Inštalačná príručka

Tímový projekt 2021/2022

Tím č. 17

Marek Ceľuch, Libor Duda, Lucia Janíková, Denis Klenovič,
Timotej Králik, Adam Slatinský, Matúš Staš

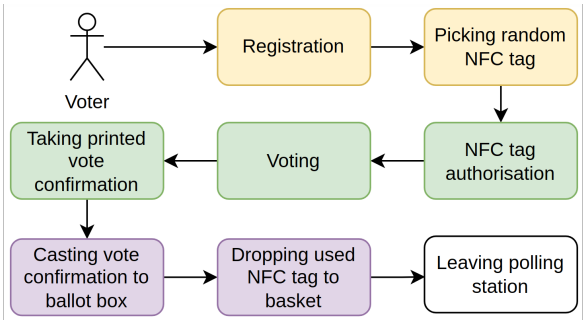
Ing. Jaroslav Erdelyi

Obsah

1. Všeobecný pohľad

Súčasný systém volieb čelí problémom ako pomalé manuálne sčítanie hlasov, vysoké organizačné náklady, je náchylný na chyby spôsobené ľudským faktorom a občas chýba dôvera širokej verejnosti. Digitalizované volebné systémy by výrazne znížili náklady na voľby, čas potrebný na finalizáciu výsledkov, spotrebu papiera a eliminovali ľudský vstup do sčítania hlasov. Preto náš tím Electie prichádza s inovatívnou vízou pre elektronizáciu volebného procesu. Hlasovacie hárky sme nahradili dotykovými obrazovkami, vďaka čomu je možné hlasy zbierať a sčítavať automatizovane.

1.1 Volebný proces

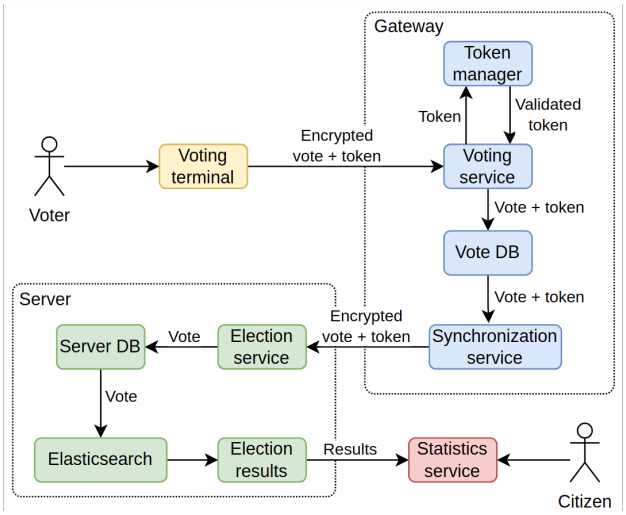


Z pohľadu voliča sa samotný proces hlasovania zásadne nemení v porovnaní s tradičným spôsobom. Volič príde do volebnej miestnosti a podrobí sa overeniu identity členom komisie. Namiesto obdržania veľkého množstva papierov s kandidátmi dostane volič NFC tag určený na autorizáciu pri volebnom termináli. Volič pristúpi k volebnému terminálu a priloží NFC tag ku čítačke a po úspešnej autorizácii je odomknutá volebná aplikácia. Veľký dotykový displej zobrazuje zoznam dostupných kandidátov. Volič môže vyhľadávať kandidátov podľa mena, prechádzať stránkami v zozname strán a vyberať preferovaných kandidátov. Volič musí potvrdiť svoju voľbu v každom medzikroku a na konci po zobrazení sumáru hlasovania opäť potvrdiť svoj výber.

Taktiež je možné odovzdať aj prázdny hlas ako to je možné pri klasických voľbách. Volebný terminál informuje voliča o úspechu voľby a vytlačí potvrdenie o hlasovaní (malý papier, ktorý obsahuje QR kód pre možnosť offline sčítania hlasov). Následne volič vhodí potvrdenie do volebnej urny a hlasovací proces je z pohľadu voliča ukončený.

1.2 Životný cyklus hlasu

Dáta reprezentujúce hlas voliča v JSON formáte sú odoslané na backend terminálu, kde sa overí platnosť voličovho autorizačného tokenu a následne je potvrdený aj jeho hlas. Šifrovaný hlas spolu s identifikátorom volebného terminálu a autorizačným tokenom voliča je odoslaný na gateway, kde sa spracuje. Voting Service dešifruje hlas kľúčom daného volebného terminálu a následne overí platnosť autorizačného tokenu. Ak je token platný, hlas sa uloží do databázy a je vrátená správa o úspešnom spracovaní požiadavky. Akonáhle terminál prijme odpoveď, tlačiareň vytlačí potvrdzujúci doklad (malý papier) s podrobnosťami o hlasovaní a QR kódom.



Po odhlasovaní je použitý autorizačný token deaktivovaný, takže s ním nie je možné znova hlasovať. Ak je gateway pripojený k internetu, Synchronization service začne odosielať šifrované hlasy na hlavný server v pravidelných intervaloch. Hlasy sú potom spracované na serveri službou Voting service, kde sa dešifrujú hlasy pomocou príslušných kľúčov a ak je elektronický podpis platný, hlas je uložený do hlavnej databázy. Hlavný server pravidelne reindexuje nové hlasy pomocou technológie ElasticSearch pre efektívne získavanie štatistík a umožnenie rôznych dopytov nad výsledkami.

Konečné výsledky sú k dispozícii hneď ako všetky gateway-e zosynchronizujú všetky svoje hlasy. Naše riešenie sme pripravili na veľké množstvo návštevníkov, preto je dopytovanie nad výsledkami vykonávané pomocou ElasticSearch-u. Táto technológia podporuje distribuované výpočty a je vysoko škálovateľná. Používateľom ponúkame vizualizáciu výsledkov volieb podľa krajov a okresov Slovenska a taktiež je možné vidieť aj rozdelenie kresiel pre strany v parlamente.

Používatelia môžu tiež zadávať vlastné dopyty filtrovaním konkrétneho mesta, regiónu, alebo iného geografického členenia. Zároveň je možné poskytovať čiastkové výsledky volieb aj pokým ešte nie sú ukončené, ak to individuálny prípad použitia umožňuje.

2. Bezpečnosť a šifrovanie

Bezpečnosť je vo voľbách, najmä v elektronických, prakticky najdôležitejším prvkom. Porušenie integrity volieb môže viesť k zmene výsledkov a v dôsledku toho k zvoleniu nesprávnych kandidátov. Takéto bezpečnostné incidenty by spravili riešenie prakticky nepoužiteľným a reputačne by zrujnovali jeho tvorcov. Preto je potrebné dostatočne dbať na bezpečnosť.

Naše riešenie zahŕňa jeden centrálny server, na ktorý sú hlasy z gateway-ov sú odosielané cez verejnú internetovú sieť. Práve táto časť komunikácie predstavuje najzraniteľnejší článok v celom volebnom procese. Existuje tu možnosť, že potenciálny útočník by túto komunikáciu odychytil a následne by bol schopný prečítať odosielané hlasy alebo v horšom prípade ich nahradiť inými.

Preto sme navhrli a implementovali vlasntý šifrovací a podpisovací protokol. Rozhodli sme sa použiť 4096bit RSA a 256bit AES algoritmy na šifrovanie prenášaných hlasov. Samotné hlasy sú zašifrované pomocou symetrického kľúča AES, ktorý je potom zašifrovaný verejným kľúčom RSA hlavného serveru. Hlasy sú tiež podpísané privátnym RSA kľúčom gateway-a, ktorý zabezpečí, že počas prenosu na server dáta nemôžu byť zmenené bez toho, aby to server zistil pri validácii podpisu.

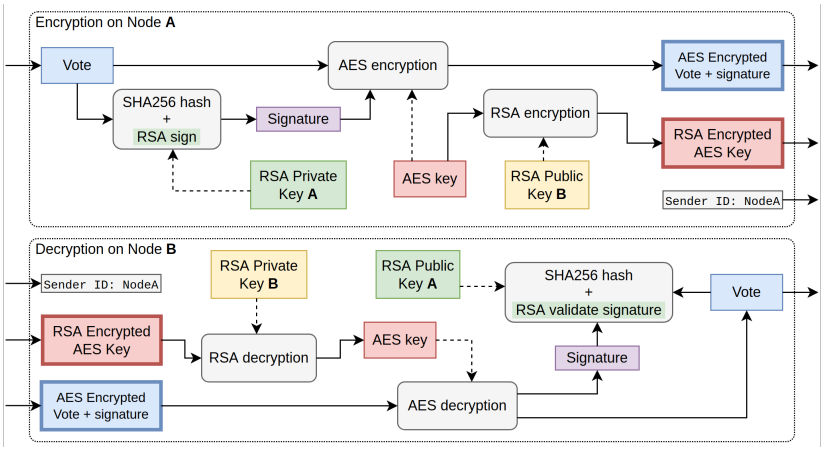
2.1 Nástrahy RSA

Pri RSA kľúčoch je potrebné zabezpečiť, aby privátny kľúč zariadenia nebol nikdy nikde zverejnený. V tom prípade je prakticky nemožné ho náhodne uhádnuť a sfalšovať správu. Algoritmus AES sa

používa kvôli jeho rýchlosti a schopnosti šifrovať správy neobmedzenej dĺžky a je v súčasnosti priemyselným štandardom.

Výmena kľúčov je najdôležitejšou súčasťou RSA šifrovania. Pri výmene verejných kľúčov po verjenej sieti je teoreticky možný man-in-the-middle útok, kedy komunikácia prechádza cez nejaký napadnutý uzol, v ktorom útočník odchytí verejné kľúče, tie si zapamätá a reálnym zariadeniam pošle vlastné kľúče bez toho, aby to zariadenia mohli odhaliť. Výmena verejných kľúčov sa u nás vykonáva ešte počas procesu konfigurácie gateway-a autorizovaným personálom pred voľbami v špecializovaných krajských volebných centrálach. Tu môže zapríčiniť chybu iba ľudský faktor, čo sa rovanko môže stať aj pri doteraz zaužívanom spôsobe volieb.

2.2 Vlastná knižnica



Pre každý gateway existuje iný RSA pár, čo znamená, že aj v prípade odhalenia jedného kľúča zostáva integrita volieb pomerne neporušená. Implementovali sme vlastnú knižnicu v Pythone, ktorá poskytuje hlavne dve metódy - šifrovanie a dešifrovanie správy. Tieto metódy potrebujú privátny kľúč lokálneho zariadenia, verejný kľúč opačného zariadenia a ID opačného zariadenia. Na základe tohto sa hlas podpíše, zašifruje AES kľúčom, AES kľúč sa zašifruje verejným RSA kľúčom, pribalí sa do finálnej správy a môže sa odoslať. Na opačnom zariadení sú tieto operácie vykonané opačne.

2.3 Volebná miestnosť

Rovnaký proces šifrovania sa používa aj vo vnútri lokálnej siete s volebnými terminálmi. Všetka komunikácia medzi volebnými terminálmi a gateway-om prebieha len po lokálnej sieti realizovanej fyzickými káblami, ktoré má pod kontrolou volebná komisia v miestnosti. Keby sa i napriek tomu útočník pokúsil pripojiť k sieti a odoslať falošný hlas, nemal by platný privátny kľúč volebného terminálu, takže jeho pokus o útok by zlyhal pri overovaní hlasu, hlas by nebol prijatý.

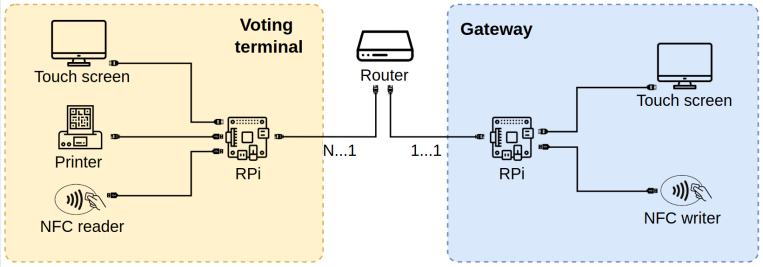
3. Inštalačná príručka

Systém Electie pozostáva z hardvérovej a softvérovej časti, pričom je možné ho spustiť ako celok navrhnutým spôsobom na poskytnutom hardvéri vo volebnej miestnosti alebo iba čisto ako softvérové komponenty na vlasntej infraštruktúre.

3.1 Príprava pred voľbami

Pred každými voľbami je potrebné zabezpečiť niekoľko vecí. - prirpaviť konfiguračný súbor so zoznam kandidátov - pripraviť zoznam volebných miestností - rozdistribuovať verejné kľúče medzi gateway zariadeniami a serverom - nahrať novú konfiguráciu na gateway zariadenia

3.2 Zapojenie zariadení vo volebnej miestnosti



Komisia vo volebnej miestnosti musí zapojiť zariadenia podľa zobrazenej schémy. V miestnosti existuje jeden router, ktorý môže, ale nemusí byť pripojený na internet. Router disponuje DHCP serverom.

3.2.1 Gateway

V miestnosti je ďalej práve jeden gateway. Ten sa skladá z Raspberry Pi, NFC zapisovačky a dotykového displeja. Dotytkový displej sa pripája k Raspberry pomocou HMDI a USB. NFC zapisovačka je pripojená pomocou USB. Ethernetovým káblom je gateway pripojený k centrálnemu routeru. Po tomto všetkom je možné pripojiť Raspberry do elektrickej siete.

3.2.2 Volebný terminál

Volebných terminálov môže byť v miestnosti 1 až N. Volebný terminál pozostáva z Raspberry Pi, dotykovej obrazovky, NFC čítačky a termotlačiarne. Obrazovka a čítačka sa pripájajú podobne ako na gateway-i. Rovnako ethernetom sa VT pripája k routeru. Tlačiareň by mala byť pripojená ethernetovým káblom priamo k Raspberry Pi s osobitným DHCP serverom, ale pre účely študentského dema postačuje pripojiť tlačiareň ethernetovým káblom priamo do toho istého routera. Po prepojení týchto komponentov je možné pridať elektrickú energiu.

3.2.3 Server

Z pohľadu volebnej komisie je server nejaký black box v cloude. Na starosti ho majú špecializovaní pracovníci verejnej správy. Aby volebné miestnosti mohli komunikovať s týmto serverom, potrebujú mať v gateway-och správne nakonfigurovanú jeho adresu.

3.3 Inštalaácia systému na vlastnej architektúre

V kontexte spúšťania nášho systému na vlastnej architektúre, či už pri reálnom použití alebo pri ďalšej študentskej práci na projekte, podrobnejšie technické detaily sú potrebné.

3.3.1 Technológie

Všetky API backendy bežia v Pythone na FastAPI frameworku. Používame Python verzie 3.10. Frontendy webových aplikácií sú u nás single page aplikácie vo frameworku Svelte. Na serveri a gateway-i používame MongoDB databázu. Pre poskytovanie finálnych štatistík existuje ešte na serveri aj inštancia ElasticSearch-u.

Naše riešenie postavené na oddelených kontajneroch, ktoré je možné inak označiť ako mikroslužby. Každý kúsok softvéru má svoj kontajner a teda nič nie je potrebné spúšťať lokálne priamo na počítači. Gateway, VT aj server sa skaldajú z viacerých služieb, ktoré je potrebné spúšťať istým spôsobom spolu. Preto je pre každú túto časť vytvorený docker-compose súbor, ktorý predpisuje požadovanú orchestráciu jednotlivých kontajnerov. Všetky časti riešenia je zaručene možné spustiť na amd64 aj arm64 architektúrach.

Je potrebné mať nainštalovaný Docker verzie aspoň `19.03` a Docker Compose aspoň `1.25.5`. V optimálnych prípadoch stačí v koreni repozritára zavolať príkaz podobný nasledovnému:

```
docker-compose up -d
```

Pre lepšie pochopenie a zorientovanie sa v aplikáciách odporúčame sa všeobecne popozerať do docker-compose súborov, Dockerfilov a start.sh skriptov, z ktorých je možné sa dozvedieť ďalšie detaily o premenných prostredia, orchestrácii a jednotlivých kontajneroch.

Nižšie úvádzamé najzákladnejší spôsob spustenia jednotlivých komponentov z koreňov repozitárov. Pre detailnejšie informácie pozri dokumentáciu jednotlivých častí.

3.3.2 Server

```
docker compose up -d --build
```

Server by mal byť dostupný na http://localhost:8222/. Overte cez http://localhost:8222/docs

Viac tu

3.3.3 Gateway

```
docker-compose up -d --build
```

Gateway by mal byť dostupný na http://localhost:8080/.

Jeho služby sú ale až na subpath-och:

Služba	Cesta
Voting service	`localhost:8080/voting-service-api/`
Synchronization service	`localhost:8080/synchronization-service-api/`
Voting process manager	`localhost:8080/voting-process-manager-api/`
Token manager	`localhost:8080/token-manager-api/`
State vector	`localhost:8080/statevector/`

Viac tu

3.3.4 Volebný terminál

Pozor: Aby sa VT dokázal zaregistrovať a spustiť, je potrebné v gateway adminovi v časti "Volebné terminály" spustiť registráciu volebných terminálov. (PIN je defaultne 0000)

```
docker-compose up -d --build
```

Volebný terminál by mal byť dostupný na http://localhost:81/

Viac tu