UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2009 **Petr BERNÝ**

Univerzita Pardubice

Fakulta ekonomicko-správní

Elektronická podání na portálu veřejné správy

Petr Berný

Bakalářská práce

2009

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Petr BERNÝ**

Studijní program: **B6209 Systémové inženýrství a informatika**

Studijní obor: **Informatika ve veřejné správě**

Název tématu: **Elektronická podání na portálu veřejné správy**

Zásady pro vypracování:

1. Základní informace, související s elektronickým podáním na portálu veřejné správy, o informačních systémech, šifrování dat a elektronickém podpisu
2. Popis Portálu veřejné správy
3. Elektronické podání na Portálu veřejné správy
4. Tvorba vlastní aplikace pro portál veřejné správy
5. Zhodnocení a využití aplikace

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

[1] **PETROUTSOS, Evangelos. Myslíme v jazyku Visual Basic .NET, 1. díl . [s.l.] : GRADA Publishing, 2003. 676 s. ISBN 80-247-0371-8.**

[2] **PETROUTSOS, Evangelos. Myslíme v jazyku Visual Basic .NET, 2. díl. [s.l.] : GRADA Publishing, 2003. 540 s. ISBN 80-247-0372-6.**

[3] **Šifrování [online]. 2000-2007 [cit. 2007-10-17]. Dostupný z WWW: <http://www.aspnet.cz/Search.aspx?Text=šifrování>. ISSN 1801-9447.**

[4] **Portál veřejné správy [online]. 2003-2007 [cit. 2007-10-17]. Dostupný z WWW: <www.portal.gov.cz>.**

[5] **Základní informace k e - Podání (společné) [online]. 2002 [cit. 2007-10-17]. Dostupný z WWW: <http://www.cssz.cz/epodani/zakladni_informace.asp>.**

Vedoucí bakalářské práce: **Ing. Milan Tomeš**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **6. října 2008**

Termín odevzdání bakalářské práce: **1. května 2009**

doc. Ing. Renáta Myšková, Ph.D.
děkanka

L.S.

doc Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 6. října 2008

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 24. 4. 2009

Petr Berný

Poděkování

Na tomto místě bych rád poděkoval vedoucímu mé bakalářské práce, za poskytnuté materiály a věcné připomínky k vypracování této práce.

SOUHRN

Bakalářská práce se zabývá problematikou elektronických podání přes portál veřejné správy, popisuje posílání přihlášky k nemocenskému pojištění se zaručeným elektronickým podpisem. Jsou v ní vysvětleny pojmy, které souvisí s touto problematikou. Dále popisuje vývoj vlastní aplikace pro elektronické podání.

KLÍČOVÁ SLOVA:

e-Government, elektronické podání, portál veřejné správy, GovTalk obálka

TITLE

Electronic filings on portal public administration

ABSTRACT

Bachelor thesis deals with electronic filing through the portal of public administration, describes the sending registration to the sickness insurance is an advanced electronic signature. The thesis explains the terms that are relevant to this issue. It also describes the development of applications for Electronic filing.

KEYWORDS:

e-Government, electronic filing, portal public administration, GovTalk envelope

Obsah:

1 Úvod 11

2 Elektronické podání 12

2.1 E-Government 12

2.2 Portál veřejné správy 12

2.2.1 Historie 13

2.2.2 Funkce 13

2.2.2.1 Informační funkce portálu veřejné správy 13

2.2.2.2 Transakční funkce portálu veřejné správy 15

3 Elektronické podání na PVS 16

3.1 Služby poskytované transakční částí portálu 16

3.2 Zabezpečení 17

3.2.1 Zabezpečená spojení 17

3.2.2 Elektronický podpis 18

3.2.3 Šifrování 18

3.2.3.1 Symetrické šifrování 18

3.2.3.2 Asymetrické šifrování 19

3.2.3.3 Hybridní šifrování 21

3.2.4 Digitální certifikát 21

3.2.5 Hash funkce 24

3.2.6 Použití elektornického podpisu 24

3.2.7 Uživatelské identifikátory 25

3.3 Osm kroků k úspěšnému e-podání 25

3.4 Transakce datové zprávy 26
3.4.1 Základní architektura 26
3.4.2 Typy datových zpráv 27
3.4.2.1 Posílané datové zprávy 27
3.4.2.2 Přijímané datové zprávy 27
3.4.3 Příklad úspěšného podání 28
3.5 Datová zpráva 30
3.5.1 Tělo datové zprávy 30
3.5.1.1 Datová věta 31
3.5.1.2 Obálka pro ČSSZ 34
3.5.1.3 Elektronický podpis 35
3.5.1.4 Zašifrování datové věty 35
3.5.2 GovTalk obálka 36
3.5.2.1 Popis dat 36
4 Vlastní zpracování 44
4.1 Zajištění potřebného digitálního certifikátu 44
4.1.1 Výběr certifikační autority 44
4.1.2 Proces získání certifikátu 45
4.1.3 Instalace certifikátu 46
4.2 Registrace u České správy sociálního zabezpečení 47
4.3 Registrace na portálu veřejné správy 47
4.3.1 Výběr role uživatele vůči veřejné správě 48
4.3.1.1 Občan 48

4.3.1.2 Organizace 48
4.3.1.3 Zástupci 48
4.3.2 Proces registrace a aktivace služeb 48
4.4 Vývoj vlastní aplikace pro podání přes PVS 50
4.4.1 Formulář a požadavky na vyplněná data 50
4.4.2 Vlastní návrh databáze 53
4.4.3 Návrh prostředí pro vstup dat 55
4.4.4 Logické testy 55
4.4.4.1 Kontrola rodného čísla 55
4.4.4.2 Kontrola IDENTIFIKAČNÍHO čísla 57
4.4.5 Generování datové zprávy pomocí aplikace 58
4.4.6 Podepsání datové zprávy 59
4.4.7 Šifrování datové zprávy 60
4.4.8 Transakce datové zprávy na portál veřejné správy 60
4.4.8.1 Odeslání a příjem datové zprávy 61
4.4.8.2 Parsování přijaté zprávy 61
4.4.9 Testování elektronického podání 62
5 Zhodnocení a využití aplikace 63
6 Závěr 64
7 Použitá literatura 66
Seznam obrázků tabulek a grafů 68
Seznam příloh 69

1 ÚVOD

Tato bakalářská práce se zabývá problematikou elektronického podání na portálu veřejné správy a vývojem softwaru pro posílání přihlášky k nemocenskému pojištění elektronickou cestou.

S rozvojem e-Governmentu, který umožňuje styk osob a podniků s úřady veřejné správy elektronickou cestou, roste i číslo počtu elektronických podání respektive poslaných formulářů. Práce je zaměřena na podání přihlášky k nemocenskému pojištění, tudíž cílovým úřadem veřejné správy bude Česká správa sociálního zabezpečení (ČSSZ).

Cílem této bakalářské práce je porozumění a popsání problematiky elektronického podání přes portál veřejné správy, se kterou souvisí pojmy jako e-Government, portál veřejné správy, digitální certifikát, šifrování, elektronický podpis aj. Druhým cílem je vytvoření vlastní aplikace, která tyto teoretické principy ověří v praxi.

Úvodní kapitoly pojednávají o e-Governmentu, portálu veřejné správy, jeho historii a funkcích.

Následuje kapitola elektronické podání na portálu veřejné správy, která se zabývá teoretickou stránkou elektronického podání, která tento pojem vysvětluje, dále se zabývá zabezpečením souvisejícím s touto problematikou a samotným podáním.

Poté bude následovat rozsáhlý oddíl týkající se vlastnímu zpracování aplikace pro elektornickéh podání, kde budou realizovány teoretické poznatky z předchozích kapitol a vývoj vlastní aplikace pro elektronické podání přes portál veřejné správy.

2 ELEKTRONICKÉ PODÁNÍ

Tato kapitola pojednává o e-Governmentu, vzniku portálu veřejné správy a o funkcích portálu, kde jednou z funkcí je i elektronické podání.

2.1 E-GOVERNMENT

Pro tento pojem neexistuje český ekvivalent, a proto je zde uvedena nejprve definice od již neexistujícího Ministerstva informatiky České republiky. Činnost tohoto ministerstva převzala Rada vlády pro informační společnost spadající pod Ministerstvo vnitra České republiky. E-government je touto institucí definován takto:

„e-Government" představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům. [10]

Z této definice není úplně zřejmé, co si vlastně pod tímto pojmem máme představit. Zjednodušeně řečeno e-Government je elektronizace výkonů veřejné správy. Jedním z několika cílů je zjednodušení komunikace občanů a firem s úřady veřejné správy, ale také zjednodušení a zefektivnění komunikace na úrovni veřejná správa-veřejná správa. Mezi další cíle patří úspora času, zrychlení vnitřních procesů, zvýšení konkurenceschopnosti v globální ekonomice, zvýšení transparentnosti aj.

2.2 PORTÁL VEŘEJNÉ SPRÁVY

Portál veřejné správy (PVS) je elektronická brána do veřejné správy. Vznikl na základě zákona č. 365/2000 Sb., o ISVS. Hlavním smyslem portálu je usnadnit občanům a firmám orientaci (informační část) a komunikaci (transakční část) s úřady veřejné správy. [16]

2.2.1 HISTORIE

Projekt portál veřejné správy je velmi mladý, v roce 2000 zákon č. 365/2000 Sb. uložil Úřadu pro veřejné informační systémy povinnost zřízení tohoto portálu. Již v tomto roce vznikl prototyp, který jen shromažďoval odkazy na internetové stránky státních institucí.

Následující rok, tedy v roce 2001, byla snaha o vytvoření „opravdového" funkčního portálu. Byla provedena projektová studie a v roce 2002 sestaven realizační tým, do kterého se zapojily firmy IBM, Microsoft a Český Telecom jako generální dodavatel. Březen 2003 přinesl v pověření nově vzniklého Ministerstva informatiky první betaverzi, která byla představena na konferenci Internet ve státní správě a samosprávě (ISSS) v Hradci Králové. Po půl roce byl spuštěn měsíční zkušební provoz pro veřejnou správu a oficiální spuštění portálu veřejné správy se konalo v říjnu na výstavě Invex. [21]

2.2.2 FUNKCE

Jednou z hlavních funkcí je umožnění komunikace přes elektronická zařízení s veřejnou správou, usnadnění orientace a komunikace firem a občanů s úřady veřejné správy.

Funkce portálu může rozdělit do dvou oblastí:

1. Informační
2. Transakční

2.2.2.1 INFORMAČNÍ FUNKCE PORTÁLU VEŘEJNÉ SPRÁVY

Informační část portálu přináší aktuální a garantované informace o České republice, parlamentu, vládě, prezidentovi a jednotlivých ministerstev. Dále zde najdeme informace o úřadech nižší úrovně, Evropské unii, adresář, zákony, životní situace, elektronické zpravodajství čtrnáctideník vlády České republiky, slovník pojmů a mapy.

Informační část portálu veřejné správy je rozdělena na tři části:

1. ***Občan***

   Pod tímto odkazem najdeme informace o všech úřadech a radnicích v České republice, jejich úřední hodiny, adresy aj. Základní formuláře a

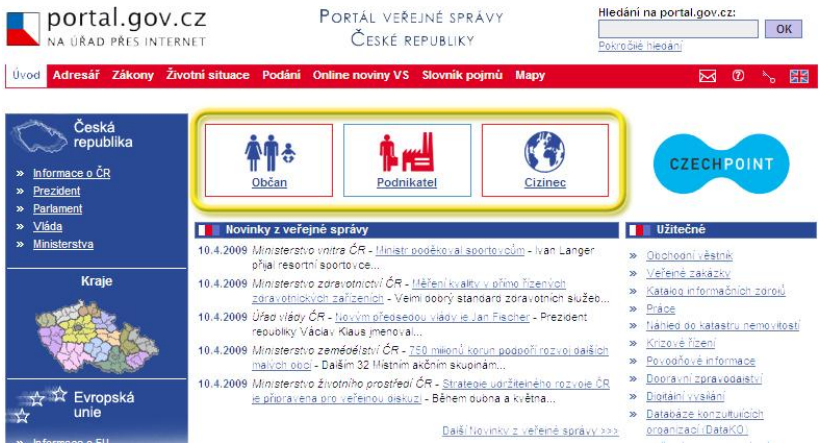
dokumenty pro jednání s úřady, životní situace, které slouží jako návody jak řešit různé situace, kde dochází k interakci občana s úřady veřejné správy, například vydání cestovního pasu. U této životní situace nám poradí, kdo může požádat o cestovní pas, jaké doklady a formuláře budeme potřebovat, který úřad máme navštívit, poplatky a další informace, které souvisí s vydáním cestovního pasu.

2. ***Podnikatel***

V této části portálu uživatel získá informace o podnikatelské činnosti, veřejných zakázkách, pracovně právních vztazích, dále informace o daňovém systému, rozvoji podnikání a spoustu dalších informací a odkazů na jiné servery, které se zabývají touto problematikou.

3. ***Cizinec***

Odkaz cizinec je určen pro jedince, kteří cestují do České republiky jako turisté, podnikatelé nebo studenti. Jedno z prvních témat je „Než přijedete do ČR“, kde se občané žijící v zahraničí mohou dočíst informace o České republice, o cestování v České republice, důležité kontakty. Mezi další témata patří pobyt na území ČR, zaměstnání, systém školství, podnikání, systém zdravotnictví a zdravotních pojišťoven.



Obrázek 1 Portál veřejné správy, zdroj: [vlastní]

Toto rozdělení je vyznačeno žlutým rámečkem na obrázkuObrázek 1 a má napomoci uživatelům stránek k lepší orientaci a celkovému zpřehlednění webových stránek.

2.2.2.2 TRANSAKČNÍ FUNKCE PORTÁLU VEŘEJNÉ SPRÁVY

Hlavním úkolem transakční části portálu je zprovoznění elektronických služeb veřejné správy, tak aby bylo možné zajistit výměnu dat mezi občany a firmami na jedné straně a orgány veřejné správy na straně druhé. Další a to samostatnou oblastí je výměna dat mezi samotnými orgány veřejné správy. Hlavním cílem je umožnění vyřizování co nejširšího okruhu činností elektronickou cestou, kdy občan nebo firma nemusí podávat klasické papírové formuláře, ale mohou tyto informace předat orgánům veřejné správy elektronickou cestou. Výrazný přínos aplikace je však i na straně zapojených institucí, které mohou s daty dále pracovat a tím odpadají náklady na převod údajů z papírové do elektronické podoby. Díky jednotnému a již odzkoušenému způsobu elektronického předávání dat se pak mohou subjekty veřejné správy zaměřovat na rychlý vývoj online služeb místo opakovaného vytváření společných základních stavebních prvků požadovaných pro všechny služby online. [22]

Transakční část portálu veřejné správy poskytuje tři základní služby: [22]

1. společnou infrastrukturu, která umožňuje propojení na jednotlivé úřady veřejné správy
2. uživatelům jednotný přístup ke všem zprovozněným elektronických službám
3. úřadům bezpečnou infrastrukturu a opakovaně použitelné komponenty

3 ELEKTRONICKÉ PODÁNÍ NA PVS

Elektronické podání je jednou z funkcí transakční části portálu veřejné správy a je dostupné na adrese https://bezpecne.podani.gov.cz/default.aspx nebo z odkazu „Podání“ v hlavní nabídce na stránkách portálu veřejné správy, jehož webová adresa je http://portal.gov.cz.

Celé řešení aplikace Elektronická podání má maximálně zjednodušit komunikaci uživatele s veřejnou správou. Bez centrálního řešení transakční části by uživatelé byli nuceni přistupovat k jednotlivým elektronickým službám veřejné správy nekonzistentním a nejednotným způsobem. V rámci různých resortů by uživatelé museli používat různá přihlašovací jména, hesla a různé způsoby komunikace. [2]

Z pohledu občanů, organizací a zprostředkovatelských firem řešení Elektronická podání nahrazuje tyto individuální přístupy a vytváří jednotný a bezpečný vstupní bod do veřejné správy. Řešení nabízí jednotné přihlášení pro všechny typy elektronických služeb, které jsou v rámci aplikace Elektronická podání implementovány, a umožňuje jednoduchou komunikaci s různými úřady veřejné správy. [2]

Pro uživatele to v praxi znamená, existenci jednoho centrálního vstupního bodu, který poskytuje bezpečné doručování elektronických formulářů pro zprovozněné služby za použití jednotné digitální identity. V případě zapojení všech elektronických služeb pro životní a obchodní situace v aplikaci Elektronická podání by občané a organizace mohli podávat veškeré elektronické dokumenty jednotným způsobem na jednom místě. [2]

3.1 SLUŽBY POSKYTOVANÉ TRANSAKČNÍ ČÁSTÍ PORTÁLU

Tabulka Tabulka 1 znázorňuje přehled poskytovaných služeb pro elektronické podání přes portál veřejné správy.

Tabulka 1 Služby poskytované pro elektronické podání přes portál veřejné správy, zdroj: [20]

SLUŽBY POSKYTOVANÉ PRO ELEKTRONICKÉ PODÁNÍ	
úřad veřejní správy	**poskytované služby**
Ministerstvo financí	Daň z přidané hodnoty
	Daň z příjmů fyzických osob
	Daň z příjmů právnických osob
	Závislá činnost
	Daň silniční
	Daň z nemovitostí
	Oznámení podle §34 zákona č.337/1992 Sb.
	Hlášení platebního zprostředkovatele
	Obecné písemnosti určené pro Finanční úřad
Ministerstvo dopravy	eTesty
Ministerstvo životního prostředí	Registr znečišťovatelů
Ministerstvo průmyslu a obchodu	Roční výkaz o poštovních službách
ČSSZ	Důchodové pojištění
	Podání evidenčních listů důchodového pojištění
	Nemocenské pojištění, Přihlášky/Odhlášky
	Přehled o příjmech a výdajích OSVČ

3.2 ZABEZPEČENÍ

Na bezpečnost se kladou vysoké nároky, jelikož dochází k posílání osobních a citlivých údajů elektronickou cestou na orgány veřejné správy. Zabezpečení je zajišťováno na těchto úrovních:

1. Zabezpečená spojení
2. Šifrování
3. Použití digitálních certifikátů
4. Uživatelské identifikátory

3.2.1 ZABEZPEČENÁ SPOJENÍ

Informace posílané a přijímané jsou přenášeny přes 128bitové zabezpečené připojení, tak zvané SSL (Secure socket layer). SSL je protokol, respektive vrstva nacházející se mezi vrstvou transportní a aplikační, která slouží k zabezpečení komunikace šifrováním a autentizaci komunikujících stran pomocí digitálních certifikátů.

3.2.2 ELEKTRONICKÝ PODPIS

Při podepisování listinných dokumentů používáme vlastnoruční podpis. Tento podpis je jedinečný a jeho zfalšování není snadné, jelikož každý máme jiný rukopis a zkušený grafolog odhalí, zda je podpis pravý respektive jen napodobený. K podepsání elektronického dokumentu je tento podpis nevyhovující tedy nepoužitelný. Elektronický dokument je snadno modifikovatelný a podepsat se zde může kdokoliv za kohokoliv, aniž by nějaký grafologický rozbor mohl najít nějaký rozdíl. Proto je zde čas na využití elektronického podpisu, který zaručí integritu zprávy a identifikaci osoby podepisující elektronickým dokument. S elektronickým podpisem souvisí šifrování, hash funkce a digitální certifikáty.

Elektronický podpis je definován jako data v elektronické podobě, která jsou připojena k jiným elektronickým datům nebo jsou s nimi logicky spojena, a která slouží jako metoda autentizace. [12]

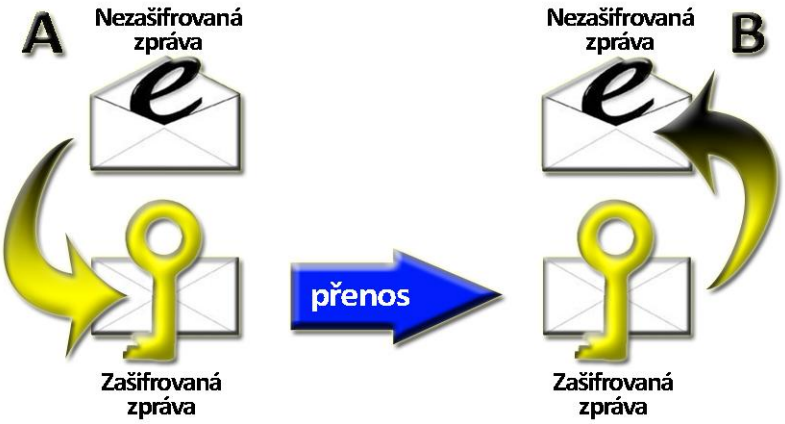
3.2.3 ŠIFROVÁNÍ

Šifrováním si představíme takový úkon, kdy například z námi či strojem čitelného textu vytvoříme pomocí šifrování text, který my nebo stroj bez znalosti šifry použité k zašifrování prostého textu nepřečteme. Používají se tři základní typy šifrování:

1. Symetrické šifrování
2. Asymetrické šifrování
3. Hybridní šifrování

3.2.3.1 SYMETRICKÉ ŠIFROVÁNÍ

Symetrické šifrování předpokládá existenci právě jednoho šifrovacího klíče, který si musí uživatelé komunikující spolu vyměnit zabezpečeným komunikačním kanálem. Postup šifrování a přenosu je patrný z obrázkuObrázek 2, kde odesílatel (A) zašifruje zprávu klíčem, který má i příjemce (B). Příjemce pomocí téhož šifrovacího klíče dešifruje zprávu a tím získá dokument, který byl na začátku tohoto procesu. Mezi výhody patří jednoduchost a rychlost. Jeho hlavní nevýhodou je prvotní krok a to výměna šifrovacího klíče. [13]

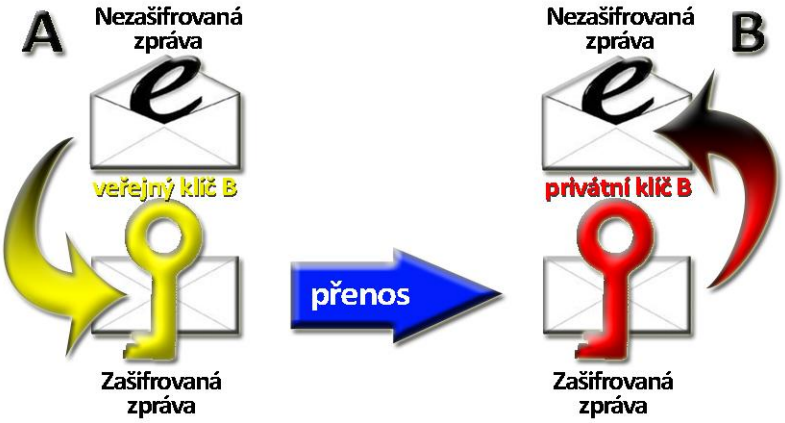


Obrázek 2 Symetrické šifrování, zdroj: [vlastní]

3.2.3.2 ASYMETRICKÉ ŠIFROVÁNÍ

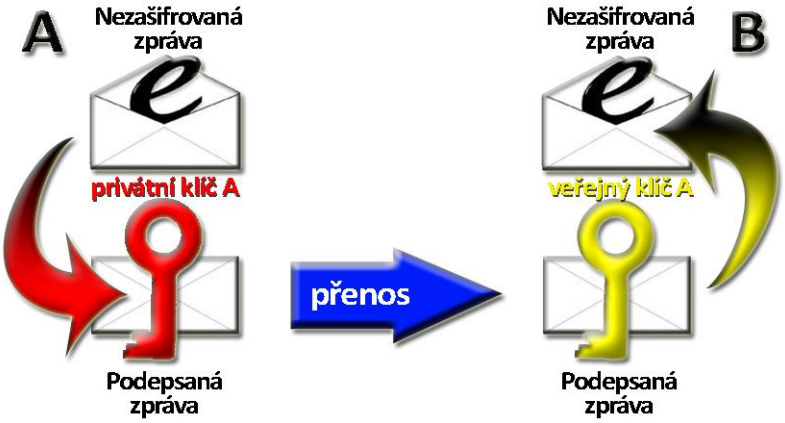
Tato šifrovací metoda předpokládá existenci dvou klíčů, první klíč je privátní a druhý veřejný. Mezi těmito klíči existuje matematický vztah, ale z veřejného klíče nelze dostupnými výpočetními operacemi získat klíč privátní. Privátní klíč by si měl vlastník pečlivě uschovat a veřejný klíč distribuovat uživatelům, se kterými bude komunikovat. Asymetrické šifrování se dá využít buď k zašifrování zprávy, nebo k podepsání zprávy. [14]

Obrázek Obrázek 3 graficky znázorňuje postup, kdy nezašifrovanou zprávu odesílatel (A) zašifruje veřejným klíčem příjemce (B). Poté může zprávu odeslat nezabezpečeným kanálem, aniž by si někdo mohl zprávu přečíst, jelikož zde platí, co je zašifrováno jedním klíčem jde dešifrovat pouze druhým klíčem. V posledním krok příjemce dešifruje zprávu vlastním privátním klíčem a dostane zprávu, která byla na počátku komunikace.



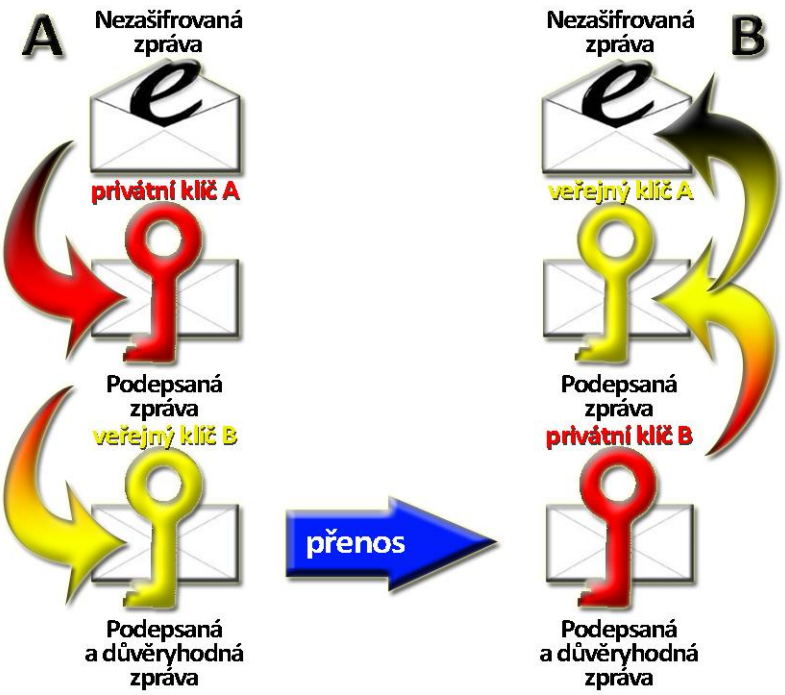
Obrázek 3 Asymetrické šifrování - šifrování zprávy, zdroj: [vlastní]

Následující obrázek Obrázek 4 se liší od minulého pouze použitím typu klíče na šifrování a dešifrování. Tento způsob zajistí identifikaci odesílatele zprávy. V prvním kroku se zašifruje, respektive podepíše zpráva privátním klíčem odesílatele (A). Jelikož veřejný klíč může mít více lidí, tudíž zpráva není šifrována proti zneužití, ale je jen podepsaná. Příjemce mající veřejný klíč odesílatele může přečíst jen zašifrovanou zprávu privátním klíčem odesílatele a tímto je zajištěna identifikace a podmínka nezpochybnitelnosti odpovědnosti.



Obrázek 4 Asymetrické šifrování - podepisování zprávy, zdroj: [vlastní]

Kombinaci předcházejících metod asymetrického šifrování je použita v obrázku Obrázek 5. Zašifrováním zprávy privátním klíčem odesílatele (A), následně veřejným klíčem příjemce (B) je dosaženo podepsané a důvěryhodné zprávy. Příjemce nejprve dešifruje zprávu privátním klíčem B, poté veřejným klíčem A. Takto získaná zpráva je důvěryhodná a příjemce (B) má jistotu, že pochází od odesílatele A. [14]



Obrázek 5 Asymetrické šifrování - kombinace metod, zdroj: [vlastní]

3.2.3.3 HYBRIDNÍ ŠIFROVÁNÍ

Hybridní šifrování spojuje předcházející popsané metody. Tato metoda vybírá pozitivní vlastnosti ze symetrického a asymetrického šifrování a tím vzniká způsob šifrování, který je bezpečný a rychlý. [15]

Postup šifrování, který specifikuje tuto metodu, je založen na zašifrování zprávy symetrickým klíčem a tento klíč je zašifrován pomalejšími asymetrickými algoritmy veřejného klíče. Tím je zajištěn bezpečný přenos šifrovacího klíče. [15]

3.2.4 DIGITÁLNÍ CERTIFIKÁT

Jako v běžném životě člověk prokazuje svoji totožnost různými doklady, tak i ve virtuálním světě je potřeba v některých situacích prokázat svoji identitu. K tomu nám ale běžné doklady totožnosti nepostačí a je třeba najít takový způsob, který spojí člověka s nějakou identifikací, která bude „čitelná“ pro počítač. Tuto specifikaci splňuje digitální certifikát.

Digitálních certifikátů máme hned několik druhů, záleží, na co jsou používány. První certifikační autorita nabízí kvalifikované certifikáty, komerční certifikáty, TWINS,

což je kombinace kvalifikovaného a komerčního certifikátu, komerční certifikát pro server a kvalifikovaný systémový certifikát. Pro účely komunikace s úřady veřejné správy je potřebný kvalifikovaný certifikát.

Kvalifikovaný certifikát je vytvořen tak, že splňuje všechny aktuální požadavky dané legislativou, Zákonem o elektronickém podpisu (Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů ve znění zákona č. 226/2002 Sb.). Je vhodný především pro komunikaci občanů se státní správou a samosprávou. Kvalifikovaný certifikát využijí všichni občané, firmy, úřady a také např. lékaři, advokáti nebo firmy komunikující často s Českou správou sociálního zabezpečení, s finančními úřady, se zdravotními pojišťovnami s celním úřadem aj. [3]

Používaní kvalifikovaných certifikátů přináší významnou úsporu času jak pro firmy, tak i pro ostatní uživatele. Účely pro které je možné certifikát použít jsou [3]:

- vytváření elektronického podpisu
- ověřování elektronického podpisu
- zajištění neodmítnutelnosti odpovědi

Abychom mohli označit digitální certifikát opravdu za důvěryhodný, musí být vydán třetí nezávislou stranou, tou je certifikační autorita. Vydáním certifikátu certifikační autorita stvrzuje, že subjekt, jenž je držitelem certifikátu, skutečně vlastní pár klíčů a to elektronický klíč veřejný a soukromý neboli privátní. [17]

Certifikát je datovým souborem ve standardizovaném a mezinárodně uznávaném formátu, který se označuje X.509. X.509 jednoznačně definuje strukturu certifikátu tedy uvádí, co by měl každý certifikát v tomto formátu obsahovat [23]:

1. ***verze (version)***

   Popisuje verzi zakódovaného certifikátu.

2. ***sériové číslo (serialNumber)***

   Celočíselné vyjádření přidělené certifikační autoritou ke každému certifikátu.

3. ***podpis (signature)***

   Identifikátor algoritmu pro algoritmus použitý certifikační autoritou k podepsání certifikátu.

4. ***vydavatel (issuer)***

   Identifikace vydavatele certifikátů, který zároveň certifikát podepíše.

5. ***platnost (validity)***

   Reprezentuje dobu, po kterou certifikační autorita zaručuje uchování informací o stavu vydaného certifikátu. Tento element obsahuje datum, kdy platnost certifikátů začíná (notBefore) a datum, které udává, kdy platnost certifikátu končí (notAfter).

6. ***subjekt (subject)***

   Identifikační údaje o držiteli, které musí certifikační autorita řádně ověřit.

7. ***informace o veřejném klíči subjektu (subjectPublicKeyInfo)***

   Tato položka v certifikátu nese informaci o identifikaci algoritmu veřejného klíče subjektu a samotný veřejný klíč subjektu.

8. ***unikátní identifikátor vydavatele (issuerUniqueID)***

   Jednoznačně identifikuje certifikační autoritu, která vydala certifikát.

9. ***unikátní identifikátor subjektu (subjectUniqueID)***

   Jednoznačně identifikuje držitele certifikátu vydaného certifikační autoritou.

10. ***rozšiřující informace certifikátu (extensions)***

3.2.5 HASH FUNKCE

Hash funkce je transformace, kde na vstupu je řetězec proměnlivé délky a výstupem je řetězec pevné délky tzv. hash nebo otisk. Mezi nejrozšířenější has algoritmy, patří MD5 a SHA-1. Nároky na hashovací funkci používanou v kryptografii [1]:

1. ***vstup může být jakékoliv délky***
2. ***výstup musí mít pevnou délku***

   Výstupem hashovací funkce, je řetězec, jehož délka je určena podle použitého algoritmu. Běžné délky výstupního řetězce jsou 128, 160, 256, 512 bitů.

3. ***hodnota hash musí být jednoduše vypočitatelná pro jakýkoli vstupní řetězec***
4. ***funkce je jednosměrná***

   Jednosměrnost funkce je podmíněna tím, že není možné jednoznačně najít k otisku původní text.

5. ***funkce je bez kolizní***

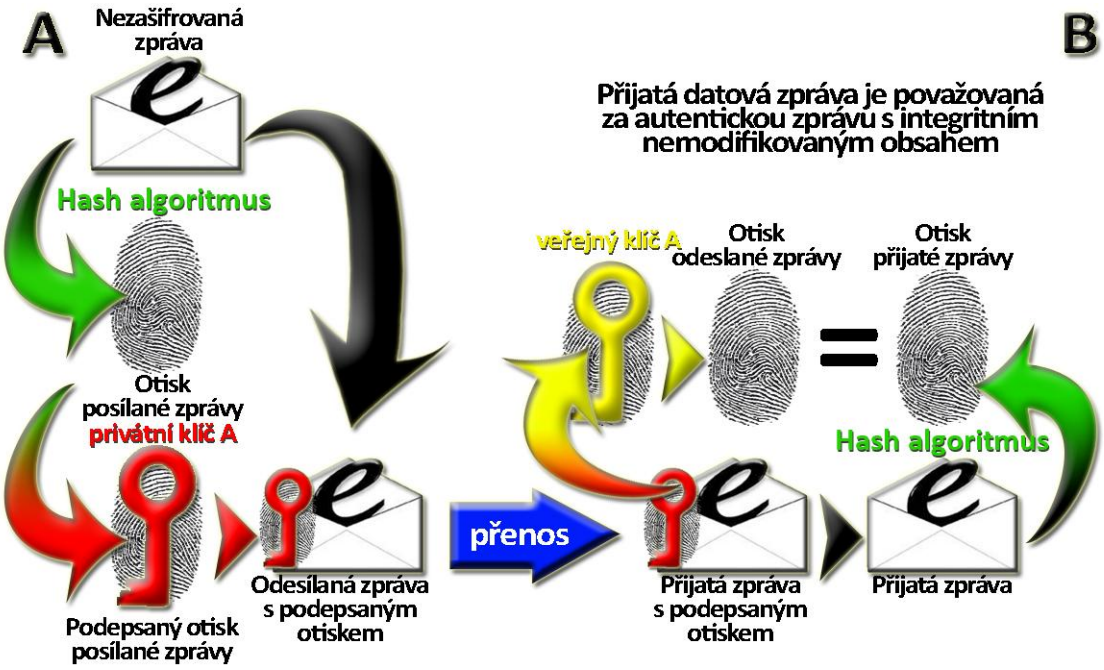
   Pokud je funkce slabě bezkolizní, to znamená, že není možné jednoznačně vymyslet takový text, který by měl stejný otisk. Silně bezkolizní funkce předpokládá neexistenci druhého textu se stejným otiskem.

3.2.6 POUŽITÍ ELEKTORNICKÉHO PODPISU

Základními algoritmy, používanými k podpisu datových zpráv, jsou algoritmy RSA (Rivest-Shamir-Adleman) a DSA (Digital Signature Algorithm). U RSA je bezpečnost založena na rozkladu velkého čísla na součin dvou prvočísel (tzv. faktorizace) a u DSA je bezpečnost postavena na matematickém aparátu diskrétních algoritmů. [18]

Při vytváření elektronického podpisu datové zprávy, je nutné nejprve vytvořit pomocí hash funkce otisk datové zprávy. Na obrázku Obrázek 6 ho reprezentuje otisk prstu. Tento otisk odesílatel (A) zašifruje privátním klíčem (A) a takto vytvořený podpis přiloží ke zprávě a odešle příjemci zprávy. Příjemce pomocí stejného hashovacího algoritmu vypočte kontrolní

vzorek přijaté zprávy, v dalším kroku veřejným klíčem (A) dešifruje přiložený podpis, tím ověří identitu odesílatele a následně porovná dešifrovaný otisk zprávy posílané a otisk zprávy přijaté. Pokud se tyto otisky rovnají, znamená to, že zpráva nebyla změněna, nerovnají-li se, někdo musel datovou zprávu na cestě od odesílatele k příjemci změnit.



Obrázek 6 Posílání podepsané zprávy elektronickým podpisem, zdroj: [vlastní]

3.2.7 UŽIVATELSKÉ IDENTIFIKÁTORY

Pokud služba nevyžaduje přihlášení pomocí certifikátu, postačí použití uživatelského identifikátoru, který vydá aplikace Elektronické podání a heslo, které si uživatel dle svého uvážení zvolí sám.

3.3 OSM KROKŮ K ÚSPĚŠNÉMU E-PODÁNÍ

1. Zajištění potřebného digitálního certifikátu
2. Registrace potřebných údajů u orgánů veřejné správy, se kterými bude probíhat komunikace
3. Registrace na portálu veřejné správy a aktivace služeb
4. Vyplnit údaje požadované aktivovanou službou

5. Z vyplněných údajů vytvořit datovou zprávu ve formátu xml, která bude odpovídat požadovaným standardům
6. Elektronicky podepsat zprávu
7. Zašifrovat zprávu
8. Odeslat zprávu přes portál veřejné správy na požadovaný orgán veřejné správy

Uvedené kroky budou podrobně rozebrány v následujících kapitolách.

3.4 TRANSAKCE DATOVÉ ZPRÁVY

Transakce datové zprávy, je jednou z hlavních a podstatných částí, bez které by elektronické podání nemohlo fungovat. Datová zpráva je přenášena od uživatele do aplikace elektronického podání a naopak. V následujících kapitolách je uvedena architektura elektronického podání a popis úspěšného elektronického podání přes portál veřejné správy na úřad České správy sociálního zabezpečení.

3.4.1 ZÁKLADNÍ ARCHITEKTURA

Celý systém transakce se skládá ze šesti základních částí, což je patrné z obrázku Obrázek 7. Uživatelská aplikace vytvoří datovou zprávu, a pošle ji prostřednictvím internetu do aplikace elektronického podání portálu veřejné správy (EP PVS). Transakční jádro, které je součástí aplikace EP PVS poskytuje jednotné prostředí pro příjem veškerých typů podání, provádí kontrolu identity odesílatele, předává podání úřadu veřejné správy respektive komunikuje s DIS serverem a zasílá potvrzení uživateli. Než je předána datová zpráva úřadu veřejné správy probíhá komunikace aplikace EP PVS se serverem DIS (Department interface server). Mezi jeho hlavní funkce patří standardizované propojení s transakčním jádrem, zabezpečuje zaručené doručení, to znamená, že doručí právě jednu ze všech xml zpráv. Příchozí zprávy opatřuje unikátním identifikátorem a časovým razítkem. Dále archivuje všechny provedené transakce pro potřeby auditu a reklamací, provádí kontrolu a transformaci datových formátů, posílá zprávy o stavu vyřízení žádosti a provádí dešifrování zabezpečeného obsahu zpráv. [4]

Obrázek 7 Základní architektura systému elektronického podání, zdorj [vlastní]

3.4.2 TYPY DATOVÝCH ZPRÁV

Datové zprávy se mohou rozdělit do dvou kategorií. První z nich jsou datové zprávy posílané a druhou kategorií jsou zprávy přijímané.

3.4.2.1 POSÍLANÉ DATOVÉ ZPRÁVY

Mezi posílané datové zprávy patří zpráva typu SUBMISSION_REQUEST, SUBMISSION_POLL a DELETE_REQUEST. Struktury těchto datových zpráv jsou uvedeny v přílohách 4-6.

Zpráva typu SUBMISSION_REQUEST zahajuje komunikaci s aplikací Elektronické podání portálu veřejné správy. Ostatní zprávy jsou reakcí na přijaté zprávy od aplikace PVS.

3.4.2.2 PŘIJÍMANÉ DATOVÉ ZPRÁVY

Aplikace Elektronického podání portálu veřejné správy generuje pět typů zpráv. Zprávy, které potvrzují úspěšné doručení posílané zprávy, končí slovem RESPONSE. Tuto odpověď můžeme dostat na zprávu SUBMISSION_REQUEST respektive SUBMISSION_POLL a tedy reakcí je zpráva SUBMISSION_RESPONSE. Durhou možností je reakce na zprávu typu DELETE_REQUEST zprávou DELETE_RESPONSE. Další možností, která může nastat, je, pokud aplikace Elektronického podání je zaneprázdněna a oznamuje nám, že podání nebylo zpracováno ani předáno dále, zároveň však aplikace přidělí podání unikátní identifikátor CorrelationID, se kterým musí naše aplikace nadále pracovat. Takové typy zpráv jsou SUBMISSION_ACKNOWLEDGEMENT a DELETE_ACKNOWLEDGEMENT. Strukturu těchto zpráv je možné si prohlédnout v příloze 7-10. Ještě schází jeden typ datové zprávy a tím je SUBMISSION_ERROR, který aplikace Elektronického podání PVS pošle, pokud je jí podstrčena buď nesprávně sestavená datová zpráva, nebo chybné údaje.

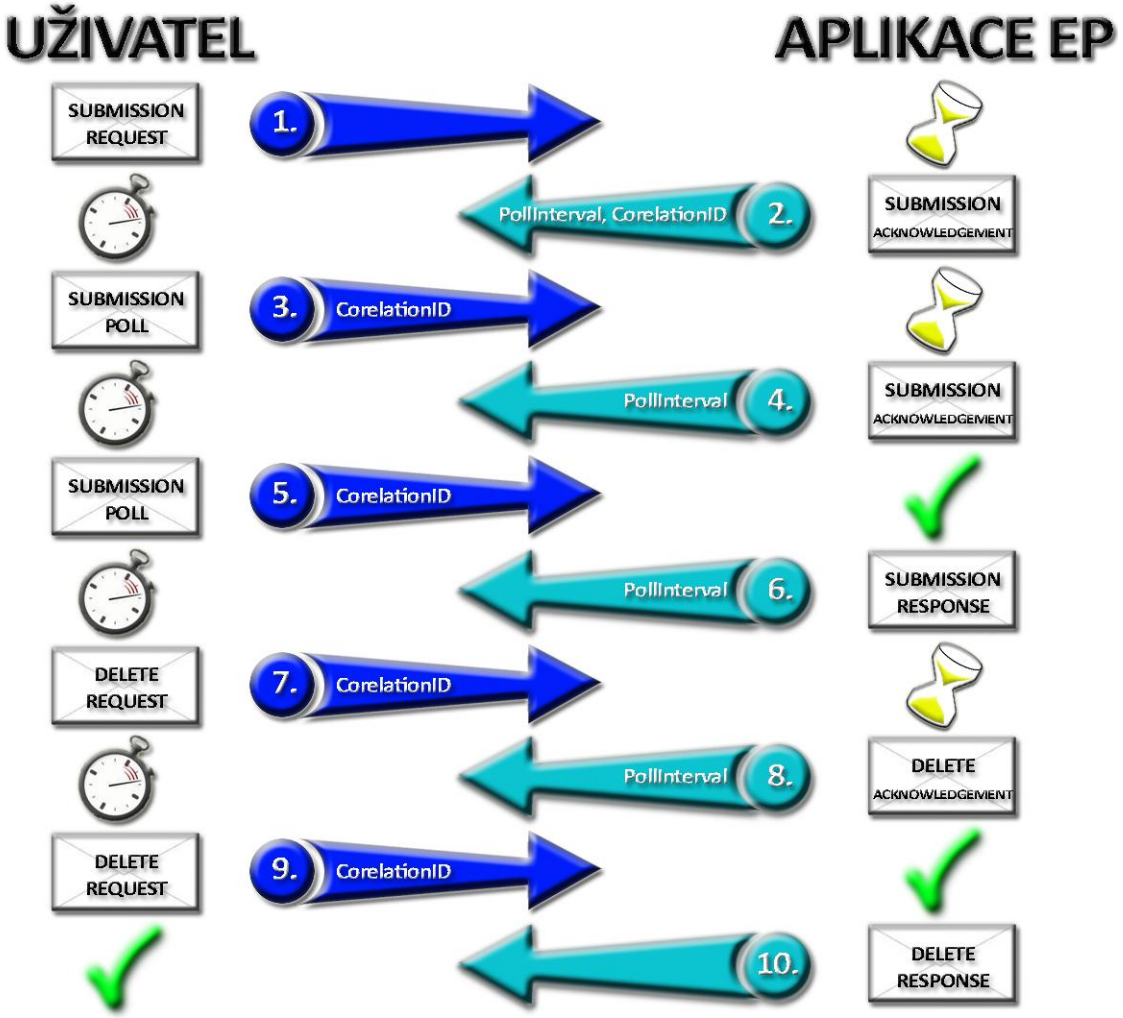
3.4.3 PŘÍKLAD ÚSPĚŠNÉHO PODÁNÍ

Za úspěšné podání, se pokládá podání doručené na úřad ČSSZ bez výskytu chyb, tudíž se nesmí v posloupnosti kroků vyskytnout zpráva SUBMISSION_ERROR. Příklad úspěšného podání je graficky znázorněn na obrázkuObrázek 8, kde na levé straně je aplikace uživatele a na druhé aplikace EP PVS. Obálka s popisem představuje zprávu posílanou buď jedné, nebo druhé straně. Zaneprázdněnost serveru je reprezentována přesýpacími hodinami, úspěšné splnění podání a vymazání informací o podání je znázorněno tímto zeleným symbolem (✓) a posledním znakem, který v schématu je, jsou stopky, které říkají, že aplikace přijala zprávu, která definuje čas, po který musí počkat před odesláním další zprávy.

Schéma úspěšného podání je znázorněno v deseti krocích, počet kroků se může pokaždé lišt, jelikož záleží na dostupnosti aplikace elektronického podání portálu veřejné správy.

1. Komunikace začíná prvním krokem aplikací uživatele, který pošle zprávu SUBMISSION_REQUEST představující nové podání
2. Aplikace EP PVS je právě zaneprázdněná a aby informovala uživatelskou aplikaci, že nemá nyní čas, pošle zprávu typu SUBMISSION_ACKNOWLEDGEMENT, do které uživateli připojí unikátní identifikátor correlation ID a poll interval.
3. Aplikace uživatele přijme zprávu, podívá se do elementu ResponseEndPoint obsahující atribut PollInterval s časem uvedeným v sekundách a hodnotu elementu říkající kam se má další zpráva poslat. Po uplynutí stanoveného času se odešle uživatelskou aplikací odpověď typu SUBMISSION_POLL na přijatou adresu a s přiděleným correlation ID.
4. Aplikace EP PVS je opět zaneprázdněná, proto znovu odešle SUBMISSION_ACKNOWLEDGEMENT.
5. Opakování kroku tři.

6. Nyní už má aplikace EP PVS čas a může zpracovat naší zprávu, pokud zpracování proběhne v pořádku, pošle zprávu SUBMISSION_RESPONSE, aby informovala uživatelskou aplikaci.
7. Nyní už zbývá vymazat původní zprávu ze systému, proto je v sedmém kroku posílána žádost o smazání neboli DELETE_REQUEST. Zpráva přejme adresu, na kterou se má poslat žádost a interval, po který má počkat, ze zprávy SUBMISSION_RESPONSE.
8. Aplikace EP je zaneprázdněna a odesílá DELETE_ACKNOWLEDGEMENT. Aplikace uživatele přijme zprávu a zjistí, že server byl zaneprázdněn, tudíž si zjistí poll interval a po jeho uplynutí pošle zprávu typu DELETE_REQUEST znovu. Aplikace EP má čas, zpracuje požadavek a informuje aplikaci uživatele o přijetí a zpracování žádosti zprávou DELETE_RESPONSE. Nyní může software informovat uživatele o úspěšném zpracování podání. Tuto informaci dostane i uživatel na email, který si registroval u České správy sociálního zabezpečení. Ukázka emailu je uvedena v příloze 11.



Obrázek 8 Úspěšné podání datové zprávy, zdroj: [vlastní]

3.5 DATOVÁ ZPRÁVA

Pod tímto pojmem je možné si představit zprávu, která se bude posílat přes portál veřejné správy na úřad České správy sociálního zabezpečení. Aby bylo možné správné doručení, bezpečný přenos a čitelnost dat, je nutné se řídit pokyny a standardy vydanými ČSSZ a portálem veřejné správy. Zprávu tvoří tělo datové zprávy a GovTalk obálka. Veškerá komunikace probíhá v jazyce xml.

3.5.1 TĚLO DATOVÉ ZPRÁVY

Tělo dokumentu je určeno výhradně pro zpracování v ČSSZ. Struktura je specifikována ČSSZ a obsahuje údaje obálky pro ČSSZ, která určuje interní zařazení v rámci systémů úřadu

a vlastní datovou větu s předávanými údaji o přihlášce. Tělo datové zprávy se člení na čtyři základní části [8]:

1. Datová věta
2. Obálka pro ČSSZ
3. Elektronický podpis
4. Zašifrovaná datová věta

3.5.1.1 DATOVÁ VĚTA

Datová věta obsahuje údaje z vyplněného formuláře. Její struktura je pevně stanovena a nesmí být pozměněna.

Kořenový element definuje o jaká data respektive, pro jakou službu jsou data určena. Pro podávání přihlášky k nemocenskému pojištění je kořenový element definován jako „PRIHL“, následuje element „employee“ který může být v datové zprávě vícekrát, což umožňuje poslat přihlášku pro více osob najednou. Celá struktura je znázorněna v xml formátu a tabulka Tabulka 2 popisuje co jednotlivé elementy a atributy reprezentují.

```
<PRIHL>
<employee dep= act= fro= dat= >
   <client bno= >
      <name sur= ona= fir= tit= />
      <birth dat= nam= cit= />
      <stat mal= sta= cnt= chl= />
      <adr str= num= pnu= cit= cnt= />
       <fdr str= num= pnu= cit= />
   </client>
   <comp vs= id= cni= nam= str= num= pnu= cit= cnt= />
   <job fro= to= rel= per= tim= day= ear= />
   <forin nam= str= num= pnu= cit= cnt= id= />
   <pens typ=  tak= />
</employee>
<employee>
.....
</employee>
.....
</PRIHL>
```

Příklad datové věty, která je výstupem aplikace, připravené k podepsání a zašifrování:

```
<PRIHL>
    <employee dep="110" act="1" fro="" dat="2009-04-09">
        <client bno="8205251028">
            <name sur="Berný" ona="" fir="Petr" tit="" />
            <birth dat="1982-05-25" nam="Berný" cit="Městec Králové" />
            <stat mal="M" sta="1" cnt="CZ" chl="0" />
            <adr str="Pražská" num="234" pnu="28908" cit="Jičín" cnt="CZ" />
            <fdr str="" num="" pnu="" cit="" />
        </client>
    <comp vs="91200283" id="10159973" cni="CN" nam="Podnik" str="Pražská" num="735" pnu="11000" cit="Praha 1"
cnt="CZ" />
    <job fro="2008-09-01" rel="0" per="" tim="30" day="5" ear="15000" />
    <forin nam="" str="" num="" pnu="" cit="" cnt="" id="" />
    <pens typ="0" tak="" />
    </employee>
  </PRIHL>
```

Tabulka 2 Datová věta přihlášky zaměstnance, zdroj: [5]

DATOVÁ VĚTA PŘIHLÁŠKY ZAMĚSTNANCE

název atributu	popis	povinnost
employee.dep	číslo okresu (org. jednotky ČSSZ)	A
employee.act	akce (přihláška/odhláška/změna/hromadný sběr/oprava)	A
employee.dat	datum vyhotovení	A
employee.fro	platnost zaslaných údajů od /datum vyhotovení opravované přihlášky	N
employee.client.bno	rodné číslo	A
employee.client.name.sur	příjmení	A
employee.client.name.ona	všechna další předchozí příjmení	N
employee.client.name.fir	jméno	A
employee.client.name.tit	titul	N
employee.client.birth.dat	datum narození	A
employee.client.birth.nam	rodné příjmení	A
employee.client.birth.cit	místo narození	A
employee.client.stat.mal	pohlaví	A
employee.client.stat.sta	rodinný stav	A
employee.client.stat.cnt	státní občanství	A
employee.client.stat.chl	počet vychovaných dětí	N
employee.client.adr.str	trvalý pobyt - ulice	A
employee.client.adr.num	trvalý pobyt - č.p.	A
employee.client.adr.pnu	trvalý pobyt - psč(postcode)	A
employee.client.adr.cit	trvalý pobyt - obec	A
employee.client.adr.cnt	trvalý pobyt - stát	A
employee.client.fdr.str	trvalý pobyt v ČR - ulice	N
employee.client.fdr.num	trvalý pobyt v ČR - č.p.	N
employee.client.fdr.pnu	trvalý pobyt v ČR - psč	N
employee.client.fdr.cit	trvalý pobyt v ČR - obec	N
employee.comp.vs	variabilní symbol zaměstnavatele	A
employee.comp.id	individuální (identifikační) číslo zaměstnavatele	N
employee.comp.cni	stát, který IČ vydal	N
employee.comp.nam	název zaměstnavatele	A
employee.comp.str	sídlo zaměstnavatele - ulice	A
employee.comp.num	sídlo zaměstnavatele - č.p.	A
employee.comp.pnu	sídlo zaměstnavatele - PSČ (postcode)	A
employee.comp.cit	sídlo zaměstnavatele - obec	A
employee.comp.cnt	sídlo zaměstnavatele - stát	A
employee.job.fro	datum vstupu do zaměstnání (zaměstnán od)	A
employee.job.to	datum ukončení zaměstnání (zaměstnán do)	N
employee.job.rel	druh výdělečné činnosti	A
employee.job.per	místo výkonu činnosti (stát)	N
employee.job.tim	pracovní úvazek - hodiny týdně	N
employee.job.day	pracovní úvazek - dny týdně	N
employee.job.ear	předpokládaný průměrný hrubý měsíční příjem	N
employee.forin.nam	poslední nositel cizozemského pojištění - název	N
employee.forin.str	poslední nositel cizozemského pojištění - ulice	N
employee.forin.num	poslední nositel cizozemského pojištění - č.p.	N
employee.forin.pnu	poslední nositel cizozemského pojištění - PSČ (postcode)	N
employee.forin.cit	poslední nositel cizozemského pojištění - obec	N
employee.forin.cnt	poslední nositel cizozemského pojištění - stát	N
employee.forin.id	číslo cizozemského pojištění	N
employee.pens.typ	druh pobíraného důchodu	N
employee.pens.tak	důchod pobírán od	N

3.5.1.2 OBÁLKA PRO ČSSZ

Obálka ČSSZ určuje zařazení elektronického podání v rámci systému ČSSZ. Včetně dat je součástí zprávy Submission - Request v elementu Body. **Chyba! Nenalezen zdroj odkazů.**

Struktura obálky je následující:

```
<Message version="1.1" xmlns="http://www.cssz.cz/XMLSchema/emp/envelope">
        <Header>
                        <Signature xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="bin.base64">
                                digitální podpis
                        </Signature>
                        <Vendor productName="jméno produktu" version="verze produktu x.y"/>
        </Header>
        <Body encrypted="yes|no" contentEncoding="gzip|raw" xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="bin.base64">
                zašifrovaná data
        </Body>
 </Message>
```

Příklad obálky s podpisem a zašifrovanou datovou větou vypadá takto:

```
<Message version="1.1" xmlns="http://www.cssz.cz/XMLSchema/envelope">
        <Header>
                <Signature xmlns:dt="urn:schemas-microsoft-com:datatypes"
                dt:dt="bin.base64">MIIFygYJKoZIhvcNAQcCoIIFuzCCBbc...<Signature>
                <Vendor productName="BP" version="1.0" />
        </Header>
                <Body encrypted="yes" contentEncoding="raw" xmlns:dt="urn:schemas-microsoft-com:datatypes"
                dt:dt="bin.base64">MIIHuAYJKoZIhvcNAQcD...</Body>
</Message>
```

Tvorba elektronického podpisu a zašifrované datové věty je popsáno v následujících kapitolách 3.5.1.3 Elektronický podpis a 3.5.1.4 Šifrování datové věty.

Tabulka Tabulka 3 Obálka České správy sociálního zabezpečení, zdroj: [5]popisuje jednotlivé elementy a atributy obsažené v obálce.

Tabulka 3 Obálka České správy sociálního zabezpečení, zdroj: [5]

OBÁLKA ČESKÉ SPRÁVY SOCIÁLNÍHO ZABEZPEČENÍ

název elementu	popis elementu
Message	Identifikace dokumentu v rámci ČSSZ (interní obálka)
Message.version	Verze obálky a struktury datové věty určené pro ČSSZ. Nastavte na hodnotu 1.1. Hodnota popisuje použitou strukturu obálky i datové věty určené ČSSZ.
Header	Hlavička obálky pro DIS server.
Signature	podpis nezašifrovaného těla dokumentu v elementu Message. Podepisuje se vlastní datová věta PRIHL (následující element Body). Podpis musí být ve formátu base64.
Vendor	Informace o produktu, který dokument vygeneroval.
	Hodnoty jsou uvedeny v atributech:
	productName="<jméno produktu>"
	version="<verze produktu x.y>"
Body	Vlastní podepsaná a následně zašifrovaná data uložená ve formátu base64
Body.encrypted	yes -> identifikace zašifrovaných dat v těle Body. Data musí být zašifrována v případě zasílání podání přes PVS.
	no -> identifikace nezašifrovaných dat v těle Body. Data nemusí být zašifrována, pokud je podání doručováno na paměťových médiích. Nezašifrovaná data musí být také transkódována v Base64
Body.contentEncoding	raw -> data v těle zprávy Body nejsou pakována do formátu gzip.
	gzip -> data v těle zprávy Body jsou pakována ve formátu gzip (LZ77). Pakování musí být provedeno až po vytvoření digitálního podpisu. Pakují se nezašifrovaná data, která musí být až následně zašifrována pokud je podání zasíláno přes PVS.

3.5.1.3 ELEKTRONICKÝ PODPIS

O elektronickém podpisu pojednává kapitola 3.2.2 Elektronický podpis. Data určená k podpisu se nacházejí ve vnořeném elementu „Body“ a výsledný podpis se vloží do elementu „Signature“.

3.5.1.4 ZAŠIFROVÁNÍ DATOVÉ VĚTY

Datová věta se šifruje asymetrickou šifrou. Pro zašifrování zprávy se využívá certifikátu od České správy sociálního zabezpečení, který obsahuje veřejný klíč. Popis procesu šifrování je uveden v kapitole 3.2.2.1 Šifrování.

3.5.2 GOVTALK OBÁLKA

GovTalk obálka je xml struktura, která je vytvořena na základě GovTalk schématu. Veškerá komunikace v transakční části portálu veřejné správy je vkládána do GovTalk obálky. [26]

Obálka může obsahovat velké množství údajů, proto v této práci budou uvedeny jen ty, které jsou využity pro podání přihlášky k nemocenskému pojištění. Pro lepší představu, jak vypadá taková obálka, je zde příklad.

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>...</Qualifier>
            <Function>...</Function>
            <CorrlationID>...</CorrelationID>
            <Transformation>...</Transformation>
            <GatewayTest>...</GatewayTest>
            <GatewayTimestamp>...</GatewayTimestamp>
        </MessageDetails>
        <SenderDetails>
            <IDAuthentication>
                <SenderID>ID podavajiciho</SenderID>
                <Authentication>
                    <Method>clear</Method>
                    <Value>heslo</Value>
                </Authentication>
            </IDAuthentication>
        </SenderDetails>
    </Header>
    <GovTalkDetails>
        <Keys>
            <Key Type="vars">variabilní symbol</Key>
        </Keys>
    </GovTalkDetails>
    <Body>
        tělo zprávy
    </Body>
</GovTalkMessage>
```

Obálka se strukturou uvedenou výše se bude posílat do aplikace elektronického podání na portálu veřejné správy, kde bude přesměrována na úřad ČSSZ. Popis jednotlivých částí obálky je uveden v následující kapitole.

3.5.2.1 POPIS DAT

Následující podkapitoly uvádí definice jednotlivých elementů a atributů vyskytujících se v datových zprávách používaných portálem veřejné správy a Českou správou sociálního zabezpečení.

- **GovTalkMessage**

  Element <GovTalkMessage> je hlavní element dokumentu (neboli „kořenový element“) každé zprávy GovTalk. Je zadáván autorem souboru a obsahuje jmenný prostor pro hlavičku GovTalk. Všechna data v dokumentech podaných do aplikace Elektronická podání jsou vložena v elementu <GovTalkMessage>. Následující řádek definuje požadovaný jmenný prostor [11]:

  ```
  <GovTalkMessage xmlns=http://www.govtalk.gov.uk/CM/envelope/>
  ```

- **EnvelopeVersion**

  Element <EnvelopeVersion> obsahuje číselnou (desítkovou) hodnotu a určuje verzi obálky zprávy, která byla použita při vytváření dané zprávy. [11]

- **Header**

  Autor každého dokumentu musí do dokumentu zahrnout element <Header>. Hlavička obsahuje data umožňující aplikaci Elektronická podání identifikovat, zpracovat, směrovat a kontrolovat dokumenty, které jsou do ní podány. Data v hlavičce elementu GovTalkMessage jsou rozdělena mezi dva odlišné bloky. Jeden blok, <MessageDetails>, poskytuje podrobnosti o samotné zprávě a druhý blok, <SenderDetails>, poskytuje podrobnosti o odesílateli zprávy. Každý soubor může obsahovat pouze jednu hlavičku. [11]

- **MessageDetails**

  Element <MessageDetails> poskytuje aplikaci Elektronická podání informace o zprávě. Údaje zadané odesílatelem zprávy poskytnou aplikaci Elektronická podání mimo jiné tyto informace [11]:

  - Zařazení zprávy

    Například dokument může obsahovat přihlášku k nemocenskému pojištění (PRIHL) České správy sociálního zabezpečení (ČSSZ), což znamená, že jeho zařazení (nastavená v elementu <Class>) bude CSSZ_PRIHL.

- Typ zprávy

  Například dokument může být úvodní zpráva (v dialogu) odeslaná z klientské aplikace do aplikace Elektronická podání. V tomto případě bude její typ (určený elementem <Qualifier>) nastaven na hodnotu request.

- Funkce, které budou provedeny. Například funkce úvodní zprávy odeslané z klientské aplikace do aplikace Elektronická podání (určená elementem <Function>) je submit.

Po podání dokumentu do aplikace Elektronická podání tato aplikace doplní hodnoty některých subelementů v elementu <MessageDetails> a odpoví autorovi zprávy. Přidá například časovou značku v elementu <GatewayTimestamp> určující čas, kdy byla zpráva přijata ke zpracování. [11]

- **Class**

Element <Class> je primární identifikátor, podle kterého aplikace Elektronická podání rozpoznává obsah dokumentu. Data zadaná do tohoto pole autorem dokumentu řídí zpracování, ověření a směrování zprávy. Element <Class> v dokumentu umožňuje aplikaci Elektronická podání zajistit použití správných pravidel pro daný konkrétní typ zprávy a správné směrování této zprávy příslušnému úřadu veřejné správy. [11]

Autor zprávy musí zahrnout element <Class> do hlavičky GovTalkHeader každé zprávy. Tento element může být zadán pouze jednou. [11]

Aplikace Elektronická podání spravuje seznam možných hodnot, aby byla zajištěna jedinečnost. [11]

Tento element také určuje pravidla ověřování, která musí aplikace Elektronická podání pro dokument použít. Řídí požadovaný stupeň ověřovacího mechanismu, neboť různé typy dokumentů vyžadují různé úrovně ověřování.

K dispozici jsou dvě metody ověření dokumentu podle odesílatele: digitální podpis nebo ID uživatele a heslo. [11]

- **Qualifier**

  Element <Qualifier> určuje typ zprávy. Možné hodnoty jsou [11]:

  - ***request (požadavek)***

    Hodnota „request“ určuje, že se jedná o zprávu od klienta vyžadujícího službu od aplikace Elektronická podání nebo od úřadu veřejné správy. Příkladem požadavku je podání dat.

  - ***acknowledgement (potvrzení)***

    Tato hodnota označuje, že aplikace Elektronická podání obdržela a přijala zprávu a že zpráva byla předána příslušnému úřadu, avšak dosud nebyla obdržena odpověď o výsledku zpracování.

  - ***response (odpověď)***

    Tato hodnota označuje, že zpráva je odpovědí aplikace Elektronická podání nebo úřadu veřejné správy potvrzující akceptaci zprávy typu "request".

  - ***poll (dotaz)***

    Tato hodnota označuje, že zpráva je dotazem klienta na získání odpovědi o výsledku zpracování předložené zprávy typu "request".

- ***error (chyba)***

  Tato hodnota představuje „negativní potvrzení“ a určuje, že aplikace Elektronická podání nebo úřad veřejné správy zjistily ve zprávě chybu.

- **Function**

  Určuje funkci, která má být provedena. Nejčastější je hodnota „submit“, což je požadovaná hodnota při podávání dokumentů do aplikace Elektronická podání a při odesílání dotazů na výsledky zpracování. [11]

- **CorrelationID**

  Řetězec zadaný v tomto elementu slouží k přiřazení všech odpovědí ze systémů úřadů státní správy. Mohou existovat dosud nezpracované dokumenty nebo dotazy na stav podání z podávající aplikace. Aplikace, která učinila podání, jej také může použít ke sledování postupu dokumentu systémem. [11]

  Aplikace Elektronická podání zapíše do tohoto elementu globálně jedinečný identifikátor dlouhý maximálně 32 alfanumerických znaků, který jedinečně identifikuje daný dokument v systému. Tato změněná verze hlavičky bude vrácena podávající aplikaci, jakmile aplikace Elektronická podání poprvé potvrdí příjem zprávy. Potvrzení odpovědi z aplikace Elektronická podání obsahující doplněný element <CorrelationID> informuje podávající aplikaci, že tento dokument úspěšně prošel předběžnými kontrolami prováděnými aplikací Elektronická podání. Po přiřazení musí být toto ID uvedeno ve veškeré následující komunikaci týkající se dané zprávy. [11]

- **Transformation**

  <Transformation> je nepovinný element, který může autor zahrnout do počátečního dokumentu s vlastním podáním. Slouží k určení formátu, ve kterém mají být vráceny zprávy z aplikace Elektronická podání. Vzhledem ke snaze

podporovat co největší počet aplikací spolupracujících s aplikací Elektronická podání budou povolena podání pomocí protokolu XML i HTML. Element Transformation umožňuje volající aplikaci určit formát, ve kterém si přeje přijímat komunikaci. [11]

- **GatewayTest**

  Element <GatewayTest> určuje, zda je zpráva odeslaná aplikaci Elektronická podání skutečná nebo testovací. Nepřítomnost tohoto elementu nebo hodnota 0 označují, že se jedná o skutečnou, nikoli o testovací zprávu. [21]

- **GatewayTimestamp**

  Element <GatewayTimestamp> je vždy přidán aplikací Elektronická podání do hlaviček všech dokumentů, které jsou do ní podány. Obsahuje časovou značku určující přesné datum a čas (na nejbližší sekundu), kdy byl dokument přijat aplikací Elektronická podání ke zpracování. [11]

  Tento čas je důležitý, protože představuje oficiální čas, kdy aplikace přijala data vložená ve zprávě. Element <GatewayTimestamp> může být vložen do jakéhokoli příchozího podání, ale pokud tomu tak je, musí být prázdný, protože časová značka bude do zprávy přidána před jejím předáním příslušnému systému veřejného úřadu. [11]

- **SenderDetails**

  Data identifikující odesílatele zprávy a metodu, pomocí které byl dokument podepsán, jsou vložena do elementu <SenderDetails>. Tento element obsahuje také podpis odesílatele, jehož typ musí odpovídat konkrétnímu typu transakce definovaného elementem <Class>. [21]

  Každý dokument podaný do aplikace Elektronická podání by měl obsahovat element <SenderDetails>. [11]

- **GovTalkDetails**

  Autor každého dokumentu musí do dokumentu zahrnout element <GovTalkDetails>. Tento element musí být umístěn ihned za datový blok <Header>. Data v bloku <GovTalkDetails> jsou rozdělena do několika různých typů dat, některá zadává aplikace Elektronická podání, některá autor dokumentu. Některé elementy v tomto bloku nejsou povinné. [11]

- **Keys**

  Element <Keys> může obsahovat jeden či více vnořených elementů <Key>. Informace uložené v elementu <Key> umožňují aplikaci Elektronická podání zkontrolovat, zda osoba podávající dokument má k tomuto kroku oprávnění jménem osoby či organizace. Těmto údajům uváděným v elementech Key se říká známé údaje. [11]

- **Key**

  Každý element <Keys> může obsahovat neomezený počet elementů <Key>. Každý z nich může obsahovat samostatný schválený identifikátor služby (známý údaj), pomocí kterého aplikace Elektronická podání může zkontrolovat, zda je odesílatel zprávy oprávněn k podání tohoto typu dokumentu do úřadů veřejné správy jménem daného zákazníka. [11]

  Zde uvedené identifikátory služeb v podobě známých údajů jsou jedinečné pro konkrétního jednotlivce či službu a musí odpovídat hodnotám zadaným ve službě Registrace a zápis při první registraci uživatele k používání elektronických služeb. [11]

  Pravidla pro konkrétní transakci určují, které známé údaje (pokud nějaké) je třeba zadat. Pravidla pro některé transakce mohou určovat, že je třeba zadat více než jeden známý údaj. Každý zadaný známý údaj se musí zobrazovat v samostatném elementu <Key>. [11]

Pokud odesílatel zadá neúplné nebo nesprávné známé údaje, bude dokument aplikací Elektronická podání odmítnut. [11]

Každý element Key obsahuje atribut Type (například "vars") a hodnotu poskytující informaci, kterou aplikace Elektronická podání vyžaduje k ověření dané transakce. [11]

- **GovTalkErrors**

Element <GovTalkErrors> je přidán do bloku GovTalkMessage cílovým úřadem veřejné správy nebo aplikací Elektronická podání v případě, že v některé zprávě podané do systému byly nalezeny chyby. Je přidán pouze v případě potřeby. Podávající aplikace by tento element neměla zadat v prvotním podání dokumentu. Tento element obsahuje podrobnosti všech nalezených chyb protokolu bez ohledu na jejich počet. V případě chyb v obsahu zprávy určené veřejnému úřadu bude element <Type> obsahovat hodnotu „business“ a další informace budou zahrnuty v textu zprávy. [11]

- **Error**

Každý element <Error> zahrnuje určitý počet vnořených elementů, které společně identifikují jednotlivé chyby nalezené během zpracování dokumentu. Autor bloku <Error> bude vždy oznamovat typ jednotlivých nalezených chyb v subelementu <Type>. Lze přidat další nepovinné elementy poskytující další informace o dané chybě, například její kód a připojenou textovou zprávu a umístění v dokumentu, kde se daná chyba nachází. [11]

4 VLASTNÍ ZPRACOVÁNÍ

Tato kapitola se zabývá vývojem vlastní aplikace pro elektronické podání přes portál veřejné správy, provedeného v prostředí Microsoft Visual Studio Professional 2008 programovacím jazykem Visual Basic .NET 2008.

Vlastní aplikace pro elektronické podání přes portál veřejné správy musí splňovat několik základních kritérií. Musí umožnit uživateli zadat data, nebo je načíst z databáze, následně provést správnost vložených dat. Dále musí umožnit data poslat zabezpečeným způsobem na portál veřejné správy a musí uživatele informovat o stavu vyřízení podání.

Pro testování e-podání je vybrána přihláška k nemocenskému pojištění podávána na České správě sociálního zabezpečení. Od 1. ledna 2009 přihláška k nemocenskému pojištění se změnila na ohlášení o nástupu do zaměstnání, ale pro testovací účely je stále ještě funkční původní přihláška k nemocenskému pojištění.

4.1 ZAJIŠTĚNÍ POTŘEBNÉHO DIGITÁLNÍHO CERTIFIKÁTU

Česká správa sociálního zabezpečení (ČSSZ) preferuje podepisování datových zpráv kvalifikovaným certifikátem od akreditované certifikační autority. O kvalifikovaných certifikátech bylo již napsáno dříve v kapitole 3.2.4.

4.1.1 VÝBĚR CERTIFIKAČNÍ AUTORITY

Vydavatelů certifikátů je na trhu spoustu, ale pro účely komunikování s veřejnou správou potřebujeme kvalifikovaný certifikát od akreditované certifikační autority. Takové certifikační autority jsou v České republice zatím jen tři a to:

- První certifikační autorita a. s.
- Česká pošta s. p.
- Eldentity a. s.

Všechny tři uvedení vydavatelé certifikátů mají ve své nabídce produktů i kvalifikovaný certifikát, tudíž všichni tři jsou vhodnými poskytovateli. Dalšími možnými kritérii může být cena

certifikátu, dostupnost registračního místa pro žadatele, důvěryhodnost, certifikační politika. Po zvážení všech kritérií, je pro účely této práce zvolen jako poskytovatel kvalifikovaného certifikátu První certifikační autoritu a. s.

4.1.2 PROCES ZÍSKÁNÍ CERTIFIKÁTU

V předchozí kapitole je uvedeno, že se bude žádat o certifikát u První certifikační autority a. s. (I. CA), která je dostupná z www.ica.cz, kde z hlavní nabídky vybereme Produkty a služby a následně z menu vybereme námi požadovaný kvalifikovaný certifikát. Zde se dozvíme základní informace o kvalifikovaném certifikátu, postup získání certifikátu. Další postup je uveden v jednotlivých krocích na stránkách žádosti o certifikát

Posledním krokem by mělo být vygenerování žádosti (cert.req), kterou je nutné uložit na přenosné paměťové médium. Obsah souboru cert.req, kde je zašifrovaná žádost kořenovým certifikátem I. CA je na obrázku Obrázek 9.

Obrázek 9 Vygenerovaná žádost, zdroj: [vlastní]

Nyní už stačí dohodnout termín s nejbližší pobočkou ČSOB, která vydává certifikáty I. CA, pokud žadatel není majitelem bankovního účtu u ČSOB. S žádostí na přenosném médiu navštíví oddělení vydávající certifikáty, kde musí prokázat totožnost primárním dokladem, tedy občanským průkazem (cizinci pasem) a sekundárním dokladem totožnosti (pas, řidičský průkaz aj.). Pracovník vystaví protokol o podání žádosti na vydání kvalifikovaného certifikátu I. CA. Protokol je k nahlédnutí v příloze 1. Zaměstnanec registrační autority pošle žádost do I. CA.

Po vyřízení formalit zaměstnanec ČSOB nahraje vygenerovaný certifikát I. CA na přenosné paměťové médium a tímto krokem se žadatel stane majitelem vlastního kvalifikovaného certifikátu určeného pro elektronický podpis. Kvalifikovaný certifikát by měl být zaslán i na email uvedený v žádosti.

4.1.3 INSTALACE CERTIFIKÁTU

Na přenosném paměťovém médiu respektive emailu by mělo být od registrační autority tedy ČSOB několik souborů.

Soubory začínající „9DDA5C“[1] obsahují vydaný certifikát na žádost žadatele. Všechny obsahují tentýž veřejný klíč, ale pokaždé v jiném formátu. Soubory cert_ca.der a cert_ca.pem obsahují certifikát certifikační autority tedy I. CA, která vydala certifikát. Oba soubory mají stejný certifikát jen v jiném formátu. Důvod vydávání certifikátů v různých formátech je prostý. Některé softwary umí načíst certifikáty pouze v určitém formátu:

Pro snadnou instalaci I. CA přikládá ještě soubor s příponou htm, kde po otevření se nachází základní informace o vystaviteli certifikátu a předmět. Pro instalaci je zde umístěné tlačítko „Instalace certifikátů“ po kliknutí se postupuje dle pokynů na obrazovce. Po úspěšném nainstalování certifikátu se objeví zpráva „Certifikát byl nainstalován“.

Obrázek 10 Úspěšná instalace certifikátu, zdroj: [vlastní]

[1] sériové číslo v hexadecimálním tvaru vydaného certifikátu

Druhou možností jak nainstalovat certifikáty je ruční instalace. Nejprve si vybere soubor s názvem cert_ca.der, dvojklikem se otevře. Zobrazí se okno, se třemi záložkami. První záložka je „Obecné“, zde se nachází informace pro koho je certifikát vystaven, kým je vystaven a platnost. Druhou záložkou jsou „Podrobnosti“ s veškerými informacemi o certifikátu, které jsou uvedené v kapitole 3.2.4. Na první záložce je v dolní části tlačítko „Nainstalovat certifikát“, po potvrzení se otevře průvodce instalací certifikátu. Jedinou modifikovatelnou volbou je místo pro uložení certifikátu. Místo pro instalaci tohoto certifikátu je ve složce pro důvěryhodné kořenové certifikační úřady. Ještě zbývá nainstalovat vlastní certifikát. Instalaci se provede obdobným způsobem, jen s tím rozdílem, že umístění pro certifikát je tentokrát složka s názvem „Osobní“.

4.2 REGISTRACE U ČESKÉ SPRÁVY SOCIÁLNÍHO ZABEZPEČENÍ

Pro úspěšné podání je nutné u České správy sociálního zabezpečení (ČSSZ) zaregistrovat některé údaje. Registrace se provede prostřednictvím emailu. Pro testování vydává ČSSZ fiktivní údaje a to variabilní symbol a registrační číslo. Aby mohla ČSSZ ověřit elektronický podpis, je nutné jim zaslat informace o vlastním digitálním certifikátu. Data, která potřebují, jsou jméno nositele, název vystavitele, sériové číslo a email, na který budou zasílány zprávy o podání přihlášky nemocenského pojištění. Po úspěšném zaregistrování u ČSSZ je odeslán email s informací o tom, že byla provedena změna registračních údajů.

Nyní ještě co bude potřeba od ČSSZ, je jejich veřejný klíč, kterým se bude šifrovat datová zprávu. Certifikát, který obsahuje tento veřejný klíč je dostupný na adrese http://www.cssz.cz/cz/e-podani/sifrovani-datovych-zprav/. Instalace certifikátu se provede obdobným postupem jako instalace kvalifikovaného certifikátu v kapitole 4.1.3 Instalace certifikátu.

4.3 REGISTRACE NA PORTÁLU VEŘEJNÉ SPRÁVY

Pro umožnění využívání služeb v transakční části portálu veřejné správy, jen nejprve nutné se registrovat. Proces registrace je popsán v následujících kapitolách, kde je uveden rozbor výběru role uživatele a vlastní registrace.

4.3.1 VÝBĚR ROLE UŽIVATELE VŮČI VEŘEJNÉ SPRÁVĚ

Registrace na portálu veřejné správy je rozdělena na tři části.

1. Občan
2. Organizace
3. Zástupci

4.3.1.1 OBČAN

Tato registrace je vhodná pro uživatele, kteří potřebují využívat služby veřejné správy pro své osobní účely. [25]

4.3.1.2 ORGANIZACE

Registrace pro organizace je určena pro živnostníka, podnikatele aj., kteří potřebují využívat služby veřejné správy pro komerční účely, či pokud potřebují využívat služby veřejné správy pro potřeby jiných subjektů (nadace, charitativní organizace aj.) [25]

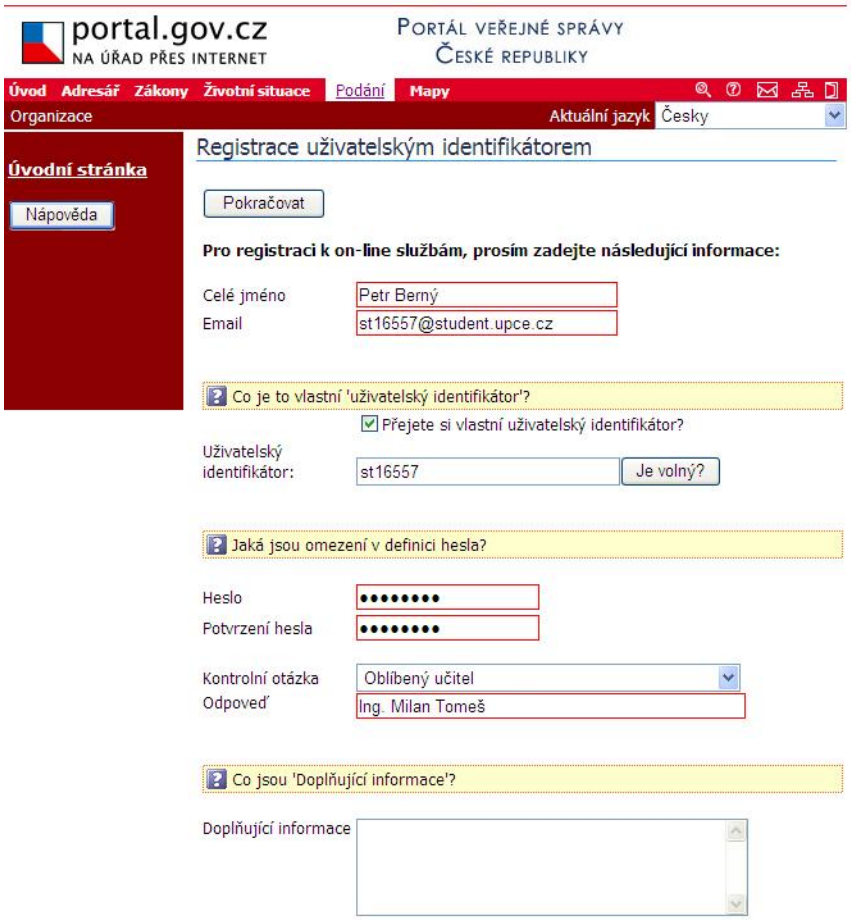
4.3.1.3 ZÁSTUPCI

V případě, že uživatel potřebuje využívat služby veřejné správy jako osoba zplnomocněná zastupovat ve vybraných věcech statutární orgány obchodních společností nebo je zplnomocněn zastupovat v dané věci občany a již má přidělený identifikátor zástupce, který obdržel od odpovídající instituce. [25]

4.3.2 PROCES REGISTRACE A AKTIVACE SLUŽEB

První krok, který se musí provést je instalace certifikátu Ministerstva vnitra České republiky, který je ke stažení na adrese https://bezpecne.podani.gov.cz/ClientObejcts/micr.der. Registrace na portále veřejné správy probíhá pomocí webového rozhraní pro účely testování na adrese https://bezpecne.dev.gov.cz a pro ostré elektronické podání na https://bezpecne.podani.gov.cz/default.aspx. Přihlášku nemocenského pojištění můžou podávat uživatelé zaregistrovaní jako organizace, tudíž se vybere odkaz „Organizace“. Následně je zde volba, zda se uživatel bude přihlašovat

uživatelským identifikátorem nebo certifikátem. Pro účely této práce postačí volba první, tedy uživatelským identifikátorem. Další a to nejdůležitější krok registrace je vyplnění registračních údajů, jako jsou jméno, email, popřípadě uživatelský identifikátor, který může být uživatelem zvolen vlastní anebo vygenerovaný portálem veřejné správy. Tento identifikátor musí být unikátní, proto při vlastním výběr je nutné ho ověřit, zda zvolený identifikátor již není zaregistrován. Dále se vyplní heslo, vybere se otázka, na kterou se portál ptá, při zapomenutí hesla a také je nutné vyplnit odpověď na zvolenou otázku.



Obrázek 11 Registrace uživatele na portále veřejné správy, zdroj: [vlastní]

Po stisku tlačítka pokračovat se dá říci, že registrace je již u konce, jelikož tento následující krok, výběr požadovaných služeb, je již možné provést po přihlášení do systému podání portálu veřejné správy. Vhodná služba pro tuto práci je pojmenována jako „Česká správa sociálního zabezpečení - Nemocenské pojištění“, potvrdí se a následně se vyplní přidělené registrační číslo a variabilní symbol Českou správou sociálního zabezpečení.

4.4 VÝVOJ VLASTNÍ APLIKACE PRO PODÁNÍ PŘES PVS

Nyní již je připraven digitální certifikát pro zaručený elektronický podpis, certifikát pro šifrování datové zprávy, registrace u České správy sociální správy, na portálu veřejné správy v sekci podání a je aktivována požadovaná služba. Následující část této práce je věnována vývoji aplikace pro elektronické podání přes portál veřejné správy.

Program by měl umožňovat vyplnění potřebných údajů pro přihlášku k nemocenskému pojištění, následnou kontrolu vložených údajů dle požadavků České správy sociálního zabezpečení, logické testy rodného čísla a identifikačního čísla, vytvořit datovou zprávu, elektronický podpis datové zprávy, zašifrovat zprávu, poslat podepsanou a zašifrovanou zprávu pomocí zabezpečeného protokolu HTTPS a přijmout odpověď na elektronické podání. Všechny vyjmenované kroky budou popsány v následujících kapitolách a subkapitolách.

4.4.1 FORMULÁŘ A POŽADAVKY NA VYPLNĚNÁ DATA

Při posílání formuláře elektronickou cestou, je nutné zajistit nějakou standardizovanou formu posílané zprávy. Česká správa sociálního zabezpečení definuje, jak mají vkládaná data do formuláře vypadat. Tedy stanovuje délku řetězce, datový typ, správnost vložených údajů, maximální a minimální hodnoty a formát dat. Omezení vydané Českou správou sociálního zabezpečení jsou definovaná pro každé políčko formuláře. Na obrázku Obrázek 12 Formulář přihlášky k nemocenskému pojištění, zdroj: [vlastní] Formulář přihlášky k nemocenskému pojištění, je uvedeno v každé buňce délka řetězce číslem v závorce černou barvou například **(35)**, na druhém místě je uveden datový typ velkými písmeny a šedou barvou, jedním takovým označením datového typu je **AZ**. U několika údajů je definován i formát vkládaných dat, znázorňují ho znaky v požadovaném formátu modrou barvou, například formát rodného čísla je **XXX XXX XXXX**. Buňky, které vyžadují logickou kontrolu vložených dat, jsou označeny písmenem **L** jako logický test. Pro přesně specifikované hodnoty poskytuje Česká správa sociálního zabezpečení číselníky. Políčka, kde se budou využívat číselníky, jsou označeny písmenem **Č**, jejich přehled je uveden v příloze 3. Pole označená **D**, budou využívat číselníky, které nejsou distribuovány Českou správou sociálního zabezpečení.

Délka řetězce je udávána v celočíselném formátu a říká, kolik znaků může mít řetězec vložený do jednoho políčka formuláře.

Datový typ určuje, jaké znaky můžou být použity v řetězci. ČSSZ rozlišuje osm datových typů. Přehled je v tabulceTabulka 4 Datové typy, kde je uvedeno označení datového typu a popis znaků, které je možné použít.

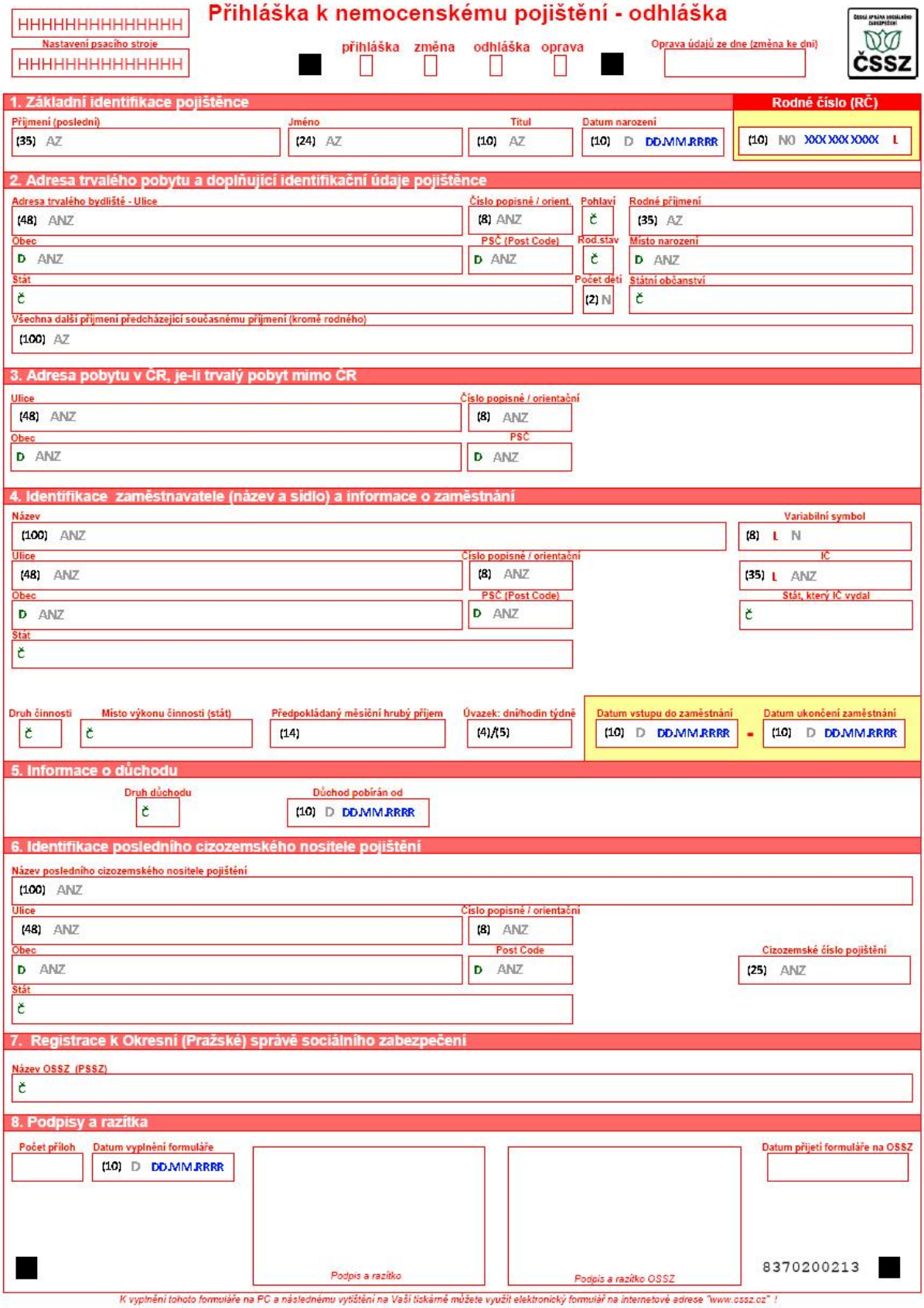
Tabulka 4 Datové typy, zdroj: [5]

DATOVÉ TYPY

typ	popis
A	alfaznaky (A - Z, a-z) + ŠŚŤŽŹšśťžźŁĄŞŻłąşĽľżŔÁÂĂÄĹĆÇČÉĘËĚÍÎĎĐŃŇÓÔŐÖ ŘŮÚŰÜÝŢßŕáâăäĺćçčéęëěíîďđńňóôőöřůúűüýţ
N	číslo - znaky 0-9, nesmí začínat nulou
AZ	alfaznaky A a znaménka: pomlčka(-), čárka (,), tečka(.), plus(+), lomítko (/), zpětné lomítko
AN	alfaznaky A a numerické znaky (0-9)
ANZ	alfaznaky A, numerické znaky N a znaménka Z
N0	číslo - znaky 0-9, může začínat nulou
D	datum ve formátu unicode RRRR-MM-DD pro odeslání zprávy, pro práci v programu formát DD.MM.RRRR
ND	číslo - znaky 0-9, může obsahovat znaménko jako první znak a des. tečku

Kontrolu vložených dat pomocí logických testů je třeba provést u rodného čísla, identifikačního čísla zaměstnavatele.

Česká správa sociálního zabezpečení definuje u některých typů vkládaných dat přesný formát. Toto omezení se vztahuje na datum a rodné číslo. Datum pro jednodušší zadávání se uvádí ve formátu DD.MM.RRRR (30.04.2009) a při odesílání se transformuje do formátu RRRR-MM-DD (2009-04-30). Rodné číslo pro přehlednost je v programu ve formátu XXX XXX XXXX, ale Česká správa sociálního zabezpečení ho požaduje bez mezer tedy XXXXXXXXXX.



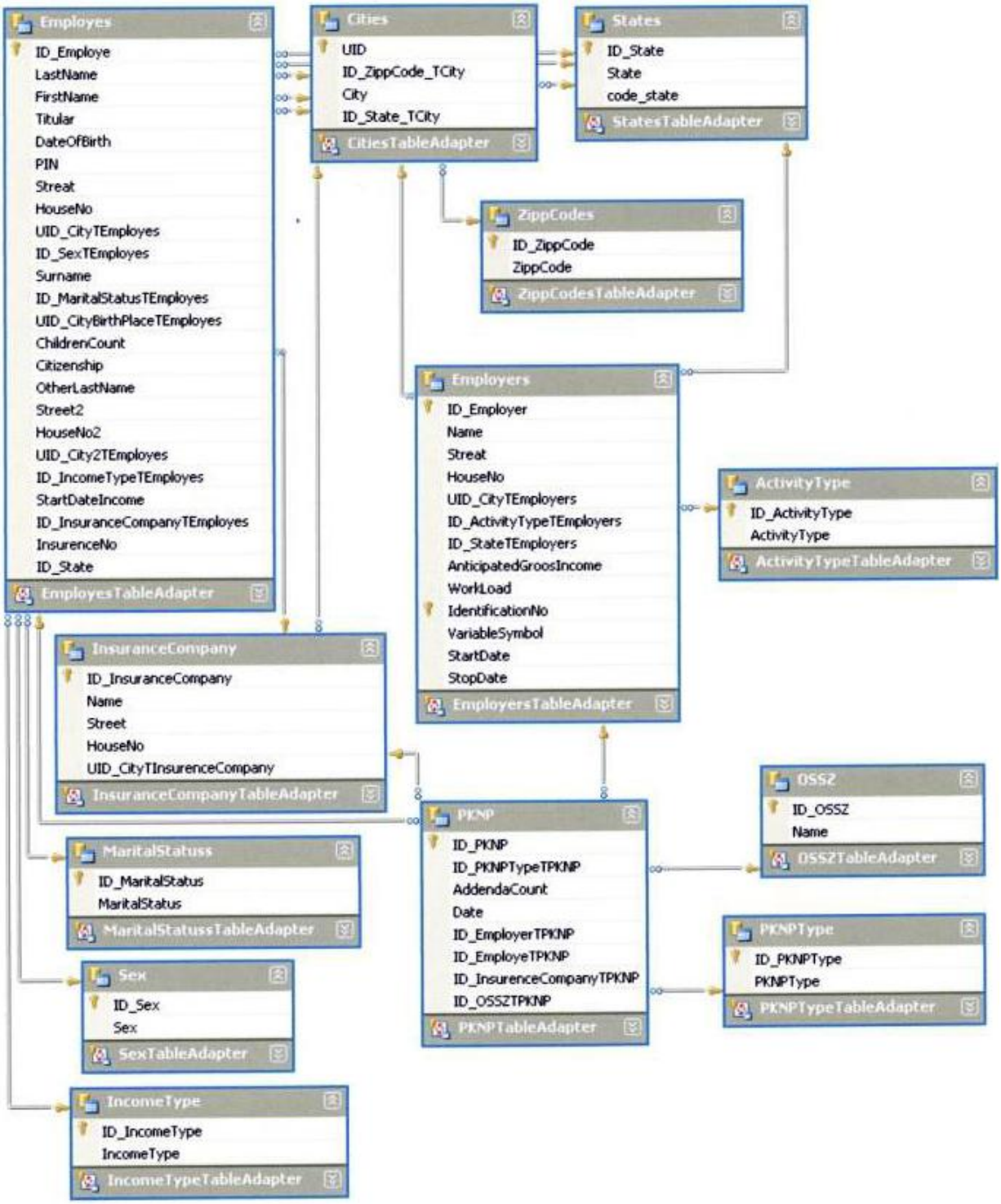
Obrázek 12 Formulář přihlášky k nemocenskému pojištění, zdroj: [vlastní]

4.4.2 VLASTNÍ NÁVRH DATABÁZE

Program bude využívat platformy Microsoft SQL Server 2005 a prostřednictvím aplikace SQL Server Management Studio Express 2005, která zajišťuje administraci SQL serveru a práci s jeho daty, vytvoříme databázi. [9]

Databáze bude obsahovat tabulky s číselníky a tabulky, které vyplývají z rozdělení formuláře, pro ukládání dat vyplněných v přihlášce k nemocenskému pojištění. Popisem používání Management Studia se tato práce zabývat nebude, jelikož to není jejím hlavní úkolem. Strukturu databáze znázorňuje obrázek Obrázek 13 ER diagram, zdroj: [vlastní] ER diagramu.

Mezi tabulky číselníků od ČSSZ patří States reprezentující státy, OSSZ – název Okresní správy sociálního zabezpečení, MaritalStatuss – rodinný stav, Sex – pohlaví, IncomeType – druh důchodu, ActivityType – druh činnosti. Ostatním číselníkům odpovídají tabulky Cities – města, ZippCodes - PSČ a ostatní tabulky odpovídají rozložení formuláře.



Obrázek 13 ER diagram, zdroj: [vlastní]

4.4.3 NÁVRH PROSTŘEDÍ PRO VSTUP DAT

Vstupním místem pro data bude sloužit formulář navržený Českou správou sociálního zabezpečený doplněný o komponenty třídy Windows Forms. U polí, která mají datový typ jiný než N tedy numerický a D neboli datum, bude použita komponenta TextBox, které se ve vlastnostech nastaví MaxLenght, česky maximální délku řetězce na hodnotu definovanou ČSSZ. Pro datový typ N je vhodným prvkem NumericUpDown, který umožňuje práci jen s čísly. Ve vlastnostech tohoto prvku je možné nastavit minimální a maximální hodnotu a skok při inkrementaci respektive dekrementaci. DateTimePicker bude sloužit pro pole vyžadující datový typ D. Zobrazení kalendáře nebo jen šipek pro úpravu data je ovlivněno volbou vlastnosti ShowUpDown na hodnotu False nebo True. Jednou z dalších vlastností je CustomFormat, která umožňuje vlastní nastavení zobrazování data. Pro dosažení data ve formátu DD.MM.RRRR (30.04.2009) musíme zadat „dd.MM.yyyy“. U definování vlastního formátu je nutné dbát na velikost písmen jelikož „mm“ není totéž co „MM“. Výraz s malými písmeny označuje minuty a MM měsíc. Pole označená na obrázku Obrázek 12 písmeny Č a D bude reprezentovat komponenta ComboBox neboli rozbalovací seznam, který bude nabývat hodnot načtených z databáze, tím bude zajištěna správnost vkládaných dat.

4.4.4 LOGICKÉ TESTY

Některé údaje je možné zkontrolovat pomocí logických testů. Nejčastěji to bývají údaje jako rodné číslo, identifikační číslo, daňové identifikační číslo, aj. Následující kapitoly uvedou logický test pro rodné číslo a identifikační číslo.

4.4.4.1 KONTROLA RODNÉHO ČÍSLA

Rodné číslo je jednoznačný a jedinečný identifikátor, přidělovaný občanům České republiky, dá se z něho vyčíst rok, měsíc a den narození a pohlaví. Pro rozlišení rodných čísel se používá od 1. 1. 1954 čtyřčíslí za lomítkem a před tímto rokem se používalo trojčíslí. Pro rodná čísla po roce 1953 existuje test pro kontrolu správnosti, který je založen na porovnávání kontrolního čísla se zbytkem po dělení rodného čísla jedenácti **Chyba! Nenalezen zdroj odkazů.**

První test, který se provede, je kontrola délky rodného čísla. Pro občany narozené po roce 1953 musí mít rodné číslo deset znaků a občané narození do roku 1954 mají rodné číslo o délce devíti znaků.

Druhým testem bude zjištění, zda rodné číslo je dělitelné či není číslem jedenáct. Existuje však výjimka, kdy po vydělení rodného čísla jedenácti vyjde zbytek roven desíti, pak kontrolní číslice je nula.

Algoritmus použitý ke kontrole rodného čísla je následující. Vysvětlení jednotlivých částí kódů je označeno jako ve visual studiu poznámky tedy „'text…“.

```
    Public Function kontrola_RC(ByVal rodne_cislo As String)
'ověření zda proměnná rodne_cislo nabývá jen číselných hodnot je ověřeno při zadávání, tudíž zde není nutné již toto ověřovat

        Dim posledni_cislo, rc, rc2 As String
        Dim ok As Boolean
        Dim zbytek As Integer
        rc = rodne_cislo.Replace(" ", "") 'odstranění mezer z řetězce
        If rc.Length = 9 Then
'pokud rodné číslo bude mít délku 9, tudíž by rok narození měl být menší než 54, což ověřuje následující podmínka, kde funkce Substring(0,2) říká odděl z řetězce dva znaky od počátečního znaku

            If rc.Substring(0, 2) < 54 Then
                ok = True
'po splnění této podmíny již neexistuje další test a můžeme prohlásit, že rodné číslo je tedy správné

            Else
                ok = False
                Return False
                Exit Function
            End If
        Else
'pokud rodné číslo má délku 10, délka rodného čísla je omezena při vstupu, proto zde už není třeba ji řešit

            posledni_cislo = rc.Substring(9, 1)
            rc2 = rc.Substring(0, 9)
            zbytek = (rc2 Mod 11) 'celočíselný zbytek po dělení rodného čísla 11

            If zbytek < 10 Then
                If zbytek = posledni_cislo Then
'poud se zbytek rovná poslední kontrolní číslici je rodné číslo správné

                    ok = True
                Else
                    ok = False
                    Return False
                    Exit Function
                End If
            ElseIf zbytek = 10 Then
```

```
'pokud se zbytek rovná číslu 10, tudíž kontrolní číslo by mělo být rovno 0, za
platnosti této podmínky je rodné číslo také správné

                If posledni_cislo = 0 Then
                    ok = True
                Else
                    ok = False
                   Return False
                   Exit Function
                End If
            End If
        End If
            Return ok
End Function
```

4.4.4.2 KONTROLA IDENTIFIKAČNÍHO ČÍSLA

Identifikační číslo je unikátním osmimístným číslem podnikatele nebo právnické osoby, přidělované živnostenským úřadem. Správné identifikační číslo musím mít osm znaků, obsahovat pouze numerické znaky a musí splňovat podmínku dělitelnosti jedenácti, která zní [7]:

$$n_0 = \left[\left(11 - \sum_{i=1}^{7} n_i * (i+1)\right) \bmod 11\right] \bmod 10$$

Kde n_i je číslice identifikačního čísla zprava.

Algoritmus kontrolující jeho správnost tedy je:

```
Public Function kontrola_IC(ByVal IC As String)

        Dim cislo, soucet, nasobek, kontrola As String
        Dim ok_ic As Boolean
        Dim i, zbytek11, zbytek10 As Integer

        If IC = "" Then 'kontrola zda bylo vloženo nějaké identifikační číslo
            ok_ic = True
            Return ok_ic
           Exit Function
        ElseIf Char.IsNumber(IC) Then 'kontrola zda zadaná hodnota je číslo
            nasobek = 9

            If IC.Length = 8 Then 'kontrola délky řetězce
                For i = 0 To 6 'výpočet kontrolního součtu
                    cislo = IC.Substring(i, 1)
                    nasobek = nasobek - 1
                    soucet = soucet + cislo * nasobek
                    cislo = ""
                Next

                zbytek11 = (soucet Mod 11) 'výpočet zbytku po dělení 11
               zbytek10 = (zbytek11 Mod 10) 'výpočet zbytku po dělení 10
                kontrola = 11 - zbytek10 'výpočet kontrolního čísla
```

```
                If kontrola = IC.Substring(7, 1) Then
'porovnání kontrolního čísla s číslem z identifikačního čísla na pozici 8

                    ok_ic = True
                Else
                    ok_ic = False
                End If
            End If
                Return ok_ic
        Else 'pokud vložené identifikační číslo obsahuje jiné znaky než numerické
           Exit Function
        End If
    End Function
```

4.4.5 GENEROVÁNÍ DATOVÉ ZPRÁVY POMOCÍ APLIKACE

Nyní je již zajištěné prostředí pro vstup dat a jejich správnost. Nyní přichází krok, kdy se bude vytvářet datová zpráva, která bude následně poslána vlastní aplikací do aplikace elektronického podání portálu veřejné správy. Postup tvorby datové zprávy bude začínat nejprve vytvořením datové větve, následně jejím podepsáním a nakonec zašifrováním. V druhém kroku se vytvoří celá datová zpráva, jejíž schéma je v příloze 4 a popis v kapitole 3.5

Pro práci s xml daty je v programu využito technologie LINQ TO XML. Tato technologie má usnadnit práci s xml, umožňuje přímo do kódu zápis v struktuře xml a pomocí sledů znaků <%= kód VB aplikace > dává možnost v jakémkoliv místě xml struktury vložit kód Visual Basicu. V práci je využito konstruktorů, XDocument, XElement, XAttribute a XNamespace. Už na první pohled, dle názvu konstruktorů, je patrné k čemu se používají. Xdocument reprezentuje xml dokument, XElement se využívá k vytvoření elementu, XAttribute atributu a XNamespace k definování namespace elementu.

Pro lepší představení problematiky je zde uvedeno několik řádků kódu:

```
Dim xml As XDocument = _
     <?xml version="1.0"?>
      <GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
        <EnvelopeVersion>2.0</EnvelopeVersion>
        <Header>
          <MessageDetails>
            <Class><%= class_ %></Class>
            <Qualifier>poll</Qualifier>
            <Function>submit</Function>
            <CorrelationID><%= correlationID %></CorrelationID>
            <Transformation>XML</Transformation>
          </MessageDetails>
          <SenderDetails/>
        </Header>
        <GovTalkDetails>
          <Keys/>
        </GovTalkDetails>
        <Body/>
      </GovTalkMessage>
xml.Save("soubor.xml")
```

Kde proměnná xml obsahuje celý xml dokument. Žlutě zvýrazněné části kódů reprezentují možnost, jak do xml vložit část kódů Visual Basic, v tomto příkladě je zde proměnná „class_“, která předá elementu „Class“ hodnotu. Z takto vytvořeného dokumentu, který zatím je jen v proměnné je možné jedním příkazem vytvořit soubor typu xml, což představuje poslední řádek kódu.

Všechny datové zprávy, které budou v aplikaci použity, jsou generovány podobným způsobem.

4.4.6 PODEPSÁNÍ DATOVÉ ZPRÁVY

Algoritmus, kterým se v aplikaci bude podepisovat datová věta je znázorněn na následujícím kódu [4]:

```
Dim uloziste As New CAPICOM.Store
Dim certifikaty As CAPICOM.Certificate
Dim podpis As String
Dim podepsana_data As CAPICOM.SignedData

podepsana_data = New CAPICOM.SignedData

Dim signatar As CAPICOM.Signer

signatar = New CAPICOM.Signer

uloziste.Open() 'otevření uložiště certifikátů

For Each certifikaty In uloziste.Certificates 'prohledávání certifikátů
```

```
...
Next

signatar.Certificate = certifikaty 'přiřazení certifikátu do proměnné signer
podepsana_data.Content = datovaVeta.ToString 'načtení datové věty do proměnné
podpis = podepsana_data.Sign(signatar, True) 'vytvoření podpisu
```

4.4.7 ŠIFROVÁNÍ DATOVÉ ZPRÁVY

Podepisování datové zprávy je realizováno pomocí řešení, které nabízí Microsoft pod názvem CAPICOM. [4]

```
Dim uloziste As New CAPICOM.Store
Dim certifikaty As CAPICOM.Certificate

Dim sifr_cssz As CAPICOM.Signer
sifr_cssz = New CAPICOM.Signer

myStore.Open()'otevření uložiště certifikátů

For Each certifikaty In uloziste.Certificates 'prohledávání certifikátů
...
Next

sifr_cssz.Certificate = myCert 'přiřazení certifikátu do proměnné signer
Dim sifr_data As CAPICOM.EnvelopedData
sifr_data = New CAPICOM.EnvelopedData

sifr_data.Algorithm.KeyLength = CAPICOM.CAPICOM_ENCRYPTION_KEY_LENGTH.CAPICOM
                                _ENCRYPTION_KEY_LENGTH_MAXIMUM

sifr_data.Algorithm.Name = CAPICOM.CAPICOM_ENCRYPTION_ALGORITHM.CAPICOM
                           _ENCRYPTION_ALGORITHM_3DES

sifr_data.Content = datovaVetev.ToString 'načtení datové věty do proměnné

sifr_data.Recipients.Add(sifr_cssz.Certificate)

Dim zasifr_zprava As String

zasif_zprava = sifr_data.Encrypt() 'zašifrování datové věty
```

4.4.8 TRANSAKCE DATOVÉ ZPRÁVY NA PORTÁL VEŘEJNÉ SPRÁVY

Zprávu, která je již vytvořená na základně podkladů PVS a ČSSZ, je nutné nějakým způsobem dopravit na portál veřejné správy. Jak probíhá komunikace je již popsáno a graficky znázorněno v kapitole 3.4.3. Jak je již z obrázku patrné, vyvíjená aplikace musí umět nejen odeslat zprávu, ale také přijmout. Dále musí umět přijatou zprávu přečíst a správně na ni reagovat.

4.4.8.1 ODESLÁNÍ A PŘÍJEM DATOVÉ ZPRÁVY

Komunikace s portálem veřejné správy zajišťuje následující kód:

```
Function send(ByVal URL As String, ByVal data As XDocument)
        Dim http As System.Net.HttpWebRequest
        Dim response As System.Net.WebResponse
        Dim respStream As System.IO.Stream
        Dim streamR As System.IO.StreamReader
        Dim streamW As System.IO.StreamWriter
        Dim RespText As String = Nothing

            http = http.Create(URL)
            http.Method = "POST"
            http.ContentType = "text/xml"
            http.Timeout = 90000
            streamW = New IO.StreamWriter(http.GetRequestStream())
            data.Save(streamW)
            streamW.Close()
            response = http.GetResponse()'odeslání datové zprávy na server
            respStream = response.GetResponseStream()'příjem odpovědi
            streamR = New IO.StreamReader(respStream,
System.Text.Encoding.GetEncoding(1250)) 'převedení přijaté zprávy do textu
            RespText = streamR.ReadToEnd()
            streamW.Close()
            Return RespText
End Function
```

4.4.8.2 PARSOVÁNÍ PŘIJATÉ ZPRÁVY

Přijatou zprávu je nutné přečíst a zjistit, co aplikace elektronického podání portálu veřejné správy poslala zpět. Posílané zprávy jsou ve formátu xml a přijímané taktéž. Struktury těchto zpráv jsou v přílohách 7-10 a popis je uveden v kapitole 3.4.2.2. Informace které je nutné zjistit jsou CorrelationID, který následně budeme používat v další komunikaci, qualifier určující zda byla zpráva zpracována nebo vrácena s chybou, pollinterval je čas, po který musí vlastní aplikace počkat, než pošle další zprávu, ResponseEndPoint určuje, na jakou adresu se bude zpráva posílat, Function definuje typ zprávy. Kód uvedený níže ukazuje, jak se do proměnných načítají hodnoty z přijaté zprávy. Hodnota elementu se zjistí pomocí názvu elementu a slovíčka „Value“. Pro zjištění hodnoty atributu je potřeba použít zavináč (@) a název požadovaného atributu.

```
xmlns = "http://www.govtalk.gov.uk/CM/envelope"
qualifier = odpoved.Descendants(xmlns + "Qualifier").Value
correlationID = odpoved.Descendants(xmlns + "CorrelationID").Value
pollinterval = odpoved.Descendants(xmlns + "ResponseEndPoint").@PollInterval
responseEndPoint = odpoved.Descendants(xmlns + "ResponseEndPoint").Value
class_ = odpoved.Descendants(xmlns + "Class").Value
function_ = odpoved.Descendants(xmlns + "Function").Value
```

Podle hodnoty proměnné function a qualifier se aplikace rozhodne jakou zprávu má poslat na portál veřejné správy. Proces komunikace je graficky znázorněn a popsán v kapitole 3.4.3 a odesílané zprávy, které se vytvoří stejným způsobem jako v kapitole 4.4.5, jsou v přílohách 5-7.

4.4.9 TESTOVÁNÍ ELEKTRONICKÉHO PODÁNÍ

Testování probíhá na testovací transakční části portálu veřejné správy, která je shodná s ostrou transakční částí portálu veřejné správy. Pro testování se využívají testovací údaje, ale je možné používat i údaje pro ostrou část aplikace elektronického podání od České správy sociálního zabezpečení. Registrace na portále veřejné správy se provádí zvlášť pro testování a zvlášť pro ostré podání.

Rozdíly mezi testovací částí a ostrou jsou v používání jiných certifikátů k navazování SSL komunikace, u testovací části není garantovaná nepřetržitá dostupnost. Testovací prostředí je vybudováno na omezeném množství hardwaru, tudíž se doporučuje posílat podání maximálně do 0,5 MB.

5 ZHODNOCENÍ A VYUŽITÍ APLIKACE

Vlastní vývoj aplikace probíhal v celku až na pár výjimek a jednom velkém problémů díky Microsoft Visual Studia Professional 2008 dobře. Tato verze má již velice dobře zpracovanou Intellisense, která při zadání prvního znaku už nabízí možné části kódu, ve spojení s linq to „cokoliv“, v této práci hlavně linq to sql a xml, dokáže výborně napovídat při tvorbě dotazů, například do databáze. Další a to významnou podporou této práci byl diskusní server určený pro vývojáře programů pro elektronické podání přes portál veřejné správy dostupný na adrese https://bezpecne.dev.gov.cz/diskuze/forums/default.aspx a webové stránky vbnet.cz.

Visual studio nabízí z prvu dobře vypadající nástroj designér pro technologii linq to sql, kde je možné vytvořit spojení s databází pouhým přetažením tabulek z databáze do projektu. Visual studio si pak sám vytvoří cennection string a spoustu kódu, které díky tomuto designéru se nemusí psát ručně. Problém nastane tehdy, pokud náhodou je potřeba provést změnu ve struktuře databáze. Například v této práci, při navrhování databáze v roce 2008 měl variabilní symbol zaměstnavatele maximálně osm znaků, od letošního roku má deset znaků, a proto byla potřeba upravit tabulka zaměstnavatele, kde bylo omezení délky sloupce pro vkládání variabilního symbolu na osm znaků. Ovšem jakákoliv následná změna v kódu, vytvořeném designérem, vytváří skoro neřešitelný problém. Veškeré dotazy hlásí chybu. Prozatím jediným řešením je smazat soubory týkající se tohoto problému a vytvořit je znovu. Poté upravit všechny dotazy respektive je vytvořit znovu. Proto používání designéru je prozatím lepší se vyhnout a psát kód ručně.

Při dodržení zásad ČSSZ a portálu veřejné správy pro tvorbu datové zprávy a její odeslání nebylo testování na samotném portálu veřejné správy v testovací části již nijak obtížně, jen časově náročné. To vyplývá z toho, že každé podání v průměru trvá kolem 3-4 minut, ale někdy i třeba jednou tolik, což je závislé na zatížení serveru.

Tato aplikace by po rozšíření počtu nabízených služeb, podporujících elektronické podání mohla být velmi užitečná. Firmám by přinesla úsporu času, práce, financí a všech nákladů souvisejících s papírovým vyřizováním formulářů úřadů veřejné správy.

6 ZÁVĚR

Tato bakalářská práce je zaměřená ne elektronické podání přes portál veřejné správy, které přináší spoustu výhod. Mezi hlavní výhody bezesporu patří dostupnost 24 hodin 7 dní v týdnu, automatická odezva informující, zda bylo podání přijato nebo zamítnuto a důvod zamítnutí, možnost okamžité opravy a nového podání, není nutné řešit problémy při tisku do tiskopisů, zejména složité nastavování tiskárny a je zajištěna vysoká úroveň zabezpečení.

Pro účely testování aplikace elektronického podání byla vybrána služba České správy sociálního zabezpečení a to přihláška k nemocenskému pojištění, kterou podává zaměstnavatel za zaměstnance.

Bakalářská práce popisuje postup podání od registrace na ČSSZ až po přijetí emailu, který informuje uživatele o úspěšném podání. Registrací u ČSSZ je získáno registrační číslo potřebné pro aktivaci služeb při registraci na portálu veřejné správy a variabilní symbol, který je rovněž potřeba pro aktivaci služby, ale dále se používá pro elektronické podání. Další registrace je nutná na portálu veřejné správy, kde je zvolen identifikátor a heslo. Oba tyto údaje jsou potřebné rovněž při podání. Posledním krokem před vlastním podáním je nutné ještě zažádat o kvalifikovaný certifikát, který je používán k elektronickému podpisu.

Dále je definována zpráva, která se posílá aplikaci elektronického podání portálu veřejné správy. Tato zpráva se skládá z datové věty, která obsahuje údaje vyplněné ve formuláři. Datová věta je podepsaná kvalifikovaným certifikátem a zašifrovaná certifikátem ČSSZ. Zprávu ještě tvoří dvě části, obálka ČSSZ a GovTalk obálka portálu veřejné správy. Takto připravená zpráva je poslána aplikaci EP PVS. Úspěšné podání je indikováno zprávou přijatou od portálu veřejné správy a emailem.

Aplikace vyvíjená v této práci umožňuje vyplnění údajů, provedení kontroly vložených dat, následné vytvoření podepsané a zašifrované zprávy, která je posílána na portál veřejné správy. Uživateli poskytuje zpětnou vazbu tím, že mu oznámí, zda je podání úspěšně doručené, nebo zda je vráceno s chybou. Program by měl uživateli ušetřit čas, který by strávil

s vyplňováním a doručováním papírového formuláře a dále mu ušetří finanční prostředky, které jsou spojeny právě z papírovou formou přihlášky.

Oba stanovené cíle a to pochopení a popsání problematiky elektronického podání na portálu veřejné správy a tvorba vlastní aplikace schopné úspěšně podat vlastní podání přes portál veřejné správy se podařilo splnit, což i dokazuje email o úspěšném podání v příloze 11.

Elektronizace úkonů veřejné správy přináší ulehčení jak uživatelům, tak i úřadům veřejné správy. V budoucnu bude docházet k rozšiřování poskytovaných služeb elektronického podání a jednou bychom se mohli dočkat plně elektronizované veřejné správy.

7 POUŽITÁ LITERATURA

[1] ABC Linuxu [online]. c1999-2009 [cit. 2009-04-14]. Dostupný z WWW: <http://www.abclinuxu.cz/slovnik/hash>. ISSN 1214-1267.

[2] Aplikace Elektronická podání. Portál veřejné správy [online]. 2007 [cit. 2009-04-11]. Dostupný z WWW: <http://www.podani.gov.cz/getfile.aspx?key=UzivatelskaPrirucka.zip&dataType=file>.

[3] Certifikáty veřejných klíčů. Zpravodaj ÚVT MU [online]. 2000 [cit. 2009-04-14]. Dostupný z WWW: <http://www.ics.muni.cz/zpravodaj/articles/181.html>. ISSN 1212-0901.

[4] Česká správa sociálního zabezpečení : Tvorba aplikací pro transakční část PVS [online]. 2004 [cit. 2009-04-20]. Dostupný z WWW: <http://www.cssz.cz/NR/rdonlyres/E37951F0-2341-49C0-BCE1-D7BADBAB0B8F/916/TvorbaAplikaciprotransakcnicastPVS.ppt>.

[5] Česká správa sociálního zabezpečení : Datová věta přihlášky zaměstnance [online]. [2009] [cit. 2009-04-20]. Dostupný z WWW: <http://www.cssz.cz/NR/rdonlyres/FC8CFE81-D185-47DA-8B0B-127E506B71BA/892/dat_veta_pr1.htm>.

[6] Česká správa sociálního zabezpečení : Nemocenské pojištění [online]. [2008] [cit. 2008-10-01]. Dostupný z WWW: <http://www.cssz.cz/cz/tiskopisy/nemocenske-pojisteni.htm>.

[7] Česká správa sociálního zabezpečení : Logické testy datové věty [online]. [2009] [cit. 2009-04-20]. Dostupný z WWW: <http://www.cssz.cz/cz/e-podani/druhy-e-podani/e-podani-prihlasek-a-odhlasek-zamestnancu-k-nemocenskemu-pojisteni/pro-tvurce-programu-na-e-podani-p-o/logicke-testy-datove-vety.htm>.

[8] Česká správa sociálního zabezpečení : Tělo zprávy [online]. [2008] [cit. 2009-04-20]. Dostupný z WWW: <http://www.cssz.cz/NR/rdonlyres/FC8CFE81-D185-47DA-8B0B-127E506B71BA/894/obalka_cssz1.htm>.

[9] Databáze a jazyk SQL. Interval [online]. 2000 [cit. 2009-04-19]. Dostupný z WWW: <http://interval.cz/clanky/databaze-a-jazyk-sql/>. ISSN 1212-8651 .

[10] E-Government [online]. 2008 [cit. 2009-04-16]. Dostupný z WWW: <http://web.mvcr.cz/archiv2008/micr/egovernment/default.htm>.

[11] HOLAŇ, Jiří. Podrobný popis GovTalk obálky verze 3.0. Aplikace elektronická podání [online]. 2006 [cit. 2009-04-20]. Dostupný z WWW: <https://bezpecne.dev.gov.cz/diskuze/files/487/download.aspx>.

[12] Informační systémy veřejné správy : Elektronický doklad v účetnictví [online]. c2001-2009 [cit. 2009-04-28]. Dostupný z WWW: <http://www.isvs.cz/e-podpis-podatelny/elektronicky-doklad-v-ucetnictvi-elektronicky-podpis-3-dil.html>.

[13] Informační systémy veřejné správy : Symetrické šifrovací algoritmy [online]. c2001-2009 [cit. 2009-04-28]. Dostupný z WWW: <http://www.isvs.cz/e-podpis-podatelny/symetricke-sifrovaci-algoritmy-16-dil.html>.

[14] Informační systémy veřejné správy : Asymetrické šifrovací algoritmy [online]. c2001-2009 [cit. 2009-04-28]. Dostupný z WWW: <http://www.isvs.cz/e-podpis-podatelny/asymetricke-sifrovani-a-jeho-prakticke-vyuziti-19-dil.html>

[15] Informační systémy veřejné správy : Hybridní šifrovací algoritmy [online]. c2001-2009 [cit. 2009-04-28]. Dostupný z WWW: < http://www.isvs.cz/e-podpis-podatelny/hybridni-sifrovaci-algoritmy-20-dil.html>

[16] Informační systémy veřejné správy : Portál veřejné správy [online]. c2001-2009 [cit. 2009-04-28]. Dostupný z WWW: <http://www.isvs.cz/portal-gov-cz/portal-verejne-spravy-k-cemu-je-nebo-muze-byt-1-dil.html>.

[17] Internet X.509 Public Key Infrastructure : Certificate and CRL Profile. Zpravodaj ÚVT MU [online]. 1999 [cit. 2009-04-14], s. 129. Dostupný z WWW: <ftp://ftp.muni.cz/pub/rfc/rfc2459.txt>.

[18] KODL, Jindřich. FYZIKÁLNÍ ÚSTAV [online]. 2000 [cit. 2009-04-16]. Dostupný z WWW: <http://www.fzu.cz/texty/ruzne/el_podpis.html>.

[19] LANGOVÁ, Petra. Novinky e - Podání v ČSSZ [online]. 2009 [cit. 2009-04-24]. Dostupný z WWW: <http://www.isss.cz/archiv/2009/download/prezentace/langova_cssz.pdf>.

[20] Portál veřejné správy České republiky : Dostupné elektronické služby [online]. c2003-2009 [cit. 2009-04-28]. Dostupný z WWW: <http://portal.gov.cz/wps/portal/_s.155/7238?docid=102305>.

[21] Portál veřejné správy odstartuje za měsíc. Lupa [online]. 2003 [cit. 2009-04-08]. Dostupný z WWW: <http://www.earchiv.cz/b03/b0915001.php3>.

[22] Portál veřejné správy. Ministerstvo informatiky [online]. 2008 [cit. 2009-04-11]. Dostupný z WWW: <http://web.mvcr.cz/archiv2008/micr/scripts/detail.php_id_411.html>.

[23] První certifikační autorita, a. s. [online]. c2000-2008 [cit. 2009-04-14]. Dostupný z WWW: <http://www.ica.cz/cz/menu/29/produkty-a-sluzby/certifikaty/>.

[24] První certifikační autorita, a. s. [online]. c2000-2008 [cit. 2009-04-17]. Dostupný z WWW: <http://www.ica.cz/cz/menu/39/produkty-a-sluzby/zadost-o-certifikat/priprava-pc/>.

[25] Portál veřejné správy [online]. c2003-2009 [cit. 2009-04-18]. Dostupný z WWW: <https://bezpecne.podani.gov.cz/default.aspx>.

[26] Portál veřejné správy : Provozní řád Transakční části Portálu veřejné správy [online]. 2008 [cit. 2009-04-20]. Dostupný z WWW: <http://www.podani.gov.cz/getfile.aspx?key=Provozni_Rad.pdf&dataType=doc>.

[27] Sbírka zákonů Česká republika [online]. 2000 [cit. 2009-03-17]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/sbirka/2000/sb099-00.pdf>.

SEZNAM OBRÁZKŮ TABULEK A GRAFŮ

Seznam obrázků

Obrázek 1 Portál veřejné správy, zdroj: [vlastní] 14

Obrázek 2 Symetrické šifrování, zdroj: [vlastní] 19

Obrázek 3 Asymetrické šifrování - šifrování zprávy, zdroj: [vlastní] 19

Obrázek 4 Asymetrické šifrování - podepisování zprávy, zdroj: [vlastní] 20

Obrázek 5 Asymetrické šifrování - kombinace metod, zdroj: [vlastní] 21

Obrázek 6 Posílání podepsané zprávy elektronickým podpisem, zdroj: [vlastní] 25

Obrázek 7 Základní architektura systému elektronického podání 27

Obrázek 8 Úspěšné podání datové zprávy, zdroj: [vlastní] 30

Obrázek 9 Vygenerovaná žádost, zdorj: [vlastní] 45

Obrázek 10 Úspěšná instalace certifikátu, zdroj: [vlastní] 46

Obrázek 11 Registrace uživatele na portále veřejné správy, zdroj: [vlastní] 49

Obrázek 12 Formulář přihlášky k nemocenskému pojištění, zdroj: [vlastní] 52

Obrázek 13 ER diagram, zdroj: [vlastní] 54

Seznam tabulek

Tabulka 1 Služby poskytované pro elektronické podání přes portál veřejné správy 17

Tabulka 2 Datové typy 51

Tabulka 3 Datová věta přihlášky zaměstnance 33

Tabulka 4 Obálka České správy sociálního zabezpečení 35

SEZNAM PŘÍLOH

Příloha 1 - Protokol o podání žádosti na vydání kvalifikovaného certifikátu I. CA 70

Příloha 2 - Smlouva o vydání a používání kvalifikovaných certifikátů – strana1 71

Příloha 3 - Číselníky 1/4 72

Příloha 3 - Číselníky 2/4 73

Příloha 3 - Číselníky 3/4 74

Příloha 3 - Číselníky 4/4 75

Příloha 4 - Struktura datové zprávy SUBMISSION_REQUEST 76

Příloha 5 - Struktura datové zprávy SUBMISSION_POLL 77

Příloha 6 - Struktura datové zprávy DELETE_REQUEST 78

Příloha 7 - Struktura datové zprávy SUBMMISION_ACKNOWLEDGEMENT 79

Příloha 8 - Struktura datové zprávy SUBMISION_RESPONSE 80

Příloha 9 - Struktura datové zprávy DELETE_ACKNOWLEDGEMENT 81

Příloha 10 - Struktura datové zprávy DELETE_RESPONSE 82

Příloha 11 - Email o úspěšním podání 83

Příloha 1 - Protokol o podání žádosti na vydání kvalifikovaného certifikátu I. CA

Protokol o podání žádosti na vydání kvalifikovaného certifikátu I.CA

Registrační číslo žádosti: **HK10000596** Kód služby: 01

Číslo registrační autority: **HK**
Datum a čas podání žádosti: **09.04.2009 09:46**

Údaje žadatele uvedené v předloženém dokladu totožnosti:

Titul:	
Příjmení:	**Berný**
Jméno:	**Petr**
Rodné číslo:	**8605251138**
Adresa pobytu:	**Bezručova 861, 28903 Městec Králové**
Typ a číslo primárního dokladu:	**Občanský průkaz:** [redacted]
Sekundární doklad:	**ŘP** [redacted]
Ostatní doklady:	

Položky žádosti, za jejichž úplnost a správnost se žadatel zaručuje:

Jméno(CN)	**Petr Berný**
Stát(C)	**CZ**
E-mailová adresa(E)	[redacted]

Požadavek na služby I.CA:

Zasílání aktuálního CRL:	**Ne**
Zveřejnění certifikátu:	**Ano**
Identifikátor MPSV:	**Ano**

Heslo pro zneplatnění certifikátu: [redacted]
Číslo karty: **-**

Jméno a příjmení operátora RA: **Ing. Eva Nováková**

Žadatel se zavazuje, že data pro vytváření elektronického podpisu odpovídající veřejnému klíči předloženému v této žádosti o kvalifikovaný certifikát byla vygenerována v souladu se zákonem ČR č. 227/2000 Sb., o elektronickém podpisu v platném znění.
Žadatel kontroloval výše uvedené údaje a stvrzuje jejich správnost.
Žadatel souhlasí se zpracováním a shromažďováním osobních údajů dle Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění, nebo Zákona č. 428/2002 Z. z. o ochrane osobných údajov v platnom znení, za účelem naplnění požadavků Zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení.
Žadatel souhlasí s tím, aby společnost První certifikační autorita, a.s. skladovala pořízené kopie jeho osobních dokladů v souladu s platnou legislativou.

V Pardubicích dne 09.04.2009

žadatel

operátor RA

První certifikační autorita, a.s.
CERTIFICATION I·CA AUTHORITY
Podvinný mlýn 2178/6
190 00 Praha 9
IČO: 264 39 395
-117-

Příloha 2 - Smlouva o vydání a používání kvalifikovaných certifikátů – strana1

Smlouva o vydání a používání kvalifikovaných certifikátů

PRVNÍ CERTIFIKAČNÍ AUTORITA, a.s., Podvinný mlýn 2178/6, Praha 9, IČ: 264 39 395, zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B 7136 (dále jen "I.CA") v zastoupení: Ing. Petr Budiš PhD, předseda představenstva a Ing. Martin Škorpil, člen představenstva, odpovědná osoba ve věcech I.CA: operátor RA Ing. Eva Nováková na straně jedné

a

Petr Berný, r.č. [redacted]
Adresa: [redacted]

(jméno, příjmení a rodné číslo žadatele o kvalifikovaný certifikát)
(dále jen "žadatel") na straně druhé

uzavírají v souladu s ustanovením § 269 odst.2 obchodního zákoníku níže uvedeného dne, měsíce a roku tuto smlouvu o vydání a používání kvalifikovaného certifikátu I.CA (dále jen „QC"), jímž se rozumí kvalifikovaný certifikát v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu v platném znění (dále jen „ZoEP"), který I.CA vede pod jedinečným jménem žadatele o kvalifikovaný certifikát (dále jen „DN") :

Stát(C)	**CZ**
Jméno(CN)	**Petr Berný**
E-mailová adresa(E)	[redacted]
Sériové číslo(SN)	**ICA - 10115752**

Výpis kvalifikovaného certifikátu v PEM formátu:

```
-----BEGIN CERTIFICATE-----
MIIEeDCCA2CgAwIBAgIEAJ3aXDANBgkqhkiG9w0BAQUFADBoMQswCQYDVQQGEwJD
WjEqMCgGA1UEAwwhSS5DQSAtIFF1YWxpZmllZCByb290IGNlcnRpZmljYXRlMS0w
KwYDVQQKDCRQcnZuw60gY2VydGlmaWthxI1uw60gYXV0b3JpdGEsIGEucy4wHhcN
MDkwNDA5MDc0OTI3WhcNMTAwNDA5MDc0OTI3WjBhMQswCQYDVQQGEwJDWjEUMBIG
A1UEAwwLUGV0ciBCZXJuw70xIzAhBgkqhkiG9w0BCQEWFHBldHIuYmVybnlAc2V6
bmFtLmN6MRcwFQYDVQQFEw5JQ0EgLSAxMDExNTc1MjCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA3LWK0wqPv3dNU6GgbmKVCEPxF+7GlKeKABzYnam7UoJEddnX
UC+LpbOtR/t3SCM1d2FP83TOQcNCvtkXjIhP03akDUPw8vGHYaD1pORj7KJY0T0n
jFF6kaSZRZ+T30O7E5HcSgxPx+72TBl17PWf0rztSE5pDVLft/ctDUpnS6MCAwEA
AaOCAbMwggGvMCQGA1UdEQQdMBugGQYJKwYBBAHcGQIBoAwMCjE4NDc4NTU2MTQw
DgYDVR0PAQH/BAQDAgTwMIGBBgNVHR8EejB4MCagJKAihiBodHRwOi8vcWNybGRw
MS5pY2EuY3ovcWljYTA4LmNybDAmoCSgIoYgaHR0cDovL3FjcmxkcDIuaWNhLmN6
L3FpY2EwOC5jcmwwJqAkoCKGIGh0dHA6Ly9xY3JsZHAzLmljYS5jei9xaWNhMDgu
Y3JsMB8GA1UdIwQYMBaAFGidftbEJTn7O6A31k/cjNF68FZZMB0GA1UdDgQWBBQk
2aneJqAm6bT52MQQN0u1dzYXojCBmAYDVR0gBIGQMIGNMIGKBgwrBgEEAYG4SAEE
CgUwejB4BggrBgEFBQcCAjBsGmpUZW50byBrdmFsaWZpa292YW55IGNlcnRpZmlr
YXQgamUgdnlkYW4gdiBzb3VsYWR1IHNlIHpha29uZW0gQ2Vza2UgcmVwdWJsaWt5
IDIyNy8yMDAwIFNiLiB2IHBsYXRuZW0gem5lbmkuMBgGCCsGAQUFBwEDBAwwCjAI
BgYEAI5GAQEwDQYJKoZIhvcNAQEFBQADggEBAI6lCvfmgZ57BENWkTF59tmKqZp/
A3VJhVeH4mdGd20VHr7plL9uXC2Lxyou6u+KZIaNhZsFx20p952Rmiz2rFyXQy4G
BFjaz11kmxuoYQ6cjCwyNx+RCyggv1ZFAmgLjkjIwH45LKDNF8xmCHYhpZlGIkW9
sjOHEN/sFiVl/DtE/HGHM2IohmYN+MmGRFAlh57bYQrFJYqzH6JLtii26ID9SDGM
m0wEq6umMRPM30jfaJ0pWIYymetxFnu98ZKKC2jLFxsM3RjL1ZVZEQ8bhriQbM3E
2CqFVjUBx12KIR4+n457WTRsom5fdCxR31Xj
-----END CERTIFICATE-----
```

Otisk prstu certifikátu (fingerprint) - MD5: [6C:A0:40:26:F1:ED:4F:1E:38:48:13:11:74:B1:D4:02]
Otisk prstu certifikátu (fingerprint) - SHA1: [48:16:74:08:1A:2C:A9:9B:23:02:C0:3D:C9:82:6D:89:EE:56:48:80]

Sériové číslo certifikátu:	**10345052 (9DDA5C hex)**
Číslo registrační autority:	**HK**
Datum vzniku certifikátu:	**09.04.2009 - 07:49:27 GMT**
Datum ukončení platnosti certifikátu:	**09.04.2010 - 07:49:27 GMT**
Registrační číslo žádosti:	**HK10000596**

QC byl vydán na základě žádosti vedené pod výše uvedeným registračním číslem a přiložených dokladů dne 09.04.2009 a je zaregistrován u I.CA se sériovým číslem 10345052 (9DDA5C hex).

Příloha 3 - Číselníky 1/4

RODINNÝ STAV

id	popis
1	svobodný(á)
2	ženatý (vdaná)
4	rozvedený(á)
5	ovdovělý(á)

POHLAVÍ

id	popis
M	muž
Ž	žena
0	nezjištěno

AKCE

id	popis
1	přihláška
2	odhláška
3	změna údajů zaměstnance
4	hromadný sběr
5	oprava chybně uvedených údajů zaměstnance

DRUH DŮCHODU

id	popis
0	nepobírá
1	starobní
2	invalidní plný
A	cizí charakteru starobního
B	cizí charakteru invalidního plného

DRUH VÝDĚLEČNÉ ČINNOSTI

id	popis
0	první pracovní poměr
1	druhý pracovní poměr
2	třetí pracovní poměr
3	dohoda o prac. činn.
4	dobrovolný pracovník pečovatelské služby
5	nepravidelná výpomoc
6	dohoda o prac. činn.
7	společník,jednatel,komandista
8	člen družstva
9	domácí zam.
A	čtvrtý pracovní poměr
B	pátý pracovní poměr
C	šestý pracovní poměr
D	dohoda o prac. čin. (třetí)
E	dohoda o prac. čin. (čtvrtá)
F	dohoda o prac. čin. (pátá)
G	dohoda o pracovní činnosti (šestá)
H	dohoda o pracovní činnosti (sedmá)
I	dohoda o pracovní činnosti (osmá)
J	dohoda o pracovní činnosti (devátá)
K	dohoda o pracovní činnosti (desátá)
T	určeno pouze pro vězeňskou službu
Z	student

Příloha 3 - Číselníky 2/4

OKRES

id	popis	id	popis
110	Praha 10	552	Chomutov
111	Praha 1	553	Jablonec nad Nisou
112	Praha 2	554	Liberec
113	Praha 3	555	Litoměřice
114	Praha 4	556	Louny
115	Praha 5	557	Most
116	Praha 6	558	Teplice
117	Praha 7	559	Ústí nad Labem
118	Praha 8	660	Havlíčkův Brod
119	Praha 9	661	Hradec Králové
121	Jihozápadní Město	662	Chrudim
122	Modřany	663	Jičín
123	Praha 23 - Jižní Město	664	Náchod
220	Benešov	665	Pardubice
221	Beroun	666	Rychnov nad Kněžnou
222	Kladno	667	Semily
223	Kolín	668	Svitavy
224	Kutná Hora	669	Trutnov
225	Mělník	670	Ústí nad Orlicí
226	Mladá Boleslav	771	Blansko
227	Nymburk	772	Brno - město
228	Praha - východ	773	Brno - venkov
229	Praha - západ	774	Břeclav
230	Příbram	775	Zlín
231	Rakovník	776	Hodonín
332	České Budějovice	777	Jihlava
333	Český Krumlov	778	Kroměříž
334	Jindřichův Hradec	779	Prostějov
335	Pelhřimov	780	Třebíč
336	Písek	781	Uherské Hradiště
337	Prachatice	782	Vyškov
338	Strakonice	783	Znojmo
339	Tábor	784	Žďár nad Sázavou
440	Domažlice	884	Jeseník
441	Cheb	885	Bruntál
442	Karlovy Vary	886	Frýdek - Místek
443	Klatovy	887	Karviná
444	Plzeň - město	888	Nový Jičín
445	Plzeň - jih	889	Olomouc
446	Plzeň - sever	890	Opava
447	Rokycany	891	Ostrava - město
448	Sokolov	892	Přerov
449	Tachov	893	Šumperk
550	Česká Lípa	894	Vsetín
551	Děčín		

Příloha 3 - Číselníky 3/4

STÁT 1/2

id	popis	id	popis
AF	Afghánistán	GH	Ghana
AL	Albánie	GI	Gibraltar
DZ	Alžírsko	GD	Grenada
AS	Americká Samoa	GL	Grónsko
VI	Americké Panenské ostrovy	GE	Gruzie
AD	Andorra	GP	Guadeloupe
AO	Angola	GU	Guam
AI	Anguilla	GT	Guatemala
AQ	Antarktida	GG	Guernsey
AG	Antigua a Barbuda	GN	Guinea
AR	Argentina	GW	Guinea-Bissau
AM	Arménie	GY	Guyana
AW	Aruba	HT	Haiti
AU	Austrálie	HM	Heardův ostrov a McDonaldovy ostrovy
AZ	Ázerbájdžán	HN	Honduras
BS	Bahamy	HK	Hongkong
BH	Bahrajn	CL	Chile
BD	Bangladéš	HR	Chorvatsko
BB	Barbados	IN	Indie
BE	Belgie	ID	Indonésie
BZ	Belize	IQ	Irák
BY	Bělorusko	IR	Írán
BJ	Benin	IE	Irsko
BM	Bermudy	IS	Island
BT	Bhútán	IT	Itálie
BO	Bolívie	IL	Izrael
BA	Bosna a Hercegovina	JM	Jamajka
BW	Botswana	JP	Japonsko
BV	Bouvetův ostrov	YE	Jemen
BR	Brazílie	JE	Jersey
IO	Britské indickooceánské území	ZA	Jihoafrická republika
VG	Britské Panenské ostrovy	GS	Jižní Georgie a Jižní Sandwichovy ostrovy
BN	Brunej Darussalam	JO	Jordánsko
BG	Bulharsko	YU	Jugoslávie
BF	Burkina Faso	KY	Kajmanské ostrovy
BI	Burundi	KH	Kambodža
XC	Ceuta	CM	Kamerun
CK	Cookovy ostrovy	CA	Kanada
TD	Čad	CV	Kapverdy
ME	Černá Hora	QA	Katar
CZ	Česká republika	KZ	Kazachstán
CN	Čína	KE	Keňa
DK	Dánsko	KI	Kiribati
DM	Dominika	CC	Kokosové ostrovy
DO	Dominikánská republika	CO	Kolumbie
DJ	Džibutsko	KM	Komory
EG	Egypt	CG	Kongo
EC	Ekvádor	CD	Kongo, demokratická republika
ER	Eritrea	KR	Korea
EE	Estonsko	KP	Korea, lidově demokratická republika
ET	Etiopie	CR	Kostarika
FO	Faerské ostrovy	CU	Kuba
FK	Falklandy	KW	Kuvajt
FJ	Fidži	CY	Kypr
PH	Filipíny	KG	Kyrgyzstán
FI	Finsko	LA	Laos
FX	France, Metropolitan	LS	Lesotho
FR	Francie	LB	Libanon
GF	Francouzská Guyana	LR	Libérie
TF	Francouzská jižní území	LY	Libye
PF	Francouzská Polynésie	LI	Lichtenštejnsko
GA	Gabon	LT	Litva
GM	Gambie	LV	Lotyšsko

Příloha 3 - Číselníky 4/4

STÁT 2/2

id	popis	id	popis
LU	Lucembursko	SV	Salvador
MO	Macao	WS	Samoa
MG	Madagaskar	SM	San Marino
HU	Maďarsko	SA	Saúdská Arábie
MK	Makedonie	SN	Senegal
MY	Malajsie	MP	Severní Mariany
MW	Malawi	SC	Seychely
MV	Maledivy	SL	Sierra Leone
ML	Mali	SG	Singapur
MT	Malta	SK	Slovensko
MA	Maroko	SI	Slovinsko
MH	Marshallovy ostrovy	SO	Somálsko
MQ	Martinik	AE	Spojené arabské emiráty
MU	Mauricius	UK	Spojené království
MR	Mauritánie	US	Spojené státy
YT	Mayotte	RS	Srbsko
XL	Melilla	CS	Srbsko a Černá Hora
UM	Menší odlehlé ostrovy USA	LK	Srí Lanka
MX	Mexiko	CF	Středoafrická republika
FM	Mikronésie	SD	Súdán
MD	Moldavsko	SR	Surinam
MC	Monako	SJ	Svalbard a ostrov Jan Mayen
MN	Mongolsko	SH	Svatá Helena
MS	Montserrat	LC	Svatá Lucie
MZ	Mosambik	KN	Svatý Kryštof a Nevis
MM	Myanmar	VA	Svatý stolec
NA	Namibie	ST	Svatý Tomáš
NR	Nauru	VC	Svatý Vincenc a Grenadiny
DE	Německo	SZ	Svazijsko
NP	Nepál	SY	Sýrie
	neuvedeno	SB	Šalamounovy ostrovy
NE	Niger	ES	Španělsko
NG	Nigérie	SE	Švédsko
NI	Nikaragua	CH	Švýcarsko
NU	Niue	TJ	Tádžikistán
AN	Nizozemské Antily	TZ	Tanzanie
NL	Nizozemsko	TH	Thajsko
NF	Norfolk	TW	Tchaj-wan
NO	Norsko	TG	Togo
NC	Nová Kaledonie	TK	Tokelau
NZ	Nový Zéland	TO	Tonga
PS	Okupované palestinské území	TT	Trinidad a Tobago
OM	Omán	TN	Tunisko
IM	Ostrov Man	TR	Turecko
PK	Pákistán	TM	Turkmenistán
PW	Palau	TC	Turks a Caicos
PA	Panama	TV	Tuvalu
PG	Papua Nová Guinea	UG	Uganda
PY	Paraguay	UA	Ukrajina
PE	Peru	UY	Uruguay
PN	Pitcairn	UZ	Uzbekistán
CI	Pobřeží slonoviny	CX	Vánoční ostrov
PL	Polsko	VU	Vanuatu
PR	Portoriko	VE	Venezuela
PT	Portugalsko	VN	Vietnam
AT	Rakousko	LR	Libérie
RE	Réunion	TL	Východní Timor
RO	Rumunsko	WF	Wallis a Futuna
RU	Rusko	ZM	Zambie
RW	Rwanda	EH	Západní Sahara
GR	Řecko	ZW	Zimbabwe
PM	Saint Pierre a Miquelon		

Příloha 4 - Struktura datové zprávy SUBMISSION_REQUEST

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>request</Qualifier>
            <Function>submit</Function>
            <CorrlationID/>
            <Transformation>XML</Transformation>
            <GatewayTest>1</GatewayTest>
            <GatewayTimestamp/>
        </MessageDetails>
        <SenderDetails>
            <IDAuthentication>
                <SenderID>st16557</SenderID>
                <Authentication>
                    <Method>clear</Method>
                    <Value>heslo</Value>
                </Authentication>
            </IDAuthentication>
        </SenderDetails>
    </Header>
    <GovTalkDetails>
        <Keys>
            <Key Type="vars">99200223</Key>
        </Keys>
    </GovTalkDetails>
    <Body>
        <Message version="1.1" xmlns="http://www.cssz.cz/XMLSchema/envelope">
          <Header>
                    <Signature xmlns:dt="urn:schemas-microsoft-com:datatypes"
                    dt:dt="bin.base64">MIIFygYJKoZIhvcNAQcCoIIFuzCCBbc...<Signature>
                    <Vendor productName="BP" version="1.0" />
          </Header>
                    <Body encrypted="yes" contentEncoding="raw" xmlns:dt="urn:schemas-microsoft-com:datatypes"
                    dt:dt="bin.base64">MIIHuAYJKoZIhvcNAQcD...</Body>
</Message>

    </Body>
</GovTalkMessage>
```

Příloha 5 - Struktura datové zprávy SUBMISSION_POLL

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>poll</Qualifier>
            <Function>submit</Function>
            <CorrlationID>EA0DF4F9DB194F9FBB103A58469A55BD</CorrlationID>
            <Transformation>XML</Transformation>
        </MessageDetails>
        <SenderDetails/>
    </Header>
    <GovTalkDetails>
        <Keys/>
    </GovTalkDetails>
    <Body/>
</GovTalkMessage>
```

Příloha 6 - Struktura datové zprávy DELETE_REQUEST

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>request</Qualifier>
            <Function>delete</Function>
            <CorrlationID>EA0DF4F9DB194F9FBB103A58469A55BD</CorrlationID>
            <Transformation>XML</Transformation>
        </MessageDetails>
        <SenderDetails/>
    </Header>
    <GovTalkDetails>
        <Keys/>
    </GovTalkDetails>
    <Body/>
</GovTalkMessage>
```

Příloha 7 - Struktura datové zprávy SUBMMISION_ACKNOWLEDGEMENT

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>acknowledgement</Qualifier>
            <Function>submit</Function>
            <TransactionID/>
            <CorrlationID>EA0DF4F9DB194F9FBB103A58469A55BD</CorrlationID>
            <ResponseEndPoint PollInterval="35">https://bezpecne.dev.gov.cz/poll</ResponseEndPoint >
            <GatewayTimestamp>2009-04-20T18:07:43.550</GatewayTimestamp>
        </MessageDetails>
        </SenderDetails>
    </Header>
    <GovTalkDetails>
        </Keys>
    </GovTalkDetails>
    <Body>
        <Signature version="1.0" xmlns="http://www.cssz.cz/XMLSchema/envelope">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            <TimeStamp>
              <date>20090420</date>
              <time>18:08:23</time>
            </TimeStamp>

                    <SignatureValue>MIIHuAYJKoZIhvcNAQcD...</SignatureValue>
        <Signature>
    </Body>
</GovTalkMessage>
```

Příloha 8 - Struktura datové zprávy SUBMISION_RESPONSE

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>response</Qualifier>
            <Function>submit</Function>
            <TransactionID/>
            <CorrlationID>EA0DF4F9DB194F9FBB103A58469A55BD</CorrlationID>
            <ResponseEndPoint PollInterval="30">https://bezpecne.dev.gov.cz/submission</ResponseEndPoint >
            <GatewayTimestamp>2009-04-20T18:07:43.550</GatewayTimestamp>
        </MessageDetails>
        <SenderDetails>
            <IDAuthentication>
                <SenderID>*****</SenderID>
                <Authentication>
                    <Method>clear</Method>
                    <Value>*****</Value>
                </Authentication>
            </IDAuthentication>
        </SenderDetails>
    </Header>
    <GovTalkDetails>
        <Keys>
            <Key Type="SpokeName" xmlns ="http://www.govtalk.gov.uk/CM/envelope">CSSZ_1_ORG</Key>
        </Keys>
    </GovTalkDetails>
    <Body Id=="0" >
        <Signature version="1.0" xmlns="http://www.cssz.cz/XMLSchema/envelope">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            <TimeStamp>
              <date>20090420</date>
              <time>18:08:23</time>
            </TimeStamp>
            <SignatureValue>MIIHuAYJKoZIhvcNAQcD...</SignatureValue>
        <Signature>
    </Body>
</GovTalkMessage>
```

Příloha 9 - Struktura datové zprávy DELETE_ACKNOWLEDGEMENT

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>acknowledgement</Qualifier>
            <Function>delete</Function>
            <TransactionID/>
            <CorrlationID>EA0DF4F9DB194F9FBB103A58469A55BD</CorrlationID>
            <ResponseEndPoint PollInterval="35">https://bezpecne.dev.gov.cz/poll</ResponseEndPoint >
            <GatewayTimestamp>2009-04-20T18:07:43.550</GatewayTimestamp>
        </MessageDetails>
        </SenderDetails>
    </Header>
    <GovTalkDetails>
        </Keys>
    </GovTalkDetails>
    <Body/>
</GovTalkMessage>
```

Příloha 10 - Struktura datové zprávy DELETE_RESPONSE

```
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
    <EnvelopeVersion>2.0</EnvelopeVersion>
    <Header>
        <MessageDetails>
            <Class>CSSZ_PRIHL</Class>
            <Qualifier>response</Qualifier>
            <Function>delete</Function>
            <TransactionID/>
            <CorrlationID>EA0DF4F9DB194F9FBB103A58469A55BD</CorrlationID>
            <ResponseEndPoint PollInterval="35">https://bezpecne.dev.gov.cz/submission</ResponseEndPoint >
            <GatewayTimestamp>2009-04-20T18:07:43.550</GatewayTimestamp>
        </MessageDetails>
        <SenderDetails/>
    </Header>
    <GovTalkDetails>
        <Keys/>
    </GovTalkDetails>
    <Body/>
</GovTalkMessage>
```

Příloha 11 - Email o úspěšním podání

Dobrý den,

děkujeme Vám za elektronicky zaslané podání.
Vaše podání přihlášek/odhlášek bylo na ČSSZ přijato.

Variabilní symbol podávající organizace: **99200223**
Identifikátor podání (PVS): 0CAAE854033C46A498836C8DC4CA4CD1
Identifikátor podání (ČSSZ): 3067F691A5754F86A5B4980FFEDB382B
Datum příchodu podání: 2009-04-20T20:40:50

Česká správa sociálního zabezpečení

Protokol o zpracování e-podání		Přihlášky/Odhlášky zaměstnanců (malých) organizací
Počet záznamů: 1 Počet logických chyb: 0		
8605251138		PRIHL -