

Elektronický hlasovací systém

Lukáš Richter



*** Nascanované zadání, strana 1 ***

*** Nascanované zadání, strana 2 ***

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne

.....

podpis studenta

ABSTRAKT

Cílem této práce je návrh a implementace funkční volební a hlasovací aplikace. Primárním využitím výsledné aplikace jsou volby do akademických senátů Univerzity Tomáše Bati ve Zlíně. Výsledný systém zaručuje anonymitu voličů a poskytuje jednoduchý způsob, jak maximálně zpřístupnit volby co nejvíce studentům.

Aplikace je postavena na PHP frameworku Nette. Návrh aplikace umožňuje její relativně snadné modifikace co do rozmístění mezi několik serverů i nezávislost na použitém systému řízení báze dat. Systém je zároveň možno doplnit o volitelné způsoby autentizace uživatelů.

Při návrhu bylo využito principu slepých digitálních podpisů a přímé komunikace klienta a serveru jako efektivního způsobu zajištění anonymity.

Klíčová slova: Elektronické volby, e-voting, RSA, slepé podepisování, PHP, Domain Driven Design, MVC, Nette, Bootstrap

ABSTRACT

The goal of this thesis is to design and implement functional electronic voting application. Primary use of the resulting application will be Academic Senate elections of Tomas Bata Univerzity in Zlin. The resulting system guarantees voter anonymity and offers a simple solution how to make voting available to as many students as possible.

Application is based on PHP framework Nette. The design of the application allows its relatively simple modification in regards of distribution among multiple servers and independence on used database management system. It is also possible to extend the system with different user authentication options.

Blind digital signatures and direct client-server communication as an effective means to assure anonymity were used to desing the application.

Keywords: Electronic voting system, e-voting, RSA, Bling Signature, PHP, Domain Driven Design, MVC, Nette, Bootstrap

Rád bych poděkoval doc. Ing. Martinu Syslovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

OBSAH

ÚVOD	8
I TEORETICKÁ ČÁST	9
1 ELEKTRONICKÉ VOLBY	10
1.1 POŽADAVKY NA ELEKTRONICKÝ VOLEBNÍ SYSTÉM	10
2 POŽADAVKY NA FUNKČNOST	12
2.1 OBECNÉ POŽADAVKY	12
2.2 SPECIFIKA PROVOZU NA UTB.....	12
2.3 NAVRHOVANÉ ŘEŠENÍ.....	12
2.4 RSA BLIND SIGNATURE	13
ZÁVĚR	14
SEZNAM POUŽITÉ LITERATURY	15
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	17
SEZNAM OBRÁZKŮ	18
SEZNAM TABULEK	19
SEZNAM PŘÍLOH	21

ÚVOD

V době rapidního rozvoje technologií, kdy se digitalizuje kde co a prakticky vše je na dosah ruky díky internetu a mobilním telefonům, se stále více aspektů života přesouvá na obrazovky v komfortu našich domovů. Týká se to například i vyřizování oficiálních záležitostí a komunikace se státní správou. Velkou výzvou je ovšem přenést jeden ze základních pilířů demokracie - volby - co nejbližší k voliči. Dostupnost voleb v internetovém prohlížeči nemusí být jen o komfortu, což dokládá aktuální pandemie Covid-19. V současné situaci by takovou možnost jistě uvítal ne jeden volič.

Cílem této práce je vytvořit funkční webovou aplikaci umožňující provozovat volby do akademických senátů Univerzity Tomáše Bati ve Zlíně, která bude uživatelsky přívětivá a zároveň bezpečná. V teoretické části budou prozkoumány obecné požadavky elektronických voleb, které by aplikace měla splňovat. Na základě stanovených požadavků a zvolené kryptografické metody zajišťující anonymitu voleb pak bude postupně navrhována aplikace.

Dále je představen architektonický vzor Model View Controller a framework Nette, se kterým mám praktické zkušenosti. Teoretickou část práce tvoří převážně abstraktní návrh aplikace, která byla od začátku tvořena s ohledem na jednoduchost budoucích úprav. Aplikace podobného typu by z pohledu zdrojového kódu a struktury měla být přehledná a její údržba a rozšiřování snadné. I z tohoto důvodu bylo při modelování i implementaci dbáno na co nejlepší dodržení zásad Domain Driven Designu.

V praktické části jsou detailněji popsány jednotlivé části aplikace a jejich funkce a vzájemné provázání. Nejpodstatnější a pravděpodobně i nejzajímavější částí je způsob zpracování a nakládání s hlasovacími lístky, kterému je věnován závěr práce.

Téma práce bylo navrženo vedoucím práce, jako možné řešení voleb na půdě UTB, jelikož vlastní aplikací nedisponuje. Vzhledem k osobním zkušenostem s programováním webových aplikací mě tato výzva zaujala především možností vytvořit aplikaci od návrhu až po její finální implementaci. Aplikace zároveň není pouze teoretickým příkladem, ale řešením reálného problému, který by mohl být uplatněn v praxi.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÉ VOLBY

Pod pojmem elektronických voleb jsou zmiňovány převážně dvě odlišná pojetí. Prvním je užití hlasovacích zařízení k uskutečnění volby přímo ve volební místnosti. Neslavně se tento způsob využíval v Nizozemí [1] a testoval v dalších zemích. U hlasovacích zařízení byla často objevena řada nedostatků a zranitelností a jejich zavedení provázely protesty a nedůvěra voličů v celý proces voleb [2]. I v případě, že jsou zařízení využita pouze částí elektorátu, jakékoli pochybnosti ovlivňují výsledky celku.

Druhým pojetím je tzv. *remote-voting*, neboli volba na dálku a představuje účast ve volbách prostřednictvím zařízení pro dálkovou komunikaci, např. přes internet. S tímto způsobem hlasování bývá spojena údajná výhoda ve vyšší volební účasti, různé studie voleb v Estonsku [3] nebo Švýcarsku [4] nicméně neukazují žádný nebo minimální nárůst účasti. Pro úzce zaměřené hlasování například na univerzitách tento vliv může být podstatně vyšší.

Návrh elektronického volebního schématu nebo protokolu a implementace takového systému je zjevně náročná a je již přes 40 let předmětem výzkumů. Výrazného rozšíření se systémy pro elektronické volby na státních úrovních nicméně nedočkaly a zůstávají na úrovni univerzit, případně lokálních voleb.

1.1 Požadavky na elektronický volební systém

Z mnoha dostupných zdrojů lze vyvodit závěr, že zatím není žádný univerzální protokol nebo standard pro elektronické volby. Existuje vícero protokolů různé komplexity s různými cíly. Je zřejmé, že protokol elektronických voleb na celostátní úrovni (parlamentní volby apod.) by měl klást podstatně striktnější nároky na takový systém v porovnání s hlasováním (semestrální dotazníky aj.) na akademické půdě. Chybějící univerzální protokol zároveň nedává jinou možnost než definovat vlastní požadavky pro každý systém zvlášť.

Existující systémy, návrhy i protokoly se, ať už více či méně, shodují v několika základních bodech, které by měl takový systém splňovat. Takto je definoval Schneier [5] v knize *Applied Cryptography*¹⁾:

1. Pouze oprávnění voliči mohou volit.
2. Nikdo nemůže volit více než jednou.
3. Nikdo nemůže určit, jak volil kdokoli jiný.
4. Nikdo nemůže duplikovat hlas kohokoli jiného.
5. Nikdo nemůže pozměnit hlas někoho jiného aniž by byl odhalen.
6. Každý volič se může přesvědčit, že jejich hlas byl zahrnut v celkovém součtu.
7. Všichni vědí, kdo volil a kdo ne (nemusí platit pro všechny systémy).

Dalším často zmiňovaným požadavkem na volební systém je jeho **bezchybnost** (přesnost). Systém je možné považovat za bezchybný, pokud všechny platné hlasy budou zahrnuty ve výsledku a žádný neplatný hlas zahrnut nebude.[6][7][8]

Náročným bodem na implementaci je i verifikovatelnost voleb (body 6 a 7). Obecně se rozlišuje univerzální a individuální [8] [6]. Individuální verifikovatelnost představuje možnost voliče ověřit, že jeho hlas byl započítán v celkovém výsledku a že odpovídá tomu, jak hlasoval. Univerzální verifikovatelnost umožňuje komukoli ověřit, že ve volbách jsou započítány hlasy pouze oprávněných voličů.

Tento bod je kontroverzní především tím, že jeho implementace spočívá v poskytnutí nějakého potvrzení o volbě voliči. Toto potvrzení ale může být velice snadno zneužito k manipulaci s výsledky voleb formou skupování hlasů. Některé navrhovaná schémata a systémy se snaží řešit i tuto výzvu [9]. Dalším podobným problémem voleb na dálku je nemožnost odhalit, pokud někdo volí pod nátlakem (*family voting*²⁾).

¹⁾1. Only authorized voters can vote. 2. No one can vote more than once. 3. No one can determine for whom anyone else voted. 4. No one can duplicate anyone else's vote. (This turns out to be the hardest requirement.) 5. No one can change anyone else's vote without being discovered. 6. Every voter can make sure that his vote has been taken into account in the final tabulation. Additionally, some voting schemes may have the following requirement: 7. Everyone knows who voted and who didn't.[5]

²⁾situace, kdy členové rodiny nevolí samostatně, ale společně - ať už dobrovolně nebo pod nátlakem

2 POŽADAVKY NA FUNKČNOST

2.1 Obecné požadavky

Ze zadání práce lze formulovat následující požadavky na aplikaci:

- musí být funkční,
- musí být responzivní - optimalizovaná pro různá zařízení,
- musí být bezpečná.

Dále při návrhu a implementaci aplikace musí být dbáno na dodržování GDPR. K implementaci aplikace by mělo být využito technologií PHP, relační databáze a kryptografie.

2.2 Specifika provozu na UTB

Volební systém představený v této práci je přizpůsoben především pro potřeby provozu na Univerzitě Tomáše Bati (UTB), proto byly do požadavků zahrnuty i další body, specifické pro UTB.

Zaměstnanci i studenti využívají k přihlašování do různých částí a aplikací UTB jednotný systém autentizace a i volební systém by měl být dostupný bez nutnosti vytvářet nové uživatelské účty. Implementace systému Single Sign-On Shibboleth by byla rozsahem nad rámec této práce, proto bylo po diskuzi s vedoucím práce zvoleno řešení využívající autentizaci přes Active Directory pomocí protokolu LDAP. Systém by neměl klást další požadavky na voliče, jako např. unikátní podpisové certifikáty.

Primární užití tohoto systému směřuje na volby do akademických senátů fakult a univerzity. Musí tedy být možné pořádat několik samostatných a nezávislých voleb najednou. Mělo by také být možné systém využít pro hlasování v akademických senátech, ale nabízí se i využití pro různé formy dotazníků spokojenosti. Systém by tedy měl umožnit volby / hlasování s více než jednou “otázkou”.

O výsledku voleb aplikace sestaví protokol a umožní jeho stažení na disk.

2.3 Navrhované řešení

Na základě analýzy různých systémů byl po konzultaci s vedoucím práce zvolen systém na bázi “slepého podepisování” (RSA Blind Signature)[10]. Toto řešení uspokojuje požadavek na anonymitu voleb - bod 3 v části 1.1 - aniž by byl ovlivněn bod 2. Právě splnění prvních tří z těchto požadavků je velice náročné pro většinu jednoduchých volebních systémů [5].

Návrh na nový způsob digitálního podpisu představený D. Chaumem v roce 1983 byl uvažován pro ověřování plateb a princip byl vysvětlen na anonymních volbách. A právě tyto dva případy jsou nejčastějším využitím slepých podpisů nebo jejich obdoby.

Chaum na příkladu anonymních voleb ukazuje, jak je možné nechat ověřit vlastní zprávu důvěryhodnou autoritou, aniž by byl prozrazen obsah zprávy samotné. Volební komisař musí opatřit hlasovací lístek svým vlastnoručním podpisem, zároveň ale nesmí vědět komu volič dává hlas. Volič tedy svůj lístek vloží do propisovací obálky a obálku nechá podepsat komisařem. Jeho podpis se díky propisovací obálce dostane i na hlasovací lístek, volič následně lístek vyjme z obálky a vloží ho do obálky volební, kterou vhodí do urny. Při sčítání hlasů pak komisař může ověřit pravost lístku díky přítomnosti vlastnoručního podpisu [10].

2.4 RSA Blind Signature

Implementace slepého podpisu je nejsnazší při použití RSA algoritmu. Ve standardní verzi algoritmu je digitální podpis zprávy m vypočítán jako $m^d \pmod{N}$, kde N je modul a d je dešifrovací exponent protokolu RSA. Verze slepého podpisu zavádí *zaslepovací faktor* r , kterým je náhodně zvolené číslo nesoudělné s N [10].

Zpráva je k podpisu předána zaslepená tímto faktorem umocněným šifrovacím exponentem e , podepisována je tedy zpráva m' .

$$m' = m \cdot r^e \pmod{N}$$

Podpis vzniká standardním způsobem, jelikož se ale jedná o podpis zaslepené zprávy, je značena jako s' .

$$s' = (m')^d \pmod{N}$$

Po podepsání zprávy je z podepsané zprávy odstraněno zaslepení inverzní operací a výsledkem je podepsaný originál zprávy.

$$s = s' \cdot r^{-1} \pmod{N}$$

Že se skutečně jedná o podpis originální zprávy vyplývá ze samotného protokolu RSA [11].

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

Tento způsob, kdy se podepisuje přímo zpráva, není vhodný - umožňuje útok na podpis - a místo zprávy m je pracováno s výsledkem kryptografické hašovací funkce (hashí) $H(m)$ [12].

ZÁVĚR

...

SEZNAM POUŽITÉ LITERATURY

- [1] Goldsmith, B.; Ruthrauff, H.: Case Study Report on Electronic Voting in the Netherlands. Dostupné z: https://www.ndi.org/sites/default/files/5_Netherlands.pdf, [b.r.].
- [2] Valášek, M.: Lesk a bída elektronických voleb [online]. Dostupné z: <https://www.altair.blog/2020/07/evolby>, 2020, [cit. 2021-05-09].
- [3] Alvarez, R. M.; Hall, T. E.; Trechsel, A. H.: Internet Voting in Comparative Perspective: The Case of Estonia. *PS: Political Science & Politics*, ročník 42, č. 3, 2009: str. 497–505, doi:10.1017/S1049096509090787.
- [4] Germann, M.; Serdült, U.: Internet voting and turnout: Evidence from Switzerland. *Electoral Studies*, ročník 47, 2017: s. 1–12, ISSN 0261-3794, doi: <https://doi.org/10.1016/j.electstud.2017.03.001>.
- [5] Schneier, B.: *Applied cryptography*. Indianapolis: Wiley, druhé vydání, 1996, ISBN 978-0471117094.
- [6] Anane, R.; Freeland, R.; Theodoropoulos, G.: e-Voting Requirements and Implementation. In *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*, 2007, s. 382–392, doi:10.1109/CEC-EEE.2007.42.
- [7] Qadah, G. Z.; Taha, R.: Electronic voting systems: Requirements, design, and implementation. *Computer Standards & Interfaces*, ročník 29, č. 3, 2007: s. 376–386, ISSN 0920-5489, doi:<https://doi.org/10.1016/j.csi.2006.06.001>.
- [8] Novotný, M.: Design and Analysis of a Practical E-Voting Protocol. In *The Future of Identity in the Information Society*, Berlin: Springer, 2009, ISBN 978-3-642-03315-5, s. 170–183.
- [9] Barros, C.; Pimenta, D.: A Receipt-Free Voting System Based on Blind Signatures and Anonymous IDs. Dostupné z: <https://sol.sbc.org.br/index.php/sbseg/article/download/4277/4208/>, 2018.
- [10] Chaum, D.: Blind Signatures for Untraceable Payments. In *Advances in Cryptology*, Boston, MA: Springer US, 1983, ISBN 978-1-4757-0602-4, s. 199–203.
- [11] Rivest, R. L.; Shamir, A.; Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, ročník 21, č. 2, 1978: s. 120–126.

- [12] Yun, C.: Adventures with RSA Blind Signing [online]. Dostupné z: <https://cathieyun.medium.com/adventures-with-rsa-blind-signing-397035585121>, 2021, [cit. 2021-05-11].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

MVC	Model View Controller
MVP	Model View Presenter
DDD	Domain Driven Design
ACL	Access Control List
SRP	Single Responsibility Principle
CSRF	Cross-site request forgery
LDAP	Lightweight Directory Access Protocol

SEZNAM OBRÁZKŮ

Obr. 2.1. Formulář založení nových voleb	23
--	----

SEZNAM TABULEK

SEZNAM FRAGMENTŮ ZDROJOVÉHO KÓDU

SEZNAM PŘÍLOH

- P I. Adresářová struktura aplikace
- P II. Založení a správa voleb v aplikaci
- P III. Průběh voleb z pohledu voliče
- P IV. Balíčky třetích stran

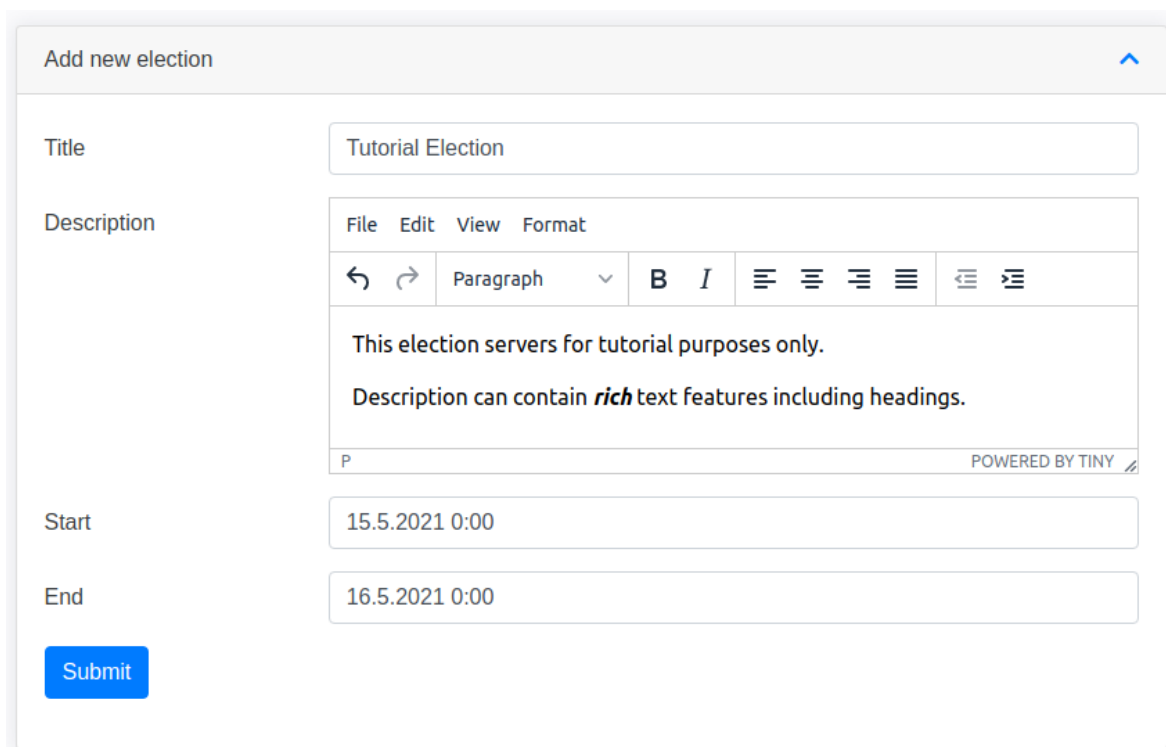
PŘÍLOHA P I. ADRESÁŘOVÁ STRUKTURA APLIKACE

```
/
├── app
│   ├── Backend
│   │   ├── Classes
│   │   ├── Presenters
│   │   │   └── templates
│   │   └── Utils
│   ├── config
│   ├── Core
│   │   ├── Classes
│   │   ├── Presenters
│   │   │   └── templates
│   │   └── Utils
│   ├── Forms
│   ├── Frontend
│   │   ├── Classes
│   │   ├── Presenters
│   │   │   └── templates
│   ├── Models
│   │   ├── Entities
│   │   ├── Factories
│   │   ├── Mappers
│   │   │   └── Db
│   │   └── Traits
│   ├── Repositories
│   ├── Router
│   └── Bootstrap.php
├── bin
├── keys
├── log
├── temp
├── vendor
├── www
├── www_backend
└── composer.lock
```

PŘÍLOHA P II. ZALOŽENÍ A SPRÁVA VOLEB V APLIKACI

Založení

- Kliknutím na tlačítko vytvoření nových voleb (v záhlaví datagridu) je zobrazen formulář pro editaci voleb.



Add new election

Title: Tutorial Election

Description: This election servers for tutorial purposes only. Description can contain *rich* text features including headings.




Start: 15.5.2021 0:00

End: 16.5.2021 0:00

Submit

Obrázek 2.1 Formulář založení nových voleb (zdroj: vlastní)

- Po vyplnění a odeslání formuláře lze uložené hodnoty upravit pomocí editačního tlačítka na příslušném řádku v datagridu.
- Na detail voleb lze přejít kliknutím na tlačítko detailu v příslušném řádku datagridu.

Tutorial Election	no	no	15.5.2021 0:00	16.5.2021 0:00	  
-------------------	----	----	----------------	----------------	---

Řádek datagridu (zdroj: vlastní)

Otázky

Nastavení otázek se provádí na záložce *Questions*. Již přidané otázky jsou zobrazeny v datagridu a lze je upravovat. Nové otázky se přidávají tlačítkem v záhlaví datagridu. Název otázky slouží pro orientaci v seznamu definovaných otázek, voliči není zobrazen.

Každá otázka musí mít nastaven minimální a maximální možný počet odpovědí. Limit se při validaci aplikuje pouze pokud je vybrána alespoň jedna odpověď. Pro nepovinné otázky tedy není nutné zadávat limit 0 (aplikace to ani nepovolí). Dalšími poli je text samotné otázky a nastavení zda je odpověď na otázku vyžadována.

Toto umožňuje dvojí řešení, pokud je vyžadována možnost zdržet se volby (hlasování). Nepovinná otázka umožňuje neodpovídat, ale ve výsledcích voleb není zohledněno, že volič se rozhodl neodpovědět (jinak než porovnáním počtu ostatních možností a odevzdaných hlasů). Druhým řešením je volbu „Zdržel se” zavést jako jednu z možných odpovědí. V takovém případě bude zohledněna tato volba i ve výsledcích. Obdobně by se dalo dívat i na odpovědi „Nechci odpovídat”, „Nevím” apod.

V poslední části formuláře je možné přidávat jednotlivé odpovědi.

- Další odpovědi lze přidávat kliknutím na tlačítko plus, odebírat tlačítkem minus.
- Minimum a maximum možných definic odpovědí je definováno ve zdrojovém kódu formuláře. Výchozí hodnoty jsou minimálně jedna a maximálně pět odpovědí.
- Výchozí hodnoty lze přepsat metodami:
 - `QuestionForm::setMultiplierCopies($copies)` pro minimum a
 - `QuestionForm::setMultiplierMaxCopies($maxCopies)` pro maximum.

Tyto metody je ideální volat v místě vytváření formuláře, tedy v `ElectionPresenter::createComponentQuestionForm()`.

- Změnit výchozí hodnoty napřímo v kódu lze ve třídě `HasMultiplier`¹⁾.

Po odeslání formuláře jsou data uložena a otázky i odpovědi je možné upravit opět pomocí editačního tlačítka. Celou otázku lze smazat červeným tlačítkem odpadkového koše. Jednotlivé odpovědi lze mazat ze samostatné záložky *Answers*.

Seznam voličů

Seznam voličů vzniká z CSV souboru nahraného prostřednictvím aplikace.

- Aktuální seznam voličů je dostupný přes záložku *Voter List*.
- Na záložce *Voter Files* je seznam již nahraných souborů.
- Nové soubory lze nahrát prostřednictvím kontextového menu dostupného po kliknutí na ikonu ozubeného kola.

¹⁾`App\Forms\HasMultiplier`

- Kterýkoli z nahraných souborů lze aplikovat pro dané volby kliknutím na zelené tlačítko „Apply”.
- Nahrané soubory lze také smazat nebo stáhnout do počítače a zobrazit jejich obsah.
- Smazání nahraného souboru neovlivní již aplikovaný seznam voličů.

Spuštění voleb

Před aktivací voleb je nutné nahrát veřejnou část RSA klíče volební komise prostřednictvím kontextového menu (ozubené kolo). Tento klíč by měl být uložen na bezpečném místě a volební komise by měla zajistit jeho patřičnou zálohu v případě ztráty nebo poškození originálu. Není možné použít klíč chráněný heslem (použitá knihovna `phpseclib` použití takového klíče nicméně umožňuje a aplikace by k tomu mohla být upravena). Úspěšně nahraný klíč je viditelný na záložce *Overview* v tabulce s šifrovacími klíči.

V tuto chvíli je možné volby aktivovat opět prostřednictvím ozubeného kola.

Ukončení voleb

- Po skončení období nastaveného pro dané volby jsou zpřístupněny další akce na detailu voleb.
- Přes kontextové menu je nyní možné nahrát privátní část klíče volební komise.
- Po úspěšném nahrání klíče je tento také vidět na záložce *Overview*
- Kliknutím na tlačítko „Decrypt and count ballots” na záložce *Results* jsou spočítány odevzdané hlasy
- Výsledky voleb jsou zobrazovány i voličům
- Pomocí kontextového menu je možné stáhnout volební protokol
- Volby je možné deaktivovat přes kontextové menu, neaktivní volby se již nezobrazují voličům.
- Ukončené volby včetně všech podstatných náležitostí je možné smazat červeným tlačítkem odpadkového koše v datagridu všech voleb. Veškeré záznamy spojené s těmito volbami budou rovněž odstraněny. Tato akce je nevratná!

PŘÍLOHA P III. PRŮBĚH VOLEB Z POHLEDU VOLIČE

UTB

UTB voting system

první volby

Volby do **AS FAI** - volební obvod studentů

Volby na funkční období 2021 až 2024. Volí se 4 zástupci.

Vyberte maximálně 4 jména kandidátů, kterým chcete dát svůj hlas. Můžete vybrat i méně.

Starts : 12.04.2021 10:01 (1 month ago)
Ends : 17.04.2021 00:00 (3 weeks ago)

VIEW RESULTS

Tutorial Election

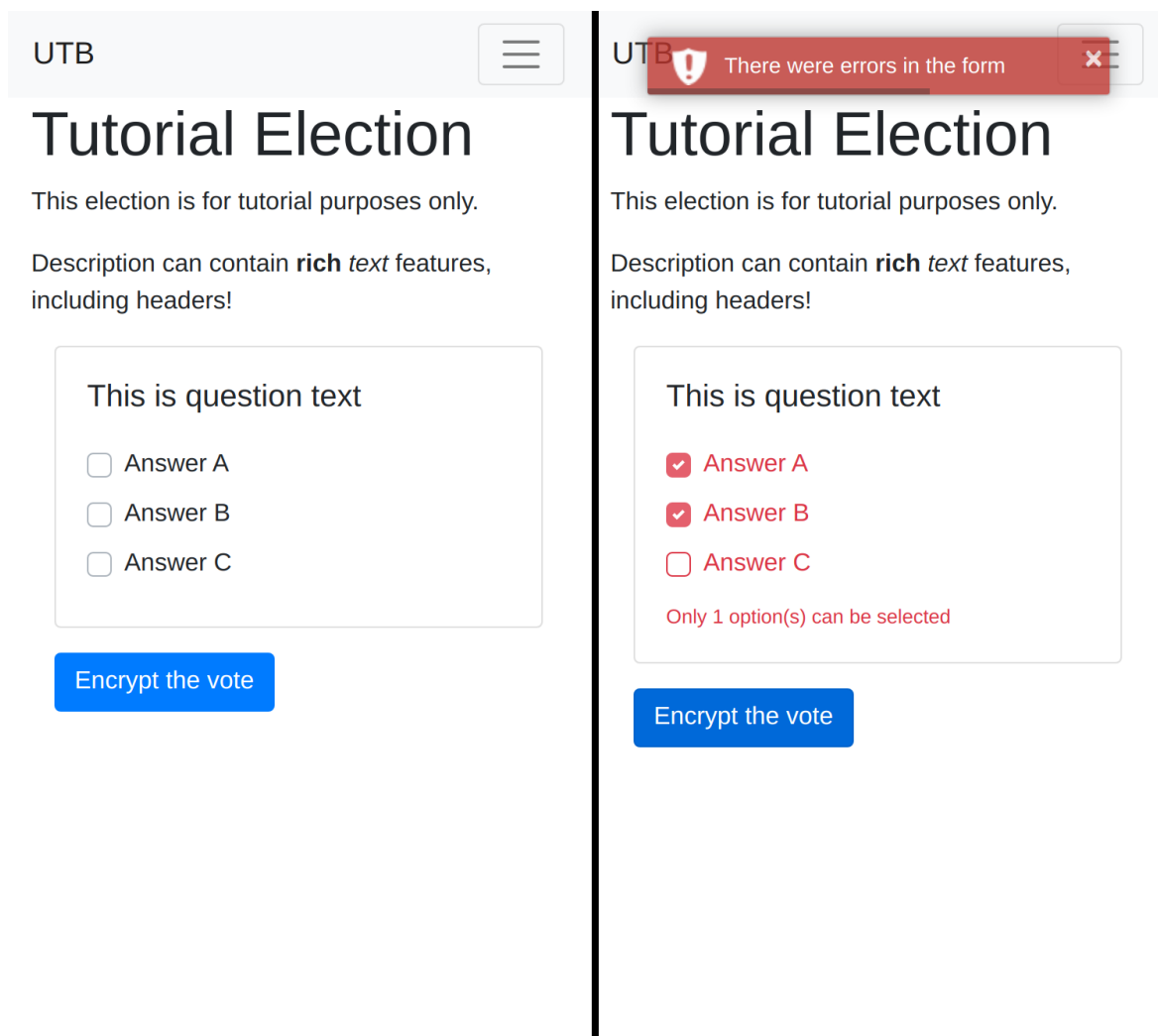
This election is for tutorial purposes only.

Description can contain **rich text** features, including headers!

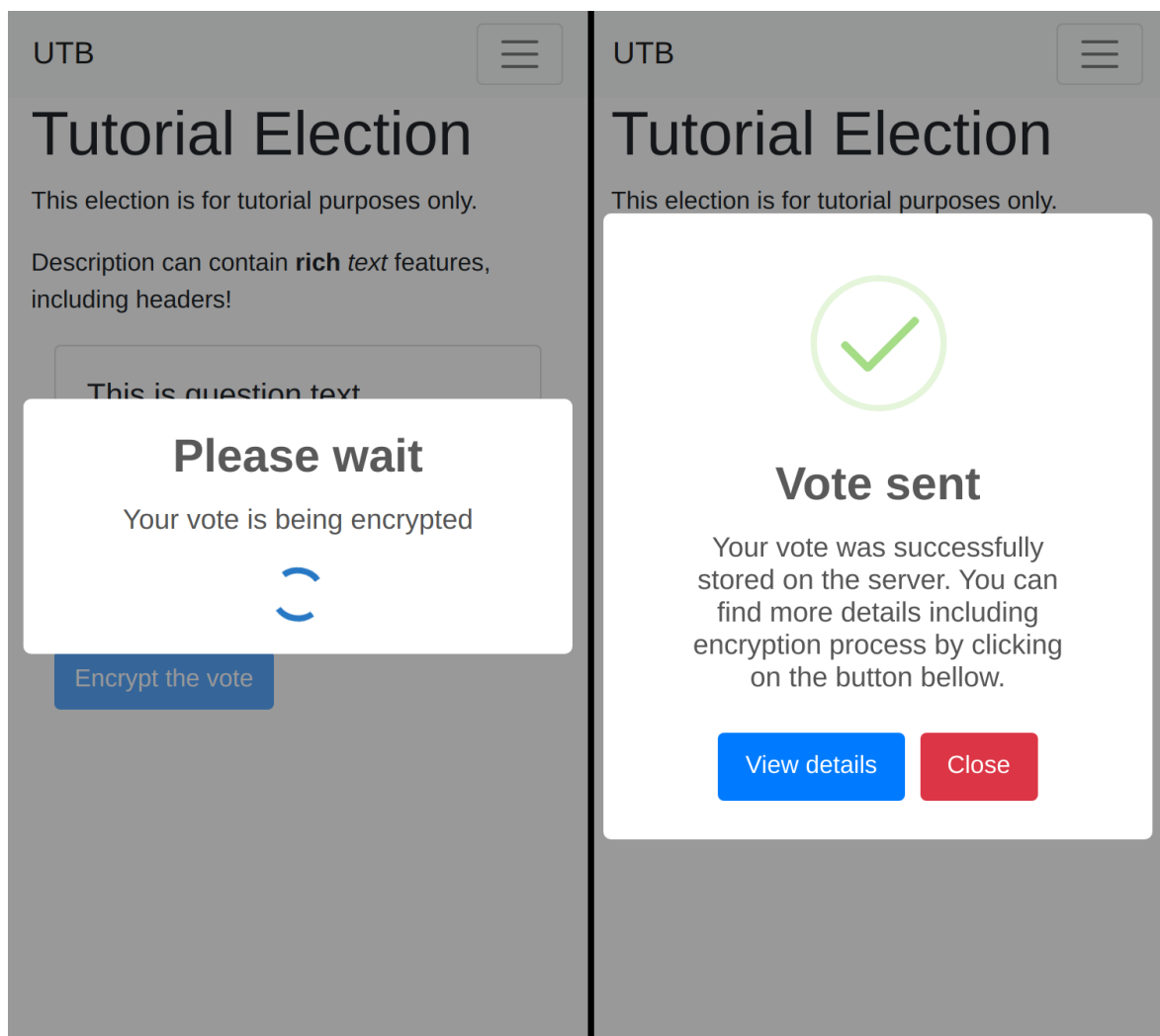
Starts : 15.05.2021 00:00 (in 1 day)
Ends : 17.05.2021 00:00 (in 3 days)

CAST MY VOTE!

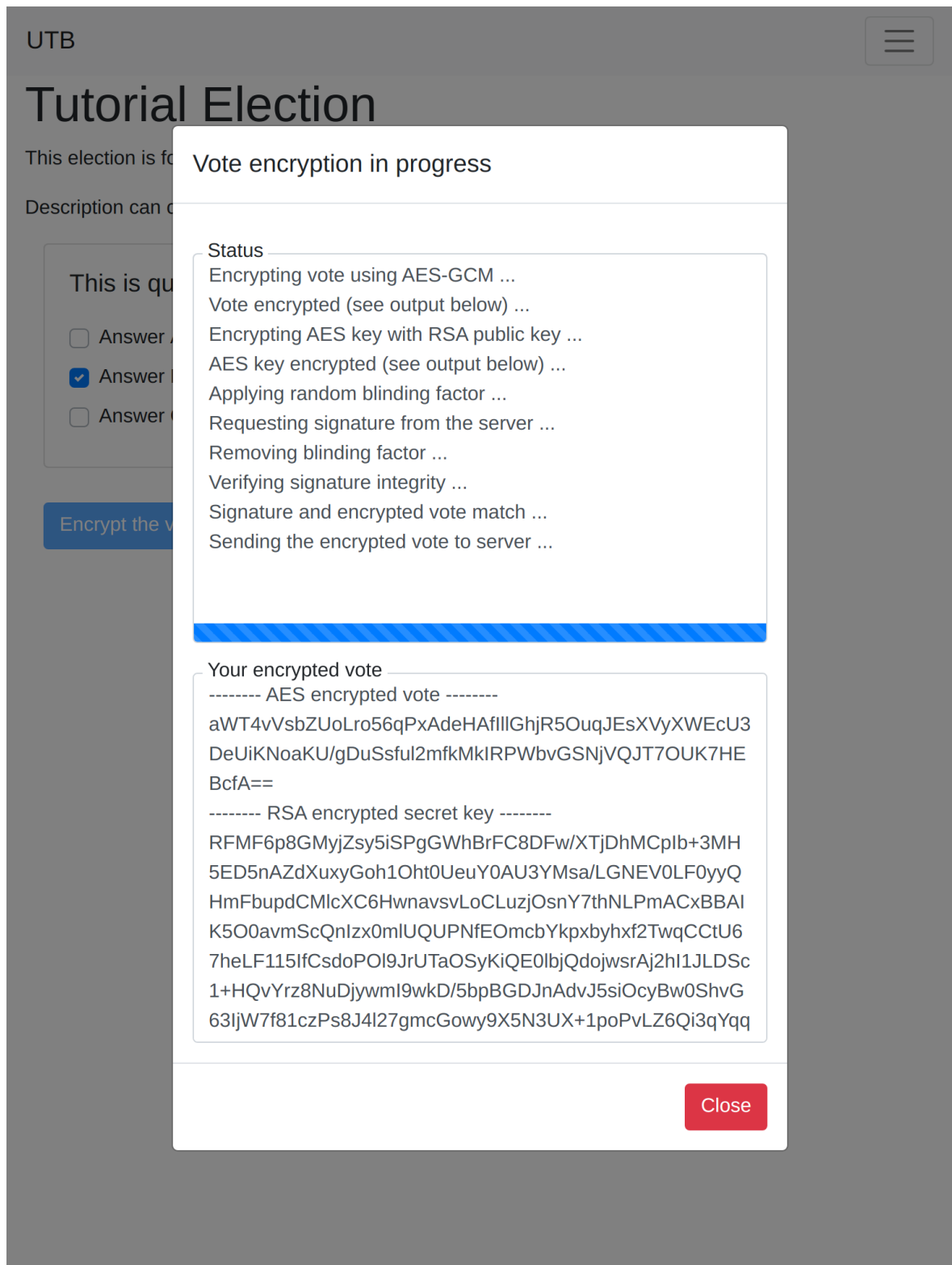
Popisek obrázku (zdroj: vlastní)



Popisek obrázku (zdroj: vlastní)



Popisek obrázku (zdroj: vlastní)



Popisek obrázku (zdroj: vlastní)

PŘÍLOHA P IV. BALÍČKY TŘETÍCH STRAN

Datagrid