České vysoké učení technické

Fakulta elektrotechnická

Analýza

Systém elekronických voleb

E-volby

3.10.2010 Tomáš Čerevka

Obsah

Vize

Informační systém E-volby uživatelům poskytne komplexní hlasovací systém, který elektronickou cestou řeší problém zdlouhavého počítání papírových volebních lístků. Bude sloužit jak pro lokální volby (sjezdy politických stran, volba zastupitelstva v družstvu, referenda v obcích, apod.), tak pro globální volby (volby do AS ČVUT, volby do poslanecké sněmovny).

Zákazníky tohoto systému jsou instituce, ve kterých probíhají různá hlasovaní či volby. Zadavatel voleb (pořadatel) v systému vytvoří volební formulář. Ten je poskytnut voličům, kteří po zabezpečeném přihlášení do systému hlasují (vyplní formulář a odešlou svůj hlas). Ukončení voleb provádí pořadatelé (volební komise). Systém sečte hlasy a výsledky voleb bude možno zobrazit na výstupním médiu (nejčastěji webová stránka).

Pro lokální volby poběží systém na jednom serveru, který nebude připojený k internetu a jediné zařízení, které s tímto serverem bude moci komunikovat bude hlasovací terminál. V těchto volbách budou jednotlivý voliči registrováni do systému na začátku sjezdu nebo jednání a buď dostanou své jedinečné ID nebo se naskenuje jejich otisk prstu a poté se k terminálu přihlásí buď svým ID nebo naskenováním otisku prstu. Na začátku sjezdu nebo jednání bude též stanovena komise, která bude tento systém v průběhu voleb řídit.

Pro globální volby budou jednotlivé moduly systému nasazeny na zvláštní servery kvůli bezpečnostním rizikům. Tento systém bude čerpat údaje o voličích z externího adresáře obyvatelstva, který bude spravován třetí stranou. Na začátku voleb je opět stanovena volební komise, která na celý průběh voleb dohlíží. Tato komise zakládá volební události, startuje proces kandidování a volení. Tyto procesy ukončuje a poté zveřejní výsledky voleb. Celý proces volení je založený na dnes již funkčním systému korespondenčního hlasování, kde občan, který chce volit musí nejdříve do první obálky zalepit svůj hlas a poté tuto obálku společně s čestným prohlášením, že takto hlasuje opravdu on, ji vloží do další obálky, kterou poté odešle na příslušný okrsek. Na okrsku komise rozlepí první obálku, přečte si čestné prohlášení a zjistí jestli tento volič může v těchto volbách hlasovat. Pokud ano, tak jeho hlas vhodí do urny. Podobně bude fungovat systém elektronického hlasování. Volič se přihlásí k validačnímu serveru a ten zjistí jestli tento volič může hlasovat ve volbách, pokud ano nabídne mu applet, ve kterém si uživatel vybere komu dá svůj hlas a odhlasuje. Applet tento hlas zašifruje veřejným klíčem voleb a validační server si ho uloží. Další proces, tedy sčítání hlasů probíhá take standartně. Na validačním serveru jsou uloženy zašifrované hlasy, které tento server neumí rozšifrovat. Tyto hlasy jsou tedy po skončení voleb odeslány na sčítací server, který už umí tyto hlasy rozšifrovat sečíst. Na konec volební komise zveřejní výsledky na webových stránkách.

Business analýza

Diagramy této analýzy jsou přiloženy v souboru [Bussiness process model.pdf] .

Projekt bude primárně zaměřen pro nasazení při volbách do akademického senátu ČVUT.

Business analýza je složena z několika business procesů, které na sebe logicky navazují.

Prvním je „zvolení komisařů“ a s tím související „založení nových voleb“, kde se tito zvolení komisaři stanou komisary pro tyto volby. Dále se v tomto procesu zvolí jestli tyto volby jsou lokální nebo globální. Pokud jsou volby lokální vybere se také příslušný certifikát, pomocí kterého se budou moci připojit jen některé zařízení.

Dalším procesem je „založení volební události“. Toto již provádí zvolení komisaři a tito komisaři v souladu s platným zákonem stanoví kolik procent musí dostat kandidát aby v této volební události byl zvolen, dále kolik procent voličů se musí k volbám dostavit, aby tyto volby byly platné, dále počet kandidátů, kteří mohou být zvolení a stát se tedy vítězi a počet náhradníků.

Na tento proces „založení volební události“ navazuje proces „nominování kandidátů“, ve kterém si každý kandidát vyplní svůj volební program a zapíše se jako kandidát v těchto volbách.

Následuje proces „volení“, kde jednotliví voliči jsou vyzváni k volení. Tito voliči,kteří jsou k volení v této volební události oprávnění se připojí k systému a zvolí jedno či více kandidátů.

Zároveň je ošetřeno, aby nemohl probíhat proces „nominování“ zároveň s procesem „volení“.

Po uplynutí doby stanovené zákonem jsou volby ukončeny a komise ukončí volební událost, systém sečte hlasy a komise zveřejní výsledky.

Přehled požadavků

Diagramy požadavků jsou vygenerovány v souboru [Requirements model.pdf] .

Funkční požadavky

- Uživatelé nominují kandidáty.
- Kandidáti jsou voleni.
- Výsledky jsou veřejné.
- Komisaři zakládají volby.
- Ukončení voleb musí učinit M z N komisařů.
- Komisaři potvrzují nominace kandidátů.
- Při opakovaném volení voliče platí jeho poslední hlas.
- Volič může být informován e-mailem.
- Volby jsou tajné vůči druhé osobě.

Nefunkční požadavky

- V lokálních volbách je možnost využít terminál.
- V lokálních volbách se volič přihlašuje jedinečným identifikátorem.
- V lokálních volbách je použit pouze jeden server.
- V globálních volbách voliči hlasují přes webový prohlížeč.

Případy užití a scénáře

Diagramy případů užití jsou vygenerovány v souboru [Use case model.pdf] .

V případech užití vystupují 4 aktoři : Administrátor, Uživatel a dále tři, kteří jsou speciálnímy připady Uživatele – Volič, Komisař a Kandidát.

Vytvoření nové komise

Aktér: Administrátor

1. Administrátor požádá o vytvoření volební komise
2. Systém zobrazí formulář pro založení volební komise
3. Administrátor vyplní formulář (zadá loginy komisařů)
4. Administrátor odešle formulář
5. Systém založí komisi a potvrdí úspěch

Post-condition : Volební komise je vytvořena

Vytvoření nových voleb

Aktér: Administrátor

Pre-kondition: Je vytvořena volební komise

1. Administrátor požádá systém o vytvoření voleb
2. Systém zobrazí formulář pro založení voleb
3. Administrátor vyplní formulář (název a typ voleb)
4. Administrátor odešle formulář (založí volby)
5. Systém provede validaci vyplněných udájů ve formuláři.
6. ALTERNATE Systém ohlásí chybu vyplnění formuláře. ZPET NA KROK 2
7. Systém založí volby a potvrdí úspěch

Post-condition: Volby jsou založeny

Vytvoření volební události

Aktér: Komisař

Pre-condition: Volby jsou založeny

1. Komisař požádá systém o založení volební události
2. Systém zobrazí formulář pro založení volební události

3. Komisař vyplní formulář (název události a popis události)
4. Komisař odešle formulář
5. Systém založí volební událost a potvrdí úspěch

Post-condition: Proces nominace kandidátu může být založen

Nominování

Aktér: Kandidát, Komisař

Pre-condition: Byla založena volební událost

1. Komisař požádá systém o ovládání volební události
2. Systém zobrazí ovládací prvky pro volební událost
3. Komisař klikne na start procesu nominování
4. Systém spustí proces nominování
5. Kandidát pošle systému kandidátní lístek
6. Systém zkontroluje kandidátní lístek
7. Systém vrátí informace o úspěchu

Volení

Aktér: Komisař, Volič

Pre-condition: Je vytvořena volební událost, na kterou je pozván uživatel

1. Komisař požádá systém o ovládání volební události
2. Systém zobrazí ovládací prvky pro volební událost
3. Komisař klikne na start procesu volení
4. Systém spustí proces nominování
5. Volič požádá systém o možnost volení
6. Systém nabídne voliči seznam volebních událostí, na které byl pozván
7. Volič vybere konkretní událost ze seznamu
8. Systém zobrazí formulář volebních události
9. Volič vyplní volební formulář
10. Volič odešle volební formulář
11. Systém provede validaci vyplněných údajů ve volebním formuláři.
12. ALTERNATE Systém ohlásí chybu vyplnění formuláře. ZPĚT NA KROK 8

13.Systém podepíše a zašifruje volební lístek a uloží si volební lístek

14.. Systém ohlásí uživateli přijetí lístku

Post-condition: Volební lístek je uložen

Ukončení volení

Aktér: Komisař

Pre-condition: Byla odstartováno volení

1. Komisař ukončí volební událost
2. Krok 1 a 2 dokud M z N komisařů neukončí volení ve volební události
3. Systém ukončí volení ve volební události a potvrdí úspěch

Post-condition: Volení ve volební události je ukončeno. Systém spočítá výsledky

Doménový model

Diagramy datového modelu jsou vygenerovány v souboru [Domain model.pdf] .

Pro účely aplikace elektronického volebního systému jsou ukládány do databáze následující objekty.

Volič je uložen v externím adresáři obyvatelstva a náš systém z této databáze potřebuje zjistit voličovo jméno a dále jeho login nebo jiný jedinečný atribut. Může to být například elektronický podpis. Z těchto jednotlivých osob, které jsou uloženy v externím adresáři se dále vybírají i komisaři. U komisaře si potřebuje elektronický volební systém uložit také jméno a nějaký jedinečný identifikátor.

Při vytvoření voleb se do databáze uloží objekt Volby, který obsahuje název voleb a typ voleb (lokální nebo globální). Dále jsou k tomuto objektu uloženy reference na komisaře, kteří byli pro tyto volby zvoleni.

Dále objekt Volby obsahuje další reference na jednotlivé volební události, které jsou konány pod záštitou těchto voleb. U objektů Volební události jsou v databázi uchovávány informace o začátku a konci procesu nominování a volení, dále jméno události, reference na voliče, kteří v těchto volbách mají právo volit. U objektu volební události jsou také uloženy reference na objekty kandidátů v těchto volbách. Kandidáti mají u sebe uloženy svůj volební program, jméno, případně fotografii a další informace.

Dalšími objekty, které se ukládají v databáze jsou Volební lístky. Tento lístek obsahuje kandidáty, které příslušný volič vybral a tento volební lístek je přiřazen k příslušné volební události.

Každá volební událost má volební výsledek, který v sobě nese informaci o vítězech voleb a náhradnících.

Vytyčení cílů

Odstranění chyb z předchozí verze projektu. Konkrétně se jedné o následující:

Závady obecného charakteru

1) Chybí implementace rozlišení rolí při přihlášení.

V kódu je náznak přípravy, ale není nijak použito. Prozatím je přihlašování napevno zabudováno do kódu a role je určena jménem.

2) Při přepínání rolí v záhlaví menu se řetězí adresa.

Opakovaným kliknutím na položku aktéra se řetězí adresa stránky.

3) Nefunkčnost přihlášení při změnách role.

Pokud zvolím určitou roli a před přihlášením ji změním, popř. se vrátím zpět k původní volbě, nelze se přihlásit i se správnými údaji. Pokud však zvolím v prohlížeči krok zpět, jsem přihlášen a mohu volit položky z menu.

4) Bylo by vhodné popsat logovací tabulku, neboť uživatel ztrácí přehled, p

od kterou rolí se vlastně loguje. Role jde vyčíst jen z adresy.

5) Absence chybových hlášek.

V podstatě žádné výjimky nejsou ošetřeny a končí errorem a pádem aplikace. Jedná se například o přepínání rolí po zalogování- voter nemá přístup k admin účtu apod.

6) Problematika bezpečnosti.

Podle současné koncepce je na jednom serveru ukládána dvojic jméno voliče-hlas. Tato varianta je velmi špatně zabezpečena, lepší by bylo např. použití hashe dvojice hesla uživatele a hlasu. Dále se nabízí otázka efektivnosti a účelnosti opakované volby. V případě jednorázového volení by se značně zjednodušilo schéma komunikace.

7) Chyba v názvu- Electronics vs Electronic

Závady sekce Voter

V dokumentaci je u nominování jako aktér popsán Kandidát. Role Kandidát však nikde v systému popsána není a jedná se zřejmě o roli Voter z čehož vyplývají nesrovnalosti ve stávající dokumentaci.

Kvůli nefunkčnosti dalších komponent se nám nepodařilo vůbec spustit vlastní volební applet a ověřit jeho funkčnost, ale domníváme se, že se vyskytne problém v případě vypsání dvou voleb. Volič bude registrován k oběma volbám, ale v appletu dle kódu není možnost výběru události.

Závady sekce Admin

Při vytváření voleb není nijak kontrolováno, zda admin vyplní typ voleb - local/internet. Volby lze vytvořit i bez typu. To způsobí další komplikace aplikaci, neboť řada tabulek má vypisovat typ voleb apod.

Administrátor nemá žádnou možnost vytvořené volby smazat nebo editovat. V případě zadání špatného typu nebo názvu by musel najit příslušnou tabulku a záznam odstranit „natvrdo“.

Nejzávažnější chybu však představuje absence možnosti přidat komisaře. Tato chyba ovlivňuje celý systém. Bez přidání komisařů nelze vytvořit volební komisi, nelze přidělit ani otevřít volby,nominovat kandidáty a tím pádem se regulérně nezobrazí ani applet volebního lístku.

Další zásadní nesrovnalostí je, že dle Use case modelu admin vytváří jen volební komisi, vytvoření voleb a volební události má pak na starosti komisař. Podle závěrečné zprávy a implementace však volby zakládá admin, což je naprosto nelogické.

Podle stávající implementace je postup následovný:

Admin vytvoří volby a přiřadí komisi, komise vytvoří volební událost(z dokumentace není jasné co se volební událostí vlastně myslí), komise otevře nominaci(domněnka, nešlo otestovat), komise přiřadí volbám voliče(domněnka, nešlo otestovat).

Přehlednější postup (částečně popsaný v dokumentaci a pravděpodobně zamýšlený tvůrci):

admin vytvoří komisi, komise vytvoří volby (create election) a tím se spustí nominace, komise vytvoří volební událost(election event),čímž přiřadí voliče a spustí hlasování.