část devátá

ÚČINNOST

§ 28

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

* * *

Zákon č. 226/2002 Sb., nabyl účinnosti dnem 1. července 2002.

Zákon č. 517/2002 Sb., nabyl účinnosti dnem 1. ledna 2003.

Zákon č. 440/2004 Sb., nabyl účinnosti dnem 26. července 2004.

Zákon č. 635/2004 Sb., nabyl účinnosti dnem 16. ledna 2005.

Zákon č. 501/2004 Sb. nabyl účinnosti dnem 1. ledna 2006.

Zákon č. 444/2005 Sb. nabyl účinnosti dnem 1. ledna 2006.

Zákon č. 110/2007 Sb. nabyl účinnosti dnem 1. června 2007.

Zákon č. 124/2008 Sb. nabyl účinnosti dnem 1. července 2008.

Zákon č. 190/2009 Sb. nabyl účinnosti dnem 1. července 2009.

Zákon č. 223/2009 Sb. nabyl účinnosti dnem 28. prosince 2009.

Zákon č. 227/2009 Sb. nabývá účinnosti dnem 1. července 2010.

Zákon č. 281/2009 Sb. nabývá účinnosti dnem 1. ledna 2011.

* * *

Čl. II

zákona č. 440/2004 Sb. zní:

Přechodná ustanovení

Poskytovatelé certifikačních služeb, kterým byla udělena akreditace k působení jako akreditovaný poskytovatel certifikačních služeb přede dnem nabytí účinnosti tohoto zákona, jsou povinni přizpůsobit službu vydávání kvalifikovaných certifikátů zákonu č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění čl. I tohoto zákona, do 1. července 2005.

Čl. LXVI

zákona č. 444/2005 Sb. zní:

Přechodná ustanovení

1. Řízení ve věcech, u nichž přešla působnost z územních finančních orgánů na celní úřady, zahájená územními finančními orgány přede dnem nabytí účinnosti tohoto zákona, dokončí orgán, který řízení zahájil.

2. Řízení zahájená územními finančními orgány příslušnými do dne nabytí účinnosti tohoto zákona dokončí tyto územní finanční orgány.

Odkazy k textu:

1) Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

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

2) Zákon č. 97/1974 Sb., o archivnictví, ve znění pozdějších předpisů.

2a) § 10 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

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

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

7) § 43 zákona č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů.

8) § 2 odst. 2 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů.