UNIVERZITA KOMENSKÉHO V BRATISLAVE

FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

ŠTÚDIA USKUTOČNITEĽNOSTI ELEKTRONICKÝCH VOLIEB

Diplomová práca

2012

Bc. Juraj Danko

UNIVERZITA KOMENSKÉHO V BRATISLAVE

FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

ŠTÚDIA USKUTOČNITEĽNOSTI ELEKTRONICKÝCH VOLIEB

Diplomová práca

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

Bratislava, 2012

Bc. Juraj Danko

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

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

Názov: Štúdia uskutočniteľnosti elektronických volieb

Cieľ: Analyzovať podmienky (právne, technické, bezpečnostné) realizácie elektronických volieb v SR.

Vedúci: doc. RNDr. Daniel Olejár, PhD.
Katedra: FMFI.KI - Katedra informatiky

Dátum zadania: 02.11.2010

Dátum schválenia: 03.11.2010

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

.....
študent

.....
vedúci práce

Ďakujem vedúcemu svojej diplomovej práce, doc. RNDr. Danielovi Olejárovi, PhD., za pomoc pre realizácii tejto zaujímavej témy a efektívnu snahu pomôcť pri jej skúmaní. Táto práca by ďalej nikdy nenadobudla súčasný stav a kvalitu bez pomoci konzultácií kryptologických riešení s RNDr. Martinom Stanekom, PhD. a RNDr. Petrom Gažim, PhD. Výraznou pomocou pri chápaní širšieho pohľadu na svet elektronických volieb boli konzultácie Mgr. Marcela Martinkoviča, PhD. a pragmatický pohľad na technickú realizovateľnosť, ktorý mi poskytol p. Ivan Debnár.

Abstrakt

Autor:	Bc. Juraj Danko
Názov diplomovej práce:	Štúdia uskutočniteľnosti 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:	108 strán
Bratislava, máj 2012	

Demokratické voľby sú spoločnosťou oprávnene vnímané ako základ modernej demokracie. Procedúry na ich vykonávanie sú výsledkom dlhodobého vývoja a ovplyvnené podmienkami a prostredím krajiny, v ktorej sú realizované. Aj preto je ich uskutočňovanie náročné po organizačnej i ekonomickej stránke. Dnes značne silnejú snahy o informatizáciu, a teda zefektívnenie fungovania spoločnosti pomocou informačných a komunikačných technológií. Proces informatizácie však neznamená iba zavedenie počítačov do systému, ale aj výrazné zmeny v procesoch, ktorými sa tieto aktivity riadia. Informatizácia spoločnosti sa v posledných rokoch výrazne dotkla aj volieb, či už v Estónsku, USA, Nórsku alebo Švajčiarsku; o elektronických voľbách sa však stále častejšie rozpráva aj u nás. Ukazuje sa, že ide o komplexný a zložitý problém; potrebné je riešiť množstvo kryptologických, technických, organizačných, bezpečnostných, legislatívnych, psychologických či ekonomických otázok. V štúdii uskutočniteľnosti elektronických volieb podávame kompaktný, formálny a ucelený pohľad na realizáciu elektronických volieb na Slovensku. V jej prvej časti analyzujeme proces volieb a preverujeme, ktoré procesy a za akých podmienok by bolo možné elektronizovať. Popisujeme tiež široké spektrum rôznorodých požiadaviek, ktoré sú na voľby kladené. Podrobne analyzujeme najmä bezpečnostné požiadavky, pretože práve bezpečnosť je predpokladom dôveryhodnosti elektronických volieb. Ďalej analyzujeme možnosti, ako tieto požiadavky realizovať. V práci analyzujeme predpoklady a súčasný stav problematiky, a to ako v praxi nasadené protokoly, tak i teoretické schémy, pri ktorých preverujeme, ako vyhovujú bezpečnostným a iným požiadavkám. Tieto sa odzrkadľujú v návrhu riešenia využívajúcom kryptografický protokol založený na prístupe a realizácii využívanom v estónskom modeli elektronických volieb. Na základe zistení navrhujeme upravený model elektronických volieb a analyzujeme ho z hľadiska ISO noriem 15408 a radu štandardov 27000. Napokon dokazujeme, že navrhnutý model je uskutočniteľný i prakticky a odha-

dujeme náklady spojené s jeho implementáciou. V závere potom sumarizujeme otvorené problémy a uvádzame námety pre ďalšie skúmanie.

Kľúčové slová: Elektronické voľby, štúdia uskutočniteľnosti, e-government, informačná bezpečnosť a manažment.

Abstract

Author:	Bc. Juraj Danko
Title:	Electronic voting feasibility study
University:	Comenius University in Bratislava
Faculty:	Faculty of Mathematics, Physics and Informatics
Department:	Department of Computer Science
Advisor:	doc. RNDr. Daniel Olejár, PhD.
Page count:	108 pages

Bratislava, 2012

Democratic elections are legitimately acknowledged by the society as the basis of the modern democracy. The procedures of the elections realization are derived from a long-term process, and highly dependent on the conditions in the respective country of their realization. For that reason is the execution of the elections quite a complex issue in both organizational and economic views. Nowadays, the attempts to informatize, and thereby to improve the effectiveness of the society using the information and communication technologies is strongly rising. However, the informatization cannot be reduced to utilization of computers by the system; further changes in the processes that drive the respective activities should be considered. The informatization has significantly affected the elections as well recently; e.g. in Estonia, USA, Norway, and Switzerland; and, interestingly, the electronic elections are more and more often discussed also in Slovakia. Seemingly, the electronization of the elections is a quite complex and complicated issue; several cryptological, technical, organizational, security, legal, psychological, and economical questions have to be discussed or solved. Our feasibility study on the electronic voting delivers a compact, formal, and complex description of the electronic elections realization in Slovakia.

In the first part, the voting process has been analyzed and conditions for respective processes electronization have been determined. Additionally, a wide range of requirements on the elections has been listed. As the security is the precondition of the electronic voting credibility, a deep analysis of the security requirements has been provided. Furthermore, the possibilities of the requirements realization have been analyzed.

The current state of art side-by-side with the presumptions of the existing protocols, both used in practice, and the theoretical schemes, have been examined to determine the fulfillment of security and non-security requirements. These are further reflected on the proposed voting scheme, which implements a cryptographic protocol based on the Estonian

electronic voting protocol approach. According to the findings, a modified electronic voting scheme has been proposed, and further analyzed using the ISO/IEC 15408 and ISO/IEC 27000 series standards. Finally, a proof of the practical usefulness of the protocol has been provided, and the expected implementation expenses have been estimated. In the conclusion, opened problems and further examination recommendations have been stated.

Keywords: Electronic voting, feasibility study, e-government, information security and management.

Predhovor

Problematika elektronických volieb sa dostala do širokého povedomia verejnosti najmä v posledných rokoch. Využívanie elektronických služieb v bankovníctve, komerčnej sfére, ale aj prvé lastovičky v štátnej správe prinášajú cenné skúsenosti s implementáciou takýchto riešení, ako aj zvyšujú dôveru ľudí v ich bezpečnosť a spoľahlivosť. Voľby sú v modernej spoločnosti bodom, na ktorý sa pozeráme ako na záruku demokratického vývoja; je teda dôležité zabezpečiť, aby ich prípadná elektronizácia bola vykonaná dôkladne a zodpovedne. Preto prichádzame so štúdiou uskutočniteľnosti elektronických volieb na Slovensku; začiatkom úspešnej realizácie je vždy dôsledný a dôkladný návrh, ktorý vychádza zo širokej a dostatočne hlbokej znalosti problematiky. Návrhom technických riešení pre elektronické voľby sa kryptológovia na celom svete zaoberajú už zo desať rokov, ale všeobecne nasaditeľný a uznávaný protokol sa dodnes neobjavil. Pokúsme sa teda vyjsť zo špecifického slovenského prostredia a priniesť návrh, ktorý bude nielen bezpečný a implementovateľný s použitím primeraných zdrojov, ale aj čo najjednoduchší a najtransparentnejší, pretože iba tak možno získať dôveru širokej verejnosti, že elektronické voľby prinášajú najviac výhod práve voličom, a to za akceptovateľnú cenu.

Ochranné známky

Obsah

Zoznam obrázkov

Úvod

Myšlienka elektronizácie ako takej je v našej spoločnosti aktuálnou už niekoľko posledných rokov. Trend digitalizácie a zjednodušovania práce prostredníctvom využitia výpočtovej techniky vykazuje v našej geografickej šírke rapídny rast predovšetkým po nežnej revolúcii, keď nie len občania ako takí, ale aj zahraniční obchodníci či inverstori čoraz častejšie poukazujú na možnosti inovácií a spružnenia služieb prostredníctvom elektronickej komunikácie i v štátnej správe. Pokračovaním týchto snáh o zvyšovanie komfortu a kvality služieb poskytovaným štátom občanom je aj elektronické hlasovanie či elektronické voľby.

Základnými dôvodmi pre elektronizáciu všeľudových hlasovaní sú predovšetkým vyššia dostupnosť, transparentnosť a dlhodobé zníženie nákladov. Ako sa ukazuje v poslednom období i u nás, dobre navrhnuté a implementované systémy v digitálnom svete dokážu pri vhodnom zaobchádzaní poskytnúť pokročilé možnosti prehľadu a kontroly, ktoré môžu viesť i k zníženiu priestoru pre nekalú súťaž či korupciu. Príkladom môžu byť napríklad internetové aukcie na verejné obstarávanie. Vyspelé možnosti identifikácie a autentifikácie umožňujú rozšíriť existujúce prostriedky a pozdvihnúť ich na vyššiu úroveň. Dostupnosť prostredníctvom elektronického kontaktu tiež potenciálne môže znamenať zvýšenie záujmu istých skupín obyvateľstva, ktoré súčasné prostriedky považujú za nepohodlné či neefektívne. Ak podobné riešenia umožnia i šetrenie prostriedkov nás všetkých, rozhodne sa oplatí zaoberať možnosťou ich realizácie.

Problém elektronických volieb však neriešime ako prví; fungujúci príklad možno nájsť v Estónsku [23], kde systém úspešne funguje už niekoľko rokov. Tiež pokročilé kryptografické protokoly uvedené napríklad v [20], [37] či [5] poskytujú silné teoretické zázemie, ktoré analyzujeme už v práci [18] a v kapitole 4 tejto práce a ktoré v časti 5 využijeme na návrh protokolu vhodného pre podmienky Slovenska. Tieto podmienky a obmedzenia, či legislatívne alebo technické, uvádzame a na základe existujúcej legislatívy analyzujeme v kapitole 2. Ukazuje sa však, že pojem elektronizácie volieb je pomerne široký a je potrebné vymedziť, ktoré časti volieb budeme elektronizovať. Spolu s vysvetlením základných kryptologických primitív používaných v návrhu protokolu sa týmto otázkam venujeme v

kapitole 3.

Z ľudskej povahy však často vyplýva skôr skepsa ako nadšenie z nových spôsobov vykonávania bežných činností. Nepochybne, pri nekorektnom alebo nedôslednom návrhu elektronické riešenia dokážu spôsobiť v systéme viac chaosu, pochybností a strachu. Aj preto je dôležité, aby podobné systémy boli pod drobnohľadom odbornej obce, akademických komunít, ale aj širokej verejnosti. Nepochybne dôležitým z hľadiska akceptovania systému verejnosťou, ako aj optimálneho využívania verejných zdrojov je analyzovať a optimalizovať náklady na realizáciu elektronických volieb; odhad jednorázových i opakovaných nákladov uvádzame v kapitole 6.

Vychádzajúc z uvedených domnienok, pokúsime sa v tejto práci podať pohľad na elektronické voľby z rôznych zaujímavých hľadísk, predovšetkým však z hľadiska informatického. Informačná bezpečnosť a systém riadenia kvality je dnes jadrom návrhu a používania každého informačného systému. S využitím noriem série ISO 9000, ISO 27000 a ISO 15408 načrtneme odporúčané spôsoby manažérstva kvality a riadenia informačnej bezpečnosti v kapitole 7. Uvidíme však, že pre šírku záberu sa nezaobídeme bez ďalších analýz pridružených oblastí, ako odboru práva, politológie a sociológie.

Z dôvodu návrhového štádia systému sa však v práci nezaoberáme úplnou analýzou podľa uvedených štandardov a noriem. Tiež nebudeme uvádzať implementačné detaily navrhnutého riešenia; možno ich však nájsť v práci [8], ktorá dotvára štúdiu uskutočniteľnosti a uvádza príklad realizácie navrhnutého protokolu.

Štúdia uskutočniteľnosti elektronických volieb nie je určená iba akademickej obci zaoberajúcej sa zvolenou problematikou. Práca slúži i ako podporný materiál v prípade reálnej implementácie či navrhnutého alebo iného zvoleného protokolu pre elektronické voľby na Slovensku alebo v krajine s podobnými legislatívnymi, spoločenskými a technickými podmienkami, a to najmä pre spoločnosti zapojené do vývoja a integrácie systému. Okrem technických analýz v kapitole 4 čitateľovi práca umožňuje porozumenie i bez hlbších znalostí v oblastiach matematiky a kryptológie; v prípade potreby je však možné vysvetlenia používaných kryptografických primitív nájsť napríklad v publikácii [2].

Elektronické voľby sú v posledných mesiacoch populárnou témou na rôznych spoločenských úrovniach. Ak by sme však mali pristúpiť k ich reálnemu nasadeniu na Slovensku, bolo by potrebné vyriešiť mnoho problémov a zodpovedať početné otázky. Dúfame, že táto práca poslúži nielen k definovaniu toho, čo je potrebné ďalej riešiť, ale niektoré riešenia i načrtne či priblíži.

Kapitola 1

Používané skratky, značky a pojmy

V tejto časti zhrnieme často využívané skratky, pojmy, definície a označenia, ktoré budeme v práci ďalej využívať.

- **Autorita**
  Pod autoritou budeme rozumieť subjekt alebo objekt určený na vykonávanie danej činnosti. Autoritu zvyčajne považujeme za dôveryhodnú a naším cieľom je dosiahnuť stav, v ktorom potrebujeme čo najmenej dôveryhodných autorít

- **GCD**
  Najväčší spoločný deliteľ (z anglického greatest common divisor)

- **Hash**
  Haš, charakteristika, odtlačok vstupných dát; pre naše potreby budeme pod hashom rozumieť deterministickú funkciu s pevnou dĺžkou výstupu. Hašovacia funkcia nie je prosté zobrazenie, zobrazuje veľkú množinu vstupov na relatívne malú množinu krátkych výstupov

- **IKT**
  Informačné a komunikačné technológie

- **Konvenčné voľby**
  V našich podmienkach pod konvenčnými voľbami rozumieme voľby v podobe, v akej prebiehajú podľa platnej slovenskej legislatívy dnes; jedinou zmenou je, že konvenčné voľby nevylučujú inú, dodatočnú možnosť hlasovania

- **mod**
  Celočíselný zvyšok po delení; $8(mod(3)) = 2$

- **Nástenka**

  Pod nástenkou (originálny pojem v angličtine: *bulletin board*) rozumieme ľubovoľné médium, ktoré je všeobecne dostupné na čítanie. Na nástenku môže ľubovoľný účastník zapisovať, a to iba na mieste, ktoré je pre neho vyhradené. Žiadne údaje zapísané na nástenke však nemožno mazať ani modifikovať. Nástenku teda možno považovať za verejný kanál s pamäťou

- **OSN**

  Organizácia Spojených Národov; internetové stránky organizácie dostupné k 6.4.2012: `https://www.un.org/`

- **Symbol $\in_R$**

  Zápis $x \in_R M$ označuje náhodný výber prvku x z množiny M

- **Threshold systém**

  Threshold systém je schéma alebo systém, v ktorej vystupuje parameter (threshold), ktorý zvyčajne určuje jej prah, odolnosť. Ako príklad môže slúžiť schéma na zdieľanie tajomstva (t, n), kde threshold t znamená, že je potrebných aspoň t z n účastníkov na vyskladanie daného tajomstva. V slovenčine by bolo možné použiť ekvivalentné slovo prah, prahový systém; avšak, pre zaužívanie označenia prebraného z angličtiny budeme v práci používať spojenie threshold systém

- **Volič, oprávnený volič**

  Pod voličom rozumieme subjekt, ktorý sa zúčastňuje volieb. Vo voľbách odovzdáva hlas. Oprávnený volič je volič, ktorý spĺňa všetky zákonné náležitosti, a má teda právo voliť v daných voľbách.

Kapitola 2

Voľby a Slovensko

Voľby sú základným stavebným kameňom demokracie nie len moderného západného typu. Vzhľadom na rozdielnu kultúru, stupeň vývoja spoločnosti a iné lokálne podmienky voľby na Slovensku sú, podobne ako v ostatných demokraticky riadených krajinách, špecifické a ich priebeh je upravený pravidlami a nariadeniami, ktoré boli dlhodobo vytvárané našimi zákonodarcami, právnikmi a náladami v spoločnosti. V tejto kapitole predstavíme aktuálnu verziu slovenských volebných zákonov a vysvetlíme princípy ich fungovania. Širší prehľad volebných systémov, príklady a dôvody ich použitia, ako aj detaily ich vykonávania možno nájsť v [7].

2.1 Profil volieb na Slovensku

Vzhľadom na špecifickú správnu štruktúru a rôzne typy zodpovedných orgánov na jednotlivých úrovniach územnej správy a samosprávy na Slovensku, i voľby do jednotlivých týchto orgánov prebiehajú rôznymi spôsobmi.

2.1.1 Súvisiaca legislatíva a volebné systémy

Pri analýze volieb sa okrem technických, organizačných, spoločenských, politických či bezpečnostných problémov a otázok stretávame aj s nemenej relevantnými otázkami právnymi. Príprava elektronických volieb vyžaduje analýzu, a nepochybne i nevyhnutné úpravy existujúcej legislatívy. Okrem vymenovania relevantných právnych predpisov uvedieme i popis príslušných volebných systémov či modelov a vysvetlíme spôsoby výpočtu výsledkov jednotlivých typov volieb.

- **Ústava Slovenskej republiky**
  Ústava sa k voľbám vyjadruje v nasledovných článkoch:

  – Článok 30 - pojednáva o práve voliť

  – Článok 69 - pojednáva o voľbách do obecných zastupiteľstiev a vyšších územných celkov

  – Články 73 a 74 - pojednávajú o voľbách do Národnej rady Slovenskej republiky

  – Článok 101 - pojednáva o voľbe prezidenta; priamo určuje, že kandidáta navrhujú poslanci alebo občania v petícii, a to "na základe petície podpísanej najmenej 15 000 občanmi" [27]; v závislosti od výkladu slova "podpísanej" možno usudzovať, že by malo byť možné uplatniť vyhlášku [26] a zákon [28] a použiť na podpísanie zaručený elektronický podpis; v opačnom prípade by tento článok pred elektronizáciou petícií bolo nutné modifikovať

  Na základe uvedeného možno usudzovať, že okrem formy vykonania petície ústava elektronické hlasovanie vo voľbách neobmedzuje.[1]

- **Zákon č. 564/1992 Zb. o spôsobe vykonania referenda**
  Nebudeme sa zaoberať dôvodmi a spôsobmi vyhlásenia referenda, keďže nie sú pre túto štúdiu relevantné; pre ďalšiu analýzu a prípadnú elektronizáciu referenda je však dôležitá formálna štruktúra referenda a jednotlivých otázok. Podľa §1 odseku 4 zákona [30] musia byť otázky formulované tak, aby na ne bolo možné jednoznačne odpovedať "áno" alebo "nie"; otázky nesmú byť navzájom podmienené.

  Výsledky referenda sa určia v dvoch krokoch; platnosť referenda je podmienená postačujúcou účasťou oprávnených voličov a jeho výsledok nadpolovičnou väčšinou hlasov.

- **Zákon č. 331/2003 Z.z. o voľbách do Európskeho parlamentu**
  Podľa §23 zákona [31] volič vo voľbách do Európskeho parlamentu volí podobne ako vo voľbách do NrSr; vyberie 1 (jeden) hlasovací lístok zvolenej strany alebo koalície, kde označí najviac 2 (dvoch) kandidátov[2]; v ďalšom budeme takéto označovanie kandidátov nazývať **preferenčný hlas**.

  Výpočet výsledkov a prideľovanie mandátov sa riadi §33 a §34 príslušného zákona.

[1] Tiež pripomíname, že prípadná zmena Ústavy vyžaduje dvojtretinový konsenzus poslancov Národnej rady Slovenskej republiky; takáto zmena by mala získať podporu naprieč celým politickým spektrom

[2] teda 0 až 2 kandidátov

- **Zákon č. 333/2004 Z.z. o voľbách do Národnej rady Slovenskej republiky**
  Voľby do Národnej rady Slovenskej republiky možno považovať za pre ďalší vývoj krajiny najdôležitejšie[3], ako aj najkomplikovanejšie spomedzi volieb a všeľudových hlasovaní, ktoré sú na Slovensku vykonávané. Podľa §30 zákona [32] volič, podobne ako vo voľbách do Európskeho parlamentu, zvolí práve 1 (jeden) hlasovací lístok, na ktorom môže označiť najviac 4[4] kandidátov preferenčným hlasom.

  Výsledky volieb sa počítajú podľa Hagenbach-Bischoffovej[5] metódy.

- **Zákon č. 346/1990 Zb. o voľbách do orgánov samosprávy obcí**
  Voľby do orgánov samospráv pozostávajú z 2 (dvoch) častí, ktoré je možné pre potreby spracovania hlasovania rozdeliť na 2 (dve) samostatné fázy, a to:

  – Voľby do obecného (mestského) zastupiteľstva, v ktorých volič označí na hlasovacom lístku "najviac taký počet kandidátov, aký má byť v príslušnom volebnom obvode zvolený"[6]

  – Voľby starostu obce (primátora), v ktorých volič označí jedného z kandidátov

  Podľa §44 sú za poslancov zvolení kandidáti, ktorí získali v danom volebnom obvode najvyšší počet hlasov. Ak nastane rovnosť hlasov kandidátov, rozhoduje ich poradie na kandidátnej listine politickej strany; ak však poradie takto určiť nie je možné[7], poradie sa určí žrebom. Podľa rovnakého paragrafu je za starostu zvolený kandidát s najvyšším počtom hlasov; v prípade rovnosti hlasov sa voľby opakujú.

- **Zákon č. 303/2001 Z.z. o voľbách do orgánov samosprávnych krajov a o doplnení Občianskeho súdneho poriadku**
  Voľby do zastupiteľstva prebiehajú podľa [34] obdobne ako voľby do obecného (mestského) zastupiteľstva (viď vyššie), voľby predsedu samosprávneho kraja prebiehajú obdobne ako voľba starostu obce (primátora) (viď vyššie).

  Určenie poslancov zastupiteľstva je zhodné s určením poslancov vo voľbách do orgánov samosprávy obcí. Voľba predsedu môže prebiehať v dvoch kolách, a to nasledovne:

[3] keďže ide o voľbu do zákonodarného úradu
[4] teda 0 až 4
[5] Hagenbach-Bischoff, švajčiarsky matematik a fyzik (1833 - 1910)
[6] [33], §31, odsek 4
[7] teda ide o kandidátov rôznych politických strán alebo o nezávislých kandidátov

  - V prvom kole je za predsedu zvolený kandidát, ktorý získal nadpolovičnú väčšinu platných hlasov
  - V druhom kole, teda ak žiaden kandidát nadpolovičnú väčšinu platných hlasov nezískal, občania volia z dvoch kandidátov s najvyšším počtom hlasov a víťazom sa stáva ten, ktorý získa v druhom kole viac hlasov; pri rovnosti sa voľby opakujú.

- **Zákon č. 46/1999 Z.z. o spôsobe voľby prezidenta Slovenskej republiky, o ľudovom hlasovaní o jeho odvolaní a o doplnení niektorých ďalších zákonov**
  Voľba prezidenta Slovenskej republiky podľa [36], §21, pozostáva z označenia práve jedného kandidáta voličom.

  Podľa §30 a §31 prebieha voľba prezidenta opäť v dvoch kolách, a to nasledovne:

  - V prvom kole je za prezidenta zvolený kandidát, ktorý získal nadpolovičnú väčšinu platných hlasov
  - V druhom kole, teda ak žiaden kandidát nadpolovičnú väčšinu platných hlasov nezískal, občania volia z dvoch kandidátov s najvyšším počtom hlasov a víťazom sa stáva ten, ktorý získa v druhom kole viac hlasov.

2.1.2 Formalizácia a kategorizácia volieb a hlasovaní

Možno zhliadnuť, že ako referendum, tak i jednotlivé voľby sú vo svojej podstate výberom z niekoľkých možností uskutočňovaným daným subjektom (voličom). Pri voľbe prezidenta ide o výber 1 z niekoľkých možností, pri voľbe do zastupiteľstiev k z l možností, a podobne. Teraz vytvoríme formálny matematický aparát a vyjadríme v ňom exaktne pojmy týkajúce sa volieb a hlasovania uvedené vo vyššie spomenutých zákonoch.

- **Referendum**
  Referendum sa vykonáva podľa modelu, ktorý budeme ďalej označovať

  $$(K : L) \times x$$

  kde K je počet možných volieb voliča pre danú otázku, L počet možných výberov (teda pri referende 2, "áno" alebo "nie") a x počet otázok.

- **Voľby do Európskeho parlamentu**
  Voľby do Európskeho parlamentu sú realizáciou modelu volieb, ktorý budeme ďalej

označovať

$$1 : K : L$$

kde 1 predstavuje výber 1 z K kandidátnych listín, na ktorom preferenčným hlasom volič zvolí najviac $L = 2$ kandidátov. Výpočet výsledkov a prideľovanie mandátov možno vyjadriť nasledovne:

1. Určí sa republikové volebné číslo (λ)

   $\sigma = \#$politických strán alebo koalícií, ktoré získali aspoň 5% platných hlasov

   $\gamma_i = \#$platných hlasov odovzdaný pre stranu alebo koalíciu i

   $$\mu = \text{počet mandátov}$$
   $$\lambda = \left\lfloor \frac{\sum_{i=0}^{\sigma} \gamma_i}{\mu + 1} + 0.5 \right\rfloor$$

2. Predbežné rozdelenie mandátov politickým stranám a koalíciám (Ξ); prvé skrutínium

   $\Xi[i] = \#$mandátov predbežne pridelených i-tej politickej strane alebo koalícii

   Platí:

   $$0 < i \leq \sigma$$
   $$\sum_{i=0}^{\sigma} \Xi[i] = \mu$$

   Potom:

   $$\Xi[i] = \left\lfloor \frac{\gamma_i}{\lambda} \right\rfloor$$

   Označme tiež zvyšky po delení:

   $$\Omega[i] = \frac{\gamma_i}{\lambda} - \Xi_i$$

3. Dodatočné (finálne) prerozdelenie mandátov (Ψ); druhé skrutínium
   Označme zoradenú množinu strán alebo koalícií s najmenším zvyškom Ω.

   $$\Lambda = \{i | \forall j \in N, j \leq \sigma : \Omega[i] \leq \Omega[j]\}$$

   Finálne prerozdelenie:

   $$\sum_{i=0}^{\sigma} \Xi_i = \mu + 1 \Rightarrow$$

$$|\Lambda| = 1 \Rightarrow \lambda = \Lambda[0]$$

$$|\Lambda| > 1 \Rightarrow \Lambda_t = \{i | \forall j \in \Lambda : \gamma_i \geq \gamma_j\}$$

$$|\Lambda_t| = 1 \Rightarrow \lambda = \Lambda_t[0]$$

$$|\Lambda_t| > 1 \Rightarrow \text{o odobratí mandátu rozhodne žreb}$$

$$\sum_{i=0}^{\sigma} \Xi_i < \mu \Rightarrow \text{zvyšné mandáty sa stranám alebo koalíciám prerozdelia}$$

$$\text{podľa najväčšieho } \Omega$$

- **Voľby do Národnej rady Slovenskej republiky**
  Voľby do Národnej rady Slovenskej republiky opäť aplikujú model $1 : K : L$, kde 1 predstavuje výber 1 z K kandidátnych listín, na ktorom preferenčným hlasom volič zvolí najviac $L = 4$ kandidátov. Prejdime k výpočtu výsledkov volieb. Označme najprv:

  $$\gamma[i] = \#\text{ platných hlasov odovzdaný pre stranu alebo koalíciu } i$$

  Pre jednoduchosť uvažujme, že sú počty hlasov zoradené od najvyššieho po najnižší (zostupne). Následne sa určia strany a koalície, ktorým budú mandáty pridelené. V prvom kroku sú zvolené strany a koalície nasledovne:

  - Politické strany, ktoré získali aspoň 5% z celkového počtu platných hlasov
  - Koalície zložené z 2 alebo 3 politických strán, ktoré získali aspoň 7% z celkového počtu platných hlasov
  - Koalície zložené z aspoň 4 politických strán, ktoré získali aspoň 10% z celkového počtu platných hlasov

  Ak by tieto požiadavky nesplnila žiadna politická strana ani koalícia, podľa §42 sa príslušné percentuálne hranice znížia o 1%, teda mandáty budú prerozdelené medzi aspoň dve politické strany a/alebo koalície, ktoré:

  - Politické strany, ktoré získali aspoň 4% z celkového počtu platných hlasov
  - Koalície zložené z 2 alebo 3 politických strán, ktoré získali aspoň 6% z celkového počtu platných hlasov

– Koalície zložené z aspoň 4 politických strán, ktoré získali aspoň 9% z celkového počtu platných hlasov

Ďalej označme:

$$n = \text{počet strán/koalícií, ktorým budú pridelené mandáty}$$

$$votes = \sum_{i=0}^{n} \gamma[i]$$

Prikročme k formalizácii výpočtu výsledkov volieb:

– Výpočet republikového volebného čísla (λ)

$$\lambda = \left\lfloor \frac{votes}{151} + 0.5 \right\rfloor$$

– Predbežné rozdelenie mandátov politickým stranám a koalíciám (Ξ); prvé skrutínium

$\Xi[i] = \#\text{mandátov predbežne pridelených } i\text{-tej politickej strane alebo koalícii}$

$$\Xi[i] = \left\lfloor \frac{\gamma[i]}{\lambda} \right\rfloor$$

Označme tiež zvyšky po delení:

$$\Omega[i] = \frac{\gamma[i]}{\lambda} - \Xi_i$$

– Dodatočné (finálne) prerozdelenie mandátov (Ψ); druhé skrutínium
Označenie strany alebo koalície s najmenším zvyškom Ω:

$$\Lambda = \{i | \forall j \in N, j \leq \sigma : \Omega[i] \leq \Omega[j]\}$$

Finálne prerozdelenie:

$$\sum_{i=0}^{\sigma} \Xi_i = \mu + 1 \Rightarrow$$

$$|\Lambda| = 1 \Rightarrow \lambda = \Lambda[0]$$

$$|\Lambda| > 1 \Rightarrow \Lambda_t = \{i | \forall j \in \Lambda : \gamma_i \geq \gamma_j\}$$

$$|\Lambda_t| = 1 \Rightarrow \lambda = \Lambda_t[0]$$

$$|\Lambda_t| > 1 \Rightarrow \text{o odobratí mandátu rozhodne žreb}$$

$$\sum_{i=0}^{\sigma} \Xi_i < \mu \Rightarrow \text{zvyšné mandáty sa stranám alebo koalíciám prerozdelia}$$

$$\text{podľa najväčšieho } \Omega$$

- **Voľby do orgánov samosprávy obcí**
  Voľby do obecného (mestského) zastupiteľstva spadajú do kategórie volebných modelov, ktoré budeme označovať

  $$K : L$$

  kde K predstavuje počet volených kandidátov[8] a L celkový počet kandidátov. Voľby starostu obce (primátora) sú voľbami spadajúcimi do modelu $K : L$, kde $K = 1$. Takýto model budeme označovať aj ako model

  $$1 : L$$

  kde L je celkový počet kandidátov.

- **Voľba prezidenta Slovenskej republiky**
  Voľba prezidenta sa riadi modelom

  $$1 : L$$

  kde L predstavuje počet kandidátov.

Ukazuje sa, že každý z uvedených modelov ($1 : L$, $K : L$, $1 : K : L$, $(K : L) \times x$) možno teoreticky konvertovať na všeobecný $1 : L$ model. Konverzia pozostáva z vytvorenia samostatnej možnosti[9] pre každú potenciálnu voľbu. Napríklad, model $K : L$, kde volič vyberá práve K z L možných kandidátov, by sme teda na všeobecný model $1 : L$ previedli vytvorením možnosti pre každú K-ticu. Vo voľbách do Národnej rady Slovenskej republiky, v ktorých by volič vyberal z 20 hlasovacích lístkov a na každom z nich by bolo 150 kandidátov, znamenalo by to po prevode do všeobecného $1 : L$ modelu[10]:

$$L = \binom{20}{1} \sum_{i=0}^{4} \binom{150}{i}$$

[8] Teda 0 až počet určený príslušným nariadením

[9] L v tomto univerzálnom modeli teda nepredstavuje kandidáta; predstavuje abstraktnejší pojem *možnosť*

[10] Uvedená konverzia je využívaná pri implementácii niektorých volebných protokolov v elektronických voľbách; nami navrhnutý protokol však toto zjednodušenie nevyžaduje

$$L = \binom{20}{1}\left[\binom{150}{0} + \binom{150}{1} + \binom{150}{2} + \binom{150}{3} + \binom{150}{4}\right]$$

$$L = 416,458,020$$

Na zakódovanie uvedeného počtu možností by sme potrebovali rádovo:

$$B = log_2(416,458,020b)$$

$$B \approx 29b$$

Teda na zakódovanie všetkých možností voľby by sme potrebovali 29 bitov.

Tiež sa ukazuje, že legislatíva riadiaca voľby na Slovensku je pomerne rozsiahla a komplikovaná; aj preto je vítaná iniciatíva jednotného volebného zákona, ktorý by priniesol jednoduchší a priamočiarejší pohľad na voľby. Jednotný volebný zákon by mal predovšetkým objasniť nejasnosti v existujúcich volebných zákonoch a zjednotiť či zjednodušiť parametre volieb, ktoré sú mimo rámec tejto práce, ako je napríklad obmedzenie predvolebnej kampane.

Kapitola 3

Elektronizácia volieb a kryptografia

Vychádzajúc z analýzy volieb, ktorú sme vykonali v kapitole 2, prikročíme ku skúmaniu možností elektronizácie volieb a popisu základných kryptografických štruktúr, ktoré elektronizáciu umožnia.

Pre našu analýzu elektronických volieb budú dôležité z hľadiska kryptografie najmä nasledujúce pojmy:

- Identifikácia a autentifikácia voliča
- Volebná aplikácia a zabezpečenie klientských PC
- Bezpečný komunikačný kanál
- Kryptografické zabezpečenie hlasu voliča (získaných dát)
- Spracovanie (prijatie, overenie, zaevidovanie, dešifrovanie) hlasu voliča
- Spočítavanie hlasov a vyhodnocovanie volieb
- Riešenie dodatočných sťažností
- Zabezpečenie požadovaných vlastností elektronických volieb

Tu uvedeným a niektorým ďalším vybraným problémom sa budeme venovať v nasledujúcich statiach.

3.1 Ciele a potenciálny prínos elektronizácie volieb

Informatizácia vo verejnej správe sľubuje zjednodušenie a zefektívnenie širokého spektra formálnych procesov, ako i zvýšenie pohodlia pre občana ako účastníka týchto procesov.

Potenciálne tiež otvára možnosť zvýšenia účasti občana na verejnom živote, a to práve vďaka zvýšeniu jeho pohodlia. Požiadavka elektronizácie verejného života je i prirodzeným pokračovaním úspešne prebiehajúcej elektronizácie súkromnej sféry nášho života. Okrem priamych či nepriamych prínosov je však potrebné zvážiť i náklady na elektronizáciu, ako aj organizačný rozmer a náročnosť organizačných opatrení, ktoré stoja na druhej miske váh oproti prebiehajúcemu procesu informatizácie spoločnosti, ktorá umožňuje vykonávať množstvo rôznorodých aktivít elektronicky, prostredníctvom IKT. Tu sa prirodzene vynára otázka elektronizácie volieb. Voľby sú prostriedkom, pomocou ktorého občan - volič realizuje svoje právo rozhodovať o veciach verejných formou voľby zástupcov[1]. Vďaka existujúcemu riešeniu v Estónsku[23] a prebiehajúcim pilotným projektom v Nórsku, Holandsku či Švajčiarsku, ktorým sa vo svojej práci [8] venuje kolega Filip Vojtko, je táto teoretická cesta podopretá skúsenosťami a požiadavkami praxe.

Stanovenie cieľov a metód merania stupňa ich dosiahnutia nám ďalej umožní analyzovať a vyhodnocovať systém elektronických volieb navrhnutý v časti 5 tejto práce. Selekcia cieľov a parametrov pre elektronizáciu volieb prebiehala na základe dlhodobého výskumu a porovnávania ako akademických článkov zaoberajúcich sa danou problematikou, tak v praxi nasadzovaných a testovaných systémov.

- **Zachovanie bezpečnosti hlasovania vo voľbách**
  Cieľom elektronizácie volieb je jednoznačne ich zefektívnenie. Dôležité je však súčasné zachovanie ďalších požiadaviek, najmä úrovne ich bezpečnosti. Ďalej sa budeme zaoberať možnosťami elektronizácie volieb, analýze bezpečnostných požiadaviek a hľadaním bezpečnostných mechanizmov, ktorými by sa dali pri jednotlivých riešeniach príslušné bezpečnostné požiadavky naplniť; budeme tiež posudzovať úroveň bezpečnosti, ktorú poskytujú, ale aj skúmať bezpečnostné a iné problémy, ktoré pri ich použití vznikajú.

- **Zníženie ceny volieb z dlhodobého hľadiska**
  Vzhľadom na masívne náklady, ktoré si vyžaduje nasadenie moderného a rozsiahleho informačného systému, ktorý bude tvoriť nevyhnutnú technickú infraštruktúru elektronických volieb, nie je možné očakávať priamočiare zníženie nákladov na voľby v krátkodobom meradle. Vzhľadom na pomerne hustý výskyt udalostí vo volebnom kalendári však má praktický význam i analýza zníženia nákladov na voľby z dlhodobého pohľadu (viac ako 10 rokov), na ktoré sa počiatočné náklady môžu rozložiť (ale i napriek tomu budú náklady zaťažené údržbou a modernizáciou celého systému).

[1] zastupiteľská demokracia

Ďalší priestor pre úsporu prostriedkov predstavuje i možnosť využitia systému alebo jeho častí v ďalších sférach verejného života.

Úspešnosť znižovania dlhodobých nákladov budeme prezentovať na odhadoch a analýzach nákladov na zavedenie, údržbu, ďalší vývoj, ako aj prevádzku volieb po elektronizácii, v časti 6.1.1.

- **Zvýšenie dostupnosti volieb voličom**
  Prostredníctvom elektronického hlasovania je možné zvýšiť potenciálny okruh voličov okrem iného aj zvýšením dostupnosti volieb, a to umožnením hlasovania z ľubovoľného počítača pripojeného do siete Internet (ako ukážeme v časti 3.2.5) alebo z ľubovoľného kontaktného bodu podľa štruktúry popísanej v časti 3.2.3.

  Úspešnosť takejto snahy je podmienená masívnou celospoločenskou diskusiou moderovanou odbornými kruhmi, ako aj širokým a komplexným informovaním verejnosti o zvolenom modeli a jeho implementácii, výhodách a rizikách či problémoch.

- **Zvýšenie stupňa informatizácie spoločnosti**
  Vedľajším efektom elektronických volieb bude nepochybne i nárast počítačovej gramotnosti, informatického a bezpečnostného povedomia; okrem iného by totiž informačná kampaň o elektronických voľbách vzdelávala širokú populáciu o princípoch počítačov, Internetu, ako i informačnej bezpečnosti, čo nepochybne môže prispieť k zlepšeniu porozumenia informačným technológiám vo veľkej časti spoločnosti.

3.2 Potenciálne možnosti elektronizácie volieb

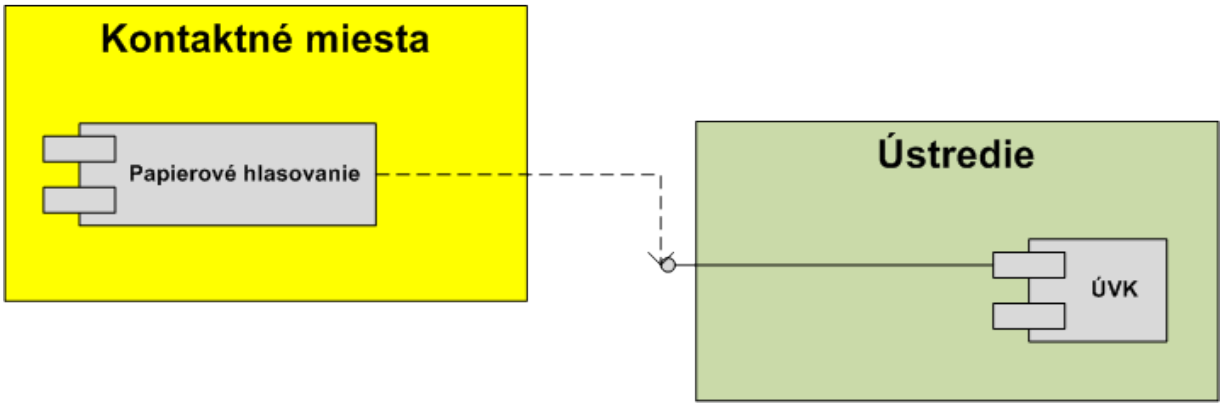
Pojem elektronické voľby nemá jednoznačnú interpretáciu. Vyjadruje totiž, že sa niektoré činnosti (procesy) v priebehu volieb vykonajú pomocou IKT, alebo s podporou IKT: odovzdávanie hlasov, zber hlasov, automatizované spracovanie výsledkov, vyhlasovanie výsledkov, a podobne. V ďalších častiach rozoberieme niekoľko modelov volieb, ktoré sa budú líšiť tým, ktoré procesy alebo činnosti budú realizované alebo podporované IKT. Začneme tradičným, konvenčným modelom volieb.

3.2.1 Súčasný model bez elektronizácie

Z dôvodu zachovania kompatibility, jednoduchšieho začlenenia do systému, ako aj rýchlejšieho akceptovania navrhovaných modelov potenciálnymi budúcimi používateľmi - voličmi

- navrhované modely vychádzajú z štruktúry volieb tak, ako sú na Slovensku implementované dnes. Teda, naším cieľom bude rozšíriť súčasné papierové hlasovanie o hlasovanie elektronické, a to tak, aby čo najviac vychádzalo zo súčasného modelu. Uveďme si preto hrubý komponentový pohľad na súčasnú podobu volieb; nazvime volebné miestnosti názvom zažitým z návrhu e-governmentu, **Kontaktné miesta**. **Ústredie** obsahujúce **Ústrednú volebnú komisiu (ÚVK)** budeme analyzovať ako druhý komponent súčasného systému.

Elektronické voľby nenahradia, aspoň nie v krátkodobom výhľade, tradičný (konvenčný) spôsob vykonávania volieb. Preto by navrhované elektronické riešenia mali byť kompatibilné s existujúcim konvenčným riešením.



Obr. 3.1: Diagram komponentov - dnešná situácia

3.2.2 Model s automatizovaným spočítavaním hlasov

Tento model je dnes už sčasti implementovaným rozšírením konvenčných volieb, kde sú hlasy spočítavané výpočtovou technikou; uvedená forma elektronizácie má priamu oporu aj v slovenských zákonoch[2].

3.2.3 Úplne elektronické voľby s možnosťou odovzdania hlasu iba v kontaktných bodoch

Prvým prirodzeným rozšírením spôsobu hlasovania na Slovensku je pridanie **Elektronického hlasovania** do Kontaktného miesta; tento model je graficky znázornený na obrázku 3.2. Konkrétne, tento model počíta s vybavením kontaktných miest dodatočnými zariadeniami, a to najmä:

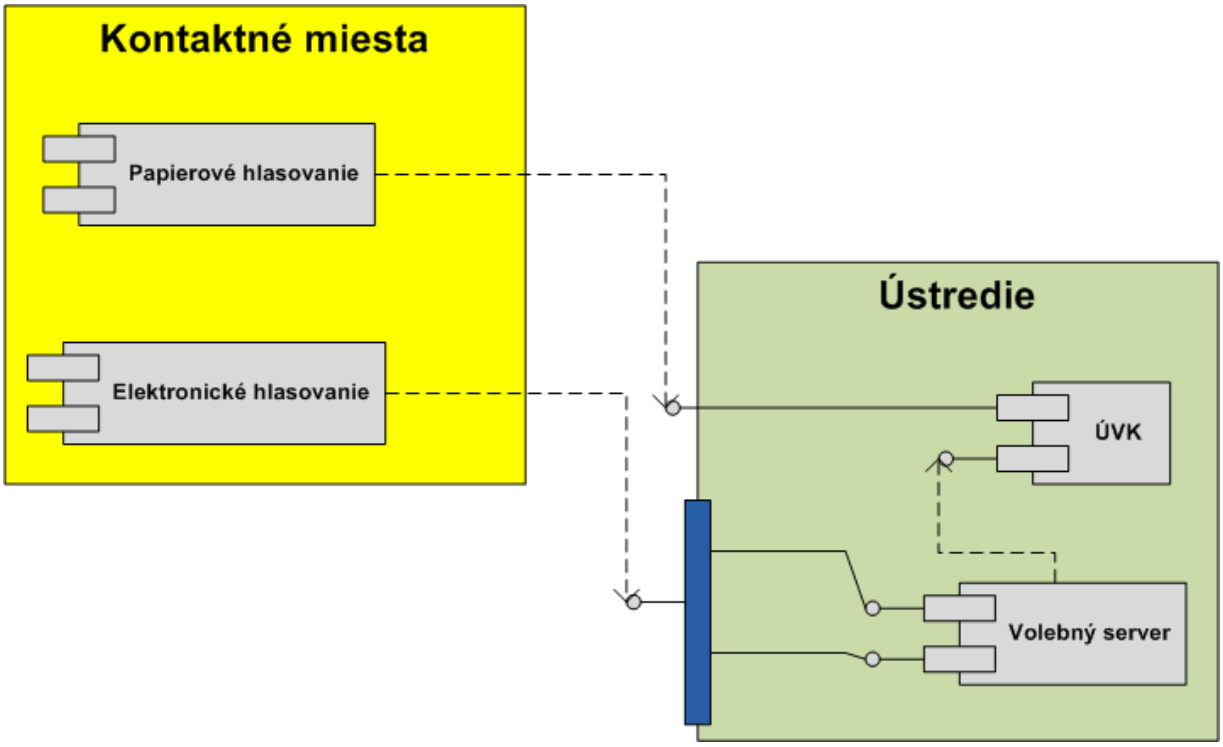
[2]napr. v [33], §54

1. Čítačkou EIK
2. Čítačkou biometrických dát (voliteľné)
3. Hlasovacím zariadením

Proces hlasovania v tomto modeli popíšeme bližšie v nasledujúcich častiach tohto dokumentu. Dôležité je spomenúť možnosť úplného vynechania Papierového hlasovania, ktoré by sa mohlo uskutočniť po splnení nasledujúcich podmienok:

1. Každý volič je vybavený EIK
2. Elektronický spôsob hlasovania je verejne akceptovaný a považovaný za spoľahlivosťou a bezpečnosťou aspoň rovnocenný Papierovému hlasovaniu

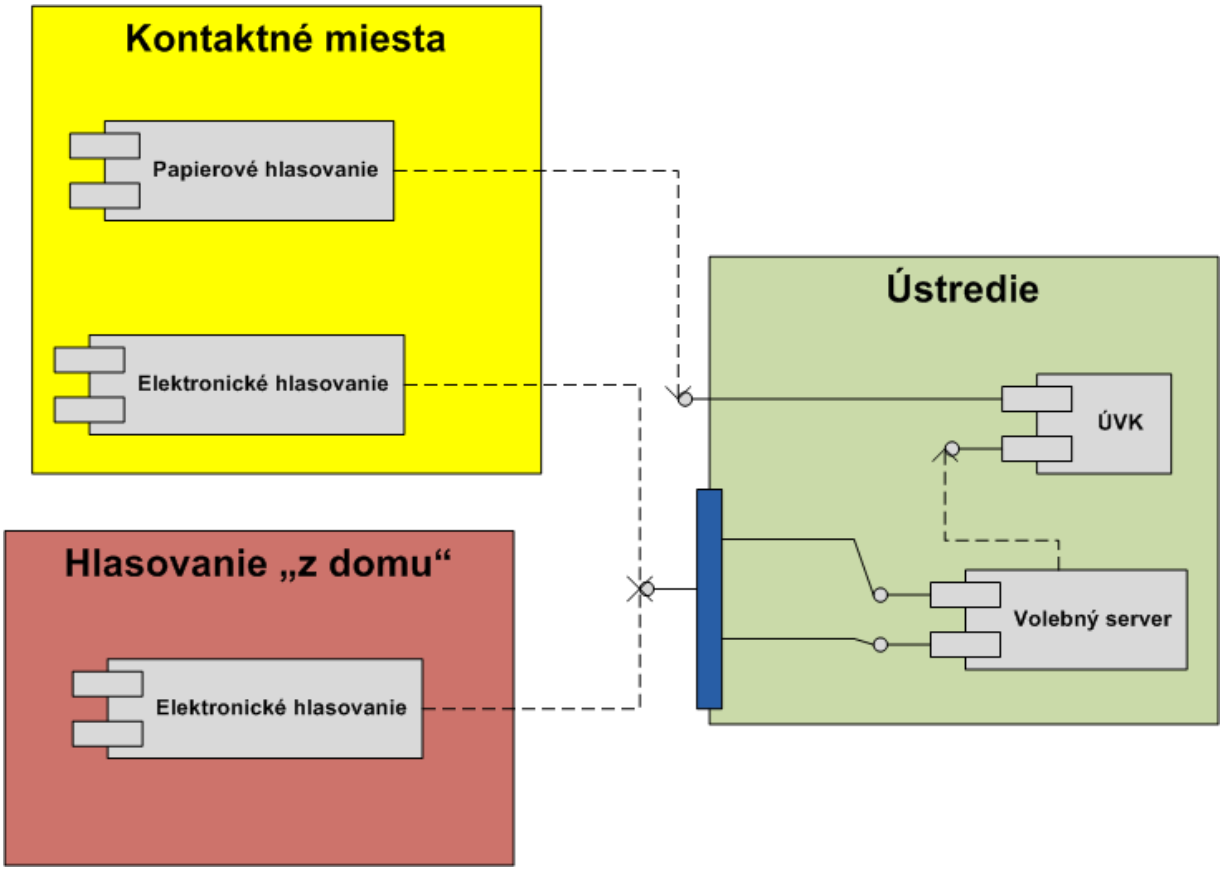
V oboch podmodeloch tohto modelu (s Papierovým hlasovaním aj bez neho), podobne ako v modeloch nasledujúcich, je dôležité mať na zreteli dôkladné zaškolenie ako volebnej komisie, tak voliča ako takého.



Obr. 3.2: Diagram komponentov - bez hlasovania z osobných počítačov

3.2.4 Úplne elektronické voľby s možnosťou odovzdania hlasu iba cez počítač

Tento model je prirodzeným zjednodušením modelu 3.2.5. Keďže odopretie možnosti hlasovania z kontaktných bodov je v strednodobom období prakticky nerealizovateľné pre podstatné zníženie dostupnosti volieb voličom sa ním však nebudeme ďalej zaoberať.



Obr. 3.3: Diagram komponentov - s hlasovaním z osobných počítačov

3.2.5 Úplné elektronické voľby

Rozšírením o možnosť hlasovania z akéhokoľvek osobného počítača s možnosťou pripojenia na verejnú sieť internet získame model s hlasovaním z osobných počítačov. Náčrt komponentov takéhoto systému možno vidieť na obrázku 3.3. Hlasovanie z domu je konceptom, ktorý je využívaný napríklad v Estónsku a popísaný v časti 4.1. Podmienky pre prípadnú elimináciu Papierového hlasovania sú identické ako v modeli bez hlasovania z osobných počítačov.

V ľubovoľnom z vyššie uvedených modelov volieb možno zachovať možnosť klasického (konvenčného) Papierového hlasovania. Miesto čisto klasického alebo výlučne elektronického hlasovania dostávame zmiešaný, hybridný model (modely) volieb.

3.3 Požiadavky kladené na elektronické voľby

Ako na každý projekt v oblasti IT, i na elektronické voľby sú kladené požiadavky z nasledujúcich 4 základných kategórií[3]:

1. **Funkčné požiadavky**, ktoré zahŕňajú najmä požiadavky na funkcie ponúkané systémom, a to volebnou aplikáciou zo strany používateľa a volebnými servermi na strane organizátora volieb. Systém by mal spĺňať nasledovné požiadavky:
   (a) **Explicitné požiadavky**, ktoré zosumarizujeme v časti 5.2
   (b) **Implicitné požiadavky**, predstavujúce súlad rozhraní so zákonnými reguláciami a medzinárodnými dohovormi, a to najmä:
      i. Príslušná slovenská legislatíva, ktorou sme sa zaoberali v časti 2.1.1
      ii. Ďalšia relevantná a záväzná legislatíva, a to najmä zákon o informačných systémoch verejnej správy [29]
      iii. Medzinárodné deklarácie a konvencie, a to najmä[4]:
         - Všeobecná deklarácia ľudských práv, prijatá a vyhlásená rezolúciou Valného zhromaždenia OSN 10. decembra 1948[5]. O práve voliť pojednáva v článku 21 v týchto bodoch:
           "Každý má právo zúčastňovať sa na správe svojej krajiny priamo alebo prostredníctvom slobodne volených zástupcov."
           "Každý má právo na rovnaký prístup k verejným službám vo svojej krajine."
           "Základom vládnej moci nech je vôľa ľudu; táto vôľa má byť vyjadrená pravidelne konanými a riadne vykonávanými voľbami, na základe všeobecného a rovného hlasovacieho práva, tajným hlasovaním alebo iným rovnocenným postupom zabezpečujúcim slobodu hlasovania."

[3]Podľa CMMI, Capability Maturity Model Integration, dostupné k 6.4.2012 na sieti Internet: `http://www.sei.cmu.edu/cmmi/solutions/info-center.cfm`

[4]zdroje pochádzajú z publikácie [1]

[5]slovenská verzia dokumentu dostupná k 6.4.2012 na sieti Internet: `http://www.vop.gov.sk/ochrana_prav/legislativa/deklaracia/`

- Medzinárodný pakt o občianskych a politických právach, prijatý Valným zhromaždením OSN 16. decembra 1966[6]. Pakt nadobudol účinnosť 23. marca 1976. Voľbami sa zaoberá najmä v článku 25 v týchto bodoch:

  "Každý občan má právo a možnosť bez akýchkoľvek rozdielov uvedených v článku 2 a bez neodôvodnených obmedzení:

  a) zúčastňovať sa na vedení verejných záležitostí priamo alebo prostredníctvom slobodne volených zástupcov;

  b) voliť a byť volený v pravidelných voľbách, ktoré sa budú konať na základe všeobecného a rovného hlasovacieho práva, tajným hlasovaním zabezpečujúcim slobodu hlasovania;"

- Dohovor o ochrane ľudských práv a základných slobôd, ktorý vznikol na pôde Rady Európy, bol podpísaný členskými štátmi Rady Európy 4. novembra 1950[7]. Jeho dodatkový protokol v znení Protokolu č. 11 v článku č. 3 Právo na slobodné voľby zmieňuje: "Vysoké zmluvné strany sa zaväzujú konať v rozumných intervaloch slobodné voľby s tajným hlasovaním za podmienok, ktoré zabezpečia slobodné vyjadrenie názorov ľudu pri voľbe zákonodarného zboru."

2. **Nefunkčné požiadavky**, ktoré zosumarizujeme a podrobne vysvetlíme v časti 5.1

3. **Business požiadavky**, ktoré sme uviedli v časti 3.1

3.4 Identifikácia a autentifikácia voliča

Problém identifikácie a následnej autentifikácie je potrebné riešiť v mnohých aplikáciach elektronickej komunikácie. Vďaka širokému záujmu odborníkov o technológie umožňujúce rýchle a relatívne bezpečné vykonanie spomenutých úkonov existuje množstvo dostupných nástrojov vykonávajúcich identifikáciu a autentifikáciu. Našim cieľom je do čo najvyššej miery využiť existujúce prostriedky alebo prostriedky, ktorých nasadenie sa v podmienkach Slovenska reálne plánuje. Za účelom identifikácie a autentifikácie voliča preto budeme používať tzv. eID karty, ktoré sú rozšírením už existujúcich občianskych preukazov o čip,

[6]slovenská verzia dokumentu dostupná k 6.4.2012 na sieti Internet: `http://www.unhcr-centraleurope.org/sk/pdf/zdroje/pravne-materialy/medzinarodne-utecenecke-pravo/medzinarodny-pakt-o-obcianskych-a-politickych-pravach.html`

[7]slovenská verzia dokumentu dostupná k 6.4.2012 na sieti Internet: `http://www.radaeuropy.sk/?928`

ktorý má občanom [8] umožňovať tvorbu zaručeného elektronického podpisu, ako aj šifrovanie komunikácie.

3.5 Volebná aplikácia

Volebná aplikácia je počítačový program, ktorý je určený oprávnenému voličovi na odovzdanie hlasu vo voľbách. Pre zabezpečenie vysokej dostupnosti elektronických volieb verejnosti je dôležité zabezpečiť aplikáciu, ktorá nie je závislá na konkrétnej platforme a je jednoduchá na používanie (pretože nemožno predpokladať, že jej používatelia sú odborníkmi na informačné technológie); jednoduchý design a ovládanie tiež zníži nároky na informačnú kampaň oboznamujúcu voličov s jej používaním. Technickým návrhom volebnej aplikácie, ako aj metód jej šírenia medzi voličov, sa budeme zaoberať v častiach 5.3.2.4 a 5.3.2.5.

3.6 Zabezpečenie klientských PC

Ideálnym ale prakticky nedosiahnuteľným stavom pre hlasovanie v elektronických voľbách z ľubovoľného osobného počítača pripojeného do siete Internet je preukázateľne bezpečný operačný systém. Na bežných používateľov totiž striehne množstvo nástrah v podobe škodlivého softvéru, ako sú napríklad trójske kone, ktorých výskytu v systéme síce možno predchádzať použitím kvalitného zabezpečovacieho systému a školením používateľov, ale ktoré nemožno v praxi nikdy úplne vylúčiť. Ďalšou, podstatne závažnejšou hrozbou, sú útoky cielené priamo na volebnú aplikáciu alebo elektronické voľby; takéto útoky totiž môžu byť prezentované tesne pred alebo počas elektronických volieb. Spoločnosti poskytujúce antivírusové a iné zabezpečovacie systémy (firewally, antispyware) totiž nemajú v takejto situácii čas na reakciu na vzniknuté ohrozenie a prostredníctvom voliča je tak vystavený nebezpečenstvu celý systém elektronických volieb. Preto je potenciálne užitočné komunikovať prípravu elektronických volieb so spoločnosťami ktoré zabezpečovacie produkty vyvíjajú, ale aj s organizáciami zaoberajúcimi sa priamou pomocou používateľom napadnutým takýmto škodlivým kódom, ako je napríklad fórum viry.cz[9]. Ďalším prínosom by mohli byť riešenia založené na používaní stanoveného operačného systému

[8] podľa vládnej novely zákona č. 224/2006 Z. z. o občianskych preukazoch

[9] Fórum viry.cz je najväčšie internetové fórum zaoberajúce sa pomocou používateľom so škodlivým softvérom v Českej republike a na Slovensku; internetové stránky fóra dostupné k 6.4.2012: `http://forum.viry.cz`

voličom. Zabezpečením operačného systému a bezpečným používaním aplikácii sa vo svojej práci General Purpose Operating System for Security Critical Applications [21] zaoberá RNDr. Jaroslav Janáček, PhD a konkrétnymi možnosťami rozšírenia systému SELinux na účely ochrany aj pre osobné počítače sa zaoberá vo svojej práci Using SELinux to Enforce Two-Dimensional Labelled Security Model with Partially Trusted Subjects [3] kolega Bc. Martin Jurčík. Použitie špeciálne upraveného operačného systému by však vyžadovalo vybudovanie dodatočného distribučného kanálu na šírenie takéhoto operačného systému, ako aj komplexnejšie školenia používateľov o jeho používaní; v ďalšej práci sa preto touto možnosťou nebudeme zaoberať.

3.7 Bezpečný komunikačný kanál

Keďže potrebujeme zabezpečiť prenos citlivých údajov medzi zariadeniami na vykonávanie elektronickej voľby (či už ide o hlasovacie zariadenie alebo osobný počítač s pripojením do siete Internet), bude potrebné vybudovať spoľahlivé a dostatočne silne kryptograficky zabezpečené spojenie medzi daným zariadením a centrálnym volebným serverom. Navrhnuté konštrukcie budú vychádzať ako zo štandardov a noriem platných v Európskej Únií, tak aj z v praxi overených a spoľahlivých riešení[10]. Konkrétna technická implementácia a voľba kryptografických riešení je závislá na situácii, v ktorej budú elektronické voľby zavádzané, ako aj na vývoji hardvéru a pokroku kryptografie; nebudeme preto uvádzať konkrétne šifrovacie algoritmy.

3.8 Kryptografické zabezpečenie získaných údajov

Vzhľadom na citlivosť údajov zhromažďovaných vo volebnej centrále je potrebné zabezpečiť ich dostatočnú ochranu pred zneužitím či modifikáciou. Nepochybne sa budeme zaoberať aj možnosťou úplného vylúčenia prepojenia týchto údajov s verejnou sieťou, ktorá sa v istých fázach elektronických volieb ukazuje ako prakticky realizovateľné a rozumné riešenie. Organizačnými opatreniami na ochranu dát sa zaoberáme aj v kapitole 7.

[10] napríklad využitie SSL/TLS v aktuálnych verziách

3.9 Potrebné kryptografické konštrukcie

V tejto časti uvedieme popis základných kryptografických konštrukcii, ktoré budeme využívať v ďalších častiach. Popisy a definície sú prevzaté z [2] a upravené pre potreby tejto práce. Ostatné použité konštrukcie, schémy a protokoly sú zväčša definované buď v citovaných prácach, alebo v publikácii [37]. Verzie kryptografických konštrukcii uvedené v tejto práci nie sú vhodné na priamočiaru implementáciu; pri implementácii je odporúčané využiť existujúce knižnice a postupy pre šifrovacie algoritmy, ako napríklad Crypto++[11] či OpenSSL[12].

3.9.1 Schéma RSA

RSA je algoritmus[13] široko využívaný v kryptografii s verejným kľúčom; jeho bezpečnosť je vybudovaná na otvorenom probléme faktorizácie veľkých čísel. Vo všetkých ďalších častiach n predstavuje verejný modul.

3.9.1.1 Šifrovacia schéma

V tejto časti uvedieme zjednodušený náčrt šifrovacej schémy RSA umožňujúci čitateľovi bez hlbších kryptografických vedomostí získať potrebný prehľad o používanej šifrovacej schéme.

Generovanie kľúča

1. Zvolia sa $p, q \in_R N, p \neq q$, prvočísla s podobnou bitovou dĺžkou[14]
2. Vypočíta sa $n = pq$
3. Vypočíta sa $\phi(n) = (p-1)(q-1)$
4. Zvolí sa $e : 1 < e < \phi(n), GCD(e, \phi(n)) = 1$
5. Vypočíta sa $d = e^{-1}(mod(\phi(n)))$

[11] dostupné k 6.4.2012 na sieti Internet: `http://www.cryptopp.com/`
[12] dostupné k 6.4.2012 na sieti Internet: `https://www.openssl.org/`
[13] prvýkrát popísaný v roku 1978 autormi Ron Rivest, Adi Shamir a Leonard Adleman
[14] zápis $x \in_R M$ označuje náhodný výber x z množiny M

Verejný kľúč je množina $\{n, e\}$, súkromný kľúč je množina $\{n, d\}$. Pre praktické použitie ANSI X9.31, IEEE 1363 a PKCS#1 dovoľujú silnejšiu požiadavku, kde p, q sú tzv. silné prvočísla, odolné voči Fermatovej faktorizácii.

Šifrovanie

Za použitia vhodného paddingu[15], napríklad OAEP alebo iného príslušným štandardom (napr. PKCS#1) odporúčaného bezpečnostného mechanizmu, sa správa M konvertuje do m takého, že $0 < m < n$. Samotné šifrovanie:

$$c = m^e(mod(n))$$

Dešifrovanie

Šifrový text c je dešifrovaný nasledovne:

$$m = c^d(mod(n))$$

Pôvodnú správu získame odstránením príslušného paddingu. Pre efektívnejší výpočet možno použiť napr. metódu Čínskej zvyškovej vety[16].

3.9.1.2 Podpisová schéma

Schéma RSA môže byť priamočiaro využitá i na vystavenie podpisu správy; podpis správy slúži na overenie pôvodu správy, teda jej odosielateľa.

Podpísanie správy

Podpisovateľ vypočíta hash správy m, ktorú podpisuje. Podpis sig sa vypočíta ako

$$sig = m^d(mod(n))$$

Takto vytvorený podpis sa priloží k odosielanej správe.

Overenie

Overenie spočíva v porovnaní hodnoty k správe priloženého podpisu s hodnotou, ktorú overovateľ vypočíta nasledovne:

$$ver = m^e(mod(n))$$

[15] vypchávka; padding je štruktúra pripojená k správe pred jej šifrovaním z dôvodu technických a kryptologických problémov vznikajúcich pri šifrovaní samotnej správy

[16] [2], kapitola 14.5, str. 610

Ak sú hodnoty zhodné, autor správy mal k dispozícii súkromný kľúč podpisovateľa, a teda je pôvodcom doručenej správy.

Takáto priamočiara podpisová schéma má niekoľko závažných bezpečnostných slabín; v praxi sa preto používajú schémy ako napríklad RSA-PSS či RSA-OAEP, ktoré sú popísané napríklad v publikácii [17]. Na šifrovanie a podpisovanie by nemal byť použitý rovnaký súkromný kľúč.

3.9.1.3 Slepé podpisy

Slepý podpis je podpis, kde obsah podpisovanej správy je pred podpísaním "rozmazaný". Schéma pre slepé podpisy je schémou, kde vystupuje odosielateľ A, ktorý chce obdržať podpis pre svoju správu, a podpisovateľ B, ktorý vlastní tajný súkromný kľúč. Cieľom protokolu je stav, v ktorom A obdržal podpis správy m, pri čom B nemá o m žiadnu informáciu, ktorú nemal pred poskytnutím podpisu. Viac informácií o schéme pre slepé podpisy možno nájsť v [2], časť 11.8.1, str. 475.

Podpísanie správy

Jednou z najjednoduchších schém pre slepé podpisy je schéma založená na algoritme RSA (viď [17]). Schéma využíva nasledovné primitíva:

$$r \in_R N; gcd(r, n) = 1$$

Rozmazávajúci faktor b:

$$b = r^e (mod(n))$$

$$m' = m \cdot b$$

Následne A odošle m' podpisovateľovi B; keďže r je náhodné a priradenie $r \to r^e(mod(n))$ je permutácia, aj b je náhodné a neposkytuje podpisovateľovi žiadnu informáciu o m. Podpisovateľ B vypočíta slepý podpis s':

$$s' = (m')^d (mod(n))$$

Odstránením rozmazávajúceho faktoru odosielateľ A získa podpis pre správu m:

$$s = s' \cdot r^{-1} (mod(n))$$

Získaný podpis je platným podpisom s, pretože $r^{ed} = r(mod(n))$, a teda:

$$s = s' \cdot r^{-1} = (m')^d r^{-1} = m^d r^{ed} r^{-1} = m^d r r^{-1} = m^d (mod(n))$$

Z dôvodu multiplikatívnej homomorfnosti RSA nemožno použiť jeden súkromný kľúč súčasne na podpisovanie a šifrovanie.

Detailné vysvetlenie a príklady na problematiku slepých podpisov možno nájsť v [2], str. 475.

3.9.2 Schémy na zdieľanie tajomstva

Schémy na zdieľanie tajomstva v práci využívame na rozdelenie tajomstva medzi viacero autorít. Schémy s thresholdom umožňujú rozdistribuovať tajomstvo tak, že pre získanie tajomstva je potrebná prítomnosť zvoleného počet autorít. Práve pomocou tohto princípu zabezpečíme rozdelenie kľúčov používaných v elektronických voľbách.

Štruktúru schém a ďalšie informácie o schémach na zdieľanie tajomstva možno nájsť v [2], časť 12.7, str. 524.

Formálne, pod $A(t, n)$ threshold schémou, kde platí $t \leq n$, rozumieme vypočítanie častí tajomstva $S_i, 1 \leq i \leq n$ z tajomstva S dôveryhodnou treťou stranou a bezpečnú distribúciu takto získaných častí tajomstva autoritám P_i. Ďalej platí:

- Ľubovoľných t alebo viac autorít dokáže vygenerovať tajomstvo S
- Žiadna množina $t - 1$ alebo menej autorít nedokáže vygenerovať tajomstvo S

Navyše, takáto schéma je *perfektná*, ak znalosť $t-1$ alebo menej častí tajomstva neposkytuje žiadnu informáciu o S. Technicky je rozdelenie tajomstva možné realizovať napríklad uložením každej jeho časti na čipovú kartu a použitím dôveryhodnej čítačky takýchto kariet na rekonštrukciu tajomstva.

Už v predpokladoch schém na zdieľanie tajomstva sa uvádza potreba dôveryhodnej tretej strany a bezpečnej distribúcie; je preto potrebné pripomenúť, že i táto časť prípravy elektronických volieb je závislá na dobrom organizačnom riadení a kvalitnej politike manažérstva kvality. Posúdenie organizačných otázok a otázok manažérstva kvality uvádzame v kapitole 7.

3.9.2.1 Shamirova schéma na zdieľanie tajomstva

Shamirova schéma na zdieľanie tajomstva je pomerne jednoduchým a silným nástrojom; technické detaily tejto schémy možno nájsť v [2], časť 12.7.2, str. 525. Schéma stavia svoju bezpečnosť na polynomiálnej interpolácii a fakte, že polynóm $y = f(x)$ stupňa $t - 1$ je jednoznačne definovaný t bodmi (x_i, y_i) (definovaním t lineárne nezávislých rovníc o t neznámych).

Distribúcia tajomstva

Cieľom je rozdelenie tajomstva $S; S \in \mathbb{N}, S \geq 0$ dôveryhodnou treťou stranou T medzi n autorít tak, aby ľubovoľná skupina aspoň t autorít dokázala úspešne zrekonštruovať tajomstvo S.

1. T zvolí $p > max(S, n), p$ je prvočíslo
2. T označí $a_0 = S$
3. T zvolí $t-1$ náhodných a nezávislých[17] koeficientov $a_1, ..., a_{t-1}; 0 \leq a_j \leq p-1$ a definuje náhodný polynóm $f(x) = \sum_{j=0}^{t-1} a_j x^j$ nad $\mathbb{Z}_p$
4. T vypočíta $S_i = f(i)(mod(p)), 1 \leq i \leq n$
5. T bezpečne odovzdá časti tajomstva S_i autoritám P_i (podľa indexu i)

Rekonštrukcia tajomstva

Rekonštrukciu tajomstva môže vykonať ľubovoľných aspoň t autorít nasledovne:

1. Prítomných t autorít poskytne svoje časti zdieľaného tajomstva; $(x, y) = (i, S_i)$
2. Pomocou Lagrangeovej interpolácie dôveryhodná tretia strana[18] vypočíta koeficienty $f(x)$ $a_j, 1 \leq j \leq t-1$ a zrekonštruuje tajomstvo $f(0) = a_0 = S$

Možno dokázať, že Shamirova schéma na zdieľanie tajomstva je *perfektná*, *ideálna*[19], *rozšíriteľná o nových používateľov*. Schéma navyše nepoužíva žiadne nedokázané predpoklady[20].

Opäť je potrebné poznamenať, že uvedený základný, jednoduchý model Shamirovej schémy nie je vhodný pre priamočiare nasadenie, pretože má niektoré praktické nevýhody (napríklad možnosť dosiahnuť podvodnou autoritou zrekonštruovanie falošného (iného) tajomstva, pričom k skutočnému tajomstvu má prístup iba podvodná autorita). Schému uvádzame pre ilustráciu a ľahšie pochopenie problematiky čitateľom. Pre implementáciu elektornických volieb možno použiť niektorú z pokročilých kryptografických knižníc, ktoré ponúkajú sofistikovanejšie kryptografické schémy a algoritmy.

[17] uvedené vlastnosti možno získať zvolením kvalitného pseudonáhodného generátora

[18] napríklad čítačka čipových kariet

[19] veľkosť časti tajomstva je rovnaká ako veľkosť tajomstva samotného

[20] na rozdiel od napr. RSA, kde využívame predpoklad o náročnosti faktorizácie veľkých čísel

Kapitola 4

Existujúce modely a protokoly

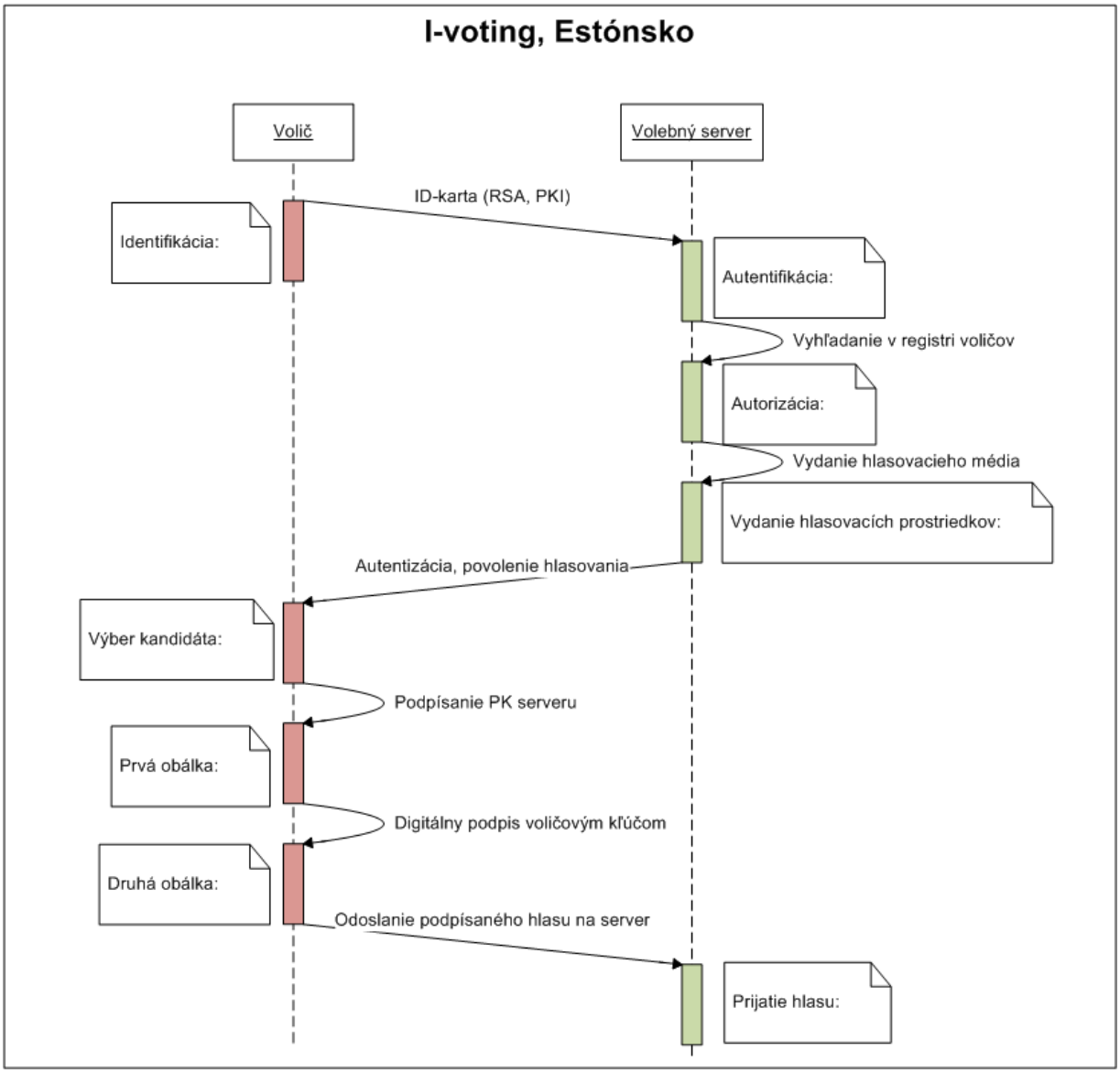
Elektronické voľby na Slovensku nie sú prvým modelom elektronického hlasovania vo svete; možno preto analyzovať, modifikovať a implementovať do našich modelov i skúsenosti z iných krajín, kde už v istej forme elektronické voľby implementované sú. Zaoberať sa budeme predovšetkým modelom estónskych I-Volieb[1], pretože ho v čase písania tejto práce považujeme za najkomplexnejší a najvhodnejší ako z hľadiska podmienok, v ktorých vznikal, tak i z hľadiska výsledkov, ktoré boli zvoleným spôsobom dosiahnuté. Uvedenou analýzou sme sa zaoberali už v práci [18], ktorá slúži ako referenčná práca pre nasledujúcu analýzu.

4.1 Estónsky model

Pri analýze modelu elektronického hlasovania v Estónsku, I-Volieb, ako aj pri zohľadňovaní jeho predpokladov a dosiahnutého stavu, sme vychádzali najmä z prezentácie [23]. I-Voľby okrem štandardného komponentu hlasovania z vyhradených kontaktných miest umožňujú voličovi hlasovať i z ľubovoľného osobného počítača prostredníctvom široko dostupnej siete Internet. Keďže v Estónsku boli v čase implementácie I-Volieb všeobecne používané ID karty obsahujúce kryptografický čip, v ktorom bol implementovaný algoritmus RSA (viď časť 3.9.1), **identifikácia** prebieha prostredníctvom týchto ID kariet. Systém odovzdania hlasu možno prirovnať k systému dvoch obálok; konkrétne, prvú obálku tvorí šifrovanie verejným kľúčom volebného serveru, ktorým sa odovzdaný hlas zašifruje po odovzdaní. Druhú obálku predstavuje digitálny podpis voliča[2].

[1] Preložené z anglického I-Voting

[2] Digitálny podpis sa poskytne prostredníctvom identifikačnej karty voliča



Obr. 4.1: Sequence diagram I-Volieb v Estónsku

Po ukončení volieb takéto virtuálne obálky umožňujú spočítavanie hlasov v dvoch disjunktných fázach, a to:

1. **Anonymizácia** – odstránenie vonkajších obálok
2. **Tabulácia** – odstránenie vnútorných obálok

Priebeh volieb v estónskom modeli možno vyjadriť nasledovnou postupnosťou aktivít. Uveďme ich postupnosť pre prípad úspešného vykonania voľby:

1. **Autentifikácia voliča** - volič vloží autentifikačné dáta a sieťový server ho autentifikuje
2. **Zaslanie zoznamu kandidátov** - sieťový server voličovi zašle zoznam kandidátov
3. **Označenie voľby** - volič označí zvoleného kandidáta, označme ho $hlas$
4. **Vygenerovanie náhodného parametra** - označme $k \leftarrow Random()$
5. **Zašifrovanie hlasu** - $Enc(hlas, k, PK)$, kde PK je verejný kľúč servera
6. **Podpísanie a odoslanie hlasu** - volič podpíše hlas svojím elektronickým podpisom: $Sign(Enc(hlas, k, PK), SK)$, kde SK je súkromný kľúč voliča[3]
7. **Overenie podpisu voliča** - sieťový server overí platnosť podpisu prijatej správy
8. **Overenie opakovanej voľby** - volebný server overí, či volič už hlas odovzdal; ponechá sa iba najnovší z hlasov, čo je možné vďaka elektronickému podpisu voliča
9. **Autorizovanie voliča** - volebný server autorizuje voliča overením jeho práva voliť; zároveň sa priloží ID voliča
10. **Uloženie a podpísanie hlasu a ID voliča** - k hlasu voliča sa pripojí jeho ID a výsledná správa sa podpíše: $Sign(ID, SK_S)$, kde SK_S je súkromný kľúč volebného servera; táto správa sa odošle späť voličovi
11. **Overenie podpisu servera** - volič overí platnosť podpisu servera. Tu aktívne zapojenie voliča do procesu voľby končí
12. **Vygenerovanie výsledného zoznamu, spočítanie hlasov** - spočítavanie prebieha na druhom serveri, ktorý je fyzicky oddelený od siete (dáta sa naň prenášajú ručne)

Ako možno vidieť zo schémy, estónsky model umožňuje viacnásobnú voľbu, čím z bezpečnostného hľadiska znižuje možnosť prinútenia voliča k voľbe. Navyše, po ukončení elektronického hlasovania volič môže svoj elektronický hlas zrušiť i v následnom konvenčnom hlasovaní (v estónskom modeli fáza elektronických volieb predchádza fáze konvenčných volieb).

[3] estónski občania disponujú ID kartami so vstavaným čipom umožňujúcim autentifikáciu a digitálne podpisovanie prostredníctvom RSA; Estónsko disponuje vlastnou PKI (Public Key Infrastructure)

Tento model sa v praxi ukazuje ako postačujúci po stránke technickej i bezpečnostnej; v časti 5 ho prehodnotíme a doplníme. Model totiž nespĺňa nasledovné požiadavky:

- Overiteľnosť; v protokole absentuje akákoľvek možnosť overenia či zo strany voliča alebo tretích strán
- Nepostačujúca miera robustnosti
- Dostupnosť hlasov na online serveroch, možnosť kompromitovať hlasy iba ovládnutím online serveru

Práve uvedené parametre budeme v časti 5 čiastočne riešiť pridaním tretej šifrovacej obálky a ďalšími rozšíreniami systému.

4.2 Schémy s využitím homomorfného šifrovania

Využitie homomorfného šifrovania vo volebných schémach je zaujímavou možnosťou, ako získať pokročilé bezpečnostné vlastnosti a jednoduchú manipuláciu s hlasmi využitím vhodných kryptografických primitív. Označme $E_r(m)$ správu zašifrovanú s využitím náhodného parametra r, správy $P = \{m_1, m_2, ..\}$ a šifrové texty $C = \{c_1, c_2, ..\}$. Pre naše potreby homomorfné schémy budú využívať pravdepodobnostný šifrovací systém s priestorom správ P a priestorom šifrových textov C, kde $(P, \oplus)$ a $(C, \otimes)$ sú grupy. Schému s parametrami $(P, C, \oplus, \otimes)$ potom nazveme homomorfnou práve vtedy, keď platí:

$$(\forall E)((c_1 = E_{r_1}(m_1)) \wedge (c_2 = E_{r_2}(m_2))$$

$$\Rightarrow ((\exists r)(c_1 \otimes c2 = E_r(m_1 \oplus m_2)))$$

Teda, zjednodušene povedané, ak vykonáme grupovú operáciu (súčin) na zašifrovaných hlasoch, dostávame identický výsledok, ako keď hlasy najprv spočítame a výsledok sčítania zašifrujeme pomocou kľúča. ide teda o operáciu platnú i vzhľadom na samotné hlasy.

Pre ilustráciu si uveďme inštanciu homomorfného šifrovania na šifrovacej schéme ElGamal; zvoľme príslušný parameter p tak, že

$$P = Z_p$$

$$C = \{(a, b) | a, b \in Z_p\}$$

Grupovou operáciou na správach (hlasoch) bude násobenie modulo p a grupovou operáciou na šifrových textoch bude násobenie modulo p po komponentoch. Dôkaz homomorfnosti takejto schémy je priamočiary:

$$E_{k_0}(m_0)E_{k_1}(m_1) = (g^{k_0}g^{k_1}, h^{k_0}h^{k_1}m_0m_1) =$$

$$= (g^k, h^k m_0 m_1) = E_k(m_0 m_1)$$

4.2.1 Schéma HS

Ako príklad homomorfnej schémy uvedieme štandardný model HS (skratka je odvodená z mien autorov - Hirt a Sako) publikovaný v [9]. HS nie je výlučne homomorfným modelom, pretože má aj prvky mixnetových protokolov[4] založených na miešaní hlasov autoritami. Uvedený model vyberáme preto, že podľa [20] preukázateľne dosahuje receipt-freeness[5], súkromnosť, robustnosť, univerzálnu i individuálnu overiteľnosť, férovosť a má aj vlastnosť demokratickosti. Vo svojej podstate schéma HS stavia svoju bezpečnosť na pravdepodobnostnom šifrovaní všetkých potenciálnych hlasov, ktoré sú v obálke (pojem obálka preberáme z estónskeho modelu) vytvorenej šifrovaním verejne dostupné. Následne autority vo viacerých kolách hlasy náhodne premiešajú a iba volič má prehľad o rozložení možností vo výslednej permutácii; z tej následne zvolí ním preferovanú voľbu a hlas odovzdá.

4.2.1.1 Predpoklady schémy

Schéma elektronických volieb HS vyžaduje splnenie nasledovných predpokladov:

- **Homomorfné šifrovanie** - použitý šifrovací systém je homomorfný (napr. ElGamal); teda,
$$Enc(m_1) \oplus Enc(m_2) = Enc(m_1 + m_2)$$
- **Overiteľné dešifrovanie** - požaduje sa, aby ľubovoľných t autorít bolo schopných, bez vplyvu na súkromnosť jednotlivých hlasov, pri použití schémy na zdieľanie tajomstva typu (t, N) vypočítať hodnotu súčtu hlasov T a poskytnúť dôkaz korektnosti dešifrovania hlasov

[4]pod mixnetovým protokolom rozumieme protokol založený na paradigme náhodného permutovania hlasov, čím protokoly zabezpečujú anonymitu hlasovania. Protokoly zvyčajne miešajú správy tým, že ich posielajú cez rôzne sieťové autority, kde každá autorita pred poslaním správ ďalej tieto premieša (konkrétna permutácia správ musí ostať tajná). Mnohé mixnetové konštrukcie volebných protokolov využívajú bezznalostné dôkazy, re-enkrypciu a schémy pre zdieľanie tajomstva

[5]teda nemožnosť ovplyvnenia; volič nedokáže dôveryhodne preukázať, či a ako hlasoval

- **Náhodná re-enkrypcia**[6] - pre ľubovoľné $e \in E(x)$, x je neznáme, existuje pravdepodobnostný algoritmus generujúci uniformne distribuované re-enkrypcie $e' \in E(x)$. Náhodný prvok použitý na generovanie e' budeme nazývať **svedok** re-enkrypcie

- **Dôkaz 1-L re-enkrypcie** - požadujeme existenciu protokolu so vstupmi $e, e_1, .., e_L, v$, kde v je svedok re-enkrypcie e v e_i (pre dané i) taký, že bezznalostne (vzhľadom na i) dokáže, že e_i je re-enkrypciou e

- **Dôkaz re-enkrypcie pre určeného overovateľa**[7] znamená existenciu protokolu, v ktorom iba vybraný overovateľ dokáže overiť, že pre dané zašifrované e, e' a svedka pre e' ako re-enkrypciu e existuje svedok

Oba dôkazy re-enkrypcie možno štandardnou konštrukciou prepracovať na neinteraktívne dôkazy napríklad využitím modifikácie Fiat-Shamirovho postupu[8].
Naplnenie predpokladov a príslušné protokoly sú popísané v [37] a [9].

4.2.1.2 Fázy schémy

Priebeh protokolu možno opäť zhrnúť do nasledovných fáz:

1. **Miešanie hlasov** - autority[9] postupne miešajú všetky potenciálne možné hlasy[10]; túto fázu protokolu možno formalizovať nasledovne:

   (a) Administračný server vytvorí štandardné šifry všetkých potenciálnych platných hlasov

   $$E^{(0)} = \{e_1^{(0)}, e_2^{(0)}, .., e_L^{(0)}\}$$

   kde $e_i^{(0)}$ šifruje generátor G_i využívanej grupy a náhodný parameter k

   (b) Autorita A_j vygeneruje j-tu permutáciu štandardných šifier platných hlasov. Autorita najprv zvolí náhodnú permutáciu $\pi_j : \{1..L\} \rightarrow \{1..L\}$ a náhodné parametre $k_1, .., k_L \in_R Z_p$

[6] re-enkrypcia znamená, že pre danú zašifrovanú správu x existuje zápis v danom zozname zašifrovaných správ, napr. $x_1, x_2, .., x_L$

[7] príklad obdobnej schémy je publikovaný napríklad v [22]

[8] [16]; praktickým problémom takéhoto zneinteraktívnenia je jeho korektnosť iba na modeli náhodného orákula

[9] autority sú dôveryhodné subjekty alebo objekty, ktoré sú určené na miešanie hlasov; viď kapitolu 1

[10] predpokladáme model volieb $1 : L$ alebo iný model prevedený do uvedenej formy

Teda, označme, že $e^{(j)}_{\pi_j(i)}$ = znova zašifrované $e^{(j-1)}_i$ pomocou náhodného parametra k_j. Hlasy sú znova zašifrované pomocou súkromného kľúča príslušnej autority

2. **Generovanie dôkazov** - na základe predpokladu schémy autorita dokáže generovať dôkaz $1-L$ re-enkrypcie, teda dôkaz korektnosti permutácie a zašifrovania výstupnej permutácie

3. **Zaslanie permutácie voličovi** - na základe predpokladu schémy autorita dokáže generovať $1-L$ dôkaz re-enkrypcie pre určeného overovateľa, ktorým je v tomto prípade volič. Prakticky ide napríklad o zaslanie permutácie voličovi cez bezpečný kanál so zabezpečenou dôvernosťou a integritou správy

4. **Analýza dôkazu voličom** - podľa zvolených parametrov threshold systému[11] volič môže odmietnuť až $N-k$ dôkazov (permutácií) od ľubovoľných autorít

5. **Odovzdanie hlasu** - volič verejne oznámi index i ním zvolenej možnosti vo výslednej permutácii platných hlasov

6. **Spočítavanie hlasov** - hlasy sa spočítajú zašifrované. Korektnosť výsledku spočítania zašifrovaných hlasov je garantovaná homomorfnosťou použitého šifrovacieho systému

7. **Dešifrovanie výsledku volieb** - správcovia súkromného kľúča vygenerujú kľúč a dešifrujú výsledok volieb; po uverejnení kľúča môže ľubovoľná tretia strana overiť korektnosť výsledku a správnosť dešifrovania. Správcovia kľúča zverejnia dôkaz o korektnom využití im prislúchajúcej časti zdieľaného tajomstva v schéme na zdieľanie tajomstva (v tomto prípade tajného súkromného kľúča)

4.2.2 Modifikácie HS

Zaujímavou modifikáciou Hirt-Sako protokolu je schéma publikovaná v [37], ktorú budeme ďalej označovať ako Rjaškovej model. Nad rámec predpokladov HS Rjaškovej model predpokladá, že použitý šifrovací systém zachováva hodnotu 0; formálnejšie, pre vstup $e = Enc(m)$ je výstupnou hodnotou šifrovacieho systému $e' = Enc(m')$, kde $m' = 0 \Leftrightarrow m = 0$, inak $m' \neq 0$ je náhodná, uniformne distribuovaná výstupná hodnota. Túto vlastnosť zachováva napríklad v práci [37] navrhnutý upravený ElGamalov kryptosystém, kde $Enc(m) = (g^k, h^k G^m)$, teda pre $Enc(m) = (x, y), m \in {Z^*_{p-1}}$[12] sa hodnoty re-enkrypcie

[11] pre definíciu pojmu threshold system viď kapitolu 1

[12] $Z^*_{p-1} = \{0, .., p-2\}$ pre p prvočíslo

$E(m') = (x', y')$ vypočítajú ako $(x', y') = (x^r, y^r)$, kde $r \in_R Z^*_{p-1}$. Ak $(x, y) = (g^k, h^k G^m)$, potom $(x', y') = (x, y)^r = (g^k, h^k G^m)^r = (g^{kr}, h^{kr} G^{mr}) = E(mr)$ a $m' = mr$. Platí $log_x x' = log_y y'$.

Ako sme už naznačili, schéma využíva robustný ElGamal kryptosystém s thresholdom. Procesy schémy možno zhrnúť do nasledovných fáz:

1. Volič rozdelí svoj hlas v medzi autority, použije sa napríklad $(t + 1, N)$ Shamirova schéma na zdieľanie tajomstva

2. Autority zašifrujú svoje podiely hlasu (podobne ako v HS schéme), volič opäť môže niektoré permutácie odmietnuť (konkrétny počet závisí od parametrov použitej Shamirovej schémy

3. Z voličom neodmietnutých podieloch sa pri spočítavaní hlasov zrekonštruuje hodnota hlasu voliča

4. Hlasy sa vynásobia a uverejní sa výsledok volieb

Pre problémy s dosiahnutím nedonútiteľnosti k voľbe v tomto rozšírení autorka uvádza ešte nasledovné dodatočné rozšírenie:

1. Autority samy vygenerujú náhodné správy s_j a zašifrujú ich; $e_j = Enc(s_j)$

2. Takéto podiely sa zverejnia na tzv. "nástenke" a autority voličovi odošlú dôkaz re-enkrypcie pre vybraného overovateľa (e_j je re-enkrypcia $e^0_j = E^0(s_j)$)

3. Volič overí dôkazy re-enkrypcie, zvolí aspoň $t + 1$ pre neho dôveryhodných autorít a vypočíta $e_v = Enc(v_i - \Sigma_{j \in A} s_j)$; zvolené autority a vypočítanú hodnotu uverejní na nástenke

4. Autority overia hlasy, vypočítajú ich hodnoty a oznámia výsledky volieb

Schémy založené na homomorfnom šifrovaní sú zaujímavé nie len z teoretického, ale i praktického hľadiska. Je v nich totiž možné naplniť požiadavky ako nedonútiteľnosť k voľbe, ktoré schémy založené na iných konštrukciách často nenapĺňajú.

4.3 Schémy založené na slepých podpisoch

Tieto schémy sú založené na aplikovaní schémy pre slepý podpis (viď časť 3.9.1.3 (často ide o schémy založené na RSA alebo podobné schémy). Takýto podpis je (zvyčajne) univerzálne overiteľný, pretože naväzuje na existujúcu infraštruktúru umožňujúcu jeho overenie.

Zaujímavé je, že autori schém založených na slepých podpisoch ich často považujú za v širokom meradle nasaditeľné do reálnych implementácií; v praxi sa však ukazuje, že schémy často majú na praktické použitie privysoké požiadavky (napríklad na vlastnosti komunikačných kanálov) a často nespĺňajú základné bezpečnostné požiadavky ako je napríklad nedonútiteľnosť k voľbe (receipt-freeness). Keďže v takýchto schémach nie je zvyčajne zaručená súkromnosť hlasu, nemožno predpokladať, že by boli verejnosťou akceptované.

4.3.1 Schéma TrustVote

Ako príklad schémy založenej na slepých podpisoch uvedieme schému TrustVote predstavenú v [6][13].

Účastníkmi volieb sú **volič**, **administračný server**, **autority**, **komisia**, **zberatelia kľúčov** a z technických zariadení **registračná nástenka** a **nástenka hlasovania**. Schéma TrustVote pozostáva z nasledovných 5 fáz:

1. **Inicializácia**, počas ktorej je primárnym aktérom administračný server. Vygeneruje $IDvolieb$ - unikátny identifikátor daných volieb a toto ID umiestni na nástenku. Podobne vygeneruje prázdny hlasovací lístok a umiestni ho na nástenku. Zoznam oprávnených voličov je zaslaný autoritám prostredníctvom kanálu zabezpečujúceho autentickosť správy (napr. využitím asymetrickej kryptografie)

2. **Príprava voliča** spočíva vo vyplnení volebného lístka a jeho zašifrovaní; volič vytvorí digitálny vodoznak definovaný ako $\hat{m} = H(ID$ voliča $||IDvolieb||m)$, kde m je náhodná hodnota a $||$ vyjadruje zreťazenie. Tento vodoznak bude ako súčasť volebného lístku anonymne identifikovať voliča v ďalšom priebehu volieb

3. **Registrácia** je fázou, v ktorej možno výhodne použiť slepé podpisy. Volič najprv spojí svoj zašifrovaný hlas s aktuálnym $IDvolieb$ a vodoznakom vygenerovaním odtlačku nasledovne:

$$h = H(\hat{m}||IDvolieb||w)$$

   Z dôvodu zvýšenia robustnosti schémy sa využíva (t, N) zdieľaná schéma pre slepé podpisy; výsledkom je, že podpis považujeme za platný, ak sa na ňom korektne podieľalo aspoň t z N poverených autorít. Označme $e = (e_1, .., e_N)$ verejné kľúče podpisovateľov a $s = (s_1, .., s_N)$ jednotlivé podpisy. Potom overenie je tvaru $verify_{e,t}(s, x) \in$

[13] Táto schéma (podobne ako väčšina schém s praktickým prínosom) je schémou hybridnou; avšak, schéma je založená na využití slepých podpisov, a preto ju uvádzame v tejto časti.

$\{0, 1\}$. Takúto schému možno založiť napríklad na RSA[14]. V protokole pokračujú autority podpísaním takto pripravenej hodnoty (pre každú autoritu volič pripraví na podpísanie potenciálne odlišnú hodnotu a odovzdá ju prostredníctvom registračnej nástenky). Ak je hodnota voličom korektne podpísaná, autorita ju môže z registračnej nástenky prečítať a podpísať svojím súkromným kľúčom. Počet potrebných komponentov podpísaných autoritami v (t, N) určuje, kedy táto fáza končí

4. **Odovzdanie hlasu** - prvým krokom odovzdávania hlasov je vytvorenie schémy pre zdieľanie tajomstva. Možno použiť napríklad Shamirovu (t, N) schému pre zdieľanie tajomstva, prostredníctvom ktorej volič rozdistribuuje podiely kľúča zberateľom kľúčov. Opäť, vyšší threshold v schéme zvyšuje robustnosť a odolnosť schémy. Ako threshold označíme parameter t v zdieľanej schéme (t, N). Druhým krokom je odovzdanie zašifrovaného hlasu a podielov s podpísaných slepým podpisom autoritami na volebnú nástenku voličom. Overovací kód pre odovzdané dáta sa vypočíta ako $h = H(\hat{m}||IDvolieb||w)$, pre zabránenie falošným hlasom sa skontrolujú aj všetky podpisy. Od tejto chvíle volič dokáže overiť, že jeho hlas bol úspešne prijatý na ďalšie spracovanie. Následne je aktívna účasť voliča na protokole ukončená

5. **Spočítavanie hlasov** začína vygenerovaním kľúča zberateľmi kľúča za účelom následného dešifrovania hlasov. V tejto fáze elektronických volieb ľubovoľný pozorovateľ dokáže korektne spočítať hlasy na nástenke, a teda hlasovanie je univerzálne overiteľné

4.4 Schémy založené na anonymnom kanále

Anonymný kanál, ako názov naznačuje, umožňuje odosielať anonymné správy - teda, prijímateľ nie je schopný vystopovať 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. Podobne ako pri schémach opierajúcich svoju bezpečnosť o anonymné podpisy, aj pri anonymných kanáloch je zvyčajne veľmi náročné dosiahnuť nedonútiteľnosť k voľbe či overiteľnosť hlasovania.

Keďže schémy TrustVote a HS využívajú myšlienku anonymného kanálu a premiešavania hlasov, neuvádzame ďalší príklad.

[14] viď 3.9.1

4.4.1 Hybridné a iné schémy

V praxi sa ukazuje potreba prepojiť prínosy jednotlivých schém a vytvoriť hybridné volebné systémy. Pre využitie v reálnom hlasovaní vo voľbách elektronickou cestou je často potrebné pristúpiť ku kompromisom, ktoré danú teoretickú schému zjednodušia a zefektívnia. Príkladom hybridnej schémy je estónsky model elektronických volieb, ktorý sme opísali v časti 4.1.

4.5 Vyhodnotenie existujúcich modelov a protokolov

Aby sme overili, či sú jednotlivé schémy alebo protokoly nasaditeľné do praxe, budeme analyzovať ich bezpečnostné parametre, zložitosť, overovať opodstatnenosť a úroveň naplnenia jednotlivých predpokladov a prípadna aj ďalšie faktory súvisiace s ich použitím v elektronických voľbách. Nefunkčné požiadavky v prehľade neuvažujeme. Niektoré výsledky sme čerpali z [20], [37] a [6].

4.5.1 Naplnenie bezpečnostných požiadaviek

V tejto časti porovnáme naplnenie bezpečnostných požiadaviek, ktoré sú uvedené v časti 5.1 tejto práce.

4.5.1.1 TrustVote

Naplnené požiadavky Schéma vďaka implementácii konceptu nástenky spĺňa požiadavky integrity a demokratickosti. Priamočiarym ignorovaním neplatných hlasov možno dosiahnuť naplnenie korektnosti, oprávnenosti k voľbe a súkromnosti. Využitie vodoznakov umožňuje individuálnu overiteľnosť korektnej manipulácie s hlasom príslušného voliča. Využitie schém na zdieľanie zvyšuje robustnosť schémy. Vlastnosti všeobecnej overiteľnosti a férovosti, ktoré táto schéma spĺňa, sú dôležité predovšetkým pre nezávislú kontrolu korektnosti volebného aktu a spravovania výsledkov hlasovania.

Nenaplnené požiadavky Nepopierateľný dôkaz hlasu možno vytvoriť jednoducho, a to odhalením "voličovho tajomstva"[15] v protokole. Tento problém je principiálny a pravdepodobne ho nemožno odstrániť systematicky; ako potenciálne čiastočné riešenie sa ponúka možnosť viacnásobného hlasovania v podobe uskutočnenia konvenčnej voľby po ukončení

[15] náhodnej hodnoty m

elektronickej časti volieb; problémom však ostáva, že volič je v takomto prípade nútený komisii odhaliť svoje tajomstvo a *id*, čím sa vlastne stráca anonymita elektronického hlasu[16].

4.5.1.2 HS

Schéma má úplne alebo čiastočne všetky hlavné požadované bezpečnostné charakteristiky. Ak odhliadneme od problematickej možnosti odovzdať náhodný hlas, oprávnenosť k voľbe bude dodržaná. Naplnená bude súkromnosť i robustnosť (vďaka využitia schém na zdieľanie tajomstva); zabezpečená je individuálna i univerzálna overiteľnosť a férovosť, predpokladaná je demokratickosť schémy. Čiastočne problematickou je receipt-freeness, teda nedonútiteľnosť k voľbe; v schéme HS by si totiž volič bol nútený pre splnenie tejto vlastnosti ručne vygenerovať výslednú permutáciu hlasov a dôkaz jej správnosti.

4.5.1.3 Estónsky model

Pravdepodobne najdôležitejšími problémami estónskeho modelu sú, ako sme naznačili v časti 4.1, možnosť kompromitovať hlasy ovládnutím online serveru a jeho nedostatočná robustnosť. Ako väčšina schém nevyužívajúcich homomorfizmus, schéma nie je univerzálne overiteľná. Naopak, schéma spĺňa požiadavky individuálnej overiteľnosti (čiastočne, priamo z protokolu; volič dostane potvrdenie o doručení hlasu k autorite, ktorú považujeme za dôveryhodnú), súkromnosti, nedonútiteľnosti k voľbe, demokratickosti či férovosti.

4.5.1.4 Rjaškovej model

Druhá uvedená modifikácia protokolu spĺňa požiadavky súkromnosti, nedonútiteľnosti k voľbe, robustnosti, univerzálnej i individuálnej overiteľnosti, ako aj férovosti. V [20] sa však uvádza existencia útoku na požiadavku oprávnenosti k voľbe v tejto schéme.

4.5.2 Zložitosť a parametre

Mnohé teoretické koncepty však nie sú prakticky realizovateľné, pretože v reálnom svete nemožno splniť (najmä pre vysokú zložitosť alebo finančnú náročnosť) predpoklady, na ktorých tieto schémy stavajú.V tejto práci sme sa aj preto pokúsili vybrať schémy, ktoré stavajú svoje požiadavky na reálnych základoch.

[16] alternatívne možno k hlasom pripojiť token identifikujúci voliča alebo schému rozšíriť o elektronický podpis hlasu kľúčom voliča

Tabuľka 4.1: Prehľad naplnenia požiadaviek uvažovanými modelmi

Požiadavka	**TrustVote**	**HS**	**Estónsky model**	**Rjaškovej model**
Demokratickosť	áno	áno	áno	**nie**
Férovosť	áno	áno	áno	áno
Overiteľnosť - individ. čiastočná	áno	áno	áno	áno
Overiteľnosť - individuálna	áno	áno	nie	áno
Overiteľnosť - univerzálna	áno	áno	nie	áno
Receipt-freeness	**nie**	áno	**viacnásobným hlasovaním**	áno
Robustnosť	áno	áno	**čiastočne**	áno
Súkromnosť	áno	áno	áno	áno

HS Zložitosť budeme počítať v počte potrebných prvkov grupy na nástenke. Pre $1 : L$ model to bude $2NL$ prvkov pre platné hlasy a $NL(2L+1)$ pre dôkazy $1-L$ re-enkrypcie. Tiež je potrebné zvážiť sťažnosti voličov a index zvoleného hlasu; výsledná zložitosť teda bude

$$O(NL^2)$$

Rjaškovej model Schéma výrazne znižuje zaťaženie bezpečného kanálu, čím je optimalizovaný objem prenášaných údajov. Pamäťová zložitosť (počet potrebných prvkov grupy) však ostáva zachovaná.

Pre lepšiu názornosť uvádzame súhrn požiadaviek v tabuľke 4.1.

Vzhľadom na uvedené vyhodnotenie, ale však najmä vzhľadom na fakt, že pre zabezpečenie dôveryhodnosti a umožnenie reálnej auditovateľnosti protokolu odbornou verejnosťou je potrebné navrhnúť protokol čo najjednoduchší s využitím minimálneho množstva komplikovaných matematických konštrukcií, rozhodli sme sa v ďalšom nevyužívať možnosti homomorfného šifrovania. Takéto schémy sú totiž pre reálne nasadenie príliš komplikované a neprehľadné, ale taktiež v nich nie sú naplnené niektoré dôležité funkčné a nefunkčné požiadavky.

Kapitola 5

Návrh systému

V tejto časti zhrnieme požiadavky kladené na volebnú schému, ako aj pristúpime k vytvoreniu jej modelu. Následne technicky popíšeme detaily navrhnutého volebného protokolu, ktorý bude spadať do kategórie úplných elektronických volieb (viď 3.2.5).

Z analýzy uvedenej v časti 4.5.2 vyplynulo, že existujúce riešenia elektronických volieb nespĺňajú všetky potrebné požiadavky. Preto je potrebné navrhnúť nový model, postavený na novom technickom protokole. Technická, organizačná a matematická zložitosť systémov využívajúcich homomorfné šifrovanie, potreba väčšieho počtu autorít, komplikované audity a nepriamočiara realizácia znižujú dôveryhodnosť technicky náročných protokolov. V tejto časti preto uvedieme protokol vyvinutý na základe transparentného a pravdepodobne ľahšie akceptovateľného estónskeho modelu 4.1.

5.1 Nefunkčné požiadavky

Vzhľadom na pochopiteľne vysoké nároky kladené odborníkmi i verejnosťou na bezpečnostné i iné charakteristiky potenciálnych elektronických volieb, vystáva mnoho požiadaviek, ktoré je potrebné zvážiť pri návrhu modelu a dôkladne ošetriť pri jeho implementácii. Podrobnejším rozborom požiadaviek kladených na manažérstvo kvality sa budeme zaoberať v časti 7.1. Z pohľadu manažérstva informačnej bezpečnosti návrh posúdime v časti 7.2. Konkrétne požiadavky, riziká či hrozby by mali byť analyzované a ošetrené na základe techník popísaných v [10] s prihliadnutím na existujúci ochranný profil [4].

5.1.1 Špecifické a bezpečnostné požiadavky

Štandardné požiadavky špecifické pre elektronické voľby, ktoré sa kryptografickým protokolom darí zvyčajne naplniť bez dodatočných predpokladov a problémov:

- **Oprávnenosť k voľbe** - voliť môžu práve všetci oprávnení voliči; dôležité je zabezpečiť, aby pri voľbách nikto nebol zvýhodnený alebo znevýhodnený, ako aj odmietnutie záškodníkov, ktorí volebné právo nemajú
- **Demokratickosť** - predstavuje prirodzenú požiadavku možnosti odovzdať práve 1 hlas každým voličom
- **Súkromnosť** voličovi zaručuje nespojiteľnosť ľubovoľného hlasu s jeho osobou. Ani volič, ani organizátor volieb a ani ľubovoľný pozorovateľ by nemali byť schopní zistiť, ako volič hlasoval
- **Robustnosť** je požiadavkou na všeobecnú odolnosť systému. Primerane malá[1] skupina voličov, ktorí sa nesprávajú podľa protokolu (zmýlia sa alebo úmyselne konajú inak), neoprávnených voličov či časť autorít môže zlyhať bez toho, aby to narušilo celkový priebeh a výsledok volieb v neakceptovateľnom meradle. Ako sa ukazuje v príkladoch protokolov v časti 4, ani táto požiadavka nie je návrhmi často naplnená, a predovšetkým modely nevyužívajúce rôzne treshold schémy (napr. Shamirovu pre delenie kľúča[2], treshold ElGamal, atp.) majú s jej napĺňaním principiálne problémy

Požiadavky, ktorých splnenie je zväčša problematické a vedie k dodatočným predpokladom alebo čiastočným riešeniam:

- **Individuálna overiteľnosť** znamená, že volič dokáže samostatne overiť, že jeho hlas sa úspešne a korektne započítal do výsledku volieb
- **Individuálna overiteľnosť - čiastočná** znamená, že volič síce nemusí dokázať overiť, že jeho hlas je započítaný vo výsledku - avšak dokáže overiť, že hlas prešiel do fázy spracovania hlasov

[1] Primerane malá v prípade voličov znamená zanedbateľná vzhľadom na ich celkový počet, v prípade autorít je zvyčajne určená ako časť menšia ako napríklad $\frac{1}{3}$ alebo iná zdôvodnená menšina a v prípade záškodníkov či útočníkov by malo ísť o odolnosť teoreticky absolútnu (v praxi, pochopiteľne, ohraničenú technickými limitmi)

[2] definícia schémy je uvedená v [2], str. 525-526

- **Univerzálna overiteľnosť**, analogicky, znamená, že ktokoľvek dokáže samostatne overiť, či všetky hlasy boli korektne spočítané a prirátané k výsledku

- **Férovosť** vyžaduje, aby nikto so zúčastnených alebo tretích strán nebol schopný získať čiastočné výsledky počas konania volieb; na zabezpečenie férovosti sa v uvažovaných návrhoch často využíva práve zdieľanie kľúča medzi viacerými autoritami a ukladanie hlasov v zašifrovanej podobe až do skončenia volieb

Spomeňme ešte jednu prirodzenú požiadavku kladenú na elektronické voľby, ktorá však, ako sa ukáže v časti 4, je vo väčšine súčasných modelov takmer nesplnená alebo vyžaduje dopĺňanie a úpravu protokolov.

- **Nemožnosť ovplyvnenia** voliča je teoretickým cieľom, podľa ktorého by nemalo byť pri zvolenej volebnej schéme možné donútiť voliča k voľbe. Ukazuje sa, že ide o požiadavku veľmi silnú a v praxi pravdepodobne nerealizovateľnú (predovšetkým ak uvažujeme model elektronických volieb s umožnením hlasovania z osobných počítačov pripojených do siete Internet). Podstatou tejto požiadavky je receipt-freeness[3]; volič by nemal byť schopný komukoľvek dokázať ako hlasoval; existujúce modely sa zväčša obmedzujú na zabezpečenie receipt-freeness, ktorá, ako sa ukazuje v časti 4, je sama o sebe ťažko vynútiteľná a dosiahnuteľná a často môže jej dosiahnutie kolidovať s dosiahnutím iných požiadaviek, ako je napríklad univerzálna overiteľnosť

5.1.2 Nešpecifické požiadavky

Požiadavky nešpecifické pre elektronické voľby:

- **Dostupnosť systému** - je potrebné zabezpečiť vysokú dostupnosť systému širokej verejnosti, a to z dvoch hľadísk; dostupnosti služby ako takej (napríklad ochrana pred útokmi typu DoS) a dostupnosti osobných počítačov, Internetu a elektronických volieb populácií. Táto požiadavka zahŕňa aj príslušnú hladinu informovanosti spoločnosti a primeranú marketingovo-informačnú kampaň

- **Spoľahlivosť systému**, ktorá je nevyhnutná najmä z dôvodu zabezpečenia všeobecnej dôvery ľudí v bezpečnosť a spoľahlivosť systému ako aj pre hladký priebeh hlasovania

- **Auditabilita systému** - je potrebné zabezpečiť možnosť analýzy a kontroly počas trvania volieb i po ich skončení, a to najmä určením vhodnej politiky pre audity

[3]absencia možnosti dokázať komukoľvek obsah svojho hlasu (voľný preklad, angličtina)

- **Transparentnosť a otvorenosť volieb** - je oprávnenou požiadavkou od naplnenia ktorej závisí, či ľudia elektronické voľby akceptujú alebo nie. Zahŕňa dobrú informovanosť spoločnosti o parametroch volebného systému, kontrolu protokolov, modelu a samotnej finálnej implementácie odbornou verejnosťou vrátane akademickej obce a spoločností zaoberajúcich sa informačnou bezpečnosťou, prehľadné zákonné úpravy volieb, operatívne riešenie vzniknutých problémov a mnoho ďalších prirodzených požiadaviek

- **Výhodnosť** ako pre štát (ekonomická výhodnosť, úspora ľudských zdrojov), tak pre voličov (napríklad voľba z pohodlia domova je z pohľadu voliča zvyčajne výhodou)

- **Flexibilita a mobilita systému**, ktoré by mali byť umožnené flexibilitou samotného návrhu a umožňovať jednoduché a lacné úpravy podľa aktuálnych požiadaviek na zmeny (volebného systému, bezpečnostných požiadaviek, spoločenskej situácie ..)

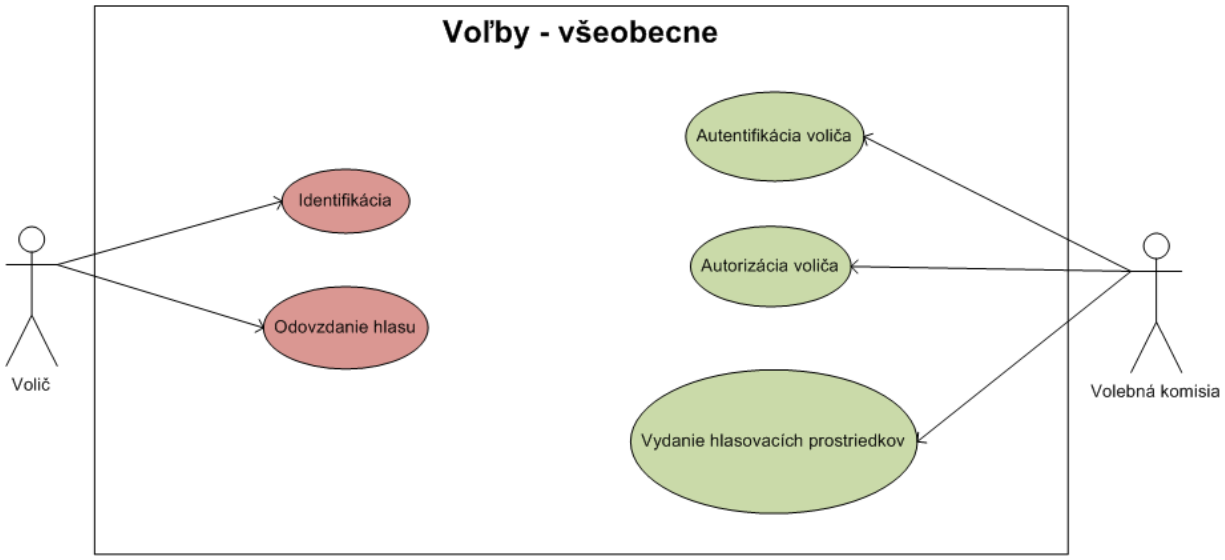
5.2 Cieľový model

Cieľový model identifikuje esenciálne akcie a procesy voľby alebo hlasovania. V use case diagrame[4] 5.2 sú základné identifikované akcie a procesy pridelené jednotlivým používateľom systému, a to najmä **voličovi**. **Volebná komisia** v tomto všeobecnom diagrame predstavuje všetkých aktérov, ktorí nie sú voličom.

Možno zhliadnuť, že primárnymi úlohami voliča sú **identifikovať sa** a **voliť**. Volebná komisia je zodpovedná za **autentifikáciu voliča**, ako aj za **autorizáciu** a následné **vydanie hlasovacích prostriedkov**. Voľba samotná už zvyčajne prebieha bez priameho zásahu volebnej komiesie[5].

[4]Slovenský preklad: Príklad použitia. Pre všeobecné zaužívanie pojmu use case budeme ďalej používať tento pojem.

[5]Samozrejme, odhliadnuc od mimoriadnych situácií, ktoré pre jednoduchosť na tejto úrovni modelu neuvažujeme

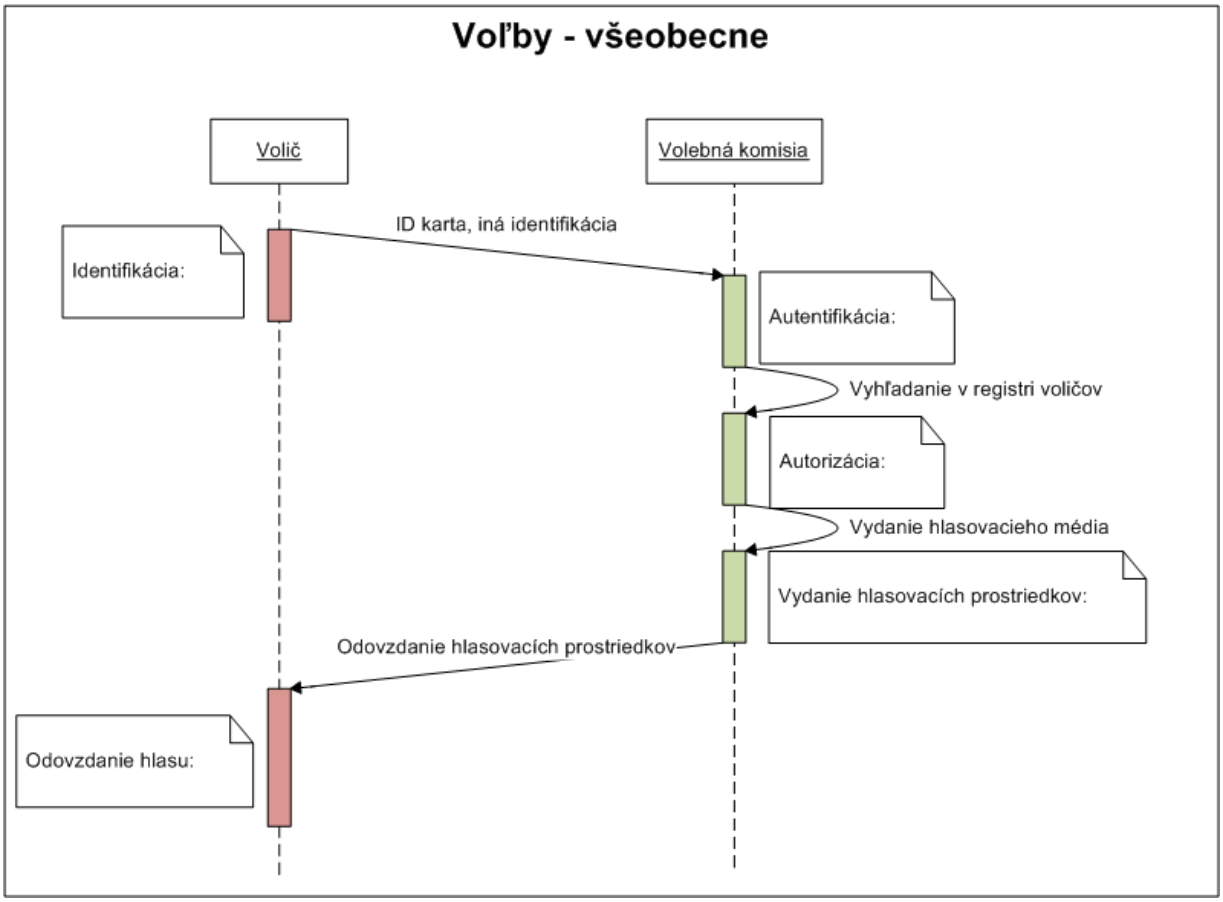


Obr. 5.1: Všeobecný UseCase diagram

V diagrame 5.2 sme formalizovali proces voľby alebo hlasovania ako taký. Možno nahliadnuť, že **identifikácia voliča** prebieha najmä prostredníctvom predloženia identifikačného dokladu a jeho overenia volebnou komisiou; v našom modeli budeme identifikačné doklady nazývať **identifikačnými kartami** a rozdeľovať do dvoch základných skupín, a to:

1. Elektronická identifikačná karta (eID)
2. Iná identifikačná karta alebo dokument

Autentifikáciu voliča vykonáva, podobne ako **autorizáciu**, volebná komisia. Autorizácia zväčša predstavuje vyhľadanie voliča v registri alebo obdobnú akciu. Po **vydaní hlasovacích prostriedkov** volebnou komisiou dochádza k voľbe samotnej, a teda k **odovzdaniu hlasu**. Keďže ide o hrubý model volieb, granularita oboch je zvolená na najvyššej postačujúcej úrovni.



Obr. 5.2: Všeobecný sekvenčný diagram

5.3 Navrhovaný protokol

5.3.1 Konvenčná časť protokolu

Popri hlasovaní prostredníctvom siete Internet je nevyhnutné v existujúcej miere[6] poskytovať voličom možnosť hlasovania v hlasovacích miestnostiach; v tejto časti popíšeme, ako bude prebiehať táto časť volebného protokolu. Perspektívne bude postačovať ponechanie možnosti elektronického hlasovania v kontaktných bodoch; z hľadiska lepšieho akceptovania zmien spoločnosťou sa však ukazuje ako užitočné ponechať po primeranú dobu i hlasovanie formou fyzického vhodenia hlasu v obálke do volebnej urny.

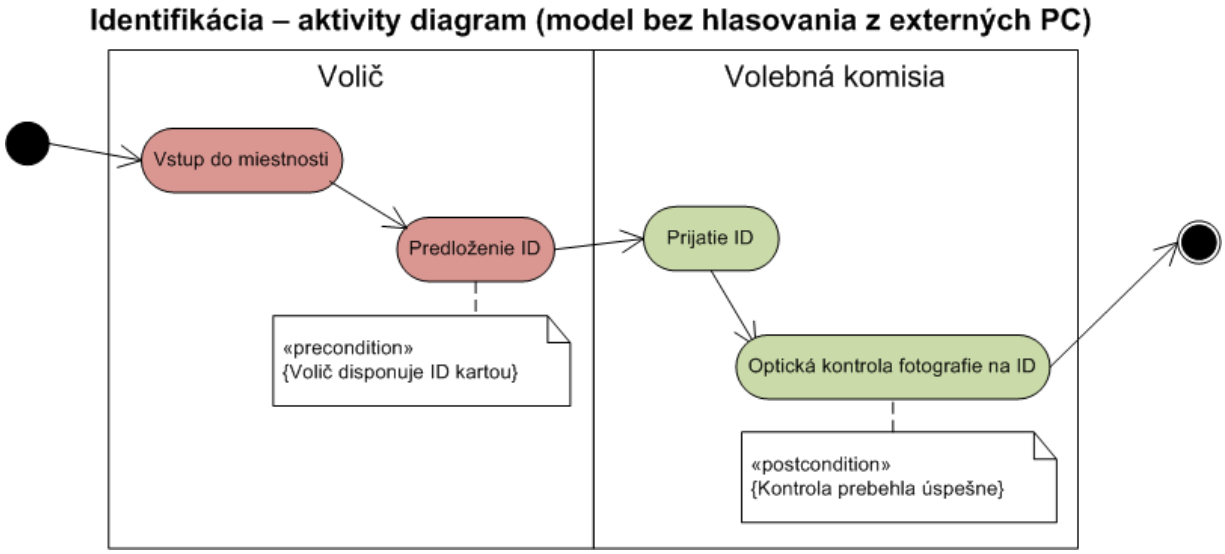
[6] aby sa neznížila dostupnosť volieb voličom

5.3.1.1 Identifikácia voliča

Základným predpokladom pre odovzdanie hlasu je identifikácia voliča, a to prostredníctvom identifikačnej karty, ktorej je vlastníkom. Volebná komisia identifikačnú kartu kontroluje tak, ako v doterajšom modeli volieb; zväčša teda ide iba o kontrolu fotografie na preukaze. Vo všeobecnosti možno identifikáciu voliča popísať nasledujúcou množinou akcií:

- Vstup do volebnej miestnosti, aktérom je volič
- Predloženie identifikačnej karty, aktérom je volič
- Prijatie identifikačnej karty, aktérom je člen Volebnej komisie
- Optická kontrola identifikačnej karty (zväčša fotografie), aktérom je člen Volebnej komisie

Aktivita identifikácie je znázornená na obrázku 5.3.



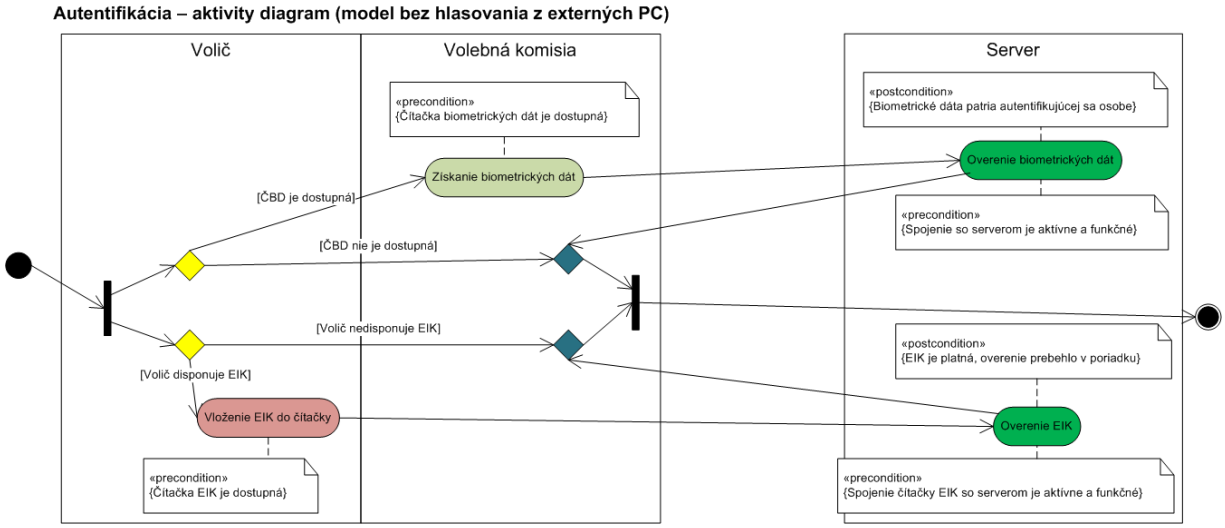
Obr. 5.3: Diagram aktivít - identifikácia (bez hlasovania z externých PC)

5.3.1.2 Autentifikácia voliča

Autentifikácia voliča zabezpečuje overenie jeho totožnosti; ako je naznačené na diagrame 5.4, overenie pozostáva z 2 častí:

- Overenie eID
- Overenie biometrických dát (voliteľné)

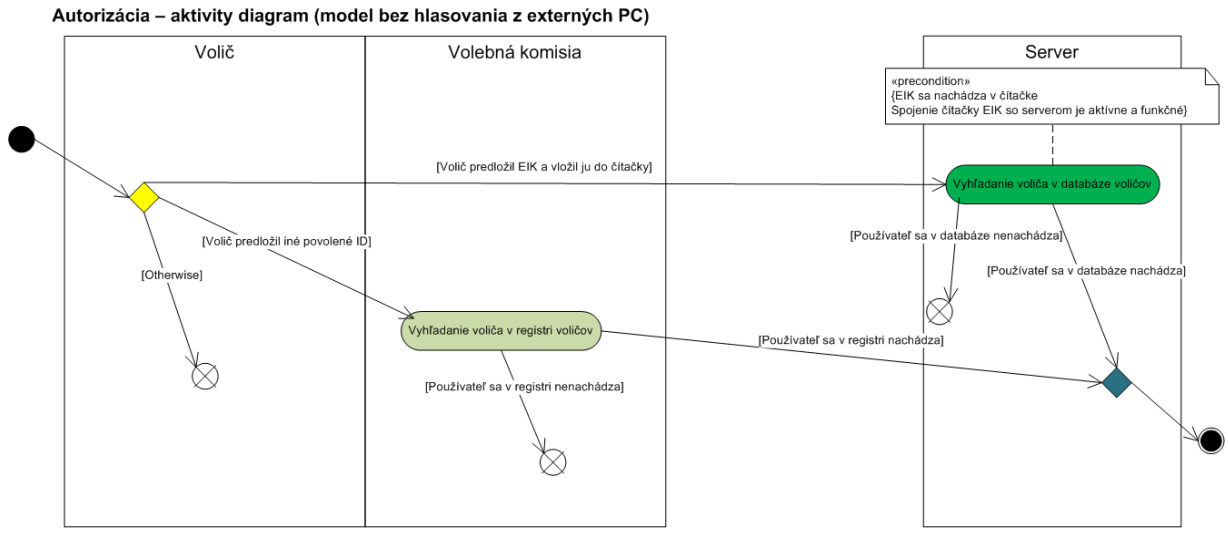
V oboch prípadoch sa získané údaje, či už čítačkou eID alebo čítačkou biometrických dát, porovnávajú s dátami v databázach na príslušných serveroch na to určených. Ak je dostupná možnosť získania a overenia biometrických údajov, oba tieto procesy musia prebehnúť úspešne, aby bola autentifikácia vyhodnotená ako úspešná; v opačnom prípade sa k autorizácii voliča nepristúpi.



Obr. 5.4: Diagram aktivít - autentifikácia (bez hlasovania z externých PC)

5.3.1.3 Autorizácia voliča

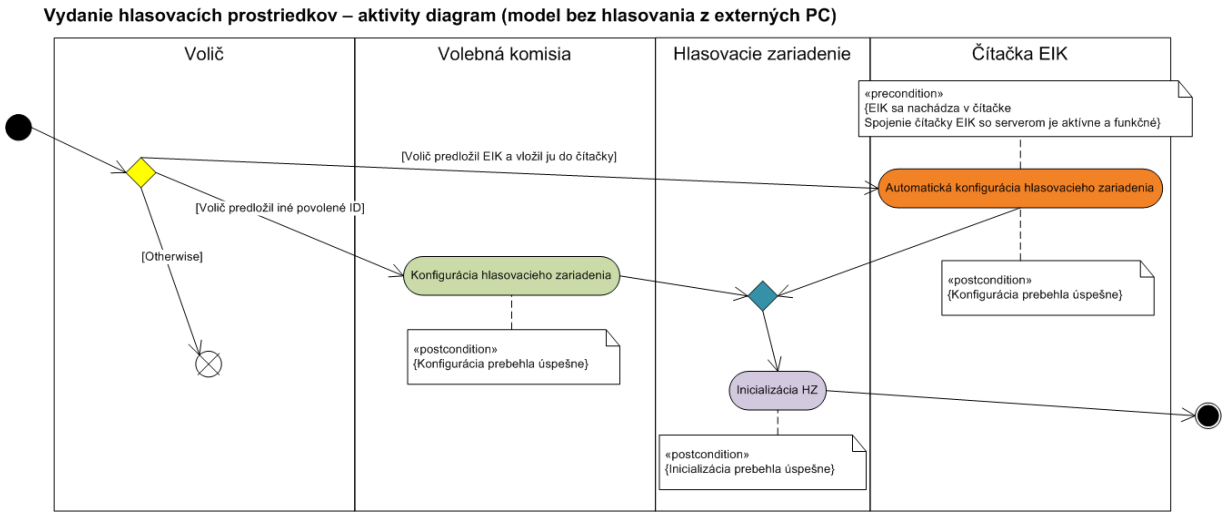
Predmetom autorizácie voliča je v prípade úspešného absolvovania identifikácie a autentifikácie voličom overiť, že je registrovaný v registri voličov, a teda oprávnený k voľbe. V prípade, že volič predložil eID, takéto overenie vykonáva priamo volebný server prostredníctvom komunikácie s čítačkou eID a príslušnou databázou, ktorá obsahuje register oprávnených voličov. Alternatívne, ak volič predložil iný povolený identifikačný dokument (napr. občiansky preukaz), voliča v registri manuálne vyhľadá poverený člen Volebnej komisie. Vyhľadanie zrejme bude spočívať vo vyhľadaní v rovnakej databáze, ktorú používa aj volebný server na autorizáciu voliča disponujúceho eID. Celá aktivita je vizualizovaná na diagrame 5.5.



Obr. 5.5: Diagram aktivít - autorizácia (bez hlasovania z externých PC)

5.3.1.4 Vydanie hlasovacích prostriedkov voličovi

V prípade, že hlasovanie v kontaktnom mieste je vykonávané prostredníctvom hlasovacích zariadení, vydanie hlasovacích prostriedkov znamená konfiguráciu príslušného hlasovacieho zariadenia. Toto zariadenie sa buď konfiguruje automaticky na základe dát získaných čítačkou eID, ak volič disponuje eID a vložil ju do čítačky, alebo ručne povereným členom Volebnej komisie, ak volič predložil iný povolený identifikačný dokument. Celá aktivita je vizualizovaná na diagrame 5.6.



Obr. 5.6: Diagram aktivít - vydanie hlasovacích prostriedkov (bez hlasovania z externých PC)

5.3.1.5 Odovzdanie hlasu voličom

Samotný proces odovzdania hlasu sa voličovi sprístupní až po úspešne vykonanej identifikácii, autentifikácii a autorizácii k voľbe. Po úspešne vykonanej konfigurácii hlasovacieho zariadenia, ktorá sa vykoná ako súčasť vydania hlasovacích prostriedkov voličovi, sa na zariadení zobrazia možnosti pre aktuálne prebiehajúce voľby. Po označení želanej voľby voličom a jej potvrdení hlasovacie zariadenie hlas odošle na volebný server, kde sa voľba overí a anonymizuje. Paralelne s týmto procesom sa voličovi, ktorý disponuje eID, karta vráti z čítačky. V prípade identifikácie voliča iným povoleným identifikačným dokumentom mu tento vráti poverený člen Volebnej komisie. Je dôležité podotknúť, že samotný tok dát medzi hlasovacím zariadením a volebným serverom nemusí prebehnúť okamžite; alternatívne môže k odovzdaniu dát dôjsť po dávkach alebo na fyzickom médiu napr. po ukončení volieb, alebo v zvolených časových intervaloch. V prípade uchovávania dát v zariadení je však potrebné zabezpečiť ich zálohovanie (v potrebnej miere) pre prípad zlyhania zariadenia, ako aj kryptografickú ochranu na zaistenie integrity,autentickosti a dôvernosti.

5.3.2 Elektronická časť protokolu

V tejto časti predstavíme protokol, ktorý odporúčame využiť ako základný stavebný kameň v prípade implementácie volieb umožňujúcich hlasovanie z ľubovoľného[7] počítača prostredníctvom siete Internet, v podmienkach Slovenskej republiky.

Technické a návrhové detaily protokolu, ako aj realizáciu pilotného projektu elektronických volieb s využitím uvedeného protokolu, možno nájsť v práci Bc. Filipa Vojtka [8].

5.3.2.1 Aktéri a systémy

V elektronickej časti volebného protokolu vystupujú nasledovní aktéri a systémy; uvádzame tiež hlavné úlohy daných komponentov systému:

- **Klientská časť**
  - Volič
    - Odovzdáva hlas
    - Overuje spracovanie hlasu (voliteľné)
  - Volebná aplikácia
    - Umožňuje voličovi odovzdať hlas vo voľbách, je nainštalovaná lokálne na osobnom počítači
- **Serverová časť**
  - Volebná komisia
  - Online server pre stiahnutie volebnej aplikácie (VAdownload)
    - Poskytuje volebnú aplikáciu
    - Poskytuje zoznam kandidátov (volebné listiny)
  - Online volebný server (OVS)
    - Komunikuje s Volebnou aplikáciou
    - Poskytuje dočasný kľúč dočasného úložiska hlasov
    - Odovzdáva hlas na ďalšie spracovanie

[7] určené požiadavky spĺňajúceho; požiadavky kladené na počítač by mali byť čo najviac minimalizované pre zabezpečenie vysokej dostupnosti možnosti odovzdať hlas elektronicky, ako aj vopred známe a presne špecifikované

    - Sprostredkúva autentifikáciu a autorizáciu voliča
  - Register voličov
  - Online server na spracovanie hlasov (OSSH)
    - Žiada o časovú pečiatku
    - Overuje hlas a vydáva potvrdenie o jeho spracovaní
  - Certifikačná autorita pre ZEP
  - Poskytovateľ časových pečiatok
  - Správcovia serverov a infraštruktúry
  - Dočasné úložisko hlasov
    - Prostredníctvom komunikácie s Registrom voličov autorizuje voliča
    - Odstraňuje neplatné hlasy
    - Odovzdáva hlasy na spočítavanie
  - Offline úložisko hlasov (OUH)
    - Vypočítava výsledok volieb
  - Server na zverejňovanie výsledkov
    - Publikuje výsledky volieb

5.3.2.2 Príprava volieb

Pred samotnou realizáciou volieb je potrebné vykonať nasledovné úkony a zabezpečiť nasledovné prostriedky:

1. Ustanoviť volebnú komisiu
2. Určiť dátum a čas konania volieb
3. Pomocou ZEP podpísať a publikovať kandidátne listiny (alebo listinu)
4. Vygenerovať kľúče pre prvú obálku (viď časť 5.3.2.3)
5. Prerozdeliť dešifrovacie tajomstvo prostredníctvom schémy na zdieľanie tajomstva (viď časť 3.9)
6. Vykonať kontrolu serverov (správcovia serverov)
7. Inicializovať elektronické voľby

5.3.2.3 Voľby

Navrhovaný volebný protokol okrem iného rozširuje estónsky model 4.1 o tretiu obálku. Hlas sa teda najprv zašifruje kľúčom pre elektronické voľby, následne podpíše ZEP voliča a šifruje dočasným kľúčom. Tieto 3 operácie budeme v ďalšom nazývať obálkami.

Zjednodušený priebeh volieb (zjednodušená štruktúra navrhovaného volebného protokolu) je zachytený v nasledovných bodoch:

1. Volič stiahne volebnú aplikáciu z Online serveru pre stiahnutie volebnej aplikácie[8]
2. Volič spustí volebnú aplikáciu
3. Volič sa identifikuje prostredníctvom eID
4. Voliča volebná aplikácia autentifikuje a autorizuje k voľbe (prostredníctvom komunikácie s volebným serverom)
5. Volič z volebného serveru stiahne dočasný kľúč pre druhú obálku a aktuálne kandidátne listiny (alebo listinu)
6. Volič zvolí požadovanú kandidátnu listinu a kandidátov pre práve vykonávané voľby (hlas) a daného voliča
7. Volebná aplikácia vygeneruje náhodné slovo (NIH), ktorý pripojí k hlasu
8. Volič potvrdí svoj hlas
9. Volebná aplikácia odošle hlas s pripojeným NIH v troch obálkach a NIH v otvorenom stave na volebný server
10. Volebný server overí štruktúru prijatých dát a odošle ich na Online server pre spracovanie hlasov
11. Online server pre spracovanie hlasov vygeneruje slepý podpis pre hlas v obálkach (viď 3.9)
12. Online server pre spracovanie hlasov požiada poskytovateľa časových pečiatok o časovú pečiatku pre hlas
13. Online server pre spracovanie hlasov odošle podpísaný NIH a hlas s časovou pečiatkou Volebnej aplikácií (týmto končí komunikácia klientskej a serverovej časti)

[8]Pre zabezpečenie autentickosti servera sa ten preukáže platným certifikátom

14. Online server pre spracovanie hlasov podpísaný hlas v troch obálkach zašle na Dočasný server

15. Po vypršaní platnosti dočasného kľúča sú dáta z Dočasného serveru presunuté (manuálne) na Offline úložisko hlasov

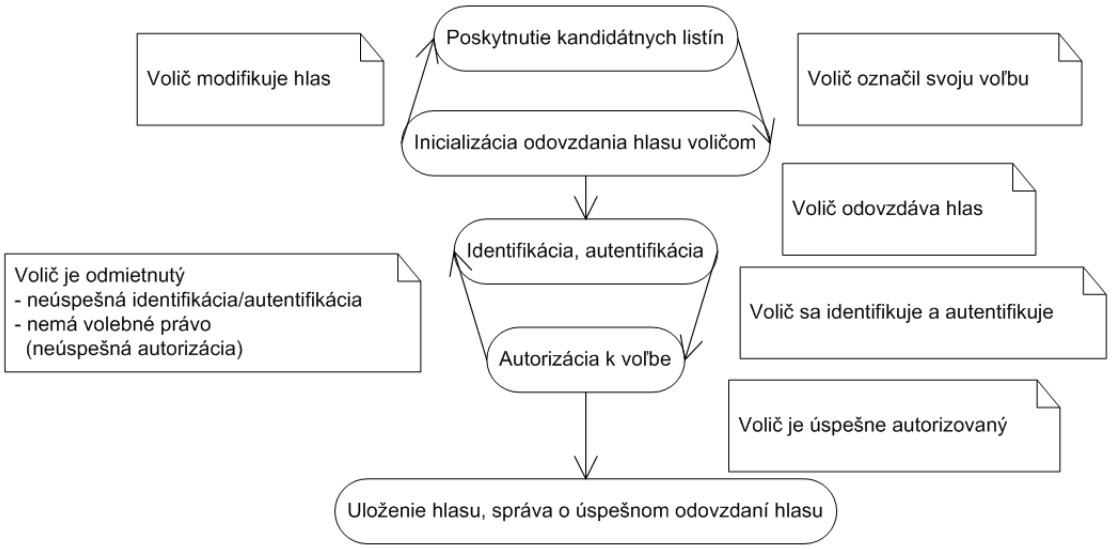
16. Po ukončení volieb Volebná komisia vygeneruje dešifrovací kľúč pre prvú obálku

17. Offline úložisko hlasov dešifruje a spočíta hlasy, výsledok zašle na Server na zverejňovanie výsledkov

18. Server na zverejňovanie výsledkov publikuje výsledky volieb

5.3.2.4 Technická realizácia

Pred detailným popisom volebného protokolu uvedieme princípy navrhovaného technického riešenia, ktoré pomôžu začleniť jednotlivé kroky do kontextu systému elektronických volieb. Protokol používame v jeho neinteraktívnej podobe - komunikácia serverovej a klientskej časti je sústredená iba do jednej časti protokolu (viď obr. 5.7).



Obr. 5.7: Schéma navrhovaného protokolu

Súhrnné technické riešenie

Súhrnné technické riešenie uvádzame na obrázku 5.8[9]. Servery pripojené priamo do siete

[9]fyzický počet serverov je ilustračný, ich reálny počet bude zvolený na základe parametrov konkrétnych použitých zariadení

Internet sú dostupné na IP adresách, ktoré sú pre potreby volieb priamo zadané vo Volebnej aplikácii. Pripojenie je, za účelom maximalizácie dostupnosti, poskytované prostredníctvom:

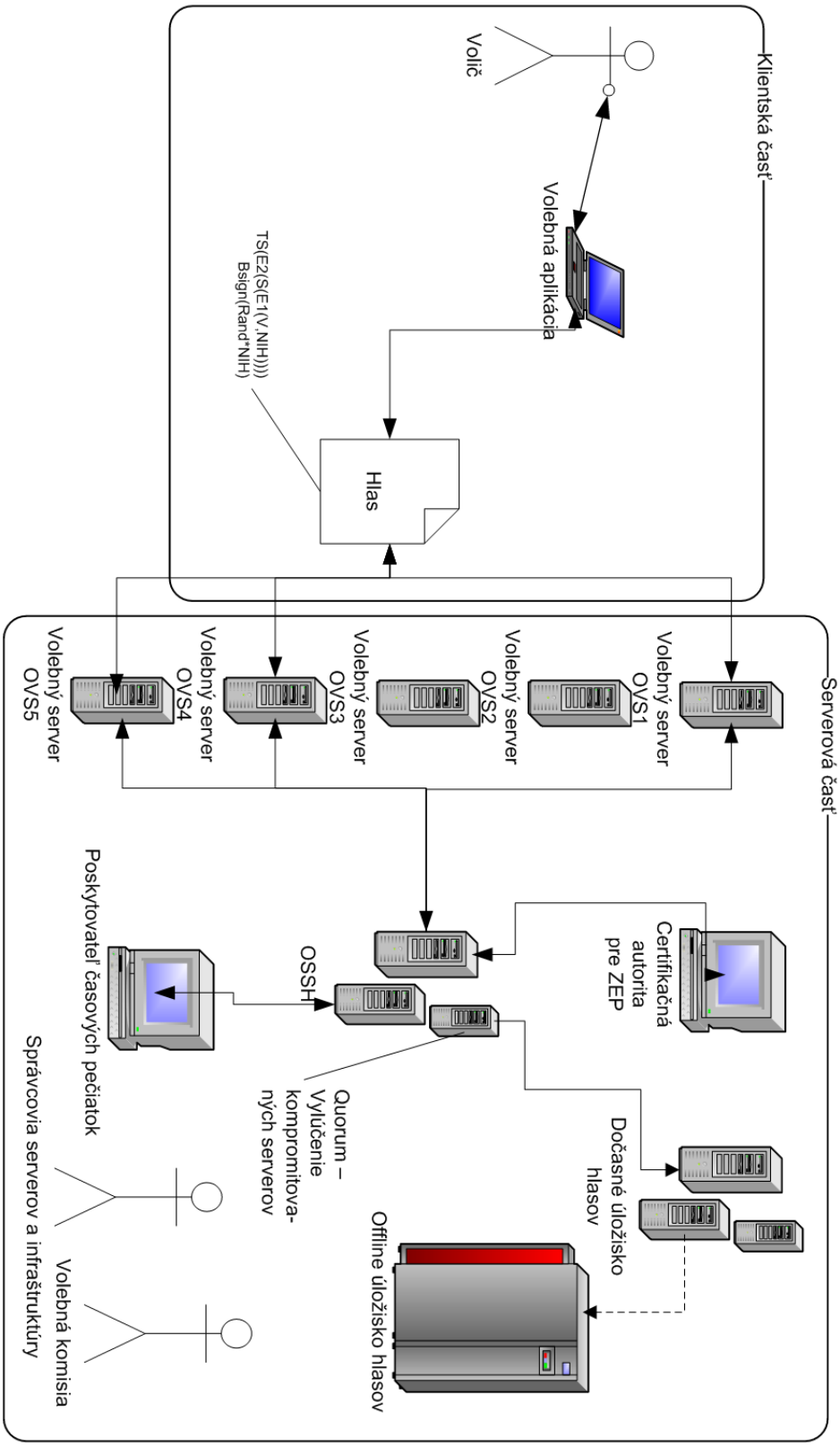
- Siete Govnet, nadrezortnej informačnej siete slúžiacej na efektívnu a bezpečnú výmenu informácií, ktorá vznikla na základe ustanovenia vlády SR č. 310 / 1993; táto sieť garantuje vysokú mieru dostupnosti a spoľahlivosti poskytovaných služieb
- Sietí ostatných poskytovateľov pripojenia do siete Internet

Volebná aplikácia komunikuje naraz s aspoň nadpolovičnou väčšinou takýchto serverov; OSSH server následne vyhodnotí zhodnosť informácií poskytnutých jednotlivými servermi a ak sú informácie totožné z nadpolovičnej väčšiny OVS, považuje hlas za korektne doručený. Na základe týchto informácií možno vylúčiť servery ktoré poskytujú dlhodobo nekorektné alebo kompromitované dáta zo siete a umožniť tak ich údržbu. Pre zvýšenie odolnosti serverov je možné využiť rôzne operačné systémy ako platformy pre OVS. Tiež je odporúčané na OVS využiť web servery navrhované pre zvládnutie vysokej záťaže ako NGINX[10] či Lighttpd[11]. Každý z využitých hardvérových komponentov poskytuje logy, ktoré je možné po vykonaní volieb auditovať[12].

[10] dostupné k 6.4.2012 na sieti Internet: `http://nginx.org/`

[11] dostupné k 6.4.2012 na sieti Internet: `http://www.lighttpd.net/`

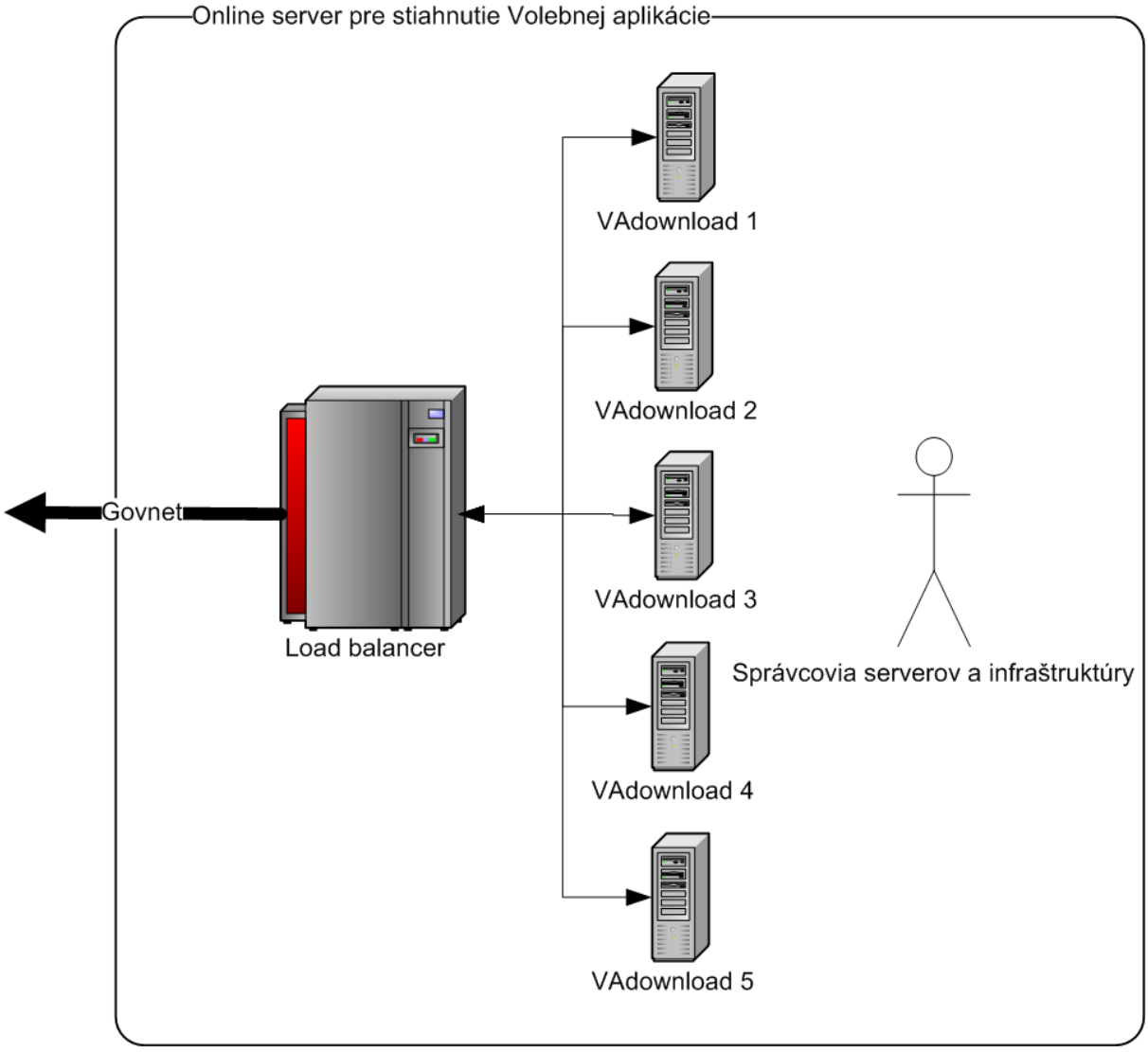
[12] pre možnú citlivosť údajov sú však logy fyzicky chránené, a to najmä po ukončení volieb



Obr. 5.8: Súhrnné technické riešenie

Štruktúra Online serveru pre stiahnutie Volebnej aplikácie

Online server pre stiahnutie VA pozostáva zo sústavy serverov pripojenej do siete Internet prostredníctvom load balanceru[13]



Obr. 5.9: Štruktúra Online serveru pre stiahnutie VA

[13]v navrhovanej implementácií pod pojmom load balancing (vyvažovanie záťaže) uvažujeme techniku, ktorá rozmiestňuje záťaž medzi dvoma alebo viacerými počítačmi, sieťovými pripojeniami, procesormi, pevnými diskami alebo inými zdrojmi za účelom dosiahnuť optimálne využitie zdrojov, maximalizovanie priepustnosti, minimalizovanie času odozvy a pomáha predchádzať preťaženiu. Využívanie viacerých komponentov s použitím load balancingu namiesto jedného komponentu môže zvýšiť spoľahlivosť (systém má vyššiu redundanciu). Služba Load Balancing je zvyčajne zabezpečená dedikovaným hardvérovým zariadením (ako viacvrstvový switch albo DNS server). Viac informácií o problematike možno nájsť v [24]

5.3.2.5 Detailný popis vykonávaných operácií

Stiahnutie volebnej aplikácie

Pri sťahovaní Volebnej aplikácie je dôležité spomenúť, že ide o stiahnutie tzv. statického obsahu, ktorého poskytovanie je jednoduchšie a menej náchylné na útoky zahltením ako poskytovanie obsahu dynamického. Odporúčané technické riešenie Online serveru pre stiahnutie VA je načrtnuté na obrázku 5.9[14]. Stiahnutie volebnej aplikácie prebieha nasledovne:

1. Volič vloží do poľa Adresa internetového prehliadača určenú adresu, ktorá bude publikovaná pred spustením elektronických volieb[15]. Volebná aplikácia je program vyvinutý na platforme Java, ActiveX, Flash alebo v inej, v čase realizácie elektronických volieb dostupnej a pre tento účel vhodnej vhodnej platforme[16]; zo strany serveru teda ide o službu ponúkania stiahnutia statického obsahu

2. Aplikácia sa spustí v internetovom prehliadači voliča

3. V aplikácii sú zadané IP adresy Online volebných serverov[17], s ktorými priamo komunikuje a inicializuje proces odovzdania hlasu

Identifikácia a autentifikácia voliča

Volič sa voči volebnej aplikácií identifikuje jemu pridelenou identifikačnou kartou s čipom; občianske preukazy s čipom budú vydávané na základe zákona [35] a pre potreby tejto práce uvažujeme, že občianske preukazy s čipom sú všeobecne rozšírené[18]. Čip občianskeho preukazu (eID) obsahuje súkromný kľúč držiteľa občianskeho preukazu, certifikát jeho verejného kľúča a aplikáciu na vytváranie ZEP (podpisovač) podľa zákona [28], ako aj digitálne dáta o občanovi resp. voličovi v rozsahu aspoň takom, v akom sú uvedené na občianskom preukaze, alebo v rozsahu primeranom potrebám implementácie elektronických volieb[19].

[14] fyzický počet serverov je ilustračný, ich reálny počet bude zvolený na základe parametrov použitých technických zariadení

[15] napr. www.evolby.sk

[16] informácie o uvedených platformách možno nájsť na internetových stránkach ich výrobcov, teda spoločností (v uvedenom poradí) Oracle, Microsoft a Adobe

[17] takto možno čiastočne predchádzať riziku napadnutia DNS serverov poskytovateľov Internetu

[18] ich penetrácia v spoločnosti bude v konečnom čase významná resp. úplná

[19] týmto zdôrazňujeme napr. uvádzanie prípadného nového identifikačného kódu občana po prípadnej zmene systému rodných čísel

1. eID, teda občiansky preukaz s čipom, volič vloží do čítačky eID pripojenej k počítaču, prostredníctvom ktorého plánuje odovzdať svoj hlas v aktuálne prebiehajúcich voľbách[20]

2. Volič spustí Volebnú aplikáciu

3. Volebná aplikácia započne komunikáciu s čítačkou a v nej vloženým eID; podľa [35], §4b, na potvrdenie totožnosti držiteľa občianskeho preukazu slúži Bezpečnostný osobný kód, ktorý volič zadá pre overenie svojej totožnosti (autentifikáciu)

Stiahnutie kandidátnych listín

Na základe identity voliča Volebná aplikácia z Online server pre stiahnutie VA stiahne množinu kandidátnych listín, ktoré sú pre dané voľby a daného voliča relevantné[21]. Komunikácia prebieha nasledovne:

1. Volebná aplikácia (podľa miesta trvalého bydliska) určí relevantné kandidátne listiny

2. Volebná aplikácia stiahne relevantné kandidátne listiny z VAdownload

Vyplnenie hlasu

Volič prostredníctvom používateľského rozhrania Volebnej aplikácie označí zvolenú kandidátnu listinu a zvolených kandidátov. Volebná aplikácia zabezpečí korektnosť hlasu, a to nasledovne:

- Overí, že volič zvolil práve jednu kandidátnu listinu (ak nie je určené inak)

- Overí, že volič zvolil správny počet kandidátov (špecifický pre dané voľby, teda napr. 0 až 4 kandidátov pre voľby do NrSr)

Kódovanie hlasu

Po vyplnení hlasu volebná aplikácia hlas zakóduje do XML dokumentu[22]. Štruktúra doku-

[20] čítačka eID bude voličovi vydaná na základe nariadenia alebo zákona, ktorý bude vydanie čítačiek upravovať; môže ísť napríklad o súbežné vydanie s vydaním nového občianskeho preukazu občanovi alebo o vydanie na inom úrade na to určenom

[21] ide najmä o zaslanie správnej listiny pri voľbách do samospráv, prípadne po implementácii viacobvodového volebného systému do NrSr

[22] eXtensible Markup Language, rozšíriteľný značkovací jazyk, vyvinutý a štandardizovaný konzorciom W3C; internetové stránky dostupné k 6.4.2012: `http://www.w3.org/XML/`

mentu je popísaná vo formáte XML Schema[23]; XML dokumenty sú vhodné na kódovanie posielanej informácie najmä pre ich jednoduchú integráciu a používanie.

Získanie dočasného kľúča

Dočasný kľúč pre elektronické voľby je kľúčom, ktorý sa obmieňa po presne určených intervaloch (napríklad 6 hodín). Jeho cieľom je najmä odľahčiť Online server na spracovanie hlasov a umožniť zníženie nielen pamäťových, ale i výpočtových požiadaviek na tento server. Dočasný kľúč je na požiadanie distribuovaný prostredníctvom Online volebných serverov, ktoré ho získajú z OSSH, ktorý ho získa z Dočasného úložiska hlasov. Uvedený postup tiež komplikuje niektoré typy útokov využívajúcich časovanie, a to priamočiarym vylúčením hlasov, ktoré nie sú šifrované platným dočasným kľúčom (prislúchajúcim danej časovej pečiatke).

Odoslanie a prijatie hlasu

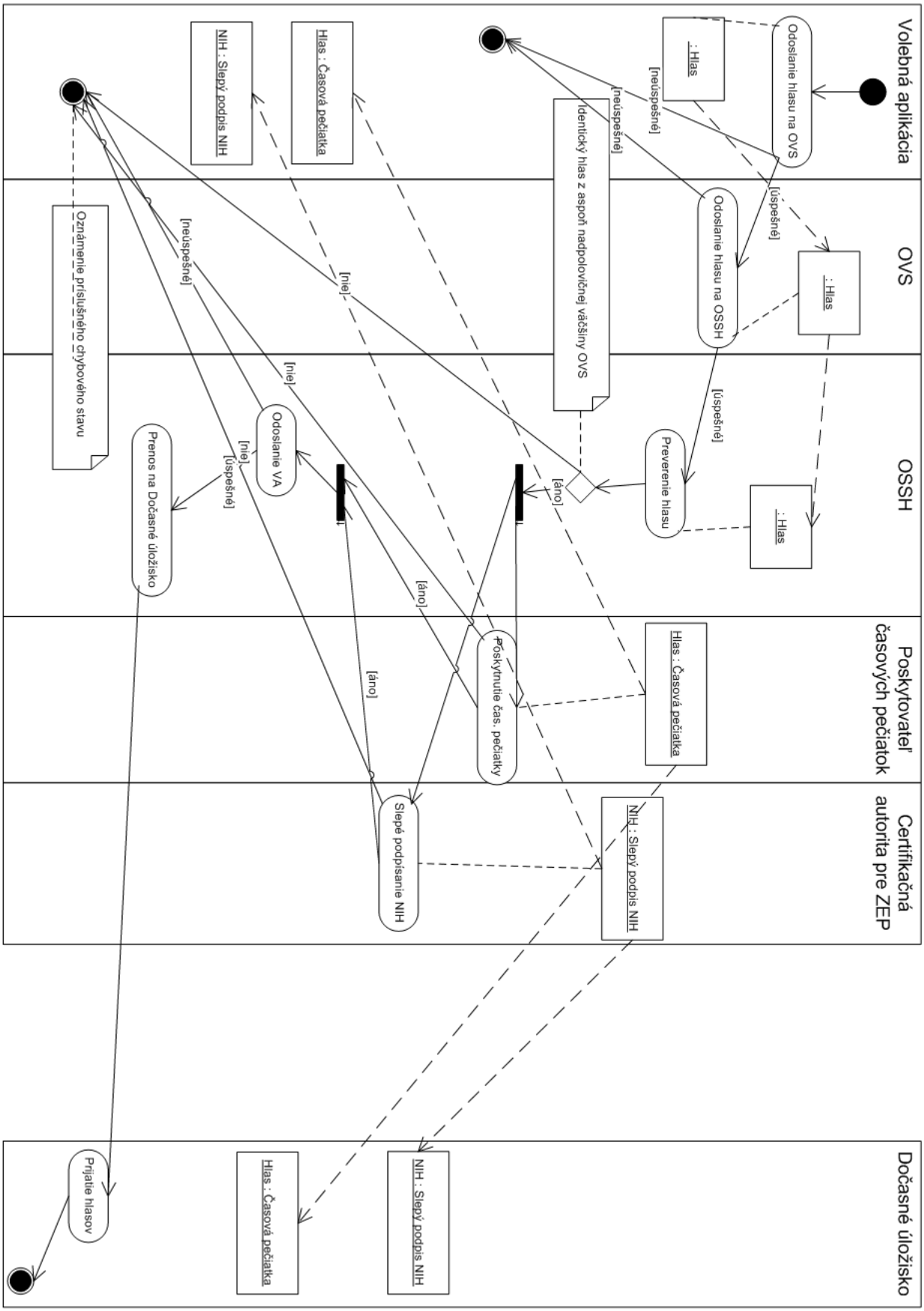
Hlas je volebnou aplikáciou odoslaný na najmenej nadpolovičnú väčšinu OVS. Tieto servery hlas odošlú na OSSH, kde sa skontroluje, či aspoň z nadpolovičnej väčšiny hlasov prišiel identický hlas. Ak bola uvedená podmienka splnená, OSSH vygeneruje slepý podpis pre doručený NIH. OSSH taktiež od Poskytovateľa časových pečiatok získa pre daný hlas časovú pečiatku. Následne je hlas spolu s podpísaným NIH OSSH uložený a volebnej aplikácii je odoslaný podpísaný NIH a hlas s časovou pečiatkou. Týmto je komunikácia medzi Klientskou a Serverovou časťou ukončená.

Následne sa hlas uloží a po vypršaní platnosti dočasného kľúča zašle na Dočasné úložisko. Tento technický krok je možné realizovať viacerými spôsobmi:

- Ručným preneseným na prenosnom médiu, napr. optické médium, na to povereným pracovníkom
- Využitím read-only súborového systému, teda súborového systému, ktorý je zdieľaný medzi OSSH a Dočasným úložiskom a povolené operácie sú práve zápis z OSSH a čítanie z Dočasného úložiska; po načítaní všetkých hlasov je načítaná dávka hlasov zo súborového systému odstránená

Pre komplexnosť tejto fázy ju vizualizujeme prostredníctvom UML Diagramu 5.10.

[23] formát vyvinutý a štandardizovaný konzorciom W3C; internetové stránky dostupné k 6.4.2012: `http://www.w3.org/XML/Schema`



Obr. 5.10: Odovzdanie a prijatie hlasu - UML diagram

Informácia pre voliča

Pre zabezpečenie čiastočnej individuálnej overiteľnosti (viď časť 5.1.1) sme implementovali systém NIH. Vďaka "trojobálkovému"systému možno poskytnúť voličovi čiastočné overenie, že jeho hlas bude započítaný do výsledku volieb, a to prostredníctvom poskytnutia nasledovných dát Serverovou časťou protokolu Volebnej aplikácii:

- **Časovej pečiatky**, ktorej aktuálnosť a platnosť dokáže VA vyhodnotiť
- **Porovnania prijatého a odoslaného hlasu**
- **Slepého podpisu NIH**, ktorého platnosť VA overí a zrekonštruuje pôvodný NIH

Zmena dočasného kľúča

Takzvaná tretia obálka, teda šifrovanie hlasu tretím kľúčom, prináša do protokolu nasledovné vlastnosti:

- Ochranu súkromnosti hlasovania, a to vďaka znemožneniu identifikácie voliča i v prípade napadnutia online časti Serverovej časti protokolu. Šifrovanie dočasným kľúčom znemožňuje identifikáciu voliča pred prenesením na Dočasné úložisko a rozbalením hlasov. Táto zmena je podstatnou modifikáciou najmä v porovnaní s estónskym modelom (viď kapitola 4.1)
- Zvýšenie spoľahlivosti a odolnosti systému vďaka možnosti odfiltrovať syntakticky nekorektné hlasy (napr. neúspešne validované voči príslušnej XML Schema)
- Zvýšenie výkonu systému vďaka voliteľnému predspracovaniu hlasov po dávkach na OSSH

Nový dočasný kľúč je vygenerovaný v prípade, že:

- Žiaden dočasný kľúč neexistuje
- Dočasný kľúč má ostávajúcu dobu platnosti kratšiu ako určená minimálna doba platnosti, napríklad 30 minút

Akceptované sú vždy hlasy, ktoré sú šifrované platným dočasným kľúčom (platnosť kľúča možno určiť z príslušnej časovej pečiatky pridruženej k hlasu). Následne sú hlasy presunuté na Dočasné úložisko (viď vyššie). Dočasné úložisko nad prijatou dávkou dát vykoná nasledovné úkony:

1. Dešifruje hlasy (odstráni z nich tretiu obálku)
2. (voliteľné)[24] Overí integritu a autentickosť hlasov pomocou preverenia platnosti ZEP
3. (voliteľné) Uloží časové pečiatky do zoznamu spracovaných časových pečiatok
4. Overí formát hlasov a hlasy v neplatnom formáte zaradí na zoznam hlasov s neplatným formátom (na základe údajov z časovej pečiatky)

Ošetreniu výnimiek, ktoré môžu pri týchto aktivitách nastať, sa venujeme v časti Určenie výsledkov volieb a 5.3.2.7.

Ukončenie hlasovania

Ukončenie hlasovania môže nastať najmä z nasledovných dôvodov:

- Hlasovanie je ukončené po uplynutí času určeného pre elektronické voľby od začiatku volieb. V prípade potreby je možné hlasovanie predĺžiť v súlade s legislatívnymi opatreniami, ktoré takéto predĺženie povolia
- Hlasovanie je ukončené pre výskyt mimoriadnej situácie. Ide o ukončenie z mimoriadnych príčin, ktoré určí príslušná legislatíva[25].

Určenie výsledkov volieb

Po ukončení hlasovania dôjde k nasledovným akciám:

1. Odpojenie Serverovej časti protokolu od siete Internet
2. OSSH odovzdá poslednú dávku hlasov na spracovanie Dočasnému úložisku[26]
3. Dočasné úložisko filtruje hlasy podľa ich platnosti a korektnosti a vytvára pomocné zoznamy nasledovne (grafické znázornenie uvádzame v diagrame 5.11):
   (a) Dočasné úložisko overí platnosť ZEP

[24] body 2 a 3 je možné realizovať pre optimalizáciu vyťaženia úložných priestorov a výpočtovej sily na spočítavanie výsledkov volieb; ich implementácia však nie je nutná pre funkčnosť systému elektronických volieb. Konkrétna realizácia akcií 2 a 3 je detailne ozrejmená v časti Určenie výsledkov volieb a na diagrame 5.11

[25] napríklad preukázaná manipulácia volieb, občianska vojna, prírodná katastrofa veľkého rozsahu, a pod.

[26] z dôvodu jednoduchšieho vylúčenia podvrhnutých hlasov po ukončení hlasovania je užitočné zabezpečiť, aby platnosť dočasného kľúča vypršala v momente ukončenia hlasovania

i. Ak je ZEP neplatný, odstráni časovú pečiatku a ZEP a umiestni hlas na zoznam neplatných hlasov

ii. Dočasné úložisko odstráni časovú pečiatku a ZEP duplicitných hlasov; hlasy umiestni na zoznam neplatných hlasov[27]

iii. Inak odstráni časovú pečiatku a ZEP a umiestni hlas na zoznam platných hlasov

4. Spermutuje zoznamy
   - Platných hlasov
   - Neplatných hlasov
5. Pripraví zoznamy
   - Platných hlasov
   - Neplatných hlasov
   - Hlasov s neplatným formátom
   - Zoznam spracovaných časových pečiatok
6. Poverení členovia správcov infraštruktúry a volebná komisia spoločne prenesú na fyzickom (napr. optickom) médiu zoznamy z predchádzajúceho bodu na Offline úložisko hlasov (OUH)
7. OUH overí integritu a autentickosť prenesených zoznamov
8. Členovia volebnej komisie zrekonštruujú kľúč na dešifrovanie výsledkov
9. OUH dešifruje platné hlasy a overí ich formát
   - Hlasy so správnym formátom započíta do výsledkov volieb a príslušný NIH zaradí do zoznamu spracovaných NIH
   - Hlasy s neplatným formátom uloží[28] do zoznamu hlasov s neplatným formátom a príslušný NIH zaradí do zoznamu spracovaných NIH
10. OUH dešifruje hlasy zo zoznamu neplatných hlasov a overí ich formát
    - Pre hlasy so správnym formátom NIH zaradí do zoznamu spracovaných NIH

[27] neuvádzame v diagrame 5.11 pre zvýšenie prehľadnosti

[28] zašifrované

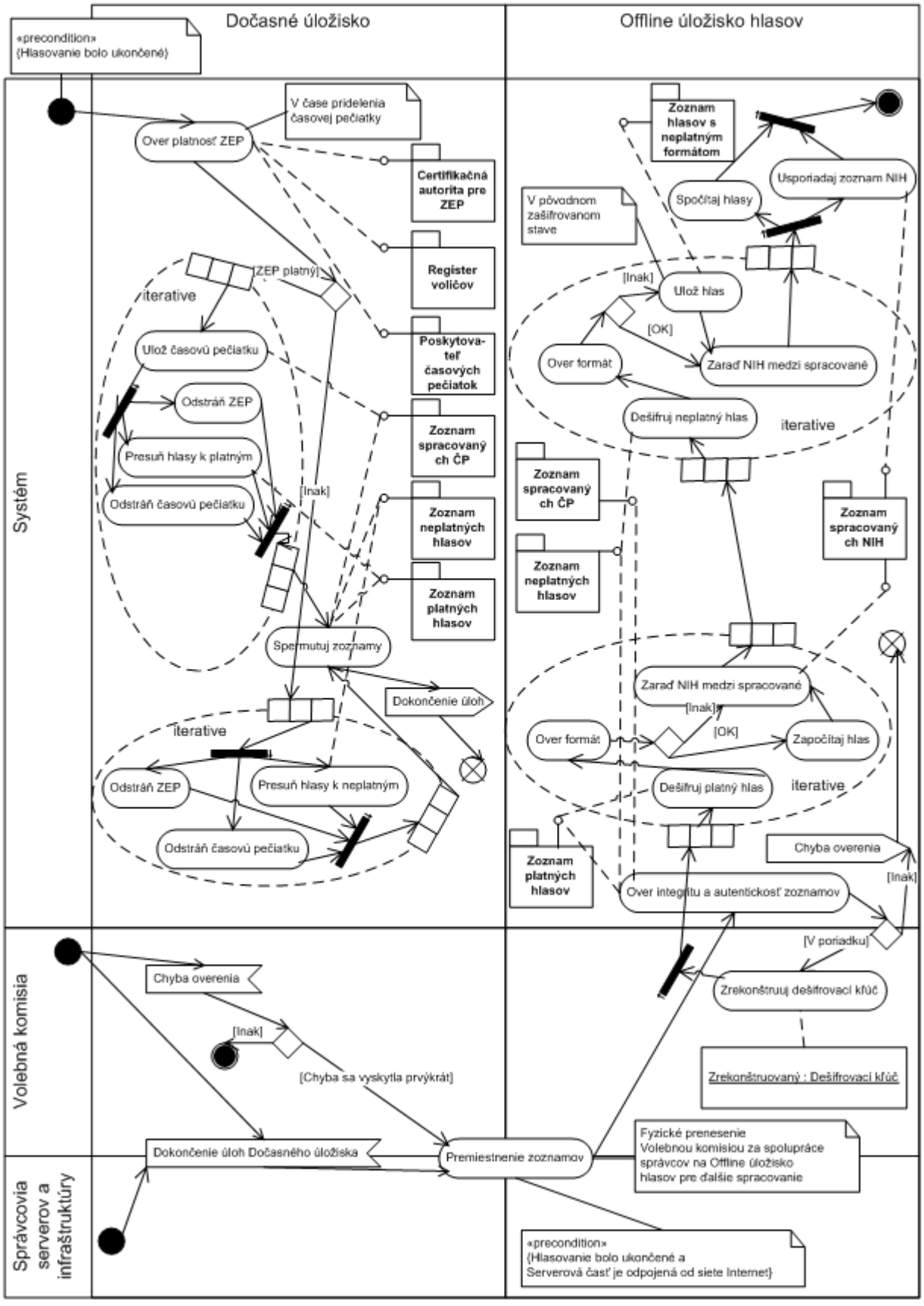
- Hlasy s neplatným formátom uloží[29] do zoznamu hlasov s neplatným formátom a príslušný NIH zaradí do zoznamu spracovaných NIH

11. OUH usporiada zoznam spracovaných NIH

12. OUH vypočíta výsledok volieb

Následne prebehnú potrebné kroky (v súlade s príslušnou legislatívou) na potvrdenie výsledkov volieb Volebnou komisiou.

[29] zašifrované



Obr. 5.11: UML diagram - Určenie výsledkov volieb

Zverejnenie výsledkov volieb a dodatočné procesy

Po potvrdení záväznosti resp. platnosti výsledkov volieb sú výsledky premiestnené (manuálne z OVS[30]) na Server na zverejňovanie výsledkov. Na server sú prenesené tieto dáta:

- Výsledky volieb
- Zoznam spracovaných NIH, čo umožní čiastočnú individuálnu overiteľnosť pre tento model elektronických volieb
- Zoznam spracovaných časových pečiatok
- Zoznam časových pečiatok hlasov s neplatným formátom (zoznam hlasov s neplatným formátom)

Paralelne bude pristúpené k nenávratnému odstráneniu všetkých dát z ostatných serverov serverovej časti systému, ako i k nenávratnému zneškodneniu prípadných použitých prenosných médií. Logy serverov sú monitorované a je k nim riadený (zakázaný) prístup.

5.3.2.6 Ďalšie usmernenia

Jednou z hlavných súčastí systému elektronických volieb je Volebná aplikácia. Ako sme už uviedli v časti 5.3.2.5, odporúčané vyhotovenie aplikácie je vo forme tzv. Internetovej aplikácie spúšťanej v prehliadači voliča. Jej výhodou oproti desktopovej aplikácii je širšia kompatibilita (v prípade využitia napr. platformy Java alebo Flash) a jednoduchšie používanie, kde používateľ nie je nútený inštalovať dodatočný softvér na počítač. Z pohľadu transparentnosti aplikácie by vývoj aplikácie mal byť otvorený kontrole a pripomienkovaniu širokej verejnosti, návrh, vývoj a testovanie vykonávané s podporou odbornej komunity a odborníkov z akademickej sféry, a to za účelom minimalizácie chýb[31] v tomto softvéri.

Hardvérové i softvérové vybavenie je potrebné pravidelne kontrolovať; v prípade možnosti zapožičania hardvérového vybavenia pre potreby volieb je odporúčaná jeho správa nezávislými odborníkmi z IT sféry.

5.3.2.7 Ošetrenie výnimiek

Pre dosiahnutie transparentného a zrozumiteľného správania sa aplikácie je dôležité reagovať na prípadné chyby či problémy vhodne zvoleným chybovým hlásením a príslušným ošetrením vzniknutej výnimky. Promptné reportovanie a riešenie problémov je nevyhnutné

[30] opäť je možné použiť napr. optické médiá alebo vhodne nakonfigurovaný read-only systém súborov

[31] a teda zraniteľností

z dôvodu zabezpečenia vysokej dostupnosti systému, ako aj jeho dôveryhodnosti v očiach verejnosti.

- Počas prípravy volieb sa preukážu pochybenia, ktoré sú závažné alebo môžu mať vplyv na priebeh alebo výsledok volieb. V takomto prípade je potrebné prijať všetky opatrenia aby k ovplyvneniu nedošlo, kontaktovať príslušných odborníkov a existujúci problém promptne vyriešiť. V prípade, že tak nie je možné vykonať do spustenia volieb, spustenie volieb je potrebné odložiť

- Volebná aplikácia neprešla interným testom autentickosti a integrity u voliča. V takom prípade môže ísť o chybu prenosu alebo o podvrhnutie resp. pozmenenie časti aplikácie a je potrebné ju opätovne stiahnuť. Ak problém pretrváva, je potrebné, aby volič informoval príslušné orgány

- Volič nemôže overiť niektorý verejný kľúč alebo zoznam kandidátov respektíve tieto údaje získať, čo znamená nedostupnosť koreňového certifikátu alebo spojenia na príslušné servery online časti protokolu. Akcie je potrebné opakovať a pri neúspechu opäť kontaktovať príslušné orgány

- Volič sa neúspešne identifikoval (neprebehla autentifikácia) voči Volebnej aplikácii; volič teda nedisponuje správnym eID alebo nemá správnu čítačku eID alebo nemá správny softvér na spoluprácu eID a Volebnej aplikácie; po preverení uvedených možností je potrebné kontaktovať príslušné orgány

- Volebnej aplikácii sa nepodarilo spojiť s Online volebnými servermi. Ak je možné overiť pripojenie používateľa do siete Internet, ide v prípade implementácie protokolu v navrhovanom technickom riešení pravdepodobne o priame napadnutie volebných serverov alebo o intenzívny útok typu DoS alebo DDoS. V takomto prípade je verejnosť potrebné informovať všeobecnými komunikačnými kanálmi o vzniknutej situácii a jej ďalšom riešení

- Dáta prijaté OSSH z rôznych OVS sa nezhodujú. Je potrebné vyhodnotiť potenciálne zdroje chyby a opakovanie chyby; v prípade častého chybného výstupu niektorého zo serverov OVS je potrebné tento server auditovať a prípadne vylúčiť zo systému

- Spracovanie hlasu na OSSH nebolo úspešné. Je potrebné identifikovať chybu (nesprávny formát, kontrolný súčet, nedoručenie zhodného hlasu z postačujúceho počtu serverov) a oboznámiť s navrhovaným riešením voliča

Ostatné vzniknuté výnimky budú ošetrené štandardnými procesmi a oznámené príslušnými chybovými hláseniami voličovi a/alebo zodpovedným orgánom.

Po ukončení volieb má volič možnosť overiť, či bol jeho hlas v rámci volieb spracovaný. Ak volič svoj NIH v zozname spracovaných NIH nenájde, je oprávnený podať sťažnosť. V prípade podania sťažnosti voličom prebieha riešenie sťažnosti nasledovne:

1. Volič poskytne príslušným orgánom NIH a časovú pečiatku, ktorú získal z Volebnej aplikácie
2. Ak sa NIH nachádza na zozname spracovaných NIH, sťažnosť je zamietnutá. Hlas bol spracovaný
3. Ak je časová pečiatka neplatná, sťažnosť je zamietnutá. Volič poskytol nekorektné údaje
4. Ak NIH nie je korektne podpísaný, sťažnosť je zamietnutá. Volič poskytol nekorektné údaje
5. Ak sa časová pečiatka nachádza na zozname hlasov s neplatným formátom, sťažnosť je zamietnutá. Hlas nemal platný formát
6. Ak sa časová pečiatka nenachádza na zozname spracovaných časových pečiatok, sťažnosť je zamietnutá. Hlas bol pravdepodobne podvrhnutý
7. Inak je sťažnosť oprávnená; je potrebné preskúmať podrobnosti, auditovať logy serverov a vyhodnotiť, či je potrebné prípadne anulovať výsledky volieb

Praktickú realizovateľnosť riešenia overíme v nasledujúcej kapitole.

Kapitola 6

Uskutočniteľnosť a náklady na elektronické voľby

Konvenčné (klasické) voľby sú pomerne nákladnou záležitosťou; ukazuje sa však, že ani elektronické voľby nebudú zadarmo. Pozrieme sa, či by sa elektronické voľby podľa modelu popísaného v časti 5 dali technicky uskutočniť a koľko by to stálo.

6.1 Náklady na realizáciu elektronických volieb

V tejto časti uvedieme horný odhad predpokladaných nákladov na realizáciu v časti 5 tejto práce navrhnutého modelu elektronických volieb na Slovensku. Náklady na informačnú kampaň, reklamnú kampaň a vzdelávaciu kampaň, ktoré budú nepochybne pred realizáciou elektronických volieb nevyhnutné, ako aj na celospoločenský dialóg o potrebne nasadenia elektronických volieb a posúdenie bezpečnostných a technických parametrov odbornou verejnosťou, sa nám, žiaľ, vyčísliť nepodarilo; uvádzame preto iba rozpis nákladov na riešenie technické a organizačné.

6.1.1 Náklady na technické riešenie

Pre odhad nákladov na technické riešenie vykonajme nasledujúce predpoklady:

1. Počet požiadaviek na Online volebné servery (horný odhad, označme σ): pri 3 miliónoch voličov, ktorí by hlasovali iba počas posledných 3 hodín priebehu elektronických volieb, pričom každý volič sa rozhodne odovzdať hlas desaťkrát;

$$\sigma = \frac{3 \cdot 10^6 \cdot 10req}{10800s} \leq 2800\frac{req}{s}$$

Kde *req* predstavuje počet požiadaviek. Ide o počet požiadaviek, ktorý nevyžaduje (v prípade, že na systém nie je podniknutý cielený útok) žiadne mimoriadne opatrenia či požiadavky na hardvér

Prejdime však k samotným predpokladaným zhora odhadnutým nákladom. Vo výpočtoch neuvádzame konkrétne modely hardvéru, uvádzame však orientačné ceny, ktoré by mali byť relevantné i v prípade neskoršej realizácie systému:

6.1.1.1 Hardvér

- Online volebné servery, ktorých budeme využívať 5 až 16:

$$16 \cdot 2000EUR = 32000EUR$$

- Offline servery pre realizáciu OSSH, OUH a ďalšie účely; malo by ísť o servery s vyššou výpočtovou silou, ktorých bude v systéme použitých spolu menej ako 8:

$$8 \cdot 5000EUR = 40000EUR$$

- Online servery pre stiahnutie volebnej aplikácie, ktorých počet zhora odhadujeme na 5:

$$5 \cdot 2000EUR = 10000EUR$$

- Load balancer, náklady na ktorý zhora odhadujeme na

$$100000EUR$$

- Dodatočné náklady na fyzické (optické) médiá, zálohovacie pásky a ďalšie vedľajšie náklady odhadujeme na menej ako

$$5000\frac{EUR}{\text{voľby}}$$

6.1.1.2 Softvér

Z hľadiska softvérového zabezpečenia systému elektronických volieb predpokladáme nasledovné finančné nároky:

- Serverové operačné systémy, ktorých budeme využívať menej ako 50:

$$50 \cdot 200EUR = 10000EUR$$

- Vývoj a nasadenie aplikácií pre elektronické voľby, ktoré podľa odhadu[1] je možné realizovať za náklady nižšie ako

$$30000 EUR$$

6.1.2 Organizačné riadenie

Konkrétnym organizačným opatreniam a politikám sa venujeme najmä v častiach 7.1 a 7.2. V tejto časti uvedieme približné náklady, ktoré očakávame pri ich realizácii.

6.1.3 Náklady

Ďalšie náklady, predovšetkým na organizačné, netechnické opatrenia a zabezpečenie služieb, odhadujeme nasledovne:

- Zabezpečenie DNS serverov a pripojení od rôznych poskytovateľov pripojenia do siete Internet odhadujeme na menej ako

$$1000 \frac{EUR}{\text{voľby}}$$

- Uskladnenie zariadení[2] odhadujeme na najviac:

$$365 \text{ dní } \cdot 24 \text{ hodín } \cdot 30 EUR \leq 270000 \frac{EUR}{\text{rok}}$$

  Ide o sumu pomerne vysokú (pri tomto odhade porovnateľnú s kúpou nového hardvéru), avšak odhad je robený pre veľmi okrajový prípad, kde by nebolo možné využiť žiadnu existujúcu infraštruktúru, priestory ani zamestnancov.

- Správcovia serverov a infraštruktúry, na ktorých náklady zhora odhadujeme pri trvaní volieb menej ako 14 dní na:

$$10000 EUR + 14 \text{ dní } \cdot 24 \text{ hodín } \cdot 100 EUR \leq 45000 \frac{EUR}{\text{voľby}}$$

6.1.4 Sumarizácia nákladov

Na základe uvedených predpokladov a výpočtov možno súdiť, že náklady na realizáciu elektronických volieb tak, ako sú navrhované v tejto práci, by pravdepodobne v uvažovaných oblastiach nemali[3] presiahnuť nasledovné odhady:

[1] vykonaného prieskumom u dodávateľov softvérových riešení

[2] na základe predbežných konzultácii je pravdepodobné, že by servery na účely organizácie volieb bolo možné zapožičať; v prípade zapožičania serverov je tento náklad irelevantný

[3] po započítaní medziročnej inflácie

Tabuľka 6.1: Sumarizácia nákladov na elektronické voľby

Jednorázové náklady	250000EUR	Jednorázové náklady predstavujú jeden cyklus životnosti použitého hardvéru; v závislosti od zvoleného hardvéru a cyklu jeho obnovovania možno predpokladať životnosť 2-7 rokov, následne bude potrebné nákup (alebo údržbu) vykonať znova
Ročné prevádzkové náklady	270000EUR	
Náklady na jedny voľby	50000EUR	

Kapitola 7

Posúdenie podľa technických štandardov

V tejto kapitole uvedieme posúdenie najmä organizačných a technických parametrov ako navrhnutého protokolu, tak i elektronických volieb ako takých, podľa zvolených technických a organizačných štandardov. Okrem technických parametrov budeme klásť dôraz na aspekt organizačný, a to najmä preventívne opatrenia a odporúčania pre prípadnú realizáciu elektronických volieb v prostredí Slovenska.

V tejto chvíli považujeme za potrebné uviesť, že prípadné reálne nasadenie elektronických volieb na Slovensku by malo byť konfrontované i s výsledkami a zisteniami pilotného projektu kolegu Bc. Filipa Vojtka [8].

7.1 Posúdenie podľa noriem radu ISO 9000

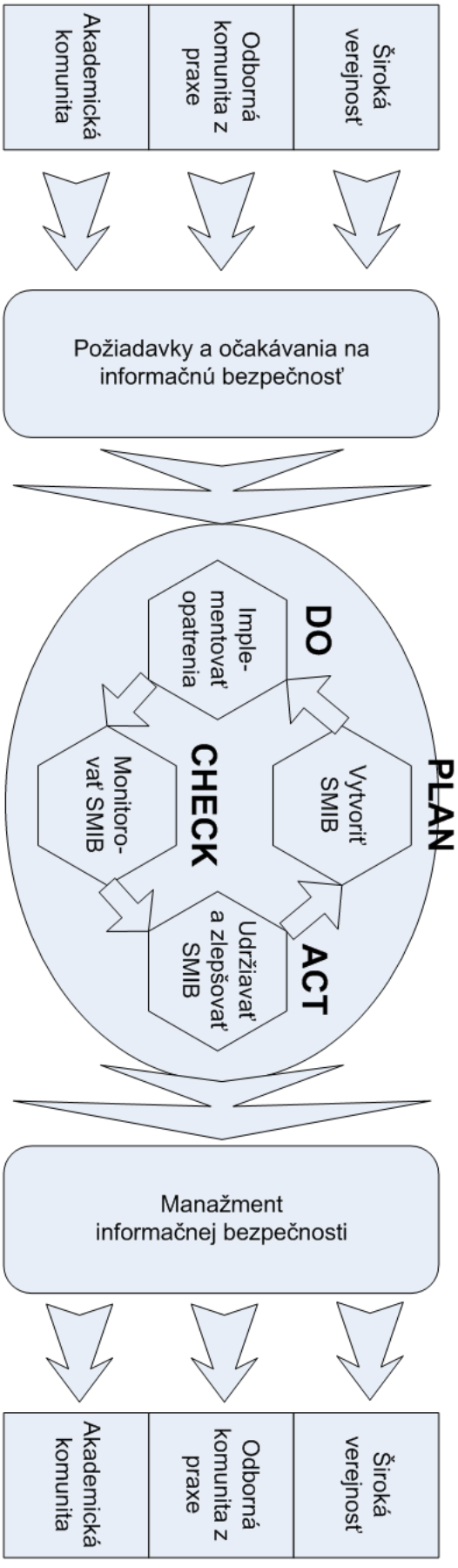
Normy radu ISO 9000 poskytujú široko rozšírený a akceptovaný prístup k riadeniu kvality[1]. Norma ISO 9001 [15] si kladie za cieľ zabezpečiť preukazovanie kvality produktu, ako aj zvyšovať spokojnosť zákazníkov. Keďže popisujeme riadenie kvality navrhovaného, nie existujúceho produktu, bude posúdenie prezentované vo forme odporúčaní a návrhov. Pred samotnými opatreniami pripomíname dôležitosť PDCA[2] cyklu pre manažment ako kvality, tak i informatickej bezpečnosti, ktorý sa týka ľubovoľného projektu nie len z oblasti IT. PDCA cyklus upravený pre konkrétne podmienky realizácie návrhu protokolu uvedeného v 5 uvádzame na obrázku 7.1. Cyklus znázorňuje nielen proces prípravy elektronických volieb na Slovensku ako systému, ale najmä nutnosť jeho stálej, cyklickej aktualizácie (zväčša vo

[1] preklad z anglického "quality management"

[2] Plan-Do-Check-Act cyklus; plánovanie-realizácia-kontrola-zlepšovanie; navrhnutý W. E. Demingom

forme auditov a nápravných resp. zlepšujúcich opatrení) a potrebu priamej spätnej väzby pre zainteresované skupiny, ktorými sú v tomto prípade najmä voliči a potenciálni voliči (široká verejnosť) a odborná komunita, či už zo sveta komerčného alebo akademického.

Systém moderného manažérstva kvality stavia najmä na procesnom prístupe ako k vývoju, tak i k uplatňovaniu a zlepšovaniu systému manažmentu kvality s cieľom zvýšiť spokojnosť zákazníka plnením jeho požiadaviek. V prípade elektronických volieb je zákazníkom volič; ide teda najmä o naplnenie požiadaviek, ktoré sme zosumarizovali v časti 3.3. Výstupom prípadnej certifikácie podľa normy ISO 9001 je preukázanie schopnosti trvalo poskytovať produkt, ktorý spĺňa príslušné predpisy a požiadavky zákazníka, ako aj neustále zlepšovať spokojnosť zákazníka efektívnou aplikáciou systému procesov, ale tiež neustále zlepšovanie a súlad výstupov s požiadavkami na systém kladenými.



Obr. 7.1: PDCA cyklus

Riadenie záznamov a dokumentácie

Ako sme naznačili už v návrhu systému v časti 5, produkovanie kvalitných a štandardných záznamov a dokumentácie je nevyhnutné z dôvodu zvýšenia transparentnosti a zabezpečenia auditovateľnosti systému elektronických volieb. Je preto potrebné najmä vytvoriť šablóny dokumentov používaných v priebehu od prípravy až po ukončenie volieb, ich pravidelnú aktualizáciu, inventarizáciu, riadenie[3] ale najmä vzdelávanie pracovníkov pracujúcich s dokumentmi nie len o technike ich používania, ale aj o dôvodoch ich dôležitosti a aplikáciach. Záznamy, ak to neodporuje ich stupňu utajenia, by mali byť dostupné v elektronickej verzii širokej verejnosti a originály archivované v príslušných archívoch.

Určenie zodpovednosti

Reflektujúc nie len časť 5 dokumentu [15] Zodpovednosť managementu, ale najmä časť 5.5 Zodpovednosť, právomoc a komunikácia, rozdelenie zodpovednosti na všetkých úrovniach riadenia je nevyhnutné pre:

- Plynulý beh systému s jasne určenými právomocami, povinnosťami a zodpovednosťou
- Jasné určenie osôb potrebných pre jednotlivé fázy elektronických volieb a zabezpečenie nahraditeľnosti zamestnancov
- Priamočiare vyvodenie zodpovednosti v prípade zlyhania

Manažment by mal navyše zaistiť dostupnosť všetkých potrebných zdrojov (či ľudských, materiálnych, finančných alebo iných), predkladanie príslušných správ o stave systému a podporovanie povedomia ostatných zamestnancov o závažnosti a dôležitosti vykonávaných činností.

Audity a preskúmania

V časti 5.6 norma [15] určuje manažmentu povinnosť v pravidelných intervaloch preskúmať systém manažérstva kvality zavedený v organizácii. Nad rámec preskúmania výsledkov auditov a spätnej väzby manažmentom sa pri elektronických voľbách ukazuje ako potrebné a žiadúce i preskúmanie odbornými komunitami (akademickými, komerčnými) a treťostrannými nezávislými organizáciami. Cieľom takéhoto preskúmania je zvýšiť mieru dôvery voličov v systém a jeho bezpečnosť, a to najmä zabezpečením transparentného preskúmania problémov a otázok, ale aj zvyčajného behu systému.

[3] pod riadením myslíme najmä kontrolu verzie a stavu dokumentu, ako aj riadených výtlačkov

Zdroje

Systém elektronických volieb navrhnutý v časti 5 pozostáva z kryptografických primitív, ktoré je potrebné zabezpečiť a naplniť v plnej miere. V opačnom prípade nie je garantované naplnenie bezpečnostných a iných požiadaviek. Je preto nevyhnutné, aby manažment a príslušné orgány zabezpečili potrebné zdroje, ako aj náhradné diely a príslušnú odbornú ľudskú silu na ich správu. Dôležitá je najmä stránka odbornosti; správcovia serverov totiž musia vedieť správne reagovať na vzniknuté situácie (preto je potrebné aj dôkladné vypracovanie pracovných postupov). Na bezpečnostné incidenty, ktoré môžu počas prevádzky vzniknúť, by mal reagovať školený personál, napríklad vo forme slovenskej vetvy CSIRT[4]; príslušným organizáciám je však potrebné (okrem zmluvných vzťahov) zabezpečiť aj potrebné množstvo kvalifikovaného personálu.

Návrh a vývoj

Pridŕžajúc sa časti 7.3 Návrh a vývoj normy [15], pri vývoji systému elektronických volieb je potrebné určiť:

- etapy návrhu a vývoja
- preskúmanie, overovanie a validáciu vhodnú pre príslušné fázy návrhu a vývoja a
- stanoviť rozdelenie zodpovednosti a právomocí

Vstupy pre návrh a vývoj pochádzajú ako z tejto práce, tak z pilotného projektu [8], ale aj z diskusie vedenej najmä s odbornou a akademickou verejnosťou.

Nákup a zabezpečenie zdrojov

Pri nákupe a zabezpečovaní zdrojov je potrebné klásť dôraz najmä na posúdenie a výber navrhovaných komponentov po stránke odbornej, a to ako stránke parametrov, tak i kvality, s prihliadnutím na možnosti ďalšej údržby.

Meranie, analýza, zlepšovanie a opravy

Podľa časti 8 Meranie, analýza a zlepšovanie normy [15] je potrebné vykonávať úkony smerujúce k preukázanie zhody produktu s navrhnutým systémom, zaistenie zhody systému manažérstva kvality, ako aj neustále zlepšovanie systému. Pre monitorovanie je možné

[4]Jednotka pre riešenie počítačových incidentov CSIRT SK; dostupné na sieti Internet k 6.4.2012: `http://www.csirt.gov.sk`

zvoliť viaceré metriky; konkrétne, možno merať cenu, rýchlosť a dostupnosť systému. Pokročilými metódami možno merať i jednoduchosť používania systému (napr. pomocou prieskumov). Nevyhnutnou súčasťou analýzy je i interný audit[5]. Zistené nedostatky je potrebné procesne ihneď riešiť a na základe určenia zodpovednosti za danú časť systému iniciovať ich opravu či zmenu.

7.2 Posúdenie podľa noriem radu ISO 27000 a normy ISO 15408

Normy ISO radu 27000 sa zaoberajú manažmentom informačnej bezpečnosti, a budú preto pre nás užitočným návodom pri posudzovaní bezpečnostného hľadiska najmä organizačných a technických parametrov navrhnutého systému elektronických volieb. Tento medzinárodný štandard je určený pre všetky typy spoločností[6], a teda aj pre veľké projekty ako je realizácia elektronických volieb. Naším cieľom nebude zaoberať sa certifikáciou podľa ISO 27001. Uvedieme pojednanie o prílohe A normy ISO 27001 [13] a príslušných odporúčaných opatrení z normy ISO 27002 [14], a to v kombinácii s označeniami a prostriedkami normy Common Criteria [10], [11] a [12] a existujúceho ochranného profilu [4].

7.2.1 Ciele posudzovania (TOE)[7]

Vzhľadom na heterogenitu prostredia pre nasadenie elektronických volieb je potrebné (v súlade s časťou 1.2 ochranného profilu [4]) rozdeliť ciele posudzovania na 2 (dve) časti, a to:

1. Klientská časť cieľov posudzovania, do ktorej patrí Volebná aplikácia a priestor počítača používaného voličom na odovzdanie hlasu

2. Serverová časť cieľov posudzovania, do ktorej patria všetky ostatné komponenty systému

Uvedené rozdelenie je nutné z dôvodu nemožnosti priameho ovplyvnenia zabezpečenia klientskej časti cieľov; je preto potrebné uvažovať s vyššou pravdepodobnosťou napadnutia

[5] a to nie len interný audit podľa ISO 9001 a ISO 27001, ale i audit bezpečnostný a audit v týchto normách neuvažovaných komponentov a vlastností systému; procesné úkony pre interný audit vychádzajú z časti 8.2.2 normy [15], ako aj z ďalších smerníc ISO určených pre vykonávanie auditu

[6] podľa [13], časť 1.2, str. 1

[7] Target of Evaluation; preklad z angličtiny

klientskej časti cieľov (osobných počítačov či volebnej aplikácie) rôznymi druhmi malware, ako aj s nekvalifikovanou obsluhou týchto staníc.

Bezpečnostným okolím systému sú systémy, ktoré s prostredím elektronických volieb interagujú (využívajú ho alebo sú ním využívané). Ide najmä o systém registra oprávnených voličov, ktorý je v elektronických voľbách využívaný na autorizovanie voliča. Ďalej spomeňme infraštruktúru verejných kľúčov PKI, ktorá umožňuje overovanie vydaných certifikátov. Je dôležité zabezpečiť, aby i systémy z bezpečnostného okolia dodržiavali bezpečnostné štandardy zavedené v systéme elektronických volieb; inak by ich bolo možné zneužiť na ohrozenie navrhovaného systému (napríklad kompromitácia systému pre autorizáciu voličov by ohrozila dodržanie požiadavky oprávnenosti k voľbe).

7.2.2 Aktíva

Komplexná analýza rizík je nad rámec tejto práce; zoznam aktív preto uvádzame na vysokej úrovni, nie detailne. Na základe usmernení časti 4.2.1 normy [13], ako aj návrhu aktív v časti 3 ochranného profilu [4], za hlavné aktíva navrhnutého systému elektronických volieb považujeme nasledovné:

- Správa s autentifikačnými údajmi voliča
- Autentifikačné údaje voliča
- Identifikačné dáta (voliča aj volebných serverov)
- Dáta v odovzdávanom hlase
- Hlas
- Uložená kópia hlasu
- Odpovede volebných serverov
- Ďalšie dáta volebných serverov (časové pečiatky, slepé podpisy)
- Dáta o voľbách (dátum a čas konania, kandidátne listiny, identifikačný kód volieb)
- Dáta spracovávané pri manipulácii s hlasmi a ich spočítavaní
- Dáta pre audit a logy
- Výsledky volieb

7.2.3 Potenciálni útočníci

Aktíva sú vystavené najmä nasledovným útočníkom:

- Sieťový útočník, profesionál, ktorý ale nedisponuje špeciálnymi prostriedkami. Je obmedzený na sieťové útoky (nemá priamy prístup k serverom). Môže mazať, modifikovať, generovať a čítať dáta počas ich prenosu, nemá však priamy prístup ani k PC voliča
- Oprávnený volič, ktorý nie je profesionálom a má prístup k volebnej aplikácii a korektným autentifikačným dátam (svojim)
- Neoprávnený volič, ktorý nie je profesionálom, má prístup k volebnej aplikácii ale nedisponuje korektnými autentifikačnými dátami
- Osoba s prístupom k volebným serverom, profesionál, ktorý nedisponuje dodatočnými dátami a možnosťami (pre fyzické obmedzenia prístupu)

Norma ISO 27001 do značnej miery rozvíja a podporuje myšlienky a požiadavky kladené normou ISO 9001; aj preto odporučíme čitateľa na časť 7.1. Nebudeme uvádzať podrobnú analýzu rizík, pretože nie sú známe detailné informácie o prostredí a ich výpočet je podmienený detailnou realizáciou projektu. Prejdime teraz prílohou A normy [13] a uveďme odporúčania a podrobnejšie informácie k jej vybraným častiam.

7.2.4 Príloha A normy ISO 27001

K časti 6 prílohy A normy [13] uveďme len toľko, že pre naplnenie bezpečnostných parametrov systému je nevyhnutný záujem manažmentu na dosiahnutí týchto parametrov; je preto potrebné korektne a úplne rozdeliť právomoci pre jednotlivé komponenty systému, určiť (i v písomnej a záväznej podobe) potrebné procedúry a dbať na ich dodržiavanie. Vlastníctvo a zodpovednosť za jednotlivé aktíva vyžadované v časti 7.1 prílohy A normy [13], a to i v ďaleko detailnejšej enumerácii ako uvádzame v časti 7.2.2, je nevyhnutné nielen pre korektné vyvodenie zodpovednosti v prípade incidentu, ale i pre štandardné fungovanie systému.

Komunikácia s tretími stranami sa, okrem profesijných organizácii ako CSIRT, obmedzuje na kontakt s príslušnými orgánmi štátnej správy a nezávislými organizáciami; pre potreby informačnej bezpečnosti je preto potrebné dbať najmä na korektné nastavenie výstupov, ktoré sú s uvedenými partnermi komunikované.

Klasifikácia informácii a ich riadenie podľa časti 7.2 prílohy A normy [13] je v prípade navrhnutého modelu relatívne priamočiara; protokol ako taký a jeho implementácia by totiž mali byť sprístupnené na posúdenie a pripomienkovanie širokej verejnosti bez obmedzení. Za klasifikované možno považovať najmä súkromné kľúče a prípadné čiastkové výsledky, ktorých nezverejnenie je nevyhnutné pre zachovanie kritéria férovosti elektronických volieb.

Časť 8 prílohy A pojednáva o ľudských zdrojoch. Zamestnanci priamo prítomní v objektoch so servermi by mali byť dôkladne preverení nielen po stránke odbornej, ale i etickej a morálnej. Možno tak predísť potenciálnym incidentom a ohrozeniam. Tiež je potrebné nastaviť prípadné disciplinárne postihy pre prípad zanedbania zo strany zamestnanca alebo zneužitia jeho právomoci. Ďalej, keďže nemožno predpokladať, že by boli všetci zamestnanci prítomní v chránených priestoroch odborníkmi na informatiku či informačnú bezpečnosť, je potrebné zabezpečiť kvalitné a pravidelné školenia pre zvyšovanie ich povedomia o práci ktorú vykonávajú, informačnej bezpečnosti a o systéme ako celku, a to v miere vyplývajúcej z ich úloh v systéme. Okamžité odobratie prístupových práv a všetkých zverených aktív v prípade ukončenia pracovného pomeru v súlade s časťou 8.3 prílohy A normy [13] je samozrejmosťou.

Riadenie fyzickej bezpečnosti serverovej časti TOE podľa časti 9 prílohy A si kladie za cieľ najmä predchádzať prístupu neautorizovaných osôb k systému, a z toho vyplývajúcemu prípadnému poškodeniu či vplyvu na zariadenia. Priestor by mal byť ohraničený vstupnými bodmi, kde vstupujúci preukážu oprávnenosť k vstupu do priestorov serverovej časti TOE. V týchto bodoch by mali byť kontrolované i pracovníkmi vnášané a vynášané predmety. Tiež je potrebné zabezpečiť fyzickú bezpečnosť objektov napríklad zamedzením vstupu cez okná alebo šachty. Žiadne komponenty systému, najmä sieťové komponenty, by nemali byť fyzicky prístupné mimo chránenej zóny a mali by byť chránené v súlade s časťou 9.2 prílohy A normy [13]. Priestory by mali byť navrhnuté alebo zvolené tak, aby ich priamo neohrozovali prírodné živly ako povodeň či zemetrasenie.

Časť 10.4 prílohy A a príslušná časť normy [14] pojednávajú o ochrane pred škodlivým a mobilným kódom. Ochrana by mala byť zabezpečená najmä preventívne monitorovaním prítomného softvéru odborným tímom zamestnancov (a to najmä pred jeho inštaláciou na zariadenia), a to i po stránke organizačnej zamedzením možnosti vloženia cudzieho kódu do počítačov. Všetky používané fyzické médiá by mali byť riadne označené a v prípade ich nepotrebnosti zneškodnené.

Logy sú v systéme uchovávané predovšetkým pre potreby ďalšieho auditovania pre-

behnutých volieb alebo riešenia vzniknutých problémov. Logy je potrebné (v závislosti na ich obsahu) primerane chrániť a zálohovať; správy o chybách ihneď doručiť zodpovedným osobám pre urýchlenie vyvodenia dôsledkov a nápravných opatrení. Najmä z dôvodu manipulácie s časovými pečiatkami je tiež potrebné zabezpečiť synchronizáciu času na prítomných zariadeniach.

Vzhľadom na citlivosť a dôležitosť údajov prítomných v systéme časti 11.2 a 11.3 prílohy A normy [13] zdôrazňujú nasadenie prísnej politiky pre vytváranie a správu hesiel používaných v systéme; prípadne je žiadúce použiť silnejšie kryptografické prvky, ako napríklad vhodne zvolené čipové karty alebo tokeny, ak je to možné. Politika čistého stolu tiež znižuje riziko možnosti úniku údajov zo systému. Dôležité je spomenúť i vzdialené prístupy do systému, ktorých prezencia by mala byť z dôvodu zvýšenia bezpečnostného štandardu minimalizovaná alebo úplne zakázaná.

Ošetrovanie vstupov a výstupov jednotlivých komponentov systému rieši najmä pilotný projekt elektronických volieb [8] kolegu Filipa Vojtka. Uveďme však, že overovanie vstupov, a to nie len po syntaktickej, ale aj sémantickej stránke, môže voličovi používajúcemu Volebnú aplikáciu výrazne zvýšiť komfort používania systému. Ďalej, vstupy do systému je potrebné validovať oproti príslušným XML schémam a kontrolovať i ďalšie na ne prípadne kladené parametre, a to ako z dôvodov korektnosti (napr. najviac štyri preferenčné hlasy pre kandidátov vo voľbách do NrSr), ale i z bezpečnostných dôvodov (ochrana pred útokmi typu SQL Injectioning a pod.). Časť 12.2 prílohy A normy [13] sa zaoberá tiež integritou správ a výstupmi ako aplikácie, tak i jej jednotlivých častí (modulov); kontrola na všetkých úrovniach systému (na úrovni modulov) umožňuje ľahšie nájsť prípadnú chybu v systéme, ako i určiť pracovníkov zodpovedných za jej odstránenie.

Riadenie kryptografických primitív by malo prebiehať ako na úrovni plošnej, celonárodnej, keďže každý volič podľa predpokladov bude disponovať čipovou kartou s príslušnými súkromnými kľúčmi, ako i v serverovej časti TOE, kde je ochrana najmä súkromného kľúča vnútornej šifrovacej obálky hlasu nevyhnutná pre vynútenie bezpečnostných vlastností navrhnutého protokolu.

Kontrola systému a hlásenie prípadných problémov podľa častí 12.6 a 13 prílohy A normy [13] by mali byť umožnené čo najširšej časti verejnosti, najmä odborníkom a akademikom, z dôvodu čo najvčasnejšieho zistenia a nahlásenia prípadných chýb a zraniteľností systému. Pre nahlásenie chýb by mala existovať komplexná ale jednoduchá procedúra, ktorá by umožnila priamočiare a promptné posúdenie nahlásenej informácie a jej riešenie.

7.2.5 Vybrané hrozby

Okrem uvedenia odporúčaní v časti 7.2.4 uvedieme i prehľad vybraných hrozieb podľa [4]. Pri hrozbách uvedieme príslušného útočníka, zasiahnuté aktíva, ako i hodnotenie dopadu hrozby na stupnici veľmi závažná - stredne závažná - málo závažná a hodnotenie pravdepodobnosti výskytu ako vysoká - stredná - nízka.

- **Odovzdanie hlasu neautorizovaným voličom** za cieľom manipulácie výsledkov volieb. Neautorizovaný volič sa môže pokúsiť zneužiť volebné právo iného, oprávneného voliča, alebo hlasovať pomocou jemu zverených prostriedkov, ktoré ho k voľbe neautorizujú. Ide o kompromitovanie aktív autentifikačných údajov voliča, správy s týmito údajmi, ako i autentifikačného tokenu. Ochrana pred týmto typom útokov je najmä prevencia zvyšovaním povedomia voličov o ochrane im zverených kryptografických prostriedkov. Systém ďalej neumožní hlasovať nikomu, kto nie je k voľbe autorizovaný[8]. Závažnosť takejto hrozby je vysoká; pravdepodobnosť jej výskytu však možno považovať za nízku.

- **Preukázanie hlasovania a donútenie k voľbe**, teda schopnosť voliča dokázať ľubovoľnej tretej strane či a ako vo voľbách hlasoval. Motiváciou tretej strany je vydieranie voliča, prípadne môže ísť o predaj resp. kúpu hlasu treťou stranou od voliča. Vzhľadom na použitú schému, ktorá voličovi neposkytuje žiaden dôkaz o spôsobe, akým vo voľbách hlasoval, je toto možné najmä hlasovaním za voliča (viď aj hrozbu odovzdanie hlasu neautorizovaným voličom vyššie), ale aj odovzdaním hlasu v prítomnosti tretej strany. Využívanou zraniteľnosťou sú najmä prípadné údaje, ktoré serverová časť TOE poskytne klientskej časti, Volebnej aplikácii. Keďže navrhnutý systém podporuje viacnásobné odovzdanie hlasu voličom, je motivácia útočníka značne znížená, pretože volič môže svoj hlas kedykoľvek (počas volieb) zmeniť. Závažnosť takejto hrozby je vysoká, keďže ide o ohrozenie ústavného práva voliča voliť; vzhľadom na navrhnuté technické riešenia však pravdepodobnosť jej výskytu považujeme za nízku.

- **Ohrozenie integrity správy** sieťovým útočníkom (profesionálom) s cieľom generovať, modifikovať, preposielať alebo mazať dáta počas ich prenosu. Ohrozenými aktívami sú teda všetky správy používané v systéme (autentifikačné dáta voliča a správa s hlasom); menej ohrozené sú dáta posielané vo vnútornej, uzavretej serve-

[8] v protokole zabezpečené autentifikáciou voliča pomocou registra oprávnených voličov

rovej časti TOE (ktoré nie sú určené Volebnej aplikácii). Motiváciou útočníka môže byť:

- Ovplyvnenie výsledku volieb modifikovaním správ obsahujúcich hlasy
- Vylúčenie niektorých voličov z hlasovania napadnutím autentifikačných a identifikačných dát
- Zmena hlasu odovzdaného voličom napadnutím kandidátnych listín
- Zavádzanie voliča o prijatí jeho hlasu modifikáciou správ potvrdzujúcich spracovanie hlasov

Uvedená hrozba je závažná; vďaka použitiu komunikácie zabezpečenej prostredníctvom SSL/TLS, zaručením autentickosti a integrity dát, ako aj ich súkromnosti silnými kryptografickými protokolmi, je však jej výskyt veľmi nepravdepodobný.

- **Ohrozenie súkromnosti hlasovania** útokom sieťového útočníka, ktorý zaútočí priamo na sieť za cieľom získania dát vo fáze spočítavania hlasov. Napadnutou zraniteľnosťou je komunikačný kanál; útočník dáta môže použiť na priradenie voličov k hlasom (narušenie súkromnosti hlasovania) alebo pre získanie čiastkových výsledkov volieb (narušenie férovosti volieb). Priamo ohrozené je najmä aktívum dáta spracovávané pri manipulácii s hlasmi a ich spočítavaní. Opäť, ohrozenie uvedených základných požiadaviek kladených na elektronické voľby je závažným ohrozením systému. Vzhľadom na odstránenie šifrovacej obálky z hlasu až po fyzickom prenesení dát na server, ktorý nie je žiadnym spôsobom pripojený do počítačovej siete, je však pravdepodobnosť výskytu hrozby nízka.

- **Ohrozenie autentifikácie serveru**, teda podvrhnutie falošného volebného serveru voličovi. Motiváciou sieťového útočníka sú možnosti uvedené pri hrozbách Ohrozenie integrity správy a Ohrozenie súkromnosti hlasovania. Ukazuje sa, že takáto hrozba je závažná a opatrenia pre minimalizáciu pravdepodobnosti jej výskytu sú pomerne náročné. Za efektívnu považujeme najmä autentifikáciu serveru pre stiahnutie volebnej aplikácie voči voličovi, kde si volič môže overiť i autentickosť stiahnutej Volebnej aplikácie[9]; následná komunikácia s Online volebnými servermi je zabezpečená pevným

[9]toto však vyžaduje výrazné zvyšovanie povedomia o informačnej bezpečnosti v spoločnosti a vytvorenie pomerne širokého spektra návodov na overenie, keďže konkrétne podmienky, v ktorých volič overenie vykonáva, môžu byť rôznorodé (rôzne operačné systémy, internetové prehliadače)

zadaním IP adries do Volebnej aplikácie. Pravdepodobnosť výskytu preto hodnotíme ako strednú.

- **Ohrozenie archívnych dát**. Osoby s prístupom k volebným serverom môžu modifikovať výsledky po ich vypočítaní. Ich motiváciou je zmena výsledkov volieb. Ohrozenými aktívami sú hlasy a výsledky volieb; dopad hrozby je veľký, pretože ide o priamu zmenu výsledkov, čím voľby stratia svoju hodnotu. Pravdepodobnosť je však veľmi nízka vďaka aplikovaniu organizačných opatrení a viacnásobnej kontroly; navyše, takúto modifikáciu by bolo možné zistiť pomocou logov.

- **Ohrozenie súkromnosti hlasovania pomocou archívnych dát**, ktoré by osoba s prístupom k volebným serverom mohla použiť pre prepojenie odovzdaného hlasu a voliča. Došlo by tak k narušeniu súkromnosti volieb, preto je dopad hrozby vysoký; pravdepodobnosť je však opäť nízka; dáta sú pred dešifrovaním anonymizované a prepojenie nie je možné priamočiaro vytvoriť.

Posúdenie uvedené v kapitole 7 je súhrnom základných praktík a usmernení potrebných nie len pre budúcu certifikáciu podľa daných noriem, ale i zabezpečenie kvality a bezpečnosti systému ako takého. V prípade implementácie danej schémy elektronických volieb je potrebné vykonať komplexnú analýzu rizík vytvoreného systému podľa série noriem ISO 27000 [13] a normy Common Criteria [10], [11] a [12], čo je nad rámec tejto práce.

Bezpečnostnú analýzu protokolu navrhnutého v kapitole 5 možno nájsť v diplomovej práci Bc. Filipa Vojtka [8], kapitola 4.6. Na základe tejto analýzy a popisu hrozieb a ich dopadov v časti 7.2.5 možno vyvodiť závery o naplnení bezpečnostných požiadaviek, ktoré sme na protokol kládli v časti 3.3, resp. v časti 5.1. Uvádzame preto tabuľku 7.1, kde sú závery zosumarizované.

Ďalšou vlastnosťou, ktorá protokol navrhnutý v časti 5 odlišuje od estónskeho protokolu popísaného v časti 4.1, či od elektronických volieb navrhnutých v Nórsku v práci [8], je zamedzenie útočníkovi vo vytvorení zoznamu oprávnených voličov, ktorí sa volieb zúčastnili[10]. Takáto informácia by totiž mohla opäť viesť k prípadnému pokusu o manipuláciu volieb ovplyvňovaním oprávnených voličov.

[10] vďaka implementácii "tretej obálky"; nie je možné spojiť voliča so zašifrovaným hlasom v prvej obálke pri napadnutí online časti volebných serverov

Tabuľka 7.1: Prehľad naplnenia bezpečnostných požiadaviek

Požiadavka	**Naplnenie požiadavky**
Demokratickosť	áno
Férovosť	áno
Oprávnenosť k voľbe	áno
Overiteľnosť - individuálna	nie
Overiteľnosť - individuálna čiastočná	áno
Overiteľnosť - univerzálna	nie
Nemožnosť ovplyvnenia	áno, viacnásobným hlasovaním
Robustnosť	áno
Súkromnosť	áno

Záver

Elektronizácia volieb zaznamenáva v posledných rokoch najmä v Európe značný progres. Projekty elektronizácie v Estónsku, Nórsku, Švajčiarsku či ďalší prebiehajúci výskum v iných krajinách dokazujú realizovateľnosť volieb elektronickou cestou. O elektronických voľbách sa v poslednom čase začína uvažovať aj na Slovensku. Naším cieľom bolo ukázať, či a za akých podmienok by bolo možné elektronické voľby implementovať v podmienkach Slovenska. Po analýze východísk a počiatočných podmienok v kapitole 2, prehľade súčasného stavu problematiky v časti 4 a následnom návrhu riešenia v časti 5 sme v kapitole 7 uviedli i vyhodnotenie a analýzu výsledku.

Podarilo sa nám preniknúť do legislatívnych problémov a požiadaviek, analyzovať existujúce riešenia vyvinuté pre podmienky iných krajín či protokoly navrhnuté pre univerzálne použitie, ako aj zúžiť spektrum aplikovateľných technológii odmietnutím napríklad protokolov založených na homomorfnom šifrovaní (vzhľadom na sčítanie). Navrhli sme volebný model, ktorý napĺňa požiadavku zachovania súčasného stavu bezpečnosti volieb, a to bez prehnaných alebo nerealizovateľných predpokladov. Realizáciu protokolu a jeho implementáciu na úrovni pilotného projektu rozpracoval v diplomovej práci [8] Filip Vojtko. My v práci uvádzame detailný technický návrh realizácie v reálnom nasadení, postavený na skúsenostiach s implementáciou iných veľkých komerčných informačných systémov na Slovensku. Okrem identifikácie požiadaviek, ktoré by mal model spĺňať a analýzy jeho vlastností sme sa pokúsili o jeho posúdenie podľa medzinárodných noriem; podarilo sa nám analyzovať základné aktíva, zraniteľnosti, hrozby a ich dopady na systém, ale nepodarilo sa nám pre systém postavený na našom modeli navrhnúť ochranný profil podľa ISO 15408. Zaoberali sme sa aj bezpečnosťou prevádzky volebného systému. Tu sme vychádzali z normy ISO 27001. Výber relevantných opatrení najmä z oblasti manažérstva informačnej bezpečnosti by mohol zjednodušiť prípravu systému pri jeho reálnom nasadzovaní. Business požiadavky kladené na systém, ktoré uvádzame v časti 3.1, sme nepriamo rozobrali v kapitole 7; zachovanie bezpečnosti sa naplniť podarilo, avšak zníženie ceny volieb z dlhodobého hľadiska, zvýšenie dostupnosti voličom a stupňa informatizácie spoločnosti záleží

od konkrétnej implementácie a nasadenia. Ich naplnenie preto bude možné analyzovať až následne.

Práca neobsahuje modely prípadných útokov na systém a návody na priamočiare riešenie prípadných incidentov, a to či už vo forme sieťových alebo iných útokov. V budúcnosti sa bude potrebné zamyslieť i nad škálovateľnosťou navrhnutého technického riešenia a spraviť analýzu jeho odolnosti voči preťaženiu či prípadným útokom. Tiež podrobnejší pohľad na sociologické a štatistické otázky rýchlosti prechodu voličov k hlasovaniu prostredníctvom siete Internet a súvisiace prepočty nákladov môžu ukázať ďalšie výzvy, s ktorými sa bude realizácia elektronických volieb na Slovensku musieť potýkať.

Problematika elektronických volieb je značne komplexná, ale i veľmi zaujímavá. Zahŕňa ako informatické, tak i kryptologické, legislatívne, spoločenské, psychologické, politické či politologické, organizačné, a samozrejme ekonomické otázky a aspekty, ktorých analýza a riešenie vyžaduje mnoho úsilia. V tejto práci sme sa pokúsili podať ucelený pohľad na problematiku zachytávajúc hlavné otázky a problémy, ktorých riešenia sú zhrnuté do navrhnutého modelu.

V prípade realizácie elektronických volieb na Slovensku bude potrebné riešiť mnoho problémov. Okrem technickej realizácie je totiž potrebné uskutočniť masívnu a odborne pripravenú informačno-vzdelávaciu kampaň pre obyvateľstvo, integrovať infraštruktúru elektronických identifikačných kariet s čipom a organizačne zabezpečiť celý priebeh volieb. Pre zabezpečenie plynulého prechodu na elektronické voľby bude potrebné zaviesť prechodné obdobie, kedy sa bude voliť elektronicky aj papierovo. Ak však tieto výzvy úspešne zvládneme a systém sa bude realizovať zodpovedne a kompetentne, voľby sa podstatne zjednodušia a na Slovensku bude možné využívať výhody demokracie vo vyššej miere.

Literatúra

[1] Alexander Kirshner: The International Status of the Right to Vote, Democracy Coalition Project, 17.12.2003, dostupné k 6.4.2012 na sieti Internet: `http://www.demcoalition.org/pdf/International_Status_of_the_Right_to_Vote.pdf`

[2] Alfred J. Menezes and Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography, CRC Press, 1997, dostupné k 6.4.2012 na sieti Internet: `http://www.cacr.math.uwaterloo.ca/hac/`

[3] Bc. Martin Jurčík: Using SELinux to Enforce Two-Dimensional Labelled Security Model with Partially Trusted Subjects, Diplomová práca, Univerzita Komenského v Bratislave, 2012

[4] Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products, BSI-CC-PP-0037, Version 1.0, 18.4.2008

[5] Dr. Rolf Haenni, Dr. Eric Dubuis, Dr. Ulrich Ultes-Nitsche: Research on E-Voting Technologie, Bern University of Applied Science, 2008

[6] Dr. Rolf Haenni, Reto Koenig, Dr. Stephan Fischli, Dr. Eric Dubui: TrustVote: A Proposal for a Hybrid E-Voting System, Bern University of Applied Science, 2009

[7] Filip Lebovič, Volebný systém pomerného zastúpenia (Diplomová práca), Univerzita Komenského v Bratislave, Právnická Fakulta, Katedra štátneho práva, 2005

[8] Filip Vojtko: Pilotný projekt elektronických volieb, Univerzita Komenského v Bratislave, 2012

[9] Hirt, Martin and Sako, Kazue: Efficient receipt-free voting based on homomorphic encryption, Proceedings of the 19th international conference on Theory and appli-

cation of cryptographic techniques, EUROCRYPT'00, Springer-Verlag, Bruges, Belgium, 2000, ISBN: 3-540-67517-5

[10] ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, verzia 3.1 rev. 3 Final, júl 2009, dostupné k 6.4.2012 na sieti Internet: `http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf`, CCMB-2009-07-001

[11] ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, verzia 3.1 rev. 3 Final, júl 2009, dostupné k 6.4.2012 na sieti Internet: `http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf`, CCMB-2009-07-001

[12] ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, verzia 3.1 rev. 3 Final, júl 2009, dostupné k 6.4.2012 na sieti Internet: `http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf`, CCMB-2009-07-001

[13] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements, 2005

[14] ISO/IEC 17799/27002:2005, Information technology - Security techniques - Code of practice for information security management, 2005

[15] ISO/IEC 9001:2008, Quality management systems - Requirements, 2008

[16] Jens Groth: Non-interactive Zero-Knowledge Arguments for Voting, 2005

[17] Johannes Böck: RSA-PSS - Provably secure RSA Signatures and their Implementation v1.0.1, Diplomová práca, Humboldt-Universität zu Berlin, 10.11.2011

[18] Juraj Danko: Elektronické voľby a ich vybrané parametre, FMFI UK Bratislava, 2011

[19] Kristian Gjosteen: Analysis of an internet voting protocol, Cryptology ePrint Archive, Report 2010/380, 2010

[20] Laure Fouard, Mathilde Duclos, Pascal Lafourcad: Survey on Electronic Voting Schemes, VERIMAG, 2 avenue de Vignate, 38610 Grières, France, 2010

[21] RNDr. Jaroslav Janáček, PhD.: General Purpose Operating System for Security Critical Applications, 2010

[22] Shahrokh Saeednia and Steve Kremer and Olivier Markowitch and Université Libre De Bruxelles: An Efficient Strong Designated Verifier Signature Scheme, Springer-Verlag, 2003

[23] Sven Heiberg, Internet Voting: the Estonian Experience, Cybernetica, 2010 Ltd. `www.cybernetica.eu`

[24] Tony Bourke: Server Load Balancing, O'Reilly & Associates, Inc., 101 Morris Street, Sebastopol, CA 95472, 2001

[25] Triinu Mägi: Practical Security Analysis of E-voting System, Tallinn University of Technology, 2007

[26] Vyhláška Národného bezpečnostného úradu 136/2009 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku, 26.3.2009

[27] Ústava Slovenskej republiky, 1.9.1992

[28] Zákon NrSr č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, 15.3.2002

[29] Zákon NrSr č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov, 20.4.2006

[30] Zákon č. NrSr č. 303/2001 Z.z. o voľbách do orgánov samosprávnych krajov a o doplnení Občianskeho súdneho poriadku, 4.7.2001

[31] Zákon NrSr č. 331/2003 Zb. o voľbách do Európskeho parlamentu, 10.7.2003

[32] Zákon NrSr č. 333/2003 Z.z. o voľbách do Národnej rady Slovenskej republiky, 13.5.2004

[33] Zákon NrSr č. 346/1990 Zb. o voľbách do orgánov samosprávy obcí, 28.8.1990

[34] Zákon NrSr č. 46/1999 Z.z. o spôsobe voľby prezidenta Slovenskej republiky, o ľudovom hlasovaní o jeho odvolaní a o doplnení niektorých ďalších zákonov, 18.3.1999

[35] Zákon NrSr č. 49/2012 Zb. ktorým sa mení a dopĺňa zákon č. 224/2006 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, 31.1.2012

[36] Zákon NrSr č. 564/1992 Zb. o spôsobe vykonania referenda, 19.11.1992

[37] Zuzana Rjašková: Electronic Voting Schemes, Diplomová práca, Fakulta Matematiky, Fyziky a Informatiky Univerzity Komenského v Bratislave, apríl 2002