

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Pilotný projekt elektronických volieb

Diplomová práca

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Pilotný projekt elektronických volieb

Diplomová práca

Študijný program: Informatika
Študijný odbor: 2508 Informatika
Školiace pracovisko: Katedra informatiky
Školiteľ: doc. RNDr. Daniel Olejár, PhD.

Bratislava, 2012

Bc. Filip Vojtko



Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Filip Vojtko
Študijný program: informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: 9.2.1. informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský

Názov: Pilotný projekt elektronických volieb

Cieľ: Vybrať vhodné riešenie elektronických volieb a implementovať ho v modelovom prostredí. Otestovať jeho funkcionality a posúdiť technické, organizačné, bezpečnostné a výkonnostné aspekty navrhovaného riešenia a možnosti jeho rozšírenia na celú SR.

Vedúci: doc. RNDr. Daniel Olejár, PhD.

Katedra: FMFI.KI - Katedra informatiky

Dátum zadania: 02.11.2010

Dátum schválenia: 04.11.2010

prof. RNDr. Branislav Rován, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Ďakujem vedúcemu svojej diplomovej práce, doc. RNDr. Danieľovi Olejárovi, PhD., za možnosť pracovať na tejto mimoriadne zaujímavej téme, trpezlivé vedenie a za cenné rady, ktoré prispeli k skvalitneniu výslednej práce. Moje poďakovanie tiež patrí doc. RNDr. Martinovi Stanekovi, PhD. za venovaný čas a objektívnu kritiku, ktorá sa podpísala na výslednej práci. Táto diplomová práca by nevznikla bez podpory mojej najbližšej rodiny.

Ďakujem.

Abstrakt

Autor: Bc. Filip Vojtko
Názov diplomovej práce: Pilotný projekt elektronických volieb
Škola: Univerzita Komenského v Bratislave
Fakulta: Fakulta matematiky, fyziky a informatiky
Katedra: Katedra informatiky
Vedúci diplomovej práce: doc. RNDr. Daniel Olejár, PhD.
Rozsah práce: 79 strán
Bratislava, máj 2012

Diplomová práca je pilotným projektom elektronických volieb realizujúcim v modelovom prostredí volebný protokol navrhnutý na základe existujúcich riešení elektronických volieb vo svete. V práci sú definované bezpečnostné požiadavky na volebné systémy, ktoré sú následne použité pri analýze vybraných existujúcich volebných schém elektronických volieb v USA, Švajčiarsku, Estónsku a Nórsku. Na základe tejto analýzy je navrhnutý nový volebný protokol pre elektronické voľby a je implementované pilotné riešenie. Práca sa ďalej zaoberá bezpečnostnými a výkonnostnými aspektami navrhovaného volebného protokolu. Analýza výkonnostných aspektov vychádza z výsledkov výkonnostných testov pilotného projektu elektronických volieb v modelovom prostredí. Výsledky diplomovej práce sú základom pre pilotný projekt elektronických volieb v Slovenskej republike.

Kľúčové slová: volebný systém, elektronické voľby, pilotný projekt, bezpečnostné aspekty, výkonnostné aspekty

Abstract

Author: Bc. Filip Vojtko
Title: Electronic voting pilot project
University: Comenius University, Bratislava
Faculty: Faculty of Mathematics, Physics and Informatics
Department: Department of Computer Science
Advisor: doc. RNDr. Daniel Olejár, PhD.
Thesis length: 79 pages
Bratislava, May 2012

Diploma thesis is an electronic voting pilot project, which realises a voting scheme in a model environment. The voting scheme has been based on existing electronic voting solutions. The thesis has defined the voting system security requirements, which had been used in an analysis of the existing electronic voting schemes that are used in USA, Switzerland, Estonia and Norway. A new electronic voting protocol based on this analysis has been proposed and a pilot solution has been implemented. The thesis has also dealt with the security and performance aspects of the proposed voting protocol. The performance aspects analysis has used results from performance tests of the electronic voting pilot project implemented in the model environment. The results of the analysis should be used as a base for the Slovak electronic voting pilot project.

Keywords: voting system, electronic voting, pilot project, security aspects , performance aspects

Predhovor

Elektronické voľby sú v odbornej i laickej verejnosti aktuálnou témou. Poznatky z rôznych informatických a elektroinžinierskych oblastí sa za posledné roky posunuli dopredu raketovým tempom. Mnohí ľudia sa preto začínajú pýtať, či už dosiahli poznatky a technológie potrebnú úroveň pre nahradenie klasických papierových volieb alebo jednoduchých hlasovacích strojov elektronickými voľbami cez Internet z pohodlia domova. Niektoré poznatky zo zahraničia dokonca naznačujú, že elektronické voľby vieme realizovať už teraz a za porovnateľných podmienok ako doterajšie papierové hlasovania. Objavujú sa početné odborné i populárne články, ktoré ovplyvňujú optimizmom a nádejou v skoré zavedenie elektronických volieb v mnohých krajinách sveta, avšak rovnako sa objavujú pesimistické články a varovania pred mnohými rizikami a hrozbami, ktoré zavedenie so sebou prináša zavedenie elektronických volieb.

Naším cieľom bude preskúmať oba tábory, pokúsiť sa zhodnotiť možnosti realizácie elektronických volieb, posúdiť možné riziká a hrozby, ktoré by realizáciou elektronických volieb mohli ovplyvniť, a navrhnúť efektívne riešenia pre ich minimalizáciu. Pokúsime sa tiež implementovať vybrané riešenie v našom modelovom prostredí a analyzovať jeho vlastnosti.

Obsah

Úvod	1
1 Prehľad pojmov	3
2 Voľby	4
2.1 Volebný systém	4
2.1.1 Realizácia volieb	5
2.1.2 Útoky na volebný systém	6
2.1.3 Požiadavky na volebný systém	7
2.1.4 Volebný systém v Slovenskej republike	9
3 Elektronické voľby	12
3.1 Úrovne elektronizácie volieb	12
3.2 Volebné schémy pre elektronické voľby	16
3.2.1 Projekt SERVE	18
3.2.2 Švajčiarsky volebný protokol	20
3.2.3 Estónsky volebný protokol	23
3.2.4 Nórsky volebný protokol	27
4 Návrh volebného protokolu	31
4.1 Požiadavky na volebný protokol	31
4.2 Roly účastníkov	32
4.3 Komponenty volebného protokolu	33
4.3.1 Volebná aplikácia	34
4.3.2 Sieťový server	34
4.3.3 Dočasné úložisko hlasov	35
4.3.4 Sčítací server	35
4.3.5 Publikáčny server	36
4.3.6 Externé komponenty	37
4.4 Volebný protokol	37
4.4.1 Prípravná fáza	38
4.4.2 Volebná fáza - hlasovanie voliča	39
4.4.3 Volebná fáza - predspracovanie hlasov	41

4.4.4	Fáza spracovania hlasov	43
4.5	Dohľad nad priebehom hlasovania	45
4.5.1	Volebná komisia	46
4.5.2	Dohľad voličov	46
4.5.3	Dohľad pozorovateľov	47
4.6	Bezpečnostná analýza	48
4.6.1	Model útočníka	48
4.6.2	Predpoklady	50
4.6.3	Analýza útočných scenárov	52
5	Implementácia volebného protokolu	58
5.1	Technické parametre	58
5.1.1	Systémové požiadavky	59
5.1.2	XML schémy	59
5.1.3	Použité kryptografické prvky	60
5.2	Komponenty volebného protokolu	61
5.2.1	Volebná aplikácia	61
5.2.2	Sieťový server	63
5.2.3	Dočasné úložisko hlasov	65
5.2.4	Sčítací server	67
5.2.5	Poskytovateľ služby časovej pečiatky	69
5.2.6	Publikačný server	70
5.2.7	Jednoduchá certifikačná autorita	71
5.3	Výkonnostné aspekty	72
5.3.1	Konfigurácia testovacej zostavy	72
5.3.2	Výsledky	73
	Záver	76
	Literatúra	78

Úvod

Téma informatizácie spoločnosti v súčasnosti rezonuje nielen v odborných kruhoch ale aj v širokej verejnosti. Osobné počítače a pripojenie na celosvetovú sieť Internet sa za posledných 10 rokov rozšírili skoro do každej slovenskej domácnosti. Okrem možnosti získať informácie a komunikovať s ľuďmi z ľubovoľného miesta na svete je v súčasnosti možné z pohodlia domova nakupovať, prehliadať multimediálny obsah, spravovať svoje finančné prostriedky či oficiálne komunikovať so samosprávou a štátnymi orgánmi. Práve elektronická komunikácia s úradmi je v Slovenskej republike dlho očakávanou novinkou, ktorú umožnili zákon o elektronickom podpise č. 215/2002 Z.z. a ďalšie úpravy existujúcej legislatívy.

Už dnes je možné s úradmi elektronicke komunikovať, získavať potrebné doklady či zaplatiť mnohé poplatky. Z pohľadu občana sa komunikácia s verejnou správou výrazne zjednodušuje, z pohľadu verejnej správy dochádza k efektívnejšiemu nakladaniu s pridelenými verejnými financiami. Občan však neprichádza do kontaktu s verejnou správou iba pri riešení svojich potrieb a povinností, demokratické zriadenie mu totiž umožňuje podieľať sa na riadení štátu a samosprávou svojich zástupcov. Voľby sú jedným zo základných pilierov demokracie a ovplyvňujú smerovanie krajiny. Skoro každý druhý rok sa občania stretávajú vo volebných miestnostiach, aby odovzdali svoj papierový hlasovací lístok v rôznych voľbách a referendách. Hlavnými nevýhodami papierových volieb sú finančná záťaž na rozpočet¹ a nezáujem či nechotu voličov dostaviť sa do hlasovacích miestností². Vo svetle finančnej krízy a záujmu politických strán o pritiahnutie voličov sa tak postupne do popredia dostáva otázka nahradenia papierových volieb elektronicke.

Ako však uskutočniť elektronicke voľby? Používa už niekto elektronicke voľby? Je vôbec možné takéto voľby uskutočniť pri zachovaní súčasných požiadaviek na bezpečnosť volieb? Aké dodatočné riziká a hrozby so sebou elektronicke voľby prinášajú? Je možné vytvoriť systém pre elektronicke hlasovanie na báze exis-

¹Usporiadanie volieb a neúspešného referenda v roku 2010 stálo daňových poplatníkov zhruba 16 miliónov eur (Návrh záverečného účtu kapitoly za rok 2010, Ministerstvo vnútra SR).

²Účasť na jednotlivých voľbách sa pohybuje od 20-60% oprávnených voličov.

tujúcich technických prostriedkov s minimálnymi dodatočnými investíciami? V diplomovej práci sa pokúsime zodpovedať na tieto otázky a vybrať vhodné riešenie pre realizáciu elektronických volieb u nás.

V kapitolách 1 a 2 zdefinujeme základné pojmy z oblasti volieb, popíšeme fázy priebehu volieb a možné útoky na volebný systém a určíme požiadavky, ktoré by mal dobrý volebný systém spĺňať, aby ho verejnosť považovala za dostatočne dôveryhodný a spoľahlivý.

V 3. kapitole sa pozrieme na možnosti elektronizácie volieb, zdefinujeme úrovne elektronizácie a popíšeme niektoré zahraničné implementácie elektronických volieb, medzi inými aj estónsku implementáciu elektronických volieb. Estónsko ako prvý štát na svete zaviedlo celoštátne elektronické hlasovanie cez Internet ako alternatívu ku klasickému papierovému hlasovaniu.

V 4. kapitole sa pokúsime na základe poznatkov z predchádzajúcich kapitol navrhnúť riešenie elektronických volieb a posúdime jeho organizačné a bezpečnostné aspekty. Na zhodnotenie vybraného riešenia naviažeme v kapitole 5, v ktorej sa zameriame na konkrétnu implementáciu elektronických volieb a posúdime jej výkonnostné aspekty.

Jednotlivými kapitolami sa budeme snažiť priniesť komplexný pohľad na problematiku realizácie elektronických volieb: od bezpečnostných aspektov cez výkonnostné až po niektoré organizačné aspekty. Vzhľadom na rozsah jednotlivých problematík sa nebudeme každej z nich venovať do maximálnych detailov, avšak veríme, že naša diplomová práca podnieti ďalší záujem o realizáciu elektronických volieb na Slovensku a vyvolá odbornú diskusiu, ktorá bude v konečnom dôsledku viesť k úspešnej realizácii niektorého z riešení elektronických volieb aj u nás, ktorá podnieti voličov k vyššej účasti na voľbách a zvýši záujem občanov o veci verejné.

Kapitola 1

Prehľad pojmov

Na úvod diplomovej práce definujeme niektoré základné pojmy, s ktorými budeme v priebehu tejto práce narábať a na ktoré sa budeme odvolávať. V priebehu diplomovej práce budeme používať základné pojmy z oblasti kryptografie, niektoré z najčastejšie využívaných pojmov uvádzame nižšie. Príklady ich použitia ako i ďalšie poznatky z oblasti kryptografie môže čitateľ nájsť v [MVO96] alebo inej odbornej literatúre.

Demokracia – „vláda ľudu“, forma politického zriadenia, v ktorom rozhoduje ľud

Zastupiteľská demokracia – demokracia, v ktorej si ľud vyberá zástupcov, ktorí konajú v jeho mene

Voľby – proces výberu zástupcov ľudu

Volič – osoba zúčastňujúca sa volieb hlasovaním;

Oprávnený volič – volič, ktorý sa nachádza na zozname voličov oprávnených zúčastniť sa volieb;

Mandát – oprávnenie k vykonávaniu činnosti uvedenej v mandáte;

Volebné obdobie – obdobie platnosti mandátu zvoleného zástupcu;

Volebná komisia – zoskupenie osôb alebo inštitúcia zodpovedná za organizáciu volieb a spracovanie výsledkov volieb;

Pozorovateľ – nezávislá osoba alebo inštitúcia dozerajúca na priebeh volieb;

Šifrovanie – transformácia údajov z čitateľnej podoby na šifrovaný text (do podoby, ktorá nie je zrozumiteľná neoprávneným osobám);

Dešifrovanie – transformácia údajov zo zašifrovanej do čitateľnej podoby;

Symetrické šifrovanie – skupina párov šifrovacích a dešifrovacích transformácií, ktoré na šifrovanie aj dešifrovanie využívajú rovnaké tajomstvo (kľúč);

Asymetrické šifrovanie – skupina párov transformácií, ktoré na šifrovanie a dešifrovanie využívajú dvojicu kľúčov - verejný a súkromný;

Elektronický podpis – kryptografická štruktúra nahrádzajúca vlastnoručný podpis v digitálnom svete;

Časová pečiatka – kryptografická štruktúra nahrádzajúca hodnovernú informáciu o čase v digitálnom svete.

Kapitola 2

Voľby

Voľby sú základným prvkom zastupiteľskej demokracie, v ktorej si spoločnosť hlasovaním vyberie zástupcov¹, ktorí budú spoločnosť reprezentovať a určovať jej smerovanie v ďalšom volebnom období, alebo rozhodne o prijatí alebo zamietnutí navrhovaných zmien (referendum). Voľby majú u nás i vo svete dlhú tradíciu a počas ich histórie vzniklo viacero spôsobov výberu zástupcov (alebo rozhodovania o návrhoch) hlasovaním, tzv. "volebných systémov".

2.1 Volebný systém

Nech V je množina všetkých oprávnených voličov, K je množina všetkých kandidátov (K a V nemusia byť disjunktné), m je počet zvoliteľných miest ($m \leq |K|$) a množina víťazov W je m -prvková podmnožina K . Potom ľubovoľné zobrazenie usporiadanej dvojice množín (K, V) na množinu víťazov W nazývame **volebný systém**.

Zo všetkých volebných systémov definujeme len vybrané dva volebné systémy, ktoré sú používané v referendách a vo voľbách do zastupiteľských orgánov Slovenskej republiky. Vzhľadom na tradíciu uvedených volebných systémov a cieľ diplomovej práce² sa nebudeme zaoberať ďalšími volebnými systémami ani špecifickými vlastnosťami rozšírení vybraných systémov³ a pre potreby pilotného projektu budeme preto v ďalších častiach diplomovej práce uvažovať jednoduchú variantu pluralitného volebného systému (1 volebný obvod, k kandidátov).

¹Napríklad voľby do Národnej rady Slovenskej republiky, voľby prezidenta Slovenskej republiky, voľby do Európskeho parlamentu, voľby do orgánov samosprávy obcí a ďalšie

²Vybrať vhodné riešenie elektronických volieb potenciálne rozšíriteľné na voľby v Slovenskej republike

³Napríklad rozšírenie o tzv. preferenčné hlasy

- **Pluralitný** (relatívny väčšinový) **volebný systém** je volebný systém, v ktorom má volič počet hlasov zodpovedajúci počtu volených mandátov. Volič určí podmnožinu kandidátov mohutnosti menšej alebo rovnajúcej počtu volených mandátov. Každý z kandidátov patriaci do tejto podmnožiny získa 1 hlas. Víťazmi volieb sa stávajú kandidáti s najväčším počtom získaných hlasov.
- **Pomerný volebný systém** je volebný systém, v ktorom sú mandáty pre kandidátov prerozdelené v pomere získaných platných hlasov k celkovému počtu platných hlasov. Volič má počet hlasov zodpovedajúci počtu volených mandátov. Volič určí podmnožinu kandidátov mohutnosti menšej alebo rovnajúcej počtu volených mandátov. Každý z kandidátov patriaci do tejto podmnožiny získa 1 hlas. Pomerný volebný systém môže byť doplnený o prah zvoliteľnosti potrebný pre získanie mandátov. Ak kandidát nedosiahne vopred určený prah zvoliteľnosti, nebude mu pridelený žiaden mandát a hlasy, ktoré získal vo voľbách sa nezapočítavajú do celkového počtu platných hlasov pri prerozdeľovaní mandátov.

2.1.1 Realizácia volieb

Voľby sú realizované v jednom alebo vo viacerých volebných kolách. Do ďalšieho volebného kola zvyčajne postupujú kandidáti s najvyšším počtom získaných hlasov v predchádzajúcom kole. Každé volebné kolo sa skladá z niekoľkých fáz:

- Prípravná fáza (vyhlásenie volieb, zverejnenie kandidátnych listín a ďalšie činnosti súvisiace s prípravou volebného systému na zahájenie hlasovania)
- Volebný akt (hlasovanie)
- Spracovanie odovzdaných hlasov
- Publikovanie a archivácia výsledkov

V nasledujúcich dvoch kapitolách sa budeme volebnými fázami podrobnejšie zaoberať vo vybraných riešeniach „papierových“ a elektronických volieb (viď. časti 2.1.3, 3.1 a 3.2).

2.1.2 Útoky na volebný systém

História organizácie volieb siaha tisíce rokov do minulosti a približne rovnako dlho pretrváva aj snaha niektorých ľudí ovplyvniť výsledky týchto volieb vo svoj prospech. [FHH10] Poznáme viaceré foriem útokov na používané volebné systémy:

- **Diskreditácia** volebného systému je forma nepriameho útoku na systém. Snahou útočníka je znížiť dôveryhodnosť volebného systému v očiach verejnosti s cieľom obmedziť a/alebo zrušiť prebiehajúce alebo pripravované voľby a prípadne presadiť iný (pre útočníka výhodnejší) volebný systém. Zraniteľné sú všetky volebné systémy, preto je potrebné transparentne minimalizovať možnosti diskreditácie volebného systému a jeho realizácie už pri ich návrhu.
- **Manipulácia s hlasmi** je forma útoku, pri ktorej sa útočník snaží pridať nové, odobrať alebo modifikovať existujúce platné hlasy, ktorými ovplyvní výsledok hlasovania v prospech (alebo v neprospech) vybraného kandidáta. Oba vyššie uvedené volebné systémy (pluralitný i pomerný) sú zraniteľné touto formou útoku, preto pri ich implementácii je nevyhnutné minimalizovať riziko zneužitia tejto zraniteľnosti.
- **Manipulácia so zoznamom kandidátov** je snaha útočníka ovplyvniť výsledok hlasovania pridávaním, modifikovaním a/alebo odstraňovaním mien zo zoznamu kandidátov. Vzhľadom na spôsob hlasovania je v prípade vhodne zvoleného formátu hlasu (hlas obsahuje meno kandidáta) sú pluralitné aj pomerné volebné systémy odolné voči útoku formou manipulácie so zoznamom kandidátov.
- **Manipulácia so zoznamom oprávnených voličov** je forma útoku, ktorá sa zameriava na zoznamy oprávnených voličov v období prípravy volieb alebo v priebehu volieb avšak pred prístupom vybraných voličov k hlasovaniu. Cieľom útočníka je zamedziť hlasovanie nepohodlným voličom ich odstránením zo zoznamu oprávnených voličov, resp. doplniť množinu oprávnených voličov o ďalšie osoby, ktoré odovzdajú hlas podľa pokynov útočníka. Pluralitné i pomerné volebné systémy sú zraniteľné touto formou útoku, preto pri ich implementácii je nevyhnutné minimalizovať riziko zneužitia tejto zraniteľnosti.
- **Ovplyvňovanie** voličov je forma nepriameho útoku na volebný systém. Útočník sa nezameriava na zraniteľnosť volebného systému, ale snaží sa rôznymi metódami ovplyvniť konečné rozhodnutie voliča. Medzi najčastejšie metódy patria korupcia a vydieranie. Zraniteľné sú všetky volebné systémy, preto pri ich implementácii je z dôvodu bezpečnosti voliča potrebné zabezpečiť, aby volič nevedel dokázať ako v skutočnosti hlasoval.

2.1.3 Požiadavky na volebný systém

Slobodnými demokratickými voľbami budeme nazývať voľby, v ktorých každý volič môže dobrovoľne odovzdať svoj hlas ľubovoľnému z kandidátov uchádzajúcich sa o mandát bez rizika perzekúcie. Ideálny volebný systém dôveryhodným spôsobom zabezpečuje slobodné demokratické voľby. Vzhľadom na mnohé hrozby útokov na volebné systémy definujeme špecifické požiadavky na bezpečnosť a dôveryhodnosť ideálneho volebného systému. **Ideálnym volebným systémom** nazývame každý volebný systém, ktorý spĺňa nasledujúce požiadavky:

- **Anonymita** - hlas voliča v čitateľnej podobe neobsahuje informácie o identite voliča, tj. v žiadnom okamihu volieb nie je možné získať informáciu, akým spôsobom volič hlasoval;
- **Férovosť** - volebný systém v priebehu konania volieb neumožňuje žiadnej zo zúčastnených strán (voliči, volebná komisia, pozorovatelia) získať čiasťtočné výsledky volieb alebo inú informáciu o výsledkoch, ktorá by mohla ovplyvniť ďalší priebeh hlasovania;
- **Integrita** - neplatné hlasy a neoprávnení voliči nemajú vplyv na priebeh a výsledok hlasovania;
- **Kompletnosť** - všetky platné hlasy oprávnených voličov sa podieľajú na výsledku hlasovania;
- **Nepreukázateľnosť** - volič nevie tretej strane ani pri dobrovoľnej kooperácii dokázať ako hlasoval;
- **Overiteľnosť (individuálna)** - každý oprávnený volič má možnosť si overiť, či sa jeho hlas podieľal na výsledku hlasovania;
- **Overiteľnosť (univerzálna)** - každý oprávnený volič alebo pozorovateľ má možnosť overiť si, či do výsledku hlasovania boli započítané všetky platné hlasy;
- **Robustnosť** - výsledok hlasovania s daným volebným systémom nie je možné ovplyvniť malým počtom neplatných hlasov alebo neštandardným správaním malej skupiny voličov;
- **Spôsobilosť** - do výsledku hlasovania sú započítané iba platné hlasy oprávnených voličov. Každý oprávnený volič do výsledku volieb prispeje iba jedným hlasovaním. Hlasy všetkých voličov sú si rovné.

V praxi sa realizácia niektorých z požiadaviek ukazuje ako problematická:

- **individuálna overiteľnosť** - zabezpečenie požiadavky na individuálnu overiteľnosť znamená poskytnutie dostatočného množstva dôveryhodných informácií o spracovaní hlasu voliča pre každého z voličov. Volič tak disponuje informáciami, ktorými vie dôveryhodne preukázať, akým spôsobom hlasoval, čo je v priamom rozpore s požiadavkou na nepreukázateľnosť.
- **univerzálna overiteľnosť** - zabezpečenie požiadavky na univerzálnu overiteľnosť znamená poskytnutie dostatočného množstva dôveryhodných informácií o spracovaní všetkých hlasov každému z voličov. Potenciálny útočník tak v prípade identifikácie hlasu konkrétneho voliča disponuje informáciami, z ktorých vie určiť akým spôsobom volič hlasoval, čo je v priamom rozpore s požiadavkami na anonymitu a nepreukázateľnosť.

Vzhľadom na zjavné konflikty niektorých požiadaviek nám v súčasnosti nie je známy žiadny volebný systém spĺňajúci všetky požiadavky, ktoré sú na ideálny volebný systém kladené. Ukazuje sa však, že v praxi nemajú všetky požiadavky rovnakú prioritu a pre zachovanie dôveryhodnosti systému je postačujúce niektoré požiadavky na volebné systémy úplne alebo čiastočne nahradiť požiadavkou na dôveryhodnú autoritu, ktorá zabezpečí slobodné demokratické voľby aj pri použití volebného systému, ktorý nie je ideálny.

V zmysle predchádzajúcich definícií definujeme **ideálny volebný systém s dôveryhodnou autoritou** ako volebný systém spĺňajúci nasledujúce požiadavky:

- Anonymita
- Férovosť
- Integrita
- Kompletnosť
- Nepreukázateľnosť
- Spôsobilosť

Robustnosť, individuálna a univerzálna overiteľnosť sú nahradené zárukou dôveryhodnej autority - volebnej komisie, ktorá sa podieľa na organizovaní volieb. Volebná komisia v rámci svojej záruky garantuje každému voličovi, že jeho platný odovzdaný hlas sa bude v prebiehajúcich voľbách podieľať na výsledku hlasovania a žiadna malá skupina hlasov alebo voličov neovplyvní zásadným spôsobom výsledok hlasovania.

Na volebný systém ako každý iný systém taktiež kladieme ďalšie nešpecifické požiadavky:

- **Auditovateľnosť** - volebný systém a jeho implementácia umožňujú priebežné a dodatočné kontroly a analýzy funkčnosti jednotlivých súčastí;
- **Dostupnosť** - systém a jeho implementácia poskytujú možnosť hlasovať všetkým oprávneným voličom;
- **Flexibilita** - volebný systém je možné jednoduchým (napr. modulárnym) spôsobom upraviť pre špecifické potreby rôznych volieb, v ktorých je nasadený alebo je plánované jeho nasadenie;
- **Spoľahlivosť** - bezchybovosť a stabilita systému a najmä jeho implementácie sú dôležitou podmienkou pre získanie a udržanie dôveryhodnosti volieb;
- **Transparentnosť** - volebný systém a jeho implementácia poskytujú otvorené (verejne dostupné) a transparentné informácie o nastavených parametroch, o priebehu hlasovania, spočítavania výsledkov a o bezpečnostných aspektoch hlasovania.

2.1.4 Volebný systém v Slovenskej republike

Voľby do Národnej rady Slovenskej republiky a voľby do Európskeho parlamentu sú v Slovenskej republike realizované prostredníctvom 1 kolového pomerného volebného systému s prahom zvoliteľnosti 5% doplneného o model preferenčných hlasov.

Voľby prezidenta Slovenskej republiky, voľby do mestských a obecných zastupiteľstiev, voľby do vyšších územných celkov a referendá sú v Slovenskej republike realizované pluralitného (relatívneho väčšinového) volebného systému s 1-2 kolami.

Priebeh hlasovania vo voľbách v Slovenskej republike

Napriek používaniu rozdielnych volebných systémov pri jednotlivých voľbách je realizácia volieb v Slovenskej republike jednotná a jednotlivé voľby sa odlišujú iba v spôsobe úpravy hlasovacích lístkov a vyhodnotenia výsledkov volieb.

Priebeh hlasovania vo voľbách v Slovenskej republike:

- Volič vstúpi do volebnej miestnosti a identifikuje sa volebnej komisií prostredníctvom občianskeho preukazu alebo pasu.

- Člen volebnej komisie overí platnosť identifikačného dokladu, v zozname oprávnených voličov overí či je volič oprávnený pristúpiť k hlasovaniu⁴, zaznačí jeho prítomnosť na hlasovaní a odovzdá voličovi príslušný hlasovací lístok s obálkou.
- Volič skontroluje úplnosť a pravosť hlasovacieho lístka i obálky a následne sa odoberie na miesto určené pre úpravu hlasovacích lístkov.
- Volič určeným spôsobom upraví hlasovací lístok, vloží hlasovací lístok do obálky a obálku uzatvorí.
- Volič vhodí obálku so svojim hlasovacím lístkom do volebnej urny a odoberie sa z volebnej miestnosti.
- Po uzatvorení volebných miestností vyberú členovia volebnej komisie z volebnej urny obálky s hlasovacími lístkami, jednotlivé obálky otvoria a spočítajú platné hlasy.
- Členovia volebnej komisie vytvoria a podpíšu volebnú zápisnicu obsahujúcu oficiálne výsledky volieb, predseda volebnej komisie vyhlási výsledky a odovzdá volebnú zápisnicu príslušným orgánom.

V súčasnosti je pri všetkých voľbách do verejnej správy s výnimkou volieb do Národnej rady Slovenskej republiky umožnené hlasovanie iba vhadením obálky s papierovým hlasovacím lístkom do volebnej urny. Vo voľbách do Národnej rady Slovenskej republiky je umožnené voličom nachádzajúcim sa v čase konania volieb mimo územia Slovenskej republiky odovzdať hlasovací lístok prostredníctvom pošty.

Vlastnosti volieb v Slovenskej republike

Súčasná realizácia „klasických papierových“ volieb v Slovenskej republike za predpokladu zabezpečenia dôveryhodnosti volebnej komisie spĺňa vlastnosti *ideálneho volebného systému s dôveryhodnou autoritou s výnimkou nepreukázateľnosti*⁵. Dôveryhodnosť volebnej komisie by mala byť dosiahnutá výberom členov komisie z volebných tímov kandidátov, v ktorých záujme je kontrola priebehu volieb a práce ostatných členov volebnej komisie, avšak v praxi sa objavujú prípady neplnenia si povinností zo strany niektorých členov volebnej komisie, ktoré znižujú dôveryhodnosť volieb a umožňujú úspešnú a neodhaliteľnú manipuláciu s výsledkami

⁴prípadne overí platnosť predloženého voličského preukazu

⁵Volič sa môže rozhodnúť prezradiť svoj hlas počas hlasovania umožnením dohľadu tretej strany pri hlasovaní formou pošty alebo označením a vynesení nepoužitých hlasovacích lístkov z volebnej miestnosti.

volieb. Z uvedeného dôvodu je vhodné pri implementácii volebného systému minimalizovať úlohu volebnej komisie.

V súvislosti s reštrukturalizáciou verejných financií, vznikom nových politických strán a klesajúcim záujmom občanov o účasť vo voľbách sa aj v Slovenskej republike začína prejavovať politická vôľa nahradiť drahé papierové voľby⁶ elektronickými voľbami cez internet. V nasledujúcich kapitolách sa zameriame na existujúce riešenia elektronických volieb vo svete, návrhu a implementácii nového volebného protokolu pre elektronické voľby pre menšie spoločenstvá. Štúdií uskutočniteľnosti elektronických volieb v Slovenskej republike sa venuje vo svojej diplomovej práci Juraj Danko [Dan12].

⁶Pre predčasné voľby do Národnej rady Slovenskej republiky boli v roku 2012 uvoľnené a v rozpočtovej kapitole Ministerstva vnútra Slovenskej republiky vyhradené prostriedky vo výške približne 8,6 mil. eur na pokrytie nákladov spojených s náhradami miezd členov volebnej komisie, tlačou a distribúciou hlasovacích lístkov, úpravou a zabezpečením volebných miestností. Ďalších približne 1,5 mil. eur bolo vyhradených v rozpočtovej kapitole Štatistického úradu Slovenskej republiky na úhradu nákladov spojených so spracovaním výsledkov volieb.[rep]

Kapitola 3

Elektronické voľby

Voľby, na ktorých čiastočnú alebo úplnú realizáciu sú použité elektronické systémy, nazývame **elektronické voľby** (skrátene e-voľby)¹. V súčasnosti² sú voľby v Slovenskej republike i vo svete realizované prevažne papierovým hlasovaním. V kontexte informatizácie spoločnosti sa však niektoré štáty rozhodli pre čiastočnú alebo úplnú elektronizáciu hlasovania. V tejto kapitole popíšeme úroveň elektronizácie volieb a uvedieme vybrané príklady realizácie elektronických volieb zo sveta, na ktoré sa budeme v priebehu diplomovej práce ďalej odvolávať. **Volebným protokolom** budeme označovať súhrn pravidiel a postupov určujúcich činnosť realizácie elektronických volieb. Pre potreby tejto diplomovej práce budeme využívať volebnú terminológiu platnú pre voľby v Slovenskej republike. Definície základných pojmov uvádzame v kapitole 1 (Slovník pojmov). V prípade príkladov zo zahraničia nahradíme špecifické pojmy a názvy ich ekvivalentnými slovenskými výrazmi a pomenovaniami.

3.1 Úroveň elektronizácie volieb

V nasledujúcej časti definujeme 5 úrovní elektronizácie volieb. Úroveň elektronizácie definujeme na základe postupnosti elektronizácie jednotlivých volebných procesov, pričom predpokladáme, že každý elektronický systém zabezpečujúci niektorý z volebných procesov má analógové (papierové) a/alebo digitálne (elektronické) vstupy a striktné digitálny výstup³. Tento pomerne silný predpoklad zavádzame pre zjednodušenie popisu možností elektronizácie volieb. V praxi existujú príklady elektronických systémov realizujúcich niektorý z volebných procesov

¹Verejnou súčasťou pojmu elektronické voľby zvyčajne používa pre pomenovanie elektronickej realizácie volebného aktu namiesto „papierového“ hlasovania. Naša definícia elektronických volieb je širšia a pokrýva viaceré úrovne použitia elektronických systémov pri realizácii volieb (viď. časť 3.1)

²máj 2012

³Nižšie úrovne sú teda vlastnými podmnožinami vyšších úrovní elektronizácie.

s analógovým výstupom, avšak nepovažujeme ich za vhodné z pohľadu dosiahnutia úrovne úplnej elektronizácie volieb vzhľadom na možnosti zabezpečenia integrity a autenticity papierových dokumentov, preto sa nimi nebudeme v našej práci zaoberať.

Voľby bez elektronizácie

Klasické „papierové“ voľby bez využitia elektronických systémov budeme považovať za východiskovú úroveň pre zavádzanie elektronických volieb a zodpovedá aktuálnemu stavu volieb v Slovenskej republike. Volič sa fyzicky identifikuje pred volebnou komisiou, vyplní papierový hlasovací lístok a vhodí ho do volebnej urny. Volebná komisia po uzatvorení volebných miestností manuálne spočíta hlasovacie lístky, vytvorí zápisnicu o priebehu volieb a dokumenty odovzdá na ďalšie spracovanie volebnej komisií vyššieho stupňa. Po vytvorení konečnej zápisnice o priebehu volieb Ústrednou volebnou komisiou sú výsledky volieb publikované v celoštátnych médiách a volebné dokumenty odovzdané príslušným orgánom na archiváciu.

Čiastočná elektronizácia volieb - elektronická archivácia

Voľby až do fázy publikovania výsledkov a archivácie volebných dokumentov prebiehajú rovnakým spôsobom ako na predchádzajúcej úrovni. Vo fáze publikácie výsledkov a archivácie volebných dokumentov sú volebné zápisnice a ďalšie dokumenty digitalizované (prevedené do elektronickej podoby) a uschované v elektronických systémoch slúžiacich na publikáciu a archiváciu volebných dokumentov.

- **Výhody** elektronickej archivácie oproti predchádzajúcej úrovni elektronizácie sú dostupnosť, rýchle vyhľadávanie v dokumentoch, menšie požiadavky na skladové priestory a za predpokladu zabezpečenia integrity a autenticity dokumentov aj zvýšená miera ochrany voči manipuláciám s výsledkami volieb po ich archivácii.
- Medzi **nevýhody** patria predĺženie doby ukončovania volieb o čas potrebný na digitalizáciu volebných dokumentov a nutnosť zabezpečenia elektronickeho systému pred narušením integrity alebo autenticity archivovaných dokumentov.

Čiastočná elektronizácia volieb - elektronické spracovanie a archivácia

Elektronické spracovanie hlasovacích lístkov a vytvorenie výsledkov hlasovania prebieha do fázy odovzdania hlasov identicky s predchádzajúcou úrovňou elektronizácie volieb. Fáza manuálneho spracovania hlasovacích lístkov, tzn. manuálneho pretriedenia a spočítania platných hlasov, je nahradená elektronickým systémom zabezpečujúcim spočítanie hlasov a vytvorenie výsledkov v digitálnej podobe, ktoré sú ďalej odovzdané na archiváciu podobne ako v predchádzajúcej úrovni. Elektronické spracovanie hlasov môže byť podľa požiadaviek, dostupných financií a predpokladaného počtu odovzdaných hlasov vykonané v každej volebnej miestnosti pod dohľadom príslušnej volebnej komisie alebo centralizovane pod dohľadom volebnej komisie vyššieho stupňa.

Elektronické spracovanie hlasov skúšobne zaviedla Ruská federácia v prezidentských voľbách 4. marca 2012 vo vybraných volebných miestnostiach. Elektronický systém identifikuje platné hlasovacie lístky, spočíta výsledok volieb pre príslušný volebný okrskok a vytvorí zápisnicu o výsledku volieb, ktorú volebná komisia skontroluje a podpíše.

- Elektronické spracovanie hlasovacích lístkov prináša **výhody** v podobe rýchlosti spracovania hlasovacích lístkov, deterministického rozhodovania o platnosti hlasovacieho lístka a minimalizácie vzniku neúmyselných chýb členov volebnej komisie pri spracovaní hlasov.
- Za **nevýhody** elektronického spracovania hlasov považujeme vysoké jednorázové vstupné náklady na vytvorenie bezpečného elektronického systému a kontrolných mechanizmov, riziká neoprávnenej manipulácie s elektronickým systémom, nesprávneho vyhodnotenia platnosti hlasovacieho lístka a straty dôvery voličov v prípade výskytu chýb v systéme po jeho nasadení.

Čiastočná elektronizácia volieb - elektronický volebný akt, spracovanie a archivácia

Posledná úroveň čiastočnej elektronizácie volieb prináša zavedenie elektronického systému pre uskutočnenie volebného aktu - vytvorenie a odovzdanie hlasovacieho lístka. Volič sa po fyzickej identifikácii odoberie k elektronickému hlasovaciemu zariadeniu, v ktorom pomocou mechanických ovládacích prvkov alebo dotykového ovládania zvolí vybraného kandidáta (alebo skupinu kandidátov). Hlasovacie zariadenie zaznamená hlas voliča a po skončení volieb poskytne výsledok hlasovania na danom zariadení.

Hlasovacie zariadenia (najskôr mechanické, neskôr elektronické) majú v mnohých štátoch sveta dlhoročnú tradíciu. Prvé hlasovacie zariadenie v Spojených štátoch amerických bolo patentované už v roku 1889, prvé elektronické hlasovacie zariadenie bolo použité v roku 1974 v štáte Illinois ⁴.

- Elektronický systém pre vykonanie volebného aktu poskytuje v ideálnom prípade oproti „klasickej“ forme hlasovania mnohé **výhody**: skrátenie času potrebného na odovzdanie hlasu, zníženie počtu neplatných hlasov z dôvodu nesprávneho vyplnenia hlasovacieho lístka, podpora hlasovania pre zdravotne postihnuté osoby, zníženie výdavkov na voľby o náklady na tlač a distribúciu hlasovacích lístkov a s nimi súvisiace zníženie ekologickej záťaže na životné prostredie.
- **Nevýhody** elektronických hlasovacích zariadení sú podobné ako v prípade elektronického spracovania hlasov. V prípade nevhodného návrhu elektronických hlasovacích zariadení alebo nedôslednej implementácie vybraného riešenia sa môžu v systéme objaviť zraniteľnosti s vážnymi dopadmi na bezpečnosť priebehu volieb a výsledku hlasovania v zmysle požiadaviek, ktoré sme na volebný systém kládli v časti 2.1.2, za pomoci niektorých typov útokov z časti 2.1.1. ⁵

Úplná elektronizácia volieb

Úplná elektronizácia volieb poskytuje všetky elektronické služby úrovni čiastočnej elektronizácie a rozširuje ich o elektronickú identifikáciu voliča a možnosť hlasovania mimo volebných miestností. Volič sa pred hlasovaním identifikuje preukázaním vlastníctva identifikačnej karty a/alebo tokenu. Hlasovanie sa v závislosti od zvoleného riešenia uskutoční na určených elektronických hlasovacích zariadeniach vo volebných miestnostiach alebo prostredníctvom volebnej aplikácie na ľubovoľnom elektronickom zariadení voliča spĺňajúcom minimálne požiadavky pre použitie volebnej aplikácie.

Úlohou volebných komisií pri úplných elektronických voľbách je dohľad nad elektronickými systémami zabezpečujúcimi služby uchovávanía a spracovania odovzdaných hlasov a prešetrenie podnetov na neštandardný priebeh volieb.

⁴Historical Timeline - Voting Machines, ProCon.org, <http://votingmachines.procon.org/view.resource.php?resourceID=000273>

⁵V roku 2006 holandská nadácia „Wij vertrouwen stemcomputers niet“ zverejnila výsledky bezpečnostnej analýzy elektronických volebných zariadení použitých v holandských parlamentných voľbách, v ktorých prezentovala úspešný útok na volebné zariadenia umožňujúci získať úplnú a prakticky neodhaliteľnú kontrolu nad výsledkom volieb [RG]. V nasledujúcom roku po strate dôvery verejnosti holandská vláda zakázala použitie elektronických volebných systémov v nasledujúcich voľbách.

Úplné elektronické voľby realizujúce identifikáciu a volebný akt na strane elektronického zariadenia voliča využívajúce na prenos hlasu do volebnej urny celosvetovú počítačovú sieť Internet budeme nazývať „internetové voľby“ (voľby cez Internet, i-voľby).

- **Výhodami** úplných elektronických volieb sú okrem výhod z predchádzajúcej úrovne aj vysoká dostupnosť volieb vrátane možnosti hlasovať zo zahraničia, obmedzenie možnosti manipulácie s hlasmi zo strany volebnej komisie, zníženie počtu volebných komisií a redukcia času potrebného na prípravu elektronických volieb.
- **Nevýhody** úplných elektronických volieb voči „klasickým papierovým“ voľbám sú strata dohľadu nad fázami identifikácie voliča a vykonávania volebného aktu, vyššie riziko úspešného pokusu o ovplyvnenie voliča a v prípade nevhodného návrhu elektronických hlasovacích zariadení alebo nedôslednej implementácie vybraného riešenia zraniteľnosti s vážnymi dopadmi na bezpečnosť priebehu volieb a výsledku hlasovania.

3.2 Volebné schémy pre elektronické voľby

Úvahy o zavedení internetových volieb ako náhrady za papierové voľby v súčasnosti rezonuje v mnohých krajinách, avšak počet štátov, ktoré umožňujú hlasovanie cez Internet na národnej úrovni, nie je veľký z dôvodu problematického zabezpečenia všetkých požiadaviek pre ideálny volebný systém (uvedených v časti 2.1.1). V tejto časti v stručnosti predstavíme existujúce teoretické riešenia elektronických volieb. Predstavíme a podrobnejšie technicky popíšeme tiež vybrané riešenia elektronických volieb použité v Spojených štátoch amerických, Švajčiarsku a v Estónsku.

Volebnou schémou (volebným protokolom) budeme nazývať postupnosť krokov realizujúcich voľby pre vybraný volebný systém. Volebné schémy môžeme na základe použitých kryptografických prvkov deliť do 4 základných skupín:

- **Volebné schémy využívajúce slepé podpisy** sú založené na myšlienke aplikovania schémy pre slepé digitálne podpisy na hlas voliča, čím je zabezpečená anonymita voliča (v zmysle požiadaviek na volebný systém, viď. časť 2.1.2). S použitím niektorých ďalších kryptografických primitív⁶ sú garantované všetky požiadavky s výnimkou nepreukázateľnosti. Použitie schém z tejto skupiny tiež výrazne obmedzuje vyžadovanie viacnásobnej aktívnej účasti voliča. [DRH]

⁶napr. šifrovanie alebo „bit commitment“

- **Volebné schémy využívajúce homomorfné šifrovanie** umožňujú pomocou aplikácie homomorfného šifrovania a vybranej aritmetickej operácie spočítať výsledky volieb bez potreby predchádzajúceho dešifrovania individuálnych hlasov voličov a neposkytujú možnosť dešifrovania čiastkových výsledkov (alebo individuálnych hlasov) len so znalosťou dešifrovacieho kľúča. Integrita a spôsobilosť sú dosiahnuté dokazovaním platnosti hlasu pri jeho odovzdaní formou bezznalostných dôkazov. Nevýhodami volebných schém založených na homomorfnom šifrovaní sú výpočtová zložitosť bezznalostných dôkazov a obmedzenie na jednoduché volebné systémy (hlasovania áno/nie) vzhľadom na spôsob počítavania výsledkov. [DRH]
- **Volebné schémy využívajúce anonymné kanály** zabezpečujú anonymitu vďaka odovzdávaniu hlasov cez komunikačné kanály, ktoré neumožňujú spätnú identifikáciu odosielateľa správy. „Podstatou schém elektronických volieb založených na anonymných kanáloch je zvyčajne sieť serverov a routrov, ktoré premiešavajú zašifrované hlasy, a zároveň poskytujú dôkazy, že pri miešaní žiaden hlas nestratili ani nepozmenili.“ [Dan] Hlavnou nevýhodou zabraňujúcou nasadeniu schém s anonymnými kanálmi sú neefektívnosť a výpočtová zložitosť.
- **Hybridné schémy** Predchádzajúce skupiny volebných schém využívajú kryptografické prostriedky, ktoré im umožňujú splniť mnohé z podmienok na volebné systémy, avšak nevýhody súčasných riešení zabraňujú ich nasadenie v praxi. Hybridné schémy využívajú kombináciu týchto kryptografických prostriedkov alebo ich častí, pričom využívajú ich prínosy a zefektívňujú predchádzajúce protokoly.

Na nasledujúcich stranách uvedieme niekoľko hybridných volebných schém, ktoré boli v praxi implementované a použité na národnej úrovni. Zameriame sa na najdôležitejšie existujúce zraniteľnosti a hrozby pre každú z volebných schém, ktoré môžu ovplyvniť dôveryhodnosť elektronických volieb. Úplné bezpečnostné analýzy uvedených volebných schém nie sú predmetom tejto diplomovej práce, pri každej zo schém uvádzame odkaz na literatúru, ktorá v prípade záujmu čitateľa obsahuje ďalšie informácie.

Prv než pristúpime ku konkrétnym volebným schémam, uvádzame predpoklady na implementáciu a prostredie, v ktorom budú volebné schémy nasadené, spoločné pre všetky volebné schémy:

- Hardvérové komponenty sú spoľahlivé a nedochádza k ich výpadkom;
- Použité kryptografické prostriedky pre šifrovanie, tvorbu elektronických podpisov a schémy na zdieľanie tajomstva sú bezpečné;
- Protokoly HTTPS a SSL sú bezpečné;

- Volebná aplikácia nie je z pohľadu ostatných komponentov považovaná za bezpečnú;
- Každý komponent overuje vstupné dáta a pracuje podľa protokolu.

3.2.1 Projekt SERVE

Secure Electronic Registration and Voting Experiment, skrátene projekt SERVE, bol experimentálny projekt zavedenia elektronického hlasovania v Spojených štátoch amerických (USA) pre členov americkej armády a pracovníkov diplomatických zborov v zahraničí pod vedením Ministerstva obrany USA. Prvé použitie bolo pôvodne plánované pre národné voľby v roku 2004, avšak projekt bol pre odhalenie vážnych bezpečnostných chýb vo februári 2004 zrušený. Pri popise projektu SERVE vychádzame z publikácií [BM07] a [Rub04].

Volebný protokol

Projekt SERVE patril medzi hybridné volebné schémy, anonymita hlasovania bola zabezpečená pomocou asymetrického šifrovania. Volebný protokol tvorili 4 komponenty:

- **Volebná aplikácia** (Voting Application) bola webovou aplikáciou na strane klienta. Vyžadovala podporu skriptovacích jazykov JavaScript a Java alebo ActiveX. Pre zabezpečenie komunikačného kanála v sieti Internet bol použitý protokol SSL, anonymita hlasovania mala byť zabezpečená zašifrovaním odosielaného hlasu verejným kľúčom úložiska hlasov.
- **Sieťový server** (Network Server) bol online server sprostredkujúci komunikáciu medzi volebnou aplikáciou a úložiskom hlasov. Hlavná úloha sieťového servera spočívala v prijatí hlasov a identifikačných údajov z volebných aplikácií a ich preposlaní na úložisko hlasov.
- **Úložisko hlasov** (Votes Storing Server) dešifrovalo prijaté hlasy, overilo platnosť hlasov aj identifikačných údajov voliča a platné hlasy bez identifikačných údajov zašifrovalo verejným kľúčom sčítacieho servera a odovzdalo v zašifrovanej podobe príslušnému sčítaciemu serveru podľa bydliska voliča. V priebehu volieb si server vytváralo zoznam voličov, ktorého úlohou bolo zabrániť viacnásobnému hlasovaniu oprávnených voličov.
- **Sčítací server** (Votes Counting Server) dešifroval prijaté hlasy a spočítal výsledky hlasovania. Pre potreby súbehu elektronických volieb s papierovými voľbami sa mal sčítací server nachádzať v každom volebnom okrsku a pri papierových voľbách poskytovať zoznam voličov, ktorí odvolili elektronicky.

Projekt SERVE sa skladal z troch fáz:

- **Registračná fáza**

1. *Sčítacie servery a úložisko hlasov* generujú páry kľúčov pre asymetrické šifrovanie, súkromné dešifrovacie kľúče sčítacích serverov sú rozdelené na časti medzi *členov volebnej komisie*;
2. Volič sa registruje do projektu SERVE a získa prihlasovacie meno a heslo slúžiace pre autentifikáciu voči *sieťovému serveru* vo volebnej fáze.

- **Volebná fáza**

1. Volič sa cez SSL spojenie pripojí k *sieťovému serveru*, získa *volebnú aplikáciu* a *zoznam kandidátov*;
2. Volič prostredníctvom *volebnej aplikácie* vytvorí hlas v , vygeneruje náhodné číslo r a pomocou *verejného kľúča úložiska hlasov* $PK[s]$ zašifruje hlas v a číslo r ;
3. *Volebná aplikácia* odošle zašifrovaný hlas a identifikačné údaje voliča na *sieťový server*;
4. *Sieťový server* overí korektnosť prijatej správy a prepošle ju na *úložisko hlasov*.

- **Fáza spracovania hlasov**

1. *Úložisko hlasov* prijme dáta zo *sieťového servera*, vygeneruje odpoveď potvrdzujúcu prijatie hlasu a odošle ju späť voličovi;
2. *Úložisko hlasov* ďalej na základe identifikačných údajov zaradí voliča do *zoznamu zúčastnených voličov*, dešifruje hlas voliča pomocou svojho súkromného kľúča, overí jeho platnosť a zašifruje ho *verejným kľúčom príslušného sčítacieho servera* a odošle ho naň;
3. *Sčítací volebný server* po skončení volieb dešifruje prijaté hlasy pomocou svojho súkromného kľúča a spočíta výsledky volieb.

Bezpečnostná analýza

Projekt SERVE v predstavenej podobe obsahuje mnohé bezpečnostné riziká, ktoré zabránili jeho nasadeniu vo voľbách a nakoniec viedli k jeho zrušeniu. Medzi najzávažnejšie hrozby tohto volebného protokolu patrili:

- **Narušenie anonymity hlasovania** – *úložisko hlasov* má vážnu zraniteľnosť: v určitom okamihu obsahuje každý hlas v otvorenej podobe spolu s identifikačnými údajmi voliča. V prípade získania kontroly nad *úložiskom hlasov* má útočník k dispozícii priebežné výsledky spolu s informáciou o voľbe každého z voličov. Druhú zraniteľnosť, ktorú môže útočník využiť pre identifikáciu hlasu voliča, obsahuje *sčítací server*: v prípade úspešného útoku na *sčítací server* má útočník možnosť identifikovať voliča hlasu získaním aktuálnej verzie *zoznamu zúčastnených voličov* po každom prijatom hlase a jeho porovnaním s jeho predchádzajúcou verziou.
- **Manipulácia s hlasmi** – Prvá zraniteľnosť z predchádzajúcej hrozby umožňovala útočníkovi tiež ľubovoľne ovplyvniť výsledok hlasovania bez odhalenia manipulácie s hlasmi.
- **Ovplyvňovanie voličov** – volič má vo voľbách iba jednu možnosť odovzdať platný hlas. Útočník môže ovplyvniť výsledok získaním hlasu voliča nedobrovoľným alebo dobrovoľným spôsobom (kúpením).

3.2.2 Švajčiarsky volebný protokol

Švajčiarsko vytvorilo hybridnú volebnú schému založenú na podobných kryptografických prostriedkoch ako projekt SERVE. Príprava elektronických volieb začala v roku 2000 a prvé pilotné testovania prebiehali od roku 2003 v kantónoch Ženeva, Neuchâtel a Bazilej. V súčasnosti bol volebný protokol rozšírený aj do zvyšných kantónov.

Volebný protokol

Pri popise volebného protokolu budeme vychádzať z oficiálneho dokumentu samosprávy ženevského kantónu [oG]. Švajčiarsky volebný protokol sa skladá z 3 komponentov:

- **Volebnú aplikáciu** tvorí webová aplikácia na strane klienta využívajúca Java applety. Pre zabezpečenie komunikačného kanála v sieti Internet bol použitý protokol SSL s obojstrannou autentifikáciou a dodatočné symetrické šifrovanie kľúčom získaným pomocou Diffie-Hellmanovej schémy na výmenu kľúčov.

- **Sieťový server** poskytuje zabezpečené prepojenie *volebnej aplikácie s úložiskom hlasov*. *Sieťový server* identifikuje prijaté dáta, overuje platnosť prijatého hlasu a preposiela platné hlasy *úložisku hlasov*.
- **Úložisko hlasov** pred zahájením volieb vytvára voličské karty, uchováva prijaté hlasy v priebehu volieb a po skončení hlasovania dešifruje prijaté hlasy a spočíta výsledky hlasovania.

Švajčiarsky volebný protokol podobne ako projekt SERVE prechádza v priebehu volieb 3 fázami:

- **Registračná fáza**

1. *Úložisko hlasov* generuje pár kľúčov pre asymetrické šifrovanie, súkromný dešifrovací kľúč sčítacieho servera je rozdelený medzi *členov volebnej komisie*;
2. *Úložisko hlasov* vygeneruje voličské karty v počte zhodnom s počtom oprávnených voličov. Voličská karta umožňuje voličovi odovzdať 1 platný hlas vo volebnej miestnosti (volič odovzdá kartu volebnej komisii), prostredníctvom pošty (volič vyplní kartu a pripojí ju k hlasu) alebo prostredníctvom elektronického hlasovania. Pre potreby elektronického hlasovania voličská karta obsahuje identifikačné číslo voličskej karty, kontrolný kód a fyzicky utajený pin kód karty;
3. Voličské karty sú distribuované oprávneným voličom prostredníctvom pošty.

- **Volebná fáza**

1. Volič sa cez SSL spojenie doplnené o *symetrické šifrovanie* pomocou kľúča získaného *Diffie-Hellmanovou schémou* pripojí k *sieťovému serveru*, získa *volebnú aplikáciu* a zoznam kandidátov;
2. Volič prostredníctvom *volebnej aplikácie* vytvorí svoj hlas a odošle ho na *sieťový server*;
3. *Sieťový server* overí korektnosť prijatej správy, platnosť hlasu a na základe čísla voličskej karty vráti *volebnej aplikácii* potvrdenie o hlasovaní spolu s kontrolným kódom;
4. Volič overí zhodu prijatého kontrolného kódu s kódom uvedeným na voličskej karte a v prípade zhody pokračuje v protokole odoslaním svojho dátumu narodenia, príslušného volebného okrsku a pin kódu voličskej karty na *sieťový server*;
5. *Sieťový server* overí prijaté dáta a oprávnenosť voliča k voľbe voči zoznamu použitých voličských kariet. V prípade úspešných kontrol *sieťový server* zašifruje hlas voliča, jeho volebný okrsek a náhodne vygenerovaný reťazec pomocou *verejného kľúča úložiska hlasov*;

6. *Sieťový server* následne vykoná atomicky nasledujúce operácie: zašifrovaný hlas odovzdá *úložisku hlasov* a zapíše číslo voličskej karty do *zoznamu použitých voličských kariet*.

- **Fáza spracovania hlasov**

1. *Úložisko hlasov* prijme dáta zo *sieťového servera* a uchová ich pre spracovanie po skončení volieb;
2. Po skončení volieb *úložisko hlasov* premieša prijaté hlasy, dešifruje ich pomocou svojho súkromného kľúča a spočíta výsledky volieb.

Bezpečnostná analýza

Švajčiarsky volebný protokol spĺňa väčšinu požiadaviek na volebné systémy: integrita, kompletnosť, individuálna overiteľnosť, robustnosť i spôsobilosť priamo vyplývajú z popísaného protokolu. Napriek doterajším úspešným skúsenostiam s protokolom vo Švajčiarsku obsahuje protokol niekoľko zraniteľností:

- **Hlas v čitateľnej podobe spolu s číslom voličskej karty** na sieťovom serveri v okamihu spracovania prijatého hlasu. V prípade úspešného útoku na sieťový server môže útočník postupne vytvárať zoznam platných hlasov, čím bude narušená férovosť volebného systému. V prípade dodatočnej znalosti zoznamu voličov s číslami pridelených voličských kariet je útočník schopný spojiť prijaté platné hlasy s identitou voličov, čím dôjde k nenaplneniu požiadavky na anonymitu hlasovania. Riziko prezradenia zoznamu voličov s pridelenými voličskými kartami je minimalizované v registračnej fáze protokolu utajením zoznamu.
- **Jednorazové použitie voličských kariet.** Volič má k dispozícii práve jednu možnosť odovzdať svoj hlas. Táto vlastnosť protokolu umožňuje útočníkovi prinútiť voliča odovzdať platný hlas podľa vôle útočníka či už pod jeho dohľadom alebo za predpokladu získania údajov od voliča i v jeho neprítomnosti bez odhalenia. Závažnosť dopadu zneužitia tejto zraniteľnosti závisí od úrovne korupcie v krajine, v ktorej elektronické voľby prebiehajú.
- **Distribúcia voličských kariet poštou.** Pošta ako nespoľahlivá doručovacia služba umožňuje odchytenie voličských kariet pred ich prevzatím skutočným adresátom. Za predpokladu útočnickej znalosti základných informácií o pôvodných adresátoch a nezaujmu oprávneného voliča o ľubovoľný typ hlasovania môže útočník využiť voličskú kartu na viacnásobné hlasovanie vo svoj prospech.

3.2.3 Estónsky volebný protokol

Estónsko sa stalo prvým štátom, ktorý od roku 2005 umožňuje národné hlasovanie elektronicky prostredníctvom Internetu. Základné kroky smerujúce k elektronickým voľbám začalo Estónsko robiť už v roku 2000, v ktorom bol prijatý zákon o digitalnom podpise. V roku 2002 bola vytvorená národná PKI infraštruktúra a začali sa vydávať prvé identifikačné karty s kryptografickým čipom umožňujúce vytvárať elektronický podpis. V lete 2003 zahájila Národná volebná komisia projekt elektronického hlasovania, ktorého výsledkom bolo pilotné testovanie v januári 2005 a následné úspešné nasadenie systému vo voľbách do samospráv v roku 2005 a do parlamentu v roku 2007.

Volebný protokol

Základným kameňom nielen elektronického hlasovania sa stala identifikačná karta občana⁷ s kryptografickým čipom podporujúcim algoritmy RSA a 3DES. Karta je chránená PIN kódom podobne ako SIM karta mobilných operátorov. Pre prácu s identifikačnou kartou je potrebné vlastniť čítačku elektronických kariet a softvér pre tvorbu elektronického podpisu.

Pri popise a analýze estónskeho volebného protokolu vychádzame najmä z dokumentov estónskej Národnej volebnej komisie⁸ [Com], [AA] a z práce T. Mägi [BM07]. Estónsky volebný protokol je postavený na 5 komponentoch:

- **Volebnú aplikáciu** tvorí webová aplikácia s využitím technológie ActiveX. Bezpečnosť komunikácie so *sieťovým serverom* je realizovaná prostredníctvom šifrovania a autentifikácie zabudovaných v protokole SSL. Volebná aplikácia zabezpečuje vytvorenie hlasu a jeho vloženie do 2 ochranných vrstiev (tzv. obálok) popísaných nižšie;
- **Sieťový server** sprostredkuje komunikáciu medzi *volebnou aplikáciou* (voličom) a *úložiskom hlasov* (volebnou infraštruktúrou). Hlavnou úlohou sieťového servera sú autentifikácia, distribúcia zoznamov volebných kandidátov, základná kontrola a transfer hlasov na *úložisko hlasov*;
- **Úložisko hlasov** slúži ako elektronická volebná urna. Uchováva prijaté elektronické hlasy voličov až do doby ukončenia hlasovania, má na starosti prvotné spracovanie hlasov a odstraňovanie neplatných hlasov;

⁷ekvivalent občianskeho preukazu v Slovenskej republike

⁸ekvivalent Ústrednej volebnej komisie v Slovenskej republike

- **Sčítací server** po skončení elektronického hlasovania spracováva prijaté platné hlasy a na ich základe vytvára výsledok elektronických volieb. Vzhľadom na to, že sčítací server nie je z bezpečnostných dôvodov pripojený do žiadnej počítačovej siete, prebieha transfer hlasov z *úložiska hlasov* pomocou fyzických dátových médií;
- **Certifikačná autorita** poskytuje infraštruktúru pre elektronický podpis. Ostatným komponentom poskytuje služby potrebné pre overenie platnosti elektronického podpisu (zoznam zrušených certifikátov, služba časovej pečiatky).

Hlasovať cez Internet je v Estónsku možné už približne týždeň pred otvorením volebných miestností, pričom volič má v estónskom volebnom protokole možnosť elektronicky hlasovať až do ich definitívneho uzatvorenia na konci volebného dňa. Svoj hlas môže kedykoľvek v rámci obdobia volieb nahradiť novým elektronickým hlasom prípadne navštíviť volebnú miestnosť v deň volieb a odhlasovať klasickým papierovým spôsobom - všetky staršie hlasovacie lístky sú anulované.

Rovnako ako predchádzajúce protokoly, aj estónsky protokol môžeme rozdeliť do troch fáz. Na rozdiel od predchádzajúcich protokolov registrácia voliča alebo distribúcia voličských kariet nie sú vzhľadom na existenciu infraštruktúry pre elektronické podpisy potrebné, preto *registračnú fázu* nahradíme *prípravnou*:

- **Prípravná fáza**

1. Volebná komisia vygeneruje pár kľúčov pre asymetrické šifrovanie hlasov, verejný šifrovací kľúč zverejní prostredníctvom *sieťového servera* a súkromný dešifrovací kľúč rozdelí podľa niektorej z kryptografických schém na *zdieľanie tajomstva* medzi členov volebnej komisie;
2. Na *sieťový server* je nahraná digitálne podpísaná volebná aplikácia platná pre pripravované elektronické voľby spolu so zoznamom kandidátov;
3. *Úložisko hlasov* získa zoznam oprávnených voličov z Registra obyvateľov;
4. Volič si overí platnosť svojej identifikačnej karty a zabezpečí si čítačku elektronických čipových kariet.

- **Volebná fáza**

1. Volič sa pripojí prostredníctvom protokolu HTTPS k *sieťovému serveru*, overí autenticitu *sieťového servera* a autentifikuje sa s použitím svojej identifikačnej karty;
2. *Sieťový server* odošle volebnú aplikáciu voličovi;

3. *Sieťový server* overí autentickosť a oprávnenosť voliča v Registri obyvateľov. Ak je výsledok pozitívny, *sieťový server* prostredníctvom *úložiska hlasov* overí počet odovzdaných hlasov voliča, inak spojenie ukončí. V prípade nenulového počtu hlasov informuje voliča o možnosti zmeny existujúceho hlasu;
4. Volič označí vo *volebnej aplikácii* svojho vybraného kandidáta;
5. *Volebná aplikácia* vytvorí hlas na základe výberu voliča a zašifruje ho spolu s náhodne vygenerovaným číslom pomocou *verejného kľúča pre asymetrické šifrovanie hlasov*, čím je vytvorená tzv. „prvá obálka“;
6. Volič vo *volebnej aplikácii* elektronicky podpíše zašifrovaný hlas. Zašifrovaný hlas spolu s elektronickým podpisom voliča tvoria tzv. „druhú obálku“;
7. *Volebná aplikácia* odošle hlas v „2. obálke“ na *sieťový server*;
8. *Sieťový server* overí, či identita voliča uvedená v digitálnom podpise hlasu sa zhoduje s identitou uvedenou pri vytváraní spojenia v úvode volebnej fázy. V prípade negatívneho výsledku ukončí spojenie;
9. *Sieťový server* prepošle hlas na *úložisko hlasov*;
10. *Úložisko hlasov* v spolupráci s *certifikačnou autoritou* overí platnosť elektronického podpisu. Ak je elektronický podpis platný, vytvorí *odpoveď* o prijatí hlasu pre voliča, inak ukončí spojenie;
11. *Úložisko hlasov* odošle *volebnej aplikácii* *odpoveď* o prijatí hlasu prostredníctvom *sieťového servera* a uloží hlas na ďalšie spracovanie po skončení hlasovania.

• **Fáza spracovania hlasov**

1. Po skončení elektronického hlasovania *úložisko hlasov* odstráni duplicitné hlasy pre každého voliča, ponechaný je iba najnovší hlas voliča;
2. *Úložisko hlasov* pre každý platný hlas overí výskyt voliča v zozname oprávnených voličov a odstráni hlasy bez záznamu v tomto registri;
3. Zostávajúce hlasy na *úložisku hlasov* sú anonymizované odstránením „2. obálky“ (elektronického podpisu);
4. Anonymizované hlasy sú nahrané na fyzické dátové médium a prenesené na **sčítací server**;
5. Členovia volebnej komisie vyskladajú *súkromný dešifrovací kľúč* a dešifrujú nahrané anonymizované hlasy;
6. *Sčítací server* spočíta platné hlasy a zverejní výsledok. V prípade súbehu elektronických volieb s papierovými voľbami sú výsledky spolu so zoznamom zúčastnených voličov odoslané príslušnej volebnej komisii.

Bezpečnostná analýza

Estónsky volebný protokol spĺňa v popísanej podobe všetky upravené požiadavky na volebný systém pre realizáciu pilotného projektu uvedené v časti 2.1.2 s výnimkou férovosti. V rámci stručnej analýzy uvádzame najzávažnejšie hrozby estónskeho volebného protokolu:

- **Kompromitácia certifikačnej authority** – volebný protokol predpokladá bezpečnosť elektronického podpisu a certifikačnej authority pre vydávanie certifikátov na tvorbu elektronických podpisov. Kompromitácia certifikačnej authority poskytuje útočníkovi možnosť významným spôsobom ovplyvniť výsledky volieb zneplatnením existujúcich alebo vydávaním nových certifikátov pre tvorbu elektronického podpisu. Prelomenie schémy pre elektronický podpis umožňuje útočníkovi bez odhalenia odovzdávať platné hlasy v mene iných voličov alebo nahrádzať hlasy uložené na *úložisku hlasov* za hlasy pre kandidátov podľa svojho výberu.
- **Zásah do prenosu hlasov z úložiska hlasov na sčítací server** – prenos platných zašifrovaných hlasov prebieha na fyzických médiách, pri ktorých hrozí výmena originálnych médií za médiá s hlasmi útočníka. Členovia volebnej komisie v estónskom volebnom protokole minimalizujú riziko naplnenia tejto hrozby zabezpečením integrity a autenticity uložených dát pomocou elektronického podpisu a fyzického zabezpečenia médií.
- **Manipulácia s odovzdanými hlasmi** – útočník môže získaním kontroly nad *úložiskom hlasov* a/alebo *sieťovým serverom*.
- **Tvorba zoznamu zúčastnených voličov – Férovosť** môže byť v estónskom volebnom protokole narušená útokom na *sieťový server* alebo *úložisko hlasov*. V prípade získania kontroly nad niektorým z uvedených komponentov volebného protokolu môže útočník bez ovplyvnenia činnosti komponentu získať informácie o identitách niektorých alebo všetkých voličov, ktorí sa už zúčastnili na elektronickom hlasovaní. Takto vytvorený zoznam zúčastnených voličov môže útočník využiť na ovplyvňovanie a korupciu voličov⁹. Estónsky protokol predpokladá organizačné zabezpečenie komponentov na strane organizátora volieb a zaznamenávanie neštandardného správania, avšak tieto opatrenia nepovažujeme za dostatočné vzhľadom na dĺžku volebnej fázy (v Estónsku až 30 dní), potenciálne zlyhania ľudského faktora (korupcia správcov komponentov) a zraniteľnosti na úrovni operačných systémov komponentov prepojených s externou počítačovou sieťou.

⁹Na základe kontroly zoznamu môže útočník vytipovať nerozhodnutých voličov a/alebo kontrolovať, či volič po odovzdaní dohodnutého hlasu neodovzdal ďalší platný hlas, ktorým platnosť pôvodného zrušil.

3.2.4 Nórsky volebný protokol

Nórske ministerstvo pre miestnu samosprávu a regionálny rozvoj zahájilo v roku 2008 projekt elektronických volieb v Nórsku. Výsledkom projektu bol pilotný projekt použitý vo voľbách do samospráv v roku 2011.

Volebný protokol

Nórsky volebný protokol je v mnohých častiach podobný estónskemu protokolu. Využíva prostriedky pre elektronický podpis, komunikačné kanály zabezpečené protokolom SSL a umožňuje voličovi meniť svoj hlas v priebehu volieb. Pre naše potreby uvádzame nórsky volebný protokol v zjednodušenej podobe, úplnú verziu protokolu môže čitateľ nájsť v [Gjo10] a [fDIR], z ktorých sme pri tvorbe popisu vychádzali.

Komponenty nórskeho volebného protokolu:

- **Volebná aplikácia** architektúrou a funkcionalitou analogická volebnej aplikácii pre estónsky protokol;
- **Identifikačný portál** verejnej správy je náhradou za infraštruktúru pre elektronický podpis, ktorú má Estónsko a slúži na autentifikáciu občana voči orgánom verejnej správy za pomoci prihlasovacieho mena a hesla;
- **Úložisko hlasov** overuje platnosť prijatých hlasov, ukladá ich na ďalšie spracovanie a čiastočne sa podieľa na tvorbe odpovede pre voliča;
- **Generátor odpovedí** vytvára odpovedné kódy pre každý odovzdaný platný hlas. Výsledné odpovedné kódy posiela voličom vo forme krátkej textovej správy (SMS);
- **Anonymizačné servery** odstraňujú duplikáty hlasov, anonymizujú a premiešavajú hlasy;
- **Sčítací server** pracuje analogicky ako sčítací server estónskeho volebného protokolu.
- **Prípravná fáza**
 1. Volebná komisia vygeneruje pár kľúčov pre asymetrické šifrovanie hlasov, verejný šifrovací kľúč zverejní prostredníctvom *úložiska hlasov* a súkromný dešifrovací kľúč rozdelí podľa niektorej z kryptografických *schém na zdieľanie tajomstva* medzi členov volebnej komisie;

2. Volebná komisia vygeneruje a rozdistribuuje kryptografické kľúče na tvorbu odpovedí¹⁰. Spolu s kľúčami sú pre každého voliča vygenerované karty s očakávanými odpoveďami obsahujúce pre každého kandidáta jedinečný kód, ktorý musí *generátor odpovedí* pri odovzdaní hlasu vygenerovať a doručiť voličovi;
3. Karty s očakávanými odpoveďami sú voličom odoslané prostredníctvom pošty pred zahájením volieb;
4. Na *úložisko hlasov* je nahraná digitálne podpísaná volebná aplikácia platná pre pripravované elektronické voľby spolu so zoznamom kandidátov;
5. *Úložisko hlasov* získa zoznam oprávnených voličov z Registra obyvateľov.

- **Volebná fáza**

1. Volič sa pripojí prostredníctvom protokolu HTTPS k *identifikačnému portálu* a autentifikuje sa s použitím svojho prihlasovacieho mena a hesla určeného pre prístup k vládnym elektronickým systémom;
2. *Úložisko hlasov* odošle volebnú aplikáciu voličovi;
3. *Identifikačný portál* overí autentickosť a oprávnenosť voliča v Registri obyvateľov;
4. Volič označí vo *volebnej aplikácii* svojho vybraného kandidáta;
5. *Volebná aplikácia* vytvorí hlas na základe výberu voliča a zašifruje ho spolu s náhodne vygenerovaným číslom pomocou *verejného kľúča pre asymetrické šifrovanie hlasov*, čím je vytvorená tzv. „prvá obálka“;
6. *Volebná aplikácia* v spolupráci s *identifikačným portálom* elektronicky podpíše zašifrovaný hlas v mene voliča. Zašifrovaný hlas spolu s elektronickým podpisom voliča tvoria tzv. „druhú obálku“;
7. *Volebná aplikácia* odošle hlas v „2. obálke“ na *úložisko hlasov*;
8. *Úložisko hlasov* v spolupráci s *certifikačnou autoritou* overí platnosť elektronického podpisu. Ak je elektronický podpis platný, vytvorí *čiasťočnú odpoveď* o prijatí hlasu pre voliča, inak ukončí spojenie;
9. *Úložisko hlasov* odošle *generátoru odpovedí* *čiasťočnú odpoveď* o prijatí hlasu a uloží hlas na ďalšie spracovanie po skončení hlasovania;
10. *Generátor odpovedí* ukončí proces generovania odpovedného kódu a výsledný kód odošle prostredníctvom SMS voličovi;

¹⁰Podrobnosti o generovaní odpovedí pre voliča a zodpovedajúcej práce obsahuje kapitola 3 dokumentu [Gjo10]

11. Volič overí prijatý odpovedný kód voči zoznamu platných odpovedných kódov v závislosti od výberu svojho kandidáta. Ak sa kódy nezhodujú alebo volič dostane kód aj v neočakávanom prípade, podá sťažnosť na volebnú komisiu.

- **Fáza spracovania hlasov**

1. Po skončení elektronického hlasovania *úložisko hlasov* odošle uložené hlasy na *anonymizačné servery*;
2. *Anonymizačné servery* odstránia duplicitné hlasy pre každého voliča, ponechaný je iba najnovší hlas voliča;
3. *Anonymizačné servery* pre každý platný hlas overia výskyt voliča v zozname oprávnených voličov a odstránia hlasy bez záznamu v tomto registri;
4. Zostávajúce hlasy na *anonymizačných serveroch* sú anonymizované odstránením „2. obálky“ (elektronického podpisu);
5. Anonymizované hlasy sú prenesené na **sčítací server**;
6. Členovia volebnej komisie vyskladajú *súkromný dešifrovací kľúč* a dešifrujú nahrané anonymizované hlasy;
7. *Sčítací server* spočíta platné hlasy a zverejní výsledok. V prípade súbehu elektronických volieb s papierovými voľbami sú výsledky spolu so zoznamom zúčastnených voličov odoslané príslušnej volebnej komisii.

Bezpečnostná analýza

Nórsky volebný protokol má vzhľadom na podobnosť s estónskym volebným protokolom podobné vlastnosti.

- Na rozdiel od estónskeho protokolu prináša **čiasťnú individuálnu overiteľnosť** - volič má možnosť overiť si, či bol jeho hlas uložený na *úložisko hlasov* pomocou odpovedných kódov. Nepreukázateľnosť je zachovaná - volič nevie dokázať, či sa jeho hlas uložený na *úložisku hlasov* podieľal na výsledku hlasovania.
- **Zabezpečenie poštového a SMS kanála** sú dôležitým predpokladom pre realizáciu volebného protokolu. Napadnutím niektorého z uvedených komunikačných kanálov môže útočník v priebehu volebnej fázy získať informácie o výbere voliča pri hlasovaní (znalosť odpovedných kódov doručovaných poštou) alebo ovplyvniť priebeh hlasovania úpravou odpovedných kódov z *generátora hlasov* (kompromitácia SMS komunikačného kanála).

- **Kompromitácia identifikačného servera** – volebný protokol predpokladá bezpečnosť elektronického podpisu a identifikačného servera. Volič sa na *identifikačný server* prihlasuje pomocou prihlasovacieho mena a hesla. Tento spôsob identifikácie na rozdiel od estónskeho protokolu nevyžaduje od voliča fyzický prístup k niektorému z bezpečnostných prvkov - útočník potrebuje pre úspešný útok poznať iba prihlasovacie údaje. Kompromitácia identifikačného servera poskytuje útočníkovi rovnaké možnosti ovplyvniť voľby ako kompromitácia certifikačnej autority v estónskom protokole.
- **Tvorba zoznamu zúčastnených voličov** – **Férovosť** môže byť v nórskom volebnom protokole narušená útokom na *úložisko hlasov* rovnako ako v prípade estónskeho volebného protokolu.

V ďalších častiach diplomovej práce budeme pod pojmom elektronické voľby uvažovať internetové voľby na úrovni úplnej elektronizácie volieb, pričom budeme tieto pojmy v texte voľne zamieňať.

Pre potreby tejto diplomovej práce sa v ďalšej časti práce vzhľadom na jej cieľ (potenciálne nasadenie vybraného riešenia vo voľbách v Slovenskej republike) zameriame na skupinu hybridných volebných schém, ktorej volebné schémy boli úspešne implementované vo viacerých krajinách sveta. Príkladmi volebných schém pre ostatné skupiny ako i podrobnejšou analýzou jednotlivých volebných schém sa vo svojich prácach zaoberajú okrem iných aj J. Danko [Dan] a R. Henni, E. Dubuis a U. Ultes-Nitsche[DRH].

Kapitola 4

Návrh volebného protokolu

V predchádzajúcich kapitolách sme sa zaoberali voľbami vo všeobecnosti, možnosťami elektronizácie volieb, typmi volebných schém (protokolov) a vybranými realizovanými volebnými protokolmi, ktoré mali vplyv na elektronizáciu volieb vo svete. Avšak každé z uvedených riešení elektronických volieb obsahuje zraniteľnosti, ktoré môže potenciálny útočník využiť vo svoj prospech. Pre dosiahnutie cieľov vytýčených pre túto diplomovú prácu sme sa rozhodli navrhnúť nový volebný protokol, ktorý ošetruje niektoré z týchto zraniteľností. Pri návrhu protokolu budeme vychádzať z úspešných návrhov estónskeho a nórskeho volebného protokolu.

Pre potreby nášho volebného protokolu pre realizáciu úplných elektronických volieb budeme uvažovať pluralitný volebný systém typu 1:K¹ realizovaný v jednom kole. Nový volebný protokol musí z dôvodu postupného zavádzania elektronických volieb umožňovať súbeh s klasickými „papierovými“ voľbami.

4.1 Požiadavky na volebný protokol

Pri návrhu nášho volebného protokolu budeme na výsledné riešenie klásť nasledovné požiadavky:

- Protokol definuje internetové voľby prebiehajúce počas niekoľkých dní;
- Splnenie požiadaviek na ideálny volebný systém s dôveryhodnou autoritou (viď. časť 2.1.2 Požiadavky na volebný systém);
- Minimálna úroveň bezpečnosti volebného protokolu je definovaná bezpečnostnou úrovňou klasických „papierových“ volieb;

¹1 volený mandát, K kandidátov

- Maximálne využitie existujúcej infraštruktúry a už dostupných prostriedkov z dôvodu efektivity využívania štátnou správou vynaložených finančných prostriedkov;
- Čiastočná individuálna overiteľnosť – volič má možnosť si overiť spracovanie svojho odovzdaného hlasu minimálne po dosiahnutie komponentu (preukázateľne) spravovaného dôveryhodnou autoritou. Splnenie požiadavky na čiastočnú individuálnu overiteľnosť zvyšuje dôveru voličov v slobodné demokratické voľby;
- Počet aktívnych zapojení voliča do elektronických volieb z dôvodu hlasovania je minimalizovaný (ideálne jednorazové zapojenie), prípravná fáza nevyžaduje aktívnu registráciu voličov do systému. Táto požiadavka je dôsledkom nezúčastňovania sa nezanedbateľnej časti oprávnených voličov pri súčasnom riešení „papierových“ volieb z dôvodov nedostatku času, pracovnej zaneprázdnenosti či rodinných aktivít.²

4.2 Roly účastníkov

V navrhovanom volebnom protokole pre realizáciu elektronických volieb sa budú vyskytovať nasledujúce roly účastníkov:

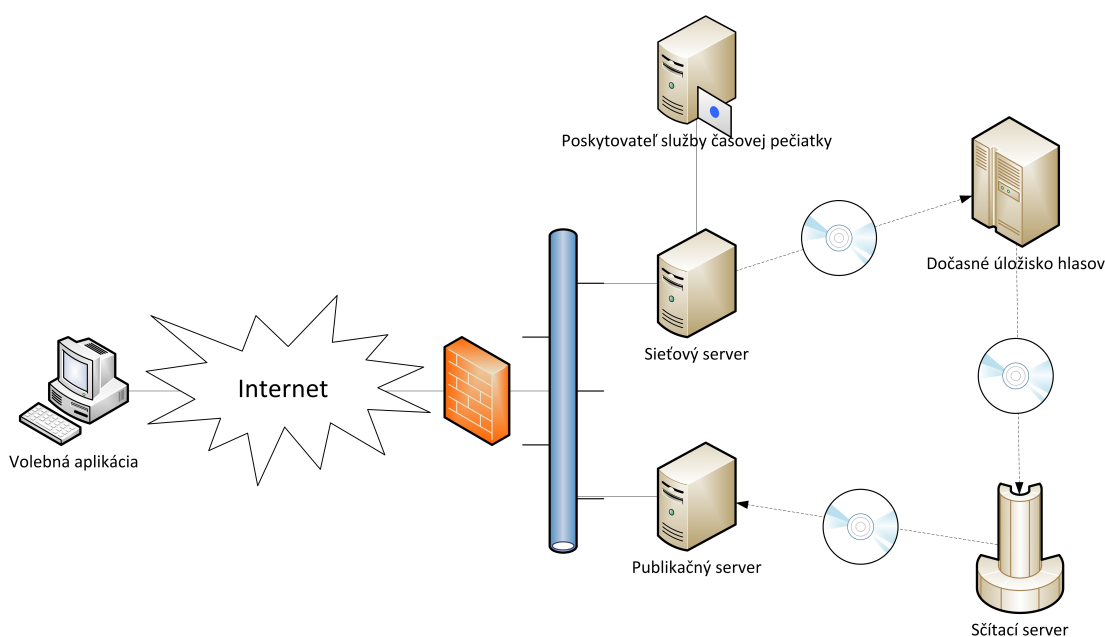
- **Certifikačná autorita** je inštitúcia spravujúca certifikáty pre elektronické podpisy voličov;
- **Člen volebnej komisie** je volič, ktorý dohliada na regulérny priebeh volieb, overuje výsledky hlasovania a rieši sťažnosti oprávnených voličov a pozorovateľov. Čestný člen volebnej komisie je člen volebnej komisie, ktorý dodržiava pokyny stanovené volebným protokolom a nemá úmysel podvárať. Členom volebnej komisie sa nemôže stať kandidát;
- **Kandidát** je volič, ktorý sa uchádza o mandát vo voľbách;
- **Poskytovateľ služby časovej pečiatky** je inštitúcia poskytujúca službu časovej pečiatky pre elektronický podpis;
- **Pozorovateľ** je nezávislá osoba alebo inštitúcia vykonávajúca dohľad nad priebehom volieb a činnosťou volebnej komisie;
- **Predseda volebnej komisie** je náhodne zvolený člen volebnej komisie. Okrem povinností člena volebnej komisie vyhlasuje oficiálne výsledky volieb;

²Povolebný prieskum 2009, Eurobarometer, str. 27,
http://www.europarl.europa.eu/pdf/eurobarometre/28_07/EB71.3_post-electoral_final_report_SK.pdf (22.4.2012)

- **Volič** je občan oprávnený zúčastniť sa volieb. Úlohou voliča je upraviť hlasovací lístok vyznačením kandidáta, ktorému sa rozhodol odovzdať svoj hlas.

Konkrétne implementácie volebného protokolu môžu definovať ďalšie roly špecifické pre dané implementácie³, ktorých existenciu budeme v návrhu predpokladať, avšak na úrovni návrhu protokolu sa nimi zaoberať nebudeme.

4.3 Komponenty volebného protokolu



Obr. 4.1: Komponenty volebného protokolu

Navrhovaný volebný protokol je tvorený niekoľkými internými a externými komponentami. V tejto časti popíšeme jednotlivé komponenty, úlohy, ktoré zohrávajú vo volebnom protokole, a účastníkov zapojených do činnosti popisovaných komponent.

³Napríklad správca servera, prevádzkovateľ komunikačného kanála a ďalšie

4.3.1 Volebná aplikácia

Volebná aplikácia je komponent navrhovaný ako samostatná aplikácia alebo applet pre webový prehliadač. Aplikácia je umiestnená u voliča, s ostatnými komponentami komunikuje prostredníctvom siete Internet. Za správu aplikácie a bezpečnosť systému, na ktorom je aplikácia nasadená, zodpovedá volič. Z pohľadu ostatných komponentov sú dáta prijaté z volebnej aplikácie považované za nedôveryhodné.

Úlohy

1. Vytvoriť a odoslať hlas v čase volieb;
2. Overiť spracovanie hlasu po skončení volieb.

Účastníci

- Volič
- Certifikačná autorita
- Sieťový server
- Publikačný server

4.3.2 Sieťový server

Sieťový server je s výnimkou *publikačného servera* jediným komponentom volebného protokolu v správe volebnej komisie, ktorý je perzistentne pripojený do siete Internet. Komponent je navrhovaný ako serverová aplikácia poskytujúca služby *volebnej aplikácii* a *dočasnému úložisku hlasov*.

Úlohy

1. Prijatť a uložiť hlas;
2. Vydať potvrdenie o prijatí hlasu;
3. Odovzdať hlasy na ďalšie spracovanie.

Účastníci

- Certifikačná autorita
- Poskytovateľ služby časovej pečiatky
- Volebná aplikácia
- Dočasné úložisko hlasov

4.3.3 Dočasné úložisko hlasov

Dočasné úložisko hlasov je komponent volebného protokolu, ktorého funkčnosť a štandardné správanie podľa protokolu garantuje volebná komisia. Komponent je izolovaný od všetkých počítačových sietí, je v činnosti iba počas vykonávania niektorej z definovaných úloh pod dohľadom volebnej komisie a komunikácia s okolím je zabezpečená prostredníctvom fyzických médií.

Úlohy

1. Bezpečne uchovávať prijaté hlasy v priebehu konania volieb až do ich ďalšieho spracovania;
2. Odstrániť hlasy v nesprávnom formáte zo zoznamu platných hlasov;
3. Odstrániť duplicitné hlasy zo zoznamu platných hlasov;
4. Odstrániť hlasy s neplatným elektronickým podpisom zo zoznamu platných hlasov;
5. Vytvoriť zoznam neplatných hlasov;
6. Anonymizovať zoznamy hlasov;
7. Odovzdať platné a neplatné hlasy na ďalšie spracovanie.

Účastníci

- Certifikačná autorita
- Členovia volebnej komisie
- Poskytovateľ služby časovej pečiatky
- Pozorovatelia
- Sieťový server

4.3.4 Sčítací server

Sčítací server je druhým z komponentov volebného protokolu, ktorého funkčnosť a štandardné správanie podľa protokolu garantuje volebná komisia. Komponent je taktiež izolovaný od všetkých počítačových sietí, je v činnosti iba počas vykonávania niektorej z definovaných úloh pod dohľadom volebnej komisie a komunikácia s okolím je zabezpečená prostredníctvom fyzických médií.

Úlohy

1. Prevod hlasov do otvorenej (čitateľnej) podoby;
2. Spočítanie výsledkov volieb;
3. Vytvorenie zoznamu identifikátorov pre potreby čiastočnej individuálnej overiteľnosti.

Účastníci

- Členovia volebnej komisie
- Certifikačná autorita
- Pozorovatelia
- Dočasné úložisko hlasov

4.3.5 Publikačný server

Publikačný server je základným komponentom volebného protokolu zabezpečujúcim presmerovanie voliča na príslušné webové adresy. Komponent poskytuje služby smerovača a z tohto dôvodu je potrebné zabezpečiť jeho nepretržitú prevádzku.

Úlohy

1. Zverejňuje certifikáty, zoznamy, výsledky;
2. Informácie o spracovaní hlasov.

Účastníci

- Členovia volebnej komisie
- Pozorovatelia
- Volebná aplikácia
- Sieťový server
- Certifikačná autorita
- Poskytovateľ služby časovej pečiatky

4.3.6 Externé komponenty

- **Certifikačná autorita pre elektronický podpis** poskytuje služby vydávania nových a zneplatňovanie existujúcich certifikátov elektronických podpisov. Komponent poskytuje sieťovú službu publikujúcu zoznam zneplatnených certifikátov CRL (z angl. Certificate Revocation List) v pravidelných intervaloch, minimálne však raz za 24 hodín.
- **Poskytovateľ služby časových pečiatok** je sieťová služba poskytujúca časové pečiatky pre elektronicky podpísané dokumenty. Komponent poskytuje služby na vyžiadanie oprávneným osobám alebo komponentom.
- **Register oprávnených voličov** je externý komponent poskytujúci oprávneným osobám alebo systémom zoznam všetkých osôb, ktoré sú oprávnené hlasovať vo voľbách.

4.4 Volebný protokol

V predchádzajúcich častiach kapitoly sme predstavili účastníkov a komponenty nového volebného protokolu, ktorý navrhujeme pre realizáciu elektronických volieb. V tejto časti sa zameriame na návrh samotného protokolu. Nižšie popísaný návrh volebného protokolu patrí do skupiny hybridných volebných schém, má 4 fázy a vychádza z estónskeho volebného protokolu, ktorý sme stručne popísali v časti 3.2.3.

Dôležitú úlohu v navrhovanom protokole zohrávajú podobne ako v estónskom alebo nórskom riešení elektronické podpisovanie a asymetrické šifrovanie. Autenticita a integrita hlasu ako i anonymita voliča odovzdávajúceho hlas sú zabezpečené uložením hlasu do troch vrstiev ochrany hlasu tvorených asymetrickým šifrovaním a elektronickým podpisom. Prvé dve vrstvy sú vytvorené analogicky ako u estónskeho riešenia, tretiu vrstvu ochrany hlasu tvorí asymetrické šifrovanie za použitia iného páru kryptografických kľúčov ako v prípade prvej vrstvy. Úlohou dodatočného šifrovania je zabrániť tvorbe zoznamu zúčastnených voličov a selektívnej manipulácii s hlasmi vybraných voličov v priebehu volieb na komponentoch volebného protokolu, ktoré nie sú počas svojej činnosti pod neustálou kontrolou členov volebnej komisie. V súvislosti s pridaním dodatočného šifrovania hlasu sme v záujme zachovania vhodných vlastností estónskeho protokolu pristúpili k nasledujúcim úpravám protokolu.



Obr. 4.2: Grafické znázornenie ochrany hlasu voliča

4.4.1 Prípravná fáza

Prípravná fáza popisuje protokol v období pred zahájením elektronického hlasovania.

1. Vytvorí sa volebná komisia podľa dohodnutých postupov, ktoré nie sú predmetom volebného protokolu. Každý člen volebnej komisie získa certifikát na tvorbu elektronického podpisu člena komisie. Členovia volebnej komisie konajú samostatne a v súlade so schválenými postupmi.
2. Volebná komisia určí termín konania volieb a zverejní elektronicky podpísaný zoznam kandidátov.
3. Volebná komisia vytvorí pár kryptografických kľúčov pre aktuálne elektronické voľby podľa zvolenej bezpečnej schémy pre asymetrické šifrovanie. Súkromný dešifrovací kľúč je pomocou bezpečnej schémy na zdieľanie tajomstva⁴ rozdelený medzi členov volebnej komisie. Verejný šifrovací kľúč je podpísaný elektronickým podpisom každého z členov volebnej komisie a zverejnený na *publikačný server*.

⁴Napr. Shamirovej schémy

4. Volebná komisia vytvorí usporiadaný zoznam nových párov kryptografických kľúčov⁵. Pre každý verejný šifrovací kľúč je vytvorený a volebnou komisiou podpísaný prislúchajúci certifikát s obmedzenou dĺžkou platnosti⁶. Intervaly platnosti certifikátov usporiadaných kľúčov zo zoznamu tvoria rastúcu postupnosť prekrývajúcich sa intervalov s pevne stanoveným prekryvom⁷, pričom v ľubovoľnom okamihu v konania volieb existuje v zozname aspoň jeden platný certifikát s verejným šifrovacím kľúčom. Prvý pár kľúčov v tomto zozname budeme ďalej v tomto popise nazývať **aktuálne kryptografické kľúče sieťového servera**. Dešifrovacie kľúče sú pomocou bezpečnej schémy na zdieľanie tajomstva rozdelené medzi členov volebnej komisie. Šifrovacie kľúče spolu s intervalom ich použiteľnosti (platnosti) sú elektronicky podpísané, zverejnené na *publikačnom serveri* a sú odovzdané na použitie v *dočasnom úložisku hlasov*.
5. Členovia volebnej komisie spolu s odborníkmi vykonávajú kontrolu funkčnosti, autenticity a integrity *volebnej aplikácie, sieťového servera, dočasného úložiska hlasov, sčítacieho servera a publikačného servera*. V prípade úspešnej kontroly pripraví *volebnú aplikáciu, sieťový server, dočasné úložisko hlasov, sčítací server a publikačný server* na spustenie hlasovania, elektronicky podpísaná *volebná aplikácia* je zverejnená na *publikačnom serveri*.
6. Oprávnený volič, ktorý sa chce zúčastniť elektronických volieb, si pred hlasovaním vybaví u *certifikačnej autority* certifikát pre elektronický podpis a potrebné zariadenia na jeho vytvorenie, ak tak ešte neurobil.

4.4.2 Volebná fáza - hlasovanie voliča

Prvá z volebných fáz sa zaoberá procesom vytvárania a odovzdávania hlasu vo *volebnej aplikácii* a prijatím hlasu na strane *sieťového úložiska* v priebehu obdobia určeného na hlasovanie.

1. Pred zahájením hlasovania v období určenom na elektronické hlasovanie si volič overí autentickosť a integritu *volebnej aplikácie*. V prípade nesúlady volič informuje volebnú komisiu.
2. Volič spustí *volebnú aplikáciu*.
3. *Volebná aplikácia* získa certifikát obsahujúci *šifrovací kľúč pre aktuálne elektronické volby*, certifikát s *aktuálne platným šifrovacím kľúčom sieťového*

⁵Tieto kľúče budú slúžiť na šifrovanie v pridanej 3. vrstve uzatvorenia hlasu, ktorú sme v krátkosti predstavili vyššie

⁶Dĺžku platnosti certifikátov odporúčame z praktických dôvodov prispôsobiť vydávaniu CRL použitých certifikačných autorít, zvyčajne 12-48 hodín.

⁷Prekryv intervalov odporúčame z praktických dôvodov prispôsobiť predpokladanej dĺžke času potrebného na vytvorenie a odovzдание hlasu voličom, zvyčajne do 15 minút.

servera, adresu *sietového servera* a zoznam kandidátov z *publikačného servera*. Volič je informovaný, ak nie je možné niektorý údaj získať, *volebná aplikácia* je ukončená a volič informuje volebnú komisiu.

4. *Volebná aplikácia* overí platnosť získaných certifikátov. V prípade neplatnosti niektorého z certifikátov, *volebná aplikácia* upozorní voliča, ktorý informuje volebnú komisiu.
5. Volič prejaví svoju vôľu hlasovať za vybraného kandidáta jeho označením vo *volebnej aplikácii*.
6. *Volebná aplikácia* vygeneruje náhodným generátorom „**náhodný identifikátor hlasu**“ (ďalej NIH) vo forme náhodného reťazca.⁸ Volič je povinný pre každý svoj hlas s rovnakou voľbou vygenerovať jedinečný NIH.⁹ V prípade 2 a viacerých hlasov s rovnakou voľbou a NIH bude za platný hlas považovaný iba prvý z prijatých hlasov.
7. *Volebná aplikácia* spojí informáciu o výbere voliča s NIH a následne tieto informácie zašifruje pomocou *šifrovacieho kľúča pre aktuálne elektronické voľby*.
8. Volič sa identifikuje voči *volebnej aplikácii*, ktorá v jeho mene elektronicky podpíše zašifrovaný hlas elektronickým podpisom voliča.
9. *Volebná aplikácia* zašifruje podpísaný zašifrovaný hlas pomocou *aktuálne platného šifrovacieho kľúča sietového servera*.
10. *Volebná aplikácia* vytvorí žiadosť o slepý podpis NIH podľa bezpečnej schémy pre tvorbu slepých elektronických podpisov, ktorú pripojí k hlasu voliča.
11. *Volebná aplikácia* vytvorí spojenie so sietovým serverom. Po nadviazaní spojenia *volebná aplikácia* odošle *sietovému serveru* hlas voliča doplnený o žiadosť o slepý podpis pre NIH. Ak nie je možné spojenie nadviazať, *volebná aplikácia* informuje voliča.
12. *Sietový server* prijme takto upravený hlas spolu so žiadosťou o slepý podpis NIH.

⁸Dĺžku reťazca odporúčame zvoliť v priamej úmere s počtom oprávnených voličov a predpokladaného množstva opakovane odovzdaných hlasov.

⁹Tento prípad môže nastať v prípade rozhodnutia voliča zmeniť svoju voľbu a následne vykonať návrat k pôvodnej voľbe. Z dôvodu čiastočnej individuálnej overiteľnosti odporúčame jedinečný NIH pre každý z odovzďavaných hlasov. Výnimkou sú prípady pokusov o nelegálne ovplyvňovanie voliča, pri ktorých odporúčame voličovi použiť rovnaký NIH pre nový hlas rušiaci platnosť pôvodného hlasu vytvoreného pod nátlakom.

13. *Sieťový server* elektronicky podpíše NIH a odošle žiadosť o pridelenie časovej pečiatky pre prijatý hlas *poskytovateľovi služby časovej pečiatky*.
14. Po obdržaní časovej pečiatky *sieťový server* uloží hlas doplnený o časovú pečiatku na svoje úložisko a odošle *volebnej aplikácii* podpísaný NIH a hlas s časovou pečiatkou. V prípade problémov na strane V prípade problémov na strane *sieťového servera* je *volebná aplikácia* informovaná o chybe.
15. *Sieťový server* ukončí spojenie s *volebnou aplikáciou*.
16. Ak *volebná aplikácia* neobdrží v stanovenom čase odpoveď zo strany *sieťového servera*, informuje voliča o chybe a ukončí spojenie.
17. *Volebná aplikácia* overí platnosť a aktuálnosť prijatej časovej pečiatky hlasu a porovná prijatý hlas s odoslanými dátami. Ak dáta nie sú zhodné alebo časová pečiatka nie je platná (resp. aktuálna), *volebná aplikácia* oboznámi voliča s príčinou nesúladu a volič informuje volebnú komisiu o potenciálnej kompromitácii *sieťového servera*.
18. *Volebná aplikácia* zrekonštruuje a overí platnosť prijatého podpisu NIH, zhodu podpísaného NIH s odoslaným a informáciu o NIH, jeho podpise a príslušnej časovej pečiatke poskytne voličovi. V prípade nesúladu *volebná aplikácia* informuje voliča o chybe a volič informuje volebnú komisiu o potenciálnej kompromitácii *sieťového servera*.

4.4.3 Volebná fáza - predspracovanie hlasov

Druhá z volebných fáz konajúca sa v priebehu hlasovacieho obdobia súbežne s prvou fázou popisuje transfer hlasov, ich prvotné spracovanie *dočasným úložiskom hlasov* a výmenu používaných aktuálnych certifikátov so šifrovacími kľúčmi. Cieľom predspracovania hlasov je zníženie požiadaviek na veľkosť diskového priestoru pre prijaté dáta z volebných aplikácií.

1. *Sieťový server* pravidelne overuje platnosť *aktuálneho šifrovacieho kľúča sieťového servera*.
2. Ak aktuálny šifrovací kľúč nie je platný (vypršala jeho platnosť, bol predčasne zrušený,...) alebo jeho platnosť bude ukončená v krátkom čase a existuje aspoň v danom čase platný certifikát v zozname certifikátov *sieťového servera*, potom *sieťový server* informuje volebnú komisiu, vyhľadá v zozname certifikátov ďalší platný certifikát a nastaví ho ako aktuálny.
3. Ak bola zrušený jediný certifikát platný v danom časovom období, *sieťový server* pozastaví svoju činnosť a informuje volebnú komisiu.

4. *Sieťový server* prijíma správy šifrované pôvodným šifrovacím kľúčom až do doby vypršania jeho platnosti. Správy šifrované iným ako pôvodným šifrovacím kľúčom alebo aktuálnym šifrovacím kľúčom *sieťového servera* v dobe ich prijatia sú považované za neplatné hlasy.
5. Po vypršaní platnosti pôvodného *šifrovacieho kľúča sieťového servera* sú vybrané všetky hlasy šifrované pôvodným šifrovacím kľúčom a premiestnené do zoznamu hlasov určených na ďalšie spracovanie na *dočasné úložisko hlasov*.
6. Členovia volebnej komisie preveria funkčnosť *dočasného úložiska hlasov*, integritu a autentickosť jeho softvérového vybavenia a uložených dát od posledného kontrolovaného prístupu volebnej komisie k *dočasnému úložisku hlasov*.
7. Členovia volebnej komisie bezpečným spôsobom manuálne premiestnia hlasy zo zoznamu hlasov určených na ďalšie spracovanie na *dočasné úložisko hlasov* na tento komponent.
8. *Dočasné úložisko hlasov* overí autentickosť a integritu zoznamu hlasov. V prípade úspešnej kontroly členovia volebnej komisie odstránia všetky prenesené hlasy zo *sieťového servera*, inak sa opakuje predchádzajúci krok.
9. Členovia volebnej komisie zrekonštruujú dešifrovací kľúč pre *sieťový server* platný pre prijatý zoznam hlasov.
10. *Dočasné úložisko hlasov* dešifruje prijaté hlasy a spracuje ich:
 - (a) Ak prijatý hlas nemá správny formát, *dočasné úložisko hlasov* zapíše údaje z jeho časovej pečiatky do *zoznamu časových pečiatok falošných hlasov* a odstráni hlas zo systému.
 - (b) Ak prijatý hlas má správny formát, *dočasné úložisko hlasov* bezpečne uloží hlas spolu s jeho časovou pečiatkou na ďalšie spracovanie po skončení hlasovania.
11. *Dočasné úložisko hlasov* informuje volebnú komisiu o výsledkoch spracovania hlasov, volebná komisia overí údaje s predpokladmi (počet spracovaných hlasov, integrita zoznamu časových pečiatok falošných hlasov atď.).
12. *Dočasné úložisko hlasov* odstráni *dešifrovací kľúč pre sieťový server platný pre prijatý zoznam hlasov* zo systému a členovia volebnej komisie fyzicky zničia všetky kópie dešifrovacieho kľúča ako i čiastkové informácie vedúce k jeho rekonštrukcii.

13. Činnosť *dočasného úložiska hlasov* je po skončení tejto fázy pozastavená, aktuálny stav systému uložený a systém je fyzickými a softvérovými prvkami zabezpečený proti neoprávnenému prístupu. Narušenie ochrany proti neoprávnenému prístupu musí byť jednoznačne identifikovateľné. Neoprávnený prístup je po zahájení prípravnej fázy každý prístup, ktorý nie je definovaný volebným protokolom.

4.4.4 Fáza spracovania hlasov

Fáza spracovania hlasov prebieha po uplynutí doby určenej na elektronické hlasovanie. V prípade súbehu s klasickými „papierovými“ voľbami prebieha táto fáza až po uzatvorení volebných miestností a doručení zoznamu voličov, ktorí sa zúčastnili klasického hlasovania. Pri spracovaní hlasov sú najskôr odstránené duplicitné a neplatné hlasy, následne sú hlasy anonymizované odstránením elektronických podpisov, premiešané a spočítané na *sčítacom serveri*. V priebehu spracovania hlasov sa vytvára *zoznam spracovaných NIH*, ktorý slúži na dosiahnutie čiastočnej individuálnej overiteľnosti.

1. Po uplynutí obdobia určeného pre elektronické hlasovanie *sieťový server* neprijíma ďalšie hlasy a členovia volebnej komisie preniesú na *dočasné úložisko hlasov* zvyšné prijaté hlasy podľa predchádzajúcej fázy.
2. *Dočasné úložisko hlasov* spracuje zvyšné hlasy podľa predchádzajúcej fázy.
3. *Dočasné úložisko hlasov* vytvorí zoznam spracovaných časových pečiatok obsahujúcich časové pečiatky všetkých hlasov v systéme.
4. *Dočasné úložisko hlasov* overí platnosť elektronických podpisov hlasov v čase pridelenia časovej pečiatky pre všetky hlasy v systéme.
5. Ak elektronický podpis nebol v uvedenom čase platný, *dočasné úložisko hlasov* odstráni časovú pečať, elektronický podpis a presunie hlas do *zoznamu neplatných hlasov*.
6. *Dočasné úložisko hlasov* odstráni časovú pečať a elektronický podpis hlasov, ktoré sú neplatné z dôvodu duplicity a presunie ich do zoznamu neplatných hlasov. Hlas je považovaný za duplicitný, ak je splnená jedna z nasledovných podmienok:
 - (a) existuje aspoň 1 hlas od rovnakého voliča so staršou časovou pečaťou, ktorý je totožný s týmto hlasom,
 - (b) existuje aspoň 1 hlas od rovnakého voliča s novšou časovou pečaťou, ktorý nie je totožný s týmto hlasom.
7. *Dočasné úložisko hlasov* odstráni časovú pečať zvyšných hlasov a presunie ich do zoznamu platných hlasov.

8. *Dočasné úložisko hlasov* premieša zoznam platných hlasov.
9. *Dočasné úložisko hlasov* premieša zoznam neplatných hlasov.
10. *Dočasné úložisko hlasov* pripraví zoznamy časových pečiatok falošných hlasov, neplatných hlasov, platných hlasov a spracovaných časových pečiatok na presun na *sčítací server*.
11. *Dočasné úložisko hlasov* informuje členov volebnej komisie o úspešnosti vykonaných úloh.
12. Členovia volebnej komisie bezpečným spôsobom manuálne premiestnia zoznamy časových pečiatok falošných hlasov, neplatných hlasov, platných hlasov a spracovaných časových pečiatok na *sčítací server*.
13. *Sčítací server* overí integritu a autentickosť prijatých zoznamov časových pečiatok falošných hlasov, neplatných hlasov, platných hlasov a spracovaných časových pečiatok.
14. Členovia volebnej komisie zrekonštruujú *dešifrovací kľúč pre aktuálne voľby*.
15. *Sčítací server* dešifruje hlasy zo *zoznamu platných hlasov* a overí ich formát:
 - (a) Ak je formát nesprávny, *sčítací server* zaradí reťazec *NIH*¹⁰ do *zoznamu spracovaných NIH* a uloží hlas v pôvodnej zašifrovanej podobe do zoznamu hlasov s neplatným formátom.
 - (b) Ak je formát správny, *sčítací server* pripočíta hlas zvolenému kandidátovi a zaradí *NIH* do *zoznamu spracovaných NIH*.
16. *Sčítací server* dešifruje hlasy zo *zoznamu neplatných hlasov* a overí ich formát:
 - (a) Ak je formát nesprávny, *sčítací server* zaradí reťazec *NIH*¹⁰ do *zoznamu spracovaných NIH*, uloží hlas v pôvodnej zašifrovanej podobe do zoznamu hlasov s neplatným formátom.
 - (b) Ak je formát správny, *sčítací server* zaradí *NIH* do *zoznamu spracovaných NIH*.
17. *Sčítací server* alfanumericky usporiada *zoznam spracovaných NIH* a vytvorí výsledok volieb.
18. *Sčítací server* informuje členov volebnej komisie o úspešnosti vykonaných úloh.

¹⁰Ak reťazec nie je možné určiť, *sčítací server* bude za *NIH* považovať reťazec na predpokladanej pozícii, kde by sa mal reťazec nachádzať

19. Členovia volebnej komisie po kontrole výsledkov elektronicky podpíšu výsledok volieb, *zoznam spracovaných NIH, zoznam spracovaných časových pečiatok, zoznam časových pečiatok falošných hlasov a zoznam hlasov s neplatným formátom.*
20. Členovia volebnej komisie manuálne premiestnia výsledok volieb, *zoznam spracovaných NIH, zoznam spracovaných časových pečiatok, zoznam časových pečiatok falošných hlasov a zoznam hlasov s neplatným formátom na publikačnom serveri, ktorý ich zverejní.*
21. Členovia volebnej komisie v spolupráci s odborníkmi nenávratne vymažú všetky dáta zo *sieťového servera, dočasného úložiska hlasov, sčítacieho servera* a spoľahlivým spôsobom odstránia dáta z použitých prenosných médií.

4.5 Dohľad nad priebehom hlasovania

Bezpečnosť volebného protokolu je postavená na bezpečných kryptografických prvkoch a kontrole dôveryhodnej autority. V predchádzajúcej časti sme popísali protokol vyžadujúci dôveryhodnú autoritu. Za dôveryhodnú autoritu považujeme volebnú komisiu. V praxi sa však ukazuje vytvorenie volebnej komisie, ktorá koná zodpovedne, čestne a ktorej činnosti dôveruje každá zo zúčastnených strán (voliči, kandidáti, pozorovatelia), ako problematické najmä z dôvodov subjektívneho prístupu členov komisie a nedôvery v čestné konanie členov volebnej komisie zo strany kandidátov a voličov.

V časti 4.1 sme špecifikovali požiadavky na volebný protokol, medzi inými aj požiadavku definujúcu minimálnu úroveň bezpečnosti úrovňou klasických „papierových“ volieb. Klasické „papierové“ voľby sú rovnako ako náš navrhovaný protokol realizované volebným protokolom s dôveryhodnou autoritou. V našom protokole preto využijeme existujúcu realizáciu dôveryhodnej autority. Autoritou je volebná komisia zložená zo zástupcov kandidujúcich strán. Dôveryhodnosť volebnej komisie je zabezpečená nižšie uvedeným predpokladom na činnosť členov volebnej komisie a dohľadom skupiny pozorovateľov a voličov na priebeh volieb podľa protokolu.

Predpoklad na činnosť členov volebnej komisie:

„Členovia volebnej komisie konajú samostatne s cieľom zabrániť zvýhodneniu kandidátov preferovaných ostatnými členmi volebnej komisie nečestným konaním niektorého z kandidátov, voličov alebo členov volebnej komisie.“

4.5.1 Volebná komisia

Úlohami volebnej komisie sú príprava elektronických volieb, úlohy stanovené volebným protokolom a dohľad nad systémami v správe členov volebnej komisie. Volebná komisia za pomoci odborníkov na bezpečnosť systémov pripravuje komponenty na použitie v elektronických voľbách a kontroluje ich vstupné a výstupné dáta. Volebná komisia tiež rieši výnimočné udalosti v priebehu konania elektronických volieb.

Medzi výnimočné udalosti zaraďujeme výpadky systémov realizujúcich komponenty volebného protokolu a informácie (sťažnosti) voličov na nefunkčnosť niektorého komponentu volebného protokolu. Volebná komisia vykoná adekvátne kroky vedúce k obnove funkčnosti elektronických volieb, ak sú tieto kroky možné bez ovplyvnenia priebehu volieb, inak volebná komisia vyhlási elektronické voľby za neplatné a odstráni všetky prijaté hlasy a údaje o oprávnených voličoch z komponentov volebného protokolu.¹¹

Volebná komisia tiež rieši sťažnosti voličov na kompromitáciu elektronických volieb po skončení elektronického hlasovania a zverejnení výsledkov.

4.5.2 Dohľad voličov

Úlohou voliča v našom volebnom protokole je okrem odovzdania svojho hlasu aj aktívna účasť na kontrole zabezpečenia elektronických volieb. Pri odovzdávaní elektronického hlasu je volič vo svojom záujme povinný osobne alebo prostredníctvom volebnej aplikácie, ktorej dôveruje, skontrolovať autentickosť volebných serverov, s ktorými komunikuje, a autentickosť, integritu a korektnosť odpovedí prijatých z volebných komponentov v zmysle navrhovaného volebného protokolu.

Po zverejnení výsledkov hlasovania má volič tiež možnosť overiť si v zozname spracovaných NIH spracovanie jeho hlasu vo volebnom protokole. Ak volič nenájde svoj NIH vytvorený a odovzdaný spolu s platným hlasom v zozname spracovaných NIH, podá sťažnosť členom volebnej komisie, ktorej poskytne svoju podpísanú kópiu NIH spolu s časovou pečiatkou hlasu. Členovia volebnej komisie vyriešia sťažnosť po jej prijatí v nasledovnom poradí :

1. Členovia volebnej komisie overia identitu sťažovateľa. Ak sťažovateľ nie je oprávnený volič, sťažnosť zamietnu ako neodôvodnenú;
2. Ak je elektronický podpis NIH neplatný alebo nepochádza zo *sieťového servera*, sťažnosť je zamietnutá s odôvodnením „poskytnuté neplatné údaje“;

¹¹Pri odstraňovaní dát môže dôjsť k odstráneniu stôp vedúcich k odhaleniu vinníka, preto je potrebné zvážiť rozsah odstraňovaných dát v závislosti povahy dôvodov vedúcich k zneplatneniu elektronických volieb.

3. Ak je časová pečiatka neplatná alebo nepochádza od *poskytovateľa služby časovej pečiatky* určeného pre dané elektronické voľby, sťažnosť je zamietnutá s odôvodnením „poskytnuté neplatné údaje“;
4. Ak sa NIH nachádza na zozname spracovaných NIH, sťažnosť je zamietnutá s odôvodnením „hlas bol spracovaný systémom pod neustálym dohľadom dôveryhodnej autority“;
5. Ak sa časová pečiatka hlasu nachádza na zozname časových pečiatok falošných hlasov, sťažnosť je zamietnutá s odôvodnením „hlas nemal platný formát“;
6. Ak sa časová pečiatka hlasu nachádza na zozname spracovaných časových pečiatok, sťažnosť je zamietnutá s odôvodnením „hlas bol spracovaný ako neplatný, hlas nebol vytvorený v súlade s volebným protokolom“;
7. Inak je sťažnosť akceptovaná.

Ak existuje aspoň 1 akceptovaná sťažnosť a dohľad nad volebnými komponentami neodhalil problémy, *sietový server* a/alebo *poskytovateľ služby časovej pečiatky* boli v priebehu volieb kompromitovaní a elektronické voľby vrátane výsledku volieb sú prehlásené za neplatné.

Dôvod zamietnutia sťažnosti voliča nemusí zodpovedať skúsenosti voliča, ak na odovzdanie svojho hlasu nepoužil odporúčanú volebnú aplikáciu. Za použitie bezpečnej a korektnej volebnej aplikácie ako i bezpečnosť zariadenia, na ktorom je volebná aplikácia spustená, zodpovedá volič.

4.5.3 Dohľad pozorovateľov

Účasť pozorovateľov na priebehu elektronických volieb má dodatočnú kontrolnú funkciu zvyšujúcu dôveryhodnosť realizácie elektronických volieb. Pozorovatelia sa zúčastňujú na všetkých aktivitách volebnej komisie v súvislosti s konaním elektronických volieb, dohliadajú na ich činnosť a upozorňujú verejnosť na odhalené pochybenia.

Pozorovatelia nemajú rozhodovacie právomoci a nemajú oprávnenie získavať údaje z volebných systémov alebo od členov volebnej komisie (napr. časti kryptografických kľúčov, prijaté hlasy atď.). Pozorovatelia majú možnosť na požiadanie získať v spolupráci s odborníkmi a správcami volebných komponentov úplné kópie použitých systémov a médií použitých na ich inštaláciu s výnimkou údajov obsahujúcich hlasy alebo informácie o hlasoch voličov, časti kryptografických kľúčov a/alebo ďalšie citlivé údaje, ktoré by mohli viesť ku kompromitácii elektronických volieb v prípade ich zneužitia nečestným pozorovateľom.

4.6 Bezpečnostná analýza

V bezpečnostnej analýze sa zameriame na bezpečnosť navrhovaného volebného protokolu pre uskutočnenie elektronických volieb a popíšeme potenciálne útoky na volebný protokol spolu s ich dopadmi na výsledok elektronického hlasovania. Úvodom si popíšeme model útočníka a následne vyslovíme niekoľko predpokladov, z ktorých budeme pri bezpečnostnej analýze vychádzať.

4.6.1 Model útočníka

V tejto časti sa budeme venovať správaniu útočníka, ktorý sa snaží ovplyvniť výsledok volieb. V ľubovoľnom volebnom protokole realizujúcom elektronické voľby je útočník s dostatočným množstvom dostupných zdrojov schopný v malom rozsahu ovplyvniť výsledok hlasovania. Útoky tohto typu je možné realizovať nepretržitou kontrolou ovplyvneného oprávneného voliča alebo skupiny oprávnených voličov, avšak z praktického hľadiska sú tieto útoky z pohľadu útočníka neefektívne a nerealizovateľné vo väčšom meradle¹². V našom modelovom prostredí budeme preto predpokladať, že útočník sa snaží o rozsiahly útok na volebný systém zneužitím niektorej zo zraniteľností volebného protokolu alebo jeho implementácie.

Správanie útočníka alebo osôb pod jeho kontrolou v priebehu útoku na elektronické voľby definuje podmnožina z nasledujúcich aktivít, ktoré sa útočník snaží vykonať bez odhalenia:

1. Získať kontrolu nad *sčítacím serverom* s cieľom ovplyvniť spočítavanie hlasov vo fáze spracovania hlasov;
2. Ovplyvniť prenos údajov z *dočasného úložiska hlasov* na *sčítací server* s cieľom zameniť alebo upraviť zoznam platných hlasov tvoriacich výsledok volieb;
3. Získať kontrolu nad *dočasným úložiskom hlasov* a *sčítacím serverom* s cieľom spárovať platné elektronické hlasy v čitateľnej podobe s oprávnenými voličmi, ktorí ich odovzdali;
4. Získať kontrolu nad *dočasným úložiskom hlasov* s cieľom odstrániť hlasy vybranej skupiny voličov;
5. Získať kontrolu nad *dočasným úložiskom hlasov* s cieľom overiť, či ovplyvnený volič dodatočne neodovzdal ďalší platný hlas;

¹²Nepretržitý dohľad nad voličom alebo menšou skupinou voličov po celú dobu elektronického hlasovania, ktorá je stanovená rádovo v týždňoch, si vyžaduje nasadenie ďalšej osoby loajálnej útočníkovi a prípadné využitie ďalších zdrojov. Útok vo väčšom meradle by bol volebnou komisiou, čestnými voličmi a pozorovateľmi ľahko odhaliteľný a voľby by boli následne zrušené/odložené.

6. Ovplyvniť prenos údajov zo *sieťového servera* na *dočasné úložisko hlasov* s cieľom upraviť zoznam hlasov, ktoré vstupujú do fáz spracovania hlasov;
7. Získať kontrolu nad *sieťovým serverom* s cieľom ovplyvniť priebeh elektronického hlasovania v momente odovzdávania hlasu vybranej podmnožiny oprávnených voličov;
8. Ovplyvniť prenos údajov z *volebnej aplikácie* na *sieťový server* s cieľom odstrániť, modifikovať alebo nahradiť hlas odovzdávaný voličom;
9. Ovplyvniť prenos údajov z *volebnej aplikácie* na *sieťový server* s cieľom zamedziť účasti na voľbách vybranej podmnožiny oprávnených voličov;
10. Získať kontrolu nad *volebnou aplikáciou* s cieľom odstrániť, modifikovať alebo nahradiť hlas odovzdávaný voličom;
11. Získať kontrolu nad *certifikačnou autoritou* s cieľom ovplyvniť vytváranie platných elektronických podpisov;
12. Získať kontrolu nad *poskytovateľom služby časovej pečiatky* s cieľmi neoprávnene vytvárať platné časové pečiatky a/alebo ovplyvniť platnosť vydaných časových pečiatok.

Využitím vybranej podmnožiny definovaných aktivít môže útočník vykonať niektorý z typov útokov špecifických pre voľby. Typy útokov definujeme podobne ako [BM07] :

- **Krádež hlasov vo veľkom rozsahu** – Útok sa zameriava na úpravu existujúcich alebo pridanie nových platných hlasov v prospech preferovaného kandidáta. V prípade zraniteľnosti volebného protokolu voči tomuto typu útoku môže útočník neoprávnene odovzdať dostatok platných hlasov, ktoré ovplyvnia výsledok hlasovania. Táto zraniteľnosť tiež môže umožniť oprávnenému voličovi odovzdať viac ako jeden hlas, čo je v rozpore s požiadavkami na integritu a spôsobilosť.
- **Znehodnotenie hlasov vo veľkom rozsahu** – Útok sa zameriava na odstránenie platných hlasov z volebného protokolu ešte pred ich doručením na komponenty, ktoré sú pod neustálym dohľadom volebnej komisie. Útok sa môže ale nemusí zamerať na selektívne odstraňovanie hlasov nepohodlných oprávnených voličov, čo je v rozpore s požiadavkami na férovosť a kompletnosť.
- **Korupcia a ovplyvňovanie voličov vo veľkom rozsahu** – Útok sa nezameriava na zraniteľnosti volebných komponentov ale na dobrovoľné alebo nedobrovoľné získanie platných hlasov od oprávnených voličov v množstve postačujúcom na ovplyvnenie výsledku volieb v prospech preferovaného kandidáta.

- **Narušenie anonymity hlasovania vo veľkom rozsahu** – Útoky tohto typu nemajú priamy vplyv na výsledok elektronického hlasovania. Úlohou útokov je odtajniť hlasovanie jednotlivca alebo skupiny oprávnených voličov, ktoré je možné využiť pri predchádzajúcom type útoku a/alebo na perzekúciu nepohodlných oprávnených voličov po skončení elektronického hlasovania. Zraniteľnosť voči tomuto typu útoku je v rozpore s požiadavkou na anonymitu čestných oprávnených voličov.
- **Zrušenie volieb** – Útočník má za cieľ presvedčiť volebnú komisiu, aby vyhlásila prebiehajúce alebo ukončené elektronické voľby za neplatné. Dôvodmi na tento typ útoku môžu byť nespokojnosť útočníka s priebehom alebo výsledkom elektronických volieb, prípadne snaha o odloženie hlasovania na neskorší termín.

Ak je volebný protokol odolný voči prvým štyrom z uvedených útokov, tak z definície spĺňa požiadavky na ideálny volebný systém s dôveryhodnou autoritou, tzn. zachováva **anonymitu, férovosť, integritu, kompletnosť** aj **neprekúpatelnosť** hlasovania. Požiadavka **spôsobilosti** je splnená za dodatočného predpokladu na komponenty volebného protokolu uvedeného pod číslom 5 nižšie. Takýto volebný protokol budeme považovať za **bezpečný**.

4.6.2 Predpoklady

V tejto časti stanovíme pre náš volebný protokol predpoklady, ktoré budeme neskôr využívať pri analýze útočných scenárov na volebný protokol, ktorými preukážeme bezpečnosť navrhovaného volebného protokolu. Predpoklady na volebný protokol pre prehľadnosť rozdelíme do niekoľkých skupín podľa subjektov, ktorých sa týkajú.

Predpoklady na kryptografické prvky

1. Medzi volebnou aplikáciou a sieťovým serverom je vytvorený bezpečný komunikačný kanál;
2. Reťazce vygenerované náhodným generátorom sú náhodné a navzájom nezávislé;
3. Schéma pre asymetrické šifrovanie použité vo volebnom protokole je kryptograficky bezpečná¹³;
4. Schéma pre elektronický podpis použitá vo volebnom protokole je kryptograficky bezpečná;

¹³V praxi sa asymetrické šifrovanie väčších objemov dát zvykne nahrádzať symetrickým šifrovaním pomocou náhodne vygenerovaného kľúča, zašifrovaného asymetrickým šifrovaním a odoslaného spolu s pôvodnou správou v takto zašifrovanej podobe

5. Schéma pre slepý elektronický podpis použitá vo volebnom protokole je kryptograficky bezpečná;
6. Schéma na zdieľanie tajomstva použitá vo volebnom protokole je kryptograficky bezpečná.

Predpoklady na účastníkov elektronických volieb

1. Čestný volič používa iba oficiálnu volebnú aplikáciu, má zabezpečené zariadenie, z ktorého hlasuje, snaží sa odovzdať iba platné hlasy a vykonáva všetky kontroly definované vo volebnom protokole.¹⁴ Budeme predpokladať, že podstatná väčšina oprávnených voličov sú čestní voliči;
2. Útočník nedisponuje súkromnými kryptografickými kľúčami určenými na tvorbu elektronického podpisu iných osôb alebo dešifrovanie hlasov (súkromné dešifrovacie kľúče SiS a súkromný dešifrovací kľúč pre aktuálne elektronické voľby)¹⁵;
3. Útočník patrí do skupiny oprávnených voličov a jeho prioritou je ovplyvniť výsledok hlasovania v prospech svojho kandidáta a/alebo zneplatniť prebiehajúce elektronické voľby;
4. Útočník má plný prístup ku komunikácii v sieti Internet;
5. Členovia volebnej komisie konajú samostatne v súlade so schválenými postupmi s cieľom zabrániť zvýhodneniu kandidátov preferovaných ostatnými členmi volebnej komisie nečestným konaním niektorého z kandidátov, voličov alebo členov volebnej komisie;
6. Volebná komisia obsahuje aspoň toľko čestných členov, aby nečestní členovia volebnej komisie nedokázali ani pri vzájomnej kooperácii zrekonštruovať dešifrovacie kľúče.

Predpoklady na komponenty volebného protokolu

1. Implementácie všetkých komponentov zodpovedajú volebnému protokolu a neobsahujú závažné chyby;

¹⁴V prípade, že volič neporozumel niektorým pokynom popisujúcim jeho účasť vo volebnom protokole, požiada kontaktné centrum volebnej komisie o vysvetlenie týchto pokynov.

¹⁵Volič neposkytuje svoj súkromný kľúč slúžiaci na tvorbu elektronického podpisu iným osobám a zodpovedá za jeho bezpečnosť. V prípade jeho kompromitácie volič okamžite požiada o zrušenie platnosti certifikátu elektronického podpisu voliča. Zneužitie kompromitovaného súkromného kľúča môže mať pre voliča rozsiahle právne následky, preto predpokladáme, že každý volič vo vlastnom záujme splní tento predpoklad.

2. Systémy, na ktorých sú implementácie komponentov nasadené, sú spoľahlivé, odolné voči výpadkom a neobsahujú vážne bezpečnostné zraniteľnosti, ktoré by mohli ovplyvniť priebeh volieb;
3. Sieťový server, dočasné úložisko hlasov a sčítací server nepredpokladajú nič o volebnej aplikácii v správe voliča;
4. Poskytovateľ služby časovej pečiatky poskytuje svoje služby spoľahlivo a výhradne komponentom volebného protokolu v správe volebnej komisie;
5. Certifikačná autorita poskytuje svoje služby spoľahlivo a výhradne oprávneným osobám;
6. Každý krok volebného protokolu je realizovaný niektorým z komponentov atomicky;
7. Dáta z každého z komponentov volebného protokolu v správe volebnej komisie sú po ukončení činnosti komponentu nenávratne znehodnotené a odstránené.

Všetky uvedené predpoklady považujeme za splniteľné, avšak vzhľadom na rozsah práce sa ich realizáciou nebudeme v tejto práci zaoberať.

4.6.3 Analýza útočných scenárov

V tejto časti analyzujeme odolnosť navrhovaného volebného protokolu voči skupinám jednotlivým typom útokov, ktoré sme popísali v časti 4.6.1. Odolnosť voči týmto typom útokov odvodíme z tvrdení, ktorých platnosť preukážeme s využitím predpokladov definovaných v predchádzajúcej kapitole. V tejto práci sa nebudeme zaoberať analýzou použitých kryptografických prvkov, ktorých bezpečnostnú analýzu je možné nájsť v mnohých odborných prácach z oblasti kryptológie.

Krádež hlasov

Tvrdenie 1: „Útočník nedokáže vytvoriť platný hlas iného oprávneného voliča“
Tvrdenie vyplýva z nasledujúcich predpokladov:

- schéma pre elektronický podpis je bezpečná (zaručuje autentickosť a integritu podpísaných dát)
- použité kryptografické prvky sú bezpečné
- útočník nemá prístup k súkromným kľúčom voliča
- certifikačná autorita koná v súlade so svojím certifikačným poriadkom¹⁶

¹⁶vydáva certifikáty iba na skutočné meno ich vlastníka, bezdôvodne neruší platnosť certifikátov, vydáva korektné časové pečiatky atď.

Útočník na základe týchto predpokladov nevie vytvoriť platný elektronický podpis oprávneného voliča bez jeho vedomia pre nový hlas v prospech útočníka.

Tvrdenie 2: „Útočník nedokáže upraviť platný hlas iného oprávneného voliča“
Ak by útočník dokázal upraviť platný hlas iného oprávneného voliča tak, aby úspešne zmenil voľbu voliča a zachoval pri tom platnosť elektronického podpisu hlasu, tak útočník by bol schopný vytvoriť platný hlas iného oprávneného voliča, čo je v spore s predchádzajúcim tvrdením.

Tvrdenie 3: „Útočník kontrolujúci komunikačný kanál nedokáže upraviť platné hlasy prenášané z volebnej aplikácie na sieťový server“
Útočník nie je schopný tvoriť elektronický podpis iného oprávneného voliča, nie je schopný dešifrovať 1. ani 3. vrstvu ochrany hlasu a nevie narušiť integritu posielaných dát vzhľadom na predpoklad bezpečného komunikačného kanála. Čestný volič navyše očakáva od sieťového servera odpoveď v špecifickom formáte, ktorej obsah si overuje voči odoslanému hlasu. Útočník za týchto predpokladov nie je schopný aktívneho zapojenia sa do komunikácie medzi volebnou aplikáciou a sieťovým serverom bez odhalenia kompromitácie komunikačného kanála.

Tvrdenie 4: „Útočník nie je schopný odovzdať platný hlas opakovaním staršieho hlasu voliča“
Tvrdenie vyplýva z realizácie fázy spracovania hlasov (viď. časť 4.4.4) v bode 6a a z jedinečnosti kryptografických párov kľúčov pre rozdielne elektronické voľby. V prípade odovzdania odchyteného hlasu voliča z predchádzajúcich volieb nebude hlas na *sčítacom serveri* správne dešifrovaný. Ak útočník odovzdá starší hlas voliča odchytený v priebehu súčasných volieb, *dočasné úložisko hlasov* v bode 6a fázy spracovania hlasov prehlási útočníkom odovzdaný hlas za neplatný a nezarádi ho do zoznamu platných hlasov pre *sčítací server*, ktoré sa podieľajú na výsledku hlasovania.

Tvrdenie 5: „Útočník kontrolujúci sieťový server nedokáže pridať platné hlasy do výsledku“
Platnosť tvrdenia vyplýva z platnosti tvrdení 1 až 4. Ak by bol volič schopný pridať alebo upraviť hlas na sieťovom serveri, ktorý by sa prejavil vo výsledku hlasovania, musel by byť schopný vykonať aj niektorú z činností popisovaných v tvrdeniach 1 až 4.

Tvrdenie 6: „Útočník nedokáže pridať alebo upraviť platné hlasy v priebehu prenosu hlasov medzi sieťovým serverom a dočasným úložiskom hlasov a/alebo medzi dočasným úložiskom hlasov a sčítacím serverom“
Na bezpečný prenos hlasov pomocou fyzických médií dohliada volebná komisia a pozorovatelia. Integrita vstupných dát je porovnávaná s výstupnými

dátami, útočník tak za predpokladu dôveryhodnej volebnej komisie a pozorovateľov nie je schopný upraviť prenášané údaje medzi komponentami volebného protokolu.

Tvrdenie 7: „Útočník s prístupom k dočasnému úložisku hlasov nedokáže pridať platné hlasy do výsledku“

Činnosť dočasného úložiska hlasov je pod neustálou kontrolou členov volebnej komisie a pozorovateľov, útočník tak nie je schopný ani pomocou škodlivého softvéru doplniť množinu platných anonymizovaných hlasov o ďalšie hlasy útočníka bez predchádzajúceho odhalenia volebnou komisiou. Útočník nie je schopný doplniť vstupné dáta pre dočasné úložisko hlasov o nové hlasy z dôvodu platnosti tvrdenia 1.

Tvrdenie 8: „Útočník s prístupom k sčítaciemu serveru nedokáže pridať platné hlasy do výsledku“

Činnosť sčítacieho servera je pod neustálou kontrolou členov volebnej komisie a pozorovateľov, útočník tak nie je schopný ani pomocou škodlivého softvéru doplniť množinu platných anonymizovaných hlasov o ďalšie hlasy útočníka bez predchádzajúceho odhalenia volebnou komisiou.

Znehodnotenie hlasov

Tvrdenie 9: „Útočník s prístupom k ľubovoľnému komponentu v správe volebnej komisie nedokáže selektovať hlasy podľa voliča alebo voľby“

Činnosť dočasného úložiska hlasov a sčítacieho servera je pod neustálym dohľadom volebnej komisie, útočník tak nie je schopný komunikovať s týmito komponentami bez odhalenia členmi volebnej komisie. Ak by tvrdenie neplatilo pre útočníka kontrolujúceho sieťový server, útočník by bol schopný dešifrovať hlasy zašifrované aktuálnym asymetrickým šifrovacím kľúčom sieťového servera, čo je v spore s predpokladmi neznalosti súkromných kľúčov útočníkom a bezpečnosťou použitej schémy pre asymetrické šifrovanie.

Tvrdenie 10: „Útočník kontrolujúci sieťový server nedokáže neodhaliteľne odstrániť platné hlasy“

Odstránenie platných hlasov oprávnených voličov s najväčšou pravdepodobnosťou zapríčiní neobjavenie sa NIH týchto hlasov v zozname spracovaných NIH. Čestní oprávnení voliči v takom prípade podajú sťažnosť volebnej komisii a tá vzhľadom na poskytnuté údaje odhalí kompromitáciu sieťového servera a vyhlási voľby za neplatné. V prípade použitia rovnakého NIH viacerými oprávnenými voličmi sa NIH môže vyskytnúť na zozname spracovaných NIH aj v prípade odstránenia niektorých platných hlasov, ktoré ho obsahujú, čím sa stane útok úspešným. Vzhľadom na predpoklad použitia náhodného generátora NIH je pravdepodobnosť takejto udalosti minimalizovaná, čo vylučuje úspešný útok vo väčšom rozsahu.

Tvrdenie 11: „Útočník kontrolujúci komunikačný kanál alebo prenosové médium medzi jednotlivými komponentami nedokáže neodhaliteľne odstrániť platné hlasy“

Čestný volič očakáva od sieťového servera odpoveď v špecifickom formáte, ktorej obsah si overuje voči odoslanému hlasu. Útočník za tohto predpokladu nie je schopný aktívneho zapojenia sa do komunikácie medzi volebnou aplikáciou a sieťovým serverom bez odhalenia kompromitácie komunikačného kanála. Na bezpečný prenos hlasov pomocou fyzických médií dohliada volebná komisia a pozorovatelia. Integrita vstupných dát je porovnávaná s výstupnými dátami, útočník tak za predpokladu dôveryhodnej volebnej komisie a pozorovateľov nie je schopný upraviť prenášané údaje medzi komponentami volebného protokolu.

Tvrdenie 12: „Útočník kontrolujúci dočasné úložisko hlasov nedokáže neodhaliteľne odstrániť platné hlasy“

Činnosť dočasného úložiska hlasov je pod neustálou kontrolou členov volebnej komisie a pozorovateľov, útočník tak nie je schopný ani pomocou škodlivého softvéru upraviť množinu platných anonymizovaných hlasov o ďalšie hlasy útočníka bez predchádzajúceho odhalenia volebnou komisiou.

Tvrdenie 13: „Útočník kontrolujúci sčítací server nedokáže neodhaliteľne odstrániť platné hlasy“

Činnosť sčítacieho servera je pod neustálou kontrolou členov volebnej komisie a pozorovateľov, útočník tak nie je schopný ani pomocou škodlivého softvéru upraviť množinu platných anonymizovaných hlasov o ďalšie hlasy útočníka bez predchádzajúceho odhalenia volebnou komisiou.

Narušenie anonymity

Tvrdenie 14: „Útočník nevie čítať obsah zašifrovaného hlasu“

Tvrdenie vyplýva z predpokladov bezpečnosti schémy pre asymetrické šifrovanie a neznalosti súkromných kľúčov útočníkom.

Tvrdenie 15: „Útočník s prístupom k dočasnému úložisku hlasov a sčítaciemu serveru nedokáže spárovať platné hlasy s identitou voliča“

Činnosti dočasného úložiska hlasov aj sčítacieho servera sú pod neustálou kontrolou členov volebnej komisie a pozorovateľov, útočník tak nie je schopný ani pomocou škodlivého softvéru získať v priebehu ich behu informácie potrebné pre prepojenie hlasov v otvorenom formáte s identitou oprávnených voličov, ktorí ich odovzdali, bez predchádzajúceho odhalenia volebnou komisiou. Informácie sú po skončení činnosti týchto komponentov bezpečne odstránené z oboch komponentov, útočník preto nemá možnosť získať potrebné informácie ani po ukončení elektronických volieb.

Korupcia a ovplyvňovanie

Tvrdenie 16: „Volič nevie tretej strane dokázať, akým spôsobom hlasoval vo voľbách“

NIH uvedený v zozname spracovaných NIH môže byť úmyselne použitý voličom vo viacerých platných hlasoch odovzdaných voličom v priebehu konania volieb. Z tohto dôvodu tretia strana ani v prípade preukázania podpísaného NIH nevie jednoznačne rozhodnúť, či hlas o ktorom volič tvrdí, že je ten, ktorý odovzdal ako posledný, nebol voličom dodatočne zmenený v prospech iného kandidáta.

Tvrdenie 17: „Útočník s prístupom k dočasnému úložisku hlasov a sčítaciemu serveru nedokáže získať informáciu o poslednom odovzdanom platnom hlase konkrétneho voliča“

Tvrdenie vyplýva z tvrdenia 14 a argumentácie k tvrdeniu 15.

Zrušenie volieb

Tvrdenie 18: „Útočník bez kompromitácie niektorého z komponentov nevie podať sťažnosť, ktorá by bola akceptovaná“

Na vytvorenie akceptovateľnej sťažnosti v zmysle riešenia sťažností útočník potrebuje získať nepoužitú platnú časovú pečiatku a elektronický podpis nespracovaného NIH. Vzhľadom na predpoklady na tvorbu elektronického podpisu a poskytovateľa služby časovej pečiatky nevie útočník získať informácie potrebné pre podanie sťažnosti, ktorá bude akceptovaná volebnou komisiou v zmysle stanovených pravidiel.

Tvrdenie 19: „Útočník s kontrolou sieťového servera a/alebo poskytovateľa služby časovej pečiatky vie podať sťažnosť, ktorá bude akceptovaná“

Útok je možné realizovať napríklad získaním platnej časovej pečiatky s využitím kontroly nad poskytovateľom služby časovej pečiatky a získaním platného slepeho elektronického podpisu pre NIH, ktorý sa nenachádza v žiadnom odovzdanom platnom hlase. Druhá možnosť realizácie útoku využívajúca kontrolu nad sieťovým serverom spočíva v selektívnom odstránení platného hlasu útočníka, na ktorého nespracovanie sa následne bude útočník sťažovať po skončení elektronických volieb.

Tvrdenie 20: „Útočník s kontrolou komunikačného kanála dokáže ovplyvniť dostupnosť elektronického hlasovania“

Volebný protokol v navrhovanej podobe je postavený na centralizovanom riešení. Útočník môže ovplyvniť dostupnosť elektronického hlasovania preťažením komponentov volebného protokolu útokmi typu „DoS“ (Denial of Service). Dopad útokov na dostupnosť elektronického hlasovania je možné minimalizovať štandardnými postupmi (decentralizácia riešenia, zavedenie maximálneho počtu požiadaviek z jedného systému za určitý čas atď.), ktorými sa však nebudeme v tejto práci zaoberať.

Z analýzy vyplýva, že útočník je za istých okolností schopný zneplatniť platný výsledok elektronických volieb, v prípade, že je pre neho nevyhovujúci, a vyvolať tak opakovanie volieb. Riziko zneužitia tejto zraniteľnosti je možné minimalizovať stanovením minimálneho počtu akceptovaných sťažností pre zrušenie elektronických volieb a dodatočným zabezpečením komponentov volebného protokolu pred neoprávneným prístupom. Táto zraniteľnosť však nemá vplyv na bezpečnosť volebného protokolu.

V predchádzajúcej neformálnej analýze bezpečnosti nášho volebného protokolu sme odôvodnili odolnosť nášho navrhovaného volebného protokolu voči útokom popísaným v časti 4.6.1 vo veľkom rozsahu. Navrhovaný volebný protokol teda spĺňa vlastnosti **ideálneho volebného systému s dôveryhodnou autoritou**. Protokol navyše prináša voličovi možnosť **čiasťočnej individuálnej overiteľnosti**, ktorá zvyšuje dôveryhodnosť elektronického hlasovania a minimalizuje možnosti nečestných členov volebnej komisie ovplyvniť výsledok hlasovania v prospech preferovaného kandidáta.

V porovnaní s estónskym protokolom náš navrhovaný volebný protokol vďaka tretej vrstve ochrany hlasu vo forme dodatočného šifrovania neposkytuje útočníkovi možnosť tvorby zoznamu zúčastnených voličov, ktorý môže následne využiť na ovplyvňovanie voličov. Navrhovaný protokol tiež prináša možnosť čiasťočnej individuálnej overiteľnosti, ktorú estónsky volebný protokol neposkytuje.

Hlavnou výhodou nášho volebného protokolu v porovnaní s nórsnym volebným protokolom je okrem zabránenia možnosti tvorby zoznamu zúčastnených voličov aj zabezpečenie čiasťočnej individuálnej overiteľnosti bez potreby dodatočných poštových a SMS kanálov.

Kapitola 5

Implementácia volebného protokolu

Jedným z cieľov našej práce je implementácia vybraného riešenia elektronických volieb. V kapitole 3 sme preskúmali existujúce volebné protokoly pre elektronické voľby cez Internet, na základe ktorých sme v kapitole 4 navrhli vlastný protokol realizujúci elektronické voľby cez Internet a popísali jeho bezpečnostné vlastnosti. V tejto kapitole sa zameriame na konkrétnu implementáciu nášho navrhovaného volebného protokolu, ktorú sme vytvorili pre posúdenie niektorých výkonnostných aspektov navrhovaného riešenia, ktorým sa budeme venovať v závere tejto kapitoly. Zdrojové kódy a skompilované súbory pre platformu Microsoft Windows vytvorené a použité pre potreby tejto diplomovej práce môže čitateľ nájsť na priloženom CD.

Upozornenie: Výslednú implementáciu neodporúčame k okamžitému nasadeniu do reálnej prevádzky vzhľadom na vynechanie niektorých prvkov z volebného protokolu, ktoré nie sú potrebné pre posúdenie výkonnostných aspektov, avšak môžu mať dopad na bezpečnosť použitého riešenia. Jedným z neimplementovaných prvkov je napríklad schéma na zdieľanie tajomstva, ktorú protokol vyžaduje z dôvodu utajenia súkromných dešifrovacích kľúčov. Zoznam neimplementovaných prvkov uvádzame v závere tejto kapitoly.

5.1 Technické parametre

Implementáciu navrhovaného volebného protokolu sme realizovali v jazyku C# pre v súčasnosti najrozšírejšiu rodinu operačných systémov. V tejto časti uvádzame základné parametre našej implementácie – systémové požiadavky, XML schémy prenášaných dátových objektov a použité kryptografické prvky pre dosiahnutie bezpečnostných požiadaviek volebného protokolu.

5.1.1 Systémové požiadavky

Microsoft Windows XP/Vista/7, resp. Windows Server 2003/2008/2008 R2

Microsoft Visual Studio 2010 (pre úpravu zdrojových kódov)

Microsoft .NET Framework 4.0

Externé knižnice

Bouncy Castle C# 1.7

OpenSSL.NET 0.4.3

5.1.2 XML schémy

Zoznam kandidátov a každý hlas voliča bez ohľadu na počet ochranných vrstiev, v ktorých je uložený, sú spracované v našej implementácii volebného protokolu vo formáte XML. V nasledujúcej tabuľke uvádzame základné XML schémy platné pre tieto objekty. Tieto ako aj ďalšie XML schémy používané vo výslednej implementácii sa nachádzajú na priloženom CD v priečinku *eVolby/xmlSchemy*.

<i>Schéma</i>	<i>Popis</i>
candidateListSchema.xsd	zoznam kandidátov
voteBallotSchema.xsd	hlasovací lístok voliča v otvorenom formáte
voteBallotFirstEnvelopeSchema.xsd	hlasovací lístok voliča uloženého do 1. vrstvy (viď. časť 4.4)
voteBallotSecondEnvelopeSchema.xsd	hlasovací lístok voliča uloženého do 1. a 2. vrstvy (viď. časť 4.4)
voteBallotThirdEnvelopeSchema.xsd	hlasovací lístok voliča uloženého do 1., 2. a 3. vrstvy (viď. časť 4.4)
nihSignatureSchema.xsd	elektronický podpis NIH vytvorený sieťovým serverom
timestampSchema.xsd	časová pečiatka pridelená poskytovateľom služby časovej pečiatky

5.1.3 Použité kryptografické prvky

Pri implementácii volebného protokolu sme využívali existujúce implementácie kryptografických schém a algoritmov v knižniciach OpenSSL.NET a Bouncy Castle C#.

Certifikáty pre verejné kľúče

- štandard X.509 v3
- formát DER
- typ verejného kľúča: RSA
- dĺžka verejného kľúča: 4096 bitov
- použitý podpisový algoritmus: RSA-SHA512
- použitá implementácia: OpenSSL.NET 0.4.3

Súkromné kľúče

- formát PEM
- typ súkromného kľúča: RSA
- dĺžka súkromného kľúča: 4096 bitov
- použitý šifrovací algoritmus: AES256-CBC
- použitá implementácia: OpenSSL.NET 0.4.3

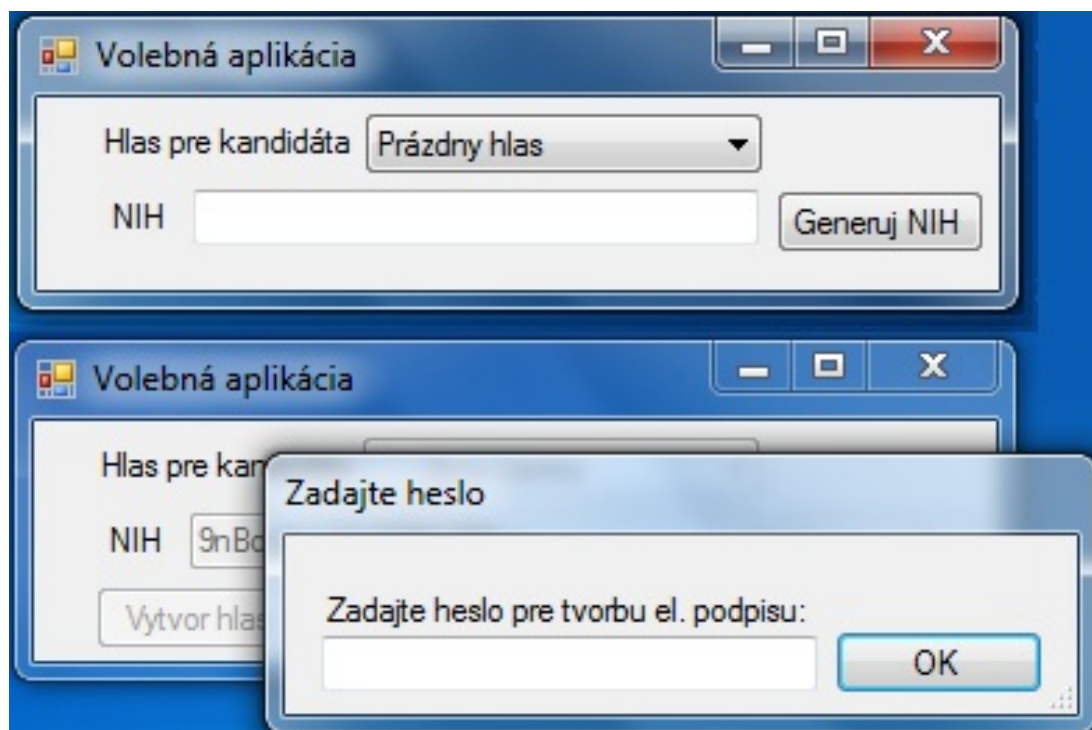
Šifrovanie

- schéma pre asymetrické šifrovanie: RSA-OAEP
- schéma pre symetrické šifrovanie: AES256-CBC (bez zarovnanania)
- použitá implementácia: OpenSSL.NET 0.4.3

Elektronický podpis

- podpisová schéma pre elektronický podpis: RSA-PSS/SHA512
- podpisová schéma pre slepý elektronický podpis: Chaumova RSA schéma pre slepé elektronické podpisy
- použitá implementácia: Bouncy Castle C# 1.7

5.2 Komponenty volebného protokolu



Obr. 5.1: Ukážky grafického rozhrania volebnej aplikácie

5.2.1 Volebná aplikácia

32-bitová spustiteľná verzia: *eVolby\bin\VolebnaAplikacia*

Zdrojové súbory: *eVolby\src\VolebnaAplikacia*

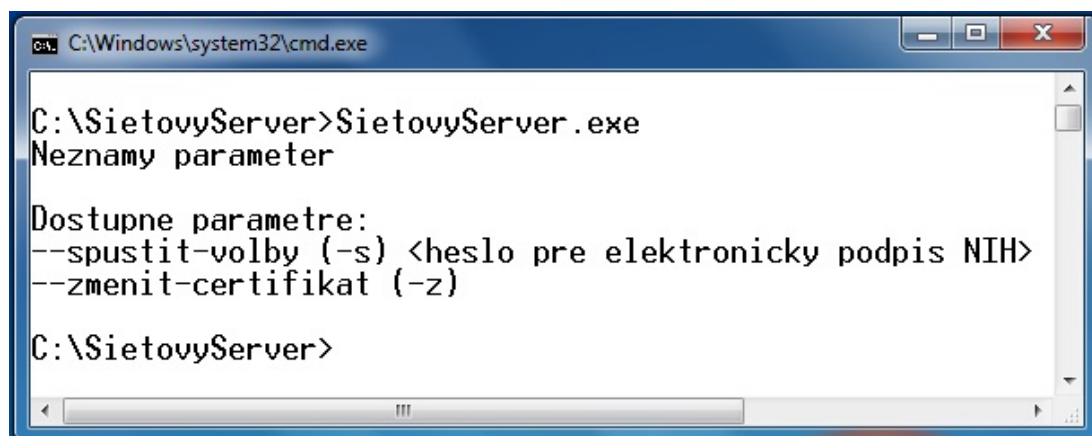
Volebná aplikácia je implementovaná ako samostatne spustiteľná aplikácia s grafickým používateľským rozhraním, ktorá umožňuje voličovi vytvoriť a odovzdať svoj elektronický hlas. Aplikácia sa ihneď po spustení pokúsi získať zoznam kandidátov a certifikáty potrebné pre jej činnosť z *publikačného servera*. Volič postupne vyberie svojho kandidáta, vygeneruje (alebo si zvolí) 20-miestny *NIH*, vyberie súbor s certifikátom pre svoj elektronický podpis, zadá heslo k súkromnému podpisovému kľúču a odošle vytvorený hlas.

- Požiadavky
 - Microsoft Windows XP (a novší);
 - .NET Framework 4.0;

- sieťové pripojenie k *publikačnému serveru* a *sieťovému serveru* (protokol IPv4);
 - platný certifikát s verejným kľúčom elektronického podpisu hlasu voliča vo formáte DER;
 - súkromný podpisový kľúč na tvorbu elektronického podpisu hlasu voliča vo formáte PEM (vyžaduje sa rovnaký názov a umiestnenie ako má príslušný certifikát) a zodpovedajúce heslo.
- Konfiguračný súbor *vaConfig.xml*
 - *candidatesListSchemaFile* – umiestnenie XML schémy zoznamu kandidátov;
 - *voteResponseSchemaFile* – umiestnenie XML schémy odpovede *sieťového servera*;
 - *outputVoteFileName* – umiestnenie posledného hlasu vytvoreného volebnou aplikáciou;
 - *temporaryDirectoryPath* – umiestnenie adresára pre dočasné súbory (končí /);
 - *temporaryOnlineStorageServerAddress* – IP adresa sieťového servera (protokol IPv4);
 - *temporaryOnlineStorageServerPort* – port sieťového servera;
 - *candidatesListUrl* – URL adresa zoznamu kandidátov;
 - *firstEnvelopeEncryptionCert* – URL adresa certifikátu obsahujúceho šifrovací kľúč elektronických volieb;
 - *thirdEnvelopeEncryptionCert* – URL adresa certifikátu obsahujúceho aktuálny šifrovací kľúč *sieťového servera*;
 - *blindSignatureOnlineServerCert* – URL adresa certifikátu elektronického podpisu *sieťového servera* pre slepý elektronický podpis prijatého NIH;
 - *publishingServerTimeout* – maximálna doba odozvy *publikačného servera*.
 - Výstupy aplikácie
 - prijatý podpísaný NIH a sériové číslo prijatej časovej pečiatky;
 - súbor *<názov>.evote* obsahujúci elektronicky podpísaný NIH a príslušnú časovú pečiatku hlasu;
 - informácia o chybe (ak nastala).

- **Dôležité upozornenia**

- Aplikácia vykonáva iba čiastočnú kontrolu elektronicky podpísaného NIH a príslušnej časovej pečiatky po ich prijatí.
- Komunikačný kanál medzi volebnou aplikáciou a sieťovým serverom nie je zabezpečený a žiadna zo strán sa neautentifikuje.



```
C:\Windows\system32\cmd.exe
C:\SietovyServer>SietovyServer.exe
Neznamy parameter

Dostupne parametre:
--spustit-volby (-s) <heslo pre elektronicky podpis NIH>
--zmenit-certifikat (-z)

C:\SietovyServer>
```

Obr. 5.2: Vstupné parametre sieťového servera

5.2.2 Sieťový server

32-bitová spustiteľná verzia: *eVolby\bin\SietovyServer*

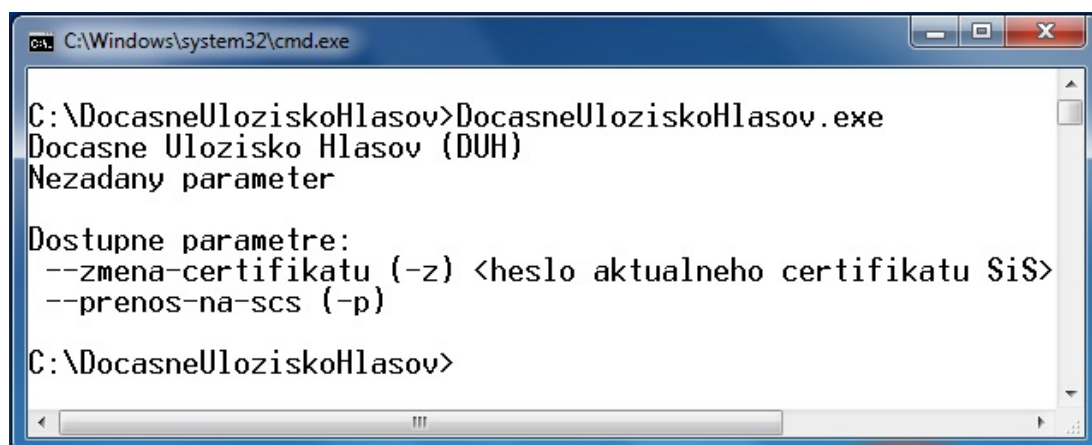
Zdrojové súbory: *eVolby\src\SietovyServer*

Sieťový server je konzolová aplikácia vyžadujúca zadanie jedného zo vstupných parametrov. Aplikácia realizuje rovnomenný komponent podľa návrhu s niekoľkými výnimkami (viď. Dôležité upozornenia nižšie).

- **Požiadavky**

- Microsoft Windows XP (a novší);
- .NET Framework 4.0;
- sieťové pripojenie k *poskytovateľovi služby časovej pečiatky* (protokol IPv4);
- platný certifikát s verejným kľúčom elektronického podpisu NIH vo formáte DER;
- súkromný podpisový kľúč na tvorbu slepého elektronického podpisu NIH vo formáte PEM a zodpovedajúce heslo.

- Konfiguračný súbor *sisConfig.xml*
 - *voteInputSchemaFile* – umiestnenie XML schémy prijatého hlasu;
 - *timestampSchemaFile* – umiestnenie XML schémy časovej pečiatky;
 - *blindSignatureCertificateFile* – umiestnenie certifikátu s verejným kľúčom elektronického podpisu NIH;
 - *blindSignaturePrivateKeyFile* – umiestnenie súkromný podpisový kľúč na tvorbu slepého elektronického podpisu NIH;
 - *onlineTimeStampAddress* – IP adresa poskytovateľa služby časovej pečiatky (protokol IPv4);
 - *onlineTimeStampPort* – port poskytovateľa služby časovej pečiatky;
 - *onlineServerPort* – port sieťového servera.
- Vstupné parametre
 1. `--spustit-volby <heslo> (-s <heslo>)` – spustí sieťový server v režime prijímania hlasov (viď. 4.4.2). Pred prvým spustením je potrebné vytvoriť súbor *Data|maxSavedVotes.toss* s obsahom 1ä súbor *Data|minSavedVotes.toss* s obsahom "0";
 2. `--zmenit-certifikat (-z)` – spustí predspracovanie hlasov na sieťovom serveri (viď. 4.4.3).
- Výstupy aplikácie
 - v prípade spustenia s parametrom 1: adresár *votes* obsahujúci prijaté hlasy;
 - v prípade spustenia s parametrom 2: adresár *votesForTransfer* obsahujúci spermutované prijaté hlasy;
 - informácia o chybe (ak nastala).
- **Dôležité upozornenia**
 - Server vykonáva iba čiastočnú kontrolu obdržanej časovej pečiatky;
 - Server nekontroluje platnosť certifikátov;
 - Komunikačný kanál medzi volebnou aplikáciou a sieťovým serverom nie je zabezpečený a žiadna zo strán sa neautentifikuje;
 - Komunikačný kanál medzi poskytovateľom služby časovej pečiatky a sieťovým serverom nie je zabezpečený a žiadna zo strán sa neautentifikuje.



```
C:\Windows\system32\cmd.exe
C:\DocasneUloziskoHlasov>DocasneUloziskoHlasov.exe
Docasne Ulozisko Hlasov (DUH)
Nezadany parameter

Dostupne parametre:
--zmena-certifikatu (-z) <heslo aktualneho certifikatu SiS>
--prenos-na-scs (-p)

C:\DocasneUloziskoHlasov>
```

Obr. 5.3: Vstupné parametre dočasného úložiska hlasov

5.2.3 Dočasné úložisko hlasov

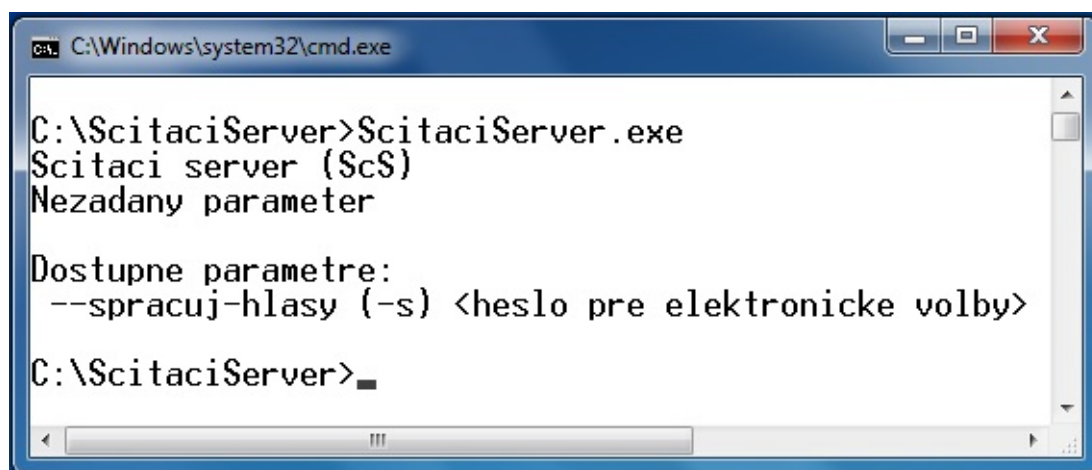
32-bitová spustiteľná verzia: *eVolby\bin\DocasneUloziskoHlasov*

Zdrojové súbory: *eVolby\src\DocasneUloziskoHlasov*

Dočasné úložisko hlasov je konzolová aplikácia vyžadujúca zadanie jedného zo vstupných parametrov. Aplikácia realizuje rovnomerný komponent podľa návrhu s niekoľkými výnimkami (viď. Dôležité upozornenia nižšie). Certifikáty sieťového servera (súbory *.der*) spolu so súkromnými kľúčmi (súbory *.pem*) sú pred prvým zahájením činnosti uložené do adresára *Certs* uložené podľa obráteného poradia platnosti od posledného platného (*1.der*, *1.pem*) po prvý platný aktuálny certifikát sieťového servera, ktorého číslo zodpovedá hodnote v konfiguračnom súbore (viď. nižšie). Navyše všetky hlasy prijaté v období platnosti aktuálneho certifikátu sú manuálne prenesené do priečinka *IncomingVotes*.

- Požiadavky
 - Microsoft Windows XP (a novší);
 - .NET Framework 4.0;
 - zoznam certifikátov sieťového servera vo formáte DER;
 - súkromné podpisové kľúče príslušné k certifikátom sieťového servera vo formáte PEM a zodpovedajúce heslá.
- Konfiguračný súbor *duhConfig.xml*
 - *voteInputSchemaFile* – umiestnenie XML schémy prijatého hlasu;
 - *voteDecryptedSchemaFile* – umiestnenie XML schémy dešifrovaného prijatého hlasu (v 2. vrstve) bez časovej pečiatky;

- *voteDecryptedWithTimeStampSchemaFile* – umiestnenie XML schémy dešifrovaného prijatého hlasu (v 2. vrstve) s časovou pečiatkou;
 - *caRootCertPublicKeyFile* – umiestnenie koreňového certifikátu certifikačnej autority pre overovanie platnosti elektronického podpisu;
 - *totalSisCertificateNumber* – celkový počet certifikátov sieťového servera, ktoré budú použité v neskoršom období, vrátane aktuálneho certifikátu.
- Vstupné parametre
 1. --zmena-certifikatu <heslo> (-z <heslo>) – spustí dočasné úložisko hlasov v režime predspracovania hlasov (viď. 4.4.3);
 2. --prenos-na-scs (-p) – spustí spracovanie hlasov pre sčítací server (viď. 4.4.4)
 - Výstupy aplikácie
 - v prípade spustenia s parametrom 1: adresár *VotesStorage* obsahujúci hlasy dešifrované niektorým z certifikátov sieťového servera podľa protokolu;
 - v prípade spustenia s parametrom 2: adresár *VotesForTransfer* obsahujúci spermutované platné hlasy dešifrované niektorým z certifikátov sieťového servera podľa protokolu a adresár *InvalidVotesForTransfer* obsahujúci spermutované platné hlasy dešifrované niektorým z certifikátov sieťového servera podľa protokolu;
 - informácia o chybe (ak nastala).
 - **Dôležité upozornenia**
 - Server vykonáva iba čiastočnú kontrolu obdržanej časovej pečiatky;
 - Server nekontroluje platnosť certifikátov;
 - Integrita prenosu hlasov zo sieťového servera na dočasné úložisko hlasov nie je overovaná;
 - Zoznamy spracovaných časových pečiatok, časových pečiatok falošných hlasov a hlasov s neplatným formátom nie sú generované.



```
C:\Windows\system32\cmd.exe
C:\ScitaciServer>ScitaciServer.exe
Scitaci server (ScS)
Nezadany parameter

Dostupne parametre:
--spracuj-hlasy (-s) <heslo pre elektronicke volby>
C:\ScitaciServer>
```

Obr. 5.4: Vstupné parametre sčítacieho servera

5.2.4 Sčítací server

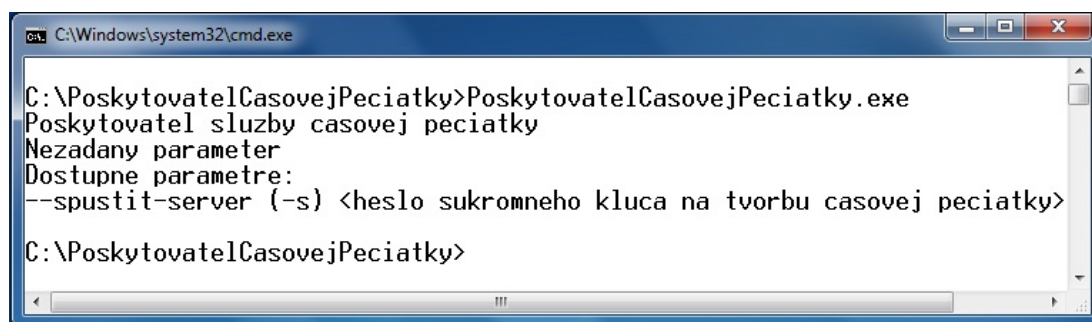
32-bitová spustiteľná verzia: *eVolby\bin\ScitaciServer*

Zdrojové súbory: *eVolby\src\ScitaciServer*

Sčítací server je konzolová aplikácia realizujúca rovnomenný komponent podľa návrhu s niekoľkými výnimkami (viď. Dôležité upozornenia nižšie). Všetky platné hlasy z adresára *VotesForTransfer* dočasného úložiska hlasov sú manuálne prenesené do priečinka *Data\IncomingVotes* a neplatné hlasy z adresára *InvalidVotesForTransfer* dočasného úložiska hlasov sú manuálne prenesené do priečinka *Data\IncomingInvalidVotes*.

- Požiadavky
 - Microsoft Windows XP (a novší);
 - .NET Framework 4.0;
 - súkromný dešifrovací kľúč pre aktuálne elektronické voľby a zodpovedajúce heslo.
- Konfiguračný súbor *scsConfig.xml*
 - *voteInputSchemaFile* – umiestnenie XML schémy preneseného hlasu;
 - *voteDecryptedSchemaFile* – umiestnenie XML schémy hlasu v otvorenom formáte;
 - *voteEncryptedSchemaFile* – umiestnenie XML schémy preneseného hlasu v 1. vrstve;

- *candidateListSchemaFile* – umiestnenie XML schémy zoznamu kandidátov;
 - *candidateListFile* – umiestnenie zoznamu kandidátov;
 - *evotingKey* – umiestnenie súkromného dešifrovacieho kľúča elektronických volieb vo formáte PEM;
 - *votesDir* – priečinok s platnými hlasmi z dočasného úložiska hlasov;
 - *invalidVotesDir* – priečinok s neplatnými hlasmi z dočasného úložiska hlasov;
 - *resultsFile* – súbor s výsledkami elektronického hlasovania;
 - *processedNIHFile* – súbor s usporiadaným zoznamom spracovaných NIH.
- Vstupný parameter
 1. `--spracuj-hlasy <heslo> (-s <heslo>)` – spustí sčítací server v režime spracovania hlasov (viď. 4.4.4).
- Výstupy aplikácie
 - výsledky elektronického hlasovania;
 - usporiadaný zoznam spracovaných NIH;
 - informácia o chybe (ak nastala).
- **Dôležité upozornenia**
 - Integrita prenosu hlasov dočasného úložiska hlasov na sčítací server nie je overovaná;
 - Zoznamy spracovaných časových pečiatok, časových pečiatok falošných hlasov a hlasov s neplatným formátom nie sú generované.



```
C:\Windows\system32\cmd.exe
C:\PoskytovatelCasovejPeciatky>PoskytovatelCasovejPeciatky.exe
Poskytovatel sluzby casovej peciatky
Nezadany parameter
Dostupne parametre:
--spustit-server (-s) <heslo sukromneho kluca na tvorbu casovej peciatky>
C:\PoskytovatelCasovejPeciatky>
```

Obr. 5.5: Vstupné parametre poskytovateľa služby časovej pečiatky

5.2.5 Poskytovateľ služby časovej pečiatky

32-bitová spustiteľná verzia: *eVolby\bin\PoskytovatelCasovejPeciatky*

Zdrojové súbory: *eVolby\src\PoskytovatelCasovejPeciatky*

Sčítací server je konzolová aplikácia realizujúca rovnomenný komponent podľa návrhu s niekoľkými výnimkami (viď. Dôležité upozornenia nižšie).

- Požiadavky
 - Microsoft Windows XP (a novší);
 - .NET Framework 4.0;
 - sieťové pripojenie k *sieťovému serveru* (protokol IPv4);
 - platný certifikát s verejným kľúčom na tvorbu elektronických časových pečiatok vo formáte DER;
 - súkromný podpisový kľúč na tvorbu elektronických časových pečiatok vo formáte PEM a zodpovedajúce heslo.
- Konfiguračný súbor *pcpConfig.xml*
 - *tempOnlineStorageServerAddress* – IP adresa *sieťového servera*;
 - *onlineServerPort* – port *poskytovateľa služby časovej pečiatky*;
 - *timestampCert* – umiestnenie certifikátu s verejným kľúčom na tvorbu elektronických časových pečiatok;
 - *timestampCertPrivateKey* – umiestnenie súkromného podpisového kľúča na tvorbu elektronických časových pečiatok.
- Vstupný parameter
 1. `--spustit-server <heslo> (-s <heslo>)` – spustí poskytovateľa služby časovej pečiatky v režime spracovania hlasov (viď. 4.4.2).

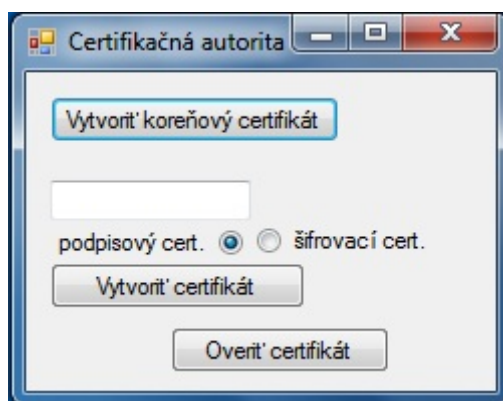
- Výstupy aplikácie
 - časová pečiatka pre obdržané dáta;
 - informácia o chybe (ak nastala).
- **Dôležité upozornenie:** Komunikačný kanál medzi poskytovateľom služby časovej pečiatky a sieťovým serverom nie je zabezpečený a žiadna zo strán sa neautentifikuje.

5.2.6 Publikačný server

Publikačný server pre potreby tejto diplomovej práce realizujeme prostredníctvom existujúcich webových serverov (napr. Apache). Server poskytuje volebnej aplikácii nasledovné informácie:

- zoznam kandidátov;
- certifikát obsahujúci šifrovací kľúč elektronických volieb;
- certifikát obsahujúci aktuálny šifrovací kľúč *sieťového servera*;
- certifikát elektronického podpisu *sieťového servera* pre slepý elektronický podpis prijatého NIH.

Dôležité upozornenie: Integrita a autentickosť poskytovaných hlasov nie je zabezpečená.



Obr. 5.6: Ukážky grafického rozhrania jednoduchkej certifikačnej autority

5.2.7 Jednoduchá certifikačná autorita

32-bitová spustiteľná verzia: *eVolby\bin\JednoduchaCertifikacnaAutorita*

Zdrojové súbory: *eVolby\src\JednoduchaCertifikacnaAutorita*

Pre potreby testovania výkonnostných aspektov implementovaného riešenia sme tiež vytvorili jednoduchú aplikáciu na vytváranie koreňového certifikátu, podpisových certifikátov voličov a certifikátov slúžiacich pre potreby šifrovania.

- Požiadavky
 - Microsoft Windows XP (a novší);
 - .NET Framework 4.0;
- Výstupy aplikácie
 - vytvorené certifikáty a príslušné súkromné kľúče v priečinku *cert* (názvy súborov zodpovedajú sériovému číslu príslušného certifikátu);
 - informácia o chybe (ak nastala).
- **Dôležité upozornenia:**
 - všetky súkromné kľúče sú chránené heslom „heslo“;
 - platnosť všetkých certifikátov je 1 rok od ich vydania s výnimkou koreňového certifikátu, ktorého platnosť je 8 rokov od jeho vydania.

5.3 Výkonnostné aspekty

Nad implementáciou uvedenou v predchádzajúcich častiach sme vykonali sériu výkonnostných testov s cieľom odhaliť výkonnosť volebných komponentov a „úzke hrdlá“ vo volebnom protokole, teda miesta, ktoré majú najväčší vplyv na výkonnosť systému. Aby sme nasimulovali podmienky elektronického hlasovania, vygenerovali sme pomocou *jednoduchej certifikačnej authority* jeden koreňový certifikát, jeden certifikát elektronických volieb, jeden aktuálny certifikát sieťového servera, jeden certifikát pre elektronický podpis NIH a 1000 certifikátov pre elektronické podpisy voličov, ktoré sme následne použili na vytvorenie 1000 platných a 1000 neplatných elektronických hlasov, ktoré sme za účelom skúmania dĺžky spracovania komponentami volebného protokolu nechali jeden po druhom spracovať jednotlivými komponentami na našom testovacom zariadení. Výsledky sme merali pomocou upravených komponentov volebného protokolu, ktoré s presnosťou približne 10ms zaznamenali čas zahájenia a čas ukončenia spracovania hlasov. Z výsledného rozdielu časov sme následne vypočítali priemerný čas spracovania jedného odovzdaného hlasu a maximálny počet hlasov spracovateľných za 24 hodín v prípade sériového spracovania hlasov.

5.3.1 Konfigurácia testovacej zostavy

Vzhľadom na implementáciu bez podpory behu vo viacerých vláknoch (s výnimkou poskytovateľa služby časovej pečiatky a časti sieťového servera sprostredkujúceho prijatie hlasu do systém) a potreby minimalizácie oneskorení vyplývajúcich zo sieťovej komunikácie sme ako testovacie zariadenie zvolili počítač vybavený 4 jadrovým procesorom a novou inštaláciou operačného systému s minimálnou množinou spustených aplikácií. Pre každý komponent volebného systému sme vyhradili jedno jadro procesora a spustili ho s maximálnou prioritou. Konfigurácia testovacieho počítača, na ktorom sme realizovali výkonnostné testy, bola nasledovná:

- procesor AMD FX-4100 (4 jadrá, 12MB cache, 3.6GHz, hardvérová podpora AES inštrukcií)
- operčná pamäť 4GB DDR3 1333MHz CL9
- pevný disk Western Digital Caviar Green (Serial ATA 300, 5400rpm, 16MB cache)
- operačný systém Microsoft Windows 7 Professional SP1 (64-bit)

5.3.2 Výsledky

<i>Fáza volebného protokolu</i>	<i>Celkový čas testu</i>	<i>Priemerný čas na 1 hlas</i>	<i>Počet hlasov za 24 hod.</i>
Vytvorenie certifikátov	1 h 3 min. 11 s	3,791 s	22 790
Odozdanie hlasu Časť 4.4.2 (1000 platných hlasov)	1 h 23 min. 54 s	5,034 s	17 163
Odozdanie predvytvoreného hlasu (1000 platných hlasov)	52 min. 4 s	3,124 s	27 656
Sieťový server - časť 4.4.3 (1000 platných hlasov)	5,008 s	0,005 s	17 280 000
Dočasné úložisko hlasov Časť 4.4.3 (1000 platných hlasov)	59,046 s	0,059 s	1 464 406
Dočasné úložisko hlasov Časť 4.4.4 (1000 platných hlasov)	7,894 s	0,008	10 800 000
Sčítací server - časť 4.4.4 (1000 platných hlasov)	43,898 s	0,044 s	1 963 636
Sčítací server - časť 4.4.4 (1000 neplatných hlasov)	44,226 s	0,044 s	1 963 636
Sčítací server - časť 4.4.4 (1000+1000 platných hlasov)	1 min. 29,513 s	0,045 s	1 920 000

Výsledky výkonnostných testov (uvedené v tabuľke vyššie) naznačujú, že najpomalšou časťou volebného protokolu je vytvorenie a odovzdanie hlasu. V prípade 30-dňového hlasovania po vzore estónskeho riešenia a za predpokladu rovnomernej distribúcie odovzdávania hlasov je testovacia zostava schopná prijať viac ako 800 tisíc hlasov, ktorých úplné výsledky vrátane zoznamu spracovaných Náhodných Identifikátorov Hlasu (NIH) budú známe približne 10 hodín¹ po ukončení hlasovania.

¹Priebeh testovania naznačuje, že samotné výsledky hlasovania (zoznam kandidátov s výsledným počtom hlasov) sú známe približne po 30% uplynutého času výpočtu a zvyšný čas je využitý na tvorbu zoznamu spracovaných NIH. Teda výsledky elektronických volieb s 800 tisíc odovzdanými hlasmi budú dostupné najneskôr už 3 hodiny po ukončení hlasovania

Tieto výsledky vzhľadom na niektoré neimplementované časti protokolu² obsahujú nepresnosti, avšak spolu s poznatkami z implementovania volebného protokolu poskytujú prehľad o výkonnostných aspektoch riešenia a približných očakávateľných časoch trvania jednotlivých fáz volebného protokolu, ktorý zhrnieme nasledujúcimi optimistickými tvrdeniami:

- **Spracovania platného a neplatného hlasu si vyžadujú približne rovnaký čas**

Žiaden komponent volebného systému s výnimkou *sčítacieho servera* nevie rozlíšiť, či volič odovzdal svoj hlas alebo do troch ochranných vrstiev vložil iba náhodné údaje, preto musí ku každému hlasu spĺňajúcemu definovaný formát pristupovať ako k platnému hlasu, čo zvyšuje riziko **hrozby zahltania** komponentov volebného systému neplatnými údajmi, ktoré zvyšujú potrebu na úložný priestor, výpočtový výkon a najmä čas potrebný na spracovanie výsledkov elektronických volieb. Toto riziko a jeho dopady je možné minimalizovať napríklad nasledovnými opatreniami:

- paralelizácia vybraných častí jednotlivých komponentov
- použitie výkonných serverov
- zavedenie progresívneho minimálneho časového intervalu medzi odovzdaním dvoch hlasov z rovnakého zariadenia (s výnimkou zabezpečených zariadení, napríklad počítačov vo volebných miestnostiach)
- vytvorenie heuristiky, ktorej cieľom je určiť a obmedziť zariadenie alebo voliča pokúšajúceho sa o zahltanie volebných komponentov

- **Súčasnú bežne dostupnú hardvérovú vybavenie postačuje na realizáciu elektronických volieb navrhovaným volebným protokolom**

Realizovaná implementácia naznačuje možnosť úspešného použitia navrhovaného volebného protokolu pri realizácii volieb v menšom meradle aj na bežne dostupných zariadeniach. V prípade predpokladu nižšieho počtu neplatných hlasov je možné pomocou testovacej zostavy (uvedenej v časti 5.3.1) v cene zhruba 400 Eur realizovať elektronické voľby nielen v menších komunitách ale aj na dedinách a v menších mestách.

²Vid'. upozornenia pri jednotlivých komponentoch volebného protokolu v časti 5.2

Na záver tejto kapitoly uvádzame zoznam neimplementovaných častí volebných komponentov, ktoré sme v rámci testovania možností a výkonnosti navrhovaného protokolu nezahrnuli do implementácie:

- bezpečný komunikačný kanál medzi *volebnou aplikáciou* a *sieťovým serverom*;
- bezpečný komunikačný kanál medzi *sieťovým serverom* a *poskytovateľom služby časovej pečiatky*;
- *volebná aplikácia*: overovanie prijatých dát;
- *sieťový server*: pravidelné preverovanie platnosti aktuálneho certifikátu sieťového servera;
- *dočasné úložisko hlasov*: overenie platnosti časovej pečiatky pri predspracovaní hlasu;
- *dočasné úložisko hlasov*: overenie platnosti certifikátov elektronických podpisov voliča v čase pridelenia časovej pečiatky – kontrola pôvodnej platnosti podpisových certifikátov a zoznamu CRL;
- *dočasné úložisko hlasov*: tvorba zoznamov časových pečiatok falošných hlasov a zoznamu spracovaných časových pečiatok;
- *dočasné úložisko hlasov, sčítací server*: overenie autenticity a integrity prijatých dát na spracovanie;
- *dočasné úložisko hlasov, sčítací server*: implementácia a použitie schém na zdieľanie tajomstva;
- elektronické podpísanie všetkých zverejňovaných dát pri ich vzniku.

Uvedené neimplementované časti volebného protokolu nemajú zásadný vplyv na výsledky výkonnostných testov, avšak z bezpečnostných dôvodov ich odporúčame doplniť do implementácie pred jej použitím v reálnych voľbách.

Záver

Realizovať elektronické voľby cez Internet alebo ponechať existujúce a rokmi overené riešenie vo forme papierových volieb? Toto bola hlavná otázka, na ktorú sme v rámci našej diplomovej práce hľadali odpoveď. Po úvodnom oboznámení sa s možnými triedami útokov na volebné systémy (časť 2.1.2), preskúmaní všetkých vlastností, ktoré požadujeme od vhodného volebného systému (časť 2.1.3), a popise priebehu hlasovania vo voľbách v Slovenskej republike (časť 2.1.4) sme získali ucelený prehľad o aktuálnom stave klasických „papierových“ volieb a požiadavkách, ktoré musíme klásť aj na prípadné elektronické riešenie realizácie volieb. V rámci uvedených častí diplomovej práce sme definovali ideálny volebný systém s dôveryhodnou autoritou, ktorý zdá sa poskytuje z pohľadu súčasných požiadaviek a skúseností voliča minimálnu množinu záruk, ktorú musí ľubovoľný volebný systém spĺňať, aby ho volič považoval za dôveryhodný a bol ochotný sa zúčastniť volieb.

V ďalšej časti sme sa rozobrali možnosti elektronizácie volieb. Stanovili sme niekoľko úrovní postupnej elektronizácie smerujúcej k úplnému nahradeniu všetkých procesov klasických papierových volieb procesmi elektronických volieb (časť 3.1). Následne sme sa podrobnejšie venovali jednej neúspešnej (projekt SERVE) a niekoľkým úspešným realizáciám elektronických volieb vo vybraných krajinách (Estónsko, Nórsko, Švajčiarsko) (časť 3.2). Preskúmali sme vlastnosti volebných protokolov týchto krajín a poukázali na možné následky zneužitia niektorých zraniteľností predmetných volebných protokolov.

Na základe poznatkov získaných zo štúdia existujúcich riešení elektronických volieb sme v kapitole 4 predstavili návrh nového volebného protokolu pre realizáciu elektronických volieb cez Internet. Volebný protokol sme postavili na úspešnom estónskom modeli, rozšírili sme ho o ďalšiu úroveň ochrany pred útokmi na „online“ komponenty volebného protokolu a voličovi sme pre zvýšenie dôveryhodnosti volebného protokolu a väčšej miere kontroly nad priebehom spracovania hlasov poskytli možnosť čiastočnej individuálnej overiteľnosti.

Navrhovaný volebný protokol sme následne podrobili neformálnej bezpečnostnej analýze, v ktorej sme odôvodnili bezpečnosť navrhovaného protokolu, a na jeho základe implementovali realizáciu volebného protokolu pre potreby posúdenia výkonnostných aspektov navrhovaného riešenia. Napriek tomu, že výsledná implementácia volebného protokolu nenapĺňa niektoré body z navrhovaného protokolu, ktoré sme z hľadiska primárneho cieľa vytvárania implementácie (posúdenie výkonnostných aspektov protokolu) nepovažovali za dôležité zahrnúť do finálneho riešenia, je za istých okolností a stanovených predpokladov pripravená na použitie vo voľbách v menších komunitách.

Výkonnostné testy (časť 5.3) nám tiež poskytli zaujímavé poznatky o „úzkych hrdlách“ navrhovaného riešenia najmä v súvislosti s pomerom neplatných hlasov k celkovému počtu hlasov, ktoré poukazujú na potrebu skúmania možností odhalenia neplatných hlasov a pokusov o zahltenie volebných komponentov v pokiaľ možno čo najskoršej fáze spracovania hlasov. Napriek uvedeným skutočnostiam výkonnostné testy priniesli zaujímavé poznatky o možnostiach realizácie elektronických volieb na aktuálne dostupných zariadeniach. Výkonnostné testy ukázali, že neparalelizovaná implementácia volebného protokolu na komponentov realizovaných na bežne dostupných osobných počítačoch so zaobstarávacou cenou približne 400 Eur je schopná efektívne realizovať elektronické voľby pre menšie komunity s rádovo tisíckami oprávnených voličov. Tento poznatok spolu s výsledkami neformálnej bezpečnostnej analýzy naznačujú z technického pohľadu optimistickú odpoveď na našu hlavnú otázku.

Realizovať elektronické voľby cez Internet alebo ponechať existujúce a rokmi overené riešenie vo forme papierových volieb? Výsledky našej práce na túto otázku odpovedajú jednoznačne v prospech elektronických volieb. Je potrebné si však uvedomiť, že realizácia elektronických volieb na úrovni niektorých z celoštátnych volieb v Slovenskej republike je citlivou témou a vyžaduje si množstvo ďalšej práce pred zahájením samotnej implementácie a pilotnej prevádzky elektronických volieb. Pokračovanie tejto diplomovej práce vidíme napríklad vo vytvorení formálnej bezpečnostnej analýzy navrhovaného volebného protokolu, návrhu volebných komponentov pre použitie vo veľkých komunitách alebo v komplexnej štúdií uskutočniteľnosti elektronických volieb v Slovenskej republike, ktorou sa zaoberá kolega Juraj Danko vo svojej diplomovej práci [Dan12].

Literatúra

- [AA] Mart Oruaas Jaan Priisalu-Anto Veldre Jan Willemsen Kaur Virunurm Arne Ansper, Ahto Buldas. E-voting conception security: analysis and measures.
- [BM07] Ahto Buldas and Triinu Mägi. Practical security analysis of e-voting systems. In *Proceedings of the Security 2nd international conference on Advances in information and computer security, IWSEC'07*, pages 320–335, Berlin, Heidelberg, 2007. Springer-Verlag.
- [Com] Estonian National Electoral Committee. E-voting system: General overview.
- [Dan] Juraj Danko. Elektronické vol'by a ich vybrané parametre. *Zborník ŠVK 2011*, pages 305–316.
- [Dan12] Juraj Danko. Štúdia uskutočniteľnosti elektronických volieb. Master's thesis, Fakulta matematiky, fyziky a informatiky, Univerzita Komenského v Bratislave, 2012.
- [DRH] Ulrich Ultes-Nitsche Dr. Rolf Haenni, Dr. Eric Dubuis. Research on e-voting technologies.
- [fDIR] Office for Democratic Institutions and Human Rights. Norway internet voting pilot project local government elections 12 september 2011: OSCE/ODIHR election expert team report.
- [FHH10] Piotr Faliszewski, Edith Hemaspaandra, and Lane A. Hemaspaandra. Using complexity to protect elections. *Commun. ACM*, 53(11):74–82, November 2010.
- [Gjo10] Kristian Gjosteen. Analysis of an internet voting protocol. *IACR Cryptology ePrint Archive*, pages 380–380, 2010.
- [MVO96] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

- [oG] State Chancellery of Geneva. Uncovering the veil on Geneva's internet voting solution.
- [rep] Vláda Slovenskej republiky. Uznesenie vlády Slovenskej republiky č. 675 z 19. 10. 2011 k návrhu Organizačno-technického zabezpečenia volieb do Národnej rady Slovenskej republiky v roku 2012.
- [RG] Andreas Bogk Dirk Engling Hannes Mehnert Frank Rieger Pascal Scheffers Barry Wels Rop Gonggrijp, Willem-Jan Hengeveld. Nedap/Groenendaal ES3B voting computer.
- [Rub04] Dr Aviel Rubin. A security analysis of the secure electronic registration and voting experiment (SERVE) january 21, 2004 Dr. David Jefferson, 2004.