Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Rozvoj služeb eGovernmentu

Antonín Černý

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Černý Antonín

Informatika

Název práce

Rozvoj služeb eGovernmentu

Anglický název

Development of eGovernment services

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku služeb eGovernmentu. Hlavním cílem práce je charakterizovat současný stav rozvoje a využití služeb eGovernmentu.
Dílčí cíle bakalářské práce jsou:
- charakteristika služeb eGovernmentu v ČR
- analýza eGovernmentu ve světě
- návrh na využití eVotingu v ČR

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Vlastní řešení je založeno na analýze podobných projektů v zahraničí, sběru informací o proveditelnosti v České republice a zhodnocení získaných podkladů. Na základě syntézy teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

Harmonogram zpracování

1) Příprava a studium odborných informačních zdrojů, upřesnění dílčích cílů práce a volba postupu řešení: 6/2014
2) Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2014 - 8/2014
3) Vypracování vlastního řešení, diskuze a zhodnocení výsledků: 9/2014 - 10/2014
4) Tvorba finálního dokumentu bakalářské práce: 11/2014 - 2/2015
5) Odevzdání bakalářské práce a teze: 3/2015

Rozsah textové části

30 - 40 stran

Klíčová slova

eGovernment, eVoting, elektronizace, veřejná správa, datové schránky, základní registry, Czech Point,

Doporučené zdroje informací

Štědroň B., Úvod do eGovernmentu v České republice: právní a technický průvodce, Praha: Úřad vlády České republiky, 2007, ISBN 978-80-87041-25-3

OECD e-Government Studies, e-Government for Better Government, Paříž: OECD Publishing, 2005, ISBN 92-64-01833-6

Mates P., Smejkal V., E-government v českém právu, Praha: Linde, 2006, ISBN 80-7201-614-8

on-line mateiály

Vedoucí práce

Jarolímek Jan, Ing., Ph.D.

Termín odevzdání

březen 2015

Elektronicky schváleno dne 31.10.2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11.11.2014

Ing. Martin Pelikán, Ph.D.

Děkan fakulty

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Rozvoj služeb eGovernmentu" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 16. 3. 2015 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu bakalářské práce Ing. Janu Jarolímkovi, Ph.D. za poskytnuté rady a pomoc při zpracování práce.

Rozvoj služeb eGovernmentu

Development of eGovernment services

Souhrn

Bakalářská práce se zabývá analýzou eGovernmentu, který má za úkol zvýšit efektivitu státní správy prostřednictvím její elektronizace. Jeho cílem je usnadnit občanům a firmám vzájemnou komunikaci se státními úřady. V teoretické části práce nejdříve charakterizuje eGovernment. Představuje symboly eGON a Klaudie, které reprezentují projekty eGovernmentu v České republice. Hlavní část rozebírá nejdůležitější projekty, které občané již využívají. Postupně jsou představeny projekty Czech POINT, datové schránky, základní registry, komunikační infrastruktura veřejné správy a elektronický podpis. Dále jsou vysvětleny bezpečnostní prvky elektronické komunikace. V závěrečné části jsou charakterizovány elektronické volby a jejich rozdělení.

Praktická část se zaměřuje na problematiku elektronických voleb. Nejprve jsou rozebrány zkušenosti se zaváděním eVoleb v zahraničí. Následuje analýza stavu v České republice a návrh možné podoby internetového hlasování po vzoru Estonska. Ve výsledku práce je pak provedeno zhodnocení současného a možného budoucího stavu elektronického hlasování.

Summary

Bachelor thesis deals with the analysis of eGovernment, which aims to increase government efficiency through its computerization. The aim of eGovernment is to facilitate citizens and businesses mutual communication with state authorities. The theoretical part characterizes eGovernment.The thesis represents symbols eGON and Claudia, representing eGovernment projects in the Czech Republic. The main part analyzes the most important projects that people already use. Gradually presents projects Czech POINT, data boxes, base registers, communications infrastructure of public administration and electronic signature. The following explains the safety features of electronic communication. In the final section outlines the electronic elections and their dividing.

The practical part focuses purely on the issue of electronic elections. The earliest work analyzes the experience with the introduction of e-voting abroad. Following analysis of the situation in the Czech Republic and the thesis proposes a possible form of Internet voting on the model of Estonia. As a result, the thesis evaluates current and possible future state of electronic voting.

Klíčová slova: eGovernment, elektronizace, veřejná správa, Czech POINT, datová schránka, elektronický podpis, šifrování, elektronické volby, internetové hlasování

Keywords: eGovernment, computerization, public administration, Czech POINT, data box, electronic signature, encryption, electronic voting, Internet voting

Obsah

1 Úvod 9
2 Cíl práce a metodika 11
3 Přehled řešené problematiky 12
3.1 Definice a principy eGovernmentu 12
3.2 Vývoj 14
3.3 eGovernment v české legislativě 16
3.4 Symboly eGovernmentu 17
3.4.1 eGON 17
3.4.2 Klaudie 18
3.5 Projekty eGovernmentu 19
3.5.1 Czech POINT 19
3.5.2 Datové schránky 24
3.5.3 Základní registry 26
3.5.4 KIVS 28
3.5.5 Elektronický podpis 29
3.6 Bezpečnostní prvky elektronické komunikace 30
3.6.1 Šifrování 31
3.6.2 Hashování 31
3.6.3 Certifikace 32
3.6.4 Autentizace 32
3.7 Elektronické volby 32
3.7.1 Definice elektronických voleb 32
3.7.2 Nevzdálené elektronické hlasování 33
3.7.3 Vzdálené elektronické hlasování 34
3.7.4 Historie eVoleb v České republice 35
4 Vlastní práce 37
4.1 Elektronické volby ve světě 37
4.1.1 Estonsko 37
4.1.2 Švýcarsko 41
4.1.3 USA 41
4.1.4 Ostatní státy 42
4.2 Elektronické volby v České republice 42
4.2.1 Připravenost České republiky na eVolby 42
4.2.2 Požadavky na elektronický volební systém 44
4.2.3 Návrh eVoleb v České republice 45
5 Výsledky a diskuse 49
6 Závěr 53
7 Seznam použitých zdrojů 55
8 Přílohy 59
8.1 Seznam obrázků 59
8.2 Seznam grafů 59
8.3 Seznam tabulek 59

1 Úvod

Informační a komunikační technologie jsou dnes běžnou součástí každodenního života. Díky svému dynamickému rozvoji se dostaly do všech oblastní vyspělé společnosti. Umožňují jednoduchou komunikaci, zjednodušují práci, šetří náš čas i peníze. Jejich vliv na život lidí narostl do té míry, že je dnešní společnost nazývána informační společností.

Informace patří v současnosti k nejcennějším komoditám. Na jejich jednoduchém šíření se výraznou měrou podílí internet. To je celosvětový systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Byl vyvinut v 60. letech minulého století v armádní instituci Advanced Research Project Agency v USA. Rozmachu se však dočkal až počátkem 90. let. V té době začíná výrazně pronikat do domácností i podniků. Dnes se stává počítač a připojení k internetu stává běžným standardem domácností. Ve většině případů má dnes každý své zařízení umožňující využívat internet, ať se jedná o osobní počítač, notebook, moderní mobilní telefony či jiná vyspělá zařízení.

Jedním ze základních předpokladů pro správné fungování informačních systémů je schopnost uživatelů tyto systémy používat. Počítačová gramotnost je naštěstí dnes ve vyspělém světě je považována za jednu ze základních dovedností.

Rozvoj informačních a komunikačních technologií postupně zasáhl i do veřejné správy. V souvislosti s tímto rozvojem se objevil pojem eGovernment. Ten lze charakterizovat jako elektronizaci veřejné správy. Smyslem eGovernmentu je umožnit snadnou a bezpečnou komunikaci mezi občanem a úřady státní správy. Dále by měl zajistit zvýšení efektivity a transparentnosti veřejné správy. Cílem je tak ušetřit občanům čas, zajistit jim dostatečný komfort a značně uspořit finanční prostředky. Pomáhá naplňovat vizi, že veřejná správa je primárně pojata jako služba občanům.

Se zaváděním eGovernmentu se vyskytují nemalé problémy. Prvním logickým argumentem proti zavádění eGovernmentuje finanční nákladnost, zejména při implementaci nových informačních systémů. Oproti soukromé sféře má veřejná správa tu nevýhodu, že pro její postupy je vyžadován legislativní rámec a proces elektronizace je tak mnohem zdlouhavější. Důležitou roli zaujímají také zaměstnanci veřejné správy, kteří se s novými systémy musí ztotožnit a naplno využívat jejich možnosti.

Význam eGovernmentu v České republice vzrostl zejména v posledních deseti letech. K jeho rozvoji v České republice nemalou měrou přispěla strategie Evropské unie, která projekty eGovernmentu podporuje prostřednictvím operačních programů a pomáhá tak s nákladným financováním.

S vývojem informační gramotnosti postupně stoupají nároky občanů vůči elektronizaci veřejné správy. Část z nich by ráda zavedla i elektronické volby, přesněji možnost elektronického hlasování. To se rozděluje na dva typy. Nevzdálené elektronické hlasování je takové, při kterém se volič musí dostavit do volební místnosti a tam odevzdat hlas elektronicky prostřednictvím terminálu. Zajímavější je ovšem vzdálené elektronické hlasování. To umožňuje hlasovat odkudkoliv, kde to technologie dovolí, například z počítače z domova. Česká republika má tu výhodu, že může čerpat ze zkušenosti jiných států, které už zkušenosti s elektronickým hlasováním mají.

2 Cíl práce a metodika

Bakalářská práce se zaměřuje na přehled eGovernmentu v České republice se zaměřením na elektronické volby.

Hlavním cílem práce je charakterizovat současný stav rozvoje a využití služeb eGovernmentu. Dílčím cílem pak je charakteristika některých konkrétních služeb a projektů, které jsou v České republice nyní k dispozici. Vlastní práce si klade za cíl analyzovat stav eGovernmentu ve světě z pohledu elektronických voleb. Na ní navazuje poslední z cílů, kterým je návrh na využití elektronických voleb v České republice a jeho zhodnocení.

Bakalářská práce je rozdělena na dvě části. První část se věnuje přehledu řešené problematiky. Druhá část je zaměřena na problematiku elektronických voleb.

Metodika první části je založena na studiu a analýze odborných informačních zdrojů, které se oblasti eGovernmentu věnují. Při studiu byly využity zdroje v tištěné i elektronické podobě. Nejprve se práce zabývá vymezení pojmu eGovernment a popisuje jeho vývoj v České republice až do současnosti. Další část se věnuje české legislativě v souvislosti s projekty eGovermentu. Dále představuje dva symboly českého eGoverment, kterými jsou eGON a Klaudie. Postupně objasňuje pojmy Czech POINT, datová schránka, základní registry, komunikační infrastruktura veřejné správy a elektronický podpis. Ke znázornění využití těchto projektů jsou využity statistická data, která jsou zpracovány ve formě grafů a tabulek. Dále se práce zabývá bezpečnostními prvky elektronické komunikace. V závěrečné části je charakterizována problematika elektronických voleb a jejich rozdělení.

Vlastní řešení je založeno na analýze podobných projektů v zahraničí, sběru informací o proveditelnosti v České republice a zhodnocení získaných podkladů. Práce uvádí zkušenosti několika států s tímto projektem. V další části je obsažen návrh na zavedení elektronických voleb v České republice a zhodnocení tohoto návrhu pomocí SWOT analýzy.

Na základě syntézy teoretických poznatků a zjištěných výsledků v analytické části práce budou přehledně formulovány závěry bakalářské práce.

3 Přehled řešené problematiky

3.1 Definice a principy eGovernmentu

eGovernment se v České republice vyskytuje již více než deset let. Přesto se stále vyskytuje značná množina lidí, kteří si pod tímto pojmem nedovedou nic představit.

Počátky eGovernmentu se datují k roku 1999 ve Velké Británii, odkud se postupně začal rozšiřovat do dalších států vyspělého světa.

Anglický výraz eGovernment je zkratkou slov electronic government, což lze přeložit jako elektronické vládnutí. Výraz eGovernment však byl přejat do všech ostatních jazyků a je používán jak v odborných kruzích, tak i v běžné řeči.

Nejstručněji lze pojem eGovernment vysvětlit jako elektronizaci veřejné správy. Pro jeho odbornější vymezení existuje velká řada definic.

OECD ho stručně definuje jako využití informačních a komunikačních technologií, a především internetu, jako prostředku k dosažení lepší vlády. [1]

„eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb.“ [2]

Definice Ministerstva vnitra České republiky říká: „eGovernment představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy.“

eGovernment podle OSN je „Trvalá povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a efektivních služeb, informací a znalostí. Praktická realizace toho nejlepšího, co může veřejný správa nabídnout.“

Hlavním cílem eGovernmentu je zvýšit efektivitu státního aparátu a usnadnit vzájemnou komunikaci nejen mezi veřejnou správou a občany, ale i v rámci samotné veřejné správy. Efektivitou je míněno zajištění rychlejšího, levnějšího a spolehlivějšího poskytování služeb státní správy. Měl by také pro občany zjednodušit jejich jednání s úřady a zajistit jim určitý komfort. K těmto cílům je zapotřebí uzpůsobit státní správu k využití informačních a komunikačních technologií, tedy elektronizace veškerých agend ve správě daných úřadů. To umožňuje lepší služby nejen pro fyzické i právnické osoby,

ale také pro úředníky, kteří pomocí ICT ušetří čas, který by jinak strávili prací s papírovými podklady.

„Cílem je rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům (občanům).“ [3]

Elektronizace veřejné správy má ovšem i své problémy. Prvním z nich je v legislativě, která je velmi komplikovaná, obsáhlá a poměrně nestálá. Druhým úskalím jsou nároky na počítačovou gramotnost veřejnosti. Značným problémem jsou finanční prostředky, které jsou potřeba zejména při zavádění nových systémů.

V České republice je v současné době řízením rozvoje eGovernmentu v gesci Ministerstva vnitra. V rámci tohoto resortu je v oblasti elektronizace zmiňováno heslo "Obíhat mají data, ne lidé".

Ivan Langer, ministr vnitra v letech 2006-2009, definoval sedm principů moderního úřadu, který měl být hlavním cílem českého eGovernmentu. [4]

1. Jednou a dost. To znamená, že údaje, které již jednou fyzické či právnické osoby poskytly jednomu orgánu veřejné správy, nebude jiný orgán znovu opakovaně vyžadovat.
2. Minimum informací. S využitím principu jednou a dost se při vyřizování agend využívá pouze omezený počet informací, které jsou potřebné, a které stát dosud nezískal.
3. Informace kdekoliv. Na základě platnosti 1. principu musí platit, že většinu agend musí být s občanem schopen vyřídit úředník na libovolném místě veřejné správy.
4. Informace samy putují. To znamená, že systém sám umí najít a ověřit potřebné informace a sám je umí aktualizovat po oznámení změny.
5. Informace kdykoliv. Platí, že systém umožní komunikaci osobně na úřadu každý den nebo elektronicky v každou denní či noční dobu.
6. Okamžitá kontrola. To znamená, že systém dokáže poskytnout žadateli, stěžovateli atd. okamžitou informaci o stavu vyřizování jeho podání.
7. Důsledná ochrana. Získané informace budou důsledně, pod hrozbou tvrdých sankcí, chráněny proti úniku a jakémukoliv jinému využití než umožňují právní předpisy.

3.2 Vývoj

Od počátku devadesátých let byla snaha jednotlivých úřadů o využití informačních systémů, která však z různých důvodů byla velmi pomalá. Neexistovala státní ucelená koncepce, a tak jednotlivé systémy byly rozdílné a často nekompatibilní. První pokus o zřízení instituce, mající za úkol naplánovat a vybudovat Státní informační systém nastal 1. listopadu 1996. Vznikl Úřad pro státní informační systém, který převzal kompetence v oblasti budování státního informačního systému od bývalého Ministerstva hospodářství ČR a Úřadu vlády ČR. První dokument, který úřad vytvořil, se nazýval "Informační politika ČR: základy strategie". [5]

V roce 1998 byla jmenována Rada pro státní informační politiku jako konzultativní orgán pro vládu ohledně otázek informační společnosti. Ta se podílela na strategie „Státní informační politika – cesta k informační společnosti“. O rok později vláda přijala Koncepci budování informačních systémů veřejné správy, která původní strategii rozšiřovala.

V roce 1999 byla otevřena možnost podat žádost o různé informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím prostřednictvím elektronické pošty.

V roce 2000 vláda přijímá Akční plán pro realizaci státní informační politiky, který určuje cíle pro období 2000-2002, a představuje tři rámcové programy k jejich dosažení. Cílem je "vybudovat a rozvíjet informační společnost a tím vytvořit předpoklady zejména pro zvýšení kvality života jednotlivých občanů, zefektivnění státní správy a samosprávy a zkvalitnění podpory rozvoje podnikání." Rámcové programy jsou informační gramotnost, elektronický obchod a elektronická veřejná správa [6]

V lednu 2003 bylo založeno ministerstvo informatiky. To bylo ústředním orgánem státní správy pro informační a komunikační technologie, telekomunikace a poštovní služby, a také koordinovalo také rozvoj českého eGovernmentu. [7]

V roce 2004, v souvislosti se vstupem České republiky do Evropské unie, vláda přijala novou strategii, která vycházela z plánu Evropské unie s názvem eEurope 2005. Jednalo se o Státní informační a komunikační politiku, která vešla v podvědomí jako e-Česko 2006.

Od roku 2005 mají veřejné instituce povinnost provozovat elektronické podatelny, které zajišťují bezpečné odesílání a přijímání datových zpráv.

V červenci 2006 je do provozu zaveden elektronický podpis. V tomto roce je déle spuštěn Daňový portál pro veřejnost či e-Invoices umožňující elektronickou fakturaci.

Od roku 2007 je vedením v oblasti eGovernmentu na místo ministerstva informatiky ministerstvo vnitra. Usnesením vlády č. 293 z 28. června 2007 je ustanovena Rada vlády pro konkurenceschopnost a informační společnost, která se stala odborným poradním orgánem vlády. [8]

11. července 2007 přijímá vláda svým usnesením novou strategii Smart Administration pro roky 2007-2015. Efektivní veřejná správa a přátelské veřejné služby (Smart Administration) je vládní strategie. Jejím cílem je zajistit koordinovaný a efektivní způsob zlepšování veřejné správy a veřejných služeb s využitím prostředků ze Strukturálních fondů v programovém období 2007-2013. Základním cílem strategie bylo transformovat a zjednodušit postupy používané ve veřejné správě i proto, aby mohly využívat moderních komunikačních a informačních technologií.

Obrázek č. 1 – Hexagon veřejné správy

Zdroj: www.smartadministration.cz

Strategie Smart Administration hledí na veřejnou správu jako na hexagon, zobrazený na obrázku č. 1. Jeho jednotlivé vrcholy symbolizují prvky veřejné správy, klíčové pro její efektivitu. [9]

V lednu 2008 byl zahájen ostrý provoz projektu Czech POINT. Od 1. října pak byla spuštěna služba eJustice, která měla za úkol usnadnit přístup k informacím týkající se soudního řízení. Ve stejném roce byl schválen zákon o elektronických úkonech a autorizované konverzi dokumentů, jinak nazývaný eGovernment Act či zákon o eGovernmentu.

V roce 2009 ministr vnitra a generální ředitel České pošty podepsali smlouvu o provozování informačního systému datových schránek.

Od července 2011 měl být zahájen ostrý provoz základních registrů, který byl nakonec o rok odložen na červenec 2012. V lednu roku 2012 se začaly vydávat nové občanské průkazy se strojově čitelnými údaji a možností zavedené kontaktního elektronického čipu.

3.3 eGovernment v české legislativě

Rozvoj eGovernmentu je vždy závislý na legislativě. Ta určuje nové postupy a umožňuje zavádět nové projekty. V České republice bylo přijato mnoho zákonů, které upravují problematiku elektronizace veřejní správy. [10]

- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 101/2000 Sb., o ochraně osobních údajů.
- Zákon č. 227/2000 Sb., o elektronickém podpisu
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě.
- Zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů.
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 111/2009 Sb., o základních registrech.

Kromě výše uvedených zákonů upravuje problematiku eGovernmentu řada vyhlášek. Mezi nejpodstatnější patří:

- Vyhláška č. 496/2004 Sb., o elektronických podatelnách.
- Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů.
- Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního
- systému datových schránek
- Vyhláška č. 364/2009 Sb., o seznamu obecních úřadů a zastupitelských úřadů

3.4 Symboly eGovernmentu

3.4.1 eGON

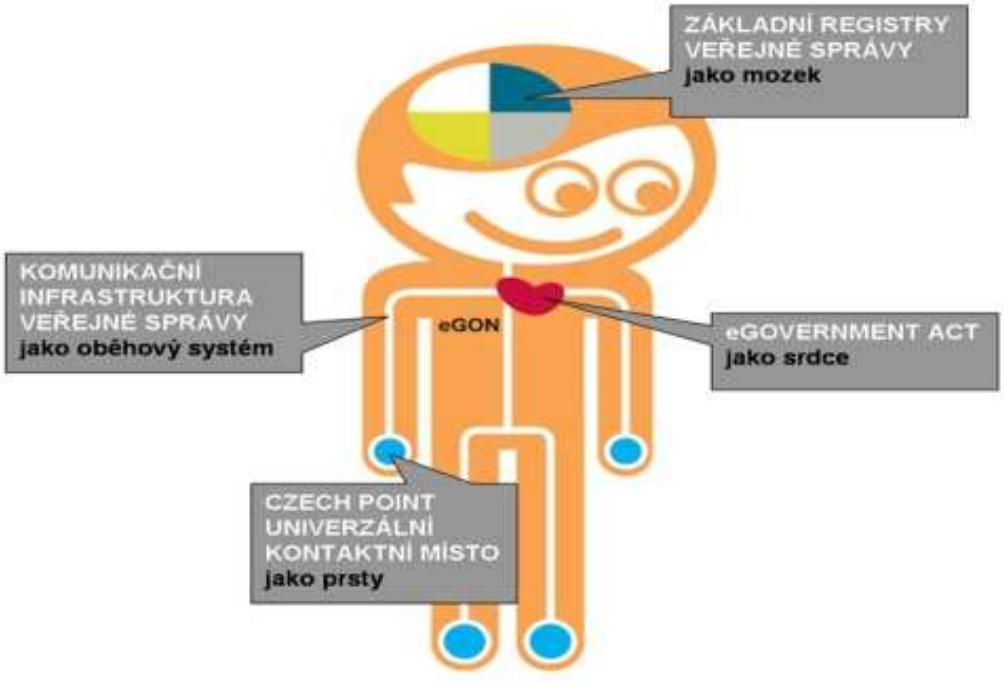
Panáček eGON je v přeneseném významu živý organismus, ve kterém vše souvisí se vším a fungování jednotlivých částí se navzájem podmiňuje. [11]

„Vzali jsme si za vzor živý organizmus, ve kterém vše obdivuhodně funguje. Prsty ucítí podnět, vyšlou signál do mozku, ten informaci vyhodnotí, správný orgán rozhodne a zpětně informuje prsty o tom, co mají dělat! Informace letí přímo, bez křižovatek, slepých cest, zbytečných průtahů.“ [12]

eGON byl představen v roce 2006 tehdejším ministrem vnitra Ivanem Langerem jako symbol českého eGovernmentu, moderního, přátelského a efektivního úřadu. eGON má být, stejně jako eGovernment, vstřícný, jednoduchý a funkční. [13]

Představuje komplexní projekt elektronizace veřejné správy, jehož hlavním cílem je usnadnění života občanům a zvýšení efektivity veřejné správy díky důmyslnému využití informačních technologií. [14]

Obrázek č. 2 – eGON



Zdroj: www.lanskroun.eu

Jak je vidět na obrázku č. 2, existenci a životní funkce eGONa zajišťují čtyři části. Srdce představuje zákon o eGovernmentu, neboli zákon o elektronických úkonech a autorizované konverzi č.300/2008 Sb. Mozek reprezentuje základní registry veřejné správy. Síť kontaktních míst Czech POINT je zobrazena jako eGONovy prsty. Bezpečný přenos dat zajišťuje Komunikační infrastruktura veřejné správy znázorněna jako oběhová soustava. [11]

3.4.2 Klaudie

Nový symbol elektronizace státní správy představili zástupci Ministerstva vnitra během 14. ročníku konference Internet ve státní správě a samosprávě v Hradci Králové. Klaudie, symbolizující prostředky cloud computingu, má zajistit, aby byly ICT projekty nejen efektivnější a levnější, ale aby také umožnily přechod od současného stavu blížícího se správě majetku k modelu poskytování a odebírání služeb. [14]

Cloud computing je sdílení hardwarových i softwarových prostředků pomocí sítě.[16]

Při přechodu na princip cloud computing se předpokládá efektivnější využití zdrojů, flexibilní využívání kapacit dle aktuální potřeby či snazší sdílení, zvyšování a snižování výkonu více systémy atd. Technologicky plánovalo ministerstvo směřovat vytvoření sdíleného flexibilního prostředí s dynamicky přidělovanými zdroji. To vše povede ke snížení nákladů na provoz informačních systémů státní správy. Při prezentaci projektu Klaudie tehdejší ministr vnitra Radek John uvedl: „Realizace i následný provoz všech projektů musí být ekonomicky uskutečnitelné. Nemůžeme si dovolit drahé a zbytečné hračky. Proto musí být smyslem projektů účelnost a užitečnost.“[14]

Srdcem Klaudie je nová verze „Centrálního místa služeb“ nazvaná CMS 2.0. Zajišťuje bezpečné a spolehlivé propojení sítí orgánů veřejné moci z pevné lokality přes přístupové body CMS (centrum/kraj/okres). CMS 2.0 tak slouží jako hlavní propojovací místo pro všechny základní eGON služby a definuje společné standardy, a to jak komunikační a bezpečnostní, tak i standardy poskytovaných služeb a jejich rozhraní.

3.5 Projekty eGovernmentu

3.5.1 Czech POINT

Czech POINT je zkratka pro Český Podací Ověřovací Informační Národní Terminál. V současné době je to nejúspěšnější projekt v rámci českého eGovernmentu. Hlavním smyslem projektu je maximálně zefektivnit občanům služby státní správy v rámci hesla „Nemají obíhat občané, ale data“.

„Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho universálního místa, kde je možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. Jde tedy o maximální využití údajů ve vlastnictví státu tak, aby byly minimalizovány požadavky na občany.“[16]

Czech POINT značně snižuje byrokracii při komunikaci s úřady. Před jeho zavedením nebylo neobvyklé, že kvůli jedné záležitosti bylo nutno navštívit více úřadů. Oproti tomu Czech POINT umožňuje občanům komunikovat se státní správou prostřednictvím jediného kontaktního místa.

Czech POINT je první služba v rámci projektu eGON, která byla v České republice zavedena. Na základě zkušeností z pilotního projektu, který běžel od března 2007, byl od ledna 2008 zahájen ostrý provoz. Postupem času se zvyšoval nejen počet poboček, ale také portfolio služeb, které Czech POINT nabízí. Významný nárůst služeb byl zaznamenán především v souvislosti se zavedením datových schránek a autorizované konverze dokumentů.

Obrázek č. 3 – logo Czech POINT

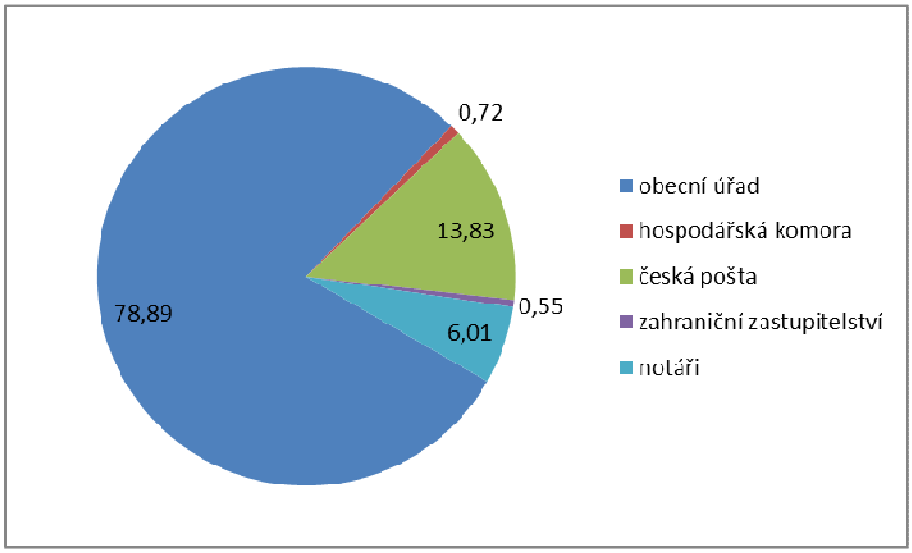
Zdroj: www.czechpoint.cz

Každé kontaktní místo je označeno logem projektu, které je zobrazeno na obrázku č. 1. „Logo Czech POINT symbolizuje blízké spojení či kontakt. Spojení, které je elegantní, čisté. A jednoduché. Jsme v kontaktu a to nám zjednodušuje život. Logo Czech POINT zpodobňuje také dalekohled či brýle, tedy optiku, která přibližuje, která přináší detailní pohled. Dívám se zblízka, a proto mám dobrý přehled.“[17]

Kontaktní místa veřejné správy jsou uvedeny v zákoně č. 365/2000 Sb., §8a odstavec 2. Kontaktními místy veřejné správy dle tohoto zákona mohou být [10]:

a) notáři
b) krajské úřady
c) matriční úřady
d) obecní úřady, úřady městských částí nebo městských obvodů územně členěných statutárních měst a úřady městských částí hlavního města Prahy, jejichž seznam stanoví prováděcí právní předpis
e) zastupitelské úřady stanovené prováděcím právním předpisem
f) držitel poštovní licence a Hospodářská komora České republiky
g) banka, které byla ministerstvem udělena autorizace k výkonu působnosti kontaktního místa veřejné správy

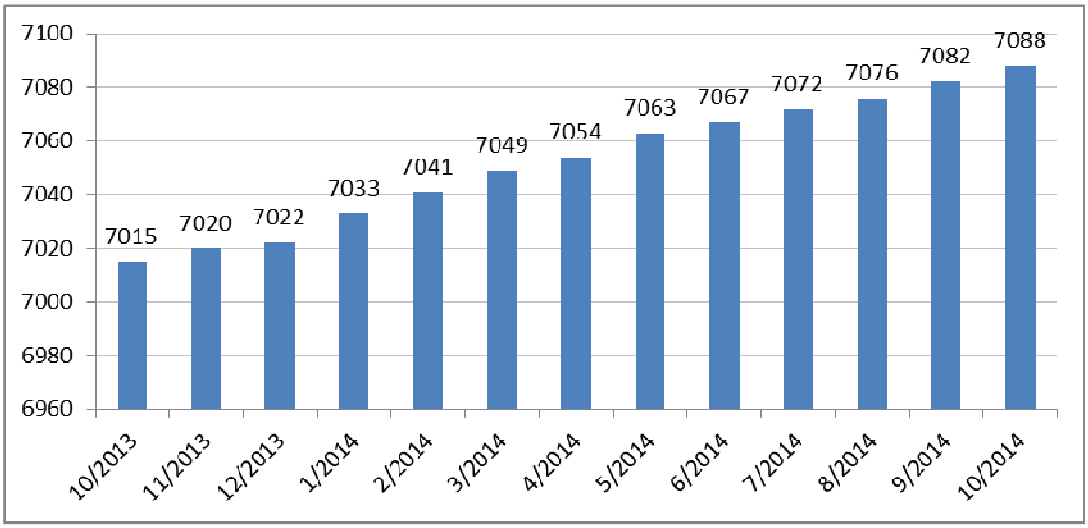
Graf č. 1 – struktura kontaktních míst



Zdroj: vlastní dle statistik Czech POINT

Z uvedeného grafu č. 1 je vidět, že bezkonkurenčně nejvíce pracovišť Czech POINTu je na obecních, městských a krajských úřadech, které zaujímají tři čtvrtiny všech poboček. Významnou úlohu zastávají také pobočky České pošty.

Graf č. 2 – vývoj počtu kontaktních míst



Zdroj: vlastní dle statistik Czech POINT

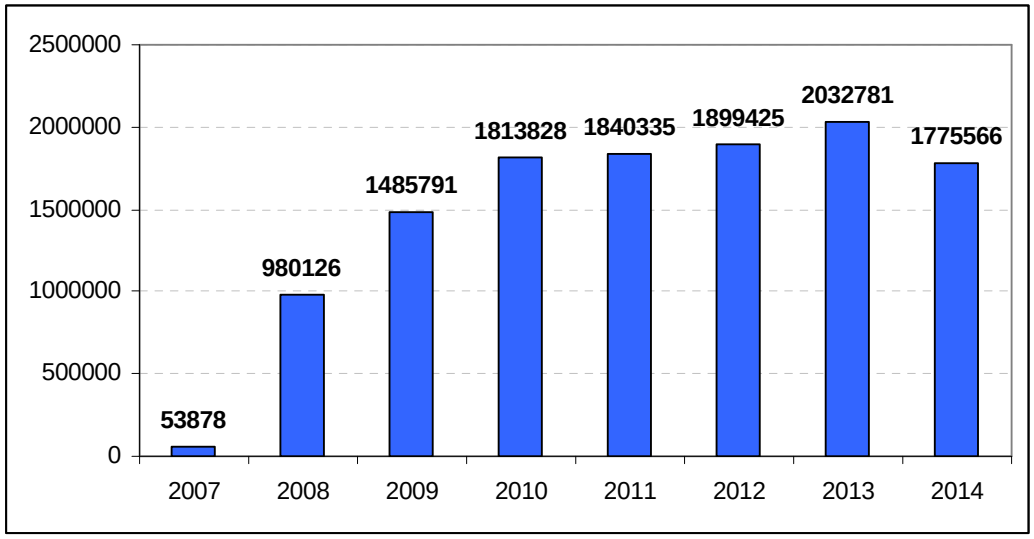
Ke dnu dni 1. 11. 2014 bylo evidováno 7088 kontaktních míst Czech POINT. Jak je vidět na grafu č. 2, počet kontaktních míst neustále stoupá, v průměru o 6 nových poboček každý měsíc. Počet nových pracovišť stoupá především na pobočkách České pošty.

Oproti počátkům projektu, kdy byly zpřístupněny výpisy ze tří veřejných registrů, v současné době poskytuje Czech POINT již velké množství služeb, které se i v budoucnu bude rozvíjet. Již dnes Czech POINT poskytuje:

- Výpis z Katastru nemovitostí
- Výpis z Obchodního rejstříku
- Výpis z Živnostenského rejstříku
- Výpis z Rejstříku trestů
- Výpis z Rejstříku trestů právnické osoby
- Přijetí podání podle živnostenského zákona (§ 72)
- Žádost o výpis nebo opis z Rejstříku trestů podle zákona č. 124/2008 Sb
- Výpis z bodového hodnocení řidiče

- Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů
- Podání do registru účastníků provozu modulu autovraků ISOH
- Výpis z insolvenčního rejstříku
- Datové schránky
- Autorizovaná konverze dokumentů
- Centrální úložiště ověřovacích doložek
- Úschovna systému Czech POINT
- CzechPOINT@office
- Základní registry
- Výpis z Veřejných rejstříků

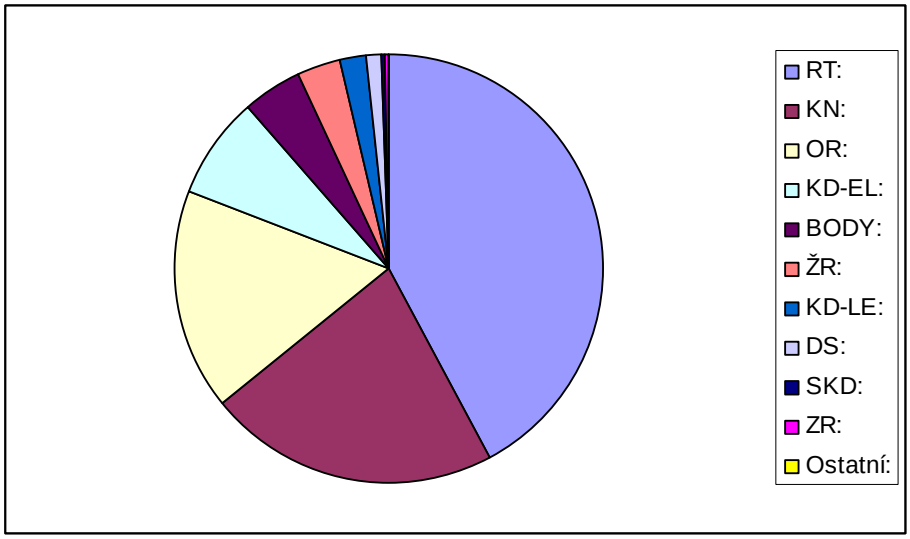
Graf č. 3 – vývoj počtu výstupů



Zdroj: vlastní dle statistik Czech POINT

Graf č. 3 ukazuje počet vydaných výstupů od roku 2007 do října roku 2014. Podle počtu výstupů je vidět, že projekt Czech POINT se těší u občanů velké oblibě, kdy roční počet výstupů se pohybuje kolem 200 tisíc. Dle grafu č. 4 je možné vidět, že největší zájem je o výpis z rejstříku trestů, jehož počet dosahuje přes 40% všech výstupů. Za ním s odstupem následují výpis z katastru nemovitostí a výpis z obchodního rejstříku.

Graf č. 4 – struktura vydaných výpisů dle kategorií



Zdroj: vlastní dle statistik Czech POINT

Rozhraní CzechPOINT@office je vytvořeno pro potřeby samotného úřadu. Jeho obsahem jsou agendy, které vykonávají úřady a orgány veřejné moci pro výkon své působnosti. V současnosti ke stávajícím službám CzechPOINT@office patří: výpis a opis z rejstříku trestů z moci úřední, autorizovaná konverze z moci úřední, agendy matriky, agendy ohlašovny a agendy soudů.[18]

„V konečné fázi projektu by občan mohl své záležitosti vyřizovat i z domova prostřednictvím internetu.“[19]

To je dnes částečně umožněno pomocí služby Czech POINT E-SHOP. Tato služba umožňuje elektronicky objednat vybrané výpisy z některých rejstříku veřejné správy online. Výpisy jsou pak na dobírku doručeny do tří pracovních dnů. [20]

Dne 8. 10. 2012 ministerstvo vnitra spustilo novou službu CzechPOINT@home neboli internetové kontaktní místo. Firmy, podnikatelé i občané, kteří dávají přednost elektronické komunikaci, tak mají možnost získat výpis z řady rejstříků informačních systémů veřejné správy v elektronické podobě, aniž by museli navštívit Czech POINT. Pro využití služby je však nutná aktivní datová schránka, do které bude výpis doručen zdarma. CzechPOINT@home nabízí elektronické výpisy z obchodního rejstříku,

z insolvenčního rejstříku, z rejstříku trestů právnických osob, z živnostenského rejstříku a ze seznamu kvalifikovaných dodavatelů. [21]

3.5.2 Datové schránky

Informační systém datových schránek je informačním systémem veřejné správy ve smyslu zákona 365/2000 Sb. Je určen k doručování dokumentů mezi orgány veřejné moci navzájem (povinně), mezi orgány veřejné moci a právnickými osobami, orgány veřejné moci a podnikajícími fyzickými osobami či fyzickými osobami. Je určován k provádění úkonů od právnických osob, podnikajících fyzických osob nebo fyzických osob směrem k orgánům veřejné moci. [22]

Datová schránka je elektronickým úložištěm, tedy datovým prostorem, který je vyhrazen právě pro orgán veřejné moci nebo právnickou osobu nebo podnikající fyzickou osobu nebo pro fyzickou osobu, kam jsou orgány veřejné moci doručovány datové zprávy, kde jsou prováděny úkony vůči orgánům veřejné moci. [22]

Datové schránky jsou určeny pro bezpečnou komunikaci orgánů veřejné moci s občany. Fungují na obdobném principu jako emailová komunikace, avšak ve srovnání s ní datové schránky představují bezpečnější formu komunikace. [2]

Zákon o elektronických úkonech a autorizované konverzi dokumentů „zrovnoprávňuje papírovou a elektronickou verzi zasílaného dokumentu“.

„Pomocí datových schránek je možné zasílat dokumenty v elektronické podobě orgánům veřejné moci a také je takto od nich přijímat… právnickým osobám jsou datové schránky zřízeny automaticky, všem ostatním na základě jejich žádosti“. [22]

Dle zákona datové schránky zřizuje a spravuje Ministerstvo vnitra České republiky. O provoz informačního systému datových schránek se stará držitel poštovní licence. Financování provozu datových schránek je zajištěno ze státního rozpočtu.

Přihlášení do datové schránky je umožněno na základě přístupových údajů, které jsou definovány vyhláškou č. 194/2009. Přístupové údaje jsou tvořeny uživatelským jménem a bezpečnostním heslem. Maximální velikost datové zprávy dodávané do datové schránky omezuje vyhláška hranicí 10 MB. Vyhláška také určuje, které formáty datové zprávy jsou přípustné, a jejich seznam je obsažen v příloze 3 dané vyhlášky. Nejvhodnějším formátem je PDF/A, který je definován ve standardech ISO.

Vlastnosti doručení datových schránek jsou[23]:

- závaznost – doručení do datové schránky má stejnou právní váhu jako do vlastních rukou
- garantované doručení – v okamžiku odeslání je odesilatel vyrozuměn o tom, jestli schránka existuje, je znepřístupněna, nebo zrušena. Za čas doručení je považován okamžik přihlášení příjemce do datové schránky.
- fikce doručení – nepřihlásí-li se příjemce do 10i dnů od odeslání datové zprávy, je tato zpráva považována za doručenou
- pomíjivost – zprávy jsou po 90 dnech od odeslání smazány, pokud si přeje příjemce další archivaci, lze provést autorizovanou konverzi na nejbližší pobočce Czech POINT nebo objednáním placené služby Datový Trezor

Rozlišují se čtyři typy datových schránek:

- Datová schránka fyzické osoby
- Datová schránka podnikající fyzické osoby
- Datová schránka právnické osoby
- Datová schránka orgánu veřejné moci

Schránka je tedy dostupná pro každého a zřízení datové schránky je bezplatné. Některé subjekty však musí datovou schránku využívat povinně. Jedná se o orgány veřejné moci, právnické osoby zřízené ze zákona a právnické osoby zapsané v Obchodním rejstříku. Ostatní právnické osoby, fyzické osoby či podnikající fyzické osoby mohou schránku získat dobrovolně a i po jejím zřízení mohou s orgány veřejné moci komunikovat písemnou korespondencí.[24]

Datová schránka je přístupná prostřednictvím portálu, jehož účelem je [25]:

- nabídnout plnohodnotný uživatelský portál pro veškeré informace a služby datových schránek spolu s možností přihlášení do datových schránek,
- vytvořit místo, kde se budou nalézat inteligentní elektronické formuláře a díky nim bude možné přes datovou schránku je úřadům odesílat. (tímto by měl nahradit transakční část Portálu veřejné správy),
- zveřejňovat věstníky ústředních správních orgánů i dalších subjektů dle § 4, odst. 2, písm. h a § 5, odst. 3 zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

Zákon o elektronických úkonech a autorizované konverzi dokumentů vstoupil v účinnost 1. 7. 2009, odkdy byla možnost využívat datové schránky. Ostrý provoz ale začal až 1. 11. 2009. Od 1. 1. 2010 je možné dodávání dokumentů fyzických i právnických osob mezi sebou. To je podmíněno žádostí soukromé osoby o zpřístupnění své schránky pro zprávy od jiných soukromých osob.

S datovými schránkami úzce souvisí autorizovaná konverze dokumentů. Konverzí se dle zákona rozumí:

a) úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky
b) úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky

Dokument, který provedením konverze vznikl, má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl. [10]

Konverze dokumentů se také dělí na[26]:

- Autorizovaná konverze na žádost - slouží pro širokou veřejnost ke konvertování nejrůznějších dokumentů. Autorizovanou konverzi na žádost provádějí všechna kontaktní místa veřejné správy – Czech POINT.
- Autorizovaná konverze z moci úřední - slouží pro vnitřní potřebu úřadu. Zajišťuje převedení dokumentu z listinné podoby do elektronické a naopak, tentokráte dokumentů ve vlastnictví úřadu. Konverzi z moci úřední mohou provádět pouze orgány veřejné moci. Pro účely této konverze se využívá služeb rozhraní CzechPOINT@office.

3.5.3 Základní registry

Základní registry jsou platformou pro bezpečné sdílení dat v rámci celé veřejné správy v České republice. [27]

Smyslem zavedení těchto registrů bylo vytvořit takovou jednotnou databázi pro veřejnou správu, která by zajistila rychlou a bezpečnou možnost aktualizace údajů a zamezila by zbytečným duplicitám.

„Zákon má stanovit základní registry, které budou jedinečnými zdroji údajů využívaných při práci veřejné správy. Mělo by tak dojít k odstranění roztříštěnosti, nejednotnosti a vícenásobného výskytu dat v zásadních databázích veřejné správy.

Nutnost zavedení základních registrů je dána skutečností, že v současné době není možné se spolehnout na aktuálnost údajů, které jsou v jednotlivých databázích obsaženy, a není možné různé databáze navzájem bezpečně sdílet. To vede k situaci, kdy občan je opakovaně nucen dodávat veřejné správě údaje, které jí již mnohokráte poskytl, případně veřejná správa pracuje s chybnými podklady.“ [28]

Základní registr obsahuje referenční údaje, referenční vazby, identifikátory fyzických osob, popřípadě autentizační údaje. Referenční vazby jsou kódy nebo identifikátory, kterými je odkazováno na referenční údaje v základních registrech. Autentizační údaje jsou údaje umožňující provést ověření identity fyzické osoby. [10]

Údaje, které jsou uvedeny v základních registrech, jsou dle zákona označeny jako údaje referenční. Pojem referenční údaj lze vyložit jako státem garantovaný správný údaj obsažený v příslušném základním registru, který orgán veřejné moci využívá při své činnosti a to, aniž by ověřoval jejich správnost. Od osob, po kterých je jiným právním předpisem doložení takových údajů požadováno, je orgán veřejné moci oprávněn požadovat poskytnutí takových údajů pouze, pokud nejsou v základním registru obsaženy, nebo jsou označeny jako nesprávné, nebo vznikne oprávněná pochybnost o správnosti referenčního údaje, nebo jsou nezbytné pro bezpečnostní řízení podle jiného právního předpisu. [29]

Podle §3 zákona č.111/2009 mezi základní registry patří:

- základní registr obyvatel („registr obyvatel“)
- základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci („registr osob“)
- základní registr územní identifikace, adres a nemovitostí („registr územní identifikace“)
- základní registr agend orgánů veřejné moci a některých práv a povinností („registr práv a povinností“)

Tyto čtyři základní registry fungují v rámci Informačního systému základních registrů, jehož správu má na starosti Správa základních registrů. Technologickou platformu informačního systému zajišťuje Komunikační infrastruktura veřejné správy a Centrální místo služeb.[30]

Správa základních registrů má za úkol zajišťovat [31]:

- provoz informačního systému základních registrů, registru obyvatel, registru osob a registru práv a povinností a jejich bezpečnost
- realizaci vazeb mezi jednotlivými základními registry prostřednictvím služeb informačního systému základních registrů
- realizaci vazeb mezi základními registry a agendovými informačními systémy prostřednictvím služeb informačního systému základních registrů
- realizaci vazeb mezi jednotlivými agendovými informačními systémy prostřednictvím služeb informačního systému základních registrů
- zpřístupnění referenčních údajů obsažených v základních registrech a údajů obsažených v agendových informačních systémech v rozsahu oprávnění obsažených v registru práv a povinností
- vedení záznamů o událostech souvisejících s provozováním informačního systému základních registrů

Informační systém základních registrů (ISZR) je definován jako jediné a referenční rozhraní pro přístup k základním registrům. Skrze referenční rozhraní jsou poskytovány komplexní služby definované v katalogu eGON služeb. Tyto služby nad základními registry jsou poskytovány všem subjektům s ohledem na jejich aktuální oprávnění v registru práv a povinností.

Důležitou součástí systému je také Převodník identifikátorů fyzických osob – ORG.

3.5.4 KIVS

Komunikační infrastruktura veřejné správy neboli KIVS jednoduše řečeno představuje sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě. Přínosem KIVS je jak zefektivnění služeb, tak výrazné úspory.

Budování KIVS bylo zahájeno v roce 2007, v situaci, kdy paralelně vedle sebe existovaly a přibývaly další a další datové linky od jednotlivých ministerstev a úřadů. Primárním cílem zavádění KIVS bylo vytvoření jednotné datové sítě, která poskytne bezpečné připojení a vysoký standard nabízených služeb. Druhým cílem bylo odstranění monopolu poskytovatelů datových služeb. [32]

Dne 23. 10. 2001 byla podepsána rámcová smlouva mezi Českou republikou a společností Český Telecom,a.s o poskytování služeb komunikační infrastruktury informačních systémů veřejné správy. Tento projekt měl umožnit do dvou let připojit

a vzájemně propojit všechny orgány veřejné správy a současně jim zajistit bezpečnou a ekonomickou komunikaci, včetně přístupu k informačním zdrojům. Až v roce 2007 byly zapojeny další společnosti: [33]

- Telefónica 02 (dříve Český Telecom)
- konsorcium společností T-Systems Pragonet a ČD-Telematika
- GTS Novera

Jádrem KIVS je centrální místo služeb. To zajišťuje vzájemné řízené a bezpečné propojování subjektů veřejné a státní správy, dále zajišťuje komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích, jakými jsou internet nebo komunikační infrastruktura EU. Zároveň tvoří jediné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS. [32]

CMS slouží jako hlavní propojovací místo eGovernmentu a zajišťuje služby pro jeho čtyři základní komunikační prostředí. Těmito prostředími jsou [34]:

- Prostředí Internetu
- Prostředí KIVS
- Prostředí Centrálních eGon služeb
- Prostředí komunikační infrastruktury EU

3.5.5 Elektronický podpis

Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. [35]

V § 2, zákona o elektronickém podpisu se elektronickým podpisem rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.

Zaručený elektronický podpis lze chápat jako jakousi vyšší formu podpisu elektronického. Zaručený elektronický podpis jsou digitální data, která podepisující osoba vytváří pomocí svého privátního klíče a zajišťuje jimi integritu a nepopiratelnost původu podepsaných dat. [36]

Podle zákona je zaručeným elektronickým podpisem ten elektronický podpis, který splňuje tyto požadavky: [10]

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat

V § 11 je jasně stanoveno, že k podepisování nebo označování dokumentu v podobě datové zprávy, jehož prostřednictvím se činí úkon vůči veřejné správě lze použít pouze uznávaný elektronický podpis nebo uznávanou elektronickou značku. Uznávaným elektronickým podpisem se rozumí:

- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby,
- zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie

Elektronický podpis, který je založen na technologii PKI, představuje využití páru kryptografických klíčů pro identifikaci komunikujících partnerů v elektronickém světě. Vlastnictví daného páru klíčů a svoji identitu pak komunikující partner prokazuje prostřednictvím příslušného certifikátu. Certifikáty jsou vydávány tzv. Certifikační autoritou, nezávislým důvěryhodným subjektem. Úkolem Certifikační autority je ověřit totožnost žadatele o certifikát a jednoznačně svázat jeho identifikaci s daty pro tvorbu elektronického podpisu prostřednictvím certifikátu, který žadateli vydává. Vydaný certifikát při komunikaci představuje jakýsi „elektronický průkaz totožnosti“. [37]

3.6 Bezpečnostní prvky elektronické komunikace

S elektronickou komunikací úzce souvisí problematika šifrování. Šifra je kryptografický algoritmus, který pomocí klíče převádí čitelnou zprávu na její nečitelnou podobu neboli šifrový text. Z technického hlediska je klíč bitová sekvence určité délky.

Se šifrováním úzce souvisí pojem hašovací funkce. Pro bezpečnou elektronickou komunikaci je vždy velmi důležitá autentizace uživatele, která má za úkol zabránit falšování identity.

3.6.1 Šifrování

První variantou šifrování textu je symetrické šifrování. To využívá jediný klíč jak pro zašifrování zprávy, tak i pro její dešifrování. Pro takovou komunikaci je nutné, aby příjemce znal klíč použitý odesílatelem. Výhodou symetrického šifrování je jeho menší výpočetní náročnost, a tím vyšší výpočetní rychlost. Nevýhodou je nutnost výměny tajného klíče mezi odesílatelem a příjemcem, protože při přenosu je možnost získání klíče třetí stranou.

Druhou technikou pro šifrování je asymetrické šifrování neboli kryptografie pomocí veřejného klíče. Oproti symetrickému šifrování, kde se využívá pouze jeden klíč, se zde používají dva separátní klíče, kdy jeden je veřejný a druhý privátní. Veřejný klíč příjemce poskytne všem, se kterými chce komunikovat, zatímco soukromý klíč musí zůstat v tajnosti. Za pomocí veřejného klíče příjemce odesílatel zprávu zakóduje a odešle ji příjemci. Ten pomocí svého privátního klíče zprávu dekóduje a přečte. Důležité je, že z privátního klíče nelze získat veřejný a naopak. Hlavní výhodou je pak samotné předání klíčů. To nemusí být nijak zabezpečené, jako tomu je u symetrického šifrování. Asymetrické šifrování umožňuje i použití privátního klíče u odesílatele a veřejného u příjemce. Toho je využívání například u elektronického podpisu.

Další šifrovací technikou je tzv. hybridní schéma, která slučuje rychlost symetrické a bezpečnost asymetrické kryptografie. Náhodně vygenerovaný klíč symetricky zašifruje data. Tento klíč je pak zašifrován asymetricky veřejným klíčem příjemce. Pak se zašifrovaný klíč a zašifrovaná data se společně odešlou příjemci, který si pomocí privátního klíče dešifruje klíč pro symetrickou šifru a s jeho pomocí dešifruje samotná data. Pomocí pomalé asymetrické šifry se totiž šifruje pouze krátký klíč, zatímco samotná dlouhá data jsou šifrována rychlou symetrickou šifrou. [38]

3.6.2 Hashování

Hašovací funkce je algoritmus pro převod vstupních dat do výstupu, který je označován jako otisk či hash. Tato funkce je jednosměrná, to znamená, že z hashe je v podstatě nemožné získat původní text, což je podstatný rozdíl od šifrování. Funkce poskytuje pro jakékoliv množství vstupní dat stejně dlouhý otisk a i malou změnou

na vstupu se dosáhne výrazné změny na výstupu. Využití otisků je především u zabezpečení hesel nebo slouží k ověření, zda nebyl soubor upravován. [39]

3.6.3 Certifikace

U veřejných klíčů v asymetrickém šifrování je třeba zaručit, že daný klíč patří správnému subjektu. To zaručují digitální certifikáty. Certifikát je datová struktura, která mimo jiné obsahuje veřejný klíč, informace o jeho majiteli a informace o vydavateli tohoto certifikátu, takzvané certifikační autoritě.

3.6.4 Autentizace

Důležitou součástí pro systém elektronických voleb je autentizace uživatele, což je proces ověření proklamované identity. Existují různé autentizační metody, které mohou být založené [40]:

- na něčem, co daný uživatel zná,
- na něčem, co daný uživatel vlastní,
- na něčem, čím daný uživatel je.

První možnost zahrnuje například znalost hesla nebo data narození. Druhá varianta počítá s vlastnictvím například identifikační karty nebo certifikátu v počítači. Nejbezpečnější variantou je využití biometrických údajů, jako jsou otisky prstů nebo scan sítnice.

Na základě kombinace různých faktorů se rozlišuje autentizace jednofaktorová, dvoufaktorová nebo vícefaktorová. Čím více faktorů je využito, tím je obtížnější zfalšovat identitu voliče.

3.7 Elektronické volby

3.7.1 Definice elektronických voleb

Podle definice Doporučení výboru ministrů Rady Evropy o právních, operačních a technických standardech elektronického hlasování „lze volby považovat za elektronické, jakmile jsou elektronické prostředky využívány alespoň v jakékoli jedné fázi volebního procesu“. Podle této definice by se však v dnešní době daly brát všechny volby jako elektronické. Proto se pojem elektronické volby využívá spíše pro proces, kdy se informační technologie využívají při odevzdávání hlasu. [41]

Definice dle Petra Šindeláře zní: „Za elektronické volby se považují volby, ve kterých volební hlas vystupuje pouze v elektronické podobě. Jedná se tedy o proces, ve kterém je akt volby občanem uskutečněn přímo prostřednictvím elektronického zařízení a jeho výsledek předán ke zpracování prostřednictvím elektronického přenosového média (komunikační sítě) a dále zpracováván výhradně elektronickou cestou. Za elektronické volby nelze považovat volby, ve kterých vystupují informační technologie pouze ve fázi zpracování výsledků, neboť ty pouze adekvátním způsobem nahrazují lidskou činnost“. [42]

Elektronické hlasování se dělí do dvou kategorií a to na vzdálené elektronické hlasování a nevzdálené elektronické hlasování.

3.7.2 Nevzdálené elektronické hlasování

Nevzdálené elektronické hlasování je také nazýváno presenční hlasování, non-remote electronic voting či poll-site electronic voting. Způsob nevzdáleného elektronického hlasování je velmi podobný současnému způsobu hlasování pomocí volebních lístků. Volič se v daný čas dostaví do příslušné volební místnosti, kde odevzdá svůj hlas. Samotné hlasování ale probíhá pomocí DRE volebního terminálu s dotykovou obrazovkou. Hlas je po potvrzení volby uložen do elektronické volební urny a po skončení voleb je zpracován v rámci sčítání hlasů.

Oproti tradičnímu způsobu hlasování pomocí volebních lístků má tento způsob jednoznačnou výhodu v rychlosti a přesnosti zpracování dat. Hlasy voličů nemusí sčítat členové volební komise, kterým to ve větších volebních obvodech zabere až několik hodin, a není vyloučena možnost chyby či úmyslné manipulace, ale sečte je příslušný software během velmi krátké doby. Podmínkou správného sečtení hlasů je však bezchybně naprogramovaný software. V případě špatného naprogramování mohou být výrazně změněny výsledky voleb a případná kontrola je velmi obtížná.

Další výhodou tohoto způsobu je možnost eliminace chybně odevzdaných hlasů, protože od softwaru lze očekávat, že uživatele, v tomto případě voliče, upozorní na případnou chybu.

Tato možnost hlasování by nahradila tradiční variantu, čímž by se ušetřily náklady na tisku a distribuci hlasovacích lístků. S nahrazením tradiční varianty hlasování ovšem nastává problém s počítačově negramotnými voliči, převážně z řad starších lidí, kteří často nemají s moderní technikou zkušenosti.

Očekávanou nevýhodou jsou velké finanční náklady na pořízení a údržbu hardwaru i softwaru. Každá volební místnost by musela být vybavena volebním terminálem s připojením na internet.

Tento způsob hlasování je využíván především ve Spojených státech amerických, kde tento systém využívá přes 30% voličů, a v Brazílii, kde je systém založení na DRE terminálech používán od roku 1997.

3.7.3 Vzdálené elektronické hlasování

Vzdálené elektronické hlasování neboli remote electronic voting je nejvyspělejším způsobem hlasování.

Volič v tomto případě není nucen být v daném čase ve volební místnosti. Pro vzdálené hlasování se využívá služeb internetu, mobilních telefonů nebo digitálních televizí. Jednoznačně nejrozšířenější je možnost hlasování pomocí internetu, neboli takzvaný iVoting (podle EU). V České republice je pod pojmem elektronické volby představován tento způsob hlasování.

Zpracování dat u tohoto způsobu je podobné jako u nevzdáleného hlasování, tudíž má některé výhody a nevýhody shodné. Patří mezi ně rychlost a přesnost zpracování, a také eliminace neplatných hlasů na straně výhod. Naproti tomu zůstává nevýhoda v závislosti na bezchybném softwaru.

Možností volit z domova či z práce se zvyšuje jistý komfort pro voliče, na základě kterého se očekává, že se zvýší volební účast. Kritici však upozorňují na to, že by někteří voliči začali brát hlasování lehkovážně a mohl tak vzrůst význam nesystémových politických stran a hnutí.

Problémovou oblastní zůstává také finanční náročnost. Na straně veřejných financí jde o náklady na vývoj, údržbu a testování softwaru. Na straně voličů se jedná o náklady na pořízení počítače s internetovým připojením, čtečky karet a samotné elektronické karty.

Pro blízkou budoucnost je internetové hlasování na rozdíl od hlasování pomocí terminálů pouhým doplňkem tradičního způsobu. Tím zůstávají náklady na tisk a distribuci volebních lístků, ale na druhou stranu zůstává alternativa pro voliče, kteří nechtějí využívat k volbě internet.

Nejdůležitějším argumentem proti zavedení internetového hlasování jsou bezpečnostní rizika. Prvním rizikem je bezpečnost volebního softwaru, u kterého nelze vyloučit možnost úmyslné či neúmyslné chyby, ani případný útok hackerů.

Problémem internetového hlasování je, že nelze zaručit tajné hlasování. Volič může být donucen hlasovat proti své vůli nebo může být výrazně ovlivněn rodinou, což je nazýváno family voting. Částečné eliminace tohoto rizika je dosaženo zavedením možnosti dodatečného hlasování ve volební místnosti, kdy by voliči byl započten papírový hlas namísto elektronického.

Zavedením internetového hlasování ve volbách by se mohly výrazně zlepšit možnosti pro zvýšení participace občanů na správě věcí veřejných ve formě zavedení referend či elektronických petic.

3.7.4 Historie eVoleb v České republice

V České republice se o zavedení internetového hlasování začalo vážněji mluvit až v roce 2007 za vlády Mirka Topolánka. Ministr vnitra jeho vlády Ivan Langer podepsal 7. dubna 2008 s tehdejších předsedou Českého statistického úřadu Janem Fischerem „Memorandum o spolupráci při koncipování, řešení, testování a realizaci systému elektronických voleb při příležitosti konference Internet ve státní správě a samosprávě“.

Z memoranda vyplývalo, že obě státní instituce se shodují na potřebě a společné vůli zahájit koncepční a praktické kroky vedoucí k realizaci projektu, jehož cílem bude umožnit voličům odevzdat svůj hlas ve volbách do zastupitelských sborů pomocí vzdáleného elektronického hlasování, například prostřednictvím internetu přímo ze svého domova, pracoviště nebo veřejného místa vybaveného připojením do internetu. Systém elektronických voleb přitom bude fungovat jako alternativa ke klasickému hlasování založeném na osobním odevzdání papírového hlasovacího lístku ve volební místnosti. Při podepisován memoranda se počítalo se zavedením elektronického občanského průkazu, který bude sloužit k jednoznačné a nezaměnitelné identifikaci voliče. Jako nutná podmínka pro zavedení systému e-voleb bylo uvedeno vybudování centrálního Registru voličů s návazností na Základní registr obyvatel. Další základní podmínkou bylo zajištění vysokého zabezpečení systému e-voleb tak, aby byla zaručena tajnost hlasování a ochrana systému před zásahy zvenčí i zevnitř. [43]

Dle představ tehdejší vlády, měla být v roce 2009 připravena technologie a zpracovaná legislativa. V následujícím roce měl být projekt vyzkoušen během senátních voleb v jednom z okrsků. První plnohodnotné elektronické volby měly být při volbách do Parlamentu České republiky v roce 2014.

Po volbách do Poslanecké sněmovny v roce 2010 se zástupci Občanské demokratické strany, TOP 09 a Věcí veřejných dohodli na koaliční smlouvě, kde se shodli na zahájení příprav projektu elektronických voleb tak, aby mohl být pilotní projekt realizován ve volebním roce 2012 a plnohodnotně zaveden od voleb do Poslanecké sněmovny v roce 2014, s termínem do 30. června 2012. V tom roce však ministr vnitra navrhl vládě odložení na roky 2015 a 2016, které vláda vzala na vědomí. V červnu 2013 podala vlád Petra Nečase demisi a projekt eVoleb již dále nepokračoval.

4 Vlastní práce

4.1 Elektronické volby ve světě

Konceptem internetových voleb se různá uskupení zabývají již značnou řádku let. Rada Evropy již v roce 2004 vydala doporučení členským státům směřující k začlenění elektronických volebních systémů do národních legislativ. Ačkoliv v mnoha zemích od začátku tisíciletí probíhalo spoustu pilotních projektů, dnes většina států od konceptu internetového hlasování ustoupila. Světlými výjimkami jsou v Evropě Estonská republika a Švýcarská konfederace.

4.1.1 Estonsko

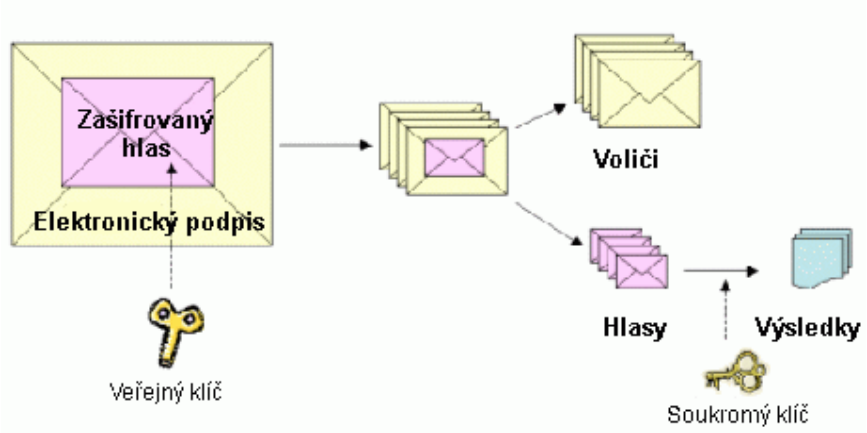
Jednoznačně nejvyspělejším evropským státem v oblasti nejen elektronických voleb, ale i celého eGovernmentu je Estonsko a po právu se řadí mezi internetové velmoci.

Velké možnosti využití eGovernmentu v Estonsku jsou dány velmi vstřícným postojem vlády vůči internetu. Estonské vzdělávání je velmi zaměřeno na informační a komunikační technologie, což zajišťuje vysokou míru počítačové a informační gramotnosti. Do legislativy bylo také zahrnuto právo na připojení k internetu od roku 2000, tudíž Estonsko je nyní zcela pokryto Wi-Fi sítí. Pro identifikaci jsou v Estonsku vydávány občanské průkazy vybavené čipem.

Průběh elektronických voleb v Estonsku je z pohledu voliče celkem jednoduchý. Volič si stáhne zabezpečenou aplikaci ze stránek www.valimised.ee. Pomocí občanského průkazu nebo pomocí mobilního telefonu s ověřenou SIM kartou se identifikuje a zadá první bezpečnostní kód pro potvrzení identity. Systém se spojí s registrem obyvatel, ověří volební práva voliče a přidělí ho do příslušného volebního okrsku. Po přihlášení provede volič výběr svého kandidáta a volbu potvrdí. Pro ověření zadá druhý identifikační kód. Pokud volba proběhne správně, objeví se potvrzující dialogové okno.

Proces elektronického hlasování v Estonsku je elektronickou obdobou korespondenčního hlasování. Volič zašifruje veřejným klíčem první obálku s hlasovacím lístkem. Tu vloží do druhé obálky, kterou podepíše digitálním podpisem a odešle ji. Systém obálky shromáždí, setřídí a odstraní neplatné hlasy. Vnější obálky jsou otevřeny a vnitřní jsou zaslány ke zpracování. Jsou dešifrovány privátním klíčem a hlasy jsou sečteny. Celý tento proces znázorňuje schéma na obrázku č. 4. [44]

Obrázek č. 4 – princip šifrování volebních hlasů



Zdroj: www.vvk.ee

Samotný Estonský volební systém je možné rozdělit na několik částí, jak je vidět na obrázku č. 5.

- Volič – elektronický volič s jeho počítačem. Vytváří zašifrovaný a elektronicky podepsaný hlas a zasílá ho do centrálního systému.
- Centrální systém – součást systému, která zodpovídá za kompletní zpracování hlasů od jejich přijetí až do prezentace výsledků.
- Key Management – vytváří a spravuje šifrovací klíče. Zatímco veřejný klíč je integrován do volební aplikace, soukromý klíč je dodáván do aplikace na sčítání hlasů.
- Audit – zaznamenává informace z centrálního systému, čímž pomáhá řešit případné stížnosti.

Samotný centrální systém je tvořen třemi servery:

- Vote Forwarding Server - tento server obstarává veškerou komunikaci mezi voličem a volebním informačním systémem. Zajišťuje autorizaci voličů pomocí elektronické karty a zasílání seznamu kandidátů. Přijímá zašifrované a podepsané volební obálky, které zasílá do Vote Storage Serveru a od něj pak přeposílá voliči potvrzení o přijetí hlasu.
- Vote Storage Server - tento server přijímá od Vote Forwarding Serveru zašifrované volební hlasy a uloží je. Po skončení voleb systém odstraní duplicitní hlasy či jinak

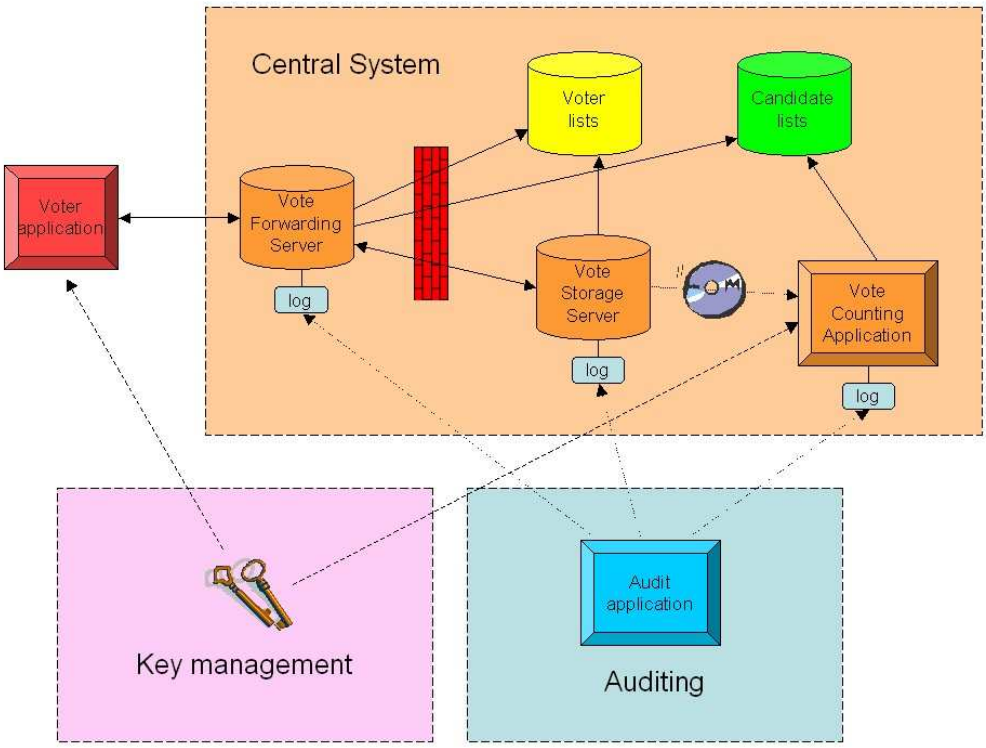
neplatné hlasy. Poté oddělí vnější obálky a vnitřní odešle do Vote Counting Serveru.

- Vote Counting Application - část systému pracující offine, do které jsou přeneseny zašifrované hlasy zbavené digitálního podpisu, což zajišťuje anonymitu volebního lístku. Server použije svůj privátní klíč k dešifrování volebních lístků, setřídí je a sečte.

Jednotlivé servery využívají dva různé registry:

- Registr voličů
- Registr kandidátů

Obrázek č. 5 – schéma estonského systému eVoleb



Zdroj - www.vvk.ee

Kvůli snaze snížit bezpečnostní riziko v rámci ovlivňování je voliči umožněno hlasovat opakovaně. Do výsledků se započítává pouze poslední volba. Volič má možnost zúčastnit se i klasického způsobu pomocí volebního lístku a tím zneplatnit svůj elektronický hlas.

Elektronické hlasování probíhá od 10. do 4. dne před otevřením volebních místností. Důvodem je, aby komise dostala seznam těch, kteří hlasovali přes internet a zabránila tak duplicitě hlasování.

Pilotní projekt proběhl v lednu 2005 v Tallinu u referenda o umístění památníku svobody. Možnost internetového hlasování tehdy využilo 14% hlasujících.

První celostátní možnost elektronického hlasování byla v říjnu 2005 při komunálních volbách, kdy tuto možnost využila pouhá dvě procenta hlasujících občanů.

Důležitou událostí byly historicky první volby do parlamentu s možností hlasování po internetu na přelomu února a března 2007. V těchto volbách využilo internet 5,5% ze zúčastněných voličů.

Tento trend postupného zvyšování využití internetu narůstal i v dalších letech. V roce 2009 proběhly v Estonsku volby do Evropského parlamentu a volby regionální, kde podíl online hlasujících voličů stoupl na 15, respektive 16%. V parlamentních volbách v roce 2011 hlasovala elektronicky již celá čtvrtina hlasujících. Statistiky internetového hlasování v Estonsku jsou zobrazeny v tabulce č. 1.

Tabulka č. 1 – statistika voleb v Estonsku

	2005	2007	2009	2009	2011	2013	2014
	Komunální volby	Parlamentní volby	Volby do EP	Komunální volby	Parlamentní volby	Komunální volby	Volby do EP
Celkový počet voličů	1 059 292	897 243	909 628	1 094 317	913 346	1 086 935	902 873
Volební účast (v %)	47,4	61,9	43,9	60,6	63,5	58	36,5
Voliči iVotingu	9 317	30 275	58 669	104 413	140 846	133 808	103 151
Podíl iVotingu na celkové účasti (v %)	1,9	5,5	14,7	15,8	24,3	21,2	31,3
Změněné el. hlasy	364	789	910	2 373	4 384	3 045	2 019
El. hlasy nahrazené papírovými	30	32	55	100	82	146	46

Zdroj: vlastní dle statistik na www.vvk.ee

4.1.2 Švýcarsko

Ve Švýcarsku je politický systém založený na velké participaci občanů. S tím souvisí časté konání referend a voleb do různých orgánů na úrovni obce, kantonu či federace. K této formě vládnutí je potřeba vysoká angažovanost voličů a tím i značná účast ve volbách a referendech. Pro zvýšení účasti se v roce 1995 zavedli poštovní volby a v návaznosti na nich se častěji ozývaly hlasy pro zavedení internetových voleb.

V roce 2000 začal kanton Ženeva s přípravou pilotního projektu elektronických voleb, na kterém se podílely společnosti Hewlett-Packard a Wisekey.

V prvních internetových volbách tohoto kantonu se pro možnost volit online rozhodla téměř čtvrtina voličů a celková účast se zvýšila o 13%.

Další úspěšné pilotní projekty proběhly v roce 2005 v kantonech Neuchâtel a Curych. V dalších letech byly postupně projekty zdokonalovány a testovány na úrovních měst i kantonů.

Od roku 2008 je internetové hlasování uzákoněno na federální úrovni. Internetové hlasování bylo umožněno také všem Švýcarům žijící v zahraničí.

4.1.3 USA

Ve Spojených státech amerických vzniklo několik systémů, které měly umožnit internetové hlasování, ale žádný z nich se nepodařilo uvést v praxi.

Nejznámějším systémem je Secure Electronic Registration and Voting Experiment (SERVE) vyvinutý pro volby v roce 2004. Systém byl určen především pro vojáky a osoby, které pobývali v době voleb v zahraničí. V systému SERVE bylo možné hlasovat během 30 dnů před termínem běžných voleb. Na rozdíl od Estonského systému, mohli voliči v USA volit elektronicky pouze jednou a nemohli se pak již zúčastnit běžných voleb.

Odlišností v oblasti architektury volebního systému byla mimo jiné existence serveru pro sčítání hlasů na každém volebním úřadu.

V rámci zpracování volebního lístku byl zvolen jiný postup také v oblasti šifrování. Volební aplikace nejdříve zašifruje volební lístek a zašle ho serveru pro zpracování dat. Ten lístek dešifruje pomocí svého privátního klíče a oddělí volební lístek a osobní údaje voliče. Poté samotný hlas zašifruje veřejným klíčem serveru pro sčítání hlasů a odešle ho. Celý tento systém byl v roce 2004 zastaven na základě analýzy bezpečnostních analytiků.

4.1.4 Ostatní státy

V Nizozemí mělo využití elektronických zařízení pro volby dlouhou tradici. V roce 2006 vznikla skupina počítačových expertů "We DO Not Trust Voting Computers" (Nevěříme hlasovacímu zařízení), která upozorňovala na bezpečnostní rizika elektronického hlasování. Výsledkem snažení této skupiny bylo zřízení dvou komisí, které nedostatky potvrdily. V návaznosti na tato zjištění vláda zrušila elektronické volby.

Po volbách z roku 2005 proběhlo v Německu několik soudních sporů na základě stížností občanů. Následně vznikla petice požadující zrušení elektronických voleb, kterou podpořilo přes 40 tisíc občanů. V roce 2009 spolkový ústavní soud rozhodl, že z důvodu netransparentnosti a neověřitelnosti výsledků voleb občany je použití elektronického hlasování protiústavní.

I v dalších zemích Evropy postupně ustoupili od konceptu internetových voleb. Hlavním důvodem bylo spojeno s bezpečností, v některých případech byla na vině i nedostatečná technologie. Ve Skotsku například některé hlasy nebyly vůbec započítány a část hlasů dorazila až se zpožděním. Ve Francii se některé hlasy přímo ztratily, jiné se nepodařilo dešifrovat, a dokonce během voleb systém elektronického hlasování spadl.

4.2 Elektronické volby v České republice

4.2.1 Připravenost České republiky na eVolby

Před samotnými úvahami nad zavedením internetového hlasování je třeba analyzovat připravenost České republiky na elektronické volby.

První kritérium pro posouzení možnosti zavedení internetového hlasování je ekonomické hledisko. Častý argument pro zavedení eVoleb je finanční úspora oproti tradičnímu způsobu hlasování. Snížení finanční náročnosti by mělo znamenat úspory především na straně tisku a distribuci hlasovacích lístků či mzdových výdajů pro členy volební komise a příslušníků Policie České republiky. Tyto argumenty by však platily v případě, že by elektronické volby plně nahradily tradiční způsob voleb.
Lze předpokládat, že v případě zavedení eVoleb do českého právního řádu, by se staly pouhým doplňkem a většina nákladů na tradiční způsob by se snížila jen mírně. Možným opatřením, které by mohlo zavedení eVoleb přinést, je zrušení druhého dne běžných voleb, které by zajisté přineslo snížení nákladů. Finanční náklady elektronických voleb jsou vysoké především při zavádění tohoto systému, zatímco provozní náklady jsou relativně

velmi nízké. V roce 2012 vydala Hospodářská komora odhad nákladů na zavedení eVoleb, který činil necelých 500 milionů korun. Detailní rozvržení nákladů je zobrazeno v tabulce č. 2. Důležité je upozornit na to, že takto vysoké náklady by byly pouze v počátku zavádění systému a systém elektronických voleb by se vyplatil, až v delším časovém horizontu.

Tabulka č. 2 – náklady na eVolby

Položka	Cena v Kč
Náklady na hardware	100 mil (max)
Vybudování systému Volby	230 mil.
Pilotní projekt	112 mil.
Provozní náklady	22 mil.
CELKEM	**464 mil.**

Zdroj: Hospodářská komora České republiky

Zavedení eVoleb do českého právního řádu by vyžadovalo výrazné změny v legislativě. Současná ústava České republiky prostřednictvím zákonům zaručuje občanům, že volební právo je:

- Všeobecné - zaručuje právo volit všem zletilým občanům České republiky bez ohledu na jejich pohlaví, rasu, národnost, původu či majetku. Mělo by také zaručit stejný přístup k volbám.
- Rovné - zajišťuje, že každá volič má právě jeden hlas a všechny hlasy mají stejnou váhu.
- Přímé - volba je prováděna přímo voličem. Právo volit nesmí být žádným způsobem převedeno na jinou osobu.
- Volba je vykonávána tajným hlasováním.

Kromě Ústavy a Listiny základních práv a svobod, které vymezují základní volební práva, se voleb týká ještě několik zákonů, především zákon o volbě prezidenta republiky, zákon o volbách do Evropského parlamentu, zákon o volbách do Parlamentu České republiky, zákon o volbách do zastupitelstev krajů a zákon o volbách do zastupitelstev obcí. Všechny tyto zákony by bylo třeba patřičně novelizovat, aby umožňovaly internetové hlasování.

Třetím hlediskem k analýze je hledisko připravenosti samotných občanů České republiky. Při zavedení tak důležité elektronické komunikace jako jsou volby, je důležitým aspektem důvěra voličů v moderní technologie. Nedůvěra v internetovou komunikaci by způsobila velmi nízkou volební účast u internetového hlasování a jeho zavedení by tak bylo zbytečné. Dalším rizikem je zvětšení digitální propasti mezi občany.

Čtvrtou a velmi podstatnou oblastí je technologické hledisko. Nejdůležitější součástí elektronických voleb je samotný informační systém. Jeho požadavky jsou rozpracovány v následující kapitole. Kromě informačního systému by bylo třeba pořídit technologie sloužící k jednoznačné autentizaci uživatele.

4.2.2 Požadavky na elektronický volební systém

Elektronický volební systém musí respektovat volební práva občanů České republiky a dodržovat veškerá bezpečnostní opatření. Před jeho vytvořením je nutné zadat jasně definované požadavky, mezi které jednoznačně patří:

- Každý volič má jeden hlas – informační systém musí vzhledem k rovnému volebnímu právu zaručit, že každému voliči bude započítán právě jeden hlas. Problém s duplicitním hlasováním by mohl nastat především u možnosti opakovaného hlasování, jako je využíván v Estonsku.
- Volit smí pouze oprávněný volič – k volbám se může dostavit každý svéprávný občan starší 18 let, který patří do daného volebního okrsku. Zatímco u klasických voleb kontroluje oprávněnost voliče volební komise na základě předloženého občanského průkazu, u internetového hlasování musí veškeré ověřování obstarat volební informační systém.
- Anonymita volby – volební lístek nesmí být spojený s určitým voličem, aby se zabránilo možnosti zjistit, kdo pro koho hlasoval. Zároveň však systém musí umožnit opakované hlasování. Tajný hlas musí tedy být spojen s voličem do ukončení voleb. Po ukončení hlasování systém definitivně oddělí voliče od jeho volebního lístku a teprve pak zjistí jeho obsah.
- Bezpečnost systému – informační systém elektronických voleb musí mít zajištěnou vysokou míru bezpečnosti, která odpovídá jeho významu. Bezpečný systém musí zajistit, že volební hlas bude zpracován, aniž by byl upraven, zpřístupněn či odstraněn. Při budování informačního systému je třeba se zabývat všemi možnými riziky, mezi které patří poruchy některé z částí systému, napadení virem

či neúmyslný i úmyslný zásah člověka. Po zavedení elektronických voleb pro celou republiku je třeba počítat s obsluhou velkého množství uživatelé v relativně krátkém čase. Proto by bezpečnostní opatření měla zabránit výpadku systému z důvodu přetížení

- Jednoduché ovládání – aby byl informační systém voleb využíván co nejširší veřejností, je třeba zajistit, aby jeho uživatelské prostředí bylo jednoduché a intuitivní pro všechny případné voliče. Ohled by měl brát mimo jiné na uživatele se zrakovým postižením nebo jiným zdravotním znevýhodněním.
- Bezchybné sčítání hlasů s možností kontroly – proces sčítání hlasů je třeba důkladně odzkoušet v rámci testovacích projektů tak, aby při ostrém spuštění byla jistota správného výsledku. Dále je zapotřebí systém vybavit mechanizmem, který by umožňoval ověřit, zda byl daný hlas započítán.

4.2.3 Návrh eVoleb v České republice

Pokud se v blízké budoucnosti politici rozhodnou znovu zahájit přípravy ke spuštění elektronických voleb, je pravděpodobné, že se budou inspirovat zemí, ve které již tento způsob hlasování funguje. Lze očekávat, že touto zemí bude Estonsko. Následující odstavce nastiňují, jakby v elektronické hlasování vypadalo v České republice.

Volby pomocí internetu by se určitě staly pouhým doplňkem klasických voleb pomocí volebních lístků, které by bylo nutné zachovat nejen pro voliče, kteří nebudou mít důvěru v elektronický způsob, ale také pro možnost změnit svůj hlas pro ty, kteří využili internetové hlasování.

Po schválení příslušné legislativy a zadání zakázky na vytvoření volebního systému, by bylo třeba zajistit splnění technických požadavků na straně uživatelů, které by sloužili k autentizaci voliče. Nejpřesnější možností autentizace je využití biometrických údajů. Případné technické vybavení k této identifikaci by však bylo velmi nákladné. Proto by s ohledem na finanční náročnost a bezpečnost bylo vhodné zvolit dvoufaktorovou autentizaci na základě vlastnictví čipové karty a znalosti příslušného kódu.

Novela zákona č. 328/1999 Sb., o občanských průkazech spolu s vyhláškou č. 400/2011 Sb., zavedly od ledna 2012 nový typ občanského průkazu, kterým je elektronický občanský průkaz. Tento průkaz se strojově čitelnými údaji existuje ve dvou variantách, a to buď s kontaktním elektronickým čipem, nebo bez něj. V současné době je varianta s čipem dobrovolná a při jejím zvolení je účtován poplatek 500 korun.

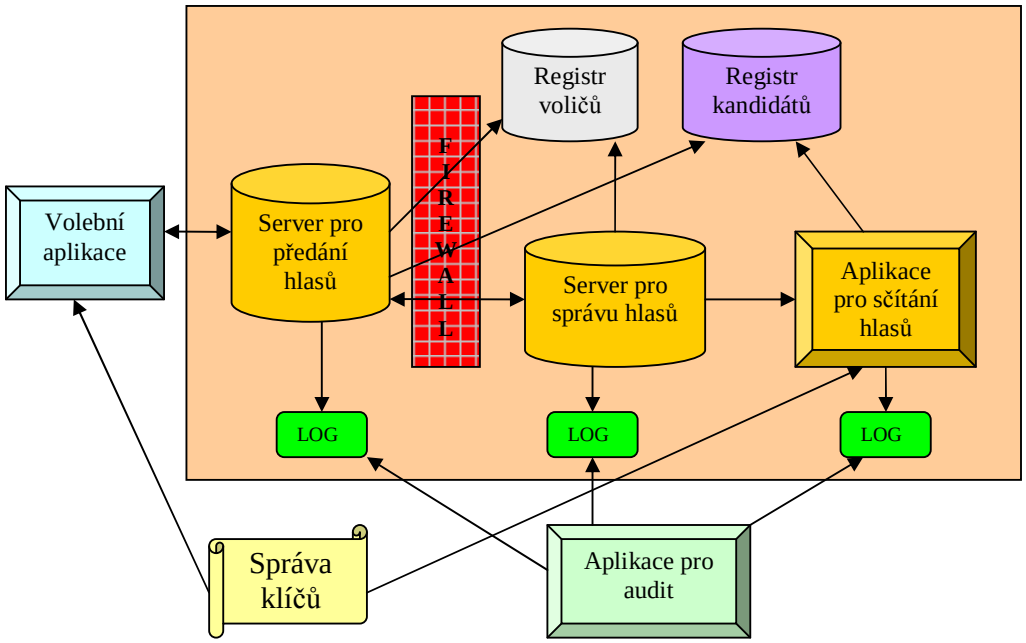
V případě spuštění projektu elektronických voleb, by bylo třeba, aby průkaz vybavený čipem měl každý občan, který hodlá využívat internetové hlasování. Čip na kartě by bylo třeba vybavit dvěma páry klíčů s certifikátem pro zabezpečení internetového hlasování. Další podmínkou je pořízení čtečky elektronické karty, která by zajistila spojení elektronického průkazu a počítače s volební aplikací.

Elektronické volby by byly zahájeny 10. den před konáním klasických voleb a ukončeny 5. den před nimi tak, aby bylo možné včas získat seznam internetových voličů a zamezit duplicitnímu hlasování. Se zavedením eVoleb by bylo logické odstranit z volebního zákona české specifikum ve formě dvou volebních dnů a zavést standardní jednodenní volby pomocí lístků.

Průběh samotného internetového hlasování by byl obdobný jako u Estonského modelu. Volič si stáhne z příslušného volebního webu zabezpečenou aplikaci určenou pro hlasování. Pomocí svého občanského průkazu s čipem a čtečky se identifikuje a zadá bezpečnostní kód pro ověření příslušné identity. Systém se spojí s registrem voličů a ověří volební práva uživatele. Po úspěšném ověření aplikace zjišťuje, zda se jedná o uživatelovu první volbu. Pokud již uživatel dříve hlasoval, je aplikací požádán o potvrzení, že chce svůj hlas změnit a pak mu je případně zobrazen nový volební lístek z jeho volebního obvodu. V případě první volby je uživateli rovnou zobrazen volební lístek. Po výběru a potvrzení kandidátní listiny je hlas zašifrován a opatřen elektronickým podpisem za pomoci druhého bezpečnostního kódu. Hlas je odeslán do systému, který zkontroluje elektronický podpis, zaznamená, že uživatel již hlasoval a potvrdí voliči příjem jeho hlasu.

Po skončení elektronických voleb systém od platných hlasů odstraní podpisy, aby nebylo možné přiřadit voliče k jednotlivému hlasovacímu lístku. Elektronické lístky jsou převedeny do aplikace pro sčítání hlasů, která odšifruje volební lístky a započte jeho obsah. Výsledky jsou předány do systému pro prezentaci výsledků stejně jako výsledky dodané volebními komisemi ze standardního způsobu hlasování.

Obrázek č. 6 – schéma českého systému eVoleb



Zdroj: vlastní dle www.vvk.ee

Architektura českého elektronického volebního systému by byla založena taktéž na Estonském modelu:

- Volební aplikace – umožňuje komunikaci voliče se systémem eVoleb.
- Server pro předání hlasů – obstarává veškerou komunikaci mezi aplikací voliče a zbytkem systému. Komunikace s ostatními prvky systému probíhá vždy přes firewall, který má za úkol zamezit neoprávněnému zásahu zvenčí. Přijaté hlasy odesílá do serveru pro správu hlasů a záznam o něm ukládá do souboru LOG1.
- Server pro správu hlasu - sdružuje veškeré přijaté hlasy až do ukončení voleb. Jeho úkolem je mimo jiné odstranění duplicit při opakovaném hlasování voliče. Veškeré zrušené hlasy se zaznamenávají do souboru LOG2. Hlasy určené pro přenos do aplikace pro sčítání jsou zaznamenány do souboru LOG3.
- Aplikace pro sčítání hlasů – zajišťuje zpracování hlasů zbavených elektronického podpisu voliče. Po odšifrování aplikace sečte správné hlasy. Případné neplatné hlasy se zaznamenají do LOG4, započtené platné hlasy do LOG5.
- Správa klíčů – je zodpovědná za vytvoření a správu klíčů pro zajištění bezpečnosti hlasů.

- Aplikace pro audit – zaznamenává zpracování jednotlivých hlasů a umožňuje tak řešit některé případné stížnosti. K tomu využívá pět LOG souborů:
  - LOG1 – přijaté hlasy ID voliče, hash (hlas)
  - LOG2 – zrušené hlasy ID voliče, hash (hlas), důvod
  - LOG3 – hlasy k započtení ID voliče, hash (hlas)
  - LOG4 – neplatné hlasy hash (hlas)
  - LOG5 – platné hlasy hash (hlas)
- Registr voličů – umožňuje ověření volebního práva a příslušnost k jednotlivým volebním obvodům. K jeho vytvoření je vhodné použít údaje v již fungujících základních registrech.
- Registr kandidátů – shromažďuje veškeré kandidáty ve všech volebních okrscích.

5 Výsledky a diskuse

O tématu elektronických voleb se vážně hovoří už od přelomu tisíciletí. Rada Evropy vydala v roce 2004 nezávazné doporučení členským státům k začlenění elektronických volebních systémů do národních volebních legislativ. I přes toto doporučení se většina států Evropy drží zavedeného systému papírových voleb, případně od elektronického způsobu odstupuje po špatných zkušenostech s jeho využitím. Nejčastějšími problémy jsou bezpečnostní rizika. Tato rizika jsou jak na straně voliče, kdy není možné zaručit přímé a tajné hlasování, tak na straně samotného systému, kdy veškeré zpracování a vyhodnocení hlasování závisí na bezchybném naprogramování.

V rámci Evropské unie je světlou výjimkou Estonsko, které je světovou velmocí z pohledu elektronizace státní správy. Vysoké využívání služeb eGovernmentu v Estonsku je umožněno vysokou počítačovou a informační gramotností, na kterou jsou v estonském vzdělávacím systému kladeny vysoké nároky. Zavedení elektronického systému voleb usnadnilo vlastnictví občanských průkazů s čipem a vysoká míra pokrytí Estonska Wi-Fi sítí. Samotný volební systém využívá pro zajištění bezpečnosti asynchronní šifrování a dvoufaktorovou autentizaci pro ověření identity voliče.

Dalším státem Evropy, který zaznamenal úspěchy v rámci elektronizace volebního sytému, je Švýcarská konfederace. Ta je známá jako vzor přímé demokracie s vysokou angažovaností voličů na správě věcí veřejných. Kvůli tomu bylo třeba umožnit voličům co nejpohodlnější způsob hlasování. Proto jednotlivá města a kantony začaly postupně se zaváděním internetového hlasování, které se postupně rozšířilo na celou konfederaci.

V dalších zemích už převažují negativní zkušenosti s elektronickým hlasováním. Nejčastějším důvodem ukončení projektů elektronických voleb byla bezpečnostní rizika a vysoké finančním náklady.

V České republice se v minulosti o zavedení internetového hlasování několikrát mluvilo, ale žádné konkrétní kroky nebyly prozatím učiněny. V současné době se o zavedení elektronických voleb na úrovni zákonodárné ani nejedná. Dle předsedy sněmovního Podvýboru pro ICT průmysl a eGovernment se problematika elektronických voleb v tomto volebním období doposud neřešila, a to ani okrajově. Obecně panují obavy, že stávající stupeň ochrany elektronického přenosu dat je prozatím v České republice na velice nízké úrovni.

Pokud by se v budoucnosti rozhodlo, že Česká republika zavede internetové hlasování jako doplněk k současnému systému, určitě by se vládní představitelé inspirovali již fungujícím systémem, pravděpodobně estonským.

Před řešením problematiky samotného informačního systému pro volby, je třeba analyzovat připravenost České republiky na tuto změnu. Častým argumentem proti internetovému hlasování jsou vyšší finanční náklady při zavádění tohoto nového systému. Dle kalkulací Hospodářské komory z roku 2012 by náklady vyšly zhruba na půl miliardy korun. V posuzování ceny elektronických voleb je však brát v potaz, že provozní náklady při dalších volbách by se pohybovaly kolem 25 milionů korun. Z dlouhodobého hlediska by se tedy nový systém jistě vyplatil.

Úspěšnost nového systému by se hodnotila podle jeho využívání. To je zcela závislé na důvěře českých voličů v daný informační systém. To by mohlo být v České republice problém, protože zde často státní správa zavádí systémy, které jsou nedokonalé.

Informační systém elektronických voleb by musel zajišťovat minimálně následující kritéria:

- Každý volič má jeden hlas, i přes možnou opakovanou volbu. Případné mazání duplicit by obstarával server pro správu hlasů.
- Volit smí pouze oprávněný volič, což by zajišťovala komunikace s registrem voličů.
- Anonymita volby, která by byla umožňována oddělením volebního hlasu od elektronického podpisu.
- Bezpečnost systému musí odpovídat jeho velkému významu. Systém musí zajistit, aby hlas byl zpracován tak, jak byl odeslán voličem. Musí být imunní vůči vnějším i vnitřním zásahům.
- Bezchybné sčítání hlasů s možností jejich kontroly.
- Jednoduché a intuitivní ovládání, které by umožnilo využití systému co největším počtem voličů.

Architektura informačního systému voleb by se stejně jako ostatní prvky inspirovala estonským modelem. Tato architektura umožňuje splnění některých důležitých kritérií.

Na základě získaných údajů, které byly v této bakalářské práci představeny, byla vytvořena stručná SWOT analýza, která by měla pomoci k prezentaci silných a slabých stránek, příležitostí i hrozeb, které by mohlo zavedení internetového hlasování přinést.

Silné stránky	**Slabé stránky**
▪ Rychlost zpracování výsledků ▪ Přesnost zpracování výsledků ▪ Eliminace neplatných hlasů ▪ Fungující základní registry ▪ Možnost opakování volby ▪ Zvýšení komfortu pro voliče ▪ Mobilita voličů	▪ Počáteční finanční náklady ▪ Náklady pro voliče ▪ Malá vybavenost voličů elektronickým občanským průkazem s čipem ▪ Legislativa ▪ Omezená zpětná kontrola hlasování
Příležitosti	**Hrozby**
▪ Zvýšení volební účasti ▪ Finanční úspory ▪ Možnost větší participace voličů na správě země ▪ Modernizace státní správy ▪ Zvýšení počítačové gramotnosti	▪ Závislost na bezchybném systému ▪ Zabezpečení systému ▪ Zabezpečení autentizace voliče ▪ Ovlivňování voličů ▪ Nedostatečná počítačová gramotnost voličů ▪ Digitální propast ▪ Nedůvěra v informační systémy ▪ Lehkovážnost volby

Smutnou skutečností je fakt, že politické strany, které mají na českém politickém spektru významnější roli, se nejen eVolbami, ale ani samotným eGovernmentem v podstatě nezabývají. Pro volby do Poslanecké sněmovny v roce 2013 nebyl rozvoj eGovernmentu významným bodem žádného z nabízených volebních programů. O elektronických volbách se některé strany okrajově zmiňují, pro jiné strany nebylo toto téma dostatečně zajímavé na to, aby se jím vůbec zabývaly.

S přihlédnutím k současnému stavu na politické scéně a k náladě ve společnosti, nelze v nejbližších letech počítat se zavedením elektronických voleb do českého právního řádu. V budoucnu však lze očekávat, že se o jejich zavedení bude znovu jednat.
V tom případě je velkou výhodou, že se naše republika může inspirovat úspěšnými projekty ze zahraničí a poučit se z chyb těch méně úspěšných.

6 Závěr

Bakalářská práce se zaměřila na problematiku elektronických voleb. Tento projekt je pro nás zatím znám pouze ze zahraničí, proto se práce zaměřuje na analýzu možností zavedení eVoleb v České republice.

Před analýzou stavu v České republice byly shrnuty zkušenosti ze států, které mají nebo měly eVolby ve svém právním řádu již zakotveny. Ze států, které mají s elektronickými volbami pozitivní zkušenosti, jsou uvedeny Estonsko a Švýcarsko.

Estonsko je velmocí z pohledu eGovernmentu a jeho obyvatelé mají vysokou počítačovou gramotnost, která umožňuje velké využití moderních technologií. Každý občan Estonska vlastní elektronický občanský průkaz, který umožňuje jednoznačnou identifikaci. Systém je založen na komunikaci mezi volební aplikací na straně voliče a centrálním systémem, který je tvořen třemi oddělenými servery pro zpracování hlasů a registry voličů a kandidátů. Zabezpečení anonymity je založeno na principu vnitřní a vnější obálky, z nichž každá využívá šifrování pomocí veřejného a privátního klíče. Internetové hlasování v Estonsku úspěšně funguje od roku 2005. Možnost volit přes internet využívá v současné době zhruba čtvrtina zúčastněných voličů.

Ve Švýcarsku, které je známe velkou participací občanů na správě země, se zavádění internetového hlasování rozvíjelo postupně od menších správních celků, jako jsou obce a kantony, až po celou konfederaci. Z tohoto důvodu jsou mezi volebními systémy jednotlivých kantonů menší rozdíly.

Většina projektů internetového hlasování byla však z různých důvodů zastavena. V USA bylo několik pokusů o zavedení internetového hlasování, kdy nejznámější byl systém SERVE pro volby 2004, zastaven na základě analýzy bezpečnostních analytiků. V Německu ústavní soud označil v roce 2009 elektronické volby za protiústavní. Bezpečnostní problémy zapříčinily zrušení voleb také v Nizozemí, kde protesty proti eVolbám iniciovala skupina počítačových expertů. Ve Skotsku či Francii nebyly některé hlasy dokonce započítány, ztratily se nebo je nebylo možné dešifrovat.

I přes výše zmíněné problémy lze očekávat, že se v budoucnu budou opakovat pokusy o zavedení elektronických voleb. Práce se zabývá otázkami, kterými je třeba se zabývat před spuštěním samotných eVoleb.

Rozhodujícím faktorem pro spuštění eVoleb je politická vůle. Ta se musí projevit v legislativě, která by zavedení nového systému umožňovala, a také při hledání prostředků na vyšší počáteční náklady.

Samotný informační systém eVoleb by musel zajistit rovné volební právo, tajnost volby, kontrolu oprávněnost voliče, bezchybné sčítání hlasů s možností kontroly, bezpečnost systému proti vnějším i vnitřním zásahům a jednoduché ovládání systému. Zajištění těchto základních požadavků je klíčem k možnosti spuštění projektu elektronických voleb v České republice. Architektura systému by se měla inspirovat fungujícím modelem z Estonska, která zajišťuje bezpečné zpracování hlasů s částečnou možností jejich kontroly.

Elektronické volby by přinesly zejména zvýšený komfort pro voliče, od kterého se očekává zvýšení volební účasti. Na druhé straně by jejich zavedení doprovázely hrozby ze strany bezpečnosti a jejich potenciál by tak nemusel být naplněn.

V nejbližší době se zavedení internetového hlasování v České republice nepředpokládá. V budoucnu je však možno čerpat inspiraci z úspěšných projektů v zahraničí a posunout tak eGovernment v České republice na vyšší úroveň.

7 Seznam použitých zdrojů

[1] OECD. E-Government for Better Government. Paris: OECD, 2005, str. 11., ISBN 92-64-01833-6

[2] LIDINDKÝ Vít, ŠVARCOVÁ Ivana, BUDIŠ Petr, LOEBL Zbyněk, PROCHÁZKOVÁ Barbora: eGovernment bezpečně. Praha: GRADA Publishing a.s., 2008 ISBN 978-80-247-2462-1

[3] ŠTĚDROŇ, Bohumír. 2007. Úvod do eGovernmentu v České republice: právní a technický průvodce. Praha: Úřad vlády ČR, 2007. ISBN 978-80-87041-25-3

[4] ODS. Modrá kniha. [online]. [cit. 2014-10-11]. <http://www.ods.cz/docs/publikace/modra_kniha.pdf>.

[5] ISVS. E-government – Strategické dokumenty (1. díl). [online]. [cit. 2014-10-11]. <http://www.isvs.cz/e-government-strategicke-dokumenty-1-dil/>.

[6] Rada vlády ČR pro státní informační politiku. Akční plán realizace státní informační politiky do konce roku 2002. [online]. [cit. 2014-10-11]. <http://www.earchiv.cz/down/sip/akcni_plan_realizace_SIP_do_2002.pdf>.

[7] ISVS. Ministerstvo informatiky. [online]. [cit. 2014-10-11]. <http://www.isvs.cz/ministerstvo-informatiky>

[8] Vláda České republiky. Rada vlády pro informační společnost. [online]. [cit. 2014-10-11]. <http://www.vlada.cz/cz/ppov/rvis/rada-vlady-pro-informacni-spolecnost-73372/>.

[9] MVČR. SMART ADMINISTRATION. [online]. [cit. 2014-10-20]. <http://www.smartadministration.cz>.

[10] Portál veřejné správy. Sbírka zákonů České republiky. [online]. [cit. 2014-10-20]. <https://portal.gov.cz/app/zakony/?path=/portal/obcan/>.

[11] MVČR. eGON jako symbol eGovernmentu - moderního, přátelského a efektivního úřadu. [online]. [cit. 2014-10-12]. <http://www.mvcr.cz/clanek/egon-93.aspx>.

[12] MIČR. eGovernment. Veřejná správa jako živý organizmus. [online]. [cit. 2014-10-12]. <http://www.czechpoint.cz/web/docs/eGon_brozura.pdf>.

[13]] Institut pro veřejnou správu. EGON vzdělávání. [online]. [cit. 2014-10-11]. <http://www.institutpraha.cz/egon>.

[14] MVČR. Klaudie – od správy majetku k modelu poskytování a odebírání služeb. [online]. [cit. 2014-10-12]. <http://www.mvcr.cz/clanek/klaudie-od-spravy-majetku-k-modelu-poskytovani-a-odebirani-sluzeb.aspx>

[15] Cloud Computing. [online]. [cit. 2014-10-15]. <http://www.cloudcomputing.cz/>.

[16] MARCHAL, Stanislav A., Josef PROKEŠ, Bohumír ŠTĚDROŇ a Zdeněk VANÍČEK. Právní aspekty eGovernmentu v České republice. Praha: Linde Praha, 2011, s. 200. ISBN 978-80-7201-855-0.

[17] Czech POINT. Manuál loga. [online]. [cit. 2014-10-15]. <http://www.czechpoint.cz/web/docs/071207-CzechPOINT_manual_07_12_07.pdf>

[18] Czech POINT. CzechPOINT@office. [online]. [cit. 2014-10-15]. <http://www.czechpoint.cz/web/?q=node/380>.

[19] Czech POINT. Co je Czech POINT. [online]. [cit. 2014-10-15]. <http://www.czechpoint.cz/web/?q=node/22>.

[20] Česká pošta. eShop Czech POINT. [online]. [cit. 2014-10-15]. <https://www.ceskaposta.cz/sluzby/egovernment/czechpoint/eshop-czechpoint>.

[21] MVČR. Ministerstvo vnitra spustilo CzechPOINT@home. [online]. [cit. 2014-10-15]. <http://www.egov.cz/clanky/ministerstvo-vnitra-spustilo-czechpointhome>.

[22] MVČR. Co jsou Datové schránky? [online]. [cit. 2014-10-15]. <http://www.datoveschranky.info/cz/o-datovych-schrankach/vse--co-jste-chteli-vedet-o-datovych-schrankach-id34695/>

[23] Informace o datových schránkách. [online]. [cit. 2014-10-16]. <http://www.datoveschranky.eu/>.

[24] LAPÁČEK, Jiří: Jak na datovou schránku a elektronickou komunikaci s úřady. Brno: Computer Press, 2012. s. 197. ISBN 978-80-251-3680-5

[25] MVČR. Portál datových schránek. [online]. [cit. 2014-10-16]. <https://www.mojedatovaschranka.cz/PortalDS>.

[26] Czech POINT. Autorizovaná konverze. [online]. [cit. 2014-10-16]. <http://www.czechpoint.cz/web/?q=node/362>.

[27] MVČR. Metodika Oznámení o vykonávání působností v agendě ve smyslu zákona č. 111/2009 Sb., o základních registrech. [online]. [cit. 2014-11-01]. <http://www.szrcr.cz/uploads/download/RPP_spravce/Metodika_oznameni_pusobnosti.pdf>.

[28] Egovernment. Základní registry veřejné správy. [online]. [cit. 2014-11-01]. <http://www.egovernment.cz/archiv/PDF%203-08/11.pdf>.

[29] SZRCR. Referenční údaj. [online]. [cit. 2014-11-01]. <http://www.szrcr.cz/referencni-udaj>.

[30] Institut pro veřejnou správu. Základní registry ve veřejné správě. [online]. [cit. 2014-11-01]. <http://www.zdarns.cz/egoncentrum/kurzy/zakladni_registry.pdf>.

[31] Správa základních registrů. [online]. [cit. 2014-11-01]. <http://www.szrcr.cz/>.

[32] MVČR. Komunikační infrastruktura veřejné správy. [online]. [cit. 2014-11-01]. <http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-komunikacni-infrastruktura-verejne-spravy.aspx>.

[33] ISVS. E-Government – KIVS. [online]. [cit. 2014-11-01]. <http://www.isvs.cz/e-government-kivs-6-dil/>.

[34] MVČR. CMS 2.0 Koncepce řešení a služeb. [online]. [cit. 2014-11-01]. <www.mvcr.cz/soubor/cms-2-0-koncepce-reseni-a-sluzeb-pdf.aspx>.

[35] MVČR. Informace k používání elektronického podpisu. [online]. [cit. 2014-11-01]. <http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx>.

[36] První certifikační autorita. Požadavky na zaručený a uznávaný elektronický podpis. [online]. [cit. 2014-11-01]. <http://www.ica.cz/Zaruceny-a-uznavany-ep>

[37] První certifikační autorita. Elektronický podpis. [online]. [cit. 2014-11-01]. <http://www.ica.cz/Elektronicky-podpis>

[38] Schacco. Šifrování nejen hybridní. [online]. [cit. 2014-11-15]. <http://www.schacco.savana-hosting.cz/vlastni_web/zobrazit_prispevek.php?id=70>

[39] Počet-znaků.cz. Hash. [online]. [cit. 2014-11-15]. <http://www.pocet-znaku.cz/hash>

[40] AMI. Vícefaktorová autentizace. [online]. [cit. 2014-11-15]. <http://www.ami.cz/publikujeme/blog/vicefaktorova-autentizace>

[41] Hospodářská komora České republiky. Informace o elektronickém způsobu hlasování. [online]. [cit. 2014-11-20]. <http://www.komora.cz/download.aspx?dontparse=true&FileID=8822>

[42] Petr Šindělář. Elektronické volby. [online]. [cit. 2014-11-20]. <http://www.egovernment.cz/archiv/PDF%204-06/4.pdf>

[43] Český statistický úřad. Memorandum o spolupráci při přípravě koncepce, řešení, testování a realizaci systému elektronických voleb v České republice. [online]. [cit. 2014-12-02]. <http://www.czso.cz/csu/tz.nsf/i/memorandum_o_spolupraci_mezi_csu_a_mv_cr/$File/memorandum_mv_csu.pdf>

[44] National Election Committee. E-Voting System. [online]. [cit. 2014-12-06]. <http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf>

8 Přílohy

8.1 Seznam obrázků

Obrázek č. 1 – Hexagon veřejné správy 15
Obrázek č. 2 – eGON 17
Obrázek č. 3 – logo Czech POINT 19
Obrázek č. 4 – princip šifrování volebních hlasů 38
Obrázek č. 5 – schéma estonského systému eVoleb 39
Obrázek č. 6 – schéma českého systému eVoleb 47

8.2 Seznam grafů

Graf č. 1 – struktura kontaktních míst 20
Graf č. 2 – vývoj počtu kontaktních míst 21
Graf č. 3 – vývoj počtu výstupů 22
Graf č. 4 – struktura vydaných výpisů dle kategorií 23

8.3 Seznam tabulek

Tabulka č. 1 – statistika voleb v Estonsku 40
Tabulka č. 2 – náklady na eVolby 43