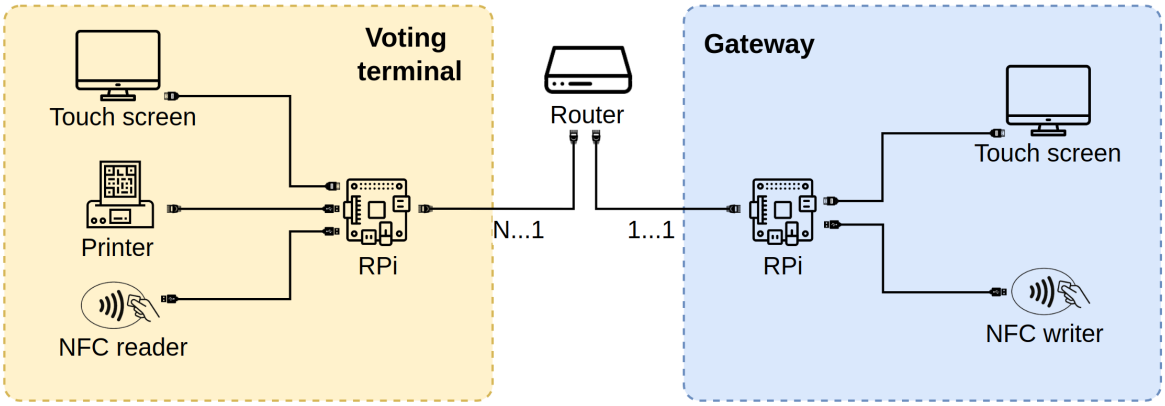
1. Zariadenia vo volebnej miestnosti

Vo volebnej miestnosti sa nachádza gateway a viaceré volebné terminály pripojené na gateway ethernetovým káblom. Gateway komunikuje s jediným centrálnym serverom, vykonáva synchronizáciu hlasov.



Volebný terminál pozostáva z 22 palcovej LCD dotykovej obrazovky, na ktorej je voličovi umožnené voliť. Obrazovka je pripojená k Raspberry Pi, ktoré komunikuje s NFC čítačkou pre umožnenie autorizácie pomocou autorizačných tokenov nahraných na NFC tagoch. Ďalej komunikuje s termo-tlačiarňou, ktorá umožňuje tlač potvrdenia o voľbe.

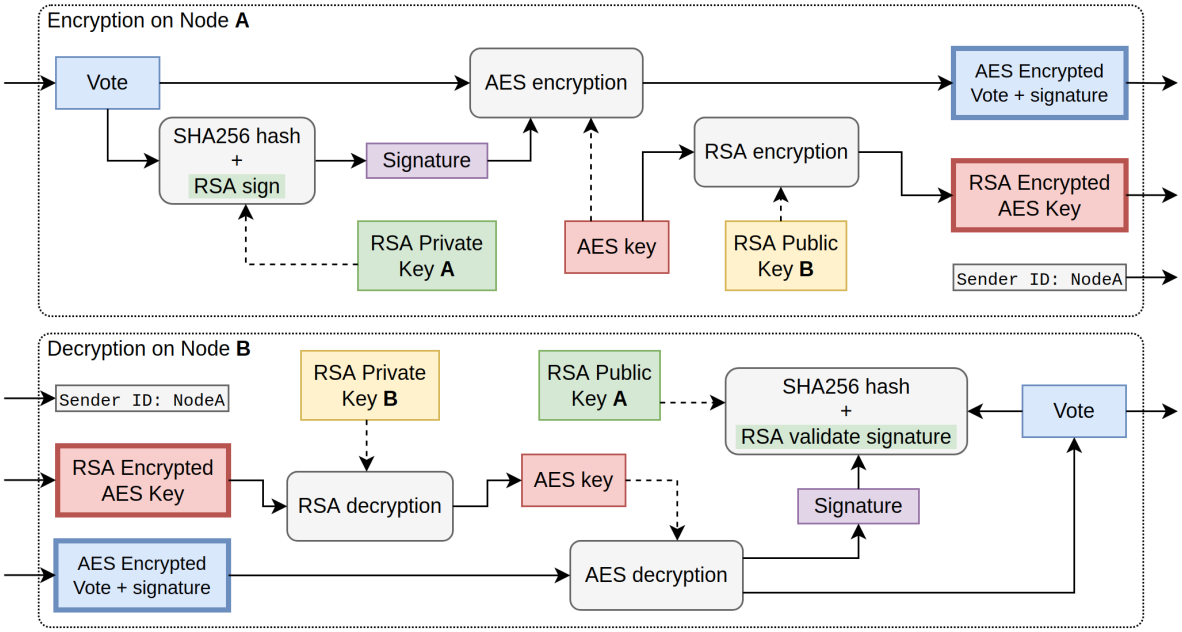
Gateway umožňuje manažovať celú volebnú miestnosť s terminálmi. Ako jediné zariadenie komunikuje priamo s centrálnym serverom cez internet. Skladá sa z Raspberry Pi, ktoré hostuje všetky mikroslužby manažujúce priebeh volieb. Ku gateway-u je pripojená malá dotyková obrazovka, ktorá slúži na prístup volebnej komisie k systému pre umožnenie riadenia priebehu volieb. Ku gateway-u je tiež pripojená NFC zapisovačka na zapisovanie generovaných autorizačných tokenov na tagy.

Hlavný server je zodpovedný za spracovanie hlasov zo všetkých gateway-ov do jednej databázy a vykonávanie štatistických výpočtov, vizualizáciu výsledkov volieb.

Nastavenia pre jednotlivé voľby sú dané konfiguráciou.

2. Šifrovanie komunikácie

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.



Keďže naše riešenie zahŕňa iba jeden centrálny server a hlasy z gateway-ov sú odosielané cez verejnú internetovú sieť, rozhodli sme sa použiť RSA a 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 asymetrickým privátnym kľúčom RSA gateway-a, ktorý zabezpečí, že počas prenosu na server dáta neboli zmenené. Zapojením súkromného kľúča volebnej miestnosti sme zabezpečili, že aj keby útočník poznal verejný kľúč hlavného servera, potrebovali by poznať aj privátny kľúč konkrétnej volebnej miestnosti. Algoritmus AES sa používa kvôli jeho rýchlosti a schopnosti šifrovať správy neobmedzenej dĺžky a je v súčasnosti priemyselným štandardom. Rovnaký proces šifrovania sa používa aj vo vnútri lokálnej siete s volebnými terminálmi.

Všetka komunikácia medzi volebnými terminálmi a gateway-om prebieha len cez lokálnu sieť Ethernet. Okrem toho je každý odoslaný hlas šifrovaný pomocou moderných kryptografických algoritmov. 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.

Výmena kľúčov je najdôležitejšou súčasťou RSA šifrovania. Výmena verejných kľúčov sa vykonáva počas procesu konfigurácie gateway-a autorizovaným personálom pred voľbami. Tu môže zapríčiniť chybu iba ľudský faktor, čo sa taktisto môže stať aj pri doteraz zaužívanom spôsobe volieb.

3. tmp 2

ahoj

3.1 tmp 2.1

ahoj 2

4. State vector

4.1 Nadpis 2

4.1.1 Nadpis 3

4.1.2 Ukážka kódu

```
import os
from dotenv import load_dotenv

from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC
from selenium.webdriver.common.by import By

load_dotenv()
PAGE_LOAD_DELAY = os.getenv("PAGE_LOAD_DELAY") # seconds

def is_text_present (driver, text):
    return str(text) in driver.page_source

def click_on (driver, element):
    driver.execute_script("arguments[0].click();", element)

def find_element (driver, identifier, by = By.CLASS_NAME):
    WebDriverWait(driver,
       PAGE_LOAD_DELAY).until(EC.presence_of_element_located((by,
       identifier)))

def find_clickable_element (driver, identifier, by = By.CLASS_NAME):
    return WebDriverWait(driver,
       PAGE_LOAD_DELAY).until(EC.element_to_be_clickable((by,
       identifier)))

def wait_for_redirect (driver, target_url):
    WebDriverWait(driver, PAGE_LOAD_DELAY).until(lambda driver:
       driver.current_url != target_url)
```

5. Voting service

5.1 Nadpis 2

5.1.1 Nadpis 3

5.1.1.1 Nadpis 4

Name	Value
Item 1	Blue
Item 2	Green