Metody identifikace voliče v elektronickém volebním systému

Identification Methods of Voter in the E-voting System

Petr Vlk

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Petr VLK**
Osobní číslo:	**A09694**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**prezenční**
Téma práce:	**Metody identifikace voliče v elektronickém volebním systému**

Zásady pro vypracování:

1. **Uveďte přehled tématu elektronické volební systémy.**
2. **Zpracujte rešerši možných přístupů k identifikaci.**
3. **Stanovte hodnotící model.**
4. **Vypracujte výchozí hodnoty kriterií v modelu.**
5. **Analyzujte vhodnost jednotlivých metod dle navrženého modelu.**
6. **Popište na případové studii nejlépe hodnocený přístup.**
7. **Navrhněte novou nebo vylepšení současné metody identifikace.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KOMISE EVROPSKÝCH SPOLEČENSTVÍ. EEurope2005: Informační společnost pro všechny [online]. Brusel : Komise Evropského společenství, [2002] [cit. 2007-05-01]. Dostupný z WWW: http://www.esfcr.cz/files/clanky/1279/plan_2005.pdf.**
2. **Parlament České republiky, Poslanecká sněmovna. Ústava České republiky [online]. Praha 1 : Parlament České republiky, [cit. 2007-10-04]. Dostupný z WWW: http://www.psp.cz/docs/laws/constitution.html.**
3. **Zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů, ve znění pozdějších předpisů [online]. 2003 [cit. 2008-12-30]. Dostupný z WWW: http://www.portal.gov.cz.**
4. **ANTOŠ, Marek. Tajné hlasování za plentou jako záruka svobodných voleb versus distanční hlasování. Časopis pro právní vědu a praxi. 2007, č. 2, s. 172.**
5. **PUIGGALI, Jordi, MORALES-ROCHA, Victor. Remote Voting Schemes: A Comparative Analysis . E-Voting and Identity. 2007, no. 4869, s. 16.**

Vedoucí diplomové práce: **Ing. Radek Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **26. února 2013**

Termín odevzdání diplomové práce: **31. května 2013**

Ve Zlíně dne 26. února 2013

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Hlavním cílem diplomové práce Metody identifikace voliče v elektronickém volebním systému je navržení rozvíjejícího nebo nového systému, aby zajištěno kvalitnějšího průběhu voleb, jistějšího sčítání hlasů a snížení rizika ovlivnění voleb. Práce popisuje o historickou stránku voleb, průběh voleb. Dále jsou v práci rozepsány různé typy systémů s popisem výhod a nevýhod, na které navazuje kapitola o metodách součtů hlasů a možnostech identifikace. Praktická část je zaměřena na srovnání typického a elektronického systému. Na závěr je popsán návrh systému s jeho možnostmi a parametry.

Klíčová slova: volební hlas, elektronický volební systém, RFID čip, biometrika, identifikace

ABSTRACT

The main target of this master thesis the Identification Methods of Voter in the E-voting System is a proposal of developing or new system to provide more quality election, secure counting of votes and reduce the risk of influencing the election. The thesis describes historical election, course of election. Further, there are discuss types of election's systems with their advantage and disadvantage what continuous with chapter about methods of counting votes and the possibilities of identification. The practical part is focused on comparing of typical system with E-voting. It is finished by proposal of system and its options and parameters

Keywords: electoral vote, electronic voting system, RFID chip, biometrics, identification

Poděkování, motto

Za podporu a spolupráci děkuji svému vedoucímu Ing. Radku Šilhavému, Ph.D.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Technologie, zákony vše se neustále mění. Vyvíjí se nové programy a stroje, které člověku usnadní práci a zkvalitní výstupy procesů. Evoluce není jen v některých oblastech, jde o celý svět, který je do koloběhu poznávání zahrnut. Je trendem, že všichni potřebují mít výsledky a data ihned, nejlépe s nulovou chybovostí. Tato skutečnost se projevuje i ve volebních systémech.

Z veřejné volby před zástupem lidí, kdy každý věděl, kdo koho hlasuje, se přechází postupem času na hlasování tajné, ale jenom malou skupinou lidí z vyšších vrstev. Poslancem může být jen člověk, který má velký majetek, to proto, aby mu nešlo jen o jeho blaho a soustředil své dovednosti na zlepšení podmínek lidu. Přes všechny podmínky byl takový systém snadno zmanipulovatelný a na konci 19. století se tvoří nové zákony, které volbu zevšeobecňují, činí ji tajnou a dostupnou většímu množství voličů, kteří mají pocit, že mohou svým výběrem ovlivnit směr vývoje jejich země. V dnešní době má právo volit každý občan splňující podmínky stanovené zákonem. Pro větší pocit jistoty o ze správnosti výsledků a rychlejší výstupy jsou zaváděny elektronické systémy, které usnadňují možnost volby požadovaného kandidáta. Jde o softwarovou aplikaci, která musí být zabezpečena proti útoku z vnějšího prostředí, mít intuitivní ovládání a ukládá průběžně data. Software je podporovaný hardwarem, na který jsou uživatel zvyklý ovládat.

Elektronické volby jsou usnadněním celého procesu a snižují nákladovost spolu se zvýšením kvality vypočtených výsledků. Přesto se najdou lidé, z řad samotných programátorů, kteří systému příliš nedůvěřují. Já se snažím ve své práci najít a skloubit taková řešení, která zajistí, co nejmenší komplikace s programem. V dnešní době využití biometriky a identifikačních čipů je zajisté ovlivnění výsledků voleb při jejich sčítání pro obyčejného člověka skoro nemožné.

I. TEORETICKÁ ČÁST

1 E-VOLBY

E-volby, nebo elektronické volby („e-voting“), je možno definovat jako volby, ve kterých volební hlas vystupuje pouze v elektronické podobě. Tedy proces, ve kterém je akt volby občanem uskutečněn přímo prostřednictvím elektronického zařízení a jeho výsledek předán ke zpracování prostřednictvím elektronického přenosového media (komunikační sítě) a dále zpracováván výhradně elektronickou cestou. (Šindelář, 2009)

1.1 Modernizace v hlasování

Za celou dobu historie se hlasování potýká s nejrůznějšími problémy. Nejpalčivějšími jsou neobjektivnost, podvody při hlasování, časová náročnost, finanční náklady, technologické problémy. Postupně tak docházelo ke změnám, které měly za úkol zvýšení výkonu voleb, ukončení podvodných volebních aktů, zlevnění, zrychlení a usnadnění procesu sčítání hlasů. V 19. století odstartovala revoluce změnu ve způsobech hlasování na tištěné lístky, přes optické snímání hlasu, součty výsledků skrze mechanické sčítačky apod. (Jones, 2003; Gritzalis, 2004; Herrnson, 2008)

1.1.1 Vytištěný volební lístek

Veřejnosti byl poprvé představen v roce 1858 v Austrálii a na svou dobu byl poměrně rychle rozšířen do všech koutů světa a stal se nedílnou součástí voleb. Nejprve byla tato technika zavedena do právního řádu v Británii. Na celostátní úrovni ho ale poprvé použil v USA ve státě Massachusetts v roce 1888. Všechny kandidátní lístky měly jednotnou podobu, byly vytisknuty státem, který je rovněž distribuoval. Všichni kandidáti měli proto stejné podmínky a volby byly nestranné. Slabým místem celého systému bylo ruční počítání lístků a nešlo zabránit pokusům o změnu výsledků voleb. Ovlivnit výsledky mohly také rozdílné kritéria o posuzování platnosti hlasů. Přibližně 2 % lístku jsou u ručního sčítání hlasu vyhodnoceny špatně, kdy komise některé nesprávně označené lístky započítala mezi platné a naopak. Na tento problém upozornila americká studie ze státu New Hampshire, která zkoumala tamější volby od 70. let 20. století. Klasický způsob ručního sčítání je typický hlavně pro evropské země. V mnoha zemích naopak už na přelomu 19. a 20. století zavádějí modernější způsoby hlasování. Patří mezi ně USA, Brazílie, Austrálie, Indie a z evropských zemí Holandsko. V USA hlasování přes vytištěné

volební lístky prakticky vymizelo, za posledních 30 let klesl z podílu všech odevzdaných hlasů ze 40 % prakticky na nulu. (Tuček, 2006; Mercuri, 2002, s. 46-50)

1.1.2 Mechanická sčítačka

Prvním zásadním využitím techniky při hlasování bylo použití hlasovacího stroje, který mechanicky počítal jednotlivá hlasování. Poprvé byl použit v roce 1892 v USA ve městě New York a postupně se rozšířil po celé zemi. Jedná se prakticky o mechanickou obdobu australského volebního lístku s tím rozdílem, že volič místo házení lístku do urny svého kandidáta stiskl příslušnou páku na sčítacím stroje. Hlasování probíhalo odděleně za plentou a byl opatřen mechanismem proti opakovanému hlasování stejnou osobou. Stroj byl pochvalován za rychlost a spolehlivost při vyhodnocování odevzdaných hlasů a omezení podvodů při hlasování. Stroj byl ale natolik složitý, že jeho údržba se často zanedbávala a jeho mechanické části nikdo nekontroloval. Navíc to je poměrně velké a těžké zařízení. Došlo tak k jeho selhání při prezidentských volbách v USA v roce 2000, přesto se stroj v některých částech země stále používá. Další velkou nevýhodou mechanické sčítačky je nemožnost ověření, zda byla volba vůbec započítána a kterému kandidátovi. Ani volební komise neměla možnost odevzdané hlasy přepočítat. Tato negativa zapříčinila postupný přechod k dokonalejším systémům. V roce 1980 volilo tímto způsobem 36,4 % voličů. V roce 2008 už mechanickou sčítačku využilo jen 6,7 % voličů. (Jones, 2003; Gritzalis, 2004; Tuček, 2006; Election Data Service. Nation Sees Drop in Use of Electronic Voting Equipment, 2008)

Obrázek 1: Mechanická sčítačka *(Zdroj: Vote: The Machinery of Democracy)*

1.1.3 Optické snímání hlasů

Tato technologie přímo souvisí s rozvojem elektrotechnických zařízení a počítačů. Způsob byl představen už v roce 1950, ale dalších 20 let trvalo než byl zaveden do praxe při volbách. Při volbách se používá v USA nebo ve Velké Británii. V USA jde v současnosti nejpoužívanější způsob hlasování. V roce 2008 ho používalo více jak 56% voličů.

Každý volič obdrží hlasovací list, na kterém jsou předtištěni kandidáti. Propiskou označí předtištěná políčka u jména svého kandidáta. Obvykle křížkem nebo jeho celým vyplněním. Celý hlasovací list vloží do čtecího zařízení - skeneru, který volbu přečte a uloží do počítačového systému. (Herrnson, 2008; Reterová, 2009)

Obrázek 2: Hlasovací lístek pro skenovací zařízení (*Zdroj: Vote: The Machinery of Democracy)*

Obrázek 3: Skenovací zařízení volebních lístků (*Zdroj: Vote: The Machinery of Democracy)*

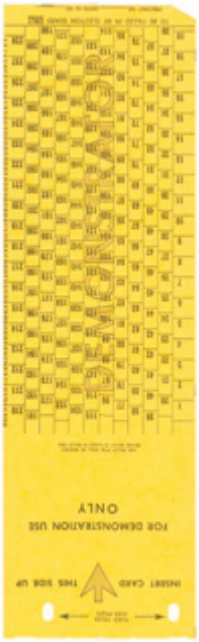
Podobné systémy známe i my a každý Čech se s nimi už setkal. V roce 2001 a 2011 proběhlo na území České republiky sčítání lidu, při kterém bylo rovněž využito optického snímání. Dále tento způsob používá společnost Sazka při podávání tipů do svých loterijních her nebo při dobíjení kreditu u mobilních operátorů. Ale ani tento způsob snímání hlasů nebyl vždy zcela bez problémů. První verze používaly snímání na bázi infračerveného světla a snímaly pouze značky vyplněné tužkou, neboli materiály na bázi

uhlíku. Dnešní snímání je už zdokonalené a používá viditelného spektra světla. Je proto schopno rozeznat běžné psací prostředky. Navíc dokáže odhalit i lístky, které jsou označeny nesprávně. Tento způsob se vyznačuje velkou spolehlivostí navíc umožňuje i zpětnou kontrolu. Pokud je volební místnost vybavena veřejnou čtečkou volebních listů, volič si může ověřit, jestli byl jeho hlas správně zpracován. Výsledky z tohoto způsobu hlasování jsou rychle dostupné.

1.1.4 Děrné štítky

Přestože byl tento systém představen až 14 let po optickém způsobu snímání hlasů, v současné době se systém děrných štítků v USA prakticky nepoužívá. Výhodou tohoto způsobu hlasování bylo jeho kompaktnější provedení. Oproti mechanické sčítačce umožňoval dodatečné přepočítání hlasů. Klasický hlasovací lístek nahradila speciální karta, na které nebyl vytištěný žádný kandidát, ale pouze kolonky, do kterých se mechanicky vytlačoval voličův hlas. K tomu sloužilo mechanické zařízení, které kartu u zvoleného kandidáta mechanicky označilo. Nevýhodou tohoto způsobu byla malá velikost karty, která vedla k problémům při velké množství kandidátů. To vedlo k malým mezerám a chybným volbám při hlasování. Karty byly špatně označeny a sčítací stroj měl problémy při vyhodnocování hlasů, kdy nebyly hlasy uznávány za platné. Na konci 20. století nastalo postupné upouštění od tohoto způsobu hlasování. Některé státy od tohoto způsobu hlasování úplně upustily. (Jones, 2003; Gritzalis, 2004; Reterová, 2009)

Obrázek 4: Děrovací zařízení (*Zdroj: Vote: The Machinery of Democracy)*



Obrázek 5: Děrný štítek (*Zdroj: Vote: The Machinery of Democracy)*

1.1.5 Přímé elektronické zaznamenání hlasů

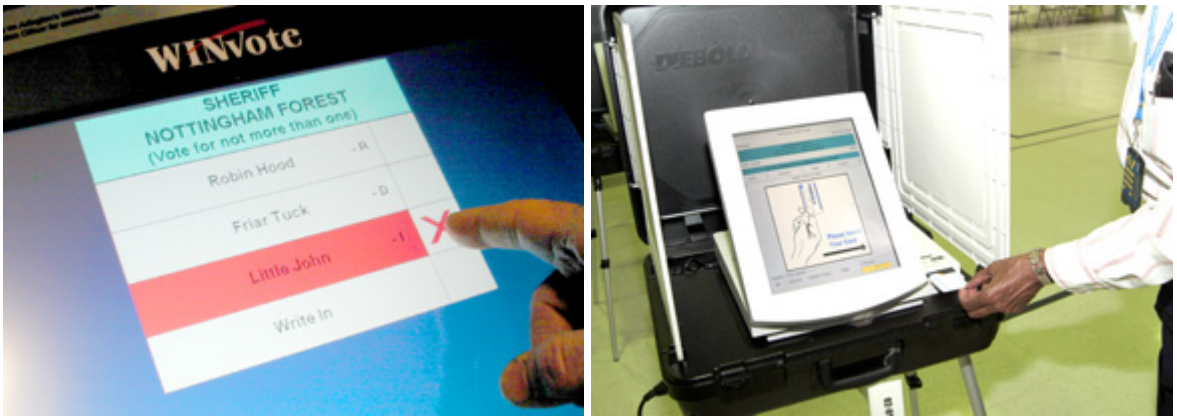
Tato technologie je dalším vývojovým stupněm při přechodu od mechanického nebo polomechanického k čistě elektronickému. Tento systém nepoužívá žádného papírového hlasovacího lístku. Takový způsob už se v minulosti objevil v podobě mechanické sčítačky, která je už dneska hodnocena jako značně nespolehlivou.

Moderní systém používá integrované obvody a speciální software. Zjednodušeně řečeno se jedná o počítač umístěný ve volební místnosti, ve kterém jsou uloženy údaje o kandidátech a politických stranách. Volič si u volebního počítače vybere svého kandidáta, označí ho a zvolený hlas se uloží. I tento způsob se postupně modernizuje podle technických možností. Původní systémy se ovládaly pomocí manuálních kláves, které odpovídaly vybranému kandidátovi. Volební systémy na počítačové bázi mají výhodu v tom, že mohou být opatřeny například dotykovou obrazovkou, která dále zpřehlední a zjednoduší volební akt. Případně může být systém opatřen přídavným zařízením, které umožní pohodlnou volbu i osobám tělesně a zdravotně postiženým. Nakonec následuje potvrzení

vykonané volby. Tento způsob patří k nejrychlejším a nejúčinnějším při zpracování výsledků. V současné době se používá v Holandsku, Belgii, Irsku, Velké Británii, Německu v USA a Brazílii. (Herrnson, 2008; Reterová, 2009)

Vzhledem k tomu, že hlasování tímto způsobem probíhá čistě elektronicky, neexistují záznamy o provedení hlasování. Za určitých podmínek by mohlo snadno dojít k ovlivnění volebních výsledků. Volební výsledky mohou být ovlivněny i kvůli technické závadě nebo softwarové chybě. K jedné takové chybě došlo v roce 2002 v USA ve státě Nové Mexiko, kdy v jednom okrsku zaregistrovali o 12 tisíc hlasů méně, než kolik občanů přišlo k volbám. (Tuček, 2006)

Tento způsob hlasování má ale i svá negativa. Samotná volba může být značně zdlouhavá. Kvůli identifikaci, vybrání svého kandidáta trvá průměrně 2 minuty. Mohou nastávat situace, kdy se doba může značně protáhnout, například při vyplňování preferenčních hlasů. Zařízení je také poměrně drahé, a proto se nedá předpokládat nasazení nadbytečnému počtu hlasovacích zařízení v každé volební místnosti.



Obrázek 6: DRE elektronické hlasovací zařízení (*Zdroj: Vote: The Machinery of Democracy)*

1.1.6 Dodatečné způsoby hlasování

Ke standardním hlasovacím způsobům existují v některých zemích i paralelní systémy hlasování. Již v minulosti byla snaha zavedení možnosti hlasovat i v případě, že se volič nezdržoval v místě svého trvalého bydliště. Vzhledem k technickým omezením to nebylo možné. Nakonec se ale vymyslel způsob, jak by bylo možné hlasovat pomocí služeb poštovních úřadů. Tento způsob je označován jako korespondenční způsob hlasování. Volič odešle úřadu v obálce volební lístek se jménem svého kandidáta nebo politické

strany. Aby byla zajištěna bezpečnost tohoto způsobu hlasování, dostane volič při korespondenčním hlasování volební materiály, kandidátky a 3 obálky. Ty slouží k zajištění tajnosti hlasování. Do první se obálky se vloží hlasovací lístek s vybraným kandidátem, do druhé obálky se vloží čestné prohlášení, že volič hlasoval osobně a v souladu s ústavou ČR a ve třetí obálce je pošle úřadu. Volební komisař po otevření obálky zkontroluje údaje o voliči, zapíše do zvláštního volebního seznamu a vhodí neotevřenou obálku do volební urny. Dále se postupuje klasickým sčítáním papírových volebních lístků. V ČR je možnost volit tímto způsobem teprve od roku 2009 do Poslanecké sněmovny a Senátu.

V zahraničí se korespondenční hlasování objevilo už roku 1981. V USA ve státě Oregon uzákonili tento způsob pro místní volby. Korespondenční volby se v Oregonu rychle ujaly a oblíbily. Přinesly úsporu nákladů za platy volebních komisařů. Zároveň zaznamenali zvýšení účasti při volbách cca o 10 %.

1.2 E-volby ve světě

První použití se datuje do 70. let 20. století, kdy se začaly používat děrné štítky. Více se rozšířily při prezidentských volbách ve Spojených státech amerických v roce 1964, kdy je použilo 7 států unie. Novější technologie optického snímání se rozšířila kromě Spojených států amerických taky v Brazílii, Indii, Venezuele a Nizozemí. V posledním jmenovaném státě však od tohoto systému upustili. Existují i hybridní systémy hlasovacích a sčítacích systémů, které kombinují nejmodernější technologie (hlasovací stroje, dotykové obrazovky apod.) s klasickým systémem, umístěné v hlasovací místnosti. Identifikace a ověření voliče probíhá standardním způsobem. Primární volby Demokratické strany v Arkansasu v roce 2000 byly jedním z prvních pokusů. Dále probíhaly např. V roce 2002 ve Velké Británii, kde měli voliči možnost hlasovat skrze terminál, zasláním SMS nebo přes digitální TV. (Novotný, 2009)

Rada Evropy vydala v roce 2004 doporučení členským státům k začlenění e-volebních systémů do národních volebních legislativ. Následně Evropská komise začala řešit koncept voleb pro volby do Evropského parlamentu roku 2009, který se týkal zhruba 450 mil. voličů. (Šindelář, 2009)

Nejnovější systémy hlasování na dálku se v současnosti používají v Estonsku, Velké Británii, Itálii nebo ve Švýcarsku. Estonsko je zemí, která zavedla elektronické hlasování jako oficiální možnost. Ve Spojených státech amerických, Kanadě nebo Francii se elektronická zařízení využívají i při lokálních volbách. (Novotný, 2009; Šindelář, 2009)

1.2.1 E-volby ve Spojených státech amerických

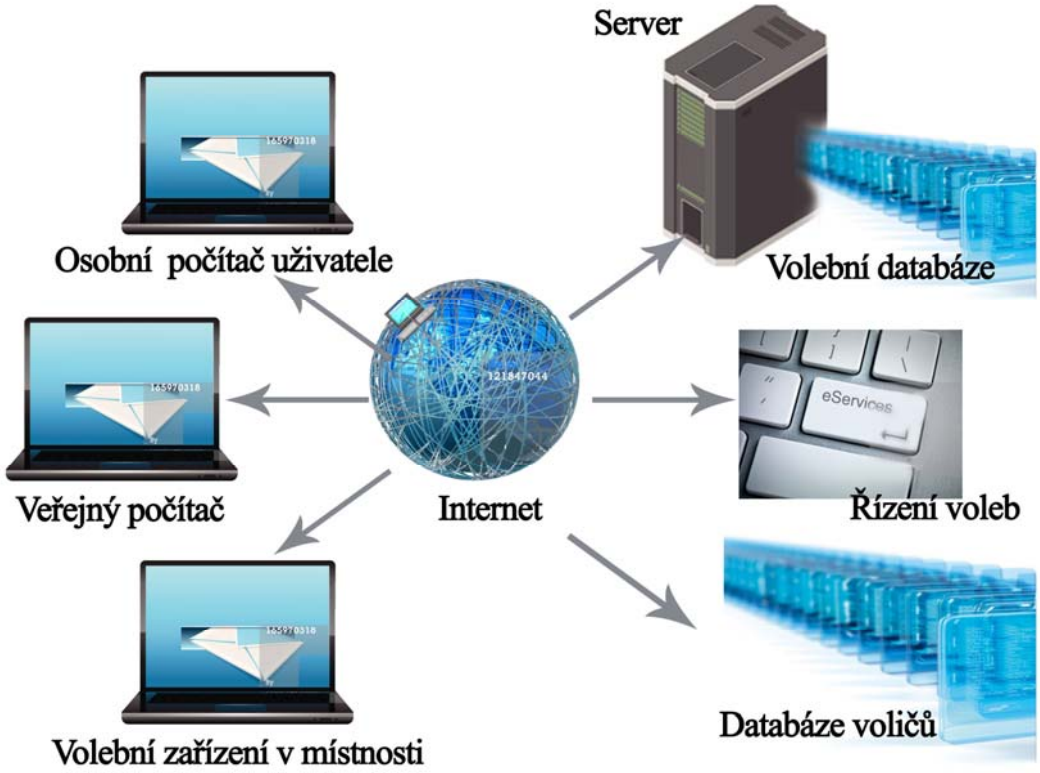
V roce 2000 usilovaly Spojené státy americké o volbu skrze internet. Prezidentské volby na Aljašce a v Arizoně byly uskutečněny elektronicky přes internet, spolu s tradičními volebními okrsky a poštovní volbou. Následně v listopadu 2000 bylo umožněno hlasovat vojenskému personálu a voličům ze zámoří za použití internetu. Projekt *volba přes internet* (Voting over Internet – VOI) byl sponzorován Federal Voting Assistance Program - americkým ministerstvem obrany. (Alvarez a Hall, 2004) Téhož roku bylo umožněno volit i na Floridě, kde nastaly problémy s voličskými seznamy. (http://blisty.cz/art/43622.html)

Další rozvoj e-voleb stagnoval. Projekt HAVA 2002 (The Help America Vote Act) byl zaměřen na rozšíření elektronických hlasovacích strojů po Spojených státech amerických. Výsledkem byl celostátní technologický „převrat“ téměř během noci, jak uvádí studie EVEREST. (Butler, 2007)

Teprve až v roce 2004 byl využit internet jako jedna z metod pro volbu do michiganských prezidentských voleb. Nicméně SERVE projekt (Secure Electronic Registration and Voting Experiment) založený na úspěšném VOI, byl pozastaven pro argumenty nedostatečné bezpečnosti volby přes internet ze strany studentů počítačové bezpečnosti. Na základě této události nastalo politicky nepříznivé prostředí pro rozvoj a návrhy inovované internetové volby, vše se dělo kvůli problémům s „ukradenými“ volebními přístroji ve státě Ohio. Zájem ze strany armádních příslušníků a voličů ze zámoří přesto nezmizel. Alabama a Floridě provedla zkušební volbu za podpory projektem UOCAVA – Uniformed and Overseas Citizen Absentee Voting Act, která byl primárně určena pro armádní osoby, které se nacházejí například v Iráku nebo Afgánistánu. V roce 2008 proběhly elektronické volby v USA ve státech Virginia, Tenessee a Texas, kde opět nastaly problémy s výběrem volebních hlasů v testovací verzi a měnily se ve prospěch jednoho z kandidátů. Dále bylo v Califorinii počítačovou chybou vymazáno 197 hlasů. (Ridvanová, 2010; Grossman, 2009)

Ohio je dalším státem USA, které využívá 2 typy zařízení: DRE (Direct Recording Electronic) a OS (Optical Scan). Dle ADA standardů musí být umožněno volit i postiženým voličům. (Husted, 2012)

Registrační systém projektu UOCAVA provozuje stát a obsahuje informace o oprávněných voličích. Data o voliči mají různé zdroje, může jít o záznamy z oddělení motorových vozidel, soudů apod. Právní úřad pak může zmíněné informace využít pro ověření oprávněnosti hlasovat a dovoluje „vhození" jednoho lístku na občana.



Obrázek 7: Systém UOCAVA *(Zdroj: Vlastní tvorba)*

Identifikace voliče ve volební místnosti

Ve volební místnosti je občan kontrolován komisí a může být požádán, aby se identifikoval. Pro ověření identity slouží:

1. Podpis
2. Identifikační karta (zejména pro vládní a vojenské osoby)
3. Řidičský průkaz

Identifikace voliče na internetu

Před samotnou volbou státy USA vyžadují ověření registrace, a to osobně nebo poštou. Pro ověření identity při vstupu na hlasovací stránky slouží:

1. Digitální podpis

1.2.2 E-volby v Estonsku

Estonsko je průkopníkem e Govermentu a nejrozvinutější zemí bývalého východního bloku. Zákon o elektronických volbách byl schválen v roce 2002 a poprvé mohli Estonci volit do komunálních voleb v roce 2005. Při parlamentních volbách v roce 2011 bylo přes internet odevzdáno 24,3 % hlasů. (Šindelář, 2009; (Estonian e-voting systém,2011; Tajtl, 2012)

Hlasování probíhá na webových stránkách určených k volbě, které jsou zabezpečené protokolem HTTPS.

Identifikace ve volební místnosti

Při identifikaci voliče je nutné předložit některý z estonských identifikačních dokumentů:

- ID karta,
- cestovní pas,
- diplomatický pas,
- námořnická knížka,
- vojenská knížka,
- řidičský průkaz,
- průkaz penzisty.

Poté volební komise zkontroluje jméno, datum narození, osobní identifikační kód, fotografii a podpis. Pokud se vše shoduje, obdrží volič od volební komise hlasovací lístek. (Voting in Polling Division of Residence, 2011)

Identifikace na internetu

Pro identifikaci na internetu je nezbytné mít ID kartu a znát příslušné PIN kódy. Dále je potřeba být u počítače s připojením na internet. Nezbytná je i čtečka čipových karet.

Etapy hlasování:

1. Vložení ID kartu do čtečky karet
2. Otevření hlasovací stránky Národního volebního výboru (www.valimised.ee)
3. Stažení volební aplikaci
4. Po spuštění uživatel musí zadat PIN 1 kód
5. Zobrazení seznam kandidátů ve volebním obvodu voliče na monitoru
6. Zadání volby jednoho nebo více kandidátů, je-li to přípustné
7. Potvrzení volby digitálním podpisem a zadáním PIN 2 kódu
8. Zobrazení potvrzení, že volba proběhla v pořádku (Internet Voting in Estonia, 2011)

Občan se přihlásí pomocí eID (elektronického občanského průkazu s jednotným charakteristickým přihlašovacím údajem – single sign on), který má v sobě zabudovaný čip se dvěma certifikáty, jeden pro podepisování a druhý pro identifikaci. Pro přístup ke službám a volbám je nezbytná čtečka karet nebo využívat službu Mobile-ID (speciální SIM karta pro mobilní telefon). Volič není omezen aktuální pozicí, hlasuje prostřednictvím jakéhokoliv soukromého počítače, který je připojen k internetu nebo z knihovny, která je standardně vybavena i čtečkami. (Tajtl, 2012; Ješuta, 2012; Estonsko: První internetové volby na světě, 2007; Estonci spustili revoluční volby po internetu, 2007)

Identifikace pomocí mobilního telefonu

1. Volič otevře speciální webovou stránku.
2. Na webové straně se vyplní číslo mobilního telefonu, na které voliči přijde kontrolní kód v SMS zprávě.
3. Volič sám sebe identifikuje pomocí zadání PIN 1 kódu do jeho mobilního telefonu.
4. Voliči se na monitoru zobrazí seznam kandidátů z okrsku jeho bydliště.

5. Volič zadá svoji volbu, která je zašifrovaná. Kontrolní kód je znova zaslán na voličův mobilní telefon v SMS zprávě.
6. Volič potvrdí svoji volbu digitální podpisem a zadá PIN 2 kód na svém mobilním telefonu.
7. Voliči se zobrazí potvrzení na monitoru počítače, že jeho volba byla přijata.

V roce 2011 nebylo možné volit pouze skrze mobilní telefon. Počítač s internetovým připojením byl nezbytný pro zadání digitálního podpisu z obdržené SMS na SIM se službou Mobile-ID. Dále je umožněna nerozhodným voličům opakovaná volba, kdy je předchozí volba zrušena. V případě, že si občan není jistý zadanou volbou, zda byla správně zpracována, má možnost se dostavit k volební komisi a svůj hlas zadat použitím papírového hlasovacího lístku a opět bude jeho elektronický hlas zrušen. (Internet Voting in Estonia , 2011)

Architektura systému se skládá z:

- volební aplikace,
- správa generování klíčů,
- centrální systém,
  - síťový (webový) server,
  - server pro uložení hlasů,
  - sčítací server,
- audit. (Internet Voting in Estonia , 2011)

Estonsko je průkopníkem e Govermentu a nejrozvinutější zemí bývalého východního bloku. Zákon a elektronických volbách byl schválen v roce 2002 a poprvé mohli Estonci volit do komunálních voleb v roce 2005. Při parlamentních volbách v roce 2011 bylo přes internet odevzdáno 24,3 % hlasů. (Šindelář, 2009; Estonian e-voting systém, 2012; Tajtl, 2012)

Hlasování probíhá na webových stránkách určených k volbě, které jsou zabezpečené protokolem HTTPS. Občan se přihlásí pomocí eID (elektronického občanského průkazu s jednotným charakteristickým přihlašovacím údajem – single sign on), který má v sobě zabudovaný čip se dvěma certifikáty, jeden pro podepisování a druhý pro identifikaci. Pro

přístup ke službám a volbám je nezbytná čtečka karet nebo využívat službu Mobile-ID (speciální SIM karta pro mobilní telefon). Volič není omezen aktuální pozicí, hlasuje prostřednictvím jakéhokoliv soukromého počítače, který je připojen k internetu nebo z knihovny, která je standardně vybavena i čtečkami. (Tajtl, 2012; Ješuta, 2012; Estonsko: První internetové volby na světě, 2007; Estonci spustili revoluční volby po internetu, 2007)

Před rokem 2011 nebylo možné volit pouze skrze mobilní telefon. Počítač s internetovým připojením byl nezbytný pro zadání digitálního podpisu z obdržené SMS na SIM se službou Mobile-ID nyní je vše jinak. Dále je umožněna nerozhodným voličům opakovaná volba, kdy je předchozí volba zrušena. V případě, že si občan není jistý zadanou volbou, zda byla správně zpracována, má možnost se dostavit k volební komisi a svůj hlas zadat použitím papírového hlasovacího lístku a opět bude jeho elektronický hlas zrušen.

1.2.3 E-volby ve Španělsku

První pilotní projekty pro elektronické volby byly spuštěny už v roce 1995, kdy byla ve volební místnosti instalována elektronická zařízení pro výběr kandidáta. Nezávazná volba do parlamentu Katalánska skrze internet proběhla v roce 2003. Katalánci v počtu 24 000, žijící v zahraniční, měli možnost volby do Parlamentu přes internet. Této možnosti využilo 730 občanů. Hlasy mohly být odevzdány prostřednictvím:

- internetu,
- mobilního telefonu s podporou Java,
- mobilního telefon přes SMS,
- papírového hlasovacího lístku.

Ke správné identifikaci slouží vygenerovaný 16 místný PIN pro každého občana, aniž by byly k PIN kódu přiřazené osobní údaje. PIN v uzavřené obálce je spolu se stručnými pokyny a pozvánkou k volbám zaslán občanovi 15 dní před samotnými volbami.

Elektronická platforma, vyvinutá společností Scytl, umožňuje volit z kteréhokoliv počítače s připojením k Internetu a jednoduchou navigací, podporující Javu. Java je nezbytná pro zajištění bezpečnosti a důvěryhodnosti, tedy základních požadavků na systém elektronických voleb. Při hlasování volič postupuje podle jednoduchého návodu na webových stránkách. Po přihlášení se identifikuje a zadá svoji volbu, která je následně v dalším okně potvrzena. Celý proces trvá jenom pár sekund.

Identifikace na internetu a průběh volby

1. Identifikace před samotnou volbou pomocí ověřovacích listin a 16 místného PIN
2. Načtení hlasovacího lístku
3. Výběr kandidáta
4. Odeslání vyplněného hlasovacího lístku
5. Obdržení ověření o úspěšné volbě (Šindelář, 2009)

1.2.4 E-volby ve Švýcarsku

Ve Švýcarsku je politický systém silně navázán na rozhodování voličů o důležitých otázkách formou referend. Komfort voliče je pro účast klíčový a politická reprezentace se začala zabývat zvýšením volební účasti. Prvním řešením byly poštovní volby, které byly v roce 1995 uzákoněny. Po jejich zavedení bylo 95 % hlasů doručeno poštou a volební účast se zvedla o 20 %.

V roce 2000 začal kanton Geneve prostřednictvím své rozpočtové organizace s pilotním projektem e-voleb, ve které pokračoval od roku 2001 ve spolupráci s Hewlett-Packard a Wiseley. Průzkum v roce 2003 ukázal, že 72% obyvatel požaduje inovaci voleb, a to on-line odevzdání hlasu.

První e-volby tak proběhly ještě v témže roce a zhruba 22 % voličů vyzkoušelo volbu on-line. Celková účast se zvýšila o 13 %. Následující rok bylo on-line odevzdáno více než 50 % hlasů. Celkem šest osob se pokusilo volit dvakrát (přes internet a současně poštou), kteří byli následně upozorněni dopisem na možnost právních sankcí. (Šindelář, 2009)

Identifikace voliče a průběh volby

V první fázi švýcarští registrovaní voliči obdrželi jejich voličskou kartu a volební materiály poštou před každými volbami a referendem. Kartu bylo možné využít při hlasování ve volební místnosti nebo byla odeslána spolu s papírovým hlasovacím lístkem poštou. Občané, kteří chtěli uskutečnit volbu elektronicky, se přihlásili přes webový server do elektronického volebního systému, kde zadali číslo jejich voličské karty. Po ověření měli umožněno zadat hlas a následně potvrdit.

Inovace výše uvedeného systému v dalších letech vedla k vytvoření systému, podobnému internetovému bankovnictví. Občan kantonu obdržel identifikační kartu, heslo

a vygenerovaný konstantní symbol, což mu zajistilo přístup do různých systémů kantonu. Mezi přístupné systémy pro občana patřila i elektronická volba. Před každou volbou byl občanovi vygenerován přídavný (specifický) kód, který mu dovolil „vhodit“ elektronický hlasovací lístek do systému.

1.2.5 E-volby v Norsku

V roce 2004 byla v Norsku ustanovena pracovní skupina řešící implementaci e-voleb do volebního systému Norska. Ministerstvo pro místní vládu a regionální rozvoj zahájilo v roce 2008 projekt „E-elections 2011“. Volby proběhly na různých místech a bylo zaregistrováno celkem 200 000 voličů. Do komunálních voleb 26,4 % voličů využilo internet a do krajských šlo o 26,97 % voličů z volebního seznamu.

Autentifikace probíhlala pomocí MinID Portalu, který slouží jako single-sign-on pro norské služby veřejného sektoru. Každý Nor vedený v národním registru si může od 13 roku věku vytvořit své ID. Ověřování probíhá pomocí PIN kódu a hesla, které jsou odeslány poštou na trvalé bydliště občana.

Norsko implementovalo do voleb i možnost zpětného ověření zadané volby. Vše začíná již při tvorbě volebních lístků. Každý lístek je tvořen pro konkrétního voliče a obsahuje unikátní kódy pro jednotlivé možnosti u kandidátů. Při odeslání pak systém propojí přes bezpečný výpočet voličovo ID s kódy stran a přes externí SMS bránu mu je zašle. Volič si porovnáním obdržených kódů ověří, zda systém započetl voličův hlas správně.

Norům záleží na otevřenosti a transparentnosti, proto byl dozor nad e- volbami zadán organizaci OSCE/ODHIR.

Architektura systému se skládá z několika domén:

- doména administrace,
- doména e-voting,
- doména sčítání papírových hlasů,
- bezpečností architektura,
- doména audit. (Ješuta, 2012)

1.3 E-volby v ČR

Elektronické volby začalo ministerstvo vnitra společně s Českým statistickým úřadem (ČSÚ) připravovat už loni. Tehdejší ministr vnitra Langer a předseda ČSÚ Jan Fischer v dubnu 2008 podepsali memorandum o přípravě koncepce, testování a realizaci systému elektronických voleb. Předpokladem je především spolehlivý systém zabezpečení, který zabrání dvojitému hlasování. Občanští demokraté elektronické hlasování představili jako součást svého volebního programu. Jde podle nich o jeden z bodů, kde se nechali inspirovali veřejností.

Tehdejší ministr vnitra Ivan Langer (ODS) si od elektronické volby slibuje aktivnější zapojení občanů do voleb, zrychlení sčítání hlasů, zjednodušení administrativy a úsporu nákladů. Snaží se tak zaujmout mladé voliče. (ODS chce volby přes internet. ČSSD návrh podpořila, 2009)

2 VOLEBNÍ ZAŘÍZENÍ

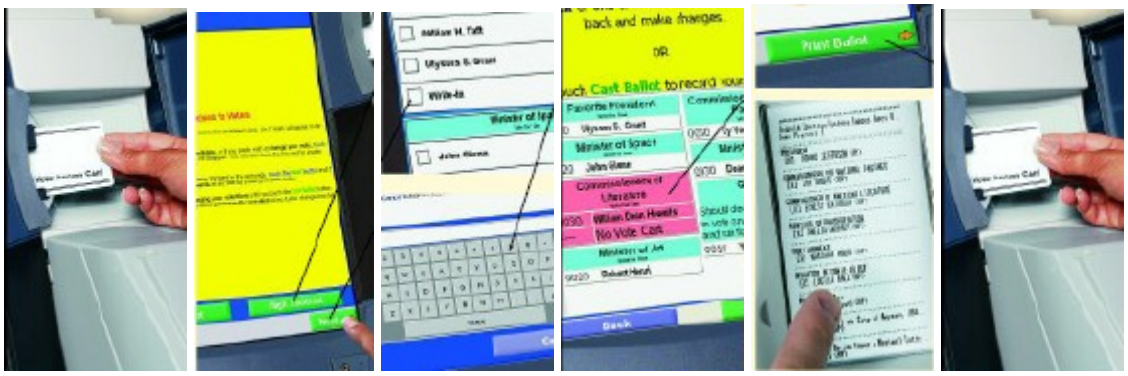
Mezi nejznámější a nejvyužívanější systémy v USA, které se řadí do přímého elektronického zaznamenávání hlasů (viz kapitola 1.1.1) patří:

2.1 Premier Elections Solutions (dříve Diebold Elections Systems)

Diebod AccuVote-TS a TSx jsou nejčastějšími přístroji využívaných při volbách. V roce 2006 bylo zařízení využito v 385 států (od Marylandu až do Georgie) a odvolilo elektronicky 10% registrovaných voličů. (Election Data Services, 2006)

Obrázek 8: Volební zařízení Diebod AccuVote-TS *(Zdroj: Scoop News)*

2.1.1 Postup volby



1. Vložení přístupové karty
2. Instrukce a nastavení čitelnosti

3. Výběr kandidáta nebo vepsání jména kandidáta
4. Grafické zobrazení správnosti volby
5. Vytisknutí lístku pro kontrolu
6. Vhození lístku do elektronické urny
7. Vyjmutí karty a navrácení členům volební komise (Voting Machines, 2012)

2.1.2 Výhody a nevýhody systému

Počítačoví experti jsou skeptičtí k systémům typu DRE (Direct Recording Electronic). Je mimořádně obtížné zabezpečit spolehlivost a bezpečnost komplexního softwaru nebo detekovat a diagnostikovat problémy, které mohou nastat. Odborníci jako Kohno, Stubblefield, Rubin, Walllach zkoumali část zdrojového kódu pro zařízení Diebold a objevili mnoho chyba zranitelností. Problém může nastat při aktualizaci systému, který není dostatečně chráněn proti záměrnému poškození útočnou stranou.

Zásadní pochybení v softwaru pro elektronické volby:

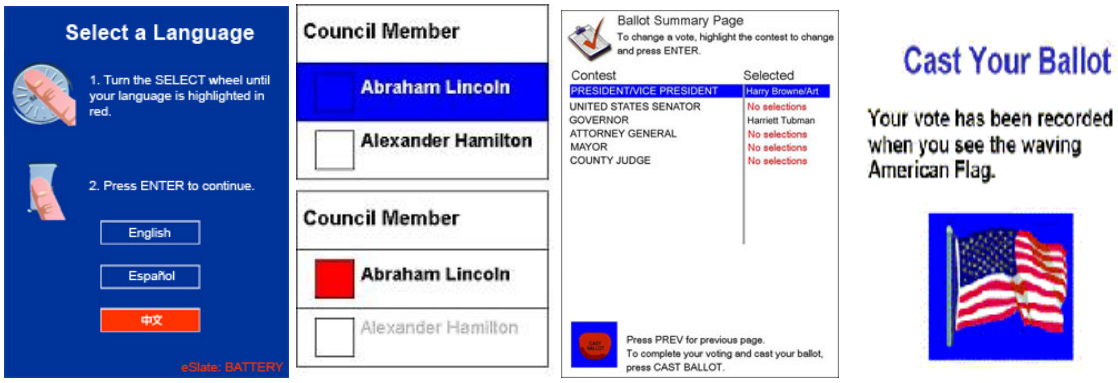
- Malware spuštěný na jednom volebním zařízení může „krást“ hlasy s malým rizikem odhalení. Zároveň můžou být změněna uložená data, deníky auditu nebo samotná počítadla, tudíž ani při pečlivém zkoumání nemusí být z takových záznamů detekována chyba.
- Kdokoliv s přístupem k volebnímu zařízení nebo příslušenství, které má být použito při volbách (např. paměťová karta) může zajistit instalaci malwaru, která trvá sotva minutu.
- Diebold zařízení je náchylné na počítačové viry, které se můžou šířit automaticky a nepozorovaně mezi přístroji před a po volební údržbě aniž by byly síťově připojeny. (Feldman, 2007)

2.2 Hart InterCivic (H-I)

O jaký jde systém – Volební přístroje využívané zejména ve státě Ohio. Pracují na operačním systému Windows. Dle Ohio SoS site, jsou přístroje používány v oblastech, Williams a Hamilton. (Mace, 2012)

2.2.1 Postup volby

Jde o bezdotykovou obrazovku, která je ovládána otočným tlačítkem pro výběr požadované položky a následné potvrzení tlačítkem Enter.



1. Nastavení jazyka a zadání vygenerovaného 4 místného kódu
2. Výběr požadované strany či kandidáta
3. Kontrola vyplněného lístku
4. Vhození lístku do elektronické urny

2.2.2 Výhody a nevýhody

Tým testující bezpečnost systému zařízení byl schopen „prolomit“ přístup k uzamčené paměťové kartě a použil ruční zařízení k načtení falešného hlasu do systému. Týmu se podařilo instalovat maligní software do serverů. (Brawley, 2012)

Negativní vliv na volební zařízení mohou mít také přístroje, které mají lidé běžně při sobě, ať už se jedná o magnety, PDA nebo iPady. (Anderson, 2007)

Obrázek 9: Volební zařízení Hart InterCivic *(Zdroj: Austinchronicle.com)*

Útočník kombinuje nové a dříve známé chyby, aby prolomil ochranu systému. (Butler, 2007) Je snadné nahradit firmware během vteřiny díky neomezenému přístupu k volebnímu zařízení.

2.3 Sequoia Voting Systems

Sequoia volební systémy jsou vlastněny a řízeny americkým poskytovatelem se sídlem v Denveru, Colorado. Výrobce uvádí stoleté zkušenosti v poskytování přesného, spolehlivého a inovativního hlasování. Zařízení obsahuje komplexní volební systém, skenovací jednotku a tiskárnu.

Obrázek 10: Sequoia hlasovací zařízení *(Zdroj: coe.berkeley.edu)*

2.3.1 Postup volby

1. Aktivace volebního lístku
2. Volba
3. Kontrola a tisk
4. Vhození volebního lístku (Voting Machines, 2012)

2.3.2 Výhody a nevýhody systémů

Volby v Palm Beach 2012 vyžadovaly ruční přepočet hlasů, při kterém byla zjištěna ztráta odevzdaných hlasů. Vědci označují Sequoia system za zranitelný a snadno nabouratelný, kdy mohou být ovlivněny výsledky voleb při zásahu do firmwaru. (Canning, 2013) Voliči se pak odvolený kandidát objeví na kontrolním lístku, ale po odchodu od zařízení může být dokončen proces volby, kdy vyjede nový lístek, na kterém je jiný než vybraný kandidát a tento hlas je započten. Volba probíhá relativně krátkou dobu, po zvolení požadovaných kandidátů je vytištěn kontrolní lístek. Lístek s volbou je uschován pro potřebu ručního přepočítání.

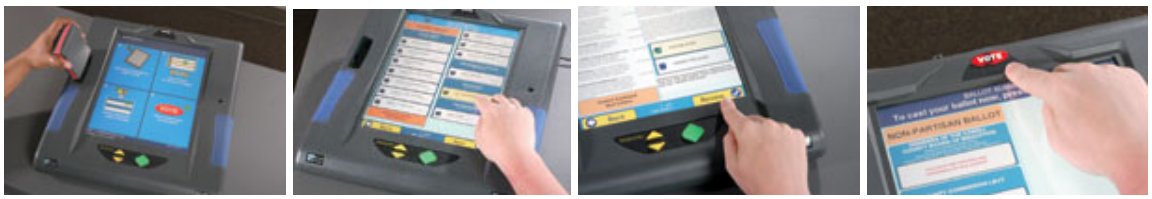
Systém je opět relativně snadno napadnutelný. Po odjištění zadního krytu zařízení, je možné zasunout vlastní datový nosič s malwarem, který ovlivňuje po potvrzení volby odevzdaný hlas.

2.4 Election Systems and Software (ES&S)

Zařízení pro volbu a sčítání hlasů je opět ovládáno dotykem. Občan je v případě pochybení upozorněn na nestandardní postup (např. pokud by chtěl volit vícekrát nebo by nezkontroloval zadané údaje) během ověřovaní zadaného výběru.

Přístroj je vybaven třemi nezávislými úložišti, které zabraňují ztrátě odevzdaného hlasu. Data jsou zaznamenávána na papírovou pásku. Porucha jednoho přístroje tím pádem neovlivní funkčnost ostatních.

2.4.1 Postup volby



1. Aktivace lístku jeho zasunutím do přístroje
2. Výběr kandidáta
3. Kontrola lístku
4. Vhození lístku do elektronické urny (Voting Machines, 2012)

2.4.2 Výhody a nevýhody systémů

Zamrznutí systému v průběhu voleb nebylo evidováno v systémových zápisech, dokonce ani řada normálních nebo abnormálních chyb nebyla nikde evidována a chyběla v záznamu. Nezapočtení hlasu do centrální databáze bylo další chybou systému. (Election systems and software unity 3.2.0.0., 2011)

3 TYPY E-VOLEB

Z pohledu provedení je možno e-volby je v zásadě rozdělit do tří skupin:

1) První skupinu tvoří volby provedené v přesně definovaném čase prostřednictvím zákonem *definovaného* elektronického zařízení umístěném v zákonem definovaném místě (volební místnosti). Tato skupina řešení je zpravidla označovaná jako „**poll-site electronic voting**“.
2) Druhou skupinu tvoří volby provedené v přesně definovaném čase prostřednictvím *libovolného* elektronického zařízení, splňujícího pouze technické požadavky kompatibility se zvolených volebním systémem, umístěným v libovolném místě planety s nutnou dostupností komunikačního prostředí. Tato skupina řešení je zpravidla označovaná jako „**remote electronic voting**“, v terminologii užívané EU jako „i-voting“ nebo českým ekvivalentem „i-volby“. (Šindelář, 2006)
3) Podle Bungala a Sridhara (2003) existuje třetí skupina – „**kiosk voting**“. Volební zařízení může být umístěno mimo volební místnost. Vhodným místem může být knihovna, nákupní centrum nebo škola. Volební platforma může být stále pod kontrolou, fyzické prostření může být sledováno a modifikováno dle potřeby.

3.1 Poll-site electronic voting

Arkansas, Georgia, New Jersey, Minnesota, Utah

Mezi klasickým systémem, který je doposud využíván, je hlavním rozdílem forma volebního lístku. Místo papírového nosiče hlasu je využit lístek elektronický, který je zpřístupněn elektronickým zařízením v místě volby.

Identifikace a autentizace jsou ověřeny komisí ve volební místnosti. Pro volbu kandidáta či strany je použito DRE (Direct Recording Electronic) volebního terminálu s dotykovou obrazovkou. Na displeji je zobrazen hlasovací lístek , který je po volbě voliče uložen do elektronické volební urny a po uzavření volebních místností dále elektronicky zpracován. (Šindelář, 2006)

3.1.1 Výhody poll-site e-voting

Elektronická volba představuje nespočet výhod oproti papírové formě, a to:

- rychlost a přesnost při vyhodnocení hlasů,
- dostupnost pro nevidomé a zrakově postižené voliče,
- rozmanitost v designu a úpravě volebního lístku,
- prevence nedobrovolných chyb při hlasování (neplatné hlasy, cizí předměty, prázdné obálky),
- jednoduchá obsluha pro voliče,
- více jazyčné rozhraní pro voliče. (Rivest, 2000)

Všechny výše zmíněné výhody s sebou nesou nižší náklady na voliče než u klasického systému s papírovými volebními lístky. Současně systém vede k vyšší účasti na volbách a splnění občanské povinnosti.

3.1.2 Nevýhody poll-site e-voting

Systém poll-site e-voting je velice podobný klasickému systému voleb, proto s sebou nese i rizika, nevýhody a diskomfort. Mohou být zmíněna:

- nemožnost volit mimo definované místo,
- nemožnost volit bez voličského průkazu,
- nemožnost opravy hlasu,
- nemožnost kontroly voliče, zda byl jeho hlas započítán správně,
- časová náročnost. (Šindelář, 2006)

3.2 Remote electronic voting

Aljaška, Arizona, Estonsko, Nizozemí, Švýcarsko, Velká Británie

Tato metoda byla použita v roce 2000 na Aljašce, v Arizoně. Uskutečnění volby je závislé na běžné dostupnosti k internetu, počítač a standardní operační systém a software. Volební systém umožňuje volit skrze PC, mobilní telefon, PDA s připojením k internetu, přes webové rozhraní, a to všude tam, kde dosahuje signál internetu – doma, z práce, dovolené. Hlasy od voliče jsou zaslány do volebního systému pomocí veřejné sítě. Největší výhodou je pohodlí občana. Bezpečnostní požadavky jsou řešeny kryptografickými metodami. (Rubin, 2002; Rosland, 2004)

Volič se musí nejdříve zaregistrovat do databáze voličů, poté jsou mu vydána přístupová hesla. V době voleb musí občan nejdříve potvrdit informace o registraci do systému, zadat přístupová hesla, dále zažádá o hlasovací lístky, které obdrží nevyplněné. Následně učiní svůj výběr a odešle vyplněný lístek.

Identifikace a autentizace je procesem, který poskytuje voliči jedinečnou digitální identitu pro odlišení od ostatních. Ověřování je provedeno za silného kryptografické šifrování, tak aby systém nebyl schopen přijmout zfalšované údaje.

Existuje spektrum ověření vzdálené identifikace:

1. 4 místný PIN (který je méně bezpečný než silné heslo),
2. dvoufaktorová identifikace (kryptografický token a PIN)
3. heslo a biometrický údaj
4. náhodně generované a časově omezené číslo. (Hasting, 2011)

Další možností identifikace pro vzdálené hlasování (platné od listopadu 2012 v Pennsylvanii):

> Volič musí poskytnout čísl řidičského průkazu, poslední 4 číslice sociálního pojištění nebo kopii občanského průkazu. Ověření identity může být provedeno přes telefon, email nebo poštu. Volební komise poté porovnává zadané údaje s obdrženými a poté rozhodne o započtení hlasu. (Voting by Absentee Ballot, 2008)

3.2.1 Výhody systému remote e-voting

- Dostupnost volby,
- pohodlnost zadání hlasů,
- rychlost a přesnost při vyhodnocení hlasů.

3.2.2 Nevýhody systému remote e-voting

- Požadavky na dostupnost připojení,
- náročnost zabezpečení identifikace voliče,

- náročnost na bezchybný přenos,
- zabezpečení ochrany PC voličem,
- zabezpečení systému proti chybám nebo útoku.

3.3 Kiosk voting

Hlasy mohou být zadány na mnoha místech. Administrátor má stále kontrolu nad platformou a komunikační sítí, ale již se nezabývá voličskými místy. Volič méně cestuje a oproti tradičním volbám je mu dopřáno větší pohodlí. Přesnost a rychlost hlasování je srovnatelná jako u poll-site voting. (Rosland, 2004)

3.4 Využití e-voleb

Elektronické volby mají široké spektrum využití od regionálních vole přes referenda, ankety až po výběrová řízení. Jak uvádí RNDR. Novotný (2009), jde zejména o minimalizaci nákladů voleb samotných, zrychlení propočtu výsledků voleb, komfort zadání hlasu, oslovení většího počtu voličů z „mladé“ generace. (Novotný, 2009)

Dalším příkladem je Švýcarsko, které využívá hlavní platformu pro komunikaci s úřady a jednou z odnoží je pak volební systém. Pro přihlášení stačí občanovi identifikační údaje a přístupová hesla. Takový systém je stále v provozu, provádí se aktualizace a je eliminováno riziko fatální chyby v průběhu voleb. V době volebního období pak volič využívá systém, který je mu dobře známý, je schopen se rychle orientovat nebo detekovat nestandardní chování platformy.

4 ZABEZPEČENÍ HLASOVÁNÍ POMOCÍ ŠIFROVÁNÍ

Jednou z podmínek pro bezproblémové elektronické volby je důvěrnost, která je upravena i zvláštními zákony o ochraně osobních údajů. Aby byla zajištěna bezpečnost dat vložených nebo vkládaných do systému, je nutné aplikovat kryptografické mechanismy, ať už symetrické nebo asymetrické.

4.1 Symetrické šifrování

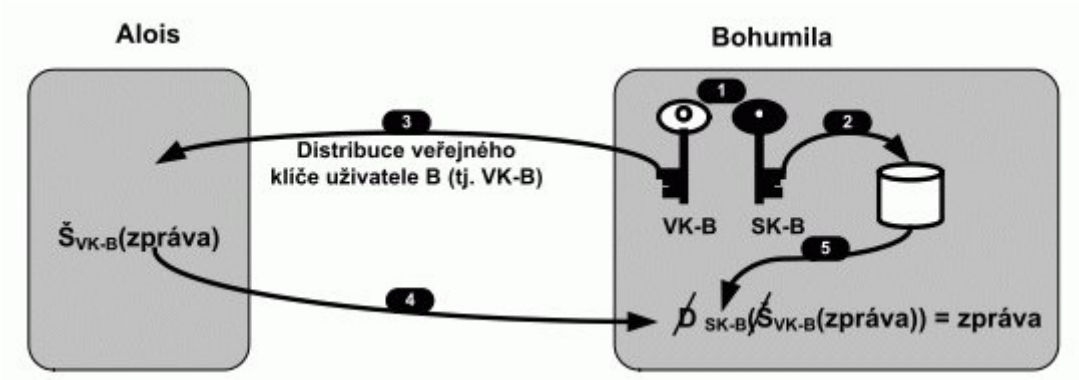
Pro symetrické šifrování textu je typické využití jednoho klíče, který slouží pro šifraci a i zpětnou dešifraci. Podmínkou je, aby klíč byl společným tajemstvím komunikujících stran. Proces započne předáním šifrovacího klíče skrze důvěryhodný kanál nebo je předat osobně druhé straně.

Symetrické šifrování v současnosti využívá algoritmy v reálném čase. Jako příklad může posloužit DES, TRIPLEDES – uváděný jako DES, IDEA, AES. Dle Budiše (2008): *„Dostatečně dlouhý klíč je stále náročné rozluštit v krátkém časovém horizontu.“*

Využití symetrických algoritmů je možností, jak ochránit důvěryhodnost přenášených zpráv. Nevýhodou ale může být náročné rozšíření mezi koncové uživatele či skupiny. (Elektronický podpis a jeho aplikace v praxi, Petr Budiš, 2008, str. 28-29)

4.2 Asymetrické šifrování

Narozdíl od symetrického šifrování využívá asymetrické šifrování dva klíče. Klíče – párová data jsou vygenerovány jedním uživatelem a je jejich jediným vlastníkem. Při zveřejnění jednoho z klíčů pro odvození druhé je kryptografie nazývána jako Veřejná kryptografie. Jako příklad může být uveden algoritmus DSA nebo RSA, který vynalezli Ronald Rivest, Adi Shamir a Len Adleman. (Budiš, 2008)



Obrázek 11: Asymetrická šifra *(Zdroj: flops.cz*)

Hlavní výhodou u asymetrického šifrování je možnost předání narozdíl od předchozího šifrování. RSA algoritmus nejdříve generuje náhodné velké číslo, dále je pomocí složitých matematických vzorců vypočteno prvočíslo, které se stává soukromým klíčem.

Algoritmem digitálního podpisu (DSA) se v roce 1991 zabýval americký institut NIST. Od té doby prošel mnoha úpravami a v současnosti je nazýván FIPS 186-3. Algoritmus řeší výpočet diskrétního logaritmu. (Wikpedia.org)

4.2.1 Využití šifrování u elektronických voleb

Párová data jsou rozdělena na veřejný a soukromý klíč. Privátní klíč má k dispozici jenom oprávněná osoba. Dešifrování probíhá ve spolupráci držitelů soukromých klíčů potřebných k dešifraci. Samotný proces je možné ověřit. Při dvou zašifrovaných hlasech pomocí metody násobení, je možné bez znalosti privátního klíče vytvořit šifrovaný text součtu hlasů. Následně je generovaný jeden text s výsledky voleb. Volič zabezpečí svůj hlas veřejným klíčem a přidá důkaz o správnosti zprávy. Po podpisu zprávy je hlas odeslán na registrační server. Probíhá ověření oprávnění voliče k volbě a korektnost přiloženého důkazu. Po úspěšné kontrole je voličův hlas zveřejněn, aby si mohl zkontrolovat, zda je jejich hlas na zveřejněném seznamu. (Novotný, 2009)

4.3 Hašovací funkce

Kryptografická hašovací funkce slouží k ochraně proti záměrnému poškození dat. Funkce je rozdílná od výše zmíněných algoritmů v generování klíčů, kdy akceptuje vstupní data, která jsou přeměněna na tzv. haš. Jde o jednosměrnou funkci, které je předána libovolně dlouhá zpráva a na výstupu je hash (otisk) o délce x-bitů. Zpětně nelze vygenerovat vstup, tzn. že nedostaneme původní zprávu. Hašovací funkci jemožné použít pro ověření

intergrity dat a pro uložení hashů hesel. Příslušná data jsou přepočtena do zápisu v hexadecimální soustavě, následně dojde k uložení na bezpečné místo. Ověření proběhne znovu vygenerováním hashe, který se porovná s původním uloženým hashem, v případě, že se data neshodují je zřejmé, že byla prolomena bezpečnost. Výhodou je ověření bezpečnosti bez prozrazení původního hesla nebo zadané zprávy.

Od prvního využití hašovací funkce došlo už k prolomení algoritmů MD5 a SHA-1, proto by se tyto algoritmy neměly používat. Mezi doposud neprolomené hašovací algoritmy patří SHA-256, SHA-512, RIPEMD-128/256 nebo RIPEMD-160/320. Další překážkou, která se může při generování objevit, je tzv. kolize, což znamená, že pro dvě různé zprávy bude vygenerován totožný hash. (Základy kryptografie pro manažery: hashovací funkce, 2010; Klíma, 2005)

Požadavky na hašovací funkci:

- nezjistitelnost zadané zprávy (vstupu),
- odlišnost generovaného hashe po úpravě znaku ve zprávě,
- zabezpečení proti kolizi. (vlastní generování požadavků)

4.4 Protokol HTTPS

HTTPS protokol zabezpečuje přenos dat mezi webovým prohlížečem a webovým serverem, aby byla zajištěna ochrana pře odposlechem, změnou přenášených dat a identity jejich zadavatele. HTTPS protokol využívá protokol HTTP, kdy jsou přenášená data šifrována pomocí SSL/TLS a kombinována se symetrickými, asymetrickými a certifikačními kryptografickými metodami. (Gourley, 2009; HTTPS - zabezpečený HTTP protokol, 2013)

4.5 Certifikáty

Veřejný klíč patří oprávněné osobě a musí být platný, aby mohlo dojít k dešifraci obdržené zprávy nebo dokumentů. Záruka platnosti řeší certifikát. Jedná se o datovou strukturu, která se skládá z veřejného klíče a certifikátu. Aby bylo zajištěno důvěryhodnosti, je doplněn podpis třetí strany (bývá označována jako CA – Certificate Authority). Ověření certifikátu může proběhnout jenom s veřejným klíčem třetí osoby. Bezpečnost doručení

klíče by měla proběhnout „offline“. Se sadou důvěryhodných veřejných klíčů se setkáváme např. ve webových prohlížečích.

Mezi nejčastějšími certifiktáty patří:

1. Certificate
    a. Version
    b. Serial Number
    c. Algorithm ID
    d. Issuer
    e. Validity (Not Before, Not After)
    f. Subject
    g. Subject Public Key Info
    h. Public Key Algorithm
    i. Subject Public Key
2. Certificate Signature Algorithm
3. Certificate Signature

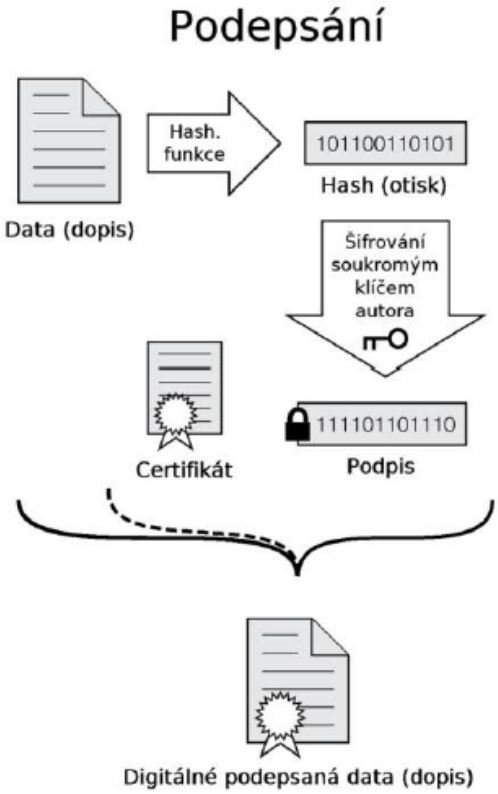
4.6 Digitální podpis

Digitální podpis slouží k ověření pravosti odesílatele. Transfer od odesílatele k adresátovi může být sledován, aby nedošlo k nežádoucímu úniku nebo modifikaci dat, jsou dokumenty chráněny digitálním podpisem.

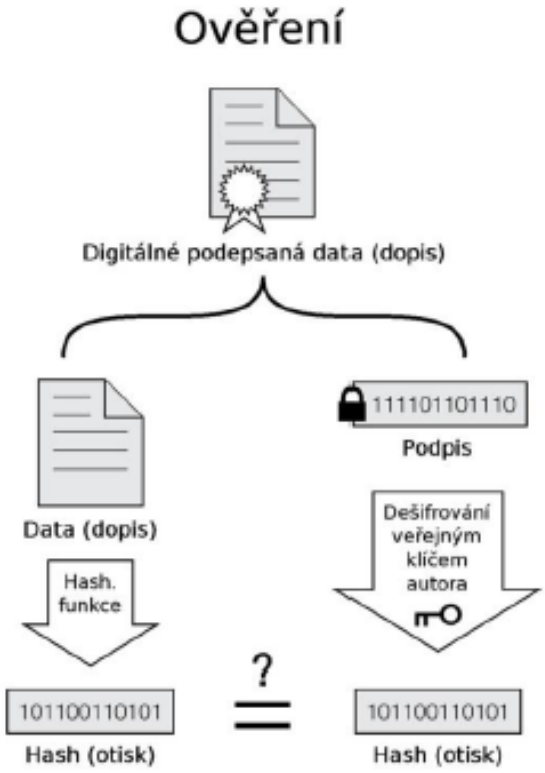
Bezpečná tvorba elektronického podpisu závisí na výběru správné hašovací funkce, aby byl generován tzv. haš. Následně je otisk zašifrován pomocí privátního klíče a spolu s daty odeslán adresátovi. (viz Obrázek 12)

Adresát obdrží zprávu a pomocí veřejného klíče dešifruje haš. Důležité je, aby příjemce a odesílatel použili stejnou hašovací funkci, jinak by nebylo možné zajistit správnou dešifraci. Haš je porovnán s přijatým dešifrovaným otiskem. Pokud jsou data identická, je zřejmé, že nedošlo k úpravě nebo poškození dat někým dalším. Do této chvíle proběhly dvě kontroly, poprvé při dešifraci a podruhé při srovnání obou haší. Pro zajištění vyšší

bezpečnosti by bylo vhodné řipojit ještě certifikát, který by potvrdil identitu odesílatele a platnost veřejného klíče. (viz Obrázek 13)



Obrázek 12: Postup šifrování s digitálním podpisem *(Zdroj: wikipedia.org)*



Obrázek 13: Postup ověření a dešifrace *(Zdroj: wikipedia.org)*

4.7 Homomorfní šifrovací schéma

Základem homomorfní šifrovací funkce jsou speciální matematické vlastnosti. Pro volby je schéma chápáno jako obraz zašifovaných hlasů, které jsou převedeny na obraz jejich výsledných součtů. Výsledný součet je dešifrován a je možné vytvořit rekonstrukci voleb.

Problémem přístupu k výpočtu je inverzní funkce k funkci původní, která nese původní výsledky voleb. Výpočet je natolik složitý, že se schéma využívá pro sčítání menších voleb nebo v případě ze dvou kandidátů. (Wikipedia.org)

II. PRAKTICKÁ ČÁST

5 ELEKTRONICKÝ VOLEBNÍ SYSTÉM

Elektronické volební systémy (EVS) znamenají pokrok a zavádění moderních technologií do běžného života. Stejně jako každá jiná stránka lidského snažení, tak i zde je snaha o zjednodušení, zpřístupnění co největšímu počtu obyvatel a o snížení nákladů. Stejně jako v ostatních oborech, i zde přinesla největší posun kupředu průmyslová revoluce v 19. století. Od té doby se vývoj technologií neustále zrychluje a jeho uvedení do praxe je v mnoha případech otázkou měsíců nebo už několika týdnů. Přestože pojem „elektronický volební systém“ zní velmi moderně a evokuje zdání, že byl uveden do praxe teprve před několika málo lety, skutečnost je úplně jiná. Je to už téměř půl století, co bylo poprvé použito elektronického systému k volbě kandidáta.

Elektronika je nejrychleji rozvíjející se obor průmyslu, a proto elektronický volební systémy ze 70. lety 20. století jsou značně odlišné od představy dnešních dnů. Dřívější elektronické volební systémy měly za úkol hlavně pomoci se sčítáním odevzdaných hlasů a tím zkrátit dobu mezi uzavřením volební místnosti a vyhlášením výsledků. Zařízení na optické snímání a následné sčítání volebních lístků vyrábí společnost ES&S (viz kapitola 2.4). Dnešní elektronické volební systémy postupně přebírají funkci plnohodnotného systému, který nahrazuje papírové hlasovací lístky. Je to obdoba revoluce jako při zavedení tajné volby na Tridentském koncilu v 16. století. Zatímco v minulosti se volební postup na několik staletí ustálil na papírových volebních lístcích a urnách, do kterých se vkládal. S rozvojem elektroniky vznikla řada postupů a technologií, které jsou buď v průběhu několika let zdokonalovány, nebo nahrazovány novými systémy. Nyní se nacházíme v době, která nabízí mnoho technologií a postupů, které si mohou konkurovat nebo se při správném použití mohou dobře doplňovat. Proto se zaměřuji na výběr systému při elektronických volbách, jenž bude pro voliče jednoduchý na obsluhu, bezpečný proti útoku jednotlivce či organizované skupiny a v neposlední řadě ekonomicky výhodný.

5.1 Zásady elektronického volebního systému

Pro dodržení funkčnosti EVS je nutné stanovit jeho zásady, aby byly řádně a jasně definovány nezbytné vlastnosti systému. Z již používaných systémů lze snadno odvodit potřeba intuitivního ovládání, zabezpečení proti útoku, ekonomičnosti a snadného zavedení do provozu. Nově však vyvstává otázka zajištění odolnosti systému.

5.1.1 Jednoduchost na obsluhu

Jedním ze zásadních faktorů, které ovlivňují, zda se systém ujme, je jeho jednoduchost na obsluhu. Příliš složitý systém může voliče zmást, což by se mohlo stát terčem kritiky nebo vést k podání žalob proti výsledkům voleb. Zároveň by příliš složitý nebo zdlouhavý systém mohl přímo nebo nepřímo ovlivňovat rozhodování občanů, zda se voleb vůbec zúčastní. Již nyní se lidé často nezúčastní voleb jen proto, že pospíchají na chatu a nechtějí ztrácet čas v pátek odpoledne zajížďkou do volební místnosti. V sobotu zase málokdo odjede z víkendového odpočinku, aby uplatnil své občanské právo jít volit. Druhým faktorem ovlivňující voliče by mohla být obava ze vzniku trapné situace při volbě a zadávání hlasů do systému. I když některé z moderní zařízení má doma prakticky každý z nás (televizor, telefon, rádio, počítač), je mezi námi spousta lidí, kteří mají obavy z dalších moderních zařízení a jejich ovládání se brání. Je to převážně u starších lidí, kteří se ještě nestačili sžít s těmito zařízeními nebo jim to nebylo doposud umožněno. Uživatelské prostředí elektronického volebního systému by mělo být natolik jednoznačné a jednoduché, aby se tyto obavy jasně vyvrátily či eliminovaly. Snadné ovládání by mělo být zaměřeno také na komisi nebo osobu pověřenou správou dat, aby se snížilo riziko špatného přenosu dat, „poškození“ systému, vynechání důležitého kroku.

5.1.2 Bezpečnost osobních údajů

Volební ověřování by nemělo ohrozit tajnost hlasování. Autentizační protokoly nesmí připojit snadno dosažitelné identifikační údaje voliče s odevzdanými hlasovacími lístky. Pokud legislativa umožní, aby hlasovací systém spojil identifikační údaje voliče ke „vhozenému“ hlasovacímu lístku, pak by tato informace měla být kódována tak, aby mohla být dešifrována pouze za výjimečných okolností.

5.1.3 Bezpečnost proti útoku

Volby jsou důležitou částí každé demokracie a měly by být svobodné, aby si občan mohl vybrat kandidáta, který je podle něj ten nejvhodnější. Vznikají tak jistá bezpečnostní rizika, pokusy o ovládnutí voleb nebo pokusy o změnu výsledků. Případy ovlivnění či úpravy voleb se stávají všude na světě.

V době papírových volebních lístků je nejpravděpodobnější způsob pozměnění výsledků zapříčiněn zaplacením hlasů (zaplatit voličům za to, aby volili určitého kandidáta). Volba jako taková již probíhá regulérně a volební komise nezaznamená žádnou chybu při sčítání hlasů. Tento způsob ovlivňování se děje hlavně při komunálních volbách, na celostátní úrovni je prakticky neproveditelný, jednak z důvodu velké možnosti odhalení, protože kupování hlasu není povolené, a jednak z finančního hlediska, kdy by náklady na celou akci dosáhly astronomické výše. Další možnost manipulace s výsledky voleb může nastat při ovlivnění volební komise. Tento způsob je jistě obtížnější, protože ve volební komisi bývají zástupci různých politických stran. Rovněž na celostátní úrovni je uskutečnění nepravděpodobné. Z tohoto pohledu se zdají být klasické volby pomocí papírových hlasovacích lístků bezpečné. Ze světa i z naší minulosti víme o zmanipulovaných a netransparentních volbách na papírové bázi. Ke zmanipulování došlo na základě nátlaku nejvyšší moci v zemi (prezident, vláda nebo jiná diktatura). Proti tomuto způsoby ovlivnění výsledků voleb existuje jen velmi málo možností nápravy. I když na průběh voleb dohlíží mezinárodní sbor pozorovatelů, nemají žádné pravomoci do nich zasáhnout.

Elektronické volební systémy mohou řešit problémy vznikající při selhání lidského faktoru, například ovlivnění volební komise, na druhou stranu vyžadují vyšší zabezpečení proti napadení a selhání systému. Starší elektronické volební systémy prakticky jenom sčítaly a vyhodnocovaly hlasy. Nejmodernější elektronické volební systémy využívají počítačové systémy a jejich síťové propojení. Riziko chyby je tak eliminováno.

Tento systém znamená pro drtivou většinu lidí nepřekonatelnou překážku při pokusu ovlivnění voleb. Běžný uživatel není schopen nabourání do počítačového systému. Existuje ale nebezpečí útoku organizované skupiny odborníků, která by si vzala za cíl volby narušit, překazit, zdiskreditovat nebo dokonce na zakázku ovlivnit. Snaha zpřístupnit lidem volby prakticky z kteréhokoliv místa na Zemi přináší velké bezpečnostní riziko, protože využívá veřejných komunikačních prostředků, jejichž monitorování není úplně možné. Z tohoto hlediska se nároky na zabezpečení systému mnohonásobně zvyšují.

Důležité je, aby byla spolehlivě vyřešeno ověření oprávněnosti občana hlasovat, přihlášení se do systému pro výběr kandidáta, zabezpečená komunikace mezi voličem, jeho počítačem a serverem, který zpracovává hlasování.

5.1.4 Ekonomičnost

Dalším důležitým faktorem při zavádění nových systémů je předpoklad zvýšení efektivnosti a snížení nákladů. Volby jsou nezbytné pro udržování demokracie, zároveň jsou finančně nákladné. Dochází proto ke slučování voleb do jednoho termínu. Přesto zůstávají náklady na platy účastníků volební komise, pronájmy volebních místností a vybavení, tisk a roznos volebních lístků na vysokých číslech. Elektronický volební systém by v ideálním případě měl přinést nové možnosti hlasování a zpřístupnění lidem, kteří by jinak nemohli volit. Dále je očekáváno snížení nákladů na tisk volebních lístků nebo pronájem volebních místností. Při zavedení elektronického volebního systému, přes který je možné hlasovat na dálku, je vysoký předpoklad využití systému občany. Podle Českého statistického úřadu bylo k listopadu 2011 připojeno 62% českých domácností k internetu, za rok už šlo o 70 % připojených. Za posledních 6 let je to nárůst o 132 %.

Podíl domácností připojených k internetu je přes 2/3 z celku, tím pádem by došlo ke snížení počtu voličů, kteří by volili klasickým papírovým způsobem. Bylo by tedy možné snížit náklady redukcí počtu volebních místností.

Druhou stranou elektronických volebních systémů jsou náklady na vývoj a zavedení do praxe. Obvykle jsou náklady za elektronické a jiné informační technologie spojovány s neúnosně vysokými náklady. Například projekt Opencard v Praze, projekt elektronických zdravotních knížek IZIP Všeobecné zdravotní pojišťovny. Vytvoření systému, který je v tomto případě čistě softwarovým informačním systémem bez speciálního hardwaru, stálo 300 miliónů korun a dalších 1,8 miliardy korun vydala VZP na provoz systému v průběhu jeho zavádění. Projekt po 10 letech skončil, kdy se ho nepovedlo dostatečně rozšířit. Přesto za dobu jeho fungování zaplatila VZP v konečné fázi přes 2 miliardy korun.

Podle typu návrhu elektronického volebního systému by kromě softwarové části potřeboval i hardwarovou podporu. Tímto způsobem se vydali například v Estonsku. Již od roku 2002 vydávají místo klasických občanských průkazů (OP) plastové ID karty v podobě platebních karet, které navíc standardně obsahují zabudovaný RFID čip. Jejich výroba není výrazně dražší oproti klasickým metodám. K čipovému dokladu totožnosti dostane občan

Estonska zdarma také čtečku čipových karet, kterou si pomocí USB portu připojí k počítači. Čtečka karet vychází asi na 100 Kč. Občanské průkazy mají z bezpečnostních důvodů omezenou platnost a pak se vyměňují za nové bez ohledu na to, zda je daná země používá u elektronických voleb nebo ne. Vybavení dokladů o RFID čipy vyjde celkově jen na několik miliónů korun, navíc by byla suma rozdělena rovnoměrně do několika let – dle končící platnosti OP. Cena elektronických čteček pro hladkou volbu je odhadnuta přibližně na 5 miliard Kč. Nezanedbatelnou položkou by byla tvorba softwarového systému a jeho bezpečnostní zajištění a hardwarové vybavení. Při nákladech přibližně 500 miliónů korun na jedno kolo voleb v ČR by byla doba návratnosti do dvou volebních období.

Obrázek 14: USB čtečka čipových karet *(Zdroj: mechanikadc.cz)*

5.1.5 Dostupnost

Současný systém dává voliči možnost volit v pátek a sobotu. Pokud je člověk oba dva dny v zaměstnání nebo je mimo ČR, nemá možnost uplatnit své právo k volbě. Překážkou může být také zdravotní stav voliče, který například leží v nemocnici. Zajištění vyššího počtu voličů s sebou nese požadavek na lepší dostupnost samotných voleb. Počet aktivních voličů ze zemí se zavedeným elektronickým systémem se rok od roku zvedá.

Právě dostupnost může být zajištěna zavedením elektronického volebního systému, využívajícího mobilní telefony, internet či kabelovou televizi. Samotná čísla ukazují, jak jsou zmíněná zařízení využívána obyvateli.

Český statistický úřad udává, že v roce 2012 využívalo v České republice mobilní telefon 96 % osob starších šestnácti let. Mobilní telefon je nejčastějším komunikačním zařízením a v téměř 100 % vlastněn mladou věkovou skupinou 16–24 let a 25–34 let. Naopak nejmenší zastoupení mobilních telefonů mezi obyvatelstvem je u osob starších 75 let (70 %). (Mazal, 2013)

V roce 2012 používalo osobní počítač 6 milionů jednotlivců, tj. 70 % populace starší 16 let. Za posledních 5 let počet uživatelů PC vzrostl o 1,5 milionu. V roce 2012 navíc poprvé všichni uživatelé osobního počítače uváděli, že zároveň používají také internet.

5.1.6 Snadné zavedení do provozu

Každý projekt by měl být navrhován tak, aby jeho uvedení do provozu nepředstavovalo ve skutečnosti zbytečné navýšení nákladů. Takové případy by mohly vést ke kompromisům mezi již zavedenou praxí a novinkami nebo absolutním odmítnutím elektronických volebních systémů. Nově navržený systém by měl projít testovacím procesem, který by poukázal na opomenuté nebo podceněné skutečnosti.

5.1.7 Odolnost systému – zajištění funkcí

Při tak důležité události jako jsou volby není možné, aby nastala situace omezující hladký průběh voleb či je dokonce přerušila nebo zapříčinila jejich opakování. Je nutné předejít problémům, kdy by:

- elektronický volební systém přestal pracovat,
- mu hrozily výpadky nebo dokonce zhroucení,

- byl napadnutelný neoprávněnou osobou,
- se systém zhroutil při hlasování více voličů zároveň.

V průběhu voleb a přepravy by volební zařízení mělo být:

- odolné vůči mechanickému poškození, které by zabránilo dalšímu hlasování,
- přístupu neoprávněných osob s virem ovlivňující volbu voliče,
- mechanickému poškození bránící stažení uložených dat.

Eventuality, které by mohly nastat, musí být přesně definovány. Není možné, aby při komunikaci přes veřejnou internetovou síť zkolabovaly servery, na kterých systém běží. Celý volební software a hardware musí být naddimenzovaný, aby nedošlo k výpadku při větším množství hlasujících voličů ve stejnou dobu a zároveň aby nedošlo k narušení voleb cíleným hackerským útokem. Terminál elektronického volebního systému umístěný ve volební místnosti musí být odolný vůči mechanickému poškození, aby nedošlo ke ztrátě uložených dat o odevzdaných hlasech. Zároveň musí být terminál navržený tak, aby nemohlo dojít k takovému poškození, které by zamezilo dalšímu hlasování nebo získání uložených dat. Připravenost zahrnuje také alternativu hlasování papírovou formou, pokud by terminály selhaly, byly napadeny nebo špatně zaznamenávaly odevzdané hlasy.

6 POROVNÁNÍ KLASICKÉHO A ELEKTRONICKÉHO OVĚŘENÍ

6.1 Klasické ověření občana ve volební místnosti

Současné ověřování probíhá ve volební místnosti, kdy některý ze členů volební komise zkontroluje některý z dokladů totožnosti a porovná s údaji, které dostal vytištěné na papíře z evidence obyvatel, zda se shoduje:

1. jméno a příjmení,
2. rodné číslo,
3. místo trvalého bydliště,
4. platnost dokladu totožnosti.

V neposlední řadě je důležité zkontrolovat, zda je volič způsobilý k právním úkonům a jestli má tím pádem právo volit. V takových případech je u jména poznámka.

Tento systém ověřování voliče je poměrně zdlouhavý. Každý člen volební komise má na starost jen určitou část z celkového počtu lidí ve volebním okrsku, ale i tak to bývají desítky či spíše stovky lidí, které má na starosti každý člen volební komise. Mohou nastat situace, kdy se v místnosti sejde více lidí a nepřímý tlak voličů na zrychlení ověřování může vést k chybě nebo nedostatečné kontrole. Může dokonce nastat situace, kdy se dostaví volič, který má doklady v pořádku, ale v seznamu voličů se nenachází. Tato situace vzniká při změnách pobytu občanů nebo změně trvalého bydliště. Seznamy voličů se zpravidla tisknou několik dnů před volbami a ověření voliče, který se v něm nenachází, se musí provádět přes evidenci obyvatel zpravidla telefonicky.

6.2 Ověřování identity občana elektronickou formou

Současným trendem je přechod od ručního/papírového ověřování k pohodlnějšímu a rychlejšímu elektronickému. Zásadní problémy by to přinést nemělo, protože většina vyspělých nebo rozvinutých zemí už nyní uchovává spoustu informací o občanovi nebo jeho aktivitách v elektronické formě. Šlo by tak o zprovoznění elektronického volebního systému a propojení nebo stažení dat z již existujících databází. Samotné ověřování přístupu do elektronického volebního systému už může probíhat mnoha způsoby.

6.2.1 Elektronický občanský průkaz

Jedna z forem identifikace je pomocí speciálního čipu, ve kterém jsou uložené informace. Tento čip s obecně nazývá RFID a v současnosti je to nejrychleji se rozvíjející systém identifikace obecně. RFID čipy máme běžně kolem sebe, aniž bychom si to třeba uvědomovali. Jejich využití je široké, ale zatím se využívají především k identifikaci nebo jako zabezpečovací prvek. Setkáváme se s nimi v bankovnictví, v ubytovacích zařízení, v obchodech a nyní i při identifikaci při volbách.

Obrázek 15: RFID čip *(Zdroj: zvedavec.org)*

Čip je poměrně malý, takže nijak zásadně člověka neomezuje, může být zalisovaný v plastové kartě, klíčence nebo nalepený. Čip nemá žádné kabely nebo kontakty, komunikace s ním probíhá pouze bezdrátově na principu rádiového přenosu dat mezi vysílačem a snímačem. Je tak i poměrně odolný vůči vodě, prachu, částečně i mechanickému poškození a má dlouhou životnost. RFID čip se skládá ze elektronického obvodu (paměťového média), dále obsahuje přijímací/vysílací anténu, nabíjecí kondenzátor a paměť. Nesmírnou výhodou tohoto systému je, že neobsahuje žádnou baterii. Princip napájení celého elektronického systému čipu spočívá v tom, že vysílač (snímač) periodicky vysílá pulsy prostřednictvím antény do okolí. Jakmile se v dosahu antény objeví přijímač (transpondér), přes jeho vlastní anténu přijme signál a ten následně využije k nabití svého kondenzátoru energií, která je dostatečná k jeho aktivaci a odpovědi zpět snímači. Ten signál od transpondéru přijme a po jeho vyhodnocení (ochranné kódy atd.) jej předá k dalšímu zpracování. Data mohou být předána ihned počítači ke zpracování nebo mohou být uložena v paměti přenosných čteček a později nahrána do počítače.

Vzhledem k rozměrům RFID čipů jsou běžně zalisovány do plastových karet z polykarbonátu o rozměrech 86,5 x 54 mm. Uvedený rozměr je stejný i pro platební karty.

Od papírových občanských průkazů nebo řidičských průkazů zalisovaných v plastové průhledné fólii se postupně upouští z důvodu jejich snazší padělatelnosti a nemožnosti instalace RFID čipů. Avšak jeho přidání je omezeno sílou karty a teplotním namáhání při zalisování. Přesto se čip dá využít i při identifikaci voliče v elektronickém volebním systému při volbě na dálku, tak i při ověření voliče přímo ve volební místnosti.

Od 1. ledna 2012 se v České republice vydávají nové občanské průkazy, které obsahují kromě „klasické“ strojově čitelné oblasti také 2D kód. Elektronický čip, který je nepovinný (za příplatek 500 Kč) nenese, kromě čísla průkazu, žádné další informace o nositeli. Lze však na něj svépomocí nahrát elektronický podpis. Elektronický občanský průkaz (tzv. eOP) musí disponovat obslužnou aplikací. Middleware pak umožňuje změnu hodnoty PIN na čipu eOP a slouží pro zápis dat a vytváření elektronických podpisů zároveň s kvalifikovaným certifikátem. K datu 25. 7. 2012 je dostupný middleware pro systémy MS Windows XP a vyšší, Linux Ubuntu 10.04 a Mac OS X 10.5 – 10.7. (Ministerstvo vnitra České republiky: Obslužná aplikace eOP (middleware), 2012)

Volič je vyzván k předložení občanského průkazu. Po přečtení informací z čipu je potřeba přiložit kartu nebo eOP ke čtečce, obvykle s USB konektorem, která je dále připojená k osobnímu počítači. Aby bylo zajištěno, že držitel identifikačního průkazu je zároveň i jeho vlastníkem a má právo volit, zadává do systému ověření svůj PIN kód. Jde o 4 místné heslo, které si občan zvolil nebo mu bylo přidělen při vydávání průkazu. Při volbě na dálku se využívá veřejných komunikačních prostředků, počítačové sítě internet, přes kterou se počítač spojí s příslušným serverem, který data a hlasy zpracovává. Aby hlasování nemohl nikdo zmanipulovat, je celý proces komunikace šifrován. Veřejným klíčem voleb se zašifruje voličův hlas, který je následně zašifrován privátním klíčem (PIN). Teprve pak jsou data odesílána přes internet.

Obrázek 16: Vzor občanského průkazu ČR

Výhodou elektronického volebního systému je možná změna omezení volby ve voličově volebním okrsku, pokud už hlasoval na jiném místě. Což by nemohlo být vykonáno kvůli nemožnosti ověření jiných okrsků při klasických volbách na bázi papírových volebních lístků. EVS zároveň umožňuje dostupnost volebních kandidátek jiných měst, okrsků, krajů nebo senátů. V přehledném prostředí elektronického terminálu by tak nebyl problém vyhledat požadovaného kandidát, aniž by musel cestovat do místa bydliště jen kvůli volbám. Volič by měl samozřejmě elektronicky zamezeno volit do zastupitelstev obcí a krajů, ve kterých nemá trvalé bydliště. Elektronický volební systém řeší i situace, kdy se člověk rozhodne svoji předchozí volbu změnit. Platná by byla poslední volba a je jedno, zda by volič hlasoval vícekrát v jedné volební místnosti nebo pokaždé v jiné. Hlas by byl přepisován nově zadanými daty. To pro případ, že by byla volba přes internet nebo SMS provedena pod nátlakem na občana nebo by volič svůj výběr kandidáta přehodnotil.

6.2.2 Mobilní telefon - SMS

Další zajímavou technologickou metodou je hlasování přes mobilní telefon. Tento způsob hlasování je zaměřen i na mladé voliče, kteří nemají o volby často zájem. Jde v zásadě o velmi podobnou formu hlasování pomocí RFID čipu a čtečky. Místo čipové karty se u hlasování přes SMS použije speciální čip umístěný přímo v mobilním telefonu. Bezpečnost hlasování je v rukou majitele, kdy nesmí být prozrazeno heslo. Zbytek postupu je stejný jen s tou výjimkou, že data se nedostanou do centra pro zpracování hlasů přímo, ale přes mobilního operátora. (Lupa.CZ: Volby v ČR, volby přes Internet a SMS, Estonsko budiž vzorem, 2008)

Nebo se volič se zaregistruje do databáze, aby mohlo být ověřeno jeho telefonní číslo, ze kterého bude volba uskutečněna. Ochrana údajů občana musí být předem specifikovaná, nejčastěji je uvedeno, že tel. číslo je použito pro oznámení konání voleb, zaslání identifikačního čísla, přihlašujících údajů a nebo potvrzující SMS o obdrženém hlasu. Telefonní číslo pak nesmí být využito k jiným než definovaným čelům. Při registraci voleb je přiřazeno identifikační číslo, kterým se volič prokazuje při odesílání hlasu.

6.2.3 Pevná linka

Volbu přes pevnou linku je možné uskutečnit poté, co volič získá speciální potvrzení o načtení volebního lístku do systému. Lístek slouží také ke zpětnému ověření ze strany voliče, že jeho hlas byl doručen a započten do systému.

Občan je přes telefon informován, jak postupovat pro zadání hlasu. Výběr je uskutečněn pomocí telefonního číselníku, mezi jednotlivými kandidáty je možné přeskakovat. Na konci telefonátu je volič upozorněn na nekompletní doplnění hlasovacího lístku a je mu poskytnut prostor na kontrolu a opravu. Výhodou je také bezplatná volební linka v předvolební době, kdy je poskytnut prostor pro seznámení se s průběhem zadávání hlasů.

Velkou výhodou je dostupnost z jakéhokoliv místa s telefonem. Volič může být indisponován zdravotně, může být negramotný, nemá signál na mobilním telefonu nebo nemá přístup k internetu, přesto je mu stále umožněno volit.

6.3 Výhody elektronického systému proti klasickému ručnímu zadávání a sčítání:

- odstranění rizika dvojí volby,
- nemožnost vhození více volebních lístků,
- odstranění početních chyb při vyhodnocování,
- dostupnost výsledků ihned po ukončení voleb,
- snížení nákladů voleb z dlouhodobého hlediska (tisk lístků a obálek, roznos, recyklace, archivace, pronájem prostor),
- rychlá aktualizace volebních kandidátů,
- průběžná archivace na centrálním serveru,

- dostupnost pro voliče a jejich vyšší počet voličů.
- zvýšení voličské účasti,
- lépe informovaní voliči,
- snížení manipulace s lístky. (The Center for Association Growth: Top Ten Benefits to Electronic Voting, 2009)

6.4 Nevýhody elektronického systému proti klasickému ručnímu zadávání a sčítání:

- časová náročnost na přizpůsobení,
- nutná úprava legislativy,
- nákladnost certifikace volebního systému,
- vysoké nároky na bezpečnost a spolehlivost,
- rovnocenný přístup pro všechny oprávněné voliče,
- přeškolení volebních komisařů na nový systém,
- politický risk spojený s testováním nového systému,
- potřeba volebních a bezpečnostních specialistů.

7 ANANALÝZA ELEKTRONICKÝCH VOLEBNÍCH SYSTÉMŮ

Jednotlivé elektronické volební systémy zmíněné v teroretické části (viz kapitola 1.2) jsou v následujících řádcích hodnoceny dle zvolených zásad (viz kapitola 5.1).

7.1 Spojené státy americké

Bezpečnost volebního zařízení a osobních dat voliče je chráněna kartou, firewallem, antivirem a šifrováním pomocí digitálního podpisu a certifikátů. Volební aplikace posílá zašifrovaný hlasovací lístek a osobní data do databáze voličů. Server pro ukládání ověří voličovo povolení k hlasování a následně odesílá voliči textovou zprávu o přijetí volby. Na serveru jsou dešifrovány volební lístky a odejmuta osobní data. Poté je volební lístek opět zašifrován bez osobních dat veřejným volebním klíčem. Aktualizace serveru pro sčítání dá podnět ostatním serverům pro stažení seznamu voličů a uložení zašifrovaných volebních lístků. Výstupem systému po ukončení voleb je konečný záznam s výsledky a seznam voličů.

Jednoduchost výběru a volby kandidáta závisí na využitém zařízení. V případě voleb ve volební místnosti volič obsluhuje dotykem elektronické zařízení, kde zadává požadovaného kandidáta. Pokud chce využít své právo volit přes internet, je povinen být registrován v databázi oprávněných voličů. Po otevření volebního prohlížeče je občan vyzván k identifikaci, aby si mohl požádat o volební lístek a následně jej vyplněný a doplněný o digitální podpis zasílá nazpět.

Bezpečnost systému za použití osobních přístrojů není možné zaručit v nejvyšší možné úrovni. Komise nedokáže vzdáleně zajistit ochranu osobních dat při vyplňování důvěrných údajů, dále může být volič nucen k volbě, která není shodná s jeho rozhodnutím. Eliminace zmíněných rizik už záleží jenom na občanovi, kde a v jaké situaci bude odesílat svůj volební lístek. Naopak elektronická zařízení ve volební místnosti by měla být zabezpečena volební komisí, tak aby systém nemohl být napaden malwarem nebo servisním útokem. Pokud by byl napaden systém, znamenalo by to riziko ohrození osobních údajů, modifikace hlasování nebo zabránění v přístupu do hlasovací služby.

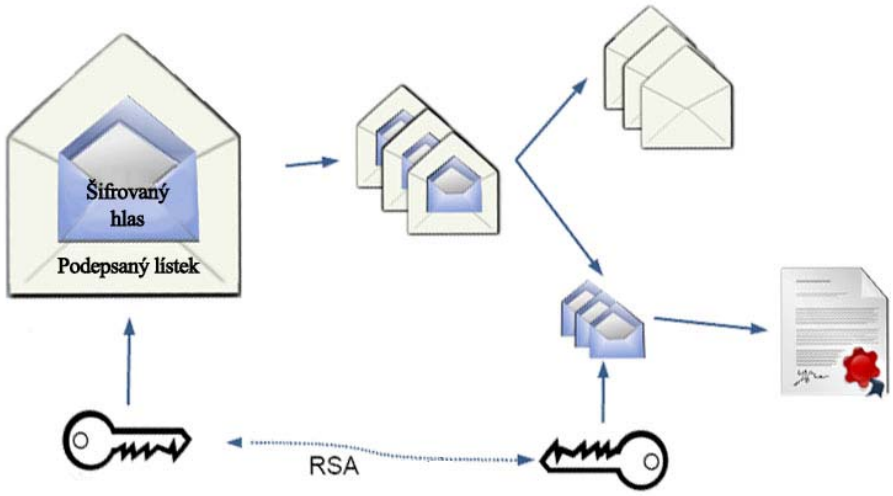
Ekonomičnost sytému a **snížení nákladů** jsou dosaženy omezením tisku papírových hlasovacích lístků, není potřeba ani četná volební komise, která ověřuje identitu voliče a předává voličskou kartu s elektronickým volebním lístkem. Počítačový server, volební

zařízení a záložní hardware pro jednu místnost vychází zhruba na 20 000 USD. **Zavedení** elektronického volebního **systému** eliminuje uvedené náklady. Amerika si pohrává s myšlenkou elektronických voleb už od roku 2000. Přesto stále přetrvávají problémy, které způsobují technické chyby nebo prohlubují nedůvěru voličů o tajnosti hlasování a započtení zadaného kandidáta. Selhání ze strany voliče může vzniknout nepozorností, kdy zapomene odeslat hlas nebo si nezkontroluje potvrzení o volbě. Na druhou stranu je elektronický proces ušetřen o zasílání lístků poštou, vyplňování průvodního dopisu, zaslání hlasovacích dokumentů městské volební komisi, otevírání obálek a sčítání hlasů, registrace výsledků voleb z jednotlivých komisí do systému, tím se stává v konečné fázi jednodušší a levnější variantou oproti papírovým volbám.

USA má dle průzkumů nejhorší voličskou účast, v průměru by mělo jít o 48 % oprávněných občanů. Elektronický systém umožňuje lidem bez auta, na dovolené, zaneprázdněné pracovními povinnostmi vybrat kandidáta a ovlivnit svým hlasem výsledek. Ve Spojených státech se snaží volbu a sčítání hlasů vylepšovat a zjednodušovat. Už v minulosti zavedli mechanické sčítací stroje, elektronické volební přístroje i volbu přes internet. Ne všechny systémy byly bez chyb a docházelo tak k chybám při sčítání hlasů, chybným volbám, nebo byly výsledky jiným způsobem ovlivněny.

7.2 Estonsko

Bezpečnost hlasování a osobních dat je zajištěna elektronickým digitálním podpisem. Server ověří, zda je vlastníkem relace stejná osoba, která podepsala volební prohlášení. Shoda dává povel pro přenos podepsaného a zašifrovaného lístku na server s ostatními lístky. Po ukončení volebního období jsou na serveru odstraněny vícečetné lístky od jednoho voliče. Poslední je považován jako aktuální. Informace o odstraněných lístcích jsou zaprotokolovány a uloženy. Dalším krokem je odejmutí digitálního podpisu od samotného hlasovacího lístku, který je stále zašifrován. Takový lístek je přenesen na off-line server pomocí datového nosiče. Pro součet odevzdaných hlasů jsou hlasovací lístky dešifrovány soukromým klíčem serveru. Přijímány jsou jen lístky ve správném formátu, které jsou započteny do konečných výsledků.



Obrázek 17: Systém šifrování v Estonsku *(Zdroj: Cybernetica)*

Jednoduchost obsluhy a zadání volby jsou dává intuitivním ovládáním, kdy volič otevře stránku pro volbu, zadá své telefonní číslo a následně je mu zaslán kontrolní kód. PIN1 slouží k identifikaci a zobrazení kandidátů z jeho volebního okrsku. Volič provede výběr, který je šifrován, poté obdrží sms s dalším kontrolním kódem na mobilní tel. Volič potvrzuje svoji volbu a přikládá digitální podpis v podobě PIN2. Celý proces je ukončen potvrzovací sms, že hlas byl přijat.

Bezpečnost systému byla ohrožena lanovým malwarem (DDoS) ze strany 20 letého studenta, proti kterému se Estonsko snaží zabezpečit při dalších volbách. Technická část je vysoce zabezpečená za použití šifrování.

Ekonomičnost je opět dána snížení nákladů na distribuci, tisk hlasovacích lístků. Celý proces s sebou nese i urychlení výpočtů a eliminuje zpoždění při předávání potřebných dokumentů a volebních materiálů.

Politický systém se snaží zvýšit účast voličů a inovuje volební systém. V současnosti je **nepříjemnější a nejrychlejší hlasování** přes internet nebo pomocí mobilního telefonu, kdy není volič omezen místem a dobou pobytu.

7.3 Španělsko

Bezpečnost hlasování je v případě Španělska zabezpečena generováním 16-ti místného kódu, který volič obdrží poštou. Ochrana kódu po převzetí zásilky závisí už jen na příjemci. Aby byla zajištěna tajnost, je kód v samostatné obálce, která je zalepená. Volič

nezadává nikde své údaje a ověřuje se zadáním kódu. Při takovém postupu nelze pak identifikovat volbu voliče, ale hlasovací lístek je pouze uložen k ostatním na server. Narušení tajnosti volby může být zapříčiněno odcizením vygenerovaného kódu, kdy by jeden volič hlasoval ještě za dalšího voliče nebo vyvinutím nátlaku na voliče, aby zvolil kandidáta proti své vůli.

Jednoduchost obsluhy je dána výstižným návodem přímo na webových stránkách, kde se uskutečňuje hlasování. Zároveň volič obdrží manuál, jak při výběru kandidáta postupovat.

Bezpečnost systému proti útoku či změně odeslaného hlasu je řešena pomocí Javy. Java je použitá k vytvoření šifrovaného dialogu mezi voličem a volební komisí., zajišťuje šifrování ve voličově prohlížeči a tuto funkci udržuje až do chvíle doručení k volební komisi. Java applet, stažený na uživatelský počítač, je opatřen digitálním podpisem. Po potvrzení vybrané volby proběhne několik šifrovacích procesů. Bezpečnost a funkčnost systému může být narušena hned v prvním kroku při snaze zabránit voliči přístup na webovou stránku, takový útok se označuje jako DDoS (distributed denial of service).

Ekonomičnost se u elektronického volebního systému opět projevuje snížením nákladů a v ochraně životního prostředí, které není tolik zatěžované.

Španělský elektronický volební systém je založen na zadání identifikačního kódu na webové stránky volebního systému. Problém je v tom, že se už žádným jiným způsobem neověřuje, zda volí příjemce kódu, nebo někdo jiný. Kód umožní komukoliv odevzdat hlas. Samotná volba už je jednoduchá a měl by ji každý zvládnout. Instrukce se dají najít na internetu tak jsou distribuovány tištěné návody. Elektronický volební systém snižuje náklady na konání voleb. Oproti jiným zemím je tento systém využíván jen pro volby bez integrace jiných vlastností a využití.

7.4 Švýcarsko

Bezpečnost osobních dat byla v první fázi voleb zajištěna voličskou kartou, kterou se občan prokazoval u voleb nebo poslal kartu společně s hlasovacím lístkem poštou. Po změně způsobu identifikace voliče, byla vytvořena databáze a multifunkční systém, který dovoluje občanovi přístup k různým systémům státu nebo města. Pro volbu je generován speciální jednorázový kód, který dovoluje hlasování přes internet.

Přestože se jedná o široce uplatnitelný systém přístupů, předpokladem je vysoká bezpečnost systému a ochrany dat uživatele. Pro odlišení klasického přístupu k přístupu k volbám je generován jedinečný kód, který podporuje bezpečnost a důvěryhodnost volby.

Jednoduchost na obsluhu je dána intuitivní webovou stránkou, kdy občan klikne na žádoucí políčko a poté se mu otevře okno, do kterého je nutné vepsat identifikační údaje a po doplnění je volič posunut dál. Až k samotnému zaslání vybraného kandidáta. Existuje malá pravděpodobnost nepochopení funkčnosti a ovládání stránky. (Ch.ch: Who is entitled to vote?, 2013)

Bezpečnost proti útoku má zajistit kontrola všech kroků při zadávání hlasu voličem, zda nedošlo k jeho manipulaci a že byl řádně započítán. Volič je tak důkladně kontrolován a zároveň není ohrožena tajnost volby. Samostatný volební stroj ve volební místnosti je potom vybaven integrovaným fotoaparátem, což má eliminovat riziko spojené s malware. (Swissinfo.ch: Security questions hang over e-voting plans, 2013)

Ekonomičnost elektronického volebního je snížena zhruba o 50%, dle Kevina Seley. Tvrdí, že náklady jsou sníženy hlavně v oblasti výcviku volební komise, není nutné členy školit. Při volbě poštou jsou náklady na odeslání v režii občana, v případě volby přes internetovou síť, jsou náklady pro voliče i stát nesrovnatelné s dosavadním systémem papírových lístků. Finanční náklady na rozvoj a správu e-voleb se pohybují kolem 15 mil. CHF v časovém horizontu 10 let. Pokud uvažujeme počet oprávněných voličů ve výši 3,5 mil. obyvatel, pak náklady na voliče v rámci roku nedosahují ani půlku franku. Elektronický systém je možné využít na referenda a volby, tudíž nejde o jednoúčelný program, ale kantony Švýcarska se mohou podílet na tvorbě databází s povolením k volbě, voličského registru a příkladů na ovládání, které opět zajistí snížení výdajů. (Krimmer, 2006)

Dostupnost – zadání hlasu nebylo nikdy snazší. Pokud je občan registrován v seznamu, obdrží poštou materiály k volbám nebo referendu a v době konání voleb dle svého uvážení hlasuje přes internet. Odpadá tak starost o dobu otevření a místo volební komise, s další cestou na poštu s vyplněným lístkem nebo místem pobytu v době voleb či referenda. Jedinou podmínkou je počítač připojený k Internetu.

Bezpečnost a funkčnost systému byla nejdříve testována v tzv. trial verzi při běžné politické události. Tento krok ověřuje a definuje další požadavky na **snadné zavedení do**

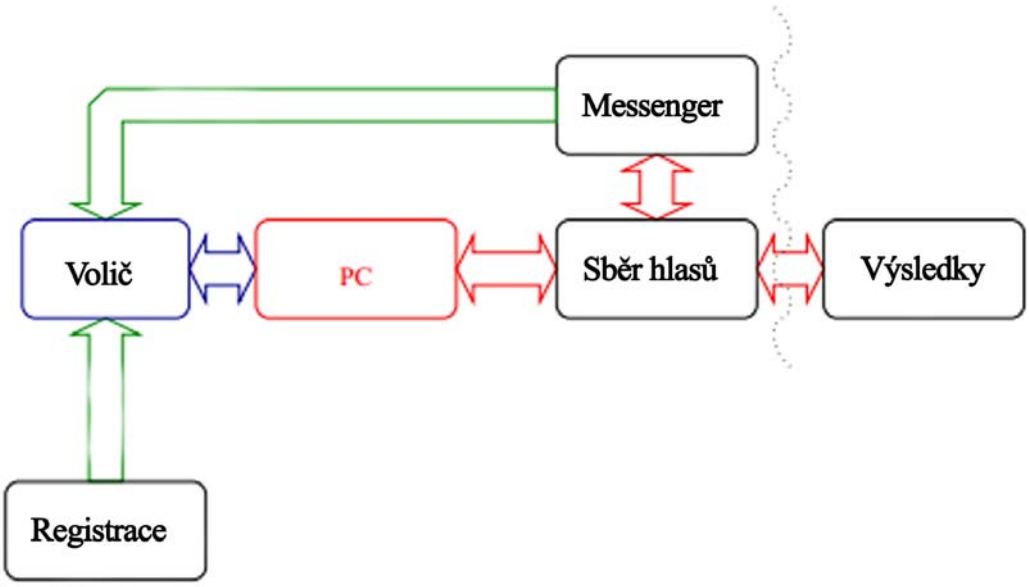
provozu. Švýcarsku se prokázala na zkoumaném vzorku nižší chybovost v zápočtu hlasů než při klasickém počítání odevzdaných hlasů.

Původní švýcarský systém spoléhal na poštovní služby, kdy byl hlasovací lístek společně voličskou – identifikační kartou zasílán v jedné obálce. Kdokoliv, komu by se obálka cestou k adresátovi dostala do rukou, by mohl pouhým otevřením obálky zjistit, kdo jak volil nebo dokonce hlasovací lístek zaměnit. Nový systém využívá multifunkční počítačový systém dostupný ze sítě internet. Výhoda tohoto systému spočívá v tom, že je využíván po celý rok ve státní a komunální sféře, což je výhodné jak z finančního, tak i z uživatelského hlediska. Volič se přihlašuje do systému, který důvěrně zná z komunikace s úřady. Rozdíl mezi volbami a ostatním použitím je jen v zadání speciálního kódu, který je pro každé volby znova vygenerován. Samotná volba je už jednoduchou záležitostí, několika kliknutí. Celkově se elektronické hlasování ve Švýcarsku osvědčilo, náklady na hlasování se snížily, stejně jako chybovost při sčítání hlasů.

7.5 Norsko

Bezpečnost osobních údajů nebo případný nátlak na volbu je ošetřen možností volit opakovaně, kdy je do výsledků započten až poslední hlas. Voliči je také umožněno jedenkrát volit papírovou formou, která nahrazuje předchozí elektronické hlasování. Obrana voliče proti nátlaku na zadání volby proti své vůli mimo volební místnost není snadná. Před tím, než občan potvrdí výběr kandidáta, musí se identifikovat před vstupem do systému. Ověřování pravosti může osob a s přístupem do systému jednoduše detekovat.

Jednoduchost je řešena včasným doručením voličských lístků, identifikačních čísel a kódů. Při přihlášení je zadáno heslo a PIN pro identifikaci. Poté je zadán výběr a hlas odeslán. Zároveň je voliči odesláno potvrzení, že hlas byl doručen a uložen.



Obrázek 18: Princip volby a ověřování *(Zdroj: Vlastní tvorba)*

Bezpečnost volebního systému v Norsku stojí na transparentnosti a šifrovacím protokolu. Šifrované hlasovací lístky jsou zasílány pomocí propojených sítí, tak aby výstup nebyl ovlivněn vstupem. Sítě mohou být založeny na vnořeném šifrování nebo rešifrování či pravděpodobnostním ověřování. Systém se také více soustředí na ochranu počítače před odesláním hlasu, který před podáním může být změněn. Jako šifrovací protokol využívá homomorfní šifrovací schéma.

Cena celého systému je v případě Norska omezena limitovanými zdroji dostupnými pro tvorbu protokolu. Zpětné potvrzení voliči o obdržení hlasu přes messenger, je považováno za nákladné. Přesto chce vláda přiblížit občanům volby a usnadnit jim výběr kandidáta.

Špatně definovaný systém může zapříčinit ztrátu nebo prolomení osobních dat. Proto je zřejmé, že zpracování rozdělené do více úkolů zvyšuje úroveň bezpečnosti.

7.6 Srovnání systémů

Systémy zahraničních elektronických volebních systémů byly hodnoceny dle zvolených zásad, kdy každá charakteristika byla bodována v rozmezí 1-5. Nejvyšší počet bodů znamená nejkvalitnější plnění. Metodou vázaného součtu bylo statisticky odvozeno nejlepší řešení hodnocených systémů. Tabulka 2 udává pořadí nejkvalitnějšího systému po nejméně spolehlivý systém. Na prvním místě je Švýcarsko, o prvenství se zasloužilo

sofistikovaným víceúčelovým systémem a širokou škálou způsobů volby aniž by byla ohrožena bezpečnost voličských dat. Hned v závěsu je Estonsko, které elektronické volby uzákonilo a upravilo právní formu. Na posledním místě se pak usadilo USA, voliči sice mají na výběr, jakým způsobem budou volit. Ale události posledních let nepřidaly volebním systémům na důvěryhodnosti. Elektronické volební systémy jsou v Americe spojené s modifikací hlasů nebo jejich nezapočtením. Navíc přístroje nejsou zrovna šťastně konstruovány a je snadné rychle poškodit systém malware a rozšířit „nákazu“ na další volební přístroje ve volební místnosti.

Max. / Min. = x / -	☑	☑	☑	☑	☑	☑
Váhy kritérií v (%)	16.67	16.67	16.67	16.67	16.67	16.67
Varianty / Kritéria	Bezpečnost dat	Jednoduchost	Bezpečnost syst	Ekonomičnost	Dostupnost	Zavedení systému
USA	3	3	1	2	4	2
Estonsko	4	4	3	5	5	5
Španělsko	4	3	3	4	4	3
Švýcarsko	5	5	4	5	5	5
Norsko	4	4	4	3	4	4

Tabulka 1: Vstupní data pro výběr nejlepšího systému

Pořadí	Název varianty	Hodnota WSA
1	Švýcarsko	1.0000
2	Estonsko	0.7778
3	Norsko	0.5000
4	Španělsko	0.3611
5	USA	0.0000

Tabulka 2: Hodnocení elektronických volebních systémů

8 NÁVRH NA ZAVEDENÍ ELEKTRONICKÉ VOLBY

8.1 Fáze bezpečnostního protokolu e-voleb

Fází, kterou se nejvíce odlišují běžné volby od elektronických, je možné chápat zejména proces ověřování identity a práva volit. Volební komise nebo volební zařízení kontroluje identitu v seznamu sestaveného na základě registru obyvatel, u e-voleb je ověření provedeno vzdáleně.

Jednotlivými kroky e-voleb mohou být:

1) **Marketing** – kampaň za účelem informování občanů o elektronickém průběhu voleb. Jakým způsobem mohou volit a zúčastnit se. Kampaň na lokální nebo radní úrovni může být provedena formou školení. Při celorepublikových nebo velkoplošných volbách je nezbytné voličům připravit demonstrační program, kde si může každý občan vyzkoušet a projít celý systém. Forma školení může proběhnout skrze internet nebo e-learningovým kurzem.
2) **Registrace voličů** – před volbami je nutné vytvořit zápis voličů do registračního seznamu, kde se vyloučí osoby mladší 18 let a osoby zbavené svéprávnosti. Kdy musí být voliči ubezpečeni o důvěryhodnosti systému a bezpečnosti zadaných dat. Seznam bude vycházet z registru obyvatel a registru vydaných elektronických občanských průkazů.
3) **Volební komise** – dle legislativy a běžných postupů je před začátkem voleb sestavena proškolená volební komise. Komise obdrží klíč k otevření elektronické volební urny pro volební místnosti a elektronické hlasování.
4) **Vlastní volby** – samotný průběh voleb, ať už klasických, elektronických nebo smíšených probíhá ve stanoveném období. Součástí volby je ověření voliče a potvrzení voliči o zadaném hlasu, který musí být bez spojitosti s obsahem zadaného hlasu a osobními daty voliče.
5) **Sčítání hlasů a publikace výsledků** – pokud je využito více metod pro zadání hlasu, vylučuje se duplicita u jednoho voliče, tak aby byl hlas zadán jenom jedenkrát. Teprve potom přichází na řadu sčítání hlasů a vydání výsledků voleb,

které započne uzavřením uren, volební komise pomocí klíče otevře elektronickou schránku s hlasy a začne sčítat. Každému voliči je umožněno před odesláním hlasu ověřit vyplněnou kandidátku na obrazovce a v případě potřeby opravit nebo potvrdit její odeslání. Volba na internetu bude ještě potvrzena na mobilní telefon nebo email, pokud volič vybere takovou možnost.

Elektronický hlasovací systém je další integrací vyspělé technologie do fungování každého moderního státu. Občané chtějí větší mírou zasahovat do fungování států, ovšem uspořádání voleb je zdlouhavý proces s velkou finanční náročností. Elektronické hlasování může celý proces voleb urychlit a finančně velmi zlevnit. Zabývá se jím spousta států a řadě z nich již elektronické hlasování funguje. Využívá se především vzdálené hlasování přes internet nebo ve volební místnosti přes elektronické hlasovací přístroje. Volba přes internet byla v prvé řadě určena pro voliče, kteří se nacházejí v zahraničí a nemají možnost hlasovat normálně ve volební místnosti. Volba obálkovou poštovní metodou hlasování je finančně velmi nákladná a při každém hlasování se náklady opakují. U elektronického hlasování jsou nejvyšší náklady při vývoji a zavádění systému do provozu. Udržování elektronického systému v provozu stojí už jen zlomek pořizovací ceny. Nejvyšší efektivity lze dosáhnout propojením internetového hlasování s elektronickým hlasováním ve volební místnosti.

8.1.1 Volba přes internet

V dnešní době je volba přes počítačovou síť internet i otázkou pohodlnosti a politici si od ní slibují i zvýšení účasti voličů při volbách. Počet domácností s přístupem na internet se každoročně zvyšuje a i s raketovým rozvojem přenosných počítačů a tabletů s připojením k síti se zvyšuje možnost hlasování ze kteréhokoliv místa. Hlasování přes internet počítá s elektronickou verzí občanského průkazu obsahující RFID čip a čtečkou karet. Občanské průkazy s integrovaným čipem se v České republice vydávají od roku 2012 a mají obsahovat digitální podpis. Z hlasování jsou vyloučení osoby mladší 18-ti let a osoby zbavené svéprávnosti. Pro volbu by stačilo navštívit speciální webovou stránku a podstoupit několik kroků:

1. Navštívit webovou stránku volebního systému
2. Vložit kartu občanského průkazu do čtečky paměťových karet
3. Přihlásit se pomocí zadáni PIN kódu, který si uživatel zvolil při vystavení karty.

4. Podle údajů z centrálního registru obyvatel se ověří, zda volič má právo volit. Dále podle trvalého bydliště připraví příslušné elektronické kandidátky.
5. Volič vybere, ve kterých volbách chce zadávat hlasy, pokud má na výběr.
6. Vybere kandidáta, stranu, preferenci nebo více kandidátů a potvrdí svůj výběr společně s přiložením digitálního podpisu.
7. Po úspěšném přijetí hlasu zašle vzdálený server potvrzení, které se zobrazí na monitoru a bude i uloženo v uživatelské části systému spolu s datem a časem volby.
8. Systém voliče následně odhlásí.
9. Pro další volbu nebo změnu se musí celý proces přihlášení opakovat

Bezpečnost: zaslání speciálního transakčního čísla pro autorizaci volby poštou, e-mailem nebo SMS zprávou nijak nezajistí, že odhlasovala jen oprávněná osoba. Neoprávněná osoba by musela disponovat občanským průkazem a znát jeho PIN. V takovém případě by si mohla změnit v systému číslo mobilního telefonu nebo e-mail pro doručení transakčního čísla. Zaslání kódu poštou by znamenalo, že si oprávněná osoba převezme transakční kód, ale samotnou volbu by mohl stejně provést někdo jiný, který by se ke kódu a občanskému průkazu dostal. Navíc by to znamenalo výrazné zvýšení nákladů na pořádání voleb, proto zasílání identifikačních dat poštou nebo sms zprávou nedoporučuji.

8.1.2 Volba ve volební místnosti

Proces identifikace a hlasování by se dal charakterizovat jako kombinace volby přes internet a původního systému hlasování ve volební místnosti. Každý oprávněný volič by měl možnost odevzdat svůj hlas bez ohledu na to, zda má přístup na internet, problémy s připojením nebo jestli už dokonce přes něj volil. Volba ve volební místnosti je brána jako pojistka v případě, že by se někdo dostal k přístupovým datům nebo donutil voliče vybrat jiného kandidáta než si přál při volbě přes internet. Ve volební místnosti se nachází minimálně 2 hlasovací terminály, které jsou připojeny přes internet se servery volebního systému. Do terminálu by ve volební místnosti nebylo možné připojit žádné paměťové médium, aby bylo zamezeno případnému napadení systému nežádoucím virem.

Volba a identifikace by probíhala následovně:

1. Volič se identifikuje občanským průkazem

2. Člen volební komise zkontroluje údaje na občanském průkazu a porovná s údaji z výpisu centrálního registru obyvatel. Zároveň zkontroluje fotografii na OP a porovná s voličem.
3. Volič se přesune k volebnímu terminálu
4. Vloží kartu občanského průkazu do čtečky paměťových karet
5. Přihlásí se pomocí zadáni PIN kódu, který si uživatel zvolil při vystavení karty
6. Podle údajů z centrálního registru obyvatel se ověří, zda volič má právo volit. Dále podle trvalého bydliště připraví příslušné elektronické kandidátky
7. Volič vybere, ve kterých volbách chce zadávat hlasy, pokud má na výběr
8. Vybere kandidáta, stranu, preferenci nebo více kandidátů a potvrdí svůj výběr
9. Po úspěšném přijetí hlasu zašle vzdálený server potvrzení, které se zobrazí na monitoru a bude i uložena v osobní části systému spolu s datem a časem volby.
10. Systém voliče následně odhlásí
11. Pro další volbu nebo její změnu se musí celý proces přihlášení opakovat

8.2 Postup určování platnosti hlasu

Jelikož má občan možnost volit zároveň jak na internetu, tak ve volební místnosti, je důležité stanovit pravidla, podle kterých se určí, který hlas se bude započítávat do výsledků voleb. V internetové variantě volby má volič možnost i opakovaně svoji volbu změnit.

Pravidla:

Z vícečetné internetové volby se bere jako platný hlas poslední odevzdaný hlas, kdy starý je vždy přemazán novějším.

Ve volební místnosti volič může hlasovat pouze jednou, případná další změna už není možná.

Pokud volič odevzdal svůj hlas v obou variantách hlasování, jako platný hlas je brán pouze ten odevzdaný ve volební místnosti.

ZÁVĚR

Po prozkoumání systému voleb z historického hlediska až do nynějších podob v různých státech je vybráno těch nejlepších parametrů pro tvorbu lepšího a uživatelsky příjemnějšího systému, umožňující pohodlné zvolení požadované strany či kandidáta. Při testování probíhají elektronické volby současně s klasickými volbami.

Okolní země využívají různé systémy voleb, ale většina funguje na systému vytvořeného společnosti SCYTL, přesto je mezi zeměmi poměrně velký rozdíl. Volební systémy se dělí na poll-, remote- and kiosk e-voting. Každý z uvedených přístupů má svá pro a proti. Poll site e-voting usnadňuje sčítání hlasů svojí částečnou elektronizací, stále je ale volič identifikován komisí, která ověřuje jeho identifikační dokumenty. Systém je v dnešní době výhodný zvláště pro seniory, kteří nejsou natolik zdatní ve využívání internetu a počítače. Definoval bych jej jako spojovací můstek s remote e-voting systémem. Vzdálené hlasování je propagováno s cílem zvýšit účast občanů na volbách, aby se podíleli větším dílem na rozhodování o své budoucnosti. Existuje několik technologií, jak poslat svůj hlas vybranému kandidátovi, např. volba pomocí pevné linky, mobilního telefonu nebo PC zařízení. Při takovém způsobu je ale kladen daleko vyšší důraz na bezpečnost osobních dat a bezpečnosti systému vůbec. Třetím typem je kiosk e-voting. Jde o výjimečnou formu volby, kdy není terminál umístěn ve volební místnosti, ale může být v knihovně a podobných veřejných prostorách. Přeci jenom člověk upřednostňuje pohodlí a rychlost před hledáním volebního terminálu, kde musí procházet zdlouhavou identifikací.

Rozhodnutí o zavedení elektronické volby s sebou v prvních letech nese vyšší náklady, protože bude udržováno více možností zadání volby. Což by mohlo zajistit plynulý přechod na nový systém. Uživatelé si na prostředí aplikace zvyknou a nebudou muset ztrácet čas přemisťováním se do volební místnosti, ověřováním identity nebo případným čekáním v zástupu voličů, kteří jdou také využít právo volby, aby ovlivnili složení poslanců na kraji či do parlamentu. Výbornou variantou se ukazuje zahrnutí volebního systému do celostátního programu, kdy by uživatel měl přístup k různým úřadům. Ověřování identity voliče nebo běžného uživatele a jeho oprávněnosti ke vstupu do systému bude vycházet z centrálního registru obyvatel. Volič se při přihlášení prokáže elektronickým občanským průkazem vybavený RFID čipem. Čip bude obsahovat informace o voliči a pro bezpečnost bude mít také nahraný digitální podpis.

ZÁVĚR V ANGLIČTINĚ

The survey of historical voting system to this time throughout foreign coutries cause a choice of the best parametrs for creating better and for user more comfortable system. There is an easy choice to cast for desired candidate. The e-voting is keeping at same time as clasical elections.

Countries arouond the Czech Republic use diferent voting systems, but most of them are on SCYTL's platform, in spite of exists quite big differences. The e-voting can be part: poll-, remote-, kiosk e-voting. All of this methods have pro and cons. Poll site e-voting makes vote counting easier its partial computerization, but the voter is still identified by the election board, whio verifies his identity documents. The current system is especially useful for seniors who are not so proficient in the use of internet and computers. I would define it as a connecting bridge with remote e-voting system. Remote voting is promoted in order to increase citizen participation in elections, to contribute a larger share in decisions about their future. There are several techniques to send your voice to selected candidate, as the choice of using a landline, mobile phone or PC device. In such a way, however, put much greater emphasis on security of personal data and security of all. The third type is a kiosk e-voting. This is an exceptional form of elections, because voting terminal is not located in the polling site but can be found in library and other public buildings. After all, people prefer convenience and speed before seeking election terminal, where they must go through a lengthy identification.

The decision to introduce e-voting means higher costs in the early years because more options will be maintained to given the option. It makes the transition to the new system seamless to the user. Users accustomed to the application environment and will not have to waste time moving into the polling station, verification of identity or potential waiting in the crowd of voters who go also use the right choices to influence the composition of the Members of the region or the parliament. Excellent option to show the inclusion of the electoral system in the national program, the user would have access to the various authorities. Verification of identity selector, or the current user and his eligibility to enter the system will be based on the central population register. The voter when you log shows an electronic identity card equipped with an RFID chip. The chip will contain information about voters and safety will also be recorded digitally signed.

SEZNAM POUŽITÉ LITERATURY

ANDERSON, Kirsten. Ohio Report Reveals Voting Machine Weaknesses. *The Huffington Post* [online]. [cit. 2013-03-18]. Dostupné z: http://www.huffingtonpost.com/kirsten-anderson/ohio-report-reveals-votin_b_77241.html

BRAWLEY, Allan. Vulnerable Voting Machines in Ohio?. *Huff Post Politics* [online]. [cit. 2013-04-29]. Dostupné z: http://www.huffingtonpost.com/allan-brawley/vulnerable-voting-machine_b_2020044.html

BUTLER, Kevin, William ENCK, Harry HURSTI, Stephen MCLAUGHLIN, Patrick TRAYNOR a Patrick MCDANIEL. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections on Project Everest. [online]. [cit. 2013-03-05]. Dostupné z: http://static.usenix.org/event/evt08/tech/full_papers/butler/butler.pdf

CANNING, Ernest. U.S. Government Demands Hand-Count of 'Paper Ballots' in Venezuelan Election, But Not Our Own. *The Brad Blog* [online]. [cit. 2013-04-29]. Dostupné z: http://www.bradblog.com/?p=9971

ELECTION DATA SERVICES. *Edssurvey.com* [online]. [cit. 2013-04-26]. Dostupné z: http://www.edssurvey.com/images/File/ve2006_nrpt.pdf

Election Data Service. Nation Sees Drop in Use of Electronic Voting Equipment. [online]. [cit. 2013-03-20]. Dostupné z: http://www.edssurvey.com/images/File/NR_VoteEquip_Nov-2008wAppendix2.pdf

Estonian e-voting system. In: *Estonia.eu* [online]. 2011 [cit. 2013-04-25]. Dostupné z: http://estonia.eu/about-estonia/economy-a-it/e-voting.html

Estonsko: První internetové volby na světě. In: *ISVS.CZ* [online]. 2007 [cit. 2013-04-27]. Dostupné z: http://www.isvs.cz/estonsko-prvni-internetove-volby-na-svete/

http://www.isvs.cz/estonsko-prvni-internetove-volby-na-svete/

Estonci spustili revoluční volby po internetu. In: *Idnes.cz* [online]. 2007 [cit. 2013-04-27]. Dostupné z: http://zpravy.idnes.cz/estonci-spustili-revolucni-volby-po-internetu-frv-/zahranicni.aspx?c=A070226_114110_zahranicni_tha

Estonian e-voting system. *Estonia.eu* [online]. [cit. 2013-05-25]. Dostupné z: http://estonia.eu/about-estonia/economy-a-it/e-voting.html

FELDMAN, Ariel, Alex HALDERMAN a Edward FELTEN. Security Analysis of the Diebold AccuVote-TS Voting Machine. *USENIX* [online]. [cit. 2013-04-11]. Dostupné z: http://votingmachines.procon.org/view.resource.php?resourceID=000276

GOURLEY, David, Brian TOTTY, Marjorie SAYER a Sailu REDDY. HTTP: The Definitive Guide. [online]. [cit. 2013-04-01]. Dostupné z: http://it-ebooks.info/read/1401/

GRITZALIS, D.A. *Secure Electronic Voting*. 2004, [cit. 2013-04-02].

GROSSMAN, Wendy. Why machines are bad at counting votes. *Theguardian* [online]. [cit. 2013-04-30]. Dostupné z: http://www.guardian.co.uk/technology/2009/apr/30/e-voting-electronic-polling-systems

HASTING, Rene PERALTA, Stefan POPOVENIUC a REGENSHIED. Security Considerations for Remote Electronic UOCAVA Voting. [online]. [cit. 2013-03-01]. Dostupné z: http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf

HERRNSON, S. P., G. R. NEIMI, J. M. HANMER, B. B. BEDERSON, G. F. CONRAD a W. M. HTTPS - zabezpečený HTTP protokol. *Promotic* [online]. [cit. 2013-05-11]. Dostupné z: http://www.promotic.eu/cz/pmdoc/Subsystems/Web/Https.htm

HUSTED, Jon. Country Voting Equipment. In: *Ohio Secretary of State* [online]. 2012 [cit. 2013-04-24]. Dostupné z: http://www.sos.state.oh.us/SOS/Upload/elections/votingsystems.aspx?page=25056

Ch.ch: Who is entitled to vote? [online]. [cit. 2013-05-15]. Dostupné z: https://www.ch.ch/en/voting-rights/

Internet Voting in Estonia. *Vabariigi Valimiskomisjon* [online]. [cit. 2013-04-27]. Dostupné z: http://www.vvk.ee/voting-methods-in-estonia/engindex

JEŠUTA, Martin. EVolby v Estonsku. In: *Restart* [online]. 2012 [cit. 2013-04-26]. Dostupné z: http://www.czrestart.cz/egovernment-eparticipace/evolby-v-estonsku

http://www.czrestart.cz/egovernment-eparticipace/evolby-v-estonsku

JEŠUTA, Martin. EVolby v Norsku. *Restart* [online]. [cit. 2013-04-27]. Dostupné z: http://www.czrestart.cz/egovernment-eparticipace/evolby-v-norsku

JONES, D.W. *Evaluation of voting technologies*. 2003, [cit. 2013-05-11].

KLÍMA, Vlastimil. Hašovací funkce, principy, příklady a kolize. [online]. [cit. 2013-03-19]. Dostupné z: http://cryptography.hyperlink.cz/2005/cryptofest_2005.htm#_Toc98987052

KRIMMER, Robert. Electronic Voting 2006. [online]. [cit. 2013-05-19]. Dostupné z: http://neu.e-voting.cc/wp-content/uploads/Proceedings%202006/1.2.braun_braendli_swiss_e-voting_27-36.pdf

Lupa.CZ: Volby v ČR, volby přes Internet a SMS, Estonsko budiž vzorem [online]. [cit. 2013-05-02]. Dostupné z: http://blog.lupa.cz/internet/volby-v-cr-volby-pres-internet-a-sms-estonsko-budiz-vzorem/

MACE, Kelvin. Reality check on Hart-Intercivic voting machine company and its owndership by Romney partisans. *DemocraticUndeground.com* [online]. [cit. 2013-03-16]. Dostupné z: http://www.democraticunderground.com/1091552

MAZAL, Jan. ČSÚ: Každý Čech s počítačem používá internet. *ChannelWorld* [online]. [cit. 2013-04-12]. Dostupné z: http://channelworld.cz/analyzy/csu-kazdy-cech-s-pocitacem-pouziva-internet-8525

MERCURI, Rebeca. *A Better Ballot Box?*. 2002, s. 46-50, [cit. 2013-04-17].

NOVOTNÝ, Marián. IW: Elektronické voľby – sci-fi alebo blízka budúcnosť?. *INFOWARE* [online]. [cit. 2013-04-09]. Dostupné z: http://www.itnews.sk/tituly/infoware/2009-11-09/c130130-iw-elektronicke-volby-sci-fi-alebo-blizka-buducnost

RETEROVÁ, Sylvie. *Alternativní způsoby hlasování: Od tradičních metod k on-line volbám*. 2009, [cit. 2013-04-18].

RIDVANOVÁ, Jana. Elektronické volební přístroje v USA opět volí jinak než voliči. *Britské listy* [online]. [cit. 2013-04-03]. Dostupné z: http://blisty.cz/art/43622.html

RIVEST, Ronald. Electronic voting. [online]. [cit. 2013-05-12]. Dostupné z: http://people.csail.mit.edu/rivest/Rivest-ElectronicVoting.pdf

ROSLAND, Geir. Remote electronic voting. [online]. [cit. 2013-05-20]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.9267&rep=rep1&type=pdf

RUBIN, Aviel. Communications of the acm. [online]. [cit. 2013-03-06]. Dostupné z: https://homepages.fhv.at/se/bp03/2003ws_bp03.ebdv_ue6.pdf

Swissinfo.ch: Security questions hang over e-voting plans [online]. [cit. 2013-04-12]. Dostupné z: http://www.swissinfo.ch/eng/swiss_news/Security_questions_hang_over_e-voting_plans.html?cid=32567608

ŠINDELÁŘ, Petr. Elektronické volby jako možný nástroj posílení demokracie. [online]. [cit. 2013-05-14]. Dostupné z: http://si.vse.cz/archive/proceedings/2006/elektronicke-volby-jako-mozny-nastroj-pro-posileni-demokracie.pdf

ŠINDELÁŘ, Petr. Elektronické volby. In: *Egovernment* [online]. 2009 [cit. 2013-04-21]. Dostupné z: http://www.egovernment.cz/archiv/PDF%204-06/4.pdf

TAJTL, Martin. Estonský eGovernment: od komunismu k internetové velmoci za 20 let. In: *Restart* [online]. 2012 [cit. 2013-04-26]. Dostupné z: http://www.czrestart.cz/egovernment/estonsky-egovernment-od-komunismu-k-internetove-velmoci-za-20-let

The Center for Association Growth: Top Ten Benefits to Electronic Voting [online]. [cit. 2013-04-26]. Dostupné z: http://www.tcag.com/connect/consider-this/governance/electronic-voting

TRAUGOTT. *Voting technology: the not-so-simple act of casting a ballot*. 2008, [cit. 2013-04-17].

TUČEK, Josef. Další volební chyba. Běžné, říkají vědci. *Aktuálně.cz* [online]. [cit. 2013-04-22]. Dostupné z: http://aktualne.centrum.cz/veda-a-zajimavosti/z-domova/clanek.phtml?id=284342

Voting Machines: How to Vote on an Electronic Voting Machine. *ProCon.org* [online]. [cit. 2013-05-04]. Dostupné z: http://votingmachines.procon.org/view.resource.php?resourceID=000276

Voting in Polling Division of Residence. *Vabariigi Valimiskomisjon* [online]. [cit. 2013-04-08]. Dostupné z: http://www.vvk.ee/voting-methods-in-estonia/voting-in-advance/advance-voting-in/

X.509 - Wickipedia, the free encyclopedia. [online]. [cit. 2013-05-21]. Dostupné z: http://en.wikipedia.org/wiki/X.509

Wikipedia, the free encyclopedia. [online]. [cit. 2013-05-21]. Dostupné z: http://en.wikipedia.org/wiki/Homomorphic_encryption

Základy kryptografie pro manažery: hashovací funkce. *Clever and Smart* [online]. [cit. 2013-05-03]. Dostupné z: http://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-hashovaci-funkce/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
CA	Certificate Autority
ČSÚ	Český statistický úřad
DDoS	Distributed denial of service
DES	Data Encryption Standard
DRE	Direkt-recording electronic voting systém
EVS	Elektronické volební systémy
EZS	Elektronický zabezpečovací systém
FPTP	First-past-the-post
HAVA	The Help Americe Vote act
ODS	Občanská demokratická strana
OP	občanský průkaz
OS	Optical scan
PC	Personal computer
PIN	Personal indetifical numer
RFID	Radio Frequency Identification
SERVE	Secure Electronic Registration and Voting Experiment
SIM	subscriber identity module
SMS	Short message service
SSL	Secure Sockets Layer
SW	Software
TLS	Transport layer security
UOCAVA	Uniformed and Overseas Citizen Absentee Voting Act
USA	United States of America
USB	Universal serial bus
VOI	Vořiny over Internet

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH