Metody dosažení spolehlivosti elektronických voleb

Methods for achieving the reliability of electronic voting

Bc. Michaela Sedlářová

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Bc. Michaela SEDLÁŘOVÁ**
Osobní číslo:	**A09396**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Metody dosažení spolehlivosti elektronických voleb**

Zásady pro vypracování:

1. **Význam elektronického hlasování v egovernmentu.**
2. **Metody dosažení spolehlivosti.**
3. **Určení kvantitativních a kvalitativních parametrů pro aplikace elektronického hlasování.**
4. **Hodnocení vybraných přístupů k elektronickým volbám.**
5. **Porovnání hodnocených přístupů.**
6. **Závěr.**

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.**
6. **Alexander Prosser, Robert Krimmer (Eds.): Electronic Voting in Europe – Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, July, 7th–9th, 2004, in Schloß Hofen / Bregenz, Lake of Constance, Austria, Proceedings. GI 2004, ISBN 3-88579-376-8**
7. **Leenes, R., Svensson, K.: Adapting E-voting in Europe: Context matters.Proceedings of EGPA, 2002.**

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

Datum zadání diplomové práce: **22. července 2011**

Termín odevzdání diplomové práce: **2. září 2011**

Ve Zlíně dne 28. února 2011

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Hlavnou témou tejto diplomovej práce sú elektronické voľby so zameraní sa na ich bezpečnosť. Práca v teoretickej časti obsahuje bližšie informácie o elektronických voľbách a ich významu pre e-government a podrobne informuje o metódach pre dosiahnutie spoľahlivosti elektronického hlasovania. V praktickej časti sa nachádza hodnotenie elektronických volebných systémov z pohľadu ich bezpečnosti, systém pre hodnotenie e-volieb, porovnanie a vyhodnotenie jednotlivých volebných systémov.

Kľúčová slová: elektronické voľby, elektronické hlasovanie, e-voľby, e-government, zabezpečenie volebného systému, formy autentizácie, asymetrické šifrovanie.

ABSTRACT

The main theme of this thesis is electronic voting, aimed at its safety. The thesis in theoretical part contents more information about electronic voting and its importance for e-government and in detail informs about the methods for achieving the reliability of electronic voting. In the practical part is the assessment of the electronic voting systems with focus on their security, system for assessment e-voting, comparison and evaluating voting systems.

Keywords: electronic voting, electronic election, e-government, security of voting system, forms of authentications, asymmetric encryption.

Na tomto mieste by som chcela poďakovať vedúcemu mojej diplomovej práce Ing. Radku Šilhavému PhD. za cenné rady, pripomienky a poskytnutie študijných materiálov pri písaní tejto práce.

Rovnako chcem poďakovať svojej rodine za podporu nielen pri písaní diplomovej práce, ale aj počas celého môjho štúdia.

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 02.09.2011 ……

podpis diplomanta

OBSAH

ÚVOD

Voľby sú významný nástroj na rozvoj demokratickej spoločnosti a základný prostriedok prenosu moci ľudu na zastupiteľské orgány. Rozvoj technológií prináša nové možnosti, ako tento nástroj realizovať moderne, elektronicky.[10]

Na úvod je použitý citát z jedného článku RNDr. Novotného, ktorý vystihuje dôležitosť volieb v každom demokratickom štáte a zároveň pripomína, že súčasné technológie umožňujú zmodernizovanie spôsobu konania volieb – elektronickým hlasovaním. Zavedenie elektronického volebného systému zároveň tvorí aj základ pre vytvorenie e-governmentu – elektronizácii verejnej správy.

Elektronické hlasovanie je bezpodmienečne moderná a komfortná forma hlasovania, ktorá ponúka možnosť hlasovať i z domu. Zároveň prináša množstvo príležitostí ako tieto voľby zmanipulovať. Z tohto dôvodu je najväčšou prioritou jednoznačne ich bezpečnosť, preto pri vytváraní systému elektronických volieb musí byť jednou z hlavných priorít vytvorenie konceptu pre ich spoľahlivosť.

Táto diplomová práca ja zameraná, ako už jej názov naznačuje, na elektronické voľby a metódy pre dosiahnutie ich spoľahlivosti. Prvá kapitola v teoretickej časti je určená pre predstavenie e-governmentu a významu elektronického hlasovania v ňom. Na prvú kapitolu nadväzuje druhá, ktorá je venovaná samotným elektronickým voľbám. Je v nej vysvetlené, čo elektronické voľby sú, jeho základné delenie a aké formy elektronického hlasovania vo voľbách už bežne prebiehajú v iných štátoch. Podrobnejšie je popísané ako prebieha internetové hlasovanie v Estónsku a elektronické hlasovanie prostredníctvom hlasovacích prístrojov a mobilných telefónov v Spojených štátoch amerických.

Metódy pre dosiahnutie spoľahlivosti elektronických volieb sú podrobne rozobrané v tretej, poslednej kapitole teoretickej časti. Ako prvé sú uvedené možnosti autentizácie voliča – identifikačnou kartou, bezpečnostným tokenom, heslom PIN kódom, alebo biometrickými údajmi. Po autentizácii nasleduje zabezpečenie samotného hlasovania šifrovaním.

Hlavnou témou v praktickej časti je hodnotenie elektronických volebných systémov z pohľadu bezpečnosti, hodnotené sú najviac používané typy elektronického hlasovania vo svete. Súčasťou je i systém pre vyhodnotenie bezpečnosti elektronického hlasovania,

na základe jednotlivých bezpečnostných prvkov v nich využitých. Na záver je i niekoľko volebných systémov vyhodnotených..

.

I. TEORETICKÁ ČASŤ

1 VÝZNAM ELEKTORNICKÉHO HLASOVANIA V E-GOVERMENTE

1.1 E-government

E-government sa zaoberá elektronizáciou výkonu verejnej správy pri aplikácii informačno-komunikačných technológií v procesoch verejnej správy. V kompetencii ho má Ministerstvo vnútra.[19] Bol navrhnutý ako jeden z programových cieľov už v roku 2002 v akčnom pláne k predloženiu Európskej rade na zasadaní v Seville.[1]

On-line komunikácia funguje v nasledujúcich procesoch:

- V rámci inštitúcií VS (G2E – Government to Employee)
- Medzi inštitúciami VS navzájom (G2G – Government to Government)
- Medzi verejnou správou a občanmi (G2C - Government to Citizen)
- Medzi verejnou správou a podnikateľkou sférou (G2B - Government to Business)
- Medzi verejnou správou a administratívou (G2A - Government to Administration) [19]

1.1.1 Potenciálne prínosy a riziká e-governmentu

Elektronizácia verejnej správy má výrazný prínos pre občanov, podnikateľov, štátnu správu i samosprávu. Pretože znižuje čas vybavovania úradných záležitostí, minimalizuje chybovosť, eliminuje viacnásobnú realizáciu rovnakých úkonov. Občan i podnikateľ bude môcť vybaviť úradné záležitosti na jednom mieste, prípadne priamo z domu, alebo kancelárie pomocou elektronického podpisu prostredníctvom ústredného portálu verejnej správy a budú i rýchlejšie spracované. Rovnako je ľahké a rýchle sa dozvedieť najnovšie a dôležité informácie. Verejná správa je preto efektívnejšia, transparentnejšia, bez zbytočného papierovania vďaka elektronickej forme spracovania dokumentov a komunikácie.[19]

Jedným z ďalších cieľov e-governmentu je väčšia účasť občanov, ktorí prostredníctvom internetu môžu ľahšie komunikovať so štátnymi úradníkmi a politikmi a zúčastňovať sa interaktívnych prieskumov, ktoré umožnia vidieť ich názory.

Hlavným rizikom sú rozhodne kybernetické útoky a následné narušenie ochrany popr. zverejnenie osobných resp. firemných údajov a informácií.

1.2 Elektronické hlasovanie a e-government

Hlavnú úlohu pri elektronizácii verejnej správy má bezpodmienečne elektronické hlasovanie. Pre verejnú správu majú voľby rozhodne veľký význam a ich elektronizácia tvorí základ e-governmentu. Samotnému elektronickému hlasovaniu sú venované nasledujúce kapitoly.

2 ELEKTRONICKÉ VOĽBY

S rozvojom informatizácie spoločnosti a rozšírením internetu sa v 21. storočí objavujú prvé pokusy s voľbami cez internet. V mnohých krajinách prebiehali voľby experimentálne, jednak na lokálnej úrovni, jednak ako doplnok k celoštátnemu hlasovaniu. Primárne voľby Demokratickej strany v Arkansase v roku 2000 boli jedným z prvých pokusov. Ďalšie prebiehali napr. vo Veľkej Británii v roku 2002, kde mali voliči možnosť vyskúšať si aj iné formy – hlasovanie pomocou terminálu, posielaním SMS správ alebo cez digitálnu TV.[10]

2.1 Čo sú elektronické voľby?

Elektronické voľby alebo e-voľby („e-voting“\), môžeme definovať ako voľby, v ktorých má volebný hlas výhradne elektronickú podobu. Teda proces, v ktorom je akt voľby občanom uskutočnený priamo prostredníctvom elektronického zariadenia a jeho výsledok odovzdaný na spracovanie prostredníctvom elektronického prenosového média (komunikačnej siete) a ďalej spracovaný výhradne elektronickou cestou. Za elektronické voľby teda nemožno považovať voľby, v ktorých vystupujú informačné technológie iba vo fáze spracovania výsledkov.[14]

Elektronické voľby sú logický a očakávaný krok na základe dnešnej „elektronizovanej“ doby. Všetko má však svoje pozitíva i negatíva. Medzi výhody rozhodne patrí rýchle sčítanie hlasov, pravdepodobný nárast najmä mladých voličov, napríklad hlasovanie cez internet dáva možnosť hlasovania i mimo trvalého bydliska, dokonca i z iného štátu, zamedzenie vzniku neplatného hlasu (napr. volič omylom na volebnom lístku zaškrtne viac kandidátov).

Za nevýhodu môžeme považovať počiatočnú nedôveru voličov a rozhodne nie malé náklady súvisiace najmä so zavedením e-volieb. Za najväčšie riziko rozhodne môžeme považovať možné zmanipulovanie výsledkov hackerskými útokmi, preto je veľmi dôležité myslieť na bezpečnosť e-volieb a ich pri zavádzaní ju brať za prioritu.

Niektoré štáty, ako už bolo spomenuté, majú už elektronické hlasovanie odskúšané, či v rámci testovania alebo reálne vo voľbách. Medzi ne patrí napríklad Nemecko, Belgicko, Estónsko, USA, Veľká Británia, Taliansko, Švajčiarsko, Španielsko, Švédsko a Fínsko. Najrozvinutejším štátom, čo sa týka e-volieb je určite Estónsko. Tento rok však volilo

elektronicky aj Írsko, Švajčiarsko a pridá sa k nim aj Turecko s Nórskom. Kompletná mapa sveta so znázornením postoja štátu k elektronickým voľbám sa nachádza v prílohe.

2.2 Remote electronic voting

„Elektronické voľby na diaľku“ sú voľby uskutočnené v presne definovanom čase prostredníctvom ľubovoľného elektronického zariadenia splňujúce technické požiadavky kompatibility so zvoleným volebným systémom [14]. Hlasovanie cez internet je už bežné napríklad v Estónsku alebo Švajčiarsku. V Španielsku a vo Veľkej Británii prebehlo hlasovanie mobilným telefónom prostredníctvom SMS správy.

2.2.1 Internetové hlasovanie v Estónsku

Tu sa elektronické voľby stávajú realitou. V marci tohto roku sa parlamentných volieb zúčastnilo viac ako 104 000 voličov elektronicky, čo je štvrtina všetkých voličov. Na základe nasledujúcej tabuľky je vidieť, že elektronické hlasovanie má v Estónsku exponenciálny rast.

Tabuľka 1 Prehľad e-voličov vo voľbách [17]

Rok konania volieb	Typ volieb	Podiel e-voličov z počtu všetkých zúčastnených voličov
2005	*regionálne voľby*	**2%**
2007	*parlamentné voľby*	**5,5%**
2009	*Európsky parlament*	**15%**
2009	*regionálne voľby*	**16%**
2011	*parlamentné voľby*	**25%**

2.2.1.1 Estónska ID karta

Od roku 2002 sa v Estónsku používajú tzv. ID karty, ktoré slúžia ako identifikačné preukazy, zároveň však majú aj strojovo čitateľný kód a mikročip. Mikročip obsahuje všetky údaje, ktoré sú na karte (okrem fotky a podpisu), dva digitálne certifikáty – jeden k autentizácii, druhý k elektronickému podpisu a súkromné kľúče chránené PIN kódmi.[15]

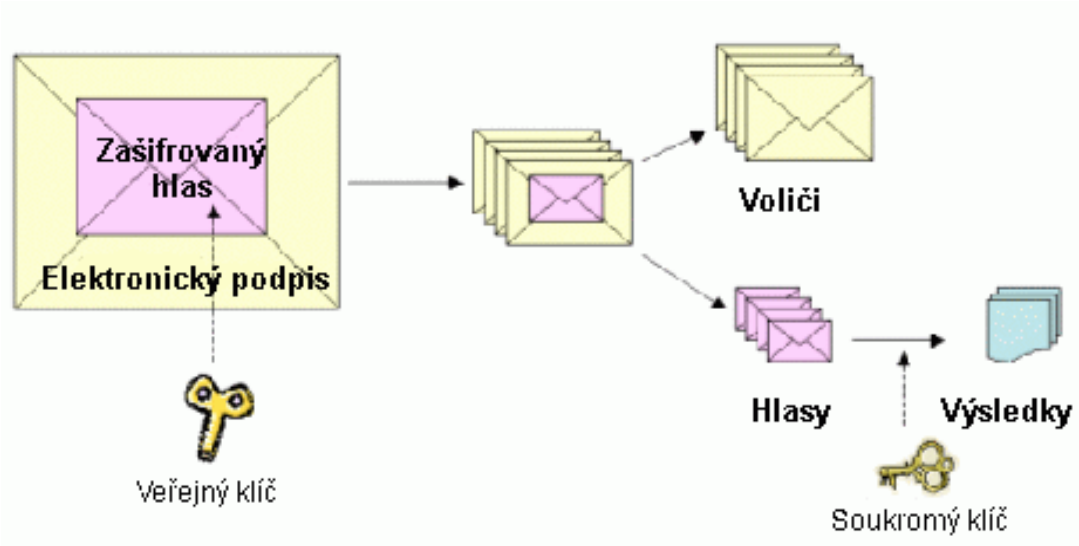
Obrázok 1 Estónska ID karta [15]

2.2.1.2 Princíp hlasovania

Základ pre hlasovanie tvorí už spomínaná ID karta a čítačka kariet. Volič sa prostredníctvom ID karty a PIN1 kódu identifikuje na stránke http://www.valimised.ee/. Server na základe registru obyvateľstva overí, či volič je oprávnený voliť a ak áno zobrazí kandidátku pre príslušný volebný obvod. Volič vykoná svoju voľbu, ktorá je následne zašifrovaná a systém si následne vyžaduje potvrdenie voľby elektronickým podpisom ku ktorému je potrebné zadať PIN2 kód. [15]

Obrázok 2 Ukážka ID karty v čítačke kariet [10]

Popisované šifrovanie v predchádzajúcom odseku je možné graficky vidieť na nasledujúcom obrázku. Prvé šifrovanie predstavuje vnútorná (ružová) obálka, druhé šifrovanie je znázornené vonkajšou (žltou) obálkou.



Obrázok 3 Bezpečnostné schéma e-volieb v Estónsku [15]

2.2.2 Elektronické hlasovanie prostredníctvom mobilného telefónu

Ďalšou možnosťou ako vykonať „elektronické voľby na diaľku“ je mobilný telefón. V niektorých štátoch už volenie prostredníctvom mobilného telefónu prebehlo a to dvomi spôsobmi, buď s telefónom s tónovou voľbou alebo prostredníctvom SMS správy.

2.2.2.1 Telefón s tónovou voľbou

S týmto typom e-volieb sa môžeme stretnúť napríklad v USA. Volič sa musí zaregistrovať ešte pred voľbami, nahlásiť telefónne číslo, z ktorého bude vykonávať voľbu, následne dostane ID číslo, ktorým sa bude identifikovať.

Samotná voľba prebieha s automatom, ktorý hovorí, čo máte robiť a zadávate svoju voľbu stláčaním príslušných čísel podobne ako u našich telefónnych operátoroch na zákazníckej linke.

Bezpečnosť tohto hlasovania je zabezpečená, tým že všetky telefónne hovory sú monitorované počítačovým systémom, umiestneným na bezpečnom mieste, ktorý je riadený a kontrolovaný len autorizovanými osobami. Počítač umožní prístup do systému len telefónnym s číslam, ktoré boli vložené do systému pred voľbami.

Systém pre hlasovanie telefónom je zakaždým testovaný pred konaním volieb, pre zabezpečenie presného naprogramovania. Tento systém nevyužíva pripojenie cez internet alebo inej dátovej siete. Jediný vstup do systému prichádza prostredníctvom DTMF tónov.

V USA sú firmy, ktoré ponúkajú bezpečné hlasovanie pre rôzne organizácie, ktoré chcú na základe tajného hlasovania obsadiť nejakú pracovnú pozíciu. Je to napríklad firma VoiceVote, priebeh hlasovania je obdobné ako som popísala u voľbách do verejnej správy.

Obrázok 4 Elektronické hlasovanie prostredníctvom mobilného telefónu [43]

2.2.2.2 SMS správou

Hlasovanie SMS správou funguje na podobnom princípe ako u telefónu s tónovou voľbou, ale všetky informácie – ID číslo voliča, PIN kód a číslo kandidáta, volič odošle SMS správou.

2.3 Poll-site electronic voting

Druhý typ elektronických volieb tzv. poll-site electronic votig sú voľby uskutočnené v presne definovanom čase prostredníctvom zákonom definovaného elektronického

zariadenia umiestneného na zákonom definovanom mieste (väčšinou vo volebnej miestnosti) [14]. Na rozdiel od predchádzajúceho typu je teda nutné rovnako ako u bežných „papierových“ volieb ísť kvôli hlasovaniu do velebnej miestnosti, kde sa hlasuje na hlasovacích prístrojoch, ktoré majú väčšinou dotykovú obrazovku a volič na nej jednoducho dá svoj hlas ním vybranému kandidátovi.

Obrázok 5 Dotyková obrazovka hlasovacieho prístroja použitého v Holandsku [11]

2.3.1 Použitie elektronických hlasovacích zariadení v Spojených štátoch amerických

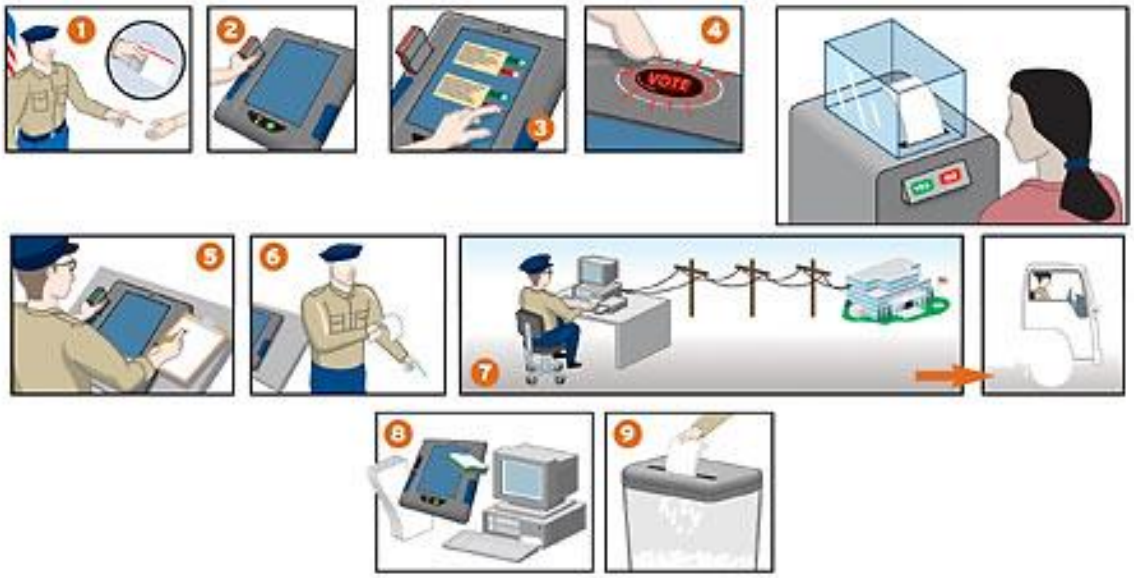
Poll-site electronic voting je bežný v Spojených štátoch amerických, kde sa elektronické hlasovanie vykonáva väčšinou prostredníctvom hlasovacích prístrojov.

2.3.1.1 Ako prebieha hlasovanie?

Priebeh volieb je podobný ako u bežných volieb, len prebieha elektronicky. Hlasovanie sa môže mierne líšiť na základe typu hlasovacieho prístroja. Nasledujúci popis hlasovania je

vykonávaný na hlasovacom zariadený ES&S IVotronic od společnosti Election Systems & Software.

1. Pracovník, vo volebnej miestnosti vám odovzdá osobný elektronický volebný lístok – PEB (Personal Electronic Ballot) obsahujúci čip, ktorý uloží do pamäte váš hlas.
2. S elektronickým volebným lístkom pôjdete do volebného boxu a vložíte ho do hlasovacieho zariadenia pre aktiváciu hlasovania.
3. Zariadenia vás nechá v jednotlivých krokoch vykonať vašu voľbu.
4. Po ukončení hlasovania stlačíte veľké červené tlačidlo pre uloženie hlasu. Hlas je následne uložený do vnútornej pamäte prístroja. Niektoré štáty následne vyžadujú overenie voľby ešte „papierovo“. Za sklenenou alebo plastovou stenou skontrolujete papierový výpis vašej voľby a následne stlačíte tlačidlo s voľbou „prijať“ alebo „odmietnuť a zadať znova“.
5. Každú hodinu pracovník manuálne skontroluje či sa zhoduje počet hlasov s počtom voličov, ktorí prišli do volebnej miestnosti.
6. Po ukončení volieb sú hlasy z každého hlasovacieho zariadenia vytlačené a nahrané do hlavnej PEB jednotky vo volebnej miestnosti.
7. Do volebných centrál sú odoslané cez šifrovanú telefónnu linku a výtlačky a hlavná PEB jednotka sú následne doručené osobne.
8. V prípade, že by bolo potrebné nové prepočítanie hlasov, alebo došlo k nejakému rozporu, všetky hlasy sú uložené na niekoľkých miestach: v hlasovacom zariadení, na výtlačku z hlasovacieho prístroja, v hlavnej PEB jednotke, v počítačoch na miestnych okrskoch a vo volebných centrálach.
9. Všetky záznamy sú zničené v súlade s právnymi predpismi štátu po uplynutí určitého počtu dní.



Obrázok 6 Priebeh hlasovania na hlasovacom zariadení ES&S IVotronic [20]

Obrázok 7 Hlasovacie zariadenie ES&S IVotronic [20]

2.3.1.2 Hlasovací prístroj Diebold Election Systems

Je jedným z najpoužívanejších hlasovacích prístrojov, ktorý umožňuje pomocou slúchadiel hlasovanie aj zrakovo postihnutým ľuďom.

Základne parametra tohto prístroja:

- 400-MHz Intel PXA-255 CPU
- Windows CE
- 64 MB flash pamäť
- Vyberateľná 32MB-128MB PCMCIA pamäťová karta pre ukladanie hlasov
- 9-12-palcový dotykový displej [20]

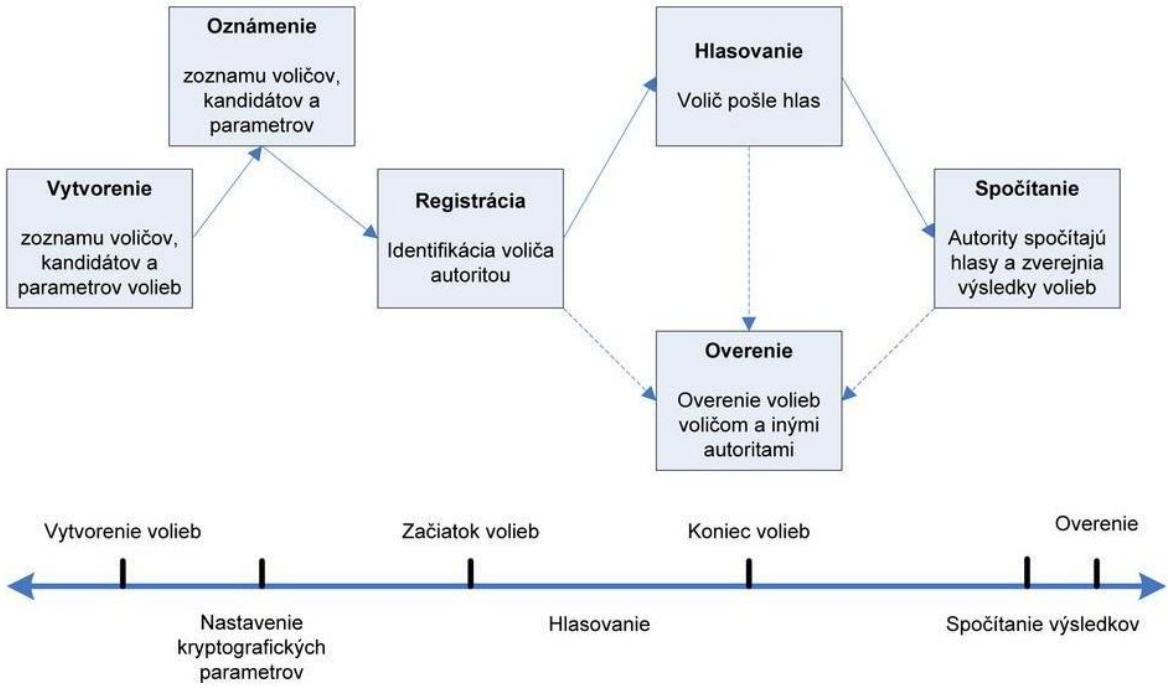
Obrázok 8 Hlasovací prístroj Diebold Accuvote-TS [20]

2.4 Bezpečnostné požiadavky na elektronické voľby

1. Oprávnenosť – len oprávnení voliči, ktorí sú na zozname voličov môžu voliť, voľba musí byť jedinečná.
2. Súkromie – nie je možné vytvoriť spojenie medzi jednotlivou voľbou a voličom.
3. Overiteľnosť – možnosť overiť, či hlas bol zaznamenaný a započítaný do výsledku volieb
    - Individuálna – samotný volič vie overiť svoj hlas
    - Univerzálna – ktokoľvek môže overiť, či hlasy boli správne spočítané

4. Nespochybniteľnosť – schéma by mala poskytovať mechanizmy na vyriešenie nezrovnalosti v každej fáze
5. Správnosť – hlasy musia byť správne zaznamenané a započítané
6. Spravodlivosť – nikto by nemal byť schopný vypočítať čiastočné výsledky, pokiaľ prebiehajú voľby
7. Robustnosť – schéma je maximálne robustná, ak je potrebná spolupráca všetkých autorít na volebný podvod resp. chybu
8. Bezdokladovosť – volič nie je schopný poskytnúť dôkaz o svojej voľbe niekomu inému
9. Nedonutiteľnosť – útočník by nemal byť schopný prinútiť voliča k určitej voľbe
10. Škálovateľnosť
11. Praktickosť – schéma by mala byť realizovateľná [14]

Elektronické voľby pozostávajú z niekoľkých fáz a tie v priebehu celých volieb musia nasledovať v presnom poradí, ako je to znázornené v nasledujúcom obrázku.



Obrázok 9 Fázy realizácie bezpečnostného protokolu elektronických volieb [10]

3 METÓDY PRE DOSIAHNUTIE SPOĽAHLIVOSTI ELEKTRONICKÝCH VOLIEB

Prioritou u elektronických volieb musí byť zabezpečenie ich spoľahlivosti. Táto kapitola je venovaná práve metódam ako túto spoľahlivosť dosiahnuť.

3.1 Formy autentizácie

Prvým bezpečnostným krokom pri elektronickom hlasovaní je autentizácia voliča, je dôležité zabezpečiť aby nebolo možné sa prihlásiť miesto niekoho iného a tak zneužiť jeho hlas. Je niekoľko spôsobov ako tomu zabrániť a dosiahnuť čo možno najväčšiu bezpečnosť. Jednou možnosťou je autentizácia nejakým predmetom, najčastejšie používaná je identifikačná karta – čipová karta alebo karta s magnetickým prúžkom, tie sú dnes už ale na ústupe, možné je tiež použiť bezpečnostný token. Druhou možnosťou je autentizácia na základe niektorej biometrickej metódy a treťou je použitie hesla alebo PIN kódu. Pre zvýšenie bezpečnosti je dobrá kombinácia aspoň dvoch týchto foriem.

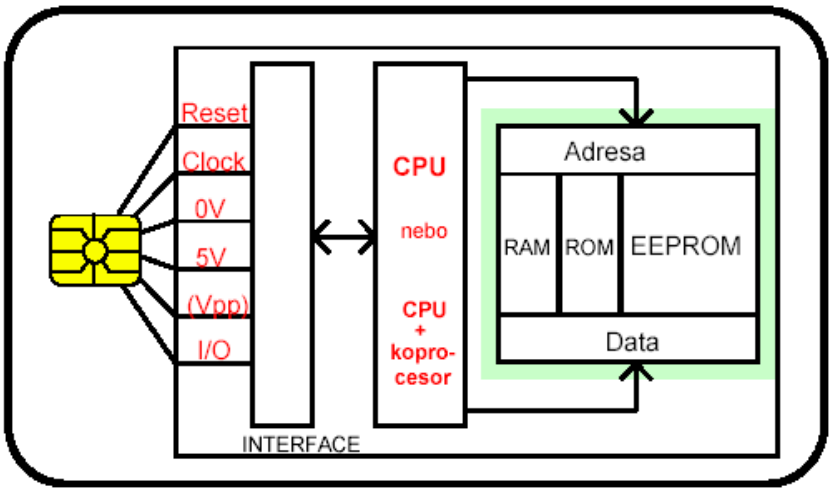
3.1.1 Čipové karty

Dnes už čipové karty nie sú žiadnou novinkou, používame ich denne a časom nám nahradia všetky „papierové doklady“. Základom čipovej karty je polovodičový čip vytvorený špeciálne pre jej konštrukciu. V súčasnosti už väčšina obsahuje mikroprocesor, špecializovaný kryptografický koprocesor, rôzne typy pamäte a prvky pre prenos dát integrované na jednom čipe. Moderné čipy majú implementované množstvo bezpečnostných mechanizmov, ktoré sťažujú rôzne typy útokov na ich bezpečnosť. Dôležitou súčasťou karty je operačný systém umiestnený v ROM pamäti v rámci výrobných fáz čipu. [39] Karta je vyrobená najčastejšie z PVC alebo ABS materiálu. Základné delenie čipových kariet je na kontaktné a bezkontaktné čipové karty.

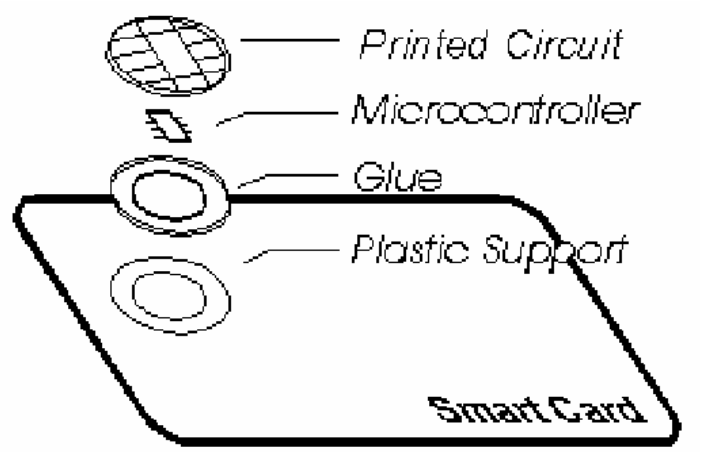
3.1.1.1 Kontaktné čipové karty

Kontaktná čipová karta sa dá rozoznať na základe plochy s ôsmimi kontaktmi, ktorých umiestnenie a funkcie sú presne stanovené v norme ISO/IEC 7816. Jednotlivé kontakty slúžia pre napájania čipu, sériovú komunikáciu, privedenie externého taktovacieho signálu

a programovacieho napätia. Dôležité sú dva kontakty rezervované pre budúce využitie, ktoré sa v súčasnosti používajú u niektorých kariet pre alternatívne USB rozhranie [39].



Obrázok 10 Štruktúra kontaktnej procesorovej čipovej karty [40]



Obrázok 11 Fyzická konštrukcia čipovej karty [40]

3.1.1.2 Bezkontaktné čipové karty

Bezkontaktné karty na rozdiel od predchádzajúcich kontaktných kariet nemusia byť pri ich použití zasunuté v čítačke kariet ani na nej priložená, úplne stačí pokiaľ je v dostatočnej blízkosti, ktorá je závislá od typu použitej karty a čítacieho zariadenia. Princípom činnosti týchto kariet je, že energia sa prenáša vo forme indukcie elektromagnetického pola z čítačky do antény čipovej karty. Energia indukovaná v anténe karty slúži k napájaniu čipu. Prenos informácie z karty do čítačky funguje na princípe záťažovej modulácie, kedy

odoberá určité množstvo energie z elektromagnetického pola čítačky a po prenose energie na kartu, karta spätne vyšle informáciu, ktorú čítačka vyhodnotí. [39]

3.1.2 Karty s magnetickým prúžkom

Karty s magnetickým prúžkom existujú už vyše štyridsať rokov. Riadia sa štandardom EMV, rozmery a umiestnenie magnetického prúžku sú dané normou ISO 7811. Magnetický prúžok môže obsahovať až tri stopy na rôznych pozíciách. Sú dva typy magnetických kariet – High Coercivity (HiCo) a Low Coercivity (LoCo). [39]

Identifikačné karty s magnetickým prúžkom slúžia len ako pamäťové médium, na ktoré sa zaznamenáva stopa s informáciami. Technológia magnetického prúžku nie je viazaná s elektronikou vo vnútri karty, je to iba magnetická vrstva nanesená na kartu pred laminációu. [39]

3.1.2.1 LoCo

Tieto karty sú jednoduchšie na kódovanie a magnetické prúžky sú väčšinou bledohnedej farby.

3.1.2.2 HiCo

Cena týchto kariet je o niečo vyššia, než u predchádzajúcich LoCo, Sú odolnejšie pred poškodením, ich prúžok je tmavý až čierny a pre kódovanie je vyžadovaný vyšší výkon.

Obrázok 12 Identifikačné karty s magnetickým prúžkom

3.1.3 Bezpečnostné tokeny

Bezpečnostný token je fyzické zariadenie, ktoré umožňuje jednoduchú autentizáciu v informačnom systéme. Používa sa buď miesto zadania hesla, alebo k heslu. Tieto zariadenia sú obyčajne dostatočne malé, vyhotovené vo forme prívesku na kľúče alebo identifikačnej karty. Niektoré obsahujú aj kryptografické kľúče, ako napríklad elektronický alebo biometrické dáta. Vyrábajú sa aj prevedenia v teplo odolnom puzdre, alebo s malými tlačidlami pre zadanie PIN kódu. [38]

Obrázok 13 Niekoľko druhov bezpečnostných tokenov [38]

Najjednoduchšie tokeny nepotrebujú pripojenie k počítaču, jeho majiteľ musí číselný kód opísať ručne ako to vidíme na nasledujúcom obrázku. Priame pripojenie k počítaču umožňujú USB tokeny, RFID tokeny, alebo niektoré umožňujú prenos vygenerovaného kľúča prostredníctvom bezdrôtovej technológie Bluetooth.

Obrázok 14 Bezpečnostný token bez pripojenia k počítaču [38]

Bezpečnostné tokeny fungujú na princípe neustále sa meniaceho kódu, ktorý sa zobrazuje na displeji tokenu a ktorý slúži ako autentifikačný kód na vstup do informačného systému spolu s identifikačnými údajmi držiteľa. Každý kód má časovo obmedzenú platnosť a užívateľ je informovaný aj o tom, ako dlho ešte bude daný kód platný. Po vypršaní času platnosti sa automaticky kód zmení. Tokeny sa používajú predovšetkým v aplikáciách, kde je vyžadovaná vysoká bezpečnosť. [38]

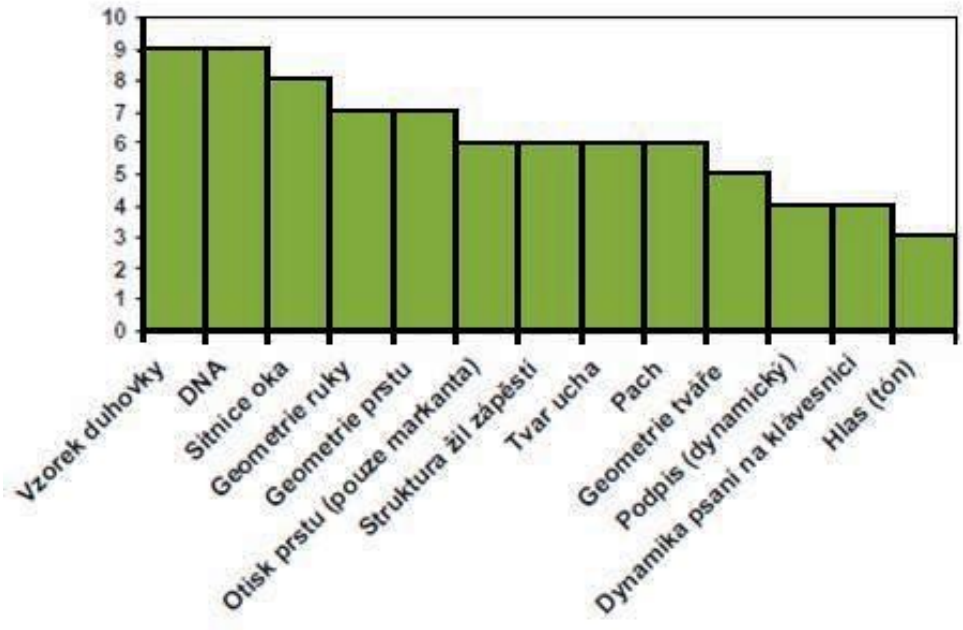
3.1.4 Biometrické metódy

Formami autentizácie sú jednoznačne aj biometrické metódy, ktorých použitie sa začína rozširovať. Na rozdiel od predošlých metód nie je potrebné mať pri sebe žiadny identifikačný prostriedok a nehrozí jeho strata alebo odcudzenie. Ľudské telo nám dáva množstvo biometrických údajov, ktoré sú preň jedinečné a je možné ho podľa nich spoľahlivo identifikovať, každého napadnú ako prvé odtlačky prstov, no je ich podstatne viac, ako napríklad geometria ruky, tváre, ucha, očná dúhovka, sietnica, hlas alebo DNA.

Vytvorenie databáze všetkých voličov a ich biometrických údajov by bolo nákladné i časovo náročné, no určite autentizácia voliča na základe biometrických údajov by bola najbezpečnejšia forma.

Tabuľka 2 Porovnanie existujúcich biometrických metód [41]

Biometrická metóda	Univerzálnosť	Unikátnosť	Stálosť	Výkonnosť	Prijateľnosť
Geometria tváre	*vysoká*	*nízka*	*stredná*	*nízky*	*vysoká*
Odtlačok prsta	*stredná*	*vysoká*	*vysoká*	*vysoký*	*stredná*
Geometria ruky	*stredná*	*stredná*	*stredná*	*stredný*	*stredná*
Klávesové údery	*nízka*	*nízka*	*nízka*	*nízky*	*stredná*
Štruktúra žíl na rukách	*stredná*	*stredná*	*stredná*	*stredný*	*stredná*
Očné dúhovky	*vysoká*	*vysoká*	*vysoká*	*vysoký*	*nízka*
Sietnica	*vysoká*	*vysoká*	*stredná*	*vysoký*	*nízka*
Podpis	*nízka*	*nízka*	*nízka*	*nízky*	*vysoká*
Hlas	*stredná*	*nízka*	*nízka*	*nízky*	*vysoká*
Termografia tváre	*vysoká*	*vysoká*	*nízka*	*stredný*	*vysoká*
Pach tela	*vysoká*	*vysoká*	*vysoká*	*nízky*	*stredná*
DNA	*vysoká*	*vysoká*	*vysoká*	*vysoký*	*nízka*
Geometria ucha	*stredná*	*stredná*	*vysoká*	*stredný*	*vysoká*



Obrázek 15 Stálosť biometrickej vlastnosti v čase [42]

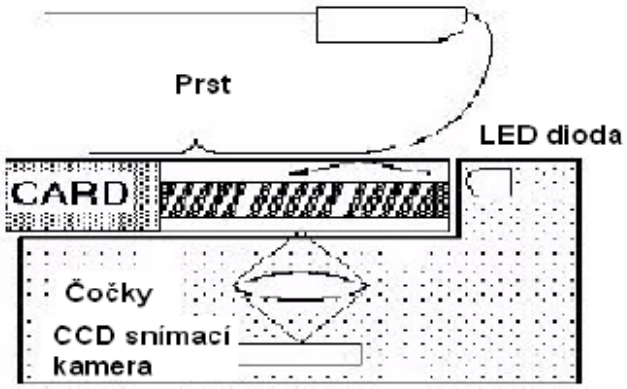
3.1.4.1 Overenie identity na základe odtlačkov prstov

Používanie odtlačku prstu (presnejšie obrazcov papilárnych línií na vonkajšej strane prstu) ako metóda pre identifikáciu sa začala používať už na konci 19. storočia, kedy Sir Francis

Galton našiel a definoval niektoré charakteristické body na prste, ktoré môžu slúžiť k identifikácii človeka.[42]

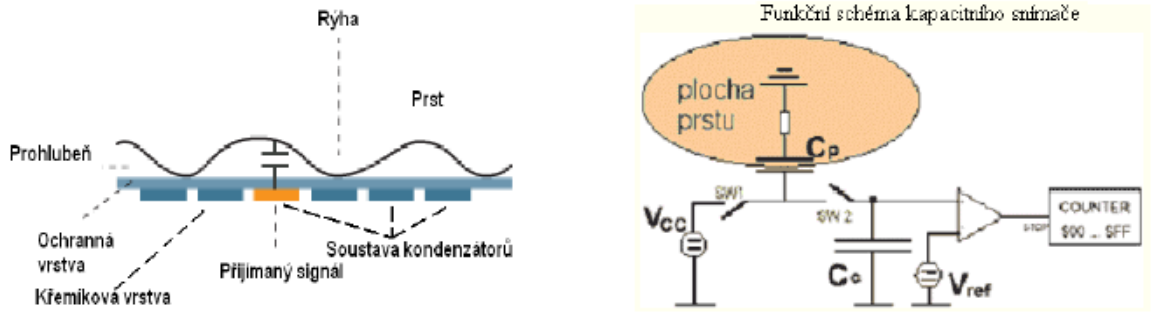
Najbežnejšími snímačmi na snímanie odtlačkov prstov sú optické, kapacitné a ultrazvukové.

Optické senzory patria medzi najstaršie technológie snímania odtlačku prsta. Hlavný princíp spočíva v pridržaní prsta nad sklenenou podsvietenou vrstvou, laserovým svetlo sa odráža od prsta a prechádza do CCD snímača, ktorý zachycuje vizuálny obraz odtlačku. Nevýhoda tohto typu je, že je pomerne náchylný k chybám. [42]



Obrázok 16 Princíp snímania reflexnými optickými prístrojmi [42]

Princíp využívaný u kapacitných snímačoch je najrozšírenejší, založený je na meraní kapacity medzi kožou prstu a aktívnymi pixlami. Veľkosť meraného elektrického pola sa mení medzi ryhami a prehĺbeninami štruktúry papilárnych línií ako príčina zmeny dielektrika medzi jednou doskou kondenzátoru (pixlom) a druhou doskou kondenzátoru (prstom). Dielektrikom je teda buď vzduchová vrstva (prehĺbenina - pixel) alebo pokožka (ryha - pixel). Citlivá snímacia plocha je tvorená desiatimi tisícmi kondenzátorov štruktúrovaných do siete. Senzory využívajúce kapacitný princíp sú najpresnejšími typmi, ich výhodou je i malý rozmer (cca 4 cm^2). [42]



Obrázok 17 Princíp snímania kapacitným snímačom odtlačkov [42]

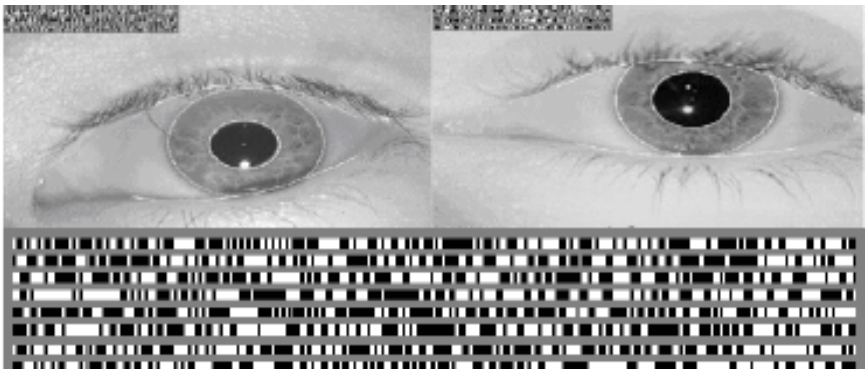
Ultrazvukové senzory na rozdiel od optických, ktoré merajú odrazené svetlo, merajú odrazenú zvukovú vlnu. Ich výhodou je, že ultrazvuk ľahko prenikne i nečistotami, ktoré by znehodnotili obraz zachytený pomocou optického snímača. [42]

3.1.4.2 Overenie identity na základe očnej dúhovky

Táto metóda sa považuje za najbezpečnejšiu. Biometrické systémy pre rozpoznávanie dúhovky sú relatívne novo vyvinuté. Prvý patent je datovaný k roku 1994 a vyvinutý americkým Úradom pre jadrovú bezpečnosť. Dúhovka je sval vo vnútri oka, ktorý reguluje veľkosť šošovky na základe intenzity svetla dopadajúceho na oko. Jej zafarbenie i štruktúra je síce geneticky závislá ale vzorkovanie nie. Dúhovka sa vyvíja behom prenatálneho rastu plodu a jej vzorkovanie je náhodné a je jedinečné pre každého človeka, dokonca i jeden človek má každú dúhovku inú. [42]

Obrázok 18 Dúhovka, jej popis a snímač biometrických dát očnej dúhovky [42]

Snímanie dúhovky si vyžaduje veľmi kvalitnú digitálnu kameru a infračervené osvetlenie oka. V priebehu snímania sa dúhovka mapuje do fázorových diagramov, ktoré obsahujú informácie o orientácii, početnosti a pozícii špecifických plôšok. Tieto informácie následne slúžia k vytvoreniu mapy dúhovky a šablóny pre identifikáciu. [42]



Obrázok 19 Lokalizovanie dúhovky a jej piktografické znázornenie [42]

3.1.4.3 Overenie identity na základe sietnice oka

Pre rozpoznávanie osoby podľa jej sietnice oka sa používa obraz ciev na pozadí ľudského oka v okolí slepej škvrny. Sietnica je svetlo-citlivý povrch na zadnej strane oka a je zložená z veľkého množstva nervových buniek. Pre získanie obrazu sa používa zdroj svetla s nízkou intenzitou žiarenia a opto-elektrický systém (dnes sa používa iba jedna infračervená LED dióda). Naskenovaný obraz je následne prevedený do podoby 40 bitového čísla. Verifikácia sietnice je veľmi presnou metódou identifikácie.[42]

3.1.4.4 Overenie identity na základe žíl na rukách

Je jednou z najnovších metód – prvé dostupné systémy sú datované k roku 2000. Táto technológia je veľmi náročná na falšovanie, pretože sieť ciev v ruke nie je voľne okom viditeľná a niektoré snímacie prístroje rozoznajú či je ruka živá (musí v nej prúdiť krv určitej teploty). Technológia spočíva v snímaní ruky špeciálnou kamerou v infračervenom svetle, tak sa získa čiernobiely obraz štruktúry žíl, ktoré tvoria zreteľný vzorec. Štruktúra žíl sa v dospelom veku príliš nemení, je výrazná a jej jedinečnosť i u jednovaječných dvojčiat preukázalo niekoľko vedeckých štúdií.[42]

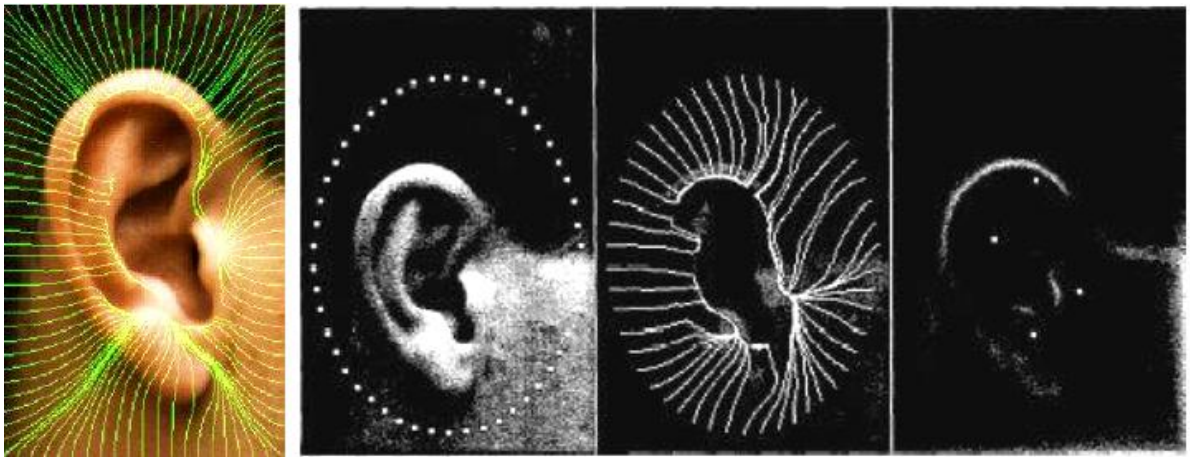
Obrázok 20 Bezdotykový snímač dlane [42]

Snímanie prebieha tak, že zdroj presvieti ruku a na základe rôznej absorpcie žiarenia krvných ciev a ostatného tkaniva sa vytvorí obraz pomocou snímacej CCD kamery. Obraz je ďalej digitalizovaný a spracovávaný pre extrahovanie siete ciev. Ukladajú sa dôležité vlastnosti – body a uhly vetvenia ciev a ich hrúbka. [42]

Obrázok 21 Extrahované žily na dlani [42]

3.1.4.5 Overenie identity na základe geometri ucha

U tejto metódy je ucho nasnímané špeciálnym optickým zariadením vo vzdialenosti cca 0,5 – 1 m. Dáta zaznamenané na snímke – morfologické vzťahy – rozmery, tvary, umiestnenie významných bodov apod. sú následne vyhodnotené v závislosti na použitom type algoritmu, porovnávané s príslušnou databázou. [42]



Obrázok 22 Biometrické meranie parametrov ucha [42]

3.1.5 Elektronický podpis

Pre autentizáciu voliča sa využíva i elektronický podpis, ktorý môže obsahovať priamo identifikačná karta spolu s ostatnými údajmi o voličovi.

Podľa zákona č.227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonov je definovaný ako údaje v elektronickej podobe, ktoré sú pripojené k dátovej správe alebo sú s ňou logicky spojené a ktoré slúžia ako metóda k jednoznačnému overeniu identity podpísanej osoby vo vzťahu k dátovej správe [24].

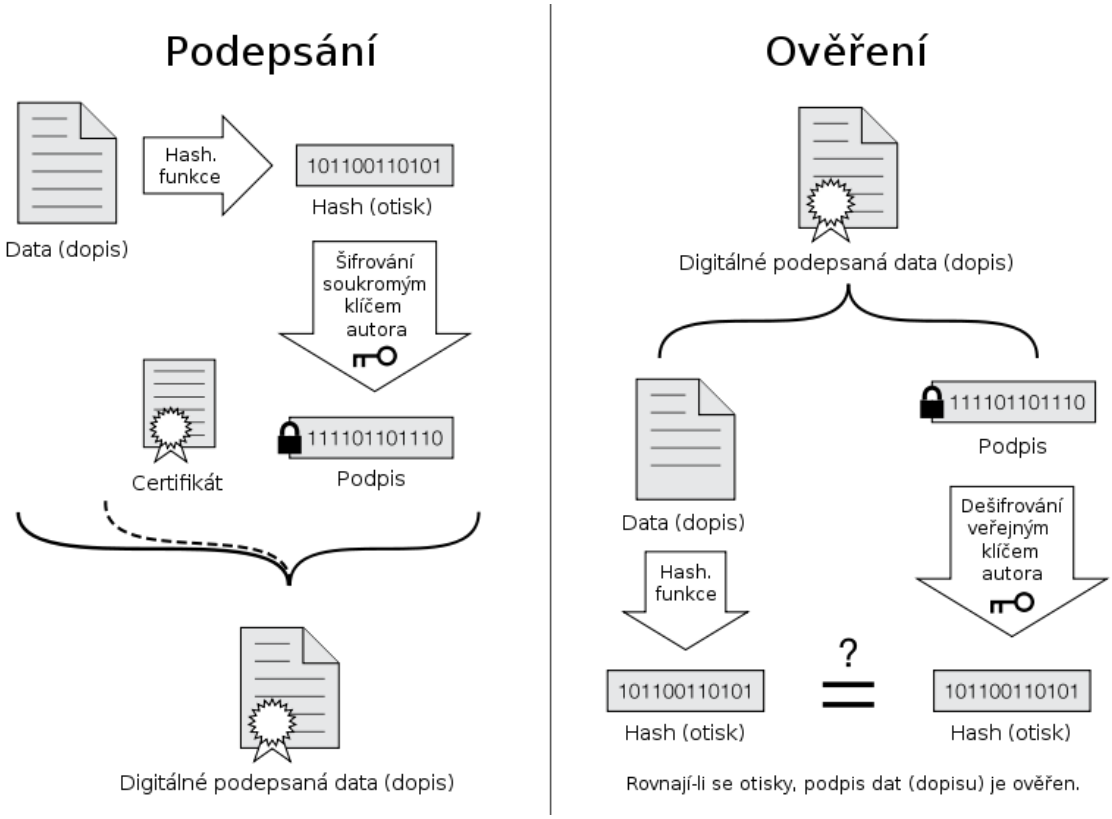
Sú dva druhy elektronického podpisu uznávaný a zaručený. Vo verejnej správe je akceptovaný len jeden a to uznávaný, ktorý je vydávaný akreditovanou certifikačnou autoritou.

Uznávaný elektronický podpis musí splňovať nasledujúce požiadavky:

1. Je jednoznačne spojený s podpisujúcou sa osobou.
2. Umožňuje identifikáciu podpisujúcej osoby vo vzťahu k dátovej správe.
3. Bol vytvorený a pripojený k dátovej správe pomocou prostriedkov, ktoré podpisujúca osoba môže udržať pod svojou výhradnou kontrolou.
4. Je k dátovej správe, ku ktorej sa vzťahuje, pripojený takým spôsobom, že je možné zistiť akúkoľvek následnú zmenu dát.[24]

Princíp pre vytvorenie elektronického podpisu je založený na asymetrickom šifrovaní, s tým rozdielom, že kľúče sa použijú naopak, pre šifrovanie súkromný kľúč a pre dešifrovanie verejný. Na jeho vytvorenie sa najčastejšie používajú asymetrické algoritmy

RSA a DSA. Dajú sa použiť samostatne alebo spolu s hashovacími funkciami MD5 (s RSA) a SHA (s DSA).



Obrázok 23 Podpísanie a overenie elektronického podpisu [23]

3.1.6 Digitálny certifikát

Digitálnym certifikátom je dátová správa, ktorá je vydaná poskytovateľom certifikačných služieb, spojuje dáta pre overovanie elektronických podpisov s podpisujúcou sa osobou a umožňuje overiť jej identitu, alebo spojuje dáta pre overovanie elektronických značiek s označujúcou osobou a umožňuje overiť jej identitu. [24] Takto definuje digitálny certifikát zákon č.227/2000 Sb. o elektronickom podpise.

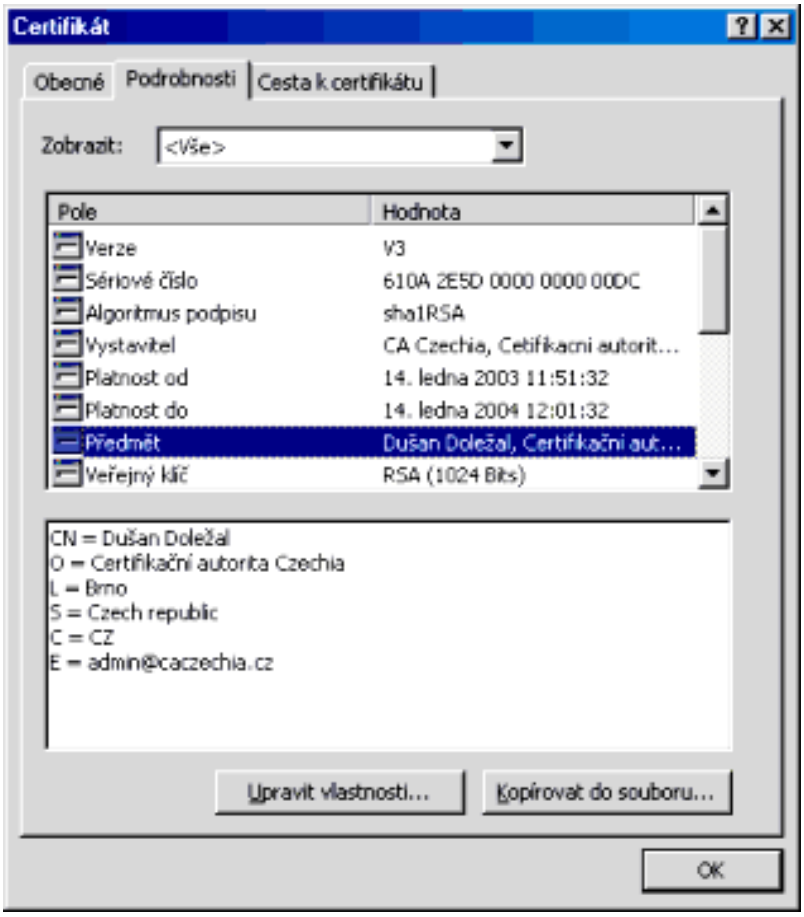
Každý certifikát musí obsahovať:

- Sériové číslo. Číslo musí byť vždy unikátne, certifikačná autorita teda nemôže vydať dva certifikáty so zhodným sériovým číslom.
- Dátum začiatku a konca platnosti certifikátu. Najbežnejšie doba platnosti certifikátu je jeden rok.

- Identifikačné údaje subjektu, ktorému je certifikát vydaný. Tieto údaje si certifikačná autorita musí spoľahlivo overiť, napríklad v prípade osobného certifikátu kontrolou dokladu totožnosti.
- Verejný kľúč. Najčastejšie sa používa dĺžka kľúča 1024 bitov. Okrem vlastného kľúča je súčasťou certifikátu tiež typ algoritmu, ktorý bude pre podpisovanie používaný.
- Identifikačné údaje subjektu, ktorý certifikát vydal, teda certifikačnej autority.[27]

Digitálny certifikát môže byť rovnako ako elektronický podpis obsiahnutý v identifikačnej karte voliča.

Obrázok 24 Všeobecné údaje o certifikáte [27]



Obrázok 25 Podrobnosti o certifikáte [27]

3.1.7 Triedy certifikátov

- Class 1 – určená pre jednotlivcov, pre e-mail.
- Class 2 – určená pre organizácie, kde je vyžadované preukázanie identity.
- Class 3 – určená pre servery a digitálne podpisy, kde je potrebné nezávislé potvrdenie identity certifikačnou autoritou.
- Class 4 – určená pre on-line obchodné transakcie medzi spoločnosťami.
- Class 5 – určená pre súkromné subjekty alebo vládnu bezpečnosť. [26]

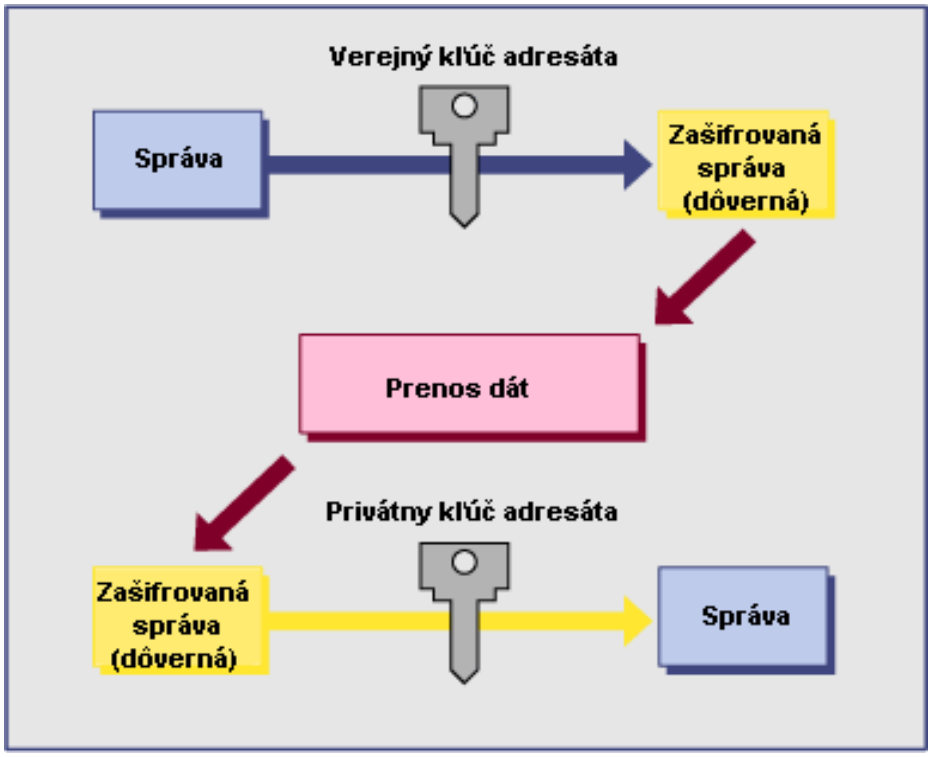
3.1.8 Certifikačná autorita

Vydávať certifikáty môže len poskytovateľ certifikátov, ktorý má požadovanú akreditáciu. Všetky povinnosti a požiadavky na akreditovaného poskytovateľa certifikátov sú taktiež definované v zákone č. 227/2000 Sb. o elektronickom podpise.

3.2 Zabezpečenie hlasovania pomocou šifrovania

3.2.1 Asymetrické šifrovanie – verejný a súkromný kľúč

Pri asymetrickom šifrovaní sa používajú dva typy kľúčov – verejný pre šifrovanie a súkromný pre dešifrovanie. Princíp je v tom, že verejný kľúč býva verejne dostupný a správa sa ním zašifruje, dešifrovať sa dá iba súkromným kľúčom, ktorý už verejne dostupný nie je a má ho iba osoba, pre ktorú sme tú správu zašifrovali a poslali jej ju.



Obrázok 26 Asymetrické šifrovanie [29]

3.2.2 Využitie asymetrického šifrovania u elektronických volieb

Verejný kľúč je pri elektronických voľbách zverejnený pre voličov a súkromný kľúč má len niekoľko oprávnených ľudí - autorít. Pri dešifrovaní je potrebná kooperácia držiteľov súkromného kľúča s pevne stanoveným minimálnym počtom autorít potrebných na dešifrovanie. Proces dešifrovania môže ktokoľvek overiť. Navyše ak máme dva zašifrované hlasy pomocou určitej operácie násobenia, nad zašifrovanými textami môžeme bez znalosti súkromného kľúča vytvoriť korektne zašifrovaný text súčtu týchto hlasov. Po použití tejto operácie zašifrovaných hlasov všetkých voličov získame jediný zašifrovaný text výsledkov volieb. Volič zašifruje hlas verejným kľúčom a pridá dôkaz o korektnosti

zašifrovanej správy, teda o tom, že obsahuje hlas len jedného z možných kandidátov. Po podpise tejto správy ju pošle registračnému serveru. Ten skontroluje oprávnenosť voliča zúčastniť sa na hlasovaní, overí podpis a korektnosť priloženého dôkazu. Ak je všetko v poriadku, registračný server zverejní voličov zašifrovaný hlas s dôkazom aj podpisom. Volič tak môže skontrolovať, či sa jeho správa nachádza na zverejnenom zozname [10], [14].

Po uplynutí času hlasovania registračný server vynásobí zverejnené zašifrované hlasy (hlasy sa sčítavajú). Tým získa a následne zverejní zašifrovaný výsledok volieb. Na ich dešifrovaní sa podieľajú autority, ktoré sú držiteľmi časti súkromného kľúča. Môžu to byť napr. politické strany, členovia volebných komisií a pod. Pri dešifrovaní je zvyčajne potrebná spolupráca aspoň polovice všetkých autorít – držiteľov podielov súkromného kľúča. Volič si môže individuálne overiť, či bol jeho hlas započítaný, nahliadnutím do zoznamov zverejnených registračným serverom. Proces vynásobenia zašifrovaných hlasov a následné dešifrovanie výsledkov volieb sú univerzálne overiteľné. Tajnosť hlasovania zabezpečuje vlastnosť šifrovacieho systému, ktorý zo zašifrovanej voľby neposkytuje žiadnu informáciu o voľbe. Držitelia častí súkromného kľúča spolupracujú len pri dešifrovaní výsledkov volieb, nie jednotlivých hlasov. Navyše dešifrovanie prebieha až po uplynutí času volieb, čím je zabezpečená vlastnosť spravodlivosti, t. j. nikto nepozná čiastočné výsledky. Korektné hlasovanie len oprávnených voličov najviac raz kontroluje registračný server [10], [14].

3.2.3 Slepý podpis

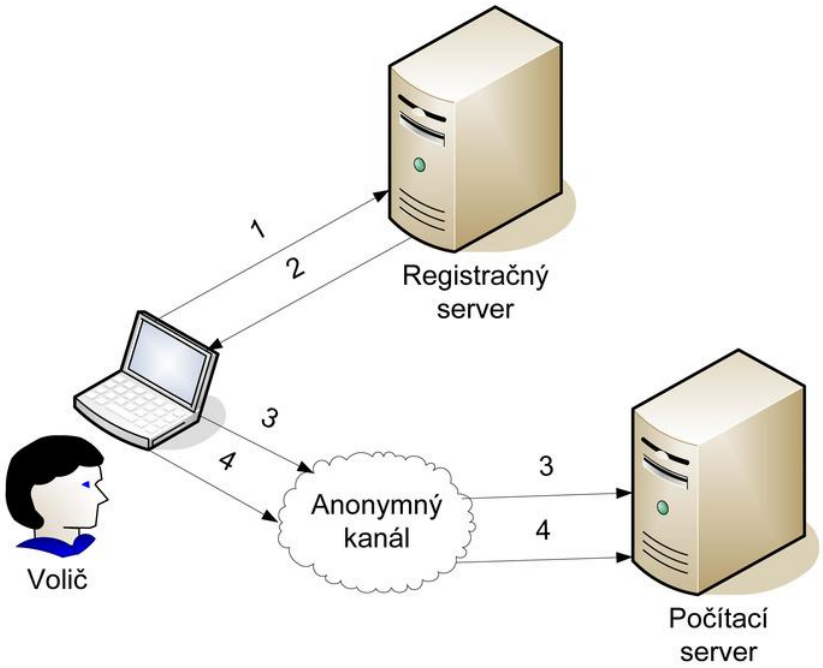
Slepý podpis ju druhom digitálneho podpisu, obsah správy je však skrytý („zaslepený“) pred jej podpísaním. Používa sa pri správach, kde je dôležitá ochrana súkromia odosielateľa.

3.2.4 Použitie slepého podpisu pri elektronickom hlasovaní

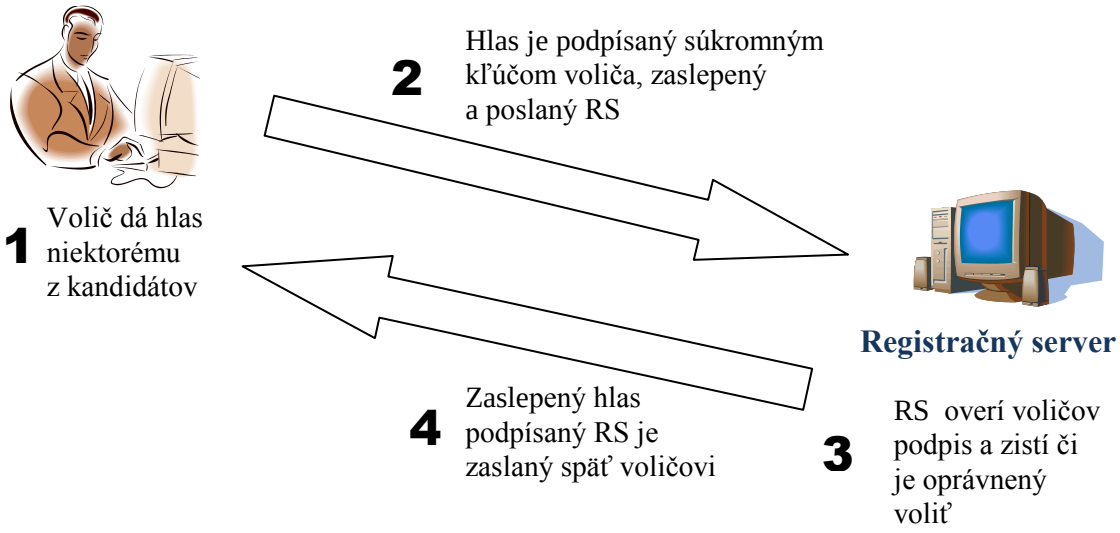
Pri elektronickom hlasovaní sa slepý podpis využíva pre zabezpečenie súkromia voliča, teda aby nebolo možné určiť spojenie medzi voličom a jeho voľbou. Volič získa verejné kľúče všetkých serverov a verejný parameter počítacieho servera, ktorý je jedinečný pre každé voľby. Súkromný parameter volieb počítacieho servera je zdieľaný niekoľkými autoritami napr. volebnou komisiou. Slepý podpis sa využije na podpísanie hlasovacej

obálky registračným serverom. Na začiatku volič pripraví „obálku“ zamknutú kľúčom, v ktorej sa nachádza hlas. Dá sa otvoriť jediným kľúčom, ktorý pozná len volič. Takisto nemožno bez znalosti kľúča získať akékoľvek informácie o jej obsahu. Obálku zaslepí, podpíše a pošle registračnému serveru v správe číslo 1. Registračný server overí voličov podpis, zistí, či je oprávnený voliť a či sa už nezúčastnil na hlasovaní. Ak je všetko v poriadku, podpíše zaslepenú obálku a pošle ju späť voličovi v správe číslo 2. Ten túto správu „odslepí“, čím získa obálku podpísanú registračným serverom. Tú pošle anonymným kanálom počítaciemu serveru pred uplynutím času na hlasovanie v správe číslo 3 [10], [14].

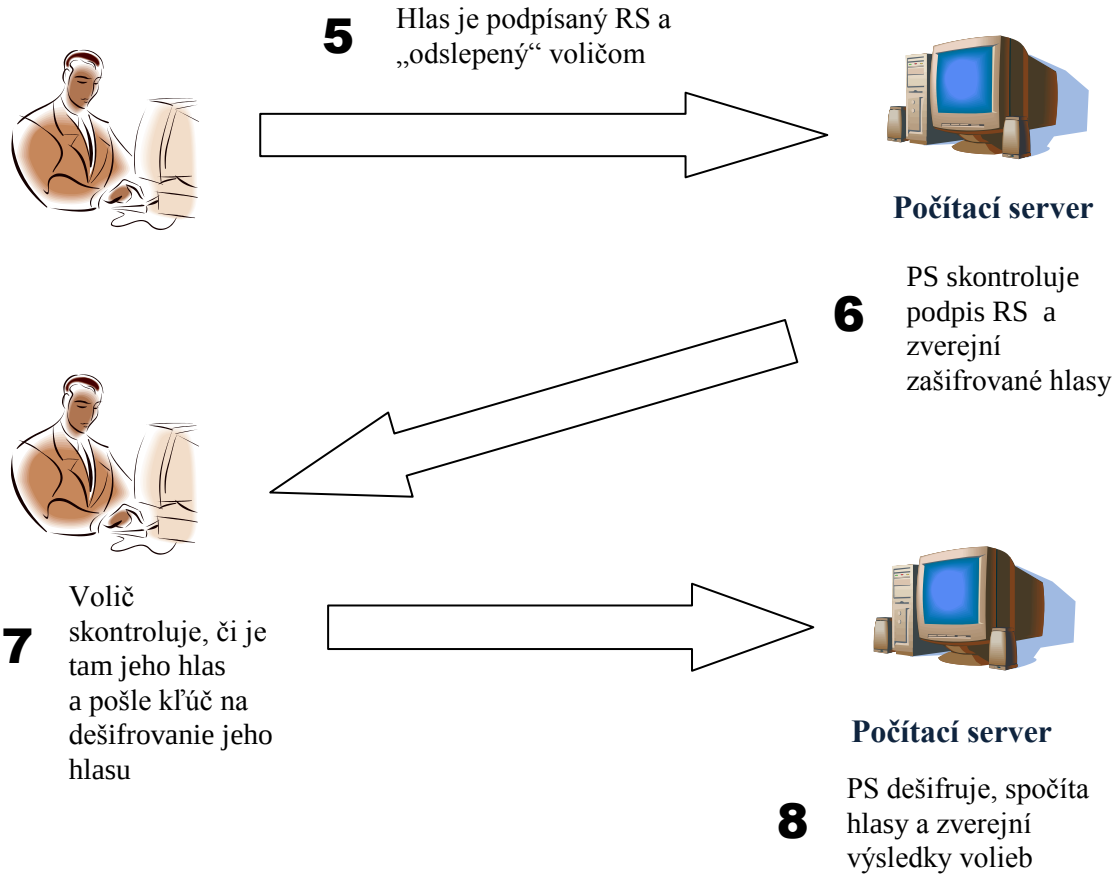
Po skončení hlasovacej fázy protokolu počítací server skontroluje podpis registračného servera na odovzdaných obálkach a zverejní korektné hlasovacie obálky. Keďže nemá kľúče potrebné na ich otvorenie, nie je schopný spočítať výsledky volieb. Volič skontroluje, či sa jeho obálka nachádza na zverejnenom zozname, a pošle pomocou anonymného kanála v správe číslo 4 kľúč na otvorenie obálky. Počítací server následne zverejní zoznam volieb, obálok a kľúčov všetkých voličov, spočíta a zverejní výsledky volieb [10], [14].



Obrázok 27 Schéma založená na slepom podpise [10]



Obrázok 28 Prvá fáza hlasovania



Obrázok 29 Druhá fáza hlasovania

3.2.5 Kryptografické algoritmy

V predchádzajúcom texte sú spomínané niektoré algoritmy, používané napríklad pre vytvorenie elektronického podpisu, na doplnenie je uvedená v nasledujúcich podkapitolách ich stručná charakteristika.

3.2.5.1 Asymetrický šifrovací algoritmus RSA

RSA je jedným z najznámejších a najpoužívanejších asymetrických šifrovacích algoritmov, ktorý je možné použiť rovnako na šifrovanie ako i na podpisovanie. Názov je vytvorený zo začiatočných písmen mien jeho autorov - Ronald Rivest, Adi Shamir a Leonard Adleman [25]. Princípom tohto algoritmu je vygenerovanie náhodného veľkého prvočísla – verejného kľúča. Tento kľúč sa následne použije aplikáciou relatívne zložitých matematických funkcií na odvodenie ďalšieho veľkého prvočísla – súkromného kľúča. Bezpečnosť tohto algoritmu je závislá na tom, že rozklad veľmi veľkých čísiel je extrémne náročný a zaberá množstvo času [30].

3.2.5.2 Algoritmus DSA

DSA - algoritmus digitálneho podpisu je štandard Americkej vlády pre digitálny podpis. Bol navrhnutý Americkým inštitútom NIST v roku 1991 pre použitie v protokole DSS (Digital Signature Standard). Poslednou úpravou prešiel v roku 2009 a teraz je vedený ako FIPS 186-3. Národný inštitút štandardov a technológie tento patent dal celosvetovo verejnosti k voľnému užívaniu bez poplatkov. Samotný algoritmus je založený na probléme výpočtu diskrétneho logaritmu [31].

3.2.5.3 Algoritmus SHA

SHA (Secure Hash Algorithm) je rozšírená hashovacia funkcia, ktorá vytvára zo vstupných dát odtlačok fixnej dĺžky. Jeho hlavnou vlastnosťou je, že malá zmena na vstupu vedie k veľkej zmene na výstupu, čo znamená vytvorenie zásadne odlišného odtlačku. Táto funkcia bola navrhnutá americkou Národnou bezpečnostnou agentúrou a je považovaná za nástupcu hash algoritmu MD5, ktorý už nie je považovaný za bezpečný. SHA je rodina piatich algoritmov: SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. Posledné štyri varianty sa súhrnne uvádzajú ako SHA-2. SHA-1 vytvorí obraz správy dlhý 160 bitov, u algoritmov SHA-2 čísla uvádzajú dĺžku odtlačku správy v bitoch. Ako každá hashovacia

funkcia aj SHA zabezpečuje hlavne kontrolu integrity dát, teda či nedošlo k ich pozmeneniu. Z toho plynie použitie napr. v digitálnych certifikátoch a následne aj elektronickom podpise [32].

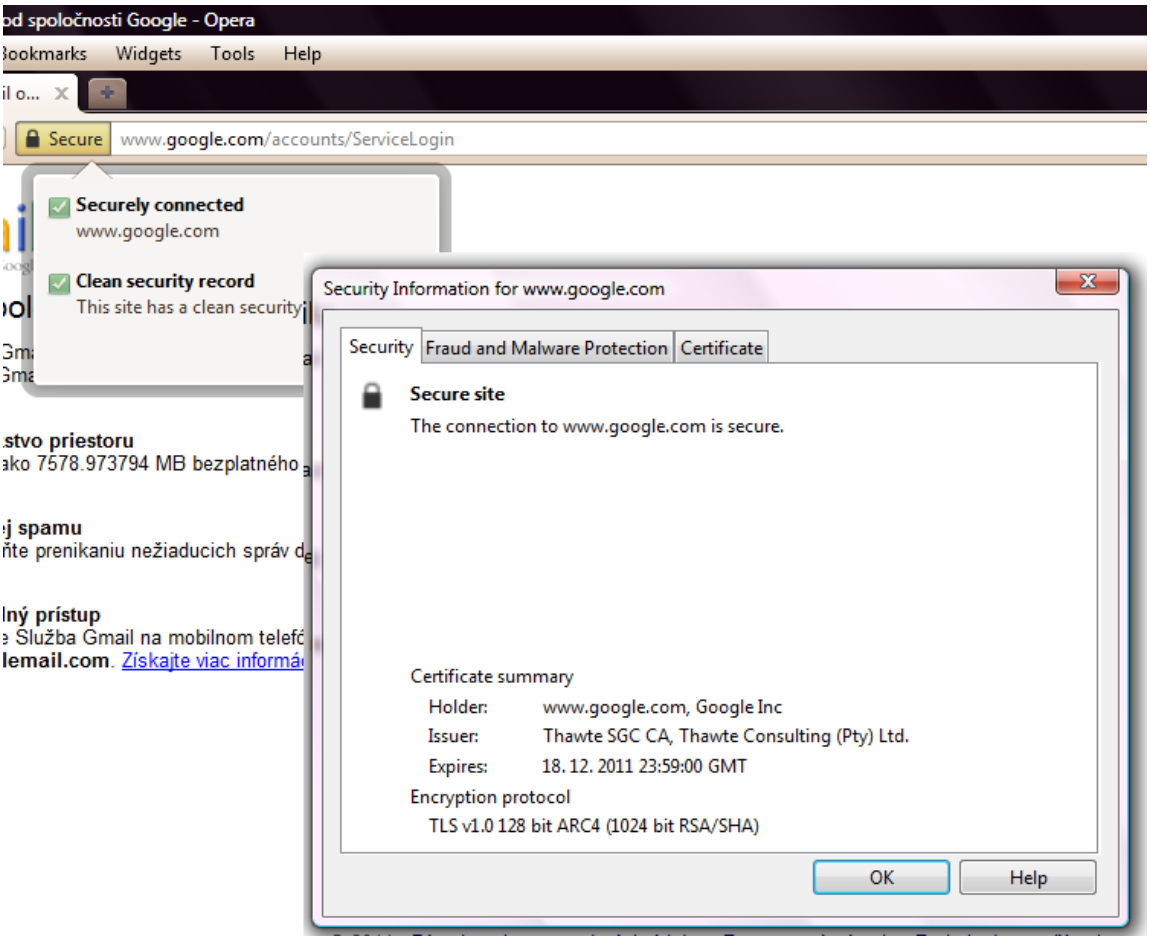
3.2.5.4 Algoritmus MD5

Algoritmus MD5 bol vyvinutý ako nástupca algoritmu MD4 za účelom odstránenia jeho nedostatkov. Algoritmus MD5 vykoná štyri priechody dátovými blokmi použitím rôznych číselných konštánt pre jednotlivé slová v správe v priebehu každého priechodu. Počet 32bitových konštánt použitých behom výpočtu algoritmu MD5 je 64, takže algoritmus MD5 nakoniec vytvorí 128bitový hash algoritmus. Už v roku 1996 boli nájdené prvé chyby v tomto algoritme, v roku 2004 však boli nájdené ďaleko väčšie chyby a od použitia MD5 v bezpečnostných aplikáciách sa upúšťa. [33], [34].

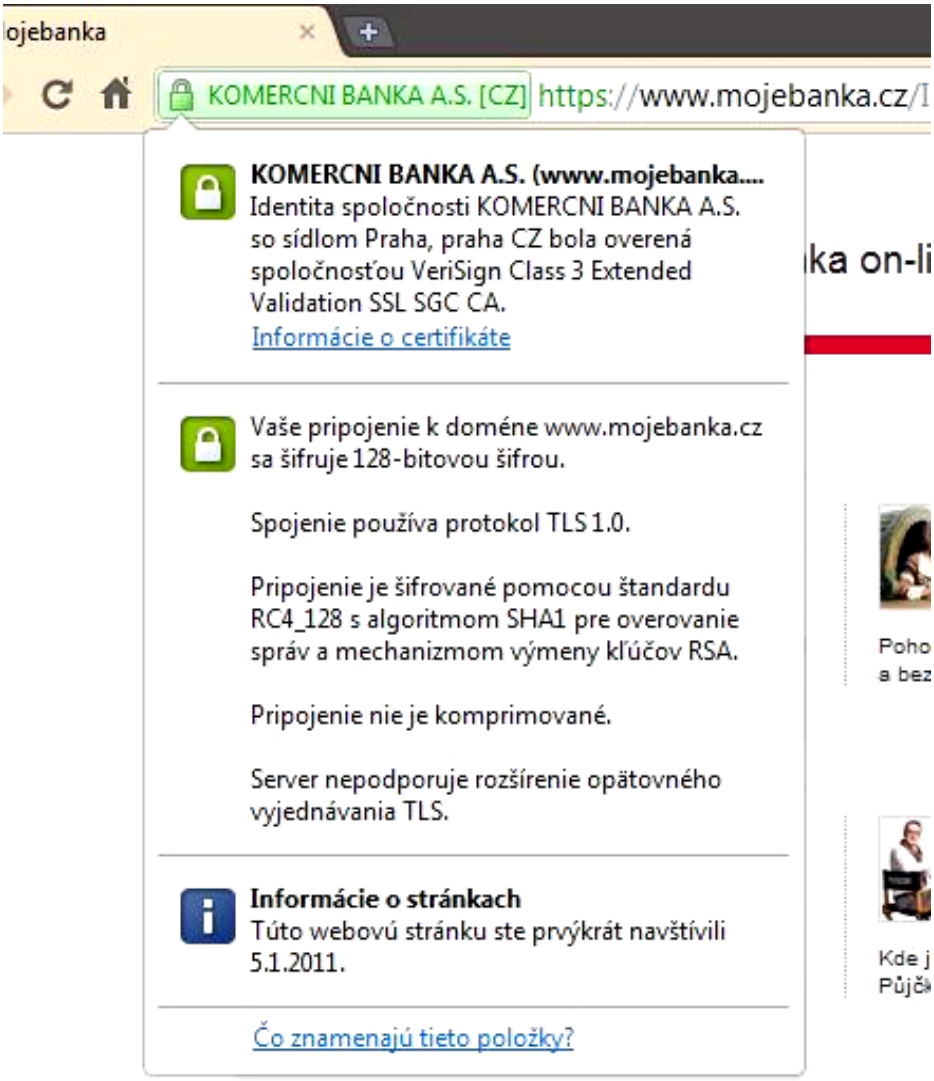
3.2.6 Protokol HTTPS

HTTPS protokol je zabezpečenejšou verziou HTTP protokolu, ktorý umožňuje zabezpečiť spojenie medzi webovým prehliadačom a webovým serverom pred odposlúchaním, podvrhnutím dát a umožňuje overenie identity protistrany. Protokol HTTPS používa protokol HTTP a prenášané dáta sú šifrované pomocou protokolu SSL alebo TLS. HTTPS využíva asymetrické šifrovanie, najčastejšie RSA [28] .

Zistiť, či je identita webovej stránky overená, môžeme veľmi jednoducho, vidíme to priamo na adresnom riadku webového prehliadača. U každého prehliadača je to zobrazenie trochu odlišné, na nasledujúcich obrázkoch je možné vidieť webový prehliadač Opera a Google Chrome. Po kliknutí na označenie zabezpečenia sa zobrazia informácie ako názov spoločnosti, informácie o certifikáte, aké sú používané protokoly a algoritmy pre šifrovanie a pod.



Obrázok 30 Adresný riadok webového prehliadača Opera



Obrázok 31 Adresný riadok webového prehliadača Google Chrome

3.3 Ochrana samotných počítačov

V neposlednom rade je dôležitá i samotná ochrana počítačov. Základom je mať kvalitný antivírový program a firewall a určite je dobré mať aj antispywarový program. Pre zvýšenie bezpečnosti sú k dispozícii systémy prevencie vniknutí a detekcie vniknutí.

3.3.1 Antivírové a antispywarové programy

Antivírové programy slúžia, ako už z ich názvu vyplýva, na ochranu počítačov proti vírom a inému škodlivému software. Medzi najznámejšie antivírové program patrí napríklad ESET NOD32 Antivirus, Norton AntiVirus, antivírový program AVG, Avast! antivirus, Symantec EndPoint Security apod. Aj u antispywarových programov už z názvu ide vyčítať

ich použitie – proti spywaru a väčšina programov chráni i pred trójskymi koňmi, adware, spamom apod.

3.3.2 Firewall

Firewall je sieťové zariadenie slúžiace k zabezpečovaniu a riadeniu k sieťovej prevádzke medzi sieťami s rôznou úrovňou dôveryhodnosti a zabezpečenia. Zjednodušene sa dá povedať, že slúži ako kontrolný bod, ktorý definuje pravidlá pre komunikáciu medzi sieťami, ktoré od seba oddeľuje. V minulosti identifikoval zdroje a ciele dát (zdrojovú a cieľovú IP adresu) a zdrojový a cieľový port, čo je dnes už pomerne nedostačujúce a moderné firewally sa opierajú prinajmenšom o informácie o stave spojenia, znalosť kontrolovaných protokolov a prípadne prvky IDS [35].

3.3.3 Pravidelné aktualizácie

Základnou prevenciou pred všetkými hrozbami je mať aktuálny operačný systém a software zabezpečujúci ochranu (antivírové, antispywarové programy...) a to je možné zabezpečiť jedine pravidelnými aktualizáciami.

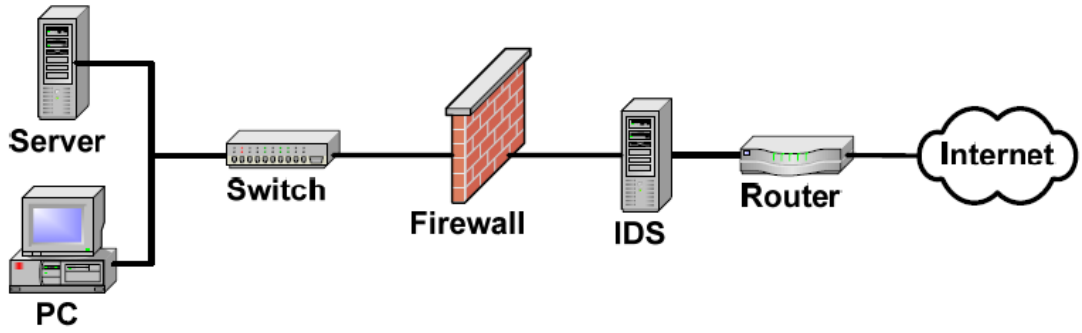
3.3.4 Systém detekcie prieniku (IDS - Intrusion Detection Systems)

Systém detekcie prieniku (Intrusion Detection System - IDS) môže byť definovaný ako súbor nástrojov, metód a zdrojov, ktoré pomáhajú odhaliť, zaznamenať alebo ohlásiť pokusy o sieťové prieniky a útoky, zaznamenáva ale i aktivity, ktoré môže ale aj nemusia byť samotným narušením. Jednoducho povedané, ide o kombináciu hardwarového a softwarového vybavenia. Vo všeobecnosti sú IDS pasívnymi systémami. Podozrivú aktivitu iba zaznamenávajú, prípadne upozornia správcu siete zaslaním poplašnej správy, sami však nerobia žiadne aktívne opatrenia, ktoré by narušeniu zabránili. Niektoré systémy však majú implementované aj aktívne opatrenia, ktoré dokážu prípadné útoky zablokovať [36].

IDS systémy sa delia do 3 kategórií:

- uzlovo orientované IDS (Host-based IDS, HIDS) – nasadzujú sa priamo na jednotlivé servery alebo užívateľské stanice

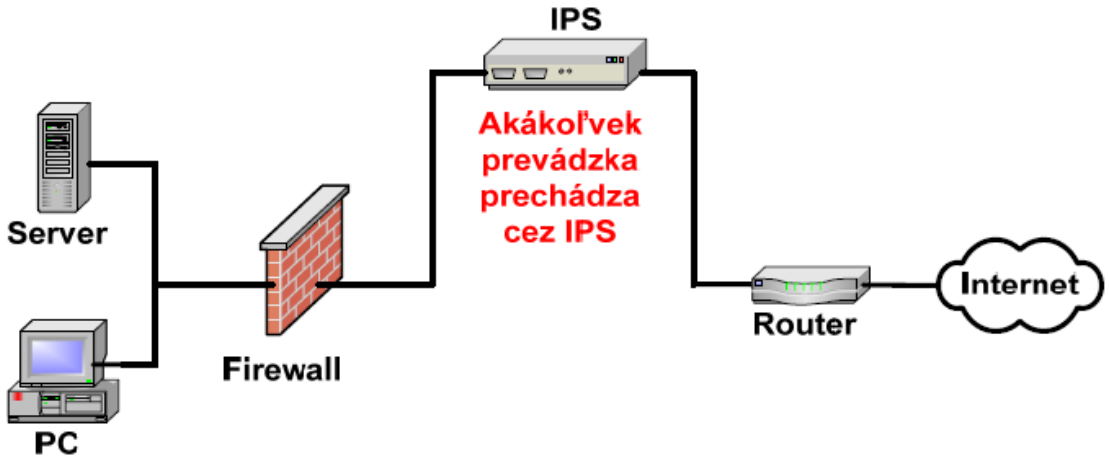
- sieťovo orientované IDS (Network-based IDS, NIDS) – monitorujú prevádzku celej siete, resp. podsiete
- hybridné IDS – kombinujú oba predchádzajúce prístupy [36]



Obrázok 32 Systém detekcie prieniku [37]

3.3.5 Systém prevencie prieniku (IPS - Intrusion Prevention Systems)

Systém prevencie prieniku (IPS - Intrusion Prevention Systems) má všetky vlastnosti predchádzajúceho systému IDS, no na rozdiel od neho dokáže detekovať a zablokovať hrozbu ešte pred jej preniknutím do systému. Dnes sa bežne používajú oba systémy súčasne.



Obrázok 33 Systém prevencie prieniku [37]

II. PRAKTICKÁ ČASŤ

4 HODNOTENIE VOLEBNÝCH SYSTÉMOV Z POHĽADU SPOĽAHLIVOSTI

4.1 Elektronické hlasovanie prostredníctvom prístroja typu DRE

O prístrojoch typu DRE – Direct recording electronic – zariadenie priameho ukladania hlasov, používaný napríklad v niekoľkých štátoch v USA, sa vyskytlo niekoľko diskusií zaoberajúcich sa ich bezpečnosťou.

4.1.1 Závery testovania hlasovacieho prístroja Diebold AccuVote-TS

1. Každý kto má fyzický prístup k hlasovacím prístrojom alebo k pamäťovým kartám, ktoré budú vkladané do prístroja môže nainštalovať škodlivý software.
2. Škodlivý software na hlasovacom zariadení pozmeňuje hlasy s veľmi nízkym rizikom odhalenia, pretože počet hlasov sa nezmení a tak nehrozí, že by pracovníci vo volebnej miestnosti zistili nezrovnalosti v počte hlasov.
3. Hlasovacie prístroje sú náchylné k vírusom a môžu rozširovať škodlivý software automaticky a neviditeľne z prístroja do prístroja pred, počas aj po voľbách. Pri demonštrácii bol vytvorený vírus, ktorý je schopný sa šíriť týmto spôsobom a infiltroval sa do každého prístroja.
4. Riziko predstavuje i odcudzenie, strata alebo poškodenie pamäťovej karty.

Vzhľadom k tomu, že tento test bol vykonávaný v roku 2006, software v novších verziách prístrojov, by mal byť odolnejší voči škodlivému softwaru. Čo je jedna z podmienok aby boli hlasovacie prístroje bezpečné, pretože bezpečnosť ide dosiahnuť ak budú starostlivo navrhované s najväčšou pozornosťou kladenou na bezpečnosť, dôkladne vykonávané testovanie a audity týchto prístrojov nezávislými stranami.

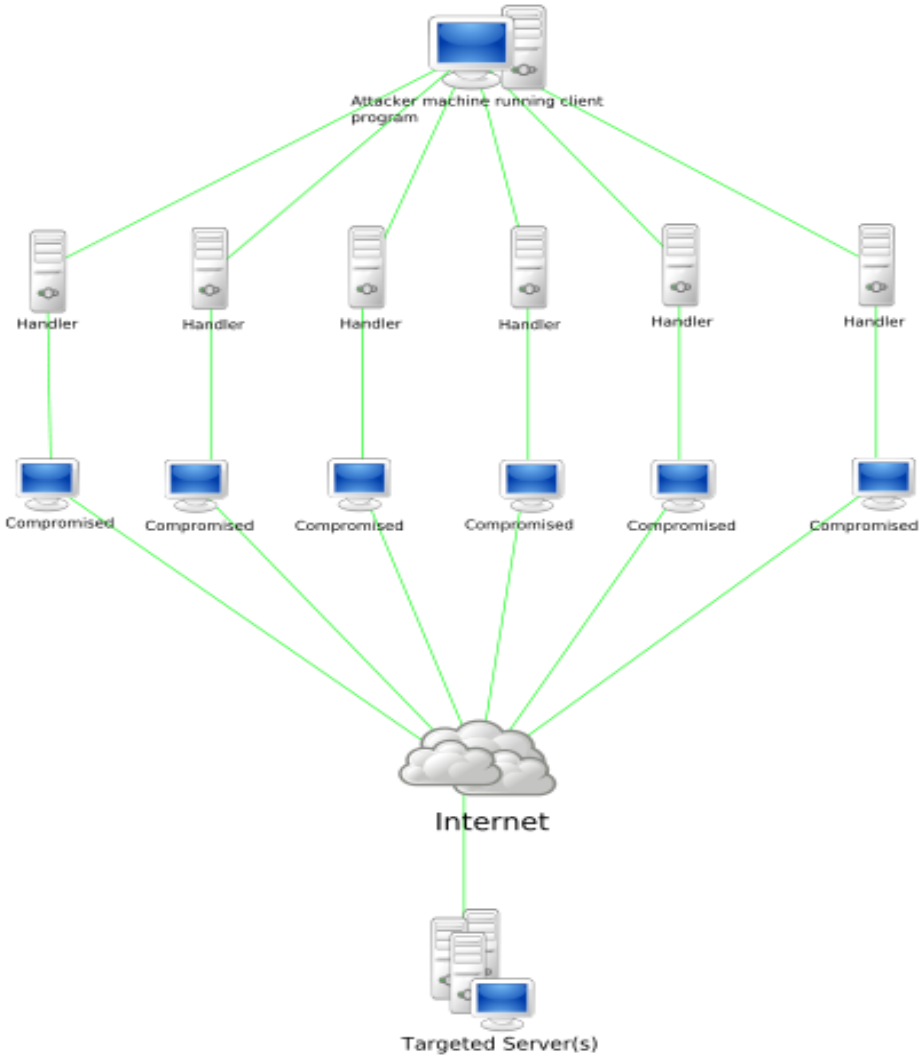
4.2 Elektronické hlasovanie prostredníctvom internetu

Hlasovanie vo voľbách prostredníctvom internetu je pravdepodobne najbezpečnejšou formou elektronického hlasovania. Samozrejme nič nie je úplne bezpečné ale ak zabezpečené elektronické hlasovanie rovnako bezpečne ako internetové bankovníctvo, tak je dostatočne spoľahlivé a ľudia mu môžu dôverovať.

4.2.1 Najväčšie hrozby pre internetové hlasovanie

Software pre dosiahnutie bezpečnosti v prostredí internetu sa neustále vyvíja, zlepšuje a zdokonaľuje, no nanešťastie to rovnako platí i o škodlivom software, ktorí takisto robí pokroky.

Jednou z najväčších internetových hrozieb je DDoS útok s ktorým sme sa už v rámci napadnutia volebného systému mali možnosť stretnúť. Čo to vlastne je? DDoS - Distributed Denial of Service (distribuované odmietnutie služby) je technika útoku na internetové stránky alebo služby, pri ktorých dochádza k zahltenie požiadavkami a pádu alebo minimálne nefunkčnosti a nedostupnosti pre ostatných užívateľov. Cieľom tohto útoku je vynútenie opakovaného resetu cieľového počítača alebo narušenie komunikácie medzi serverom a obeťou tak, aby ich komunikácia bola nemožná alebo aspoň veľmi pomalá. [46]



Obrázok 34 Schéma DDoS útoku [46]

Útoky typu DDoS nie sú zďaleka jediným nebezpečenstvom. Jedným z ďalších je phising, podvodná technika používaná na Internete k získaniu citlivých údajov ako sú napríklad heslá. Jej princípom je rozosielanie e-mailových správ, ktoré môžu vyzerať ako oficiálny e-mail a žiada o zadanie údajov na odkazujúcu stránku, ktorá napodobňuje prihlasovacie okno, obeť tam zadá prihlasovacie meno a heslo a tým tieto údaje prezradí útočníkom. [47] Pri e-voľbách by mohol útočník poslať e-mail s odkazom na falošný server, ktorý bude vyzerať ako volebný a volič tak prezradí svoje prihlasovacie údaje.

Malware, čo je všeobecné označenie škodlivého softwaru sa takisto šíri Internetom a dostáva sa do počítača, ktorý nie je dobre zabezpečený. Patria sem napríklad vírusy, červy, trójske kone, adware a spyware.

Počítačový vírus je program, ktorý dokáže rozmnožovať sám seba pridávaním svojho kódu do iných programov. Pre svoje rozširovanie teda podobne ako biologický vírus potrebuje hostiteľa – iný program. Z toho vyplýva, že do počítača sa môže dostať jedine tak, že spustíme nainfikovaný program. Spolu so spustením nainfikovaného programu sa aktivuje vírus v operačnej pamäti, a potom napadne i ďalšie súbory v počítači. Internetové červy sú tou časťou vírusu, ktorá je zodpovedná za jeho šírenie. [48]

Spyware zisťujú informácie o počítači a jeho používateľovi a bez súhlasu odosielajú cudzej osobe. Informácie môžu byť najrôznejšieho druhu, ako napríklad zoznam emailových adries, zoznam najčastejšie navštevovaných stránok, apod. Najnebezpečnejším druhom spywaru sú tzv. keyloggery, ktoré zaznamenávajú všetky stlačené klávesy. Prostredníctvom takýchto programov sa dajú získať prístupové heslá do počítačového systému, čísla kreditných kariet, registračné kľúče k programom a ďalšie informácie. [48]

Adware je software, ktorý zobrazuje reklamu. Takéto programy sú najčastejšie súčasťou iného programu, ktorý nie je škodlivý. Nebezpečenstvo týchto programov je v tom, že integrované reklamné systémy sú často spywarom. [48]

Trójsky kôň je škodlivý kód pribalený k zdanlivo neškodnému softwaru, môžu mať najrôznejšie účinky (môžu i priamo ohroziť počítač). Najzákernejším druhom trójskych koňov sú však droppery. Tieto v pravidelných intervaloch do systému vypúšťajú najrôznejší malware. Môžu obsahovať klasické vírusy, červy ale i spyware. Odhalenie trójskeho koňa sťažuje i technika nazývaná rootkits. Touto technikou trójsky kôň dokáže poprieť svoju existenciu v systéme. Túto techniku môže trójsky kôň najľahšie využiť v

prípade, že ho otvoríme s oprávneniami správcu systému. Ďalšou nebezpečnou akciou, ktorú môžu trójske kone vykonávať, je otvorenie tzv. zadných vrátok (backdoor). Cez tieto „zadné vrátka“ sa vie útočník dostať do systému bez toho, aby poznal prístupové meno a heslo. [48]

Všetok tento škodlivý software nemusí priamo ohroziť elektronický volebný systém, no môže spôsobiť nemalé problémy a komplikácie a tým spochybniť dôveryhodnosť výsledkov volieb.

5 SYSTÉM PRE HODNOTENIE ELEKTRONICKÝCH VOLIEB

Bezpečnosť elektronických volieb nezaručí len použitie jednej z metód, ktoré sú opísané v 4. kapitole, ale je potrebná ich vzájomná kombinácia. Samozrejme, že čím viac bezpečnostných prvkov je v danom elektronickom volebnom systéme použitých, tak ich spoľahlivosť narastá. Je však pochopiteľné, že nie každé zabezpečenie má rovnakú váhu na celkovú bezpečnosť, preto dva volebné systémy s rovnakým počtom použitých metód pre zabezpečenie nemusia byť rovnako spoľahlivé.

Najprehľadnejšou a najjednoduchšou formou ako zistiť spoľahlivosť každého elektronického volebného systému je vytvoriť prehľad všetkých dostupných metód a priradiť k ním akú veľkú váhu v bezpečnosti volebného systému predstavujú. Nie je však jednoduché vytvoriť systém pre hodnotenie bezpečnosti elektronických volieb, ktorý by bol plne univerzálny a bolo možné ho použiť na akékoľvek elektronické voľby, pretože existuje rada rôznych zabezpečení. Ďalším problémom je neustály vývoj v oblasti informačných technológii, o niekoľko rokov sa state systém nedostačujúci a budú v ňom absentovať dôležité prvky, tomu však ide zabrániť pravidelnou aktualizáciou a dopĺňaním.

Nasledujúca tabuľka č.3 predstavuje systém pre hodnotenie elektronických volieb, je zameraná najmä na hlasovanie prostredníctvom internetu. Obsahuje prehľad najbežnejších metód a foriem, ktorými je možné volebný systém zabezpečiť.

Tabuľku č.3 je možné rozdeliť do dvoch častí – na identifikáciu voliča a zabezpečenie hlasovania. Identifikácia voliča je rozdelená podľa toho akou formou sa volič prihlasuje - identifikácia čipovou kartou, bezpečnostným tokenom, biometrickou metódou alebo ostatnými formami zabezpečenia. Pri identifikácii čipovou kartou a bezpečnostným tokenom sú uvedené jednotlivé prvky, ktoré môžu obsahovať a u každého je bodové ohodnotenie ktoré sa sčítava ak sú v nich tie prvky obsiahnuté. Rovnako je to u biometrickej metódy, kde sú uvedené najbežnejšie formy a ohodnotené na základe ich spoľahlivosti a unikátnosti. Ostatné formy zabezpečenia sú prvky, ktoré sa môžu použiť aj samostatne bez identifikačného predmetu, volič ich môže získať napríklad poštou do vlastných rúk, alebo ich roznášajú osoby poverené v jednotlivých volebných obvodoch.

Pri použití niektorého z identifikačných predmetov, sú k dispozícii ďalšie body. V druhej časti je zabezpečenie hlasovania šifrovaním, kde je napríklad asymetrické šifrovanie

a softwarové zabezpečenie, kde sa nachádzajú najbežnejšie zabezpečenia ako napríklad antivírový program alebo firewall.

Tabuľka 3 Hodnotenie jednotlivých bezpečnostných prvkov v elektronických voľbách

Identifikácia čipovou kartou	S údajmi o voličovi		S elektronickým podpisom		S digitálnym certifikátom		S biometrickým údajom				Helso alebo PIN kód			
	2		5		5		Na základe príslušného biometrického údaju				4			
Identifikácia bezpečnostným tokenom	Len s generovaním hesla		S elektronickým podpisom		S digitálnym certifikátom		S biometrickým údajom							
	4		5		5		Na základe príslušného biometrického údaju							
Identifikácia biometrickou metódou	Odtlačok prsta	Očná dúhovka	Sietnica oka	Geometria ruky	Geometria ucha	Geometria tváre	Štruktúra žíl na rukách	Termografia tváre	Hlas	Klávesové údery	Pach tela	Podpis		
	6	6	6	5	5	3	4	6	3	2	3	2		
Jednotlivé formy zabezpečenia	PIN kód		Silné heslo		Elektronický podpis		Digitálny certifikát		Rodné číslo		Iný bezpečnostný kód		Iné osobné údaje voliča	
	4		4		5		5		3		4		2	

	Overenie poslaním SMS kódu na zaregistrované mobilné číslo						
	4						
Použitie predmetu pri identifikácii	Čipová karta	Bezpečnostný token	Osobná identifikačná karta				
	4	4	3				
Iné opatrenia pre identifikáciu voliča	Zmena identifikačných kódov/hesiel/PIN kódov apod. pred každými voľbami						
	3						
Zabezpečenie hlasovania šifrovaním	Asymetrické šifrovanie	Slepý podpis	Iné bezpečné šifrovanie	Protokol HTTPS	Volič vlastní šifrovací kľúč		
	5	5	5	5	5		
Softwarové zabezpečenie hlasovania	Antivírový program	Firewall	Antispywarový program	Systém prevencie prieniku	Systém detekcie prieniku		
	4	4	4	4	4		

Spolu tabuľkou č.3 je už jednoduché spočítať „bodový zisk“ každého volebného systému, ktorý sa priradí v nasledujúcich tabuľkách ku správnemu bodovému rozsahu.

Pre správny výpočet slúžia nasledujúce vzorce, prvý je pre výpočet celkového zabezpečenia a pozostáva zo zabezpečenia identifikácie voliča, ktorá sa vypočíta pomocou druhého vzorca, zo zabezpečenia hlasovania, ktoré sa vypočíta pomocou tretieho vzorca a administratívnych opatrení, ktoré sa pri zabezpečení môžu vyskytnúť.

$$Z = 2\sum Z_i + 3\sum Z_h + \sum a$$

$$Z_i = \sum k + t + b + f + p$$

$$Z_h = \sum f + p + h + s$$

Z – Celkové zabezpečenie
Z_i – Zabezpečenie identifikácie voliča
Z_h – Zabezpečenie hlasovania
a – Administratívne opatrenia
k – Identifikácia čipovou kartou
t – Identifikácia bezpečnostným tokenom
b – Identifikácia biometrickou metódou
f – Jednotlivé formy zabezpečenia
p – Použitie predmetu pri identifikácii
h – Zabezpečenie hlasovania šifrovaním
s – Softwarové zabezpečenie hlasovania

K dispozícii sú tri vyhodnotenia, prvé (tabuľka č.4) je pre vyhodnotenie celého elektronického volebného systému spolu so softwarovým zabezpečením, druhé (tabuľka č.5) je len pre zistenie stupňa zabezpečenia identifikácie voliča a tretie (tabuľka č.6) je vyhodnotenie volebného systému (identifikácia voliča + zabezpečenie hlasovania) ak nemáme k dispozícii všetky informácie o softwarovom zabezpečení.

Vyhodnotenie podľa tabuľky č.4 môžeme použiť, ak máme k dispozícii všetky informácie o volebnom systéme, ktorý ideme hodnotiť, čiže i vrátane softwarových zabezpečení, ktoré pri bežnom popise elektronického volebného systému k dispozícii nie je.

Tabuľka 4 Stupeň zabezpečenia volebného systému

Stupeň zabezpečenia	Počet bodov
Spoľahlivé zabezpečenie	100 a viac
Dobré zabezpečenie	85 – 99
Priemerné zabezpečenie	60 – 84
Nízke zabezpečenie	40 – 59
Nedostatočné zabezpečenie	menej ako 39

V nasledujúcej tabuľke č.5 je k dispozície pre zistenie stavu zabezpečenie identifikácie voliča. Nie je tam brané do úvahy žiadne iné zabezpečenie.

Tabuľka 5 Stupeň zabezpečenia identifikácie voliča

Stupeň zabezpečenia	Počet bodov
Spoľahlivé zabezpečenie identifikácie	20 a viac
Dobré zabezpečenie identifikácie	15 – 19
Priemerné zabezpečenie identifikácie	9 – 14
Nízke zabezpečenie identifikácie	5 – 8
Nedostatočné zabezpečenie identifikácie	menej ako 4

Tabuľka č.6 sa bude využívať pre výpočet zabezpečenia elektronických volebných systémov asi najčastejšie. Berie do úvahy všetky zabezpečenia hlasovanie a identifikácie voliča okrem softwarových.

Tabuľka 6 Stupeň zabezpečenia na základe identifikácie voliča a použitej bezpečnostnej schémy

Stupeň zabezpečenia	Počet bodov
Spoľahlivé zabezpečenie	70 a viac
Dobré zabezpečenie	50 – 69
Priemerné zabezpečenie	30 – 49
Nízke zabezpečenie	20 – 29
Nedostatočné zabezpečenie	menej ako 19

Na základe predchádzajúcich tabuliek je vidieť, že so zvyšujúcim počtom použitých bezpečnostných prvkov sa zvyšuje bezpečnosť i samotného volebného systému. Neznamená to však, že by najideálnejší elektronický volebný systém bol taký, že by obsahoval všetky možné dostupné zabezpečenia.

5.1 Hodnotenie vybraných volebných systémov

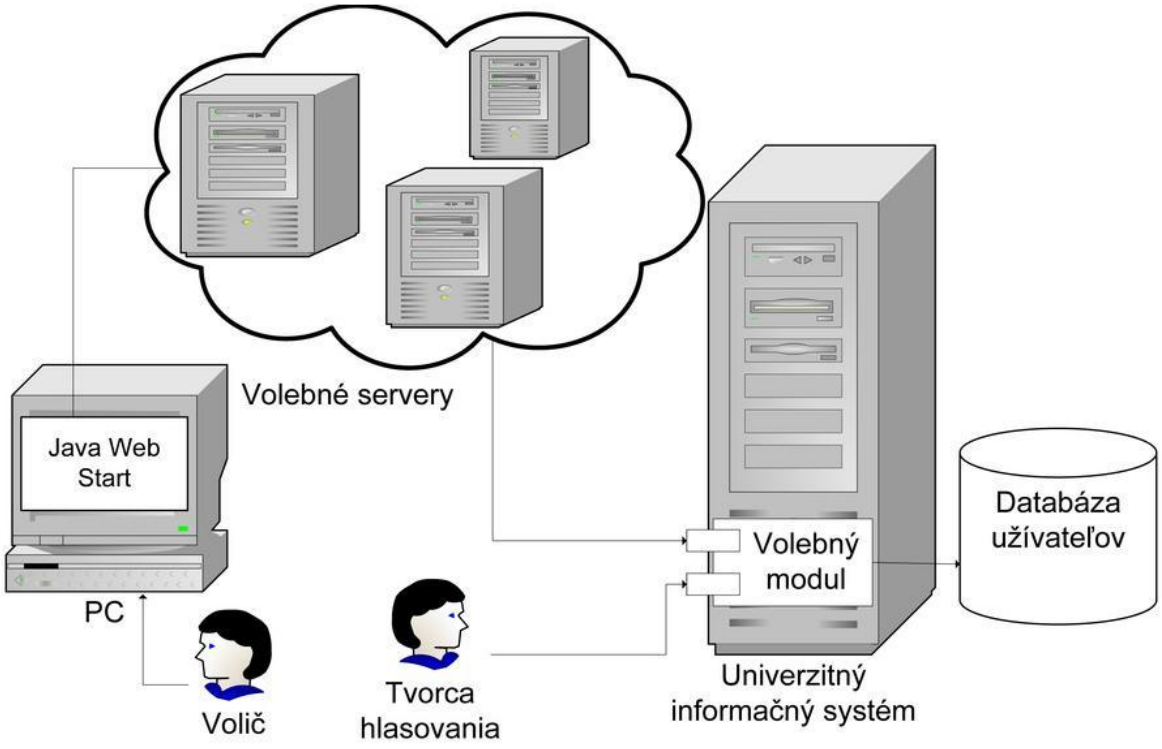
Nasleduje vyhodnotenie vybraných volebných systémov pomocou vytvoreného systému pre hodnotenie. Pre hodnotenie bol vybraný elektronický volebný systém v Estónsku, Švajčiarsku a akademický volebný systém.

5.1.1 Akademický volebný systém

Tento volebný systém bol navrhnutý RNDr. Mariánom Novotným ako koncepcia pre akademický volebný systém, ktorý môže poskytnúť volebné služby pre rôzne univerzitné aplikácie, ako napr. univerzitný informačný systém, portál virtuálnej kolaborácie, videokonferenčný systém atď. Cieľom bolo navrhnúť univerzálny hlasovací systém, ktorý bude podporovať rôzne typy volieb, napr. hlasovania komisií, voľby do akademických orgánov, anonymné ankety o predmetoch, anonymné dotazníky a hlasovanie pri videokonferenciách. Tieto volebné aplikácie tak nebude nevyhnutné programovať zvlášť pre jednotlivé informačné systémy.[10]

5.1.1.1 Popis volebného systému

Tvorca hlasovania pomocou informačného systému vytvorí hlasovanie s povinnými parametrami, ako sú typ voľby, začiatok a koniec, zoznam kandidátov (otázok), zoznam oprávnených voličov a pod. Voličovi sa po spustení klientskej aplikácie Java Web Start a prihlásení do systému pomocou svojho súkromného kľúča zobrazia všetky hlasovania, v ktorých je oprávnený sa zúčastniť. Po výbere hlasovania a svojej voľby odvolí. Po skončení volieb bude oboznámený s výsledkami a pomocou klienta si môže overiť, či bol jeho hlas započítaný.[10]

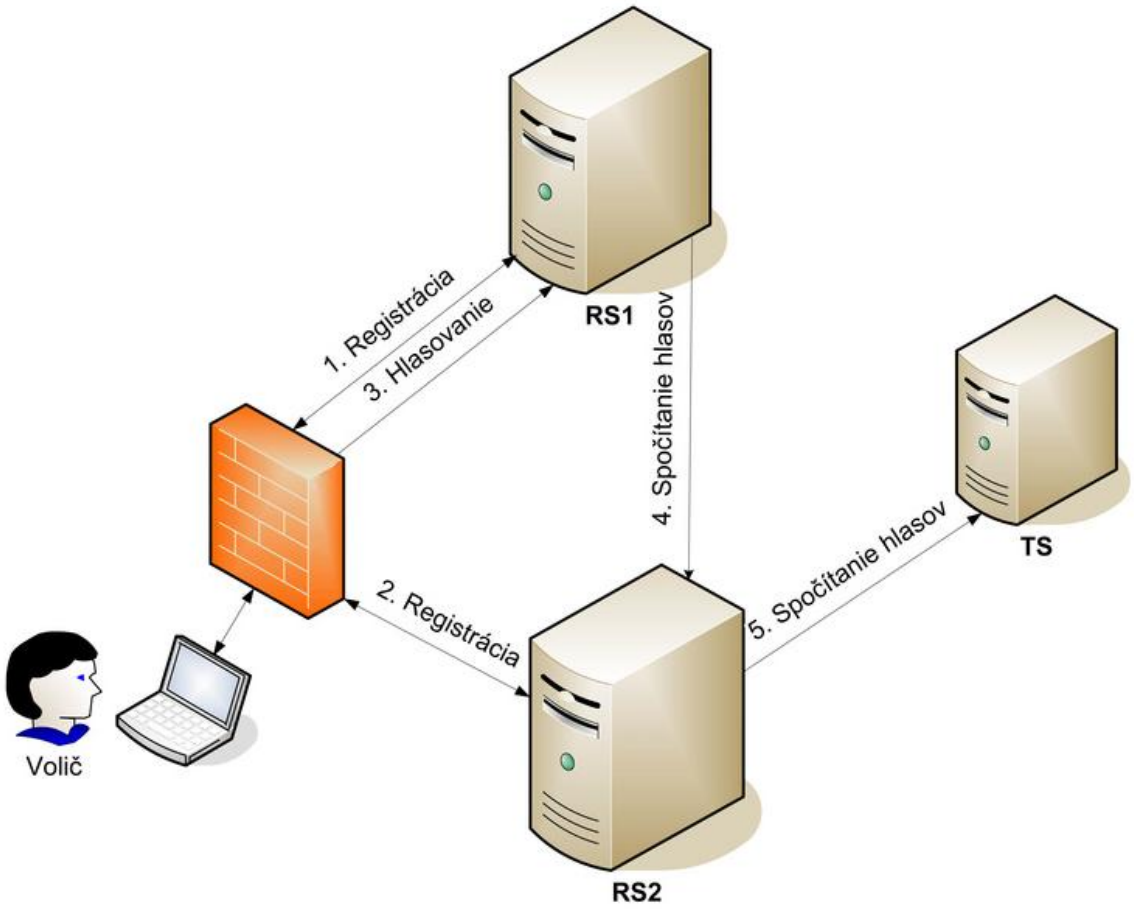


Obrázok 35 Architektúra Akademického volebného systému [10]

Na realizáciu akademického volebného systému bol navrhnutý kryptografický protokol, v ktorom funguje infraštruktúra verejných kľúčov – PKI, kde každý potenciálny volič vlastní súkromný kľúč a certifikát na podpisovanie. Certifikát zabezpečuje zviazanie voliča s jeho verejným kľúčom a poskytuje aj mechanizmy na overenie jeho platnosti. Protokol vyžaduje tri servery – dva registračné a jeden sčítací. Vychádza zo základnej schémy založenej na slepom podpise. Registračné servery majú zoznamy oprávnených voličov. Sú zdvojené pre ich vzájomnú kontrolu, keďže server môže posielať falošné hlasy namiesto registrovaných voličov, ktorí sa vo volebnej fáze nezúčastnia. Rovnako slúžia ako jednoduchá mixnetová sieť na zabezpečenie anonymného kanála, ktorý tento protokol nevyžaduje. Navyše v rozšírenej verzii schéma poskytuje aj bezdokladovosť hlasovania. [10]

Volič si prostredníctvom klientskej aplikácie stiahne zoznam kandidátov a zvolí svoju voľbu. Pri registrácii na registračnom serveri RS1 získa obálku svojej voľby podpísanú serverom RS1. Túto obálku postupne zašifruje verejnými kľúčmi všetkých serverov. Podpis odtlačku (hashu) tejto správy serverom RS2 získa volič pri registrácii na tomto serveri. Bude slúžiť ako oprávnenie na poslanie zašifrovanej obálky vo volebnej fáze. Po uplynutí času na hlasovanie server RS1 dešifruje jednotlivé hlasy. Tie potom

lexikograficky usporiada a pošle serveru RS2 , ktorý ich takisto dešifruje, preusporiada a postúpi TS serveru. Ten po dešifrovaní skontroluje podpisy servera RS1 na obálkach a zverejní zoznam obálok a hlasov.[10]



Obrázok 36 Komunikácia v bezpečnostnom protokole pre Akademický volebný systém [10]

V navrhnutej schéme sa môžu na hlasovaní zúčastniť len oprávnení voliči, ktorí sú na príslušnom zozname, a to najviac raz. Zabezpečuje to elektronický podpis voliča, ktorým sa registruje na registračných serveroch. Tie povoľujú registráciu len osobám z príslušného zoznamu iba raz. Tajnosť hlasovania zabezpečuje slepý podpis počas registrácie. Vo volebnej a sčítacej fáze by mohol útočník odpočúvaním siete zistiť komunikačné spojenie medzi voľbou a počítačom, z ktorého sa hlasovalo. Tomuto bráni mixovanie hlasov všetkými servermi v sčítacej fáze. Za predpokladu, že aspoň jeden server nie je pod kontrolou útočníka, nemožno získať komunikačné spojenie medzi voľbou a voličom. Protokol v základnej schéme podporuje individuálnu overiteľnosť a v rozšírenej bezdokladovej verzii univerzálnu. Volič šifruje svoju hlasovaciu obálku verejnými kľúčmi

všetkých serverov. K obálke voliča, ktorý už odvolil, sa môže útočník pre poznanie čiastočných výsledkov dostať len pomocou spolupráce všetkých troch serverov. Protokol takisto podporuje zdieľanie kľúča na dešifrovanie obálok viacerými autoritami, ako napr. členmi volebnej komisii. Volič by v rozšírenej verzii nemal vlastniť doklad, ktorým by vedel preukázať svoju voľbu niekomu inému. Volič spolu s obálkou posiela popierateľným šifrovaním kľúč na otvorenie obálky. Pre každého kandidáta môže vypočítať iný kľúč na otvorenie obálky a tým tvrdiť, že volil daného kandidáta. Takýmto spôsobom môže oklamať útočníka. [10]

Volebný systém bol otestovaný v projekte Moderné európske voľby. Procesy v pozadí systému e-volieb sú z technickej stránky mimoriadne komplexné. Pre voliča však odovzdávanie hlasu vyzerá ako jednoduchý úkon. Študentom počas simulácie stačilo iba vložiť do čítacieho zariadenia svoj čipový voličský preukaz a zadať PIN, ktorým je preukaz chránený. Potom si z počítačovej aplikácie vybrali stranu, ktorej chceli dať svoj hlas, a jednoduchým kliknutím svoju voľbu odoslali. Na túto simuláciu zabezpečila fungujúcu infraštruktúru PKI spoločnosť Disig, a. s., ktorá vystavila certifikáty pre volebné servery a pre každého voliča vygenerovala certifikát s príslušným súkromným kľúčom. Ten bol uložený na čipovej karte. Na registračných serveroch sa nachádzali zoznamy čísel občianskych preukazov oprávnených voličov pre túto akciu. Zároveň pre každého voliča vygenerovala spoločnosť v spolupráci s dobrovoľníkmi Mládežníckeho parlamentu Prešova certifikát s príslušným súkromným kľúčom, ktorý bol uložený na čipovej karte. [10]

5.1.1.2 Hodnotenie volebného systému

I keď nejde v podstate o volebný systém, ktorý by sa využíval na komunálnej resp. na celoštátnej úrovni ale je určený pre akademické účely, je vypracovaný na veľmi dobrej úrovni. Pre zabezpečenie spoľahlivosti je vytvorený protokol s infraštruktúrou verejných kľúčov, s tým že voliči vlastnia súkromné kľúče a certifikát. Komunikácia medzi voličom a servermi je zabezpečená šifrovaním na základe slepého podpisu. Aby sa volieb nemohli zúčastniť neoprávnený voliči, registračné servery obsahujú zoznamy oprávnených voličov a pre ich vzájomnú kontrolu sú zdvojené. Tajnosť hlasovania je zabezpečená už spomínaným slepým podpisom v registračnej fáze. Bezpečnosť hlasu je zaistená proti

odpočúvaniu mixovaním hlasov všetkými servermi v sčítacej fáze a tak by musel mať útočník pod kontrolou celý server aby získal spojenie medzi voličom a jeho voľbou.

Tento volebný systém má jednoduchú registráciu i obsluhu. Voliči sa identifikujú čipovou kartou a PIN kódom svoj hlas odošlú kliknutím na kandidáta a následne na políčko „odoslať“. Náročnosť tejto voľby môžeme prirovnať napríklad k výberu hotovosti v bankomate.

5.1.1.3 Vyhodnotenie zabezpečenia na základe vytvoreného systému pre hodnotenie elektronických volieb

Zabezpečenie volebného systému vyhodnotíme na základe vytvoreného systému pre hodnotenie elektronických volieb na základe jednotlivých zabezpečení a bezpečnostných opatrení, ktoré sú vo volebnom systéme použité.

Tabuľka 7 Zoznam použitých zabezpečení

	Počet bodov	
Čipová karta	3	Identifikácia voliča
PIN kód	4	
Elektronický podpis	5	
Súkromný kľúč	5	Hlasovanie
Digitálny certifikát	5	
Schéma založená na slepom podpise	5	

V predchádzajúcej tabuľke č.7 je zoznam použitých prvkov vo volebnom systéme. Ktoré následne dosadíme do vzorcov z kapitoly 5. Ako prvé vypočítame zabezpečenie identifikácie voliča.

$$Z_i = \sum k + t + b + f + p = 3 + 4 + 5 = 12$$

Už túto hodnotu môžeme dosadiť do tabuľky č.5, pre zistenie zabezpečenia identifikácie voliča, 12 bodov je priemerné zabezpečenie. Následne vypočítame zabezpečenie hlasovania.

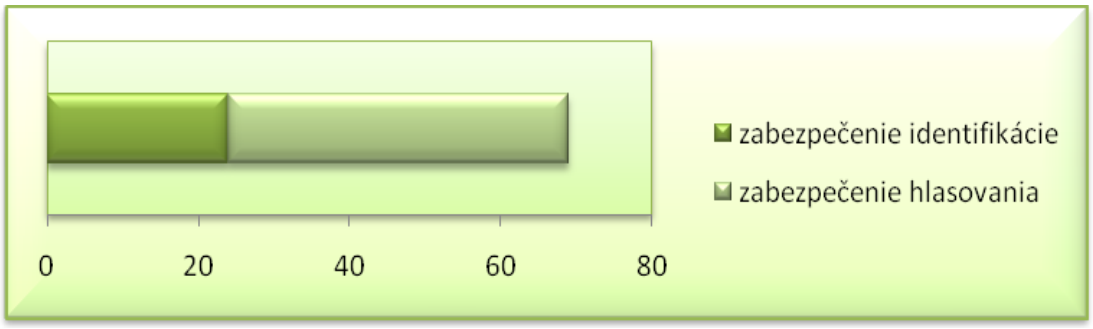
$$Z_h = \sum f + p + h + s = 5 + 5 + 5 = 15$$

Potom vypočítané hodnoty dosadíme do posledného vzorca pomocou ktorého sa vypočíta celkové zabezpečenie.

$$Z = 2\sum Z_i + 3\sum Z_h + \sum a = 2.12 + 3.15 = 69$$

Celkové zabezpečenie získalo 69 bodov, ktoré dosadíme podľa tabuľky č.6, pretože nemáme k dispozícii softwarové zabezpečenie, do správneho bodového rozhrania a vyšlo dobré zabezpečenie.

Na obrázku č.37 je graf na ktorom je znázornený pomer medzi zabezpečením identifikácie voliča a hlasovania.



Obrázok 37 Graf pomeru zabezpečenia identifikácie a hlasovania

5.1.2 Švajčiarsky volebný systém

Elektronické hlasovanie prebieha v niekoľkých švajčiarskych kantónoch. Pre účel hodnotenia použijeme ženevský. Pilotný projekt v Ženeve začali pripravovať už v roku 2000.

Kantón Ženeva mal veľmi dobrý základ pre zavedenie elektronických volieb vďaka distančnému spôsobu hlasovania – poštou. Kantón má už dlhodobo centrálny elektronický voličský zoznam. Približne 90 % voličov zvyklo vo voľbách hlasovať poštou, tak nemali problém odkloniť sa od tradičného spôsobu hlasovania a elektronické hlasovanie zrejme nepovažovali za veľkú zmenu.[16]

5.1.2.1 Popis volebného systému

Voliči dostanú tri týždne pred voľbami oficiálne dokumenty potrebné na hlasovanie, medzi ktorými je aj osobná hlasovacia karta. Každá karta má osobitné číslo, ktoré volič uvádza pri tradičnom hlasovaní alebo sa karta posiela s lístkom pri hlasovaní poštou. Pre účely

elektronického hlasovania sa na karte nachádza osobný identifikačný kód. Karta teda umožňuje hlasovať elektronicky prostredníctvom internetu alebo poštou v určenú dobu alebo osobne v deň volieb.[16]

Volič najskôr hlasuje, až potom nasleduje formálna identifikácia, ktorá legalizuje poslaný hlas. Až v tejto poslednej fáze dochádza ku komunikácii so serverom, ktorá je zašifrovaná vyplnením, online formulára, kde volič uvedie osobné číslo z karty, osobný identifikačný kód, ktorý sa nachádza na hlasovacej karte po zoškrabaní príslušného okna (týmto sa karta znehodnotí a nemôže byť použitá na hlasovanie osobne alebo poštou) a dátum narodenia. Ihneď po identifikácii sa voličovi potvrdí, že jeho hlas bol prijatý (bez zverejnenia obsahu hlasu). Takéto potvrdenie si voliči môžu nechať zaslať aj cez e-mail. Server by mal zvládnuť spracovať do 2000 hlasov za hodinu. Elektronický hlas je po odovzdaní zašifrovaný a odoslaný do elektronickej volebnej schránky do ktorej nemá nikto prístup a do niektorého zo serverov. Na otvorenie volebnej schránky sú potrebné dva kľúče, ktoré dostanú náhodne vybraní zástupcovia politických strán vo volebnej komisii. Totožnosť voliča a obsah hlasovacieho lístka sú oddelené a uschovávané v dvoch rôznych súboroch, nedá sa teda zistiť, kto ako hlasoval. Správcovia systému vykonali niekoľko hackerských útokov, na základe ktorých sa systém ukázal ako bezpečný.[16]

5.1.2.2 Hodnotenie volebného systému

U švajčiarskeho volebného systému, kde sa hlasuje prostredníctvom internetu, nie je potrebná inštalácia žiadnych ďalších programov. Pre identifikáciu pri elektronických voľbách jednoducho pridali na hlasovaciu kartu osobné identifikačné číslo, ktoré sa mení pred každým hlasovaním, čím ušetrili nemalé výdavky napríklad za čipové karty. Pre zvýšenie bezpečnosti sa hlasovacia karta obnovuje pred každými voľbami.

Pre úspešnú registráciu musí volič zadať číslo karty, ak by sa ho niekto pokúsil uhádnuť, má šancu jednu k miliarde. Ak je volič uznaný ako oprávnený je vytvorené spojenie so zabezpečeným serverom. Po vykonaní voľby systém predloží voličovi rekapituláciu jeho voľby, aby ju mohol skontrolovať a následne potvrdiť alebo zmeniť a potvrdiť svoju identitu zadaním dátumu narodenia a osobný identifikačný kód, ktorý je pod zotriteľnou vrstvou. Niektoré funkcie ako napríklad Print Screen sú počas hlasovania nefunkčné, aby sa nedala voľba zdokumentovať. Voľba ani nijako neostáva v počítači automaticky uložená.

Hlasovanie je šifrované náhodným miešaním alfanumerických znakov, komunikácia prebieha cez protokol HTTPS a volič môže overiť identitu a certifikáty pravosti druhej strany. Pre zachovanie tajnosti hlasovania sú identita voliča a jeho hlasovací lístok uložené v dvoch rôznych súboroch.

5.1.2.3 Vyhodnotenie zabezpečenia na základe vytvoreného systému pre hodnotenie elektronických volieb

Vyhodnotenie zabezpečenia volebného systému získame na základe vytvoreného systému pre hodnotenie elektronických volieb na základe jednotlivých zabezpečení a bezpečnostných opatrení, ktoré sú vo volebnom systéme použité, rovnako ako u predchádzajúceho akademického volebného systému.

Tabuľka 8 Zoznam použitých zabezpečení

	Počet bodov	
Zmena osobného identifikačného čísla pred každými voľbami	3	Identifikácia voliča
Osobná hlasovacia karta	3	
Osobitné číslo na karte	4	
Osobný identifikačný kód	4	
Dátum narodenia	2	
Šifrovanie volebného hlasu	5	Hlasovanie
Protokol HTTPS	5	

V predchádzajúcej tabuľke č.8 je zoznam použitých prvkov vo volebnom systéme. Ktoré následne dosadíme do vzorcov z kapitoly 5. Ako prvé vypočítame zabezpečenie identifikácie voliča.

$$Z_i = \sum k + t + b + f + p = 3 + 3 + 4 + 4 + 2 = 16$$

Už túto hodnotu môžeme dosadiť do tabuľky č.5, pre zistenie zabezpečenia identifikácie voliča, 16 bodov je dobré zabezpečenie. Následne vypočítame zabezpečenie hlasovania.

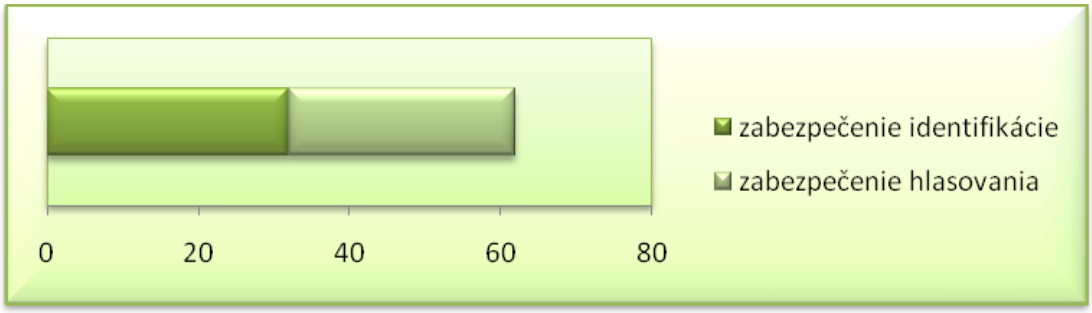
$$Z_h = \sum f + p + h + s = 5 + 5 = 10$$

Potom vypočítané hodnoty dosadíme do posledného vzorca pomocou ktorého sa vypočíta celkové zabezpečenie.

$$Z = 2\sum Z_i + 3\sum Z_h + \sum a = 2.16 + 3.10 = 62$$

Celkové zabezpečenie získalo 62 bodov, ktoré dosadíme podľa tabuľky č.6, pretože nemáme k dispozícii softwarové zabezpečenie, do správneho bodového rozhrania a vyšlo dobré zabezpečenie.

Na obrázku č.38 je graf na ktorom je znázornený pomer medzi zabezpečením identifikácie voliča a hlasovania.



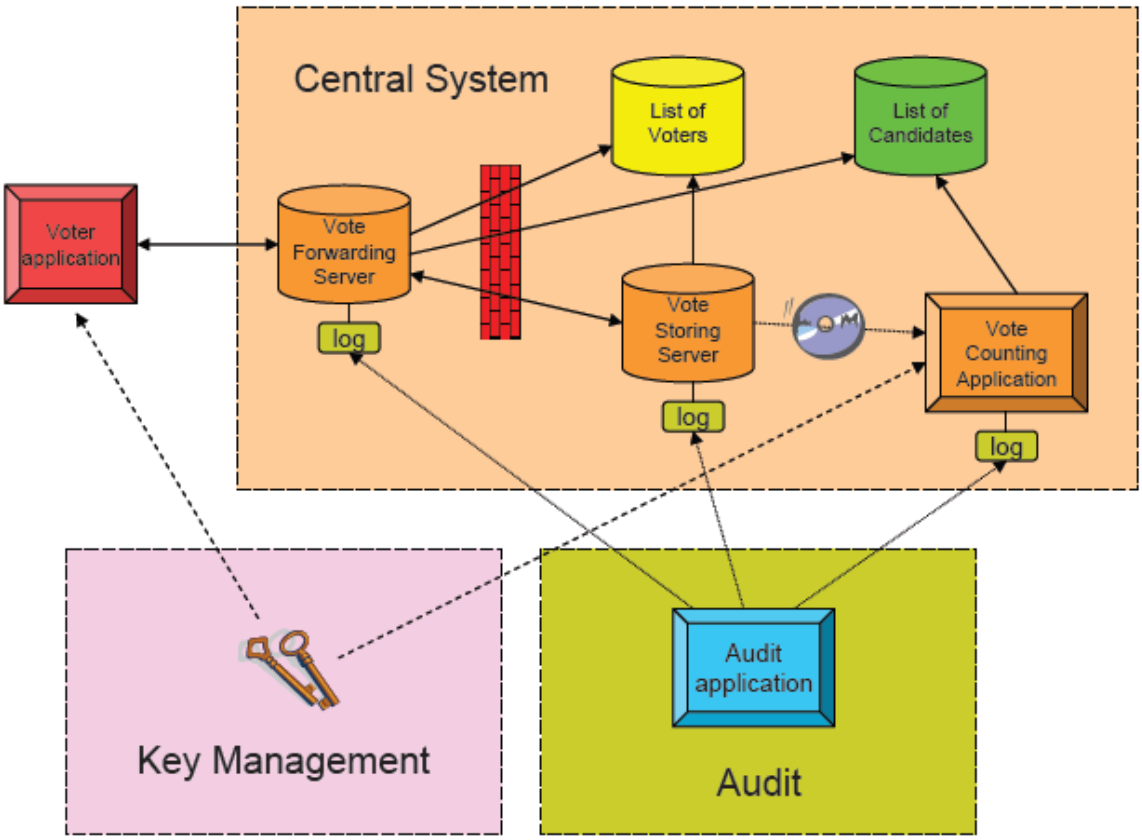
Obrázok 38 Graf pomeru zabezpečenia identifikácie a hlasovania

5.1.3 Estónsky volebný systém

V Estónsku prebehlo testovanie internetového volebného systému už v roku 2002, v roku 2005 prebehlo v rámci komunálnych volieb a tento rok v marci hlasovalo prostredníctvom internetu 25% voličov.

5.1.3.1 Popis volebného systému

Princíp volebného systému bol už načrtnutý v druhej kapitole. Volič sa prostredníctvom ID karty a PIN1 kódu identifikuje na stránke http://www.valimised.ee/. Server na základe registru obyvateľstva overí, či volič je oprávnený voliť a ak áno zobrazí kandidátku pre príslušný volebný obvod. Volič vykoná svoju voľbu, ktorá je následne zašifrovaná, toto šifrovanie predstavuje tzv. vnútornú obálku. Systém si následne vyžaduje potvrdenie voľby elektronickým podpisom ku ktorému je potrebné zadať PIN2 kód. Tento podpis predstavuje tzv. vonkajšiu obálku. V poslednom kroku systém voličovi potvrdí, že jeho hlas bol zaznamenaný. [15]



Obrázok 39 Architektúra estónskeho volebného systému [49]

Okrem rady pokročilých bezpečnostných prvkov obsahujú ID karty strojovo čitateľný kód a mikročip, ktorý obsahuje údaje vytlačené na karte okrem fotografie a podpisu. Na čipe sú tiež uložené dva digitálne certifikáty a súvisiace privátne kľúče chránené PIN kódmi. Jeden z certifikátov slúži k autentizácii, druhý k elektronickému podpisu. Používanie certifikátov nie je obmedzené, čo znamená, že môžu slúžiť i ku komunikácii s osobami, organizáciami i štátom. [15]

Autentizačný certifikát obsahuje i e-mailovú adresu užívateľa vo formáte meno.priezvisko-_NNNN@eesti.ee, kde NNNN sú štyri čísla zaručujúce jedinečnosť adresy pre osoby s rovnakými menami. Adresa sa nemení so zmenou certifikátu ani ID karty a mala by občanovi slúžiť celý život. S touto adresou nie je spojená žiadna e-mailová služba, každý si túto adresu musí presmerovať na svoj existujúci e-mailový účet, pričom je možné pre presmerovanie až 5 adries. Tento e-mail slúži predovšetkým ku komunikácii medzi štátom a občanom, ale používanie nie je obmedzené. So spojením s certifikátom je možné e-maily elektronicky podpísať alebo šifrovať. Predpokladá sa, že v budúcnosti bude možné na základe dohôd medzi rôznymi subjektmi napr. bankami alebo poisťovňami a štátom ID kartu integrovať s platobnými kartami ale i ďalšími kartami založenými na podobnom

princípe. V hlavnom meste Tallinne je už možné používať ID karty ako elektronické cestovné lístky na mestskú hromadnú dopravu. [15]

5.1.3.2 Hodnotenie volebného systému

Možnosť volieb cez internet vychádza v Estónsku z predpokladu, že tento spôsob volieb ponúka rovnakú mieru bezpečnosti a dôveryhodnosti ako tradičný systém. Nové ID karty pritom umožňujú bezpečnú autentizáciu voliča a bezpečné odovzdanie hlasu s pomocou elektronického podpisu. Podľa oficiálnych vyjadrení estónskych predstaviteľov bola otázka zabezpečenia kľúčovou požiadavkou na volebný systém.

Je veľmi praktické, že použitie ID karty je viacúčelové. Každý môže využiť certifikát na bezpečnú komunikáciu s kýmkoľvek.

5.1.3.3 Vyhodnotenie zabezpečenia na základe vytvoreného systému pre hodnotenie elektronických volieb

Vyhodnotenie zabezpečenia estónskeho volebného systému získame rovnako ako u predchádzajúcich dvoch volebných systémov na základe vytvoreného systému pre hodnotenie elektronických volieb na základe jednotlivých zabezpečení a bezpečnostných opatrení, ktoré sú vo volebnom systéme použité.

Tabuľka 9 Zoznam použitých zabezpečení

	Počet bodov	
ID karta	3	Identifikácia voliča
Údaje o voličovi	2	
1. PIN kód	5	
1. digitálny certifikát	5	
2. PIN kód	5	Hlasovanie
2. digitálny certifikát	5	
Elektronický podpis	5	
Asymetrické šifrovanie	5	

V predchádzajúcej tabuľke č.9 je zoznam použitých prvkov vo volebnom systéme. Ktoré následne dosadíme do vzorcov z kapitoly 5. Ako prvé vypočítame zabezpečenie identifikácie voliča.

$$Z_i = \sum k + t + b + f + p = 3 + 2 + 5 + 5 = 15$$

Už túto hodnotu môžeme dosadiť do tabuľky č.5, pre zistenie zabezpečenia identifikácie voliča, 15 bodov je dobré zabezpečenie. Následne vypočítame zabezpečenie hlasovania.

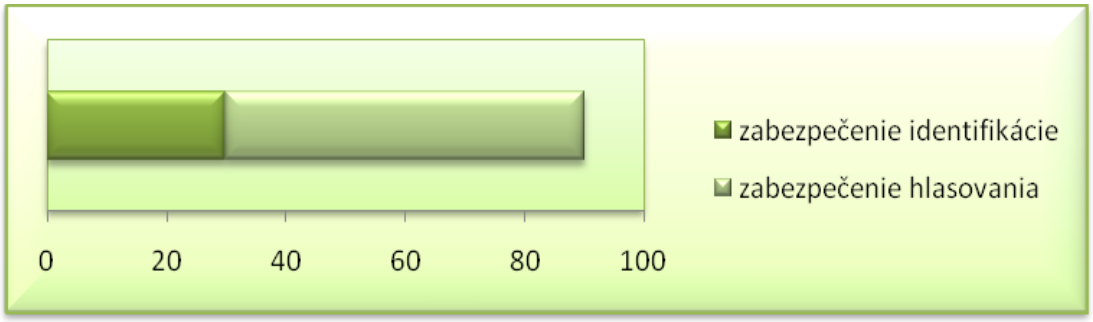
$$Z_h = \sum f + p + h + s = 5 + 5 + 5 + 5 = 20$$

Potom vypočítané hodnoty dosadíme do posledného vzorca pomocou ktorého sa vypočíta celkové zabezpečenie.

$$Z = 2\sum Z_i + 3\sum Z_h + \sum a = 2.15 + 3.20 = 70$$

Celkové zabezpečenie získalo 70 bodov, ktoré dosadíme podľa tabuľky č.6, pretože nemáme k dispozícii softwarové zabezpečenie, do správneho bodového rozhrania a vyšlo spoľahlivé zabezpečenie.

Na obrázku č.40 je graf na ktorom je znázornený pomer medzi zabezpečením identifikácie voliča a hlasovania.

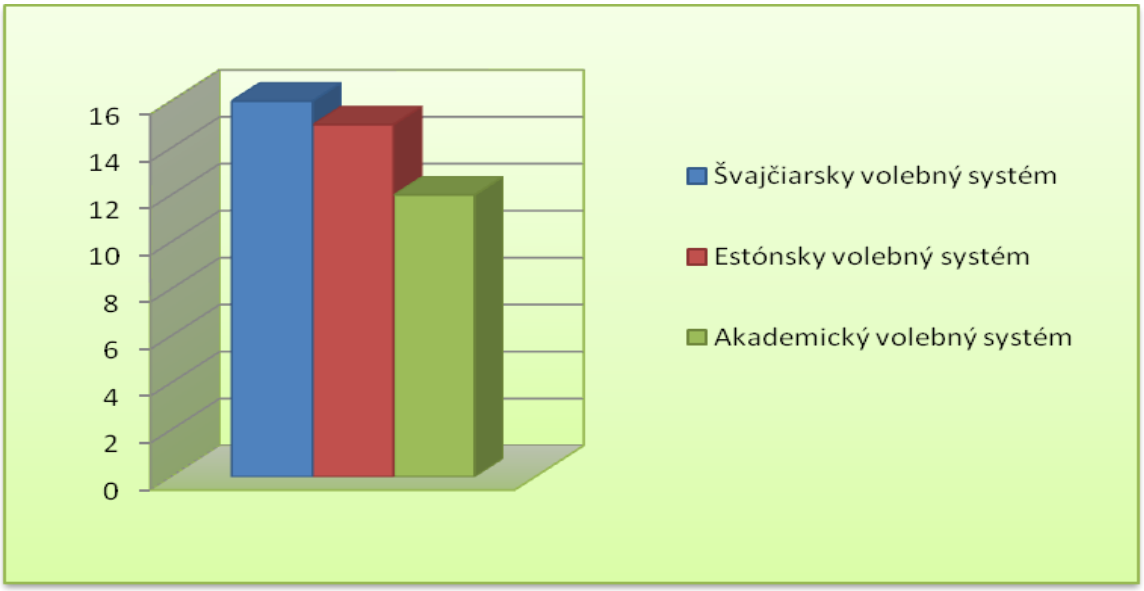


Obrázok 40 Graf pomeru zabezpečenia identifikácie a hlasovania

5.2 Grafické porovnanie hodnotených elektronických volebných systémov

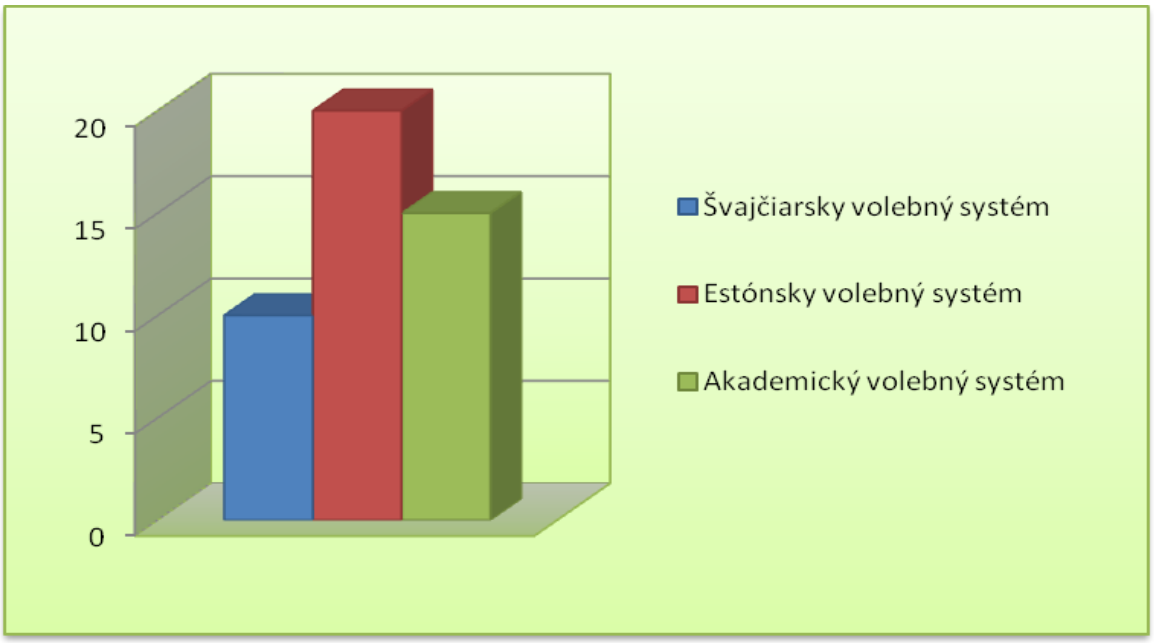
Na základe predchádzajúcich vyhodnotení môžeme teraz jednotlivé elektronické volebné systémy porovnať.

Na obrázku č.41 je graf zobrazujúci porovnanie zabezpečenia volebných systémov. Ako je z grafu vidno, najviac bodov získal švajčiarsky a najmenej akademický.



Obrázok 41 Graf - porovnanie volebných systémov na základe zabezpečenia identifikácie

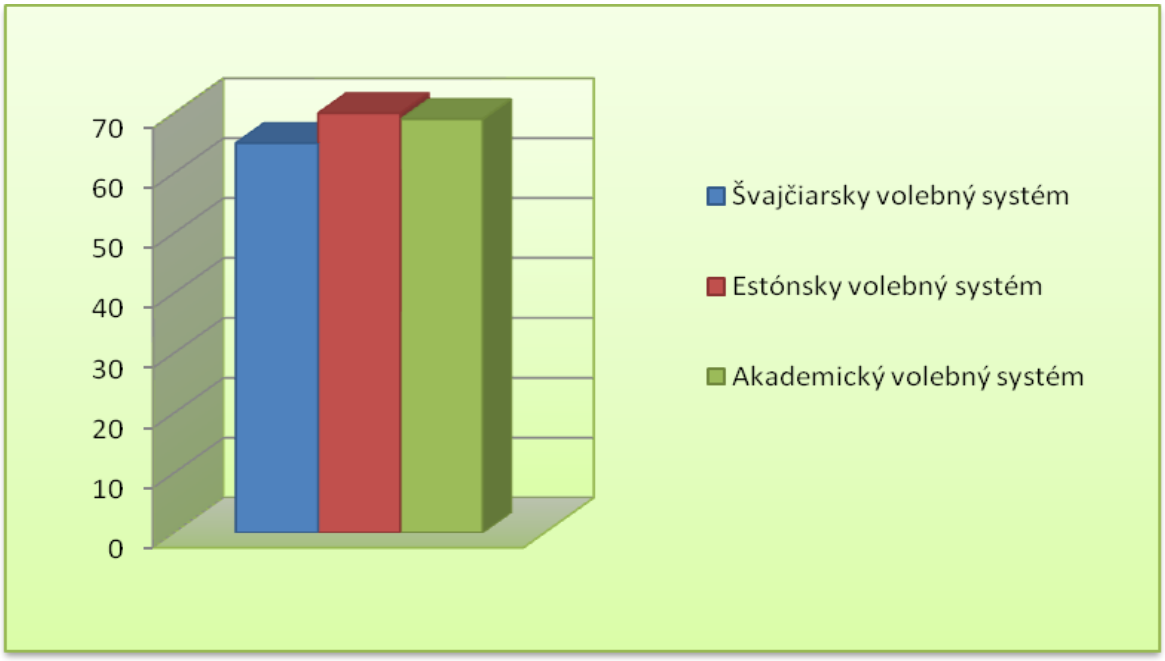
Na obrázku č.42 je na grafe zobrazené porovnanie jednotlivých volebných systémov na základe zabezpečenie hlasovania. V tomto prípade najviac bodov má estónsky a najmenej švajčiarsky.



Obrázok 42 Graf - porovnanie volebných systémov na základe zabezpečenia hlasovania

Na nasledujúcom obrázku č.43 je graf na ktorom môžeme vidieť porovnanie celkových zabezpečení jednotlivých systémov. Ako je vidieť na poslednom grafe rozdiely na

celkovom zabezpečení nie sú veľké. Najviac bodov má estónsky volebný systém – 70, akademický ma len o jeden bod menej a švajčiarsky o osem bodov.



Obrázok 43 Graf - porovnanie volebných systémov na základe celkového zabezpečenia

6 POROVNANIE A ZÁVEREČNÉ VYHODNOTENIE VOLEBNÝCH SYSTÉMOV

Základné rozdelenie elektronických volieb je na remote electronic voting a poll-site electronic voting, teda na tie ktoré sú vykonávané „na diaľku“ a tie ktoré sú vykonávané vo volebnej miestnosti. Najväčší rozdiel medzi nimi je rozpoznateľný už podľa tohto rozdelenia. Pri voľbách vo volebnej miestnosti voliči hlasujú prostredníctvom hlasovacích prístrojov, pri tých „na diaľku“ je viac metód, ktoré sú už vyskúšané a bežné v niektorých štátoch, buď hlasovaním mobilným telefónom alebo internetovým hlasovaním.

Všetky tri systémy elektronických volieb, ktoré boli hodnotené v predchádzajúcej kapitole sú vykonávané „na diaľku“ - prostredníctvom internetu. Ich zabezpečenie ale vôbec nie je identické.

Ako je vidieť v predchádzajúcej kapitole, či už z tabuľky č.3 ktorá obsahuje systém pre hodnotenie elektronických volebných systémov alebo následne pri samotnom hodnotení systémov jednotlivých štátov, zabezpečenie pozostáva z niekoľkých zabezpečení, ktoré na seba nadväzujú a vzájomne sa dopĺňajú, niektoré majú na spoľahlivosť vplyv väčší, iné menší.

V podkapitole 5.2 sú graficky znázornené vyhodnotenia volebných systémov, ktoré boli vypočítané v kapitolách predchádzajúcich. Ako prvé je zobrazené na obrázku č.41 zabezpečenie identifikácie. Prvým bezpečnostným krokom pri elektronickom hlasovaní je autentizácia voliča, je dôležité zabezpečiť aby nebolo možné sa prihlásiť miesto niekoho iného a tak zneužiť jeho hlas. Najviac bodov získal švajčiarsky volebný systém, kde najdôležitejšími prvkami, čo sa identifikácie voliča týka sú osobné číslo na karte a osobný identifikačný kód, ktorý sa pre zvýšenie bezpečnosti pred každými voľbami mení.

I keď na základe spoľahlivosti získal švajčiarsky systém najviac bodov, premyslenejšiu, komfortnejšiu i technologicky modernejšiu formu identifikácie majú ostatné dva systémy a to čipovú kartu. Čo sa týka estónskeho tam získava táto identifikačná karta i multifunkčné využitie, čím získavajú i voľby nový moderný charakter.

Pre zabezpečenie hlasovania bolo pochopiteľne u všetkých troch použité šifrovanie. Pri zohľadnení všetkých ostatných zabezpečení získal najviac bodov estónsky elektronický volebný systém ako je vidieť na grafe na obrázku č.42, ktorý zároveň dosiahol najviac

bodov i v celkovom vyhodnotení vypočítanom na základe posledného vyhodnocovacieho vzorca, porovnanie celkových zabezpečení jednotlivých elektronických volebných systémov bol zobrazený na obrázku č.43.

Zabezpečenie tohto elektronického volebného systému, je spoľahlivé, pretože samotné šifrovanie je ešte doplnené o elektronický podpis s digitálnym certifikátom a o ďalší PIN kód.

Už z predchádzajúcich popisov jednotlivých elektronických volebných systémov je vidieť, že akademický volebný systém má veľa spoločného s estónskym. Estónsky je však spoľahlivejší a získal preto i viac bodov, pretože v ňom je použitých viac bezpečnostných opatrení.

Ak by sme si mali vybrať ktorý elektronický volebný systém je najlepší, ako základ by sme mohli zobrať práve estónsky, v rámci identifikácie, by však bolo vhodné doplniť identifikáciu biometrickou metódou, napríklad odtlačkom prsta, čím by sa zaistila nutná fyzická prítomnosť voliča a nestačilo by odcudzenie, či inak získané identifikačné prvky ako je čipová karta alebo PIN kódy.

ZÁVER

Rovnako ako elektronická pošta, elektronické bankovníctvo sa v budúcnosti stane bežné i elektronické hlasovanie vo voľbách. Cieľom tejto diplomovej práce bolo priblížiť problematiku elektronického hlasovania, metódy pre zabezpečenie spoľahlivosti volieb a vytvorenie systému pre hodnotenie bezpečnosti volebného systému.

Najbežnejšími formami elektronického hlasovania sú internetové hlasovanie a hlasovanie hlasovacími prístrojmi. Okrem týchto dvoch v niektorých štátoch prebieha aj hlasovanie mobilným telefónom, SMS hlasovaním alebo telefónom s tónovou voľbou. Najväčším priekopníkom čo sa elektronického hlasovania týka je Estónsko, no i v ďalších štátoch je bežne používané ako je Švajčiarsko, USA, Veľká Británia, Taliansko, Švédsko, Belgicko, Nórsko alebo Fínsko.

Elektronické hlasovanie má tiež hlavnú úlohu pri elektronizácii verejnej správy. Pre verejnú správu majú voľby rozhodne veľký význam a ich elektronizácia tvorí základ e-governmentu. Elektronické voľby so sebou prinášajú výhody aj nevýhody. Medzi výhody patrí rýchle sčítanie hlasov alebo zamedzenie vzniku neplatného hlasu. Za nevýhodu môžeme považovať počiatočnú nedôveru voličov a rozhodne nie malé náklady súvisiace najmä so zavedením e-volieb. Za najväčšie riziko rozhodne môžeme považovať možné zmanipulovanie výsledkov hackerskými útokmi.

Najvhodnejšie je pravdepodobne pre elektronické hlasovanie využitie internetu. Či už z pohľadu bezpečnosti, ale i z pohľadu komfortnosti, nie je nutné ísť hlasovať do volebnej miestnosti, čo môže zvýšiť počet voličov, najmä mladých ľudí, ktorí pracujú denne na počítači. U elektronických volieb, ktoré sa vykonávajú tradične vo volebnej miestnosti na hlasovacích prístrojoch je jednou z mála výhod oproti ostatným spomínaným metódam, že je možné zabezpečiť i fyzickú ochranu voličov, aby ich nikto nemohol pri volení donútiť hlasovať v prospech iného kandidáta proti ich vôli.

Internetové hlasovanie je dostatočne bezpečné ak sa dodržia bezpečnostné požiadavky. Základom je spoľahlivá autentifikácia, bezpečnosť sa priamo úmerne zvyšuje so zvyšujúcim sa počtom informácii, ktorými sa volič identifikuje. Preto je najlepšie pre identifikáciu použiť minimálne tri identifikačné údaje resp. informácie. Dôležité je zabezpečiť komunikačný kanál medzi voličom a volebným serverom šifrovaním. Pre komunikáciu by sa nemal využívať protokol HTTP ale jeho zabezpečenú verziu HTTPS.

Rovnako je dôležité používať kvalitný software a hardware. A vyriešiť otázku ich zabezpečenia. Samozrejmosťou sú antivírové programy, firewall, aktualizácie softwaru apod. Tiež je dôležité aby k volebnému serveru nemali prístup neoprávnené osoby. Nevyhnutné je aby pred každými voľbami bolo vykonané testovanie celého volebného systému nezávislou skupinou odborníkov, čím sa odhalia prípadné chyby a nedostatky systému a môžu sa následne vyriešiť.

Pre jednoduché zistenie, ako je systém elektronických volieb spoľahlivý je v kapitule 5 na základe jednotlivých zabezpečení a bezpečnostných opatrení, ktoré sú vo volebnom systéme použité vytvorený systém pre hodnotenie elektronických volebných systémov, ktorý ide jednoducho použiť ak máme k dispozícii popis volebného systému, z ktorého môžeme zistiť aké zabezpečenia sú v ňom použité.

Ako príklad boli v tejto práci hodnotené tri volebné systémy – švajčiarsky, akademický a estónsky. Ako najbezpečnejší nám podľa hodnotenia vyšiel estónsky, ktorý bol v Estónsku odskúšaný už v niekoľkých voľbách a ukazuje sa, že jeho zabezpečenie je dostatočne spoľahlivo navrhnuté.

ZÁVER V ANGLIČTINE

Similarly like electronic mail, electronic banking becomes routine also the electronic elections in voting. The aim of this thesis was to bring the electronic voting, methods for achieving the reliability of electronic voting close and creating system for assessment security of the voting system.

The most common forms of electronic voting are Internet voting and voting with voting machines. Apart these two forms, in some states is also a mobile phone voting, through SMS or touch-tone telephone. The biggest pioneer in e-voting is Estonia, but also in other countries is commonly used as Switzerland, USA, Great Britain, Italy, Sweden, Belgium, Norway or Finland.

Electronic voting also has a major role in the electronization of government. Voting is very important for government and its electronization form a base of e-government. Electronic elections have advantages and disadvantages. Advantages include fast vote counting, possible increasing especially young voters or preventing of invalid votes. For disadvantage can be considered an initial distrust of voters, and certainly not a small expenses be connected with the introduction of e-voting. The greatest risk we can consider the manipulation of the voting results by hacker attacks.

The best way is probably to use the Internet e-voting. From the view of security, or also in the view of comfort, because is not important to go into the polling station, which may increase the number of voters, particularly young people, who work daily on the computer. For electronic voting, which is performed traditionally in the polling station on voting devices is one of the few advantages that, it is possible to secure the physical protection of voters that no one could force them in election to vote in favor of another candidate against their will.

Internet voting is safe if we keep safety requirements. The base is the reliable authentication, security, the proportion increases with increasing amount of information which identifies the voter. Therefore, it is best used to identify at least three identification data or information. It is important to ensure a channel of communication between voters and election server by encryption. Communications should not use the HTTP protocol but its more secure HTTPS version.

It is also important to use best quality software and hardware. And solve the issue of their security. Of course there are antivirus programs, firewall, software updates, etc.. It is also important for unauthorized persons not to have access to the election server. It is essential that before every election has been done testing the electoral system by an independent group of experts to reveal any errors and bugs, and can be subsequently resolved.

For easy finding how reliable is system of electronic elections is in chapter 5 on the base of individual securities and safety measures that are used in the electoral system is a system for evaluating electronic electoral systems, which is easy to use if we have a description of the electoral system from which we can determine what security systems are used in it in disposal.

As an example in this work were evaluated three voting systems – Swiss, academic and Estonian. As the safest by rating went the Estonian one, which has been tested in Estonia by several elections and shows that its provision is designed with reasonable certainty.

ZOZNAM POUŽITEJ LITERATÚRY

[1] KOMISE EVROPSKÝCH SPOLEČENSTVÍ. eEurope2005: Informační společnost pro všechny [online]. Brusel : Komise Evropského společenství, [2002] [cit. 2011-02-01]. 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. 2011-02-04]. 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. 2011-01-30]. 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.

[6] Alexander Prosser, Robert Krimmer (Eds.): Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, July, 7th-9th, 2004, in Schloß Hofen / Bregenz, Lake of Constance, Austria, Proceedings. GI 2004, ISBN 3-88579-376-8

[7] Leenes, R., Svensson, K.: Adapting E-voting in Europe: Context matters.Proceedings of EGPA, 2002.

[8] Cev.ie [online]. 2006 [cit. 2011-02-22]. Commission on Electronic Voting: Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. Dostupné z WWW: <http://www.cev.ie/htm/report/download_second.htm>.

[9] FISCHER, Eric. The Direct Recording Electronic Voting Machine. CRS Report for Congress. 2006, s. 1-22. Dostupný z WWW: http://usinfo.org/enus/government/elections/docs/CRS%20Electronic%20Voting%209[1].26.06.pdf.

[10] NOVOTNÝ, Marián. Elektronické voľby – sci-fi alebo blízka budúcnosť?. IT NEWS [online]. 2009, 9, [cit. 2011-02-22]. Dostupný z WWW:

<http://www.itnews.sk/tituly/infoware/free-clanky/2009-11-09/c130130-iw-elektronicke-volby-sci-fi-alebo-blizka-buducnost>.

[11] Technovelgy.com [online]. 2008 [cit. 2011-02-22]. Electronic Voting Banned In Netherlands. Dostupné z WWW: <http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=1685>.

[12] Howstuffworks.com [online]. 2002 [cit. 2011-03-02]. How E-voting Works. Dostupné z WWW: <http://www.howstuffworks.com/e-voting.htm>.

[13] Wikipedia.org [online]. 2011 [cit. 2011-03-02]. Electronic voting. Dostupné z WWW: <http://en.wikipedia.org/wiki/Electronic_voting>.

[14] FRANKOVIČ, Radoslav. ELEKTRONICKÉ VOĽBY. Košice, 2009. 40 s. Diplomová práce. Univerzita Pavla Jozefa Šafárika v Košiciach.

[15] Internetprovsechny.cz [online]. 2006 [cit. 2011-03-10]. Internet v praxi: Komunální volby v Estonsku, dočkáme se i u nás?. Dostupné z WWW: <http://www.internetprovsechny.cz/internet-v-praxi-komunalni-volby-v-estonsku-dockame-se-i-u-nas/>.

[16] OKRUHLICOVÁ, Martina. Parlamentný inštitút [online]. 2002 [cit. 2011-03-10]. Kancelária Národnej rady Slovenskej republiky. Dostupné z WWW: <www.p3.sk/sk/evoting/prehladEvote.doc>.

[17] Blog.sme.sk/ [online]. 2011 [cit. 2011-03-16]. Elektronické voľby sa stávajú realitou. Dostupné z WWW: <http://meciar.blog.sme.sk/c/258838/Elektronicke-volby-sa-stavaju-realitou.html>.

[18] E-voting.cc [online]. 2010 [cit. 2011-03-16]. E-voting.cc/static/evoting/files/e-voting-map-2010. Dostupné z WWW: <http://www.e-voting.cc/static/evoting/files/e-voting-map-2010.pdf>.

[19] Informatizacia.sk [online]. 2011 [cit. 2011-03-22]. Informatizácia verejnej správy. Dostupné z WWW: <http://www.informatizacia.sk/egovernment/519s>.

[20] About.com [online]. 2010 [cit. 2011-03-22]. Is E-Voting Safe?. Dostupné z WWW: <http://pcworld.about.net/magazine/2206p121id115608.htm>.

[21] NEUMANN, Peter. Csl.sri.com [online]. 2003 [cit. 2011-03-29]. Security Criteria for Electronic Voting. Dostupné z WWW: <http://www.csl.sri.com/users/neumann/ncs93.html>.

[22] GRITZALIS, Dimitris. Secure electronic voting. United States of America : Kluwer Academic Publishers, 2003. 240 s. ISBN 1-4020-7301-1.

[23] Wikipedia.org [online]. 2011 [cit. 2011-03-29]. Elektronický podpis. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Elektronický_podpis>.

[24] Mvcr.cz [online]. 2000 [cit. 2011-03-30]. Úplné znění zákona č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů. Dostupné z WWW: <http://www.mvcr.cz/soubor/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

[25] STANEK, Martin. Základy kryptológie [online]. 2004 [cit. 2011-03-30]. Základy kryptológie. Dostupné z WWW: <http://www.dcs.fmph.uniba.sk/~stanek/crypto/main2.pdf>.

[26] Http://cs.wikipedia.org [online]. 2011 [cit. 2011-03-30]. Digitální certifikát. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t>.

[27] Interval.cz [online]. 2003 [cit. 2011-03-30]. Co to je digitální certifikát. Dostupné z WWW: <http://interval.cz/clanky/co-to-je-digitalni-certifikat/>.

[28] Wikipedia.org [online]. 2011 [cit. 2011-03-31]. HTTPS. Dostupné z WWW: <http://cs.wikipedia.org/wiki/HTTPS>.

[29] Dtca.sk [online]. 2005 [cit. 2011-04-14]. Princípy bezpečnej komunikácie . Dostupné z WWW: <http://www.dtca.sk/support/principles.php>.

[30] Sosvranovska.eu [online]. 2006 [cit. 2011-04-14]. Šifrovanie. Dostupné z WWW: <http://www.sosvranovska.eu/KLOKOCOVA/CO%20V%20SKOLE/INF%20pomĂ´cky/Šifrovanie.pdf2006>.

[31] Wikipedia.org [online]. 2011 [cit. 2011-04-15]. Digital Signature Algorithm. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Digital_Signature_Algorithm>.

[32] Wikipedia.org [online]. 2011 [cit. 2011-04-15]. Secure Hash Algorithm. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Secure_Hash_Algorithm>.

[33] Wikipedia.org [online]. 2011 [cit. 2011-04-15]. Message-Digest algorithm. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Message-Digest_algorithm>.

[34] Testnet-8.net [online]. 2004 [cit. 2011-04-15]. Testnet-8.net. Dostupné z WWW: <http://testnet-8.net/modules.php?name=News&file=article&sid=13>.

[35] Wikipedia.org [online]. 2011 [cit. 2011-04-16]. Firewall. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Firewall>.

[36] ZEMAN, Peter. BEZPEČNOSŤ V POČÍTAČOVÝCH SIEŤACH S OHĽADOM NA DETEKCIU ÚTOKOV. Žilina, 2006. 43 s. Bakalářská práce. ŽILINSKÁ UNIVERZITA V ŽILINE.

[37] SIROTNÝ, Miroslav. TOPOLOGIE SÍTÍ A JEJICH MONITOROVÁNÍ. Brno, 2010. 53 s. Diplomová práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ.

[38] Wikipedia.org [online]. 2011 [cit. 2011-04-19]. Security token. Dostupné z WWW: <http://en.wikipedia.org/wiki/Security_token>.

[39] ZOBANÍK, Kamil. Trendy vývoje identifikačních prostředků osob. Zlín, 2007. 85 s. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[40] HANÁČEK, Petr; MATYÁŠ, Vašek. Čipové karty v informačních systémech [online]. 2007 [cit. 2011-04-19]. Čipové karty v informačních systémech. Dostupné z WWW: <http://www.fit.vutbr.cz/~hanacek/papers/Datakon03.pdf>.

[41] Posterus.sk [online]. 2010 [cit. 2011-04-20]. Biometrické metódy pre rozpoznávanie obrazov ľudských tvárí. Dostupné z WWW: <http://www.posterus.sk/?p=5334>.

[42] ŠČUREK, Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. Ostrava, 2008. 58 s. Studijní text. VŠB TU Ostrava.

[43] Votenet.com [online]. 2011 [cit. 2011-04-23]. Telephone Voting. Dostupné z WWW: <http://www.votenet.com/telephone_voting.cfm>.

[44] Vermont-elections.org [online]. 2004 [cit. 2011-04-26]. VERMONT SECRETARY OF STATE. Dostupné z WWW: <http://vermont-elections.org/elections1/VoteByPhone.html#System Security>.

[45] FELDMAN, Ariel; HALDERMAN, Alex; FELTEN, Edward. Princeton.edu [online]. 2006 [cit. 2011-05-03]. Security Analysis of the Diebold AccuVote-TS Voting Machine. Dostupné z WWW: <http://citp.princeton.edu/pub/ts06full.pdf>.

[46] Wikipedia.org [online]. 2011 [cit. 2011-05-04]. Denial-of-service attack. Dostupné z WWW: <http://en.wikipedia.org/wiki/Denial-of-service_attack>.

[47] Wikipedia.org [online]. 2011 [cit. 2011-05-04]. Phishing. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Phishing>.

[48] Wikipedia.org [online]. 2011 [cit. 2011-05-04]. Malware. Dostupné z WWW: <http://sk.wikipedia.org/wiki/Malware>.

[49] MADISE, Ülle. E-voting.cc [online]. 2006 [cit. 2011-08-16]. E-voting in Estonia experience. Dostupné z WWW: <http://www.e-voting.cc/static/evoting/files/First_Experience_with_E-Voting_in_Estonia.pdf>.

[50] Mailclad.com [online]. 2003 [cit. 2011-08-15]. The Geneva Internet voting system. Dostupné z WWW: <http://www.mailclad.com/articles/pre_projet_eVoting_eng.pdf>.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

VS	Verejná správa
SMS	Short Message Service
ID	Identity Document
PIN	Personal Identification Number
PEB	Personal Electronic Ballot
CPU	Central processing unit
PCMCIA	Personal Computer Memory Card International Association
USB	Universal Serial Bus
RFID	Radio Frequecy IDentification
ROM	Read-Only Memory
PVC	Polyvinylchlorid
ABS	Akrylonitrilbutadienstyren
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CCD	Charge-coupled device
RSA	Rivest, Shamir, Adleman
DSA	Digital Signature Algorithm
SHA	Secure Hash Algorithm
MD5	Message Digest 5
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
IPS	Intrusion Prevention Systems

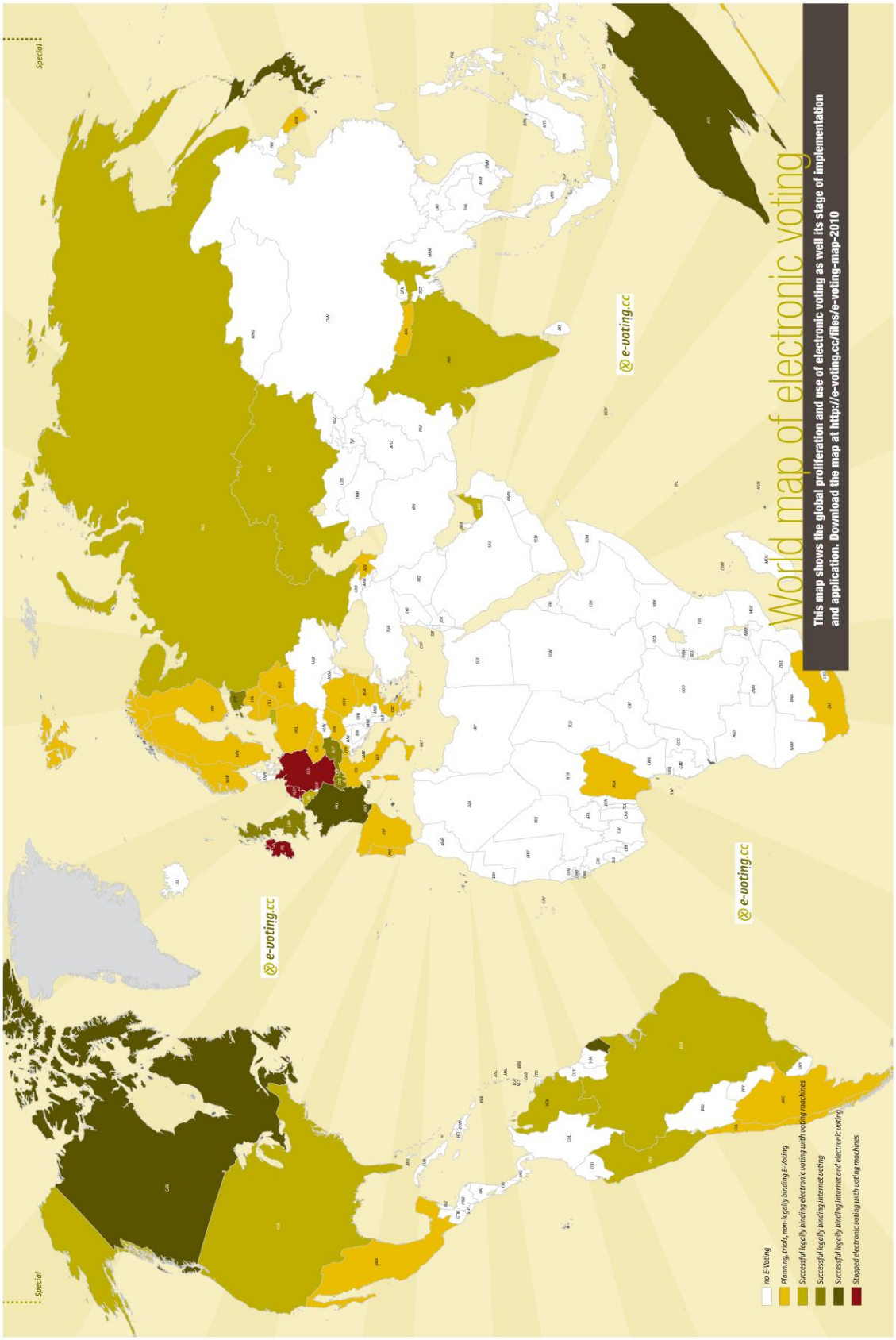
IDS	Intrusion Detection System
HIDS	Host-based Intrusion Detection System
NIDS	Network-based Intrusion Detection System
DRE	Direct Recording Electronic
DDoS	Distributed Denial of Service
RS	Registračný server
PS	Počítací server

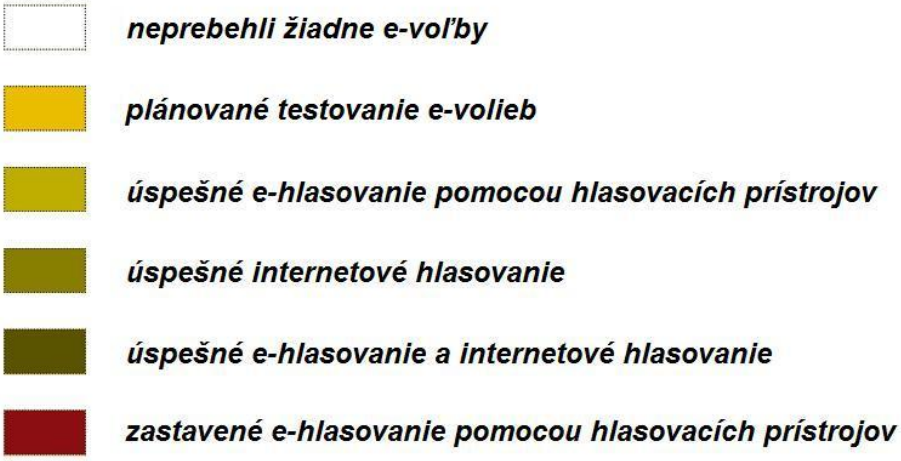
ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: MAPA ZNÁZORŇUJÚCA VZŤAH ŠTÁTOV SVETA K ELEKTRONICKÝM VOĽBÁM [18]




neprebehli žiadne e-voľby
plánované testovanie e-volieb
úspešné e-hlasovanie pomocou hlasovacích prístrojov
úspešné internetové hlasovanie
úspešné e-hlasovanie a internetové hlasovanie
zastavené e-hlasovanie pomocou hlasovacích prístrojov