Optimalizace podávání evidenčních listů důchodového pojištění elektronickou cestou

The Electronic Optimization of Pension Insurance Record Administration

Bc. Lubomír Sítek

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lubomír Sítek**
Osobní číslo:	**A11381**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Optimalizace podávání evidenčních listů důchodového pojištění elektronickou cestou**

Zásady pro vypracování:

1. **Proveďte literární rešerši tématu zadání práce.**
2. **Objasněte principy podávání evidenčních listů a jejich zabezpečení pomocí PKI.**
3. **Formou projektu navrhněte způsob využití elektronického podpisu při workflow evidenčních listů.**
4. **Realizujte navžené řešení a proveďte jeho optimalizaci v konkrétních podmínkách.**
5. **Vyhodnoťte kvalitu řešení a proveďte jeho diskusi.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. PETERKA, Jiří. Báječný svět elektronického podpisu. Praha: CZ.NIC, 2011, 430 s. ISBN 978-80-904248-3-8.
2. DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.
3. DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
4. BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc: ANAG, 2008, 157 s. ISBN 978-80-7263-465-1.
5. MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Vyd. 1. Brno: Computer Press, 2007, 154 s. ISBN 978-80-251-1511-4.

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je zjednodušení administrativy, snížení finančních nákladů a zrychlení komunikace díky efektivnějšímu podávání evidenčních listů důchodového pojištění pro Českou správu sociálního zabezpečení, pouze elektronickou cestou, s využitím elektronického podpisu. Veškeré navrhované metody a změny předávání informací jsou koncipovány v souladu s platnou právní legislativou a vnitřními předpisy. K tomuto účelu jsou v práci popsány aktuální právní aspekty, problematika elektronického podpisu z pohledu bezpečnosti, žádost o vystavení kvalifikovaného certifikátu zaměstnance, záloha certifikátu a změna nastavení používaného mzdového informačního systému Fluxpam firmy Flux s.r.o., který umožňuje zpracování dávkového elektronického podání.

Klíčová slova: elektronický podpis, evidenční list důchodového pojištění, certifikační autorita, kvalifikovaný certifikát, privátní klíč, veřejný klíč, úložiště certifikátů, PKI, zákon o elektronickém podpisu.

ABSTRACT

The main goal of this thesis is to simplify administration, reduce financial costs and make communication faster through more efficient filing of pension insurance records only electronically way with using the electronic signature. All of the proposed methods and changes in the transmission of information and connection with the portal of Česká správa sociálního zabezpečení (The Czech Social Security Administration) are designed in accordance with applicable legislation and internal regulations. For this purpose, there are described current legal aspects, issues of the electronic signature from a security perspective, request for a qualified certificate for the employee, backup of the certificate and changes in the settings used in payroll system Fluxpam from Flux Ltd., which allows to batch the electronic submission.

Keywords: electronic signature, pension insurance record, certification authority, qualified certificate, private key, public key, certificate store, PKI, electronic signature law.

Chtěl bych touto cestou poděkovat doc. Mgr. Romanu Jaškovi, Ph.D. za odborné vedení diplomové práce a vstřícný přístup. Dále bych chtěl poděkovat mé přítelkyni Ing. Lucii Kališové za pomoc se závěrečnou gramatickou úpravou práce, ochotu a trpělivost během studia. Mé poděkování patří také Mgr. Olze Neprašové za odbornou pomoc s překlady do anglického jazyka.

Motto: Štěstí je, když budete chtít to, čeho jste dosáhli! Úspěch je, když dosáhnete toho, co jste chtěli!

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Dynamický vývoj moderních informačních a komunikačních technologií přinesl významné dopady nejen na podnikatelské prostředí, ale prakticky na všechny obory a oblasti lidských aktivit. Jedním z fenoménů dnešní doby je bezesporu elektronický podpis, který se v posledních letech dostal do povědomí obyvatelstva a stoupá o něj také zájem odborníků. Stát dokonce v mnoha případech jeho užití nařizuje, zejména v souvislosti s celkovou elektronizací veřejné správy. Vzali jej proto na vědomí také zákonodárci, kteří dokončili a neustále novelizují legislativní procesy a zákony o elektronickém podpisu.

Cílem mé diplomové práce je vysvětlit pojem elektronický podpis, analyzovat principy elektronického podepisování a ověřování, technické i zákonné normy, které se k němu vztahují a zhodnotit jeho využitelnost v praxi při podávání evidenčních listů důchodového pojištění pouze elektronickou cestou. Práce s elektronickými podpisy je zásadně jiná, než práce s vlastnoručními podpisy, proto bude rozebrána také bezpečnost a stanoveny bezpečnostní zásady v konkrétních podmínkách.

Prvotním impulzem pro zpracování diplomové práce na dané téma byl požadavek vedení organizace k trvalému zjednodušování administrativy, zrychlování komunikace a snižování finančních nákladů v organizaci. V diplomové práci objasním postup získání kvalifikovaného certifikátu, popíši finanční náročnost projektu, jeho ekonomické přínosy pro celou organizaci a realizuji navržené řešení, jehož výstupem bude optimalizace při podávání dávek pro Českou správu sociálního zabezpečení pouze elektronickou cestou.

Jako hlavní přínos mé diplomové práce spatřuji v předání praktických zkušeností s elektronickým podpisem při podávání evidenčních listů důchodového pojištění a možnosti nezaujatě zhodnotit současný stav a vývojové tendence ve zmíněné oblasti.

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE

Elektronický podpis je jedním z hlavních nástrojů **identifikace** (identifikuje podepsanou či podepisující osobu a poskytuje nám údaje o identitě této osoby) a **autentizace** (proces ověření proklamované identity subjektu) fyzických osob v prostředí internetu. Elektronický podpis připojený k datové zprávě se stal rovnoprávným ekvivalentem vlastnoručního podpisu na písemném dokumentu. V současné době mohou občané využívat elektronický podpis vůči orgánům veřejné správy především v oblasti správy daní, obecných správních řízeních, v oblasti státní sociální podpory a zdravotní péče a dále také úřady při vzájemné komunikaci mezi ostatními úřady. V oblasti elektronického podpisu se používá specifická terminologie, a proto pro přesné vysvětlení většiny pojmů je nutné znát řadu souvislostí a hlavně principů, o které se fungování elektronického podpisu opírá.

1.1 Zpráva, dokument

V oblasti elektronického podpisu se používají termíny **dokument** a **datová zpráva**. Z obecného hlediska nemusí být mezi dokumentem a datovou zprávou rozdíl. V praxi ale např. u datových schránek[1] rozeznáváme zcela zásadní rozdíl mezi datovou zprávou a dokumentem, který je obsažen (připojen) k datové zprávě. Od zprávy také obvykle nepožadujeme delší životnost (potřebujeme ji pouze pro jednorázový přenos informace), zatímco s dokumentem potřebujeme mnohdy pracovat řadu let. V diplomové práci budou proto zmiňovány primárně dokumenty a jejich podepisování. Je třeba také pamatovat na skutečnost, že písemný dokument může mít jak listinnou, tak i elektronickou formu.

1.2 Podpis, elektronický podpis, digitální podpis

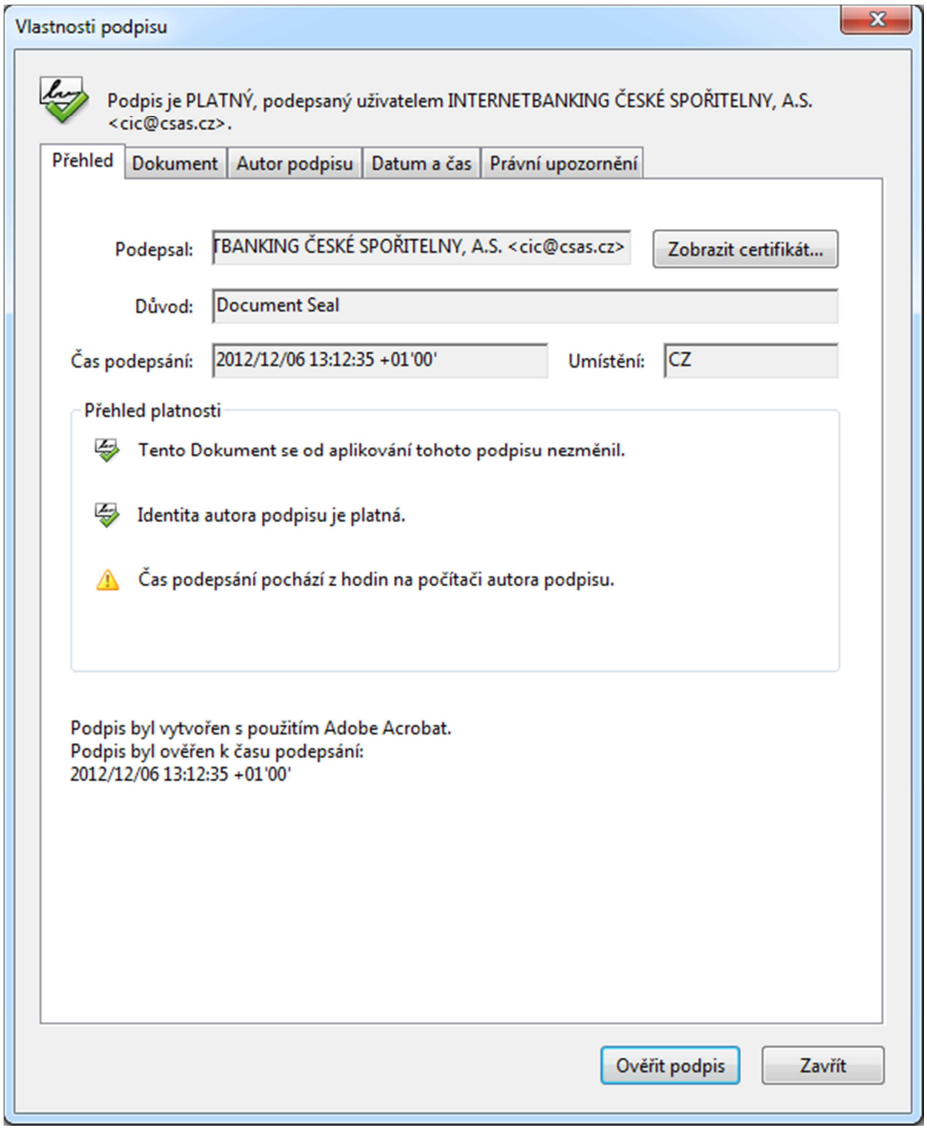
Klasický písemný dokument je mnohdy nutné podepsat, ať už vlastnoručním podpisem nebo ověřeným vlastnoručním podpisem (notářem či jinak úředně ověřeným). Pokud bychom vlastnoruční podpis dali ke zkoumání grafologovi, zabýval by se tím, jak je veden tah perem, jaký je sklon a tvar jednotlivých znaků. V případě elektronického podpisu, který se připojuje k dokumentům v elektronické formě, by nic takového nemělo smysl zkoumat.

[1] Datové schránky jsou elektronickým úložištěm, na které se doručují dokumenty orgánů veřejné moci a stejně tak i vůči nim. Tento způsob komunikace nahrazuje klasické doručování v listinné podobě.

Elektronický podpis ve své podstatě není ničím jiným než číslem a může obsahovat následující část řetězce:

MIIGkDCCBHigAwIBAgIKSRz0ugABAAAagzANBgkqhkiG9w0BAQUFADBRMQswCQYDVQQGEwJDWjEnMCUGA1UECgweTWluaXN0ZXJzdHZvIHNwcmF2ZWRsbm9zdGkgxIxSMRkwFwYDVQQDExBNU3AgU2VydmlzIENBIDAxMB4XDTEyMDMwMTIwMDkyNVoXDTEz

Ostatní aplikace, které pracují s elektronickými podpisy, zobrazí informace svým uživatelům v příjemnější a podrobnější podobě. Na následujícím obrázku je zobrazeno ověření elektronického podpisu internetového bankovnictví v aplikaci Adobe Reader:



Obrázek 1: Vlastnosti podpisu v aplikaci Adobe Reader

Zdroj [Vlastní tvorba]

V praxi se setkáváme také s pojmem **digitální podpis,** což by mělo být přesnějším označením pro ten druh podpisu, který má povahu čísla. V běžné praxi, zákonech a vyhláškách se pracuje pouze s pojmem elektronický podpis, proto v diplomové práci bude zmiňován pouze tento pojem a kdykoliv bude zmíněn elektronický podpis bez dalšího upřesnění, bude tím myšlen **zaručený nebo uznávaný elektronický podpis**, který „uzná“ úřad (orgán veřejné moci), pokud s ním budeme komunikovat elektronickou cestou.

1.3 Integrita, nepopiratelnost, důvěrnost, autenticita

Jednou ze záruk, kterou zaručený elektronický podpis poskytuje, **je integrita** dokumentu. Znamená jeho neporušenost ve smyslu celistvosti a neměnnosti. Elektronický podpis dává záruku, že podepsaný dokument se od okamžiku svého podpisu nezměnil nebo naopak řekne, že dokument byl pozměněn (nedozvíme se ovšem na jakých místech).

Další důležitou zárukou elektronického podpisu je tzv. **nepopiratelnost** (též neodmítnutelnost). Podepsaná osoba nemůže popřít, že podpis vytvořila ona (nemůže odmítnout důsledky svého podpisu) za podmínky, že tento zaručený elektronický podpis je dostatečně kvalitní (založený na kvalifikovaném certifikátu) ve smyslu, že se můžeme spolehnout na to, co říká ohledně identity podepsané osoby.

Záruku, kterou elektronický podpis neposkytuje, je zajištění **důvěrnosti** ve smyslu zajištění toho, aby se s daným obsahem dokumentu nemohla seznámit nepovolaná osoba, což v prostředí dnešního internetu nelze snadno realizovat. V praxi se důvěrnosti dosahuje vhodným zašifrováním příslušného obsahu, např. kterýkoliv elektronický dokument můžeme jak podepsat, tak i zašifrovat daným šifrovacím algoritmem.

Pravost, resp. autentičnost neboli **autenticita** je dalším pojmem, se kterým se lze setkat v souvislosti s elektronickými dokumenty. Elektronický podpis nám díky integritě dokumentu, který je opatřený zaručeným elektronickým podpisem, může říci, zda dokument byl pozměněn nebo vyměněn.

1.4 Elektronické značky, časová razítka

I když je elektronický podpis určen pouze fyzickým osobám (za příslušnou právnickou osobu jedná a podepisuje opět fyzická osoba), tak v praxi se nicméně vynutila obdoba elektronického podpisu, která je dostupná i jiným subjektům, než jen fyzickým osobám (firmy, organizace a organizační složky státu). Jde o tzv. **elektronickou značku**, která je

po technické stránce zaručeným elektronickým podpisem a nepředpokládá se, že by bezprostřední popud k jejímu vzniku musel vždy dávat člověk, který se nejprve seznámil s obsahem toho, co podepisuje. Elektronickou značku může již vytvářet i stroj, resp. aplikace, bez přímé účasti fyzické osoby (právní důsledky ale samozřejmě nese ten, kdo aplikaci nastavil tak, aby vytvářela elektronické značky).

Dalším důležitým pojmem je **časové razítko**. To je po technické stránce také zaručeným elektronickým podpisem, ale na rozdíl od něj ještě přidává garantovaný údaj o čase jeho vzniku. Časový údaj je převzat ze systémových hodin na počítači nebo serveru kde podpis vzniká. Tento čas si uživatel nebo administrátor ovšem může nastavit, jak chce. Z tohoto důvodu se na časový údaj v rámci elektronického podpisu nemůžeme vždy spolehnout. Z tohoto důvodu se v praxi používají spíše tzv. kvalifikovaná časová razítka, která jsou důvěryhodnější než časová razítka (bez přívlastku), protože je vytváří kvalifikovaný poskytovatel služeb (nejen časových razítek).

Tabulka 1: Rozdíly podpisů, značek a razítek

Zdroj [Vlastní tvorba]

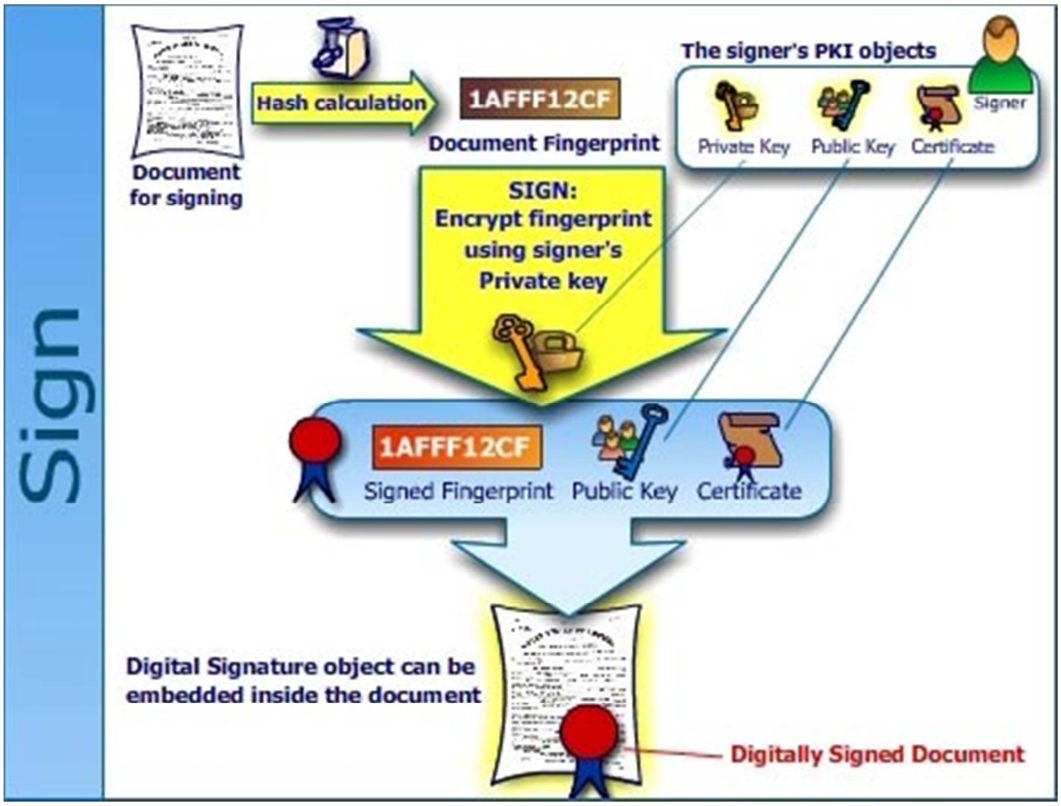
elektronický podpis	bez dalšího označení	podepsanou osobou může být pouze fyzická osoba
	Zaručený	
	Uznávaný	
elektronická značka	bez dalšího označení	označující osobou může být jak fyzická, tak i právnická osoba
	Uznávaná	
časové razítko	bez dalšího označení	
	kvalifikované	

1.5 Klíče, asymetrická kryptografie

Klíče jsou termínem, se kterým se při vytváření elektronického podpisu běžně operuje. Po technické stránce jsou to opět čísla, u kterých udáváme jejich délku v bitech. Nejdůležitější je oblast jejich použití při samotném vzniku a ověřování podpisu. Celý princip elektronického podpisu je v tom, že při vytváření podpisu (podepisování) a při ověřování podpisu se používá různá dvojice klíčů. Jde tedy o asymetrické řešení, u kterého rozlišujeme mezi **veřejným** (public key) a **soukromým** (private key**) klíčem**. Soukromý klíč (privátní) si musíme pečlivě hlídat, zabezpečit a neměli ho poskytovat dalším osobám, aby nedošlo k případnému zneužití. Důvodem je právě to, že soukromý klíč potřebujeme pro vytvoření vlastního elektronického podpisu a jednoznačně nás identifikuje. Veřejný klíč naopak můžeme a měli bychom poskytnout komukoli, kdo si bude chtít ověřit

platnost našeho podpisu, aby se mohl příjemce ujistit o platnosti našeho podpisu. Proto je díky asymetrické kryptografii zajištěno, aby soukromý a veřejný klíč (párová data) fungovaly tak, jak je zmíněno výše.

Vlastní podepsání elektronického dokumentu je celkem jednoduché, a to hlavně z toho důvodu, že za celý průběh zodpovídá specializovaný software, takže uživatel pouze zvolí dokument a vydá potřebný příkaz. Elektronický podpis přitom vzniká následujícím způsobem, který je zobrazen na obrázku 2. Vypočte se hash (hash calculation) dokumentu, tento se zašifruje s použitím privátního klíče (private key). Tím je elektronický podpis vytvořen a následně je přiložen k dokumentu (signed fingerprint). Příjemci se odešle původní dokument (ten není nijak šifrován ani jinak chráněn před zraky nepovolaných osob) spolu s veřejným klíčem (public key) a certifikátem (certificate). Příjemce pak postupuje tak, že k dokumentu znovu vypočte hash a pomocí veřejného klíče odšifruje elektronický podpis, čímž získá původní otisk - jejich porovnáním pak zjistí, zda dokument nebyl pozměněn, tj. zda se jedná skutečně o dokument, který odesilatel napsal a podepsal – princip podepsání dokumentu je znázorněn na obrázku níže, podrobněji bude princip vytváření a ověřování elektronického podpisu vysvětlen ve 2. a 3. kapitole.



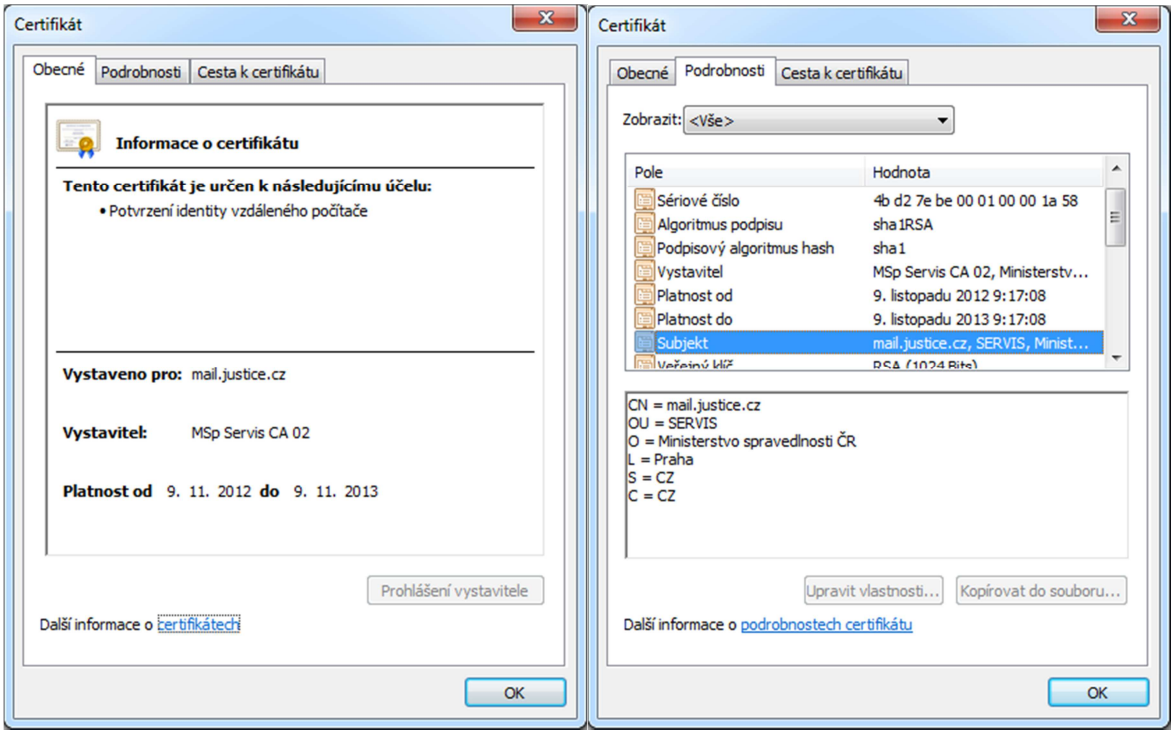
Obrázek 2: Podepsání dokumentu elektronickým podpisem

Zdroj [7]

1.6 Certifikáty

Certifikát je potvrzením o tom, že konkrétní veřejný klíč, vložený do certifikátu jako jeho součást, patří té osobě, jejíž identita je popsána v certifikátu. Současně zaručuje i to, že konkrétní osoba je držitelem odpovídajícího soukromého klíče. Proto, aby se příjemce mohl spolehnout na to, že skutečně jde o náš veřejný klíč, stačí využít nějakou dostatečně důvěryhodnou autoritu, která potvrdí, komu veřejný klíč patří. Aby potvrzení nemusela deklarovat pokaždé znovu, vystaví k tomu účelu jakési opakovaně využitelné potvrzení, které sama podepíše právě výše zmiňovaným certifikátem.

V praxi mohou být certifikáty buď osobními certifikáty (vydávány fyzickým osobám pro vytváření elektronických podpisů) nebo systémovými certifikáty (vydávány fyzickým i právnickým osobám pro vytváření elektronických značek, časových razítek a šifrované komunikace případně identifikaci serverů).



Obrázek 3: Systémový certifikát vydaný Ministerstvu spravedlnosti

Zdroj [Vlastní tvorba]

1.6.1 Komerční a kvalifikované certifikáty

Existuje také jiné dělení certifikátů na tzv. komerční certifikáty a kvalifikované certifikáty. Rozdíl mezi nimi je v tom, že požadavky na kvalifikované certifikáty a jejich obsah jsou

vymezeny v zákoně, zatímco v případě komerčních certifikátů zákon jejich obsah nevymezuje[2]. V praxi se používají osobní nebo systémové kvalifikované certifikáty pro podepisování a ověřování podpisů, značek a razítek. Komerční certifikáty mají širší oblast použití než kvalifikované certifikáty, které lze ze zákona použít jen pro první zmiňovaný účel. Na rozdíl od kvalifikovaných certifikátů nejsou však komerční certifikáty automaticky uznávány. Obě komunikující strany se musí dohodnout (např. smluvně), že budou důvěřovat komerční certifikační autoritě. Komerční certifikáty mohou být vydávány osobám i technologickým komponentám (aplikace, zařízení, servery) například pro následující účely:

- ověření elektronických podpisů,
- zajištění šifrované komunikace (např. aktivace šifrovaného SSL spojení),
- autentizace uživatelů - přihlášení do aplikací pomocí certifikátu.

Mezi komerční certifikáty patří i některé speciální druhy certifikátů jako například testovací nebo emailové certifikáty pro přístup k určité, většinou firemní, emailové schránce. Obsahu kvalifikovaného certifikátu můžeme ovšem věřit nejvíce, protože vydávající certifikační autorita zkoumá identitu fyzické nebo právnické osoby nejdůkladněji, a také za její správné zjištění ručí v nejvyšší možné míře.

1.6.2 Kvalifikované a akreditované certifikační autority

Vydavatel, který certifikát vydává je běžně označován jako **certifikační autorita**, zkratkou **CA**. Podle zákonů a vyhlášek je vydavatel označován jako poskytovatel certifikačních služeb. Certifikační autoritou může být i firemní serverová infrastruktura, která bude vydávat své vlastní certifikáty zaměstnancům pro přístup ke svým aplikacím nebo službám. Nejvíce nás ovšem budou zajímat tzv. **kvalifikované certifikační autority**. To jsou ty, které poskytují certifikační služby, vydávají kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů a splnily ohlašovací povinnost a všechny další požadavky[3]. Kterákoliv z kvalifikovaných certifikačních autorit může požádat stát, aby prověřil splnění všech požadavků zákona a v případě shody udělil této certifikační autoritě

[2] Zákon 220/2000 Sb., o elektronickém podpisu nezná pojem „komerční certifikát“, v praxi se pod tento pojem zahrnují všechny certifikáty, které nejsou kvalifikované.
[3] Podle §6 zákona 227/2000 Sb., o elektronickém podpisu

akreditaci. Akreditací se z kvalifikovaných certifikačních autorit stávají tzv. akreditované certifikační autority. Ministerstvo vnitra České republiky vykonává povinnosti stanovené zákonem č. 227/2000 Sb., o elektronickém podpisu, a stanovuje požadavky podle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, a to zejména:

- udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb,
- vyhodnocování shody nástrojů elektronického podpisu s požadavky stanovenými zákonem o elektronickém podpisu a prováděcí vyhláškou,
- ověřování kvalifikovaných certifikátů poskytovatelů certifikačních služeb, kteří požádali o udělení akreditace,
- provádění dozoru nad dodržováním zákona o elektronickém podpisu,
- vytváření postupů kvalifikovaných poskytovatelů certifikačních služeb,
- zabezpečování ochrany dat pro vytváření elektronických značek a časových razítek,
- ověřování zahraničních kvalifikovaných certifikátů.

Zpracovává také návrhy právních předpisů týkajících se elektronického podpisu a v jeho působnosti je rovněž zajištění mezinárodní spolupráce v této oblasti a plnění úkolů plynoucích z členství ČR v mezinárodních organizacích. V České republice nebyla v roce 2012 žádná kvalifikovaná certifikační autorita, která by nebyla současně akreditovaná.

Pro získání certifikátu u některé akreditované certifikační autority je nejprve potřeba si připravit zákonem vyžadované podklady pro uzavření smlouvy, a to občanský průkaz nebo pas u fyzické osoby a vyplněnou smlouvu o poskytování certifikačních služeb podepsanou statutárním zástupcem, výpis z obchodního rejstříku a doklad o jmenování statutárního zástupce u právnické osoby. Na kontaktním místě certifikační autority dojde během jedné návštěvy k uzavření smlouvy, zavedení do systému a vydání certifikátu, který má platnost jeden rok. Obnova a vystavení následného certifikátu už probíhá elektronickou cestou bez nutnosti návštěvy kontaktního místa (obnova musí proběhnut v období před koncem platnosti certifikátu). Za vydaný certifikát se platí v CZK.

Certifikační autorita plní dvě základní funkce:

- **certifikační** - zaručující, že deklarovaný veřejný klíč přísluší dané osobě,

- **validační** - potvrzující platnost certifikátu.

V případě certifikace se jedná o vydávání certifikátů uživatelům, kdy certifikát je dokument, který stvrzuje, že veřejný klíč (uvedený na certifikátu) patří jednoznačně dané osobě. Certifikát zároveň obsahuje další informace týkající se uživatele, doby platnosti klíče, informace o používání klíče a informace o certifikační autoritě. Certifikát je podepsán elektronickým podpisem certifikační autority. V případě komunikace mezi dvěma uživateli si uživatelé nejdříve ověří podpis svého partnera pomocí jeho veřejného klíče a posléze si ověří autentičnost veřejného klíče partnera ověřením podpisu certifikátu pomocí veřejného klíče certifikační autority. V daném případě se požadavek na důvěryhodnost vztahuje pouze k certifikační autoritě.

V případě validace se uživatel dotazuje u certifikační autority na platnost certifikátu svého partnera. Systém dotazů může být řešen on-line nebo i využitím seznamu neplatných certifikátů, tj. seznamu certifikátů, jejichž platnost byla ukončena před stanovenou dobou platnosti. Tzv. zaručený elektronický podpis neboli elektronický podpis založený na certifikátu v současné době vydávají tři schválené subjekty, které obdržely od Ministerstva vnitra ČR[4] oprávnění vydávat kvalifikované certifikáty. Jsou jimi:

Tabulka 2: Seznam certifikačních autorit

Zdroj [Vlastní tvorba]

Certifikační autorita	Cena kvalifikovaného certifikátu[5]
První certifikační autorita, a. s.	495,- včetně DPH (21%)
eIdentity, a.s.	474,- včetně DPH (21%)
PostSignum QCA (služba České pošty, s. p.)	396,- včetně DPH (21%)

Na závěr téhle podkapitoly bych rád shrnul výhody elektronického podpisu:

- Elektronický podpis umožňuje ověření identity podepisujícího - příjemce bezpečně ví, kdo je autorem či odesílatelem zprávy.
- Ověření integrity zprávy - příjemce má jistotu, že zpráva nebyla změněna v průběhu transportu, což ruční podpis může zajistit jen stěží.

[4] Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2, písm. e) zákona č. 227/2000 Sb.

[5] Uvedené ceny jsou platné na rok 2013 podle ceníků uveřejněných na webových stránkách jednotlivých autorit.

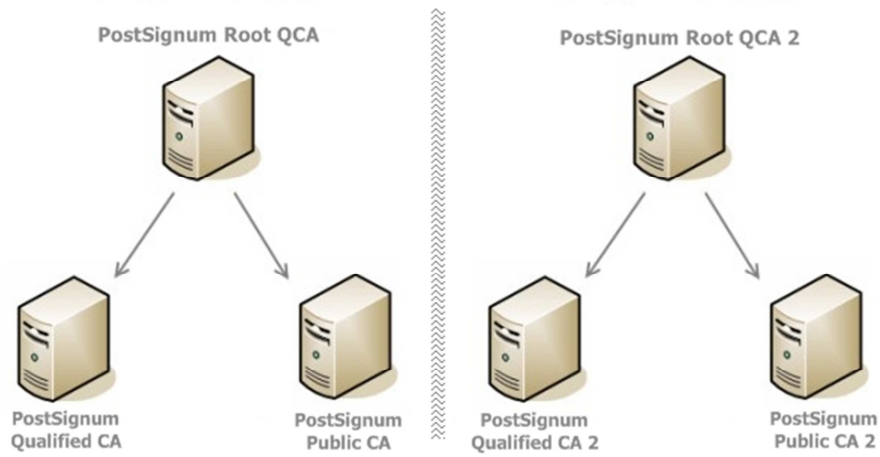
- Zaručuje nepopiratelnost zprávy - odesílatel nemůže popřít, že danou zprávu s daným obsahem opravdu odeslal.
- Nenapodobitelnost podpisu - prostředky k podpisování může mít daná osoba pod svou výhradní kontrolou.

1.6.3 Kořenové a podřízené certifikační autority

Certifikační autority, zejména ty akreditované, jsou z praktických důvodů často vnitřně členěny na **kořenové autority**, které vše zastřešují, a **podřízené autority**, které teprve vydávají různé druhy certifikátů koncovým zákazníkům. V diplomové práci budu popisovat veškeré technické řešení používané certifikační autoritou PostSignum, jejíž služby a certifikáty případová organizace používá k přístupu do datových schránek. Certifikační autorita PostSignum používá níže uvedené hierarchické členění – od počátku roku 2010, v souvislosti s přechodem na hashovací funkci SHA-256[6], jednu kořenovou certifikační autoritu (PostSignum Root QCA2) a dvě podřízené certifikační autority:

- PostSignum QCA 2 - vydává kvalifikované certifikáty, časová razítka a značky.
- PostSignum VCA 2 - vydává komerční certifikáty.

Na obrázku 4 je zobrazena stromová struktura certifikační autority PostSignum (kořenová autorita PostSignum Root QCA používala do konce roku 2009 hashovací funkci SHA-1).



Obrázek 4: Vnitřní členění CA PostSignum

Zdroj [8]

[6] SHA (Secure Hash Algorithm) je rozšířená hashovací funkce, která vytváří ze vstupních dat výstup (hash) fixní délky. Jeho hlavní vlastností je, že malá změna na vstupu vede k velké změně na výstupu, tj. k vytvoření zásadně odlišného otisku.

1.7 Právní legislativa

Jak už bylo řečeno, Ministerstvo vnitra vykonává povinnosti stanovené zákonem č. 227/2000 Sb., o elektronickém podpisu, a stanovuje požadavky podle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. Zpracovává také návrhy právních předpisů týkajících se elektronického podpisu a v jeho působnosti je rovněž zajištění mezinárodní spolupráce v této oblasti a plnění úkolů plynoucích z členství ČR v mezinárodních organizacích.

Certifikační autorita PostSignum splňuje podmínky kladené na kvalifikované poskytovatele certifikačních služeb a také požadavky kladené na bezpečnost jak na technologické úrovni, tak v oblasti předpisové základny:

- zákonem č. 227/2000 Sb., o elektronickém podpisu v platném znění,
- vyhláškou 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb,
- vyhláškou 212/2012 Sb., o ověřování platnosti zaručeného elektronického podpisu,
- zákonem č.101/2000 Sb., o ochraně osobních údajů.

1.7.1 Zákon č. 227/2000 Sb., o elektronickém podpisu

Dne 29. 6. 2000 byl ve Sbírce zákonů, částce 68, zveřejněn zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Smyslem zákona o elektronickém podpisu je umožnit použití digitálního podpisu v rámci elektronické komunikace jako ekvivalent vlastnoručního podpisu při běžné listinné formě komunikace, a také zavedení legislativního pořádku do oblasti používání elektronického podpisu. Je zde upřesněna používaná terminologie a definovány příslušné pojmy tak, aby byl odlišen stupeň důvěryhodnosti a bezpečnosti jednotlivých elektronických podpisů. Zákon byl vytvořen na základě směrnice Evropské unie 1999/93/EC ze dne 13. 12. 1999.

Dne 26. července 2004 nabyla účinnosti novela zákona o elektronickém podpisu (**č. 440/2004 Sb.**). Tento předpis nově zavedl pojem „kvalifikované časové razítko“, které prokazuje existenci elektronického dokumentu v čase. Další novinkou byla možnost používat „elektronické značky“. Pro ty se stejně jako pro zaručený elektronický podpis

používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy.

Dne 15. dubna 2010 nabyla účinnosti novela zákona o elektronickém podpisu (**č. 101/2010 Sb.**). Tento předpis v reakci na rozhodnutí Komise EU 2009/767/ES přidává Ministerstvu vnitra povinnost vést a zveřejňovat seznam důvěryhodných certifikačních služeb a stanoví orgánům veřejné moci povinnost uznávat kvalifikované certifikáty vydané v ostatních členských státech EU.

Dne 1. 7. 2012 nabyla účinnosti novela zákona o elektronickém podpisu (**č. 167/2012 Sb.**). Novela zavádí pojem „uznávaný elektronický podpis“ a „uznávanou elektronickou značku“. V návaznosti na přímo použitelný předpis Evropské unie - „Rozhodnutí Komise 2011/130/EU ze dne 25. února 2011, kterým se stanoví minimální požadavky na přeshraniční zpracování dokumentů elektronicky podepsaných příslušnými orgány podle směrnice 2006/123/ES Evropského parlamentu a Rady o službách na vnitřním trhu“, **stanovuje k podepisování nebo označování dokumentu** v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči státu; územnímu samosprávnímu celku; právnické osobě zřízené zákonem, zřízené nebo založené státem, územním samosprávním celkem nebo právnickou osobou zřízenou zákonem; právnické osobě vykonávající působnost v oblasti veřejné správy (týká-li se dokument této působnosti); fyzické osobě vykonávající působnost v oblasti veřejné správy (týká-li se dokument této působnosti), **používat uznávaný elektronický podpis nebo uznávanou elektronickou značku v referenčním formátu stanoveném v Rozhodnutí Komise 2011/130/EU.** Rovněž stanovuje postup pro případy, kdy není použit referenční formát. Zákon 227/2000 Sb., tak nově ukládá povinnosti i v oblasti používání elektronického podpisu.

1.7.2 Zákon č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů

Dne 2. 8. 2006 byla ve Sbírce zákonů zveřejněna vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb. 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 a značek. 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.

Druhá část vyhlášky ukládá kvalifikovaným poskytovatelům certifikačních služeb povinnost provádět audit systému řízení bezpečnosti informací (tuto povinnost může poskytovatel splnit i certifikací systému řízení bezpečnosti informací) podle normy ČSN BS 7799-2 – Systém managementu bezpečnosti informací – Specifikace s návodem pro použití. Tato norma byla zrušena a nahrazena normou ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. **Kvalifikovaní poskytovatelé certifikačních služeb mají z uvedeného důvodu provádět audit systému řízení bezpečnosti informací podle normy ČSN ISO/IEC 27001**, která normu vyjmenovanou ve vyhlášce nahrazuje. Vyhláška stanovuje, že při provádění auditu systému řízení bezpečnosti informací se postupuje podle požadavků normy ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu. Tato norma byla k 1. 7. 2012 zrušena a nahrazena ČSN EN ISO 19011 - Směrnice pro auditování systémů managementu.

1.7.3 Vyhláška č. 212/2012 Sb., o struktuře údajů a postupech ověřování

Dne 20. 6. 2012 byla ve Sbírce zákonů, částce 75 zveřejněna vyhláška 212/2012 Sb., o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu). V příloze vyhlášky jsou také uvedeny standardy kryptografických asymetrických algoritmů a hashovacích funkcí.

1.7.4 Další právní předpisy

Seznam dalších právních a vnitřních předpisů:

- **Směrnice Evropského parlamentu a Rady č. 1999/93/ES** ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.
- **Zákon č. 300/2008 Sb.**, o elektronických úkonech a autorizované konverzi dokumentů.
- **Zákon č. 499/2004 Sb.**, o archivnictví a spisové službě.

- **Nařízení generální ředitelky Vězeňské služby České republiky č. 4/2004** o vedení všeobecné administrativy.
- **Nařízení generálního ředitele Vězeňské služby České republiky č. 5/2011** o provozu datových schránek a elektronické podatelny ve Vězeňské službě České republiky.

1.8 Bezpečnost elektronického podpisu

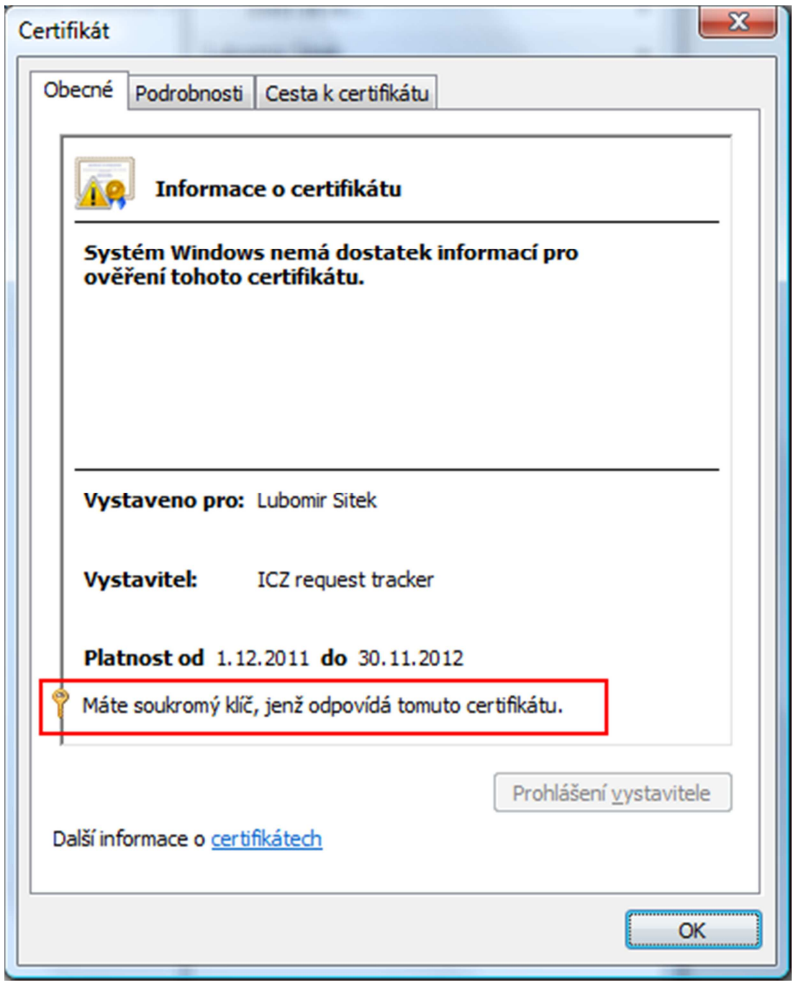
Ministerstvo vnitra zveřejňuje soubor doporučení pro osoby, které používají elektronický podpis. V případě, že je elektronický podpis používán pro „citlivé“ operace, např. internetové bankovnictví a finanční transakce obecně, je třeba věnovat těmto doporučením zvýšenou pozornost. Zákon č. 227/2000 Sb., o elektronickém podpisu stanoví podepisující osobě tyto povinnosti:

- zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu, s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření zaručeného elektronického podpisu (soukromý klíč); kvalifikovaný certifikát je následně zneplatněn.

Jako koncoví uživatelé chceme pracovat s elektronickým podpisem zcela rutinně. A to jak ověřovat platnost elektronických podpisů (či elektronických značek a časových razítek), které vytvořil někdo jiný, tak i vytvářet své vlastní elektronické podpisy na nejrůznějších elektronických dokumentech či zprávách. Případně využívat postupy, metody a technologie elektronického podpisu k dalším činnostem, například k šifrování, k bezpečnému přihlašování apod. Všechny tyto činnosti přitom mohou být na námi používaných počítačích maximálně usnadněny, při zachování nezbytných zásad bezpečnosti. V zásadě může být vše zredukováno jen na jediné kliknutí (ověření skrze zadání zabezpečujícího údaje, například hesla či PINu při vytváření podpisu).

V počítači jsou certifikáty ukládány do tzv. **úložiště (úložiště certifikátů,** anglicky **Certificate Store**, zkratkou **CS**). Certifikáty třetích stran, a nikoli „naše“ jsou plně veřejné a využívají se pouze pro vyhodnocování platnosti (cizích) podpisů, značek či razítek. Proto na spolehlivost jejich uložení nejsou kladeny žádné zvýšené požadavky a důvěrnost tohoto

uložení (tj. aby je nemohl získat někdo jiný) již není zapotřebí vůbec. Přesně opačné to je v případě našich osobních certifikátů, které chceme využívat při vytváření našich elektronických podpisů či dokonce značek. Tyto certifikáty jsou samy o sobě veřejné, takže jejich kompromitace by nás také nemusela nijak bolet. Problém je však v tom, že spolu s těmito certifikáty si do úložišť potřebujeme ukládat i jim odpovídající **soukromé klíče.**



Obrázek 5: Certifikát, se kterým je v úložišti uložen i odpovídající soukromý klíč

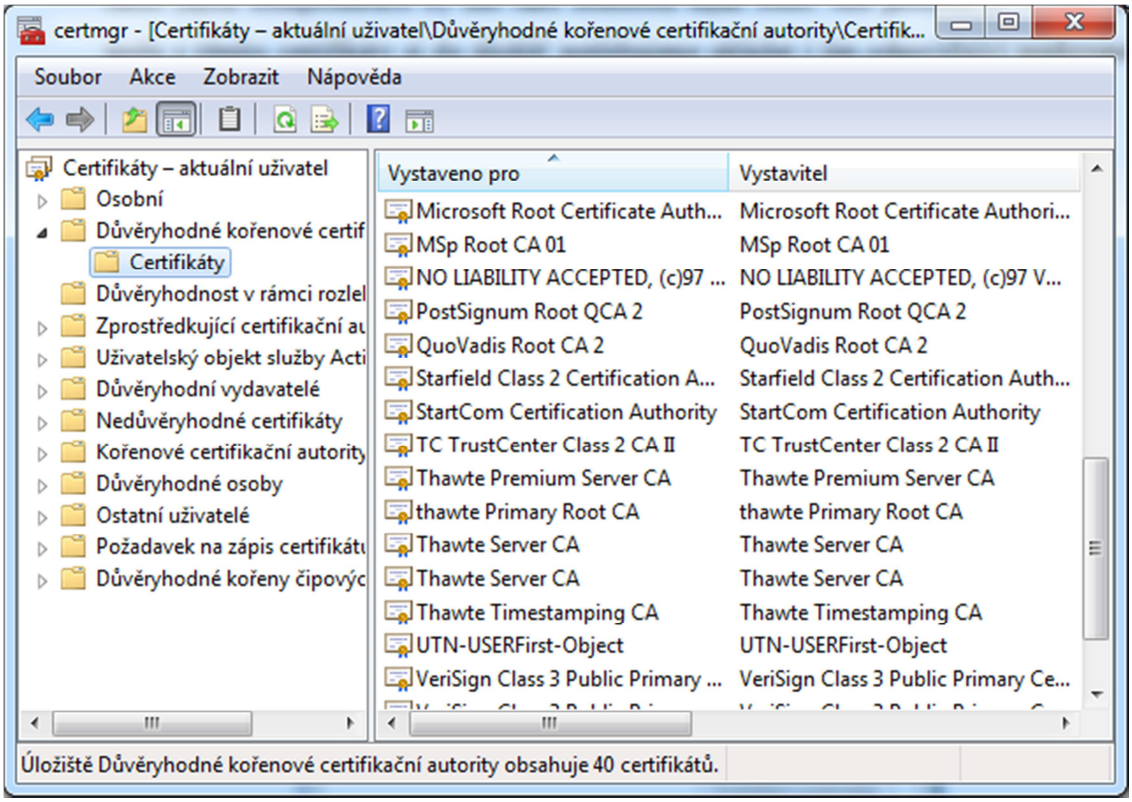
Zdroj [Vlastní tvorba]

A tady jsou již nároky na spolehlivost a důvěrnost uložení naopak velmi vysoké, protože případná kompromitace soukromého klíče (jeho zkopírování, smazání apod.) by byla zcela zásadním problémem (řešitelná situace předčasným zneplatněním certifikátu). Určitým řešením je aplikování zvýšené ochrany soukromého klíče v úložišti, která se uplatňuje v situacích, kdy má být se soukromým klíčem nějak manipulováno. Tedy při vytváření konkrétního elektronického podpisu. V prostředí Microsoft Windows (dále jen „MS“) máme k dispozici tři různé úrovně ochrany soukromého klíče, mezi kterými můžeme volit:

- **vysoká úroveň:** při každém požadavku na použití soukromého klíče bude nutná autentizace (zadání správného hesla),
- **střední úroveň:** každý požadavek na použití soukromého klíče je nutné explicitně odsouhlasit (odkliknout, ale bez nutnosti zadání hesla),
- **nízká úroveň:** při použití soukromého klíče nebude vyžadována žádná akce uživatele.

Nastavení těchto úrovní, včetně volby hesla, se provádí již při prvotním generování soukromého klíče. Stejně tak se ale provádí (znovu, s novou volbou hesla) při případném vkládání (importu) certifikátu i se soukromým klíčem do jiného úložiště.

Pokud jde o používání elektronického podpisu pro finanční operace a internetové komunikace obecně, je nutné si uvědomit, že používání libovolného nástroje má svoje výhody a nevýhody a že každá činnost je spojená s určitým rizikem. Proto je vždy nutné najít vhodnou hranici mezi užitkem, mírou rizika a investicí do zabezpečení. A míru rizika minimalizovat.



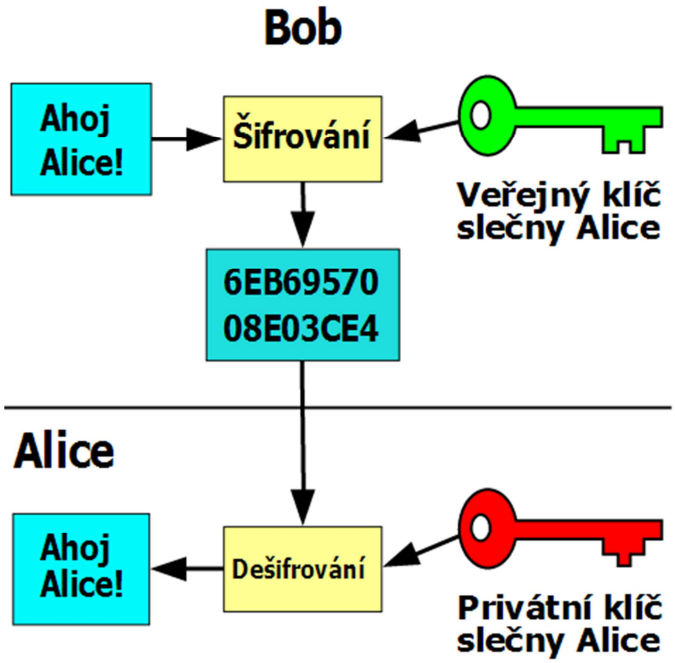
Obrázek 6: Úložiště certifikátů v prostředí Microsoft Windows

Zdroj [Vlastní tvorba]

2 PRINCIP VYTVÁŘENÍ ELEKTRONICKÉHO PODPISU

V této kapitole podrobněji popíši podstatu elektronického podpisu, zejména způsob jeho vzniku, který je založen na asymetrické kryptografii a na infrastruktuře veřejného klíče.

Jak už bylo okrajově zmíněno v kapitole 1.5, asymetrická kryptografie se od symetrické liší používáním dvojice klíčů. Umožňuje výměnu klíčů v nezabezpečeném prostředí a uplatnění najde i v oblasti elektronického podpisu. Pokud si dříve chtěli lidé vyměňovat šifrované zprávy, museli se buď sejít, nebo jiným způsobem si doručit společný klíč pro symetrickou šifru. Při použití asymetrické kryptografie žádná schůzka není nutná. Každý má svůj veřejný klíč, který může druhé straně poslat například elektronickou poštou bez obav z jeho zneužití, protože z jednoho klíče není možné v „rozumném“ čase odvodit klíč druhý a zprávu zašifrovanou veřejným klíčem je schopen dešifrovat pouze majitel správného soukromého klíče. Strany si vymění veřejné klíče a může začít šifrovaná komunikace.



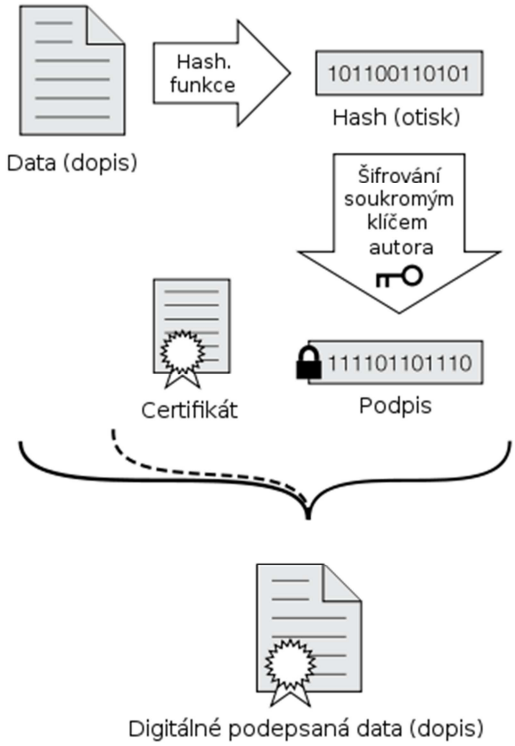
Obrázek 7: Asymetrické šifrování

Zdroj [9]

Jenže toto není způsob, který by byl využíván pro elektronický podpis. Ten totiž pracuje na opačném principu. Co je naším cílem při obdržení elektronicky podepsaného dokumentu? Zjistit, zda jej podepsal skutečně člověk, uvedený jako odesilatel. I k tomuto můžeme využít asymetrické kryptografie. Pokud někdo zašifruje dokument svým soukromým klíčem, jsou jej schopni dešifrovat naprosto všichni. To je naprosto

nepřijatelné pro šifrovanou komunikaci, ale nám plně vyhovující. Položme si nyní otázku, kdo mohl zašifrovat zprávu, kterou jsme obdrželi a dešifrovali pomocí veřejného klíče? Nikdo jiný, než majitel soukromého klíče. A pokud je držen soukromý klíč v tajnosti, je to jediná osoba. Tím jsme se dostali k principu elektronického podpisu.

Chybí nám jistota, že klíč vlastní opravdu ten jedinec, který je uveden jako odesílatel a ne jen někdo, kdo se za něj vydává. Využijeme služeb důvěryhodné třetí strany neboli certifikační autority. Ta za nás ověří identitu podepisující osoby, zkontroluje její veřejný klíč a proces zakončí vydáním certifikátu, který stvrzuje vazbu mezi osobou a klíčem. Po obdržení podepsané zprávy, ověříme platnost certifikátu a můžeme si být jisti, že nám píše skutečně osoba v certifikátu uvedená. Certifikát není vstupem pro šifrovací proces, nejčastěji je pouze přílohou.



Obrázek 8: Princip vytvoření elektronického podpisu

Zdroj [12]

Nyní můžeme dokončit postup podepisování v praxi. Nejprve máme datovou zprávu, kterou chceme podepsat. Tu, protože její podepisování by trvalo dlouho[7], necháme projít

[7] Nevýhodou asymetrické kryptografie je její malá rychlost. Její použití je značně pomalejší, než u symetrických šifer. Proto se u elektronického podpisu používá ještě jeden mezikrok. Tím je využití hashovací funkce.

hashovací funkcí a získáme tak její krátký otisk. Pro potřeby elektronického podpisu se v současnosti využívá algoritmus SHA-256 s RSA šifrováním a s veřejným klíčem podepisující osoby o velikosti 2048 nebo 4096 bitů. RSA je šifra s veřejným klíčem a jedná se o první algoritmus, který je vhodný jak pro podepisování, tak šifrování. Při dostatečné délce klíče je považován za bezpečný. Otisk podepíšeme (zašifrujeme soukromým klíčem) a připojíme k datové zprávě. Datovou zprávu s podepsaným hashem odešleme příjemci. Podrobnosti o hashovací funkci jsou uvedeny v kapitole 2.3.

2.1 Nástroje a data pro vytváření elektronického podpisu

Nástrojem pro vytváření elektronického podpisu je myšlena aplikace, pomocí které budeme svůj elektronický podpis vytvářet. Aplikace pro vytváření elektronických podpisů přitom nemusí mít pouze jednoúčelovou formu, která slouží právě a pouze k podepisování. Může jít o jednu z funkcí nějaké aplikace, která primárně slouží k jiným účelům (jako kancelářské balíky MS Office, virtuální tiskárny pro tvorbu PDF dokumentů nebo různé personální a mzdové aplikace). Aplikaci pro vytváření elektronického podpisu nemusíme nějak specificky chránit proti zcizení, aby se nedostal do rukou někomu jinému, naopak data pro vytváření ano. Daty je podle zákona o elektronickém podpisu myšlen soukromý klíč uživatele, využívaný při tvorbě zaručeného elektronického podpisu.

2.2 Zabezpečení integrity podepsaného dokumentu

Zabezpečením integrity není myšleno zabránění jakýmkoli změnám podepsaného dokumentu, ale je myšlena možnost spolehlivě rozpoznat, pokud by k nějaké změně došlo. Má-li elektronický podpis zajišťovat integritu podepsaného dokumentu, musí být na tomto dokumentu nějakým způsobem závislý. Musí určitou formou odrážet jeho obsah, aby při sebemenší změně tohoto obsahu již podpis neodrážel korektně jeho obsah.

2.3 Hashování a hashovací funkce

Důvodem pro potřebu hashování je to, že při podepisování (ale i při označování, neboli při vytváření elektronických značek, stejně jako při vytváření časových razítek, při šifrování apod.) potřebujeme pracovat s bloky dat o pevné velikosti. Metody a algoritmy, které se k podepisování používají, jsou takhle navrženy. Navíc je vhodné i to, aby ony bloky pevné velikosti byly dostatečně malé, aby jejich zpracování (nejen v rámci elektronického

podepisování, ale třeba i šifrování) mohlo být dostatečně rychlé. Proto se při tvorbě elektronického podpisu nešifruje privátním klíčem odesilatele celá zpráva, ale nejprve se na zprávu použije hashovací funkce. Hash je matematická funkce, která z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky. Výsledný řetězec (otisk) by měl maximálně charakterizovat původní text.

Ještě v roce 2009 se i v oblasti elektronického podpisu nejčastěji používala hashovací funkce SHA-1. SHA navrhla organizace NSA (Národní bezpečnostní agentura v USA) a vydal NIST (Národní institut pro standardy v USA) jako americký federální standard. SHA je rodina pěti algoritmů: SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. Poslední čtyři varianty se souhrnně uvádějí jako SHA-2. SHA-1 vytvoří obraz zprávy dlouhý 160 bitů. Čísla u ostatních čtyř algoritmů značí délku výstupního otisku v bitech. Z hlediska bezpečnosti musí hashovací funkce splňovat následující požadavky:

- **Odolnost vůči získání předlohy** - pro všechny výstupy z hashovací funkce je výpočetně nemožné získat vstup, kterému odpovídá daný otisk. Z dané hash hodnoty nelze získat původní dokument.
- **Odolnost vůči získání jiné předlohy** - je výpočetně prakticky nemožné najít dokument, jehož hash hodnota odpovídá hash hodnotě původního dokumentu.
- **Odolnost vůči nalezení kolize** - je prakticky nemožné najít dva dokumenty se stejnou hash hodnotou.

Kryptografické algoritmy, které mohou být používány v oblasti elektronického podpisu, musí respektovat neustálý rozvoj v oblasti kryptoanalýzy a výpočetních technologií. Z toho důvodu ustupuje Česká republika stejně jako ostatní členské státy EU od používání dosud využívaného algoritmu SHA-1, jehož ukončení nařídilo v roce 2010 Ministerstvo vnitra ČR vydáním informací k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu. [10] Dokument implementuje směrnici ETSI TS 102 176-1 V2.0.0 (2007-11), vydanou Evropským ústavem pro telekomunikační normy (European Telecommunications Standards Institute, ETSI). Ministerstvo vnitra se při zveřejňování kryptografických algoritmů a jejich parametrů řídí touto směrnicí a stanoví pro jednotlivé algoritmy dobu, po kterou lze předpokládat, že budou považovány za bezpečné, jak lze vidět v Tabulce č. 3. Podle směrnice bylo nezbytné ukončit používání hashovací funkce třídy SHA-1 a nahradit ji bezpečnější hashovací funkcí třídy SHA-2. Poskytovatelé certifikačních služeb v České republice ukončili používání algoritmu SHA-1

při vydávání kvalifikovaných certifikátů k 31. 12. 2009. V současné době je aktuální směrnice ETSI TS 102 176-1 V2.1.1 (2011-07) vydaná v roce 2011. [11]

Tabulka 3: Doporučené hashovací funkce

Zdroj [11]

entry name of the hash function	1 year	3 years	6 years	10 years (speculative)
sha1	unusable	unusable	unusable	unusable
ripemd160	unusable	unusable	unusable	unusable
sha224	usable	usable	usable	unknown
sha256	usable	usable	usable	unknown
sha384	usable	usable	usable	usable
sha512	usable	usable	usable	usable
Whirlpool	usable	usable	usable	usable

Směrnice stanovuje také následující délky klíčů pro tvorbu elektronického podpisu s využitím algoritmu RSA.

Tabulka 4: Doporučené parametry délky klíčů algoritmu RSA

Zdroj [11]

Parameter	1 year	3 years	6 years	10 years (speculative)
MinModLen	1 536	2 048	2 048	?

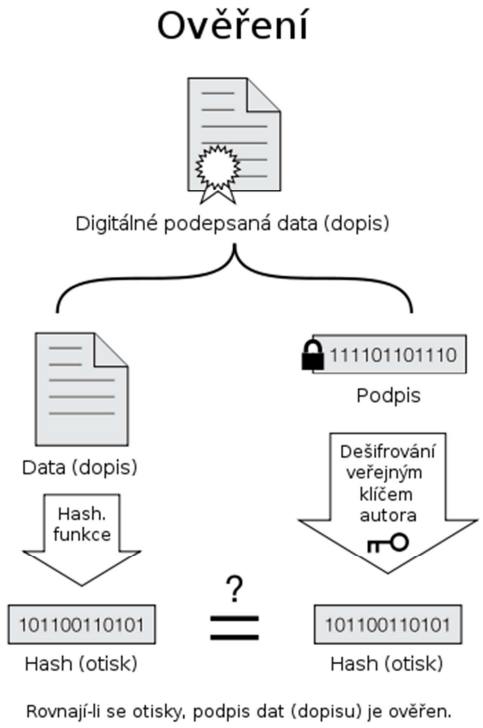
Z tabulky je zřejmé, že délka klíče 1024 bitů pro algoritmus RSA je již považována za nedostatečnou.

Zákon o elektronickém podpisu sice neumožňuje ministerstvu vnitra přikazovat nebo omezovat použití konkrétních kryptografických algoritmů uživatelům elektronického podpisu, jeho pravomoc ovšem sahá k akreditovaným poskytovatelům certifikačních služeb, kteří musejí veškeré změny a bezpečnostní pravidla zapracovat do své certifikační politiky, kterou jsou povinni respektovat a dodržovat všichni uživatelé elektronického podpisu.

3 PRINCIP OVĚŘENÍ ELEKTRONICKÉHO PODPISU

Práce s elektronickými podpisy neobnáší pouze jejich vytváření a přidávání ke konkrétním elektronickým dokumentům, stejně tak je nutné tyto podpisy následně vyhodnocovat. Tedy zabývat se tím, zda lze ověřit a prokázat jejich platnost.

Příjemce obdrží zprávu, z certifikátu pozná, kdo mu zprávu posílá a použije příslušný veřejný klíč. Tím, že hash rozšifruje veřejným klíčem, který je uveden v certifikátu, ověří, že mu zprávu odeslal opravdu držitel certifikátu. Následně spočítá z datové zprávy svůj hash (na Obrázku 9 je označen na levé straně). Porovná svůj hash s dešifrovaným hashem od odesílatele. Pokud jsou si hashe rovny, nebyl změněn obsah datové zprávy od doby jejího podepsání. Tím si ověřil integritu obsahu. Pokud by si chtěly dva subjekty vyměňovat podepsané a ještě i šifrované zprávy, použijí i symetrickou šifru pro zašifrování obsahu. Podepsaná zpráva není totiž šifrovaná a může si ji tedy kdokoliv přečíst.



Obrázek 9: Princip ověření elektronického podpisu

Zdroj [12]

3.1 Základní pravidla ověření elektronického podpisu

Ze všeho nejdříve naznačím některé základní skutečnosti a pravidla pro získání vhodného nadhledu a potřebného povědomí o celé problematice ověřování platnosti elektronických

podpisů. Celé vyhodnocování elektronického podpisu může skončit třemi různými variantami výsledku:

- zjištěním, že elektronický podpis je **platný** - jsme schopni ověřit a prokázat platnost podpisu,
- zjištěním, že elektronický podpis je **neplatný** - jsme schopni ověřit a prokázat neplatnost podpisu,
- zjištěním, že **„nevíme“** (že platnost podpisu nedokážeme posoudit, že nejsme schopni ověřit, zda podpis je či není platný).

Při samotném zkoumání platnosti elektronického podpisu musí být provedeno více různých úkonů, či alespoň vzato do úvahy více různých skutečností a faktorů. Musí být ověřena integrita podepsaného dokumentu. Ta je pro platnost elektronického podpisu podmínkou nutnou, nikoli ale postačující:

- je-li integrita porušena, můžeme rovnou konstatovat, že podpis je neplatný, ve smyslu varianty 2 předchozího výčtu (proto podmínka nutná),
- opačně to ale rozhodně neplatí: je-li integrita podepsaného dokumentu neporušená, podpis může být platný, ale také nemusí. Stále tedy připadá v úvahu jak varianta 1, tak i varianty 2 a 3 (ve smyslu předchozího výčtu), a rozhodují mezi nimi další faktory.

Dále musí být ověřena platnost certifikátu, na kterém je podpis založen, a to k posuzovanému okamžiku. Jde opět o podmínku nutnou, ale ne postačující (pro variantu 1 v předchozím výčtu, tedy pro platnost podpisu). Nejprve je tedy nutné určit posuzovaný okamžik:

- platnost certifikátu k posuzovanému okamžiku je třeba hodnotit ze dvou různých pohledů současně - podle jeho řádné platnosti, která je v certifikátu uvedena, a dále podle toho, zda k posuzovanému okamžiku nebyl certifikát revokován (předčasně zneplatněn).

K tomu, aby mohl být certifikát shledán platným, musí být splněny obě dílčí podmínky - jeho řádná platnost (k posuzovanému okamžiku) ještě nesměla skončit, a certifikát nesměl být (k posuzovanému okamžiku) revokován. Pokud kterákoli z podmínek splněna není, certifikát nemůže být hodnocen jako platný. Stejným způsobem musí být ověřena platnost všech nadřazených certifikátů na certifikační cestě (tj. nadřazených tomu certifikátu,

na kterém je založen zkoumaný elektronický podpis). Není-li kterýkoli z nadřazených certifikátů (k posuzovanému okamžiku) platný, je výsledek ověření platnosti podpisu různý podle toho, co je důvodem neplatnosti certifikátu:

- pokud byl některý z nadřazených certifikátů k posuzovanému okamžiku revokován (předčasně zneplatněn), pak je nutné konstatovat, že podpis je neplatný (ve smyslu varianty 2),
- pokud k posuzovanému okamžiku již skončila řádná platnost nadřazeného certifikátu.

Konstatovat platnost elektronického podpisu (ve smyslu varianty 1, tedy ve smyslu naší schopnosti ověřit a prokázat platnost) můžeme pouze při „kladném“ souběhu tří logických podmínek:

- integrita podepsaného dokumentu nebyla porušena,
- certifikát, na kterém je podpis založen, byl k posuzovanému okamžiku platný (ještě neuplynula doba jeho řádné platnosti). Aby mohl být platný, musejí být platné i všechny jeho nadřazené certifikáty,
- certifikát, na kterém je podpis založen, nebyl k posuzovanému okamžiku revokován (předčasně zneplatněn). Totéž musí platit i pro všechny nadřazené certifikáty.

Relativně nejjednodušším úkonem, v rámci vyhodnocování platnosti elektronického podpisu, je ověření integrity podepsaného dokumentu. Tedy zjištění toho, zda od podpisu došlo k nějaké (jakékoli) změně dokumentu (což znamená porušení integrity), nebo zda k žádné změně nedošlo (což znamená neporušenou integritu). Způsob ověření integrity přitom vychází ze základních principů asymetrické kryptografie, kterou jsem popsal ve druhé kapitole.

3.1.1 Seznam zneplatněných certifikátů

Certifikační autorita vydává v pravidelných intervalech tzv. seznam zneplatněných certifikátů (Certificate Revocation List, CRL). V něm jsou zapsány informace o certifikátech, které jejich vlastníci prohlásili za neplatné (nechali je zneplatnit). K tomu dochází např. tehdy, když je zcizen soukromý klíč vlastníka nebo skončí podmínky pro používání certifikátu.

II. PRAKTICKÁ ČÁST

4 ÚVOD DO PROBLEMATIKY

Prvotním impulzem pro zpracování optimalizace podávání evidenčních listů důchodového pojištění byl požadavek vedení organizace k trvalému zjednodušování administrativy, zrychlování komunikace a snižování finančních nákladů ve Vězeňské službě České republiky (dále jen „VS ČR“). V organizaci pracuji jako vedoucí oddělení informatiky na organizační jednotce Věznice Břeclav, a dále také jako dispečer pro mobilní a Exchange komunikace. V dané oblasti již s certifikáty pracuji, proto mě napadla myšlenka optimalizace podávání evidenčních listů s využitím zabezpečení PKI[8] namísto klasického tištěného podávání.

Posláním Vězeňské služby ČR je zajišťovat výkon vazby, výkon trestu odnětí svobody a bezpečnost a pořádek v soudních budovách. Vězeňská služba spravuje a střeží věznice a detenční ústavy. Dále střeží, předvádí a eskortuje vězněné osoby. K dalším úkolům patří výzkum v oboru penologie, jehož výsledky aplikuje v praxi. V České republice se nachází 36 věznic, z toho 10 vazebních a dva detenční ústavy, celkový počet vězněných osob je 22 644 (údaje k datu 31. 12. 2012). [15]

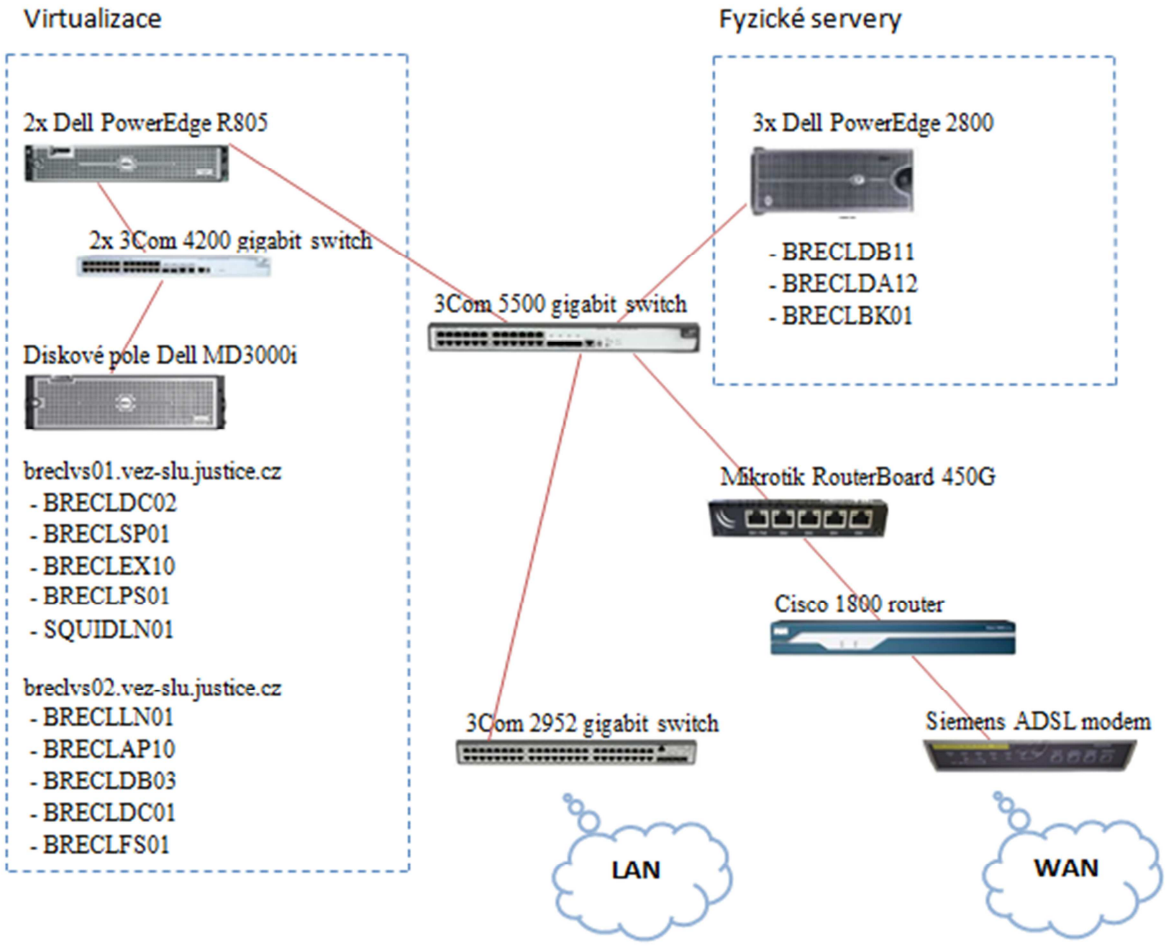
Obrázek 10: Věznice, vazební věznice a detenční ústavy v ČR

Zdroj [13]

[8] Public Key Infrastructure je soubor hardware, software, lidí, metod a politik, který slouží k jednoznačnému přiřazení veřejného klíče konkrétní entitě při využití elektronického podpisu.

4.1 Popis serverové infrastruktury

Každá organizační jednotka má vlastní serverové centrum, které se nachází v administrativní budově v klimatizované místnosti s omezeným přístupem. Servery běží nepřetržitě (24 hodin denně, 7 dní v týdnu) a zajišťují přístup uživatelů do domény, a dále k databázovým, souborovým a tiskovým službám. Větší část serverů běží na virtualizační technologii od společnosti VMware. Doména je založena na prostředí Microsoft Windows a spravována pomocí Active Directory[9]. Zálohování probíhá po síti na servery, které jsou vybaveny páskovou mechanikou v mimo pracovní část dne. Zapojení infrastruktury je hvězdicového typu, jak je zobrazeno na následujícím obrázku.



Obrázek 11: Serverová infrastruktura

Zdroj [Vlastní tvorba]

[9] Active Directory je implementace adresářových služeb firmou Microsoft pro použití v prostředí systému Microsoft Windows. Active Directory umožňuje administrátorům nastavovat politiky, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře.

4.2 Evidenční list důchodového pojištění

Vedení evidenčních listů důchodového pojištění (dále jen „ELDP“) je jednou z povinností zaměstnavatelů uloženou zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů. Zaměstnavatel vede ELDP pro každou osobu účastnou důchodového pojištění vždy za jednotlivý kalendářní rok, případně jeho část, došlo-li k zahájení výdělečné činnosti zakládající účast na důchodovém pojištění nebo k jejímu ukončení v průběhu kalendářního roku. ELDP se vede i pro poživatele starobního důchodu, který ještě nedovršil důchodový věk (tzv. poživatel předčasného starobního důchodu, jemuž výplata starobního důchodu po nástupu do zaměstnání nenáleží) a za rok 2009 i pro poživatele starobního důchodu výdělečně činného po dovršení důchodového věku, pokud byl kdykoliv v minulosti nebo byl v roce 2009 účasten důchodového pojištění v cizině. Od 1. 1. 2010 s ohledem na změnu právní úpravy ve vztahu k nárokům na zvýšení důchodu za dobu výdělečné činnosti při pobírání starobního důchodu je nutno vést ELDP i pro všechny poživatele starobního důchodu.

Za každý kalendářní rok po účetní závěrce (závěrce mzdových listů), nejpozději však do 30. dubna následujícího kalendářního roku, a v případě skončení účasti na důchodovém pojištění před 31. 12. daného kalendářního roku do 1 měsíce po konečném vyúčtování příjmů, nejpozději do 31. ledna následujícího kalendářního roku se do ELDP zapisují:

- identifikační údaje zaměstnavatele,
- jméno, poslední příjmení, rodné příjmení, datum a místo narození, místo trvalého pobytu a rodné číslo občana,
- druh výdělečné činnosti,
- doba účasti na důchodovém pojištění,
- doba důchodového pojištění,
- vyměřovací základ pro pojistné na sociální zabezpečení a příspěvek na státní politiku zaměstnanosti,
- doby, které se při stanovení osobního vyměřovacího základu při výpočtu důchodu vylučují,

- doby, které se ode dne dosažení věku potřebného pro vznik nároku na starobní důchod nepovažují za výkon výdělečné činnosti pro účely zvýšení procentní výměry starobního důchodu.

Zaměstnavatel je povinen vyhotovit stejnopisy evidenčního listu. Jeden stejnopis je povinen předložit občanovi k podpisu a založit do své evidence a druhý stejnopis, který opatří podpisem pověřeného zaměstnance nebo jiného oprávněného zástupce a svým razítkem, je povinen vydat občanovi, a to nejpozději v den, kdy předkládá evidenční list příslušnému orgánu sociálního zabezpečení. Evidenční listy se předkládají České správě sociálního zabezpečení prostřednictvím Okresní správy sociálního zabezpečení, v jejímž obvodu je útvar zaměstnavatele, ve kterém je vedena evidence mezd. Jde-li o osoby ve služebním poměru, nebo o občana, jemuž vznikl nárok na důchod z důchodového pojištění příslušníků ozbrojených sil, předkládá se evidenční list orgánům ministerstev obrany, vnitra nebo spravedlnosti podle toho, který orgán je příslušný k rozhodování o dávkách důchodového pojištění. Zaměstnavatel je povinen předložit evidenční list:

- do 30 dnů ode dne zápisu údajů do evidenčního listu (zápis se provádí za každý kalendářní rok po účetní závěrce nejpozději však do 30. dubna následujícího kalendářního roku); skončilo-li zaměstnání před 31. prosincem a je nepochybné, že občan nejpozději do 3 měsíců opět ve stejném kalendářním roce do zaměstnání u stejného zaměstnavatele nastoupí, nemusí být evidenční list předložen a lze pokračovat v záznamech na dřívějším evidenčním listu,
- do 30 dnů ode dne svého zániku,
- do 8 dnů ode dne obdržení výzvy orgánů sociálního zabezpečení.

Při úmrtí občana se předkládá evidenční list důchodového pojištění:

- na vyžádání orgánu sociálního zabezpečení ve lhůtě jím určené,
- do 3 měsíců od úmrtí, nebyl-li do té doby evidenční list vyžádán orgány sociálního zabezpečení.

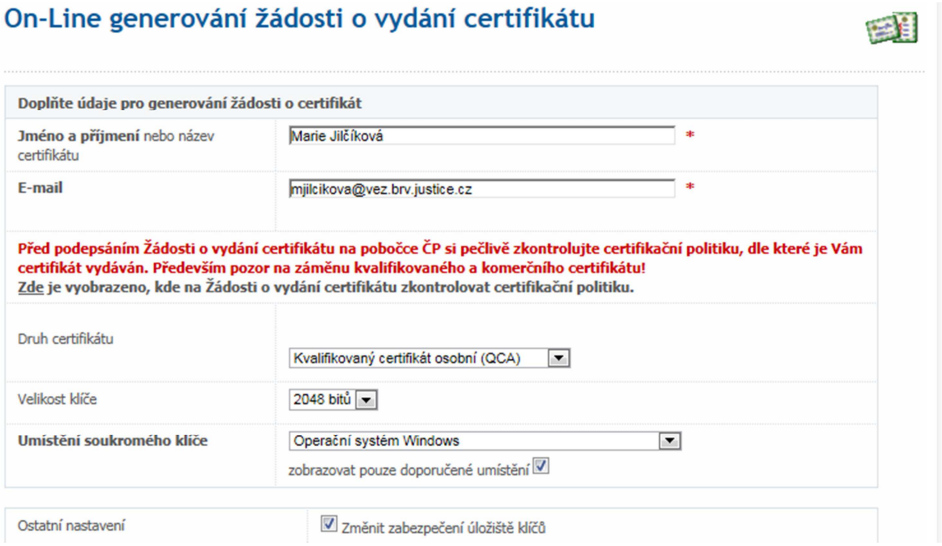
ELDP se předkládají buď na předepsaných tiskopisech vydaných Českou správou sociálního zabezpečení (příloha P I) nebo je možné namísto tiskopisu předkládat i formou **elektronického podání podávaného přes podatelnu VREP**. VREP (veřejné rozhraní pro e - podání) je nové komunikační rozhraní (komunikační kanál), vybudované Českou správou sociálního zabezpečení, pro příjem elektronických podání. Elektronické podání

obsahuje datové věty ELDP v elektronické podobě v definovaném formátu. Před odesláním ELDP na rozhraní VREP je nutné dávku podepsat kvalifikovaným certifikátem. Před využíváním služeb elektronického podání je nutná registrace na České správě sociálního zabezpečení (dále jen „ČSSZ“), kdy je současně zaevidován kvalifikovaný certifikát uživatele, který bude podání realizovat. Kvalifikovaný certifikát je v systému ČSSZ použit k identifikaci a autorizaci klienta. Pokud dojde k zaslání dokumentu podepsaným platným kvalifikovaným certifikátem, jehož identifikátory (viz kapitola 4.3.1) ČSSZ klient nesdělil, podání bude zamítnuto. Registraci je možné uskutečnit elektronicky bez osobní návštěvy Okresní správy sociálního zabezpečení, za předpokladu, že vyplněný tiskopis „Oznámení o pověření k zajištění všech úkonů souvisejících
s e-podáním ČSSZ“ (příloha P V), podepsaný platným kvalifikovaným certifikátem statutárního zástupce zaměstnavatele, případně jiné oprávněné osoby, bude zaslán elektronicky do e-podatelny nebo datové schránky příslušné ČSSZ.

4.3 Generování žádosti o certifikát

Pro každý certifikát konkrétního uživatele musí být vygenerována samostatná žádost. Pokud ještě některá organizační jednotka nevyužívá služeb PostSignum, je nutné uzavřít smlouvu o poskytování certifikačních služeb (příloha P II), úvodní list (příloha P III) a údaje pro vydání certifikátu (příloha P IV) s Českou poštou. Před samotným generováním žádosti o certifikát musí uživatel postupovat podle následujících kroků. Z níže uvedeného postupu bude vytvořen manuál pro zřízení certifikátu, který bude metodickou pomůckou organizačním jednotkám a bude uložen na intranetu VS ČR:

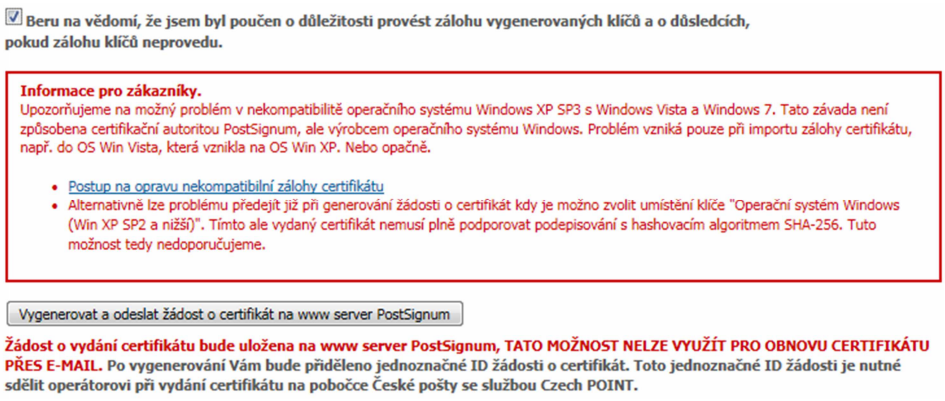
- na stránce http://www.postsignum.cz kliknout na odkaz „Generování žádosti o certifikát“,
- ve formuláři vyplnit jméno, příjmení a email uživatele (druh certifikátu, velikost klíče a umístění soukromého klíče ponechat ve výchozích hodnotách),
- v ostatním nastavení zaškrtnout volbu „Změnit zabezpečení úložiště klíčů“ (z důvodu zajištění vysoké úrovně zabezpečení uložených klíčů a vyžadování hesla při každém podpisu) a volbu „Beru na vědomí, že jsem byl poučen o důležitosti provést zálohu vygenerovaných klíčů a o důsledcích, pokud zálohu klíčů neprovedu“ (pro případ havárie počítače, poškození úložiště klíčů nebo potenciální ztráty soukromého klíče),



Obrázek 12: Generování žádosti o certifikát

Zdroj [Vlastní tvorba]

- nakonec je nutné žádost vygenerovat kliknutím na tlačítko „Vygenerovat a odeslat žádost o certifikát na www server PostSignum“ (po vygenerování přijde uživateli emailem jednoznačné ID žádosti o certifikát, které je nutné sdělit operátorovi na pobočce České pošty se službou Czech POINT[10]).



Obrázek 13: Odeslání žádosti o certifikát

Zdroj [Vlastní tvorba]

4.3.1 Standard X.509

Kvalifikovaná certifikační autorita PostSignum Qualified CA vydává certifikáty odpovídající standardu X.509 verze 3. Standard ITU-T X.509[11] je mezinárodně platné

[10] Český Podací Ověřovací Informační Národní Terminál slouží jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa.
[11] Mezinárodní telekomunikační unie (International Telecommunication Union) připravuje technické specifikace pro telekomunikační systémy, sítě a služby, včetně jejich provozu, fungování a údržby.

doporučení, které popisuje formu využití PKI. Každá certifikační autorita vydává svou certifikační politiku, která stanoví pravidla a postupy pro vydávání kvalifikovaných certifikátů pro osobní použití, obsahuje informace o struktuře vydávaných certifikátů, výčet povolených použití vydávaných certifikátů, poskytovaných služeb a zásady nakládání s certifikáty. Podpisem smlouvy případně žádosti o vydání certifikátu žadatel stvrzuje, že se seznámil s obsahem certifikačních politik. Při podepisování smlouvy, zejména v příloze seznamu žadatelů (příloha P IV), uvádí žadatel o certifikát standardem požadované údaje. Jméno osoby, užívající vydaný certifikát, je uvedeno ve jménu certifikátu. Certifikáty jsou vydávány zákazníkům, resp. zaměstnancům zákazníků (organizací), které stanoví zástupce organizace. Při tvorbě certifikačních politik a certifikační prováděcí směrnice, je zejména přihlíženo k následujícím dokumentům:

- CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements,
- ČSN ISO/IEC 27001: 2006 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky,
- ČSN ETSI TS 101 456 Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty,
- ČSN ISO/IEC TR 13335: Informační technologie – Směrnice pro řízení bezpečnosti IT,
- ČSN ISO/IEC 17799: Informační technologie – Bezpečnostní techniky Soubor postupů pro management bezpečnosti informací RFC 2511 – Internet X.509 Certificate Request Message Format,
- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ,
- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework ,
- RFC 3739: Internet X.509 Public Key Infrastructure Qualified Certificates Profile,
- vyhláška Ministerstva informatiky č. 378/2006 Sb. ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb,
- zákon č. 101/2000 Sb., o ochraně osobních údajů v aktuálním znění,
- zákon č. 227/2000 Sb., o elektronickém podpisu v platném znění.

Profil kvalifikovaného osobního certifikátu podle standardu X.509 je uveden na následujícím obrázku.

Položka	Hodnota	Pov.	Změna	ORG	PFO	NFO
Version	3 (0x2)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Serial number	sériové číslo certifikátu přidělené certifikační autoritou					
SignatureAlgorithm	sha256WithRSAEncryption					
Issuer						
Country	CZ	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Organisation	Česká pošta, s.p. [IC 47114983] *uvedené číslo je IČ České pošty, s.p.*					
CN	PostSignum Qualified CA 2					
Validity						
Not Before	Počátek platnosti vydaného certifikátu (UTCTime)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Not After	Konec platnosti vydaného certifikátu (UTCTime)					
Subject						
Country	CZ	**ano**	ne	X	X	X
Locality	trvalé bydliště / kontaktní adresa fyzické osoby	ne	**ano**			X
Organisation	jméno právnické osoby nebo podnikající fyzické osoby ve tvaru: jméno zákazníka [IČ ič zákazníka]	**ano**	**ano**	X	X	
OU	rozlišující organizační jednotka právnické osoby nebo podnikající fyzické osoby, stanovená poskytovatelem certifikačních služeb	ne	**ano**	X	X	
OU	organizační jednotka, kde pracuje žadatel o certifikát	ne	**ano**	X	X	
OU	jednoznačné číslo žadatele o certifikát v prostředí zákazníka – organizace nebo podnikající fyzické osoby hodnota údaje serialNumber v případě nepodnikající fyzické osoby	**ano**	**ano**	X	X	X
CN	jméno a příjmení osoby (včetně případných titulů)	**ano**	ne	X	X	X
serialNumber	jednoznačný identifikátor osoby, přidělovaný poskytovatelem certifikačních služeb ve tvaru: *Pčíslo*	**ano**	ne	X	X	X
Title	funkce žadatele o certifikát	ne	**ano**	X	X	
Subject Public Key Info						
Algorithm	rsaEncryption	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
SubjectPublicKey	veřejný klíč podepisující osoby o velikosti 2048 nebo 4096 bitů					
Extensions	rozšíření certifikátu podle tabulky 3					
Signature	elektronická značka poskytovatele certifikačních služeb					

Obrázek 14: Profil kvalifikovaného osobního certifikátu dle standardu X.509

Zdroj [17]

4.4 Instalace vystaveného certifikátu

Při vydání certifikátu na pobočce České pošty se službou Czech POINT je nutné předat operátorovi přenosné paměťové médium (flash disk) s uloženou žádostí o certifikát, případně jen sdělit ID žádosti a předložit občanský průkaz. Následná instalace certifikátu na klientské stanici proběhne následujícím způsobem:

- instalace certifikátu musí být provedena na počítači pod uživatelským účtem, pod kterým bylo provedeno vygenerování klíčů a žádosti o certifikát (viz kapitola 4.2),

- na stránce http://www.postsignum.cz kliknout na odkaz „Instalace vydaného certifikátu“ a v pravé části tlačítkem „Procházet“ vybrat certifikát, který je uložený na flash disku a kliknout na „Instalovat certifikát“,
- po úspěšné instalaci certifikátu provést zálohu klíčů a certifikátu do souboru, který bude uložen na bezpečném místě mimo počítač (z důvodu možné budoucí obnovy certifikátu např. po havárii pevného disku).

Certifikáty uživatelů jsou zveřejňovány (jen ty certifikáty, u nichž dal držitel souhlas k jejich zveřejnění) na webových stránkách kvalifikovaného poskytovatele a lze je vyhledat podle sériového čísla certifikátu případně emailové adresy žadatele. Tímto krokem je certifikát úspěšně naimportován do operačního systému a zbývá už jen nastavit mzdovou aplikaci FluxPam.

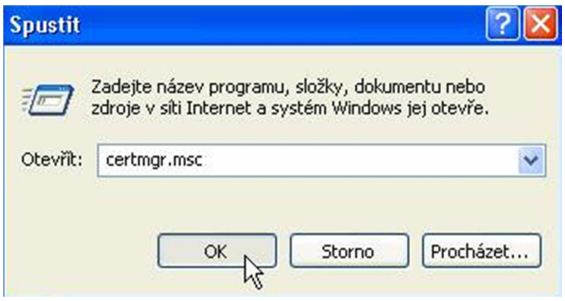
Subjekt	T=mzdová účetní,serialNumber=P69243,CN=Marie Jilčíková,OU=38/8D,OU=Věznice Břeclav,O=Česká republika, Vězeňská služba ČR [IČ 00212423],C=CZ	
E-mailová adresa:	mjilcikova@vez.brv.justice.cz	
Sériové číslo	1415961	
Vydán dne	7.2.2013	
Platný do	7.2.2014	
Vystavitel	PostSignum QCA	
Stav	**Platný**	DER / PEM / TXT(UTF-8)

Obrázek 15: Informace o osobním certifikátu

Zdroj [16]

4.5 Zálohování certifikátu a soukromého klíče

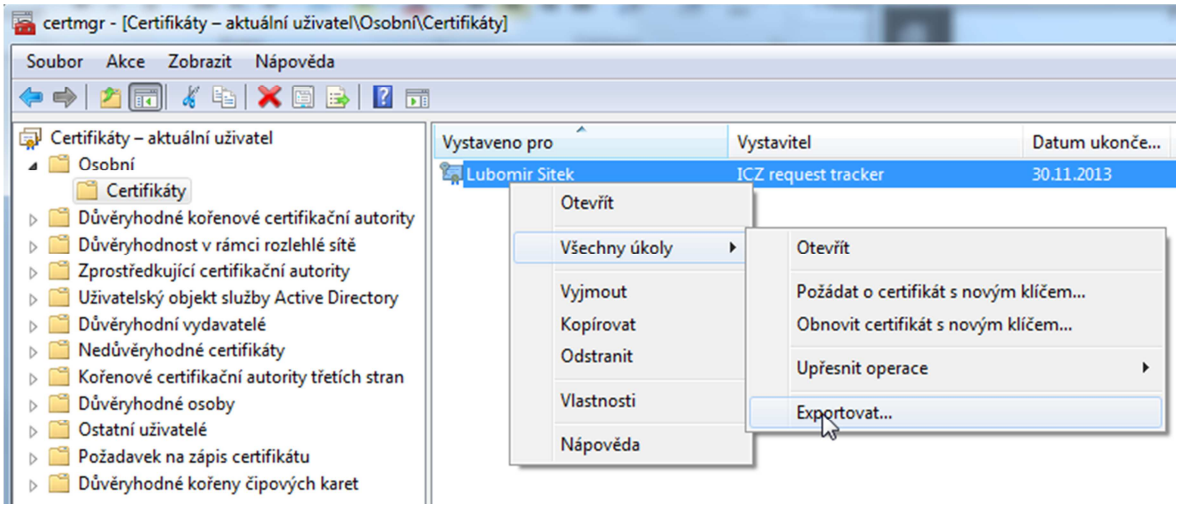
Z důvodu možné havárie počítače (zejména pevného disku), poškození úložiště klíčů nebo potenciální ztráty soukromého klíče je velice vhodné vytvořit si zálohu certifikátu a uložit jej na bezpečné místo. V prostředí operačního systému Microsoft Windows je možné využít manažera certifikátů (certmgr.msc), který lze spustit z příkazového řádku.



Obrázek 16: Spuštění manažera certifikátů

Zdroj: [Vlastní tvorba]

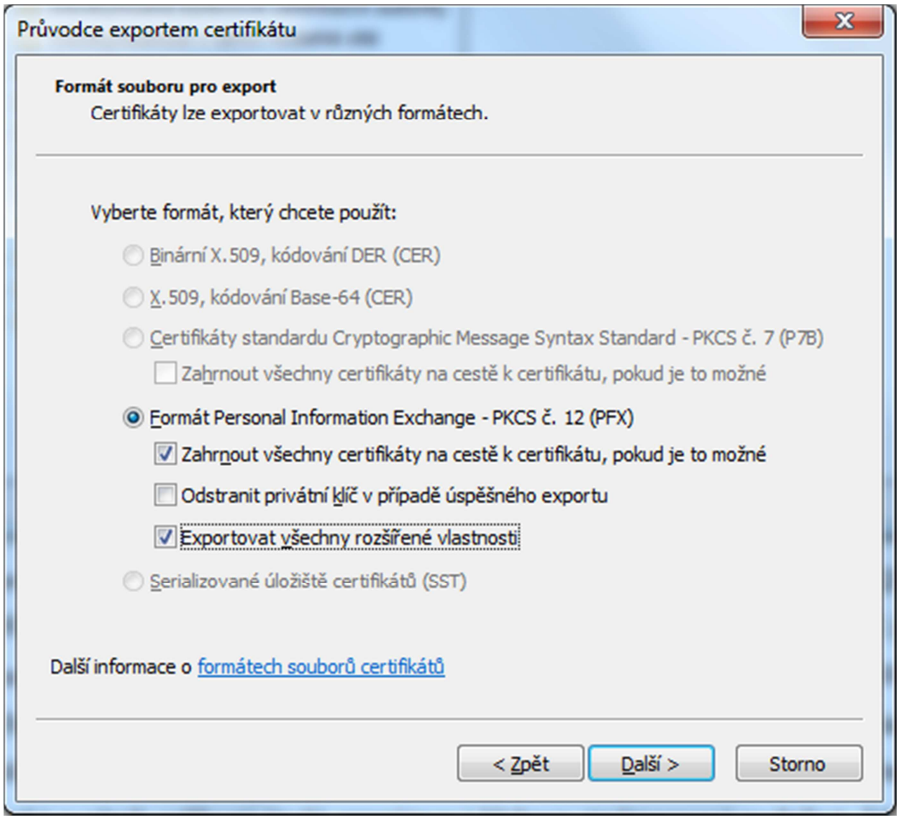
V manažeru certifikátů lze najít kvalifikovaný osobní certifikát v úložišti osobních certifikátů. Pravým tlačítkem zvolíme „Všechny úkoly“ a klikneme na „Exportovat“. Následně se spustí průvodce exportem certifikátu.



Obrázek 17: Export certifikátu

Zdroj: [Vlastní tvorba]

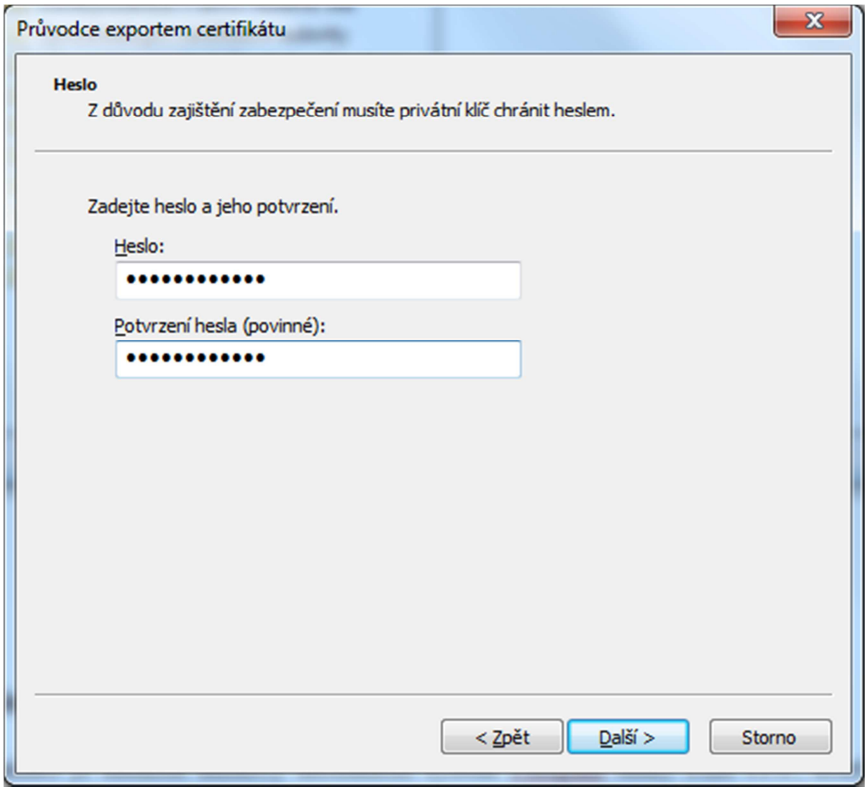
V průvodci vybereme „Ano, exportovat privátní klíč“ a na další obrazovce ponecháme výchozí volby formátu souboru, ve kterém bude certifikát uložen.



Obrázek 18: Formát souboru pro export

Zdroj: [Vlastní tvorba]

V dalším okně průvodce exportem je nutné zvolit heslo, kterým má být exportovaný soubor chráněn. Doporučuji zadat silné heslo (minimální délka 8 znaků, speciální znaky a velká a malá písmena). Pokud export proběhne v pořádku, zobrazí se v následujícím okně zpráva potvrzující úspěšný export. Soubor se zálohou certifikátu a soukromého klíče má příponu „*.pfx“. Vytvořený soubor lze poté kdykoliv použít pro obnovu certifikátu, se souborem je třeba zacházet s náležitou péčí, zejména zabránit přístupu k souboru třetím osobám, protože tato záloha by mohla být snadno zneužita.



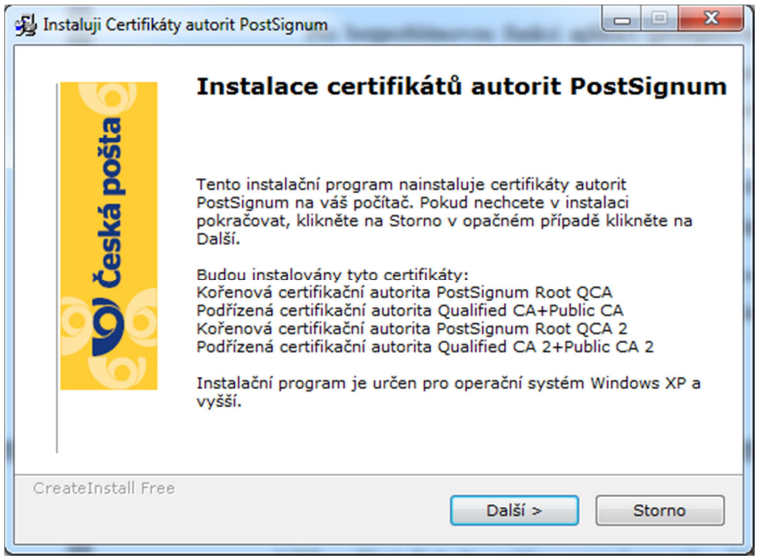
Obrázek 19: Vložení hesla k záloze

Zdroj [Vlastní tvorba]

4.6 Instalace kořenových certifikátů

Pro bezproblémovou funkci aplikací (podepisování PDF, e-mail, webový prohlížeč) a správné vyhodnocení platnosti elektronického podpisu v operačním systému, je nezbytné nainstalovat kořenový certifikát certifikační autority. Instalací certifikátů autorit do operačního systému zajistíme důvěryhodnost používaných kvalifikovaných certifikátů. Při použití osobního kvalifikovaného certifikátu vydaného certifikační autoritou, které důvěřujeme, pak operační systém či jiná aplikace chápe tyto certifikáty jako důvěryhodné.

Chybějící kořenové certifikáty certifikační autority PostSignum je možné nainstalovat z její domovské webové stránky. Lze využít automatickou instalaci stažením instalačního balíčku nebo ruční instalaci stažením jednotlivých certifikátů certifikačních autorit. Nejrychlejší a nejjednodušší způsob je využití automatické instalace. Na webových stránkách www.postsignum.cz stačí kliknout na odkaz „Certifikáty a CRL autorit“ a dále kliknout znovu na odkaz „Certifikáty autorit“. Na stránce stáhnout instalační balíček „CA_postsignum.exe“, uložit jej do počítače a soubor spustit. Po spuštění souboru nás provede průvodce instalací certifikátů. Po kliknutí na tlačítko „Další“ zakřížkujeme v následujícím okně volbu „Souhlasím s instalací“ a znovu klikneme na tlačítko „Další“. Poté dojde k nainstalování kořenových certifikátů do systému. Po ukončení instalace je vhodné zkontrolovat, zda jsou kořenové certifikáty uloženy ve správném úložišti (certifikáty PostSignum Root QCA a PostSignum Root QCA 2 v úložišti důvěryhodných kořenových certifikačních autorit).



Obrázek 20: Průvodce instalací kořenových certifikátů

Zdroj [Vlastní tvorba]

4.7 Změna nastavení mzdové aplikace

V organizaci je nasazen mzdový informační systém Fluxpam firmy Flux s.r.o., který umožňuje také dávkové elektronické podání. Program FLUXPAM 5 je 32bitová aplikace, pracující pod Microsoft Windows, schopná pracovat s různým typem databází (MS SQL server 2000, 2005, MSDE 2000, Express 2005, Express 2008 nebo Oracle). Ve VS ČR je Fluxpam nasazen jako síťová aplikace, která přistupuje k datům prostřednictvím SQL 2000 serveru (brecldb03.vez-slu.justice.cz). Program slouží

ke komplexnímu zpracování personalistiky a mezd v organizacích všech typů (státní správa, soukromý sektor, výrobní podniky atd.) a všech velikostí (malé organizace i hluboce strukturované podniky). Jeho předností je jednoduchá obsluha, přehlednost a okamžitý přepočet všech hodnot po změně jakékoliv položky. Má dlouholetou praxi ve státní správě a řeší komplexně její problematiku (platové postupy, formu odměňování atd.).

Pro změnu podávání ELDP pouze elektronickou cestou je nutné uživatelům ekonomického oddělení (mzdovým účetním) nastavit v aplikaci spojení s portálem České správy sociálního zabezpečení pomocí komunikačního kanálu VREP. Implementace služby VREP v maximální možné míře zachovává kompatibilitu s implementací služby na transakční části dřívějšího Portálu veřejné správy (dále jen „PVS“). Podávající nemusí zřizovat žádné účty (registrovat se jako na PVS). Oprávnění pro jednotlivé služby elektronického podání se kontroluje jen na ČSSZ, takže podávající, kteří v současné době podávají přes PVS, nemusejí kromě konfigurace podávacího software nic dalšího měnit. Není nutná návštěva ČSSZ, neboť oprávnění zasílat podání za danou organizaci jsou platná napříč komunikačními kanály, tedy i pro VREP. Elektronické podání zasílané prostřednictvím komunikačního kanálu VREP musí být podepsáno kvalifikovaným certifikátem a zašifrováno šifrovacím certifikátem ČSSZ. Vlastní šifrování a podpis probíhá pomocí miniaplikace “FLUX PVS SERVER“ ve mzdovém programu Fluxpam a data se odesílají přes zabezpečený https protokol.

Certifikáty	
Certifikát šifrování pro ČSSZ	SERIALNUMBER=S1352, CN=DIS.CSSZ.2013, OU=Odbor
Ladění	
Ověření certifikátu SSL	Ano
Trace GovTalk zpráv	Ano
Zápis hlášení do log souboru	Ano
PROXY server	
Použít proxy server	Ano
Proxy	172.25.44.30:3128,
Připojení	
Časový limit připojení	120
Komunikační kanál	VREP
Url adresa serveru PVS	https://bezpecne.podani.gov.cz/submission
Url adresa serveru VREP	https://vrep1.cssz.cz/VREP/submission
Způsob zpracování	
Způsob zpracování	Odeslat elektronicky na PVS
Zvláštní nastavení	
Uživatelská nastavení společná pro všechny fir	Ano

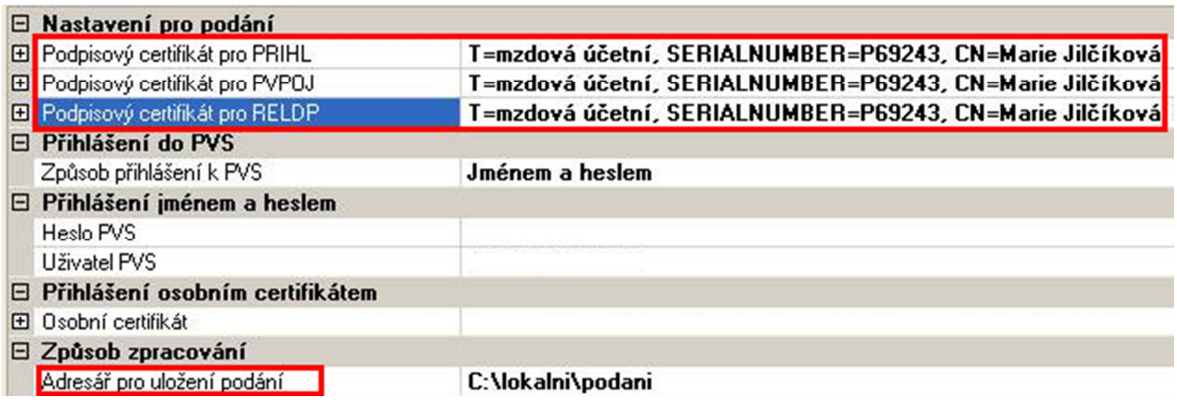
Obrázek 21: Nastavení aplikace FluxPam (obecné)

Zdroj [Vlastní tvorba]

Nastavení pro elektronické podání ELDP lze v aplikaci provést pod aktuálně přihlášeným uživatelem („Makra - Tiskový manažer – Zaměstnanci - Roční ELDP - Přehled balíčků –

PVS - Nastavení PVS“). V obecném nastavení (viz obrázek 21) je nutné zvolit certifikát šifrování pro ČSSZ. Certifikát lze stáhnout z webových stránek ČSSZ, doporučuji jej uložit na síťovém adresáři společně s aplikací FluxPam, případně uživateli certifikát standardně nainstalovat do operačního systému. V obecném nastavení je ještě nutné vybrat komunikační kanál VREP a nastavit proxy server pro přístup aplikace k internetu dle nastavení dané OJ (nezapomenout vyplnit jméno a heslo konkrétního uživatele z důvodu ověřování na proxy serveru). Ostatní hodnoty v obecném nastavení doporučuji ponechat na výchozích hodnotách.

V uživatelském nastavení (viz obrázek 22) stačí vybrat kvalifikovaný certifikát uživatele, který slouží pro vlastní podepsání dávky. Adresář pro uložení podání slouží jako dočasné místo během zpracování a není nutné jej vyplňovat, aplikace poté využije dočasný adresář využívaný operačním systémem, po odeslání dávky uvedený adresář smaže. Všechny zpracované a odeslané dávky je možné kdykoliv podle potřeby zobrazit v aplikaci, dávky jsou uloženy na databázovém SQL serveru (BRECLDB03.vez-slu.justice.cz).



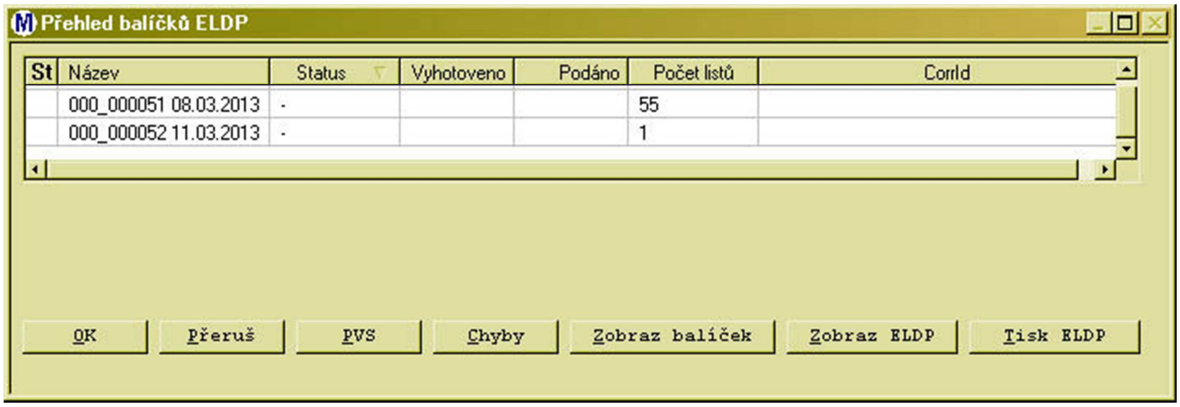
Obrázek 22: Nastavení aplikace FluxPam (uživatelské)

Zdroj [Vlastní tvorba]

4.8 Podání ELDP elektronickou cestou

Vytvoření balíčku s evidenčními listy důchodového pojištění se v programu zpracuje stejným způsobem jako doposud. Změna nastává při elektronickém odeslání dávky, namísto tisknutí formuláře ELDP. Před odesláním dávky je nutné balíček podepsat. Následujícím způsobem lze dávku s evidenčními listy odeslat do ČSSZ:

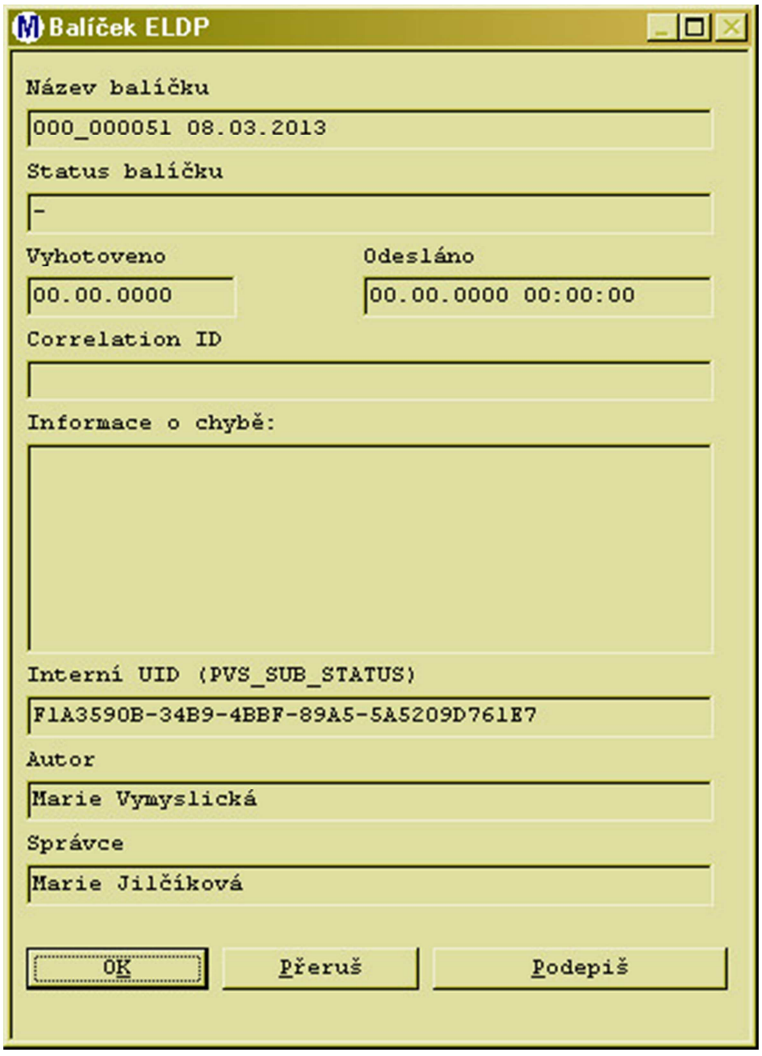
- v menu „Makra - Tiskový manažer – Zaměstnanec - Roční evidenční list DP - Přehled balíčků“ kliknout na tlačítko „Zobrazit balíček“,



Obrázek 23: Přehled balíčků ELDP

Zdroj: [Vlastní tvorba]

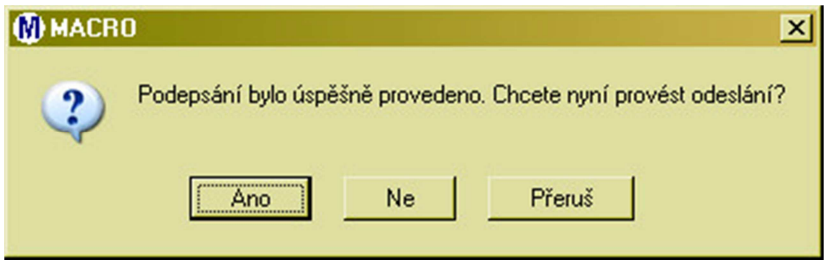
- v zobrazeném balíčku je dále nutné kliknout na tlačítko „Podepiš“, poté dojde k vlastnímu podepsání dávky kvalifikovaným certifikátem uživatele,



Obrázek 24: Vlastnosti balíčku ELDP

Zdroj: [Vlastní tvorba]

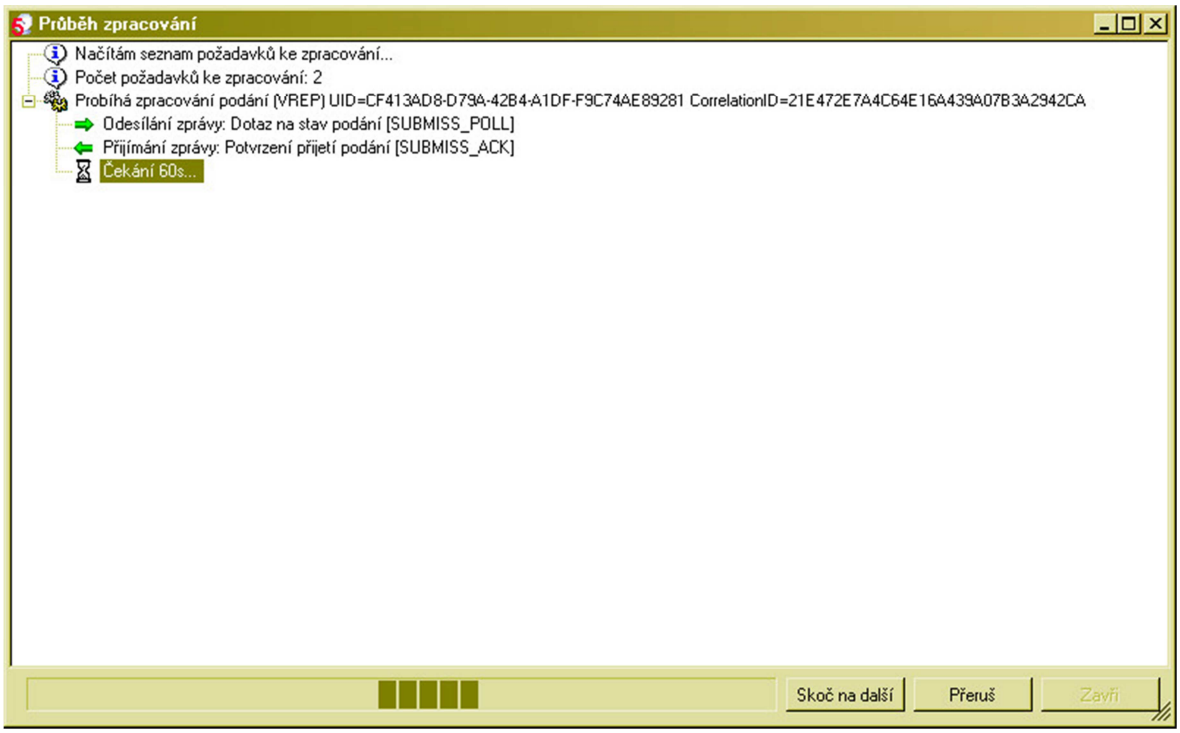
- aplikace dávku podepíše, po zobrazení informačního okna potvrdíme tlačítkem „Ano“ provedení odeslání podepsaného balíčku na ČSSZ,



Obrázek 25: Potvrzení odeslání

Zdroj: [Vlastní tvorba]

- následně dojde k odeslání dávky, další informační okno programu uživateli sděluje průběh zpracování a je nutné vyčkat, až se okno uzavře.

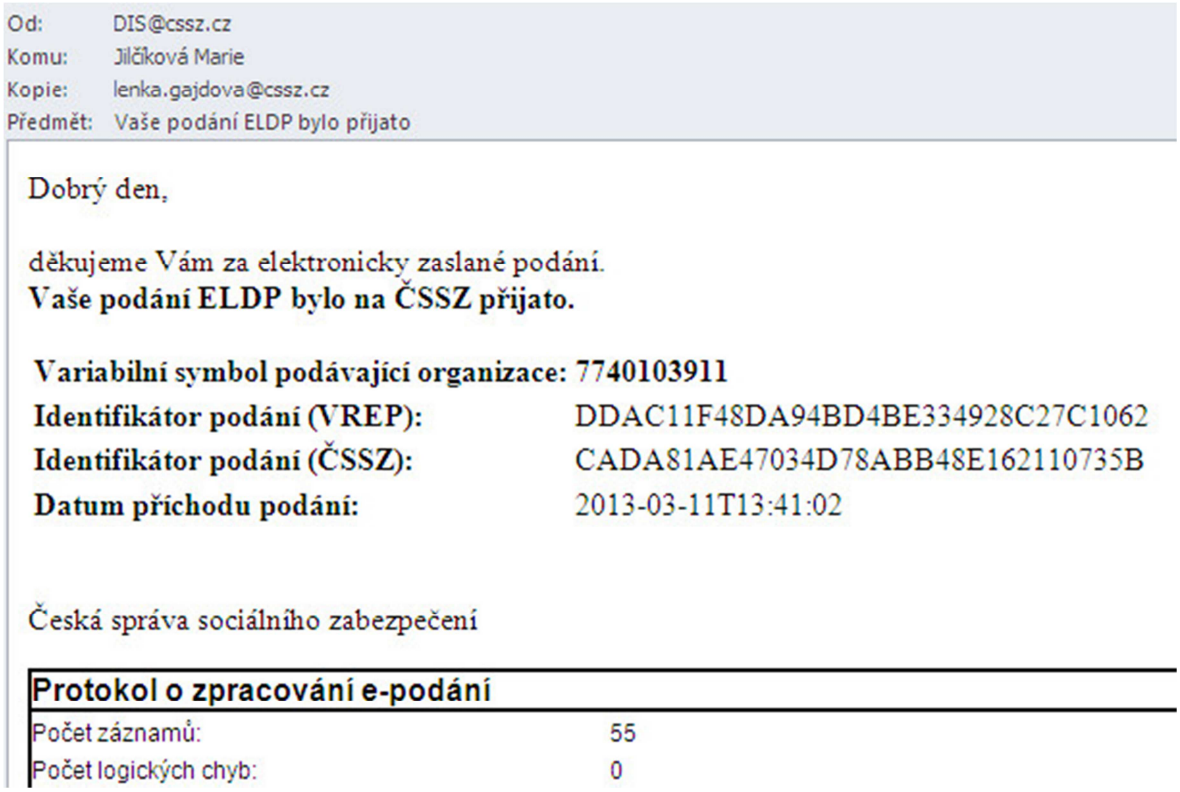


Obrázek 26: Průběh zpracování podání ELDP

Zdroj: [Vlastní tvorba]

Pokud byl balíček v pořádku odeslán a evidenční listy byly správně vyplněny, přijde uživateli emailem potvrzující zpráva „Vaše podání ELDP bylo přijato“. V opačném případě, pokud byly v evidenčních listech chybné údaje, přijde uživateli zpráva „Vaše podání ELDP bylo zamítnuto“ s připojeným seznamem chybných evidenčních listů a popisem kódu chyby (uživatel má okamžitou zpětnou informaci o přijatém nebo

zamítnutém podání včetně popisu chyb u konkrétních ELDP). V takovém případě musí uživatel opravit chybné ELDP a podání provést znovu.



Od: DIS@cssz.cz
Komu: Jilčíková Marie
Kopie: lenka.gajdova@cssz.cz
Předmět: Vaše podání ELDP bylo přijato

Dobrý den,

děkujeme Vám za elektronicky zaslané podání.
Vaše podání ELDP bylo na ČSSZ přijato.

Variabilní symbol podávající organizace: 7740103911
Identifikátor podání (VREP): DDAC11F48DA94BD4BE334928C27C1062
Identifikátor podání (ČSSZ): CADA81AE47034D78ABB48E162110735B
Datum příchodu podání: 2013-03-11T13:41:02

Česká správa sociálního zabezpečení

Protokol o zpracování e-podání

Počet záznamů:	55
Počet logických chyb:	0

Obrázek 27: Potvrzení přijetí podání ELDP

Zdroj: [Vlastní tvorba]

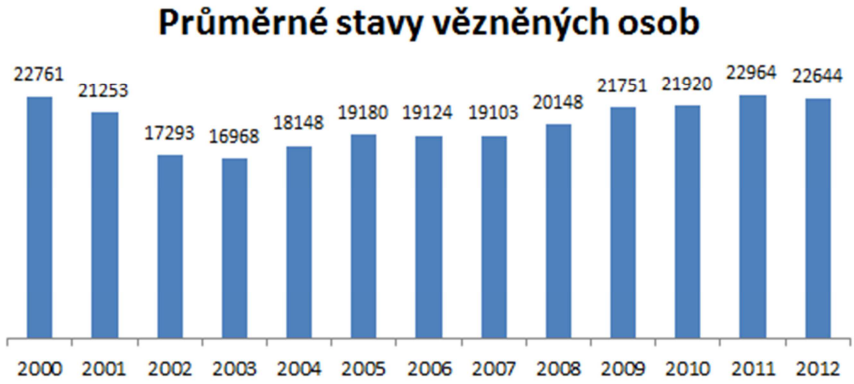
Také v aplikaci v přehledu balíčků je poté změněn status odeslané dávky na „Přijato“ a zelený znak informuje o úspěšném podání. Podrobnější informace o jednotlivých ELDP v odeslaném balíčku lze zobrazit kliknutím na tlačítko „Zobraz ELDP“.

Obrázek 28: Přehled úspěšně odeslaných ELDP

Zdroj: [Vlastní tvorba]

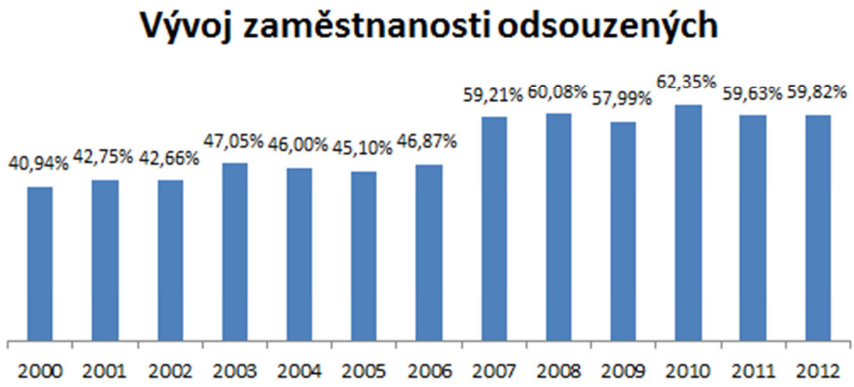
4.9 Přínosy pro organizaci

Evidenční listy, které se předkládají ČSSZ, je možné namísto tištěného tiskopisu (doposud používané řešení) podávat formou elektronického podání, které jsem navrhnul a funkčnost ověřil v kapitole 4.5 a 4.6. Největší přínos spatřuji v úspoře času (odpadá tisknutí formulářů a jejich fyzické předávání na Okresní správu sociálního zabezpečení) a zrychlení komunikace s ČSSZ. Další přínos vidím ve snižování finančních nákladů v organizaci úsporou za tiskové řešení. Úsporu vyčíslím v rámci celé organizace, která musí předkládat roční ELDP za zaměstnance a pracující odsouzené. Početní stav zaměstnanců a pracujících odsouzených bude vycházet ze statistického hlášení [15] a vybraných ukazatelů ve vývoji [18] k 31. 12. 2012. Jak lze vidět na obrázcích níže, počet zaměstnanců za rok 2012 byl 11 348 a počet pracujících odsouzených byl 13 546 (59,82% z celkového počtu). Za rok 2012 by musela VS ČR pro ČSSZ vytisknout 24 894 tiskopisů ELDP.



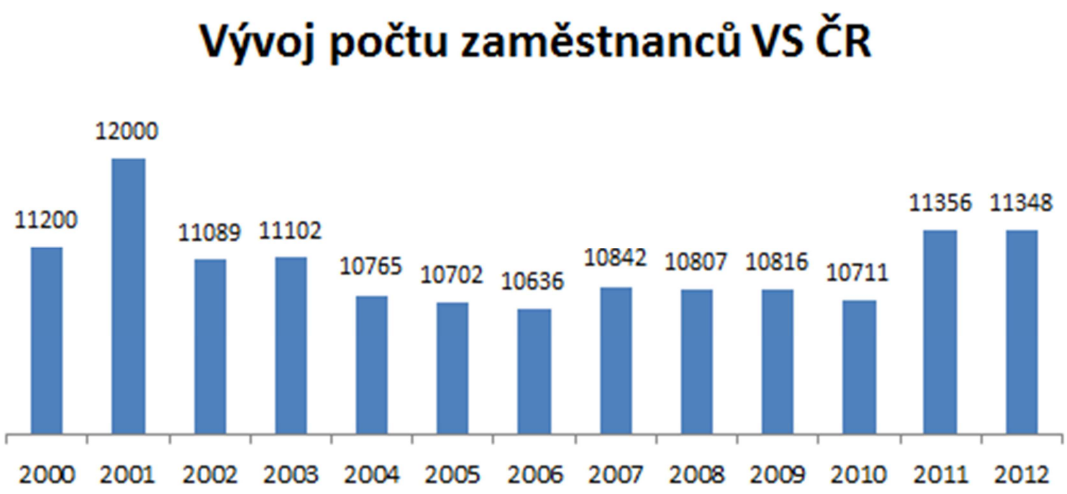
Obrázek 29: Průměrné stavy vězněných osob

Zdroj [18]



Obrázek 30: Vývoj zaměstnanosti odsouzených

Zdroj: [18]



Obrázek 31: Vývoj počtu zaměstnanců VS ČR

Zdroj [18]

Formulář ročního hlášení ELDP (Příloha P I) je rozměru A5, na jeden list formátu A4 lze proto vytisknout dva formuláře. V tabulce č. 5 uvádím nejpoužívanější síťové tiskárny v organizaci, které jsou připojeny ke koncovým zařízením na ekonomických odděleních a jsou vhodné pro tisk formulářů. Konkrétní typy tiskáren ze všech lokalit jsem zjistil pomocí tiskových serverů a dotazu na vedoucí oddělení informatiky z organizačních jednotek. Na základě zjištěných informací navrhuji provést také optimalizaci tiskového řešení u těch organizačních jednotek, které používají na ekonomických odděleních síťové barevné laserové tiskárny, které doporučuji vyměnit nebo přesměrovat tisk na síťové černobílé laserové tiskárny.

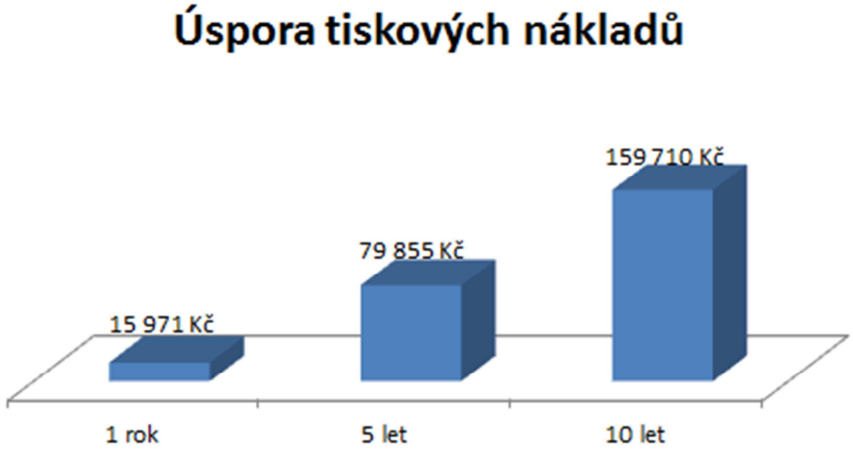
Tabulka 5: Náklady na tisk

Zdroj [Vlastní tvorba]

Tiskárna	Typ	OJ	Náklady na A4
OKI C7300dn	Barevná	Rapotice	3,96 Kč
OKI B8300dn	Černobílá	Břeclav	0,43 Kč
OKI MB470	Černobílá	Znojmo	0,71 Kč
HP M401dn	Černobílá	Kuřim	0,59 Kč
OKI B410	Černobílá	Brno	0,70 Kč
Průměrná cena včetně DPH			**1,28 Kč**

Náklady na tisk jedné stránky A4 jsou vypočítány jako průměr nákladů jednotlivých tiskáren pomocí kalkulátoru tiskových nákladů. [19] Do výpočtu nákladů na tisk jednoho listu A4 zahrnuji průměrnou cenu kusu papíru (0,20 Kč bez DPH), výrobcem udávanou výtěžnost náplní při 5% pokrytí a aktuální cenu spotřebního materiálu od centrálního

dodavatele, se kterým má odbor informatiky uzavřenou smlouvu. Roční úspora za tisk evidenčních listů pro ČSSZ činí 15 971,- Kč s DPH (tisk 12 477 listů A4).



Obrázek 32: Úspora tiskových nákladů v čase

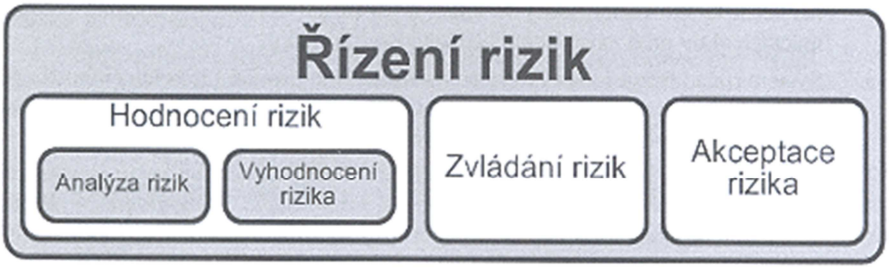
Zdroj [Vlastní tvorba]

5 BEZPEČNOSTNÍ ZÁSADY UŽIVATELE

VS ČR by měla věnovat trvalou pozornost nadstandartnímu zabezpečení mzdové aplikace Fluxpam pro ochranu důvěrnosti a integrity jeho aktiv, dostupnosti a spolehlivosti celé aplikace. Pro zajištění bezpečnosti autorizace vlastního podání ELDP je využívána funkce elektronického podpisu pomocí kvalifikovaného certifikátu vydaného akreditovanou certifikační autoritou. Přes veškerá opatření, realizovaná zejména v systémovém prostředí aplikace Fluxpam, je nutné věnovat náležitou pozornost také rizikům na straně klienta, resp. jeho uživatelů, vyplívajících ze způsobu přípravy a předání dávek s příkazy, zajištění ochrany podpisového certifikátu, klientské stanice a systémového prostředí. **Dodržováním následujících zásad lze tato rizika eliminovat. Navrhuji také, aby byly zásady (zejména povinnosti administrátora) zapracovány do vnitřních předpisů[12].**

5.1 Rizika a účinná ochrana

Řízení rizik je klíčovým nástrojem pro systematické řízení bezpečnosti informací. Systém řízení bezpečnosti informací je část celkového systému řízení organizace, založená na přístupu organizace k rizikům dle ISO/IEC 27001: 2005. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopných snížit negativní dopady těchto rizik. Dobrá a přesná znalost bezpečnostních rizik vede k účinnému vynakládání úsilí při prosazování bezpečnostních opatření, které přinášejí větší efektivitu. Řízení rizik je proto základem pro každý systém řízení bezpečnosti informací a navíc podstatným způsobem ovlivňuje efektivitu fungování celého systému. Terminologie spojená s řízením rizik a vztahy mezi termíny jsou uvedeny na následujícím obrázku.



Obrázek 33: Uspořádání terminologie řízení rizik

Zdroj [3]

[12] NGŘ 20/2005 o provozu výpočetní techniky ve VS ČR

V následujících odstavcích jsem se snažil analyzovat rizika spojená s využíváním kvalifikovaných certifikátů zaměstnanců. Nezajištěná ochrana informačních systémů, v nichž se připravují dávky s příkazy, představuje největší nebezpečí, které spočívá v podvržení příkazů ještě před podpisem dávky a následnému předání ke zpracování. Následně je dávka podepsána a odeslána uživatelem, který si podezřelého příkazu nevšimne.

Jak k tomu může dojít: Informační systém na straně klienta vytvoří soubor s dávkou a uloží jej na disk klientské stanice. K tomuto souboru má přístup jiný uživatel v síti, např. administrátor, kolega, servisní organizace, případně i útočník prostřednictvím škodlivého softwaru, který může soubor pozměnit běžným editorem.

Jak tomu předcházet: Nesdílet PC, zabránit neřízenému přístupu administrátorů, servisu, zajistit ochranu před škodlivým softwarem a minimalizovat dobu, po kterou je soubor na disku nechráněn. Soubor musí být neprodleně zpracován po svém vytvoření, uživatel nesmí opustit PC v době mezi vytvořením souboru a jeho podepsáním.

Privátní klíč kvalifikovaného certifikátu je určen výhradně svému uživateli. Nedostatečná ochrana privátního klíče umožní potencionálnímu útočníkovi tento klíč nebo celý certifikát získat a následně vložit a elektronicky podepsat dávku stejným způsobem jako uživatel případně jinak zneužít k elektronickému podepisování.

Jak k tomu může dojít: Například, když uživatel svěří instalaci certifikátu třetí osobě, nebo jej uloží do svého PC v exportovatelném tvaru, případně nezvolí silný způsob jeho zabezpečení (heslem) či nastaví příliš slabé heslo.

Jak tomu předcházet: Doporučuji pořídit certifikát instalovaný na tokenu nebo čipové kartě přímo u certifikační autority, v ostatních případech je nezbytné instalovat certifikát do PC v režimu silného zabezpečení, bez možnosti jeho exportu a se silným heslem (alespoň 10 znaků, s volbou malých a velkých písmen, číslic a znaků). Certifikát, zejména privátní klíč, uživatel v žádném případě nepředává třetí osobě.

Nedostatečné zabezpečení klientské stanice přistupující k Internetu může způsobit nežádoucí zavlečení softwaru, kterého útočník využije ke skrytému spojení do aplikace nebo krádeži privátního klíče kvalifikovaného certifikátu, případně jeho hesla.

Jak k tomu může dojít: Neopatrným prohlížením webových stránek nebo otevíráním příloh elektronické pošty si může uživatel stáhnout škodlivý software (vir, trojský kůň, spyware[13]) na své PC přistupující k aplikaci Fluxpam.

Jak tomu předcházet: Uživatel je povinen uplatňovat základní zásady obezřetnosti při prohlížení webových stránek Internetu a při otevírání zejména nevyžádané pošty, používat firewally, antivirové, antispamové či antimalwarové programy pro zvýšení ochrany svého PC a systémového prostředí. Dále je nutné věnovat pozornost pravidelnému a systematickému vyhledávání zranitelností v systému (chybějící opravy softwaru, chybné konfigurace, slabá hesla) a zajistit jejich odstranění.

Sdílená prostředí v rámci organizační struktury uživatele představují riziko přístupu dalších osob ke klientské stanici, např. IT specialistů, administrátorů či servisní organizace.

Jak k tomu může dojít: V organizaci mohou k PC uživatele přistupovat IT specialisté, helpdesk, servisní organizace a kolegové sdílející dané PC.

Jak tomu předcházet: Důsledným řízením přístupových práv, volbou bezpečného úložiště pro podpisový klíč na tokenu nebo čipové kartě.

Útočníci využívají celé škály metod sociálního inženýrství a prostředků, aby vylákali přihlašovací údaje uživatelů pro přístup do aplikace Fluxpam.

Jak k tomu může dojít: Prostřednictvím podvržené webové stránky uživatel nevědomě poskytne své přihlašovací údaje cizí osobě.

Jak tomu předcházet: Nereagovat na nevyžádanou elektronickou poštu a jiné formy vylákání přihlašovacích údajů (tzv. phishing[14]).

---

[13] Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele.

[14] Phishing (někdy převáděno do češtiny jako rybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů nebo od IT administrátorů.

5.2 Povinnosti uživatele a administrátora

Na základě analýzy rizik v předchozí kapitole navrhuji bezpečnostní zásady pro uživatele a správce sítě, kteří jsou povinni:

- zajistit vysokou úroveň zabezpečení systému pro přípravu dávek určených pro zpracování v aplikaci Fluxpam, aby s nimi nebylo možné neautorizovaným způsobem manipulovat před předáním do ČSSZ,
- zajistit adekvátní úroveň zabezpečení klientských počítačů uživatelů, zejména prostředky firewallů, antivirového, antispamového softwaru a dalšími prostředky pro ochranu před škodlivým softwarem, zejména viry, trojskými koni, spamem, spyware apod., dále systematickým vyhledáváním známých zranitelností, aktualizací operačního systému a instalovaných aplikací a dále omezením přístupu klientských stanic k nebezpečnému obsahu a adresám v Internetu,
- zajistit systémovou a fyzickou ochranu privátního klíče certifikátu pro vytváření elektronického podpisu/elektronické značky nejlépe technickými prostředky (token, čipová karta) nebo alespoň nastavením vysoké úrovně zabezpečení, tj. s přístupem pouze přes silná hesla, při uložení klíčů do zabezpečeného softwarového úložiště na klientské stanici a v neexportovatelném tvaru,
- zajistit pravidelné aktualizace a opravy softwaru, především operačního systému, prohlížeče webových stránek a dalších instalovaných aplikací,
- přihlášení uživatele k operačnímu systému realizovat pomocí standardního uživatelského účtu bez administrátorského oprávnění, a dostatečně složitého hesla, resp. na základě jiného mechanismu s odpovídající nebo vyšší úrovní bezpečnosti,
- vhodnými prostředky bránit neoprávněným osobám v užívání počítače a zejména aplikace Fluxpam, např. odhlášením nebo alespoň uzamčením počítače v době nepřítomnosti uživatele,
- nereagovat na výzvy k poskytnutí přihlašovacích údajů třetími osobami (spam, phishing), přihlašovací údaje jsou určeny pouze danému uživateli,
- zajistit co nejbezpečnější způsob předání dávek s příkazy, optimálně tak, aby byla dávka elektronicky podepsána již v systému, ve kterém jsou dávky v prostředí klienta připravovány,
- zajistit bezodkladné předání dávek ke zpracování.

ZÁVĚR

Veškeré mnou navržené metody a změny při podávání evidenčních listů důchodového pojištění, které jsou podloženy studiem odborné literatury, norem, standardů, legislativy a využívají infrastrukturu PKI při elektronické formě podání, splnily cíl diplomové práce. Elektronický podpis ušel za svou historii poměrně dlouhou cestu a pro uživatele, kteří se orientují v principech spojených s elektronickým podpisem, je zpravidla jeho užívání jednoduchou záležitostí. Pro ty uživatele, kteří se ještě z nějakého důvodu v problematice neorientují, je v diplomové práci popsán přehled problematiky elektronického podpisu, praktické zkušenosti a nezaujatě zhodnocen současný stav a vývojové tendence ve zmíněné oblasti.

Přínosem mé diplomové práce pro praxi je mnou navržené řešení podávání evidenčních listů důchodového pojištění. Věřím, že praktická část diplomové práce bude cennou pomůckou k pochopení dané problematiky pro všechny uživatele, kteří hodlají navržené řešení využívat i ve své organizaci.

Hlavní přínos spatřuji v úspoře času, jelikož odpadá tisknutí formulářů a jejich fyzické předávání na Okresní správu sociálního zabezpečení a v celkovém zrychlení komunikace s Českou správou sociálního zabezpečení, protože odpovědi na případné chyby v podání jsou také okamžitě elektronickou cestou předány odesilateli. Další podstatný přínos spatřuji ve snížení finančních nákladů organizace.

První kapitola obsahuje teoretické informace, výklad klíčových pojmů, seznámení se s infrastrukturou PKI a nastínění principu vytváření elektronického podpisu s využitím asymetrické kryptografie. Je zde také rozebrána aktuální legislativa, směrnice EU a zákon o elektronickém podpisu. V závěru je probrána problematika bezpečnosti z pohledu uživatele při využívání elektronického podpisu.

Druhá kapitola se více zabývá technologickými aspekty při vytváření elektronického podpisu. Vysvětluje asymetrickou kryptografii, hash a doporučené hashovací funkce podle směrnice EU a zabezpečení integrity podepsaného dokumentu.

Třetí kapitola popisuje základní principy a pravidla při ověření elektronického podpisu a vysvětluje seznamy zneplatněných certifikátů.

Praktická část diplomové práce se ve čtvrté kapitole věnuje uvedení do problematiky změny podávání evidenčních listů důchodového pojištění, generování žádosti k získání

a instalaci kvalifikovaného certifikátu, kořenového certifikátu a zálohování soukromého klíče. Jsou zde popsány změny a postupy ve mzdovém programu, kterým budou posílány dávky ELDP a v závěru vyjmenovány přínosy pro organizaci.

V poslední páté kapitole praktické části jsou analyzovány bezpečnostní rizika, která vyplívají z používání certifikátů. Na základě analyzovaných rizik jsou stanoveny bezpečnostní zásady pro uživatele a administrátory.

ZÁVĚR V ANGLIČTINĚ

All suggested methods and changes of electronic submission of pension evidence records are based on study of literature, norms, standards, legislation and PKI infrastructure. The proposed methods and changes fulfilled the aims of this diploma thesis. The electronic signature has changed a lot and for users who are familiar with its principles it is relatively simple. For users who are not aware of it; the overview, practical experience, current situation and development tendencies of the electronic signature are described.

The main contribution of my diploma thesis for practice is suggested solutions of administration of pension evidence records. I believe that the practical part of the thesis gives a valuable tool for understanding the problem for all users who want to use suggested solutions in their organizations.

The main contribution can be seen in saving the time because of no necessity to print forms and submit them in person, but main positive aspect lays in the overall speedup of communication with Czech Social Security Administration, because the responses to potential mistakes are immediately transmitted to the sender. Another important contribution can be seen in reduction of costs.

The first chapter presents theoretical information, definitions of key words, explanation of infrastructure PKI and principles of creating electronic signatures using asymmetric cryptography. The current legislation, EU regulations and electronic signature laws are also analysed. In the conclusion of the chapter the problems of security from the electronic signature users' point of view are examined.

The second chapter deals with technological aspects of creating the electronic signature. Asymmetric cryptography, hash and suggested hash functions in accordance with EU regulations and security of the signed document are explained.

The third chapter describes basic principles and rules of the electronic signature verifying and explains registers of invalidate certificates.

The forth chapter of the practical part is dedicated to the explanation of changes of pension insurance records administration, generation of requests for acquiring and installation of qualified certificates, root certificates and back-up of the private key. The changes and methods in a salary program, which is used to send benefits ELDP are described. The benefits for organization are also named.

In the last fifth chapter of the practical part security risks, which emerge from using the certificates, are analysed. According to the analysed risks the security principles for users and administrators are defined.

SEZNAM POUŽITÉ LITERATURY

[1] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011, 430 s. ISBN 978-80-904248-3-8.

[2] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.

[3] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[4] BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. 1. vyd. Olomouc: ANAG, 2008, 157 s. ISBN 978-80-7263-465-1.

[5] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, 2007, 154 s. ISBN 978-80-251-1511-4.

[6] FORD, Warwick a Michael S BAUM. *Secure electronic commerce: building the infrastructure for digital signatures and encryption*. 2nd ed. Upper Saddle River, NJ: Prentice Hall PTR, 2001, 612 p. ISBN 01-302-7276-0.

[7] WILDE, Erik. Security Issues. *UC Berkeley School of Information* [online]. 2008 [cit. 2012-09-26]. Dostupné z: http://dret.net/lectures/web-fall08/security

[8] Technické řešení. *Certifikační autorita PostSignum* [online]. 2012 [cit. 2012-09-26]. Dostupné z: http://www.postsignum.cz/technicke_reseni.html

[9] Asymetrická kryptografie. *Wikipedie* [online]. 2013 [cit. 2013-01-10]. Dostupné z: http://cs.wikipedia.org/wiki/Soubor:Asymetrick%C3%A1_kryptografie.svg

[10] Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu. *Ministerstvo vnitra České republiky* [online]. 2010 [cit. 2013-02-16]. Dostupné z: http://www.mvcr.cz/soubor/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronickeho-podpisu.aspx

[11] ETSI TS 102 176-1 V2.1.1 (2011-07). *ETSI Publication Download Area: Search Results* [online]. 2011 [cit. 2013-02-16]. Dostupné z: http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf

[12] Elektronický podpis. *Wikipedie* [online]. 2013 [cit. 2013-01-20]. Dostupné z: http://cs.wikipedia.org/wiki/Soubor:Digital_Signature_diagram_cs.svg

[13] Mapa věznic, vazebních věznic a detenčních ústavů ČR. *Vězeňská služba České republiky* [online]. 2013 [cit. 2013-01-26]. Dostupné z: http://vscr.cz/client_data/1/user_files/19/image/Tiskov%C3%A9%20odd%C4%9Blen%C3%AD%20G%C5%98%20VS/st%C3%A1l%C3%A9/mapky/v%C4%9Bznice%20kraje.jpg

[14] Evidenční listy důchodového pojištění. *Česká správa sociálního zabezpečení* [online]. 2013 [cit. 2013-02-19]. Dostupné z: http://www.cssz.cz/cz/duchodove-pojisteni/povinnosti/prislusnost-zamestnavatelu-k-plneni-ukolu-pri-provadeni-duchodoveho-pojisteni/evidencni-listy-duchodoveho-pojisteni.htm

[15] Měsíční statistické hlášení. *Vězeňská služba České republiky* [online]. 2012 [cit. 2013-02-19]. Dostupné z: http://vscr.cz/client_data/1/user_files/19/file/spr%C3%A1vn%C3%AD/statistiky/M%C4%9Bs%C3%AD%C4%8Dn%C3%AD%20statistick%C3%A9%20hl%C3%A1%C5%A1en%C3%AD%20/2012/MSH12-2012.pdf

[16] Certifikáty uživatelů. *Certifikační autorita PostSignum* [online]. 2012 [cit. 2013-02-19]. Dostupné z: http://www.postsignum.cz/certifikaty_uzivatelu.html

[17] Certifikáty Certifikační politiky QCA. *Certifikační autorita PostSignum* [online]. 2012 [cit. 2013-02-19]. Dostupné z: http://www.postsignum.cz/files/politiky/QCA_osobni_crt_v2-1.pdf

[18] Vybrané ukazatele ve vývoji. *Vězeňská služba České republiky* [online]. 2012 [cit. 2013-02-21]. Dostupné z: http://vscr.cz/generalni-reditelstvi-19/o-nas/zakladni-informace-4/vybrane-ukazatele-ve-vyvoji-10189

[19] Náklady na tisk a výběr vhodné tiskárny. *OKI v České republice* [online]. 2012 [cit. 2013-02-21]. Dostupné z: http://czech.oki.com/printers/promotions/detail.aspx?id=tcm:100-26894-16

[20] Certifikáty. *Certifikační autorita PostSignum* [online]. 2013 [cit. 2013-03-12]. Dostupné z: http://www.postsignum.cz/certifikaty.html

[21] Ceny služeb platné od 1. 9. 2010. *APCS eIdentity a.s.* [online]. 2013 [cit. 2013-03-12]. Dostupné z: http://www.eidentity.cz/Prices.html

[22] Ceník. *I.CA* [online]. 2013 [cit. 2013-03-12]. Dostupné z: http://www.ica.cz/Cenik

[23] Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb. *Ministerstvo vnitra České republiky* [online]. 2011 [cit. 2012-09-26]. Dostupné z: http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb-320051.aspx

[24] Informace k používání elektronického podpisu. *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2012-09-26]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx

[25] Postup pro získání certifikátu. *Certifikační autorita PostSignum* [online]. 2012 [cit. 2012-09-26]. Dostupné z: http://www.postsignum.cz/postup_pro_ziskani_certifikatu.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

a.s. Akciová společnost.

atd. A tak dále.

BS British Standards, britské standardy.

CA Certifikační autorita, subjekt vydávající certifikáty k veřejným klíčům.

CRL Certificate Revocation List, seznam zneplatněných certifikátů.

CS Certificate Store, úložiště certifikátů.

CWA CEN Workshop Agreement, referenční dokumenty Evropského výboru pro normalizaci (European Committee for Standardization).

CZK Czech crown, mezinárodní kód české měny.

ČSN Česká technická norma, tvorbu a vydávání v současné době zajišťuje Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSSZ Česká správa sociálního zabezpečení, instituce státní správy ČR.

ČR Česká republika.

DPH Daň z přidané hodnoty, nepřímá spotřební daň.

ELDP Evidenční list důchodového pojištění.

EN Evropská norma.

ETSI The European Telecommunications Standards Institute, Evropský ústav pro telekomunikační normy.

EU Evropská unie, uskupení evropských států.

ID Identification, identifikace.

IEC International Electrotechnical Commission, Mezinárodní elektrotechnická komise, vypracovávající a publikující mezinárodní normy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory.

ISO International Organization for Standardization, Mezinárodní organizace pro normalizaci.

ITU-T International Telecommunication Union, sekce Telecommunication

	Standardization Sector, instituce vydávající standardy k telekomunikacím.
MSDE	Microsoft SQL Server Data Engine, relační databázový systém vyvinutý společností Microsoft.
NIST	The National Institute of Standards and Technology, Národní institut pro standardy a technologie Spojených států amerických.
NSA	The National Security Agency, Národní bezpečnostní agentura, vládní kryptologická organizace Spojených států amerických.
PDF	Portable Document Format, souborový formát pro ukládání dokumentů.
PIN	Personal Identification Number, osobní identifikační číslo sloužící pro přístup k citlivým informacím.
PKI	Public Key Infrastructure, označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie.
QCA	Kvalifikovaná certifikační autorita, vydává osobní kvalifikované certifikáty.
RFC	Request for query, standardizační dokumenty pro prostředí internetu.
RSA	Rivest – Shamir – Adelman, asymetrická šifra pojmenovaná podle počátečních písmen příjmení autorů.
s.p.	Státní podnik.
SHA	Secure Hash Algorithm, rozšířená hashovací funkce.
SHA-1	Hashovací algoritmus, délka hashe 160 bitů.
SHA-2	Hashovací algoritmy (SHA-224, SHA-256, SHA-384, SHA-512).
SHA-224	Hashovací algoritmus, délka hashe 224 bitů.
SHA-256	Hashovací algoritmus, délka hashe 256 bitů.
SHA-384	Hashovací algoritmus, délka hashe 384 bitů.
SHA-512	Hashovací algoritmus, délka hashe 512 bitů.
SSL	Secure Sockets Layer, protokol poskytující zabezpečení komunikace šifrováním a autentizací komunikujících stran.
SQL	Structured Query Language, standardizovaný dotazovací jazyk používaný

	pro práci s daty v relačních databázích.
tzv.	Takzvaný.
USA	The United States of America, Spojené státy americké.
VCA	Veřejná certifikační autorita, vydává komerční certifikáty.
VS	Vězeňská služba, ozbrojený bezpečnostní sbor, zajišťující výkon vazby a výkon trestu odnětí svobody.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: EVIDENČNÍ LIST DŮCHODOVÉHO POJIŠTĚNÍ

Evidenční list důchodového pojištění

Nastavení psacího stroje

Technický kód

za rok

Typ ELDP

Oprava ELDP ze dne

ČSSZ

1. Identifikace pojištěnce

Rodné číslo pojištěnce

Příjmení (poslední)

Jméno

Titul

Datum narození

Ulice

Číslo domu

Rodné příjmení

Obec

Pošta

PSČ

Místo narození

2. Průběh pojištění v daném roce

Kód

Od

Do

Dny

1 2 3 4 5 6 7 8 9 10 11 12 1.-12.

Vyloučené doby

Vyměřovací základ

Doby odečt.

Znepl.

Vojenská služba - V
Civilní služba - C
PPM/PP - M

Druh

Od

Do

Druh

Od

Do

Celkem

Celkem

Celkem

3. Identifikační údaje organizace a podpisy

Název organizace

Identifikační číslo organizace

Variabilní symbol organizace

Ulice

Číslo domu

Vydělečná činnost v organizaci od

Obec

PSČ

Datum vyhotovení ELDP

2 3 4 2 6 4 5 3 1 0

Datum a podpis pojištěnce

Podpis a razítko organizace

Datum, podpis a razítko OSSZ

I/2008 ČSSZ 89 382 2

PŘÍLOHA P II: SMLOUVA O POSKYTOVÁNÍ CERTIFIKAČNÍCH SLUŽEB

Číslo smlouvy [1]	

SMLOUVA O POSKYTOVÁNÍ CERTIFIKAČNÍCH SLUŽEB

(zákazník – právnická osoba nebo podnikající fyzická osoba)

1. Smluvní strany

Poskytovatel

Česká pošta, s.p.
zastoupená: .....
se sídlem **Politických vězňů 909/4, 225 99 Praha 1**
IČ: **47114983** **DIČ: CZ47114983**
zapsaná v **obchodním rejstříku, vedeném u Městského soudu v Praze, sp. zn. A 7565**
Bankovní spojení **ČSOB, a.s., č.ú.133406370/0300**

Zákazník

Název / Obchodní firma / Jméno a příjmení: [2] .....
Sídlo / místo podnikání: [2] .....
IČ: [2] ..... DIČ: .....
Doklad o právní subjektivitě: [2] .....
Zastoupený / jednající: [3] .....
Organizační jednotka: .....
Adresa pro zasílání faktur: [4] .....

uzavírají níže uvedeného dne, měsíce a roku ve smyslu § 269 odst. 2 zákona č. 513/1991 Sb., obchodního zákoníku, ve znění pozdějších předpisů (dále jen „obchodní zákoník") a zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů (dál jen „ZEP"), tuto smlouvu.

Legenda:

1 Doplní pracovník České pošty.
2 Údaje musí souhlasit s údaji v předloženém dokladu o právní subjektivitě zákazníka (např. ve výpise z obchodního rejstříku, ve výpise ze živnostenského rejstříku).
3 Uvede se statutární zástupce zákazníka, nebo osoba jím zmocněná k podepsání této smlouvy. Pokud je v dokladu o právní subjektivitě zákazníka uveden způsob jednání a podepisování, musí být při podepisování smlouvy a její přílohy nebo při podepsání zmocnění k podepsání této smlouvy dodržen.
4 Uvede se, liší-li se od sídla/místa podnikání zákazníka.

2. Trvání smlouvy

Tato smlouva se uzavírá na ☐ dobu neurčitou
☐ dobu určitou Od ..... do .....

3. Rozsah poskytovaných služeb

Zákazník má nárok využívat následující služby Poskytovatele. Poskytnutí služby je podmíněno dodáním zákaznického formuláře, v němž jsou specifikovány parametry služby.

Certifikáty vydávané kvalifikovanou certifikační autoritou PostSignum QCA:

1. kvalifikované osobní certifikáty
2. kvalifikované systémové certifikáty

Certifikáty vydávané komerční certifikační autoritou PostSignum VCA:

3. komerční osobní certifikáty
4. komerční serverové certifikáty
5. komerční šifrovací certifikáty

4. Obecné parametry poskytovaných služeb

4.1 Zákazník **podnikající fyzická osoba** ☐ uděluje [5] / ☐ neuděluje [5] souhlas se zpracováním osobních údajů (jméno, příjmení a adresa) za účelem marketingu či propagace produktů a služeb poskytovatele ve smyslu čl.7, odst.2b, Všeobecných obchodních podmínek vybraných elektronických služeb České pošty. Souhlas je dobrovolný a uděluje se na dobu trvání smluvního vztahu. Zákazník bere na vědomí informace o svém právu na přístup k těmto osobním údajům, právu na opravu těchto osobních údajů i povinnosti poskytovatele na požádání sdělit informace o jejich zpracování, jakož i o dalších právech stanovených v §21 zákona č. 101/2000 Sb.

Zákazník **právnická osoba** ☐ uděluje [5] / ☐ neuděluje [5] souhlas s využitím adresy za účelem marketingu či propagace produktů a služeb poskytovatele.

4.2 Zákazník požaduje ☐ zasílat [5] / ☐ nezasílat [5] žadatelům o certifikáty upozornění na končící platnost certifikátů.

Legenda:
5 Označte křížkem příslušné políčko.

5. Pověřené osoby zákazníka

5.1 Pověřené osoby zákazníka jsou oprávněny s poskytovatelem jednat ve věci služeb, které jsou předmětem uzavírané smlouvy.

5.2 Seznam pověřených osob je uveden v přílohách č. _____ k této smlouvě. Seznam pověřených osob musí obsahovat alespoň jednu pověřenou osobu, kterou může být i osoba uvedená v části 1 této smlouvy jako zástupce zákazníka, a je-li zákazníkem fyzická osoba, tak tato fyzická osoba.

6. Společná a závěrečná ustanovení

6.1 Dne 3.8.2005 se na základě rozhodnutí Ministerstva informatiky ČR stala Česká pošta, s.p. akreditovaným poskytovatelem certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu.

6.2 Právní vztahy výslovně neupravené touto smlouvou se řídí příslušnými ustanoveními dokumentů uvedených v čl. 6.3 a 6.4 této smlouvy a obecně závaznými právními předpisy. V případě rozporu textu této smlouvy a těchto dokumentů, má přednost text této smlouvy.

6.3 Práva a povinnosti zákazníka i poskytovatele jsou uvedeny v těchto dokumentech: Všeobecné obchodní podmínky vybraných elektronických služeb České pošty, Certifikační politiky. Aktuální verze dokumentů jsou k dispozici na webových stránkách www.postsignum.cz. Podpisem této smlouvy zákazník prohlašuje, že se seznámil s obsahem těchto dokumentů a že s nimi souhlasí.

6.4 Cena za poskytované služby je uvedena v Ceníku služeb, jehož aktuální verze je umístěna na webových stránkách www.postsignum.cz.

6.5 Změny v dokumentech uvedených v odstavcích 6.2 a 6.3 nepodléhají udělení písemného souhlasu ze strany zákazníka. Plánované změny těchto dokumentů budou v předstihu zveřejněny na stránkách www.postsignum.cz.

6.6 Spory, které z tohoto vztahu vzniknou, se řeší u věcně a místně příslušného soudu.

6.7 Tato smlouva je vyhotovena ve dvou stejnopisech. Každá smluvní strana obdrží jedno vyhotovení smlouvy.

6.8 Akceptací této smlouvy ze strany poskytovatele dojde k uzavření smlouvy o poskytování služeb certifikační autority PostSignum.

7. Podpisy smluvních stran

Za poskytovatele

Místo	Datum
Jméno a příjmení	Podpis a razítko

Za zákazníka

Místo	Datum
Jméno a příjmení	Podpis a razítko

Číslo smlouvy [1]	

Příloha č. [redacted] smlouvy o poskytování certifikačních služeb
SEZNAM POVĚŘENÝCH OSOB

(zákazník – právnická osoba nebo podnikající fyzická osoba)

Udaje o pověřených osobách [2]

1.	**Jméno**		Tituly před		**Podpis pověřené osoby**
	Příjmení		Tituly za		
	Rodné číslo [3]				
	E-mailová adresa				
	Telefon				
	☐ Zasílat [4] / ☐ nezasílat [4] pověřené osobě informace o vydaných certifikátech e-mailem. [5]				
	☐ Zasílat [4] / ☐ nezasílat [4] pověřené osobě informace o zneplatněných certifikátech e-mailem. [5]				

2.	**Jméno**		Tituly před		**Podpis pověřené osoby**
	Příjmení		Tituly za		
	Rodné číslo [3]				
	E-mailová adresa				
	Telefon				
	☐ Zasílat [4] / ☐ nezasílat [4] pověřené osobě informace o vydaných certifikátech e-mailem. [5]				
	☐ Zasílat [4] / ☐ nezasílat [4] pověřené osobě informace o zneplatněných certifikátech e-mailem. [5]				

3.	**Jméno**		Tituly před		**Podpis pověřené osoby**
	Příjmení		Tituly za		
	Rodné číslo [3]				
	E-mailová adresa				
	Telefon				
	☐ Zasílat [4] / ☐ nezasílat [4] pověřené osobě informace o vydaných certifikátech e-mailem. [5]				
	☐ Zasílat [4] / ☐ nezasílat [4] pověřené osobě informace o zneplatněných certifikátech e-mailem. [5]				

Legenda:

1 Doplní pracovník České pošty.

2 Tučně vyznačené položky jsou povinné.

3 Pokud nebylo rodné číslo přiděleno v CR, vyplňte datum narození, pohlaví a občanství.

4 Označte křížkem příslušné políčko.

5 Informace jsou pověřeným osobám zasílány e-mailem. Informace je nutné si vyžádat, a to zasláním e-mailové zprávy na adresu postsignum@cpost.cz.

Pověřené osoby svým podpisem souhlasí s poskytnutím osobních údajů certifikační autoritě poskytovatele a s jejich zpracováním za účelem prokázání totožnosti v rozsahu jméno, příjmení a rodné číslo (u cizinců bez RČ přiděleného v ČR též datum narození, pohlaví a občanství) a dále údaje e-mailová adresa a telefon, které slouží pro zasílání informačních zpráv týkajících se poskytovaných certifikačních služeb (informování o zpracování zákaznických formulářů, informace o vydaných / zneplatněných certifikátech, atd.). Souhlas se uděluje na dobu trvání smluvního vztahu.

Pověřené osoby svým podpisem prohlašují, že byly poučeny ve smyslu § 11 a 12 zákona č. 101/2000 Sb., v tom smyslu, že povinnost poskytnout osobní údaje uvedené v tiskopisu nevyplývá ze zvláštních zákonů, ale jejich poskytnutí je dobrovolné. Pověřené osoby berou na vědomí, že pokud tyto informace neuvedou, nemohou být zákazníkovi ze strany poskytovatele poskytnuty požadované služby.

Pověřené osoby dále berou na vědomí informace o svém právu na přístup k osobním údajům, které jsou zpracované za účelem poskytnutí požadovaných služeb zákazníkovi (za účelem prokázání totožnosti a pro zasílání informačních zpráv), právu na opravu těchto osobních údajů i povinnosti poskytovatele na požádání pověřeným osobám sdělit informace o jejich zpracování, jakož i o dalších právech stanovených v §21 zákona č. 101/2000 Sb.

Podpisy smluvních stran

Za zákazníka

Za poskytovatele

PŘÍLOHA P III: SEZNAM ŽADATELŮ – ÚVODNÍ LIST

Číslo smlouvy [1]	

SEZNAM ŽADATELŮ
Úvodní list

(zákazník – právnická osoba nebo podnikající fyzická osoba)

1. Zákazník [1]

Název / Obchodní firma /
Jméno a příjmení: .....

IČ: .....

2. Osoba předkládající Seznam žadatelů (pověřená osoba[2], statutární orgán[3], podnikající fyzická osoba[3] nebo zmocněnec[3])

Jméno a příjmení: .....

Kontaktní telefon: .....

Kontaktní e-mail: .....

Legenda:

1 Doplňte údaje dle platné smlouvy.

2 Pokud má **pověřená osoba** kvalifikovaný nebo komerční osobní certifikát vydaný certifikační autoritou České pošty PostSignum, nemusí se dostavit osobně, ale může tento formulář včetně příloh poslat elektronicky podepsaným e-mailem na obchodní místo certifikační autority České pošty. Seznam obchodních míst, včetně kontaktů, je na webových stránkách www.postsignum.cz.

3 Pokud formulář předkládá statutární orgán, zmocněnec, podnikající fyzická osoba, která není zároveň pověřenou osobou, musí předložit doklad (výpis z OR, ZR, zmocnění) o tom, že je osobou oprávněnou jednat za zákazníka.

3. Přílohy Seznamu žadatelů – Udaje o žadatelích

Osoba předkládající Seznam žadatelů žádá, aby byly do evidence certifikační autority České pošty zaznamenány údaje žadatelů, které jsou uvedeny na jednotlivých číslovaných přílohách:

- ☐ Údaje pro vydávání certifikátů – přílohy č. _____
- ☐ Změna údajů pro vydávání certifikátů – přílohy č. _____

4. Podpis osoby předkládající Seznam žadatelů

.....	.....	.....
Místo	Datum	Podpis žadatele

5. Ověření podpisu osoby předkládající Seznam žadatelů pracovníkem Ceské pošty

Jméno a příjmení ověřovatele: .....

Datum a podpis ověřovatele: .....

PŘÍLOHA P IV: SEZNAM ŽADATELŮ – ÚDAJE PRO VYDÁVÁNÍ CERTIFIKÁTŮ

Číslo smlouvy [1]	

Příloha č. Seznamu žadatelů

ÚDAJE PRO VYDÁVÁNÍ CERTIFIKÁTŮ

(zákazník – právnická osoba nebo podnikající fyzická osoba)

1. Údaje o žadateli

Žadatel zaveden: (vyplňuje pracovník pošty) ☐

Jméno		**Tituly před**	
Příjmení		**Tituly za**	
Rodné číslo [2]			
Číslo zaměstnance			
Kontaktní e-mailová adresa			

☐ Přidělit [3] / ☐ nepřidělit [3] žadateli Identifikátor klienta MPSV (IK MPSV).

2. Údaje o osobních certifikátech

Požaduji vydání certifikátu dle certifikační politiky: [7] ☐ Kvalifikované osobní certifikáty
☐ Komerční osobní certifikáty

Povinné položky certifikátu:	*Pravidlo zavedeno:* (vyplňuje pracovník pošty) ☐
CN (jméno a příjmení, příp. tituly)	Viz údaje o žadateli v bodě 1.
OU3 (číslo zaměstnance)	Viz údaje o žadateli v bodě 1.
E-mailová adresa 1 [4]	
Nepovinné položky certifikátu:	
OU2 (organizační jednotka) [5]	
Title (funkce zaměstnance) [5]	
Jiné jméno (údaj určený zákazníkem) [6]	
E-mailová adresa 2	
E-mailová adresa 3	

☐ Zveřejnit [3] / ☐ nezveřejnit [3] vydaný certifikát na webových stránkách certifikační autority.
☐ Vložit [3] / ☐ nevložit [3] Identifikátor klienta MPSV (IK MPSV) do kvalifikovaného certifikátu.

3. Údaje o ostatních certifikátech

Požaduji vydání certifikátu dle certifikační politiky: [7] ☐ Kvalifikované systémové certifikáty
☐ Komerční serverové certifikáty

Povinné položky certifikátu:	*Pravidlo zavedeno:* (vyplňuje pracovník pošty) ☐
CN (název certifikátu) [8]	
Nepovinné položky certifikátu:	
OU2 (organizační jednotka) [5]	
Jiné jméno (údaj určený zákazníkem) [6]	
E-mailová adresa 1	
E-mailová adresa 2	
E-mailová adresa 3	

☐ Zveřejnit [3] / ☐ nezveřejnit [3] vydaný certifikát na webových stránkách certifikační autority.

Legenda:

1 Doplňte údaje dle platné smlouvy.

2 Pokud nebylo rodné číslo přiděleno v CR, vyplňte datum narození, pohlaví a občanství.

3 Označte křížkem příslušné políčko.

4 Pokud se e-mailová adresa 1 shoduje s kontaktní e-mailovou adresou v sekci Udaje o žadateli, nevyplňuje se.

5 V souladu odst. 2 § 1 Nařízení vlády č. 495/2004 Sb. musí být položky **OU2** a **Title** povinně vyplněny v případě osobních certifikátů pro zaměstnance orgánů veřejné moci.

6 Není předepsán obsah údaje **Jiné jméno**. Zákazník může uvést jakýkoliv text podle vlastního uvážení.

7 Označte křížkem certifikační politiku, dle které chcete vydat certifikát. Lze označit i více certifikačních politik současně.

8 Zádáte-li o vydání certifikátu, který má v názvu doménové jméno, je potřeba doložit formulář **Prohlášení vlastníka domény**.

PŘÍLOHA P V: OZNÁMENÍ O POVĚŘENÍ K ZAJIŠTĚNÍ VŠECH ÚKONŮ SOUVISEJÍCÍCH S E-PODÁNÍM ČSSZ

Oznámení o pověření k zajištění všech úkonů souvisejících s *e* - Podáním ČSSZ

(pro zastupující osobu)

Zastupující osoba

variabilní symbol IČ

se sídlem

ID datové schránky[1)]

jednající statutárním orgánem
(v případě, že se jedná o právnickou osobu)

zastupující při plnění povinností v oblasti nemocenského a důchodového pojištění a pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti zaměstnavatele:
(uvádí se variabilní symbol, název a sídlo zaměstnavatele)[2)]

+
-
-
-
-

oznamuje, že níže uvedené osoby byly pověřeny zajištěním všech úkonů souvisejících s[3)]

- ☐ předkládáním evidenčních listů důchodového pojištění (dle § 39 zákona č. 582/1991 Sb., ve znění pozdějších předpisů)
- ☐ přihlašováním a odhlašováním zaměstnanců a dalších úkonů (dle § 94 zákona č. 187/2006 Sb., ve znění pozdějších předpisů)
- ☐ předkládáním Přehledu o výši pojistného (dle § 9 zákona č. 589/1992 Sb., ve znění pozdějších předpisů)
- ☐ předáváním všech údajů a skutečností souvisejících s výplatou dávek nemocenského pojištění a dalších úkonů (dle § 97 zákona č. 187/2006 Sb., ve znění pozdějších předpisů):

+					
rodné číslo	jméno a příjmení[2)]	sériové číslo certifikátu[4)]	vystavitel certifikátu[4)]	e-mailová adresa	
					-

V _____ dne _____

_____
podpis zaměstnavatele
(razítko)

Upozornění:
Oprávněnost k zastupovaní je nutné doložit plnou mocí.

1) Uvede se v případě e-Podání zasílaného prostřednictvím datové schránky (e - Podáním se rozumí elektronická podání předávaná ve formě datových vět formátu XML).
2) V případě většího počtu zaměstnavatelů (pověřených osob) lze tyto uvést na zvláštní příloze.
3) Nehodící se škrtněte.
4) Údaj není nutné vyplnit v případě, že k Oznámení připojíte veřejnou část kvalifikovaného certifikátu. Tiskopis lze použít k nahlášení nového certifikátu, nebo lze pro tyto účely použít službu e - Podání UserCert.

Tiskopis ČSSZ