FACULTY OF ENGINEERING
AND ARCHITECTURE

Online Voting System Presentation - Group 4

Information Security 2023-2024

GHENT
UNIVERSITY

Demo

https://localhost:3001

Voter Authentication

GHENT
UNIVERSITY

its
me

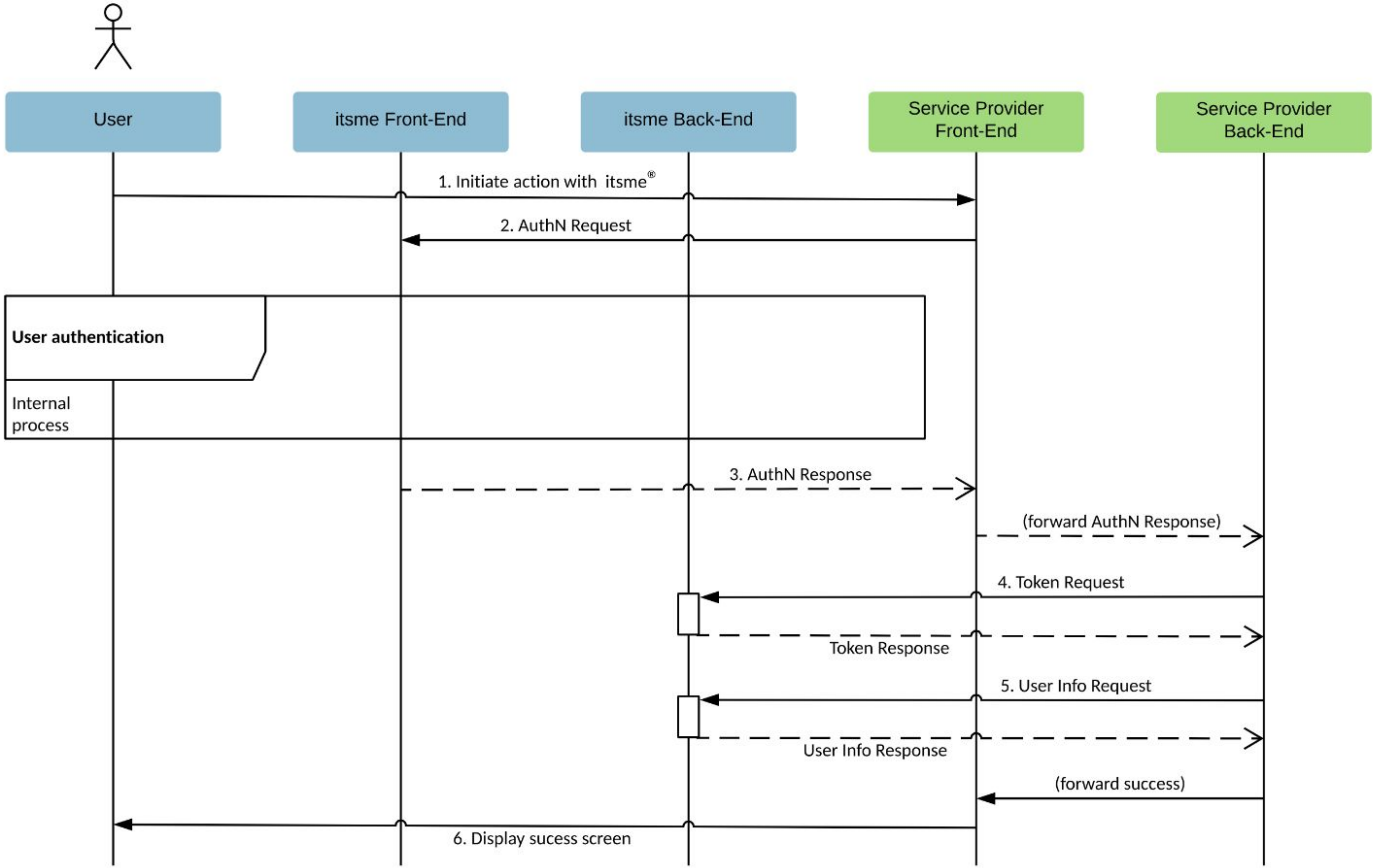
Why Itsme?

- Passwordless login (Social Engineering Attacks)

- HTTPS (TLS) -> OV or EV (no DV)

- Use of Asymmetric Encryption (Backend & itsme)

~~RSA-512~~ RSA-2048 ✓



GHENT UNIVERSITY

Limitations of itsme

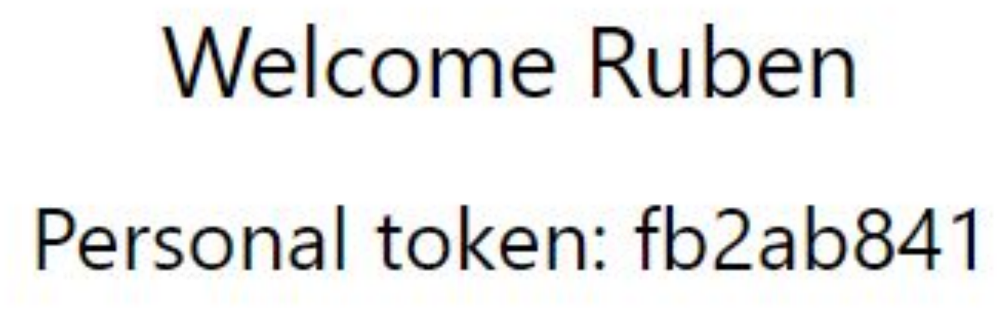
→ Limited to Belgian citizens

→ Accessibility

- Dependence on Smartphones
- Difficulty of Setup

Website Authentication & Non-repudiation

Website Authentication



Welcome Ruben

Personal token: fb2ab841

- Extension
  - Unique code per voter sent in invitation letter
  - Code shown after user authentication

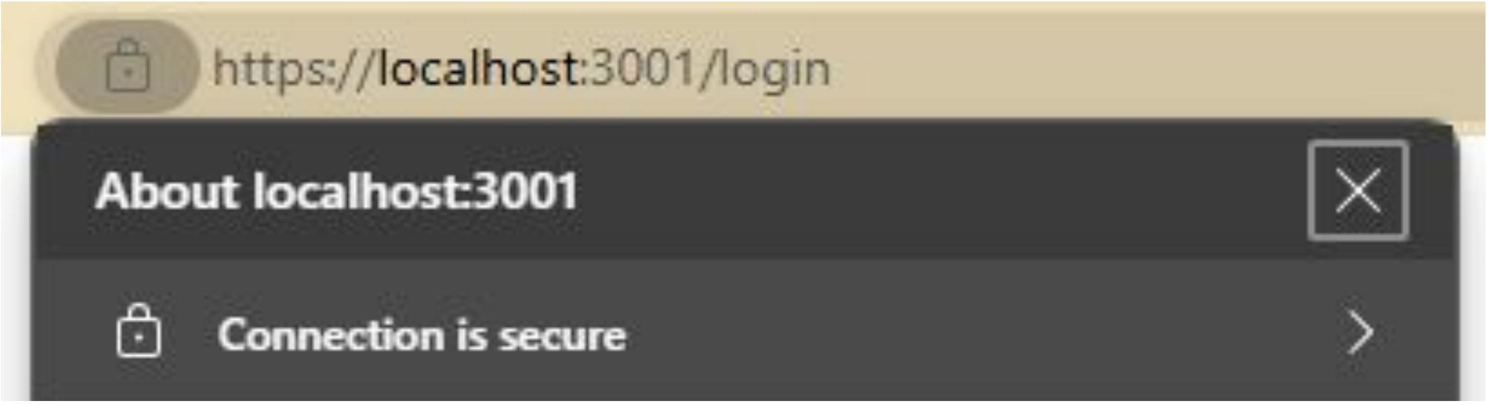
Non-Repudiation

- Compulsory voting
  - Voters need to be able to prove they voted
- Send Digitally Signed proof document to voters
  - Private / public key pair
  - (EC)DSA

Data Transmission

Data Transmission

- “Just use TLS”
- Authentication, Confidentiality, Integrity
- Added measure: constant-size messages
  - Prevents side-channel attack



https://localhost:3001/login

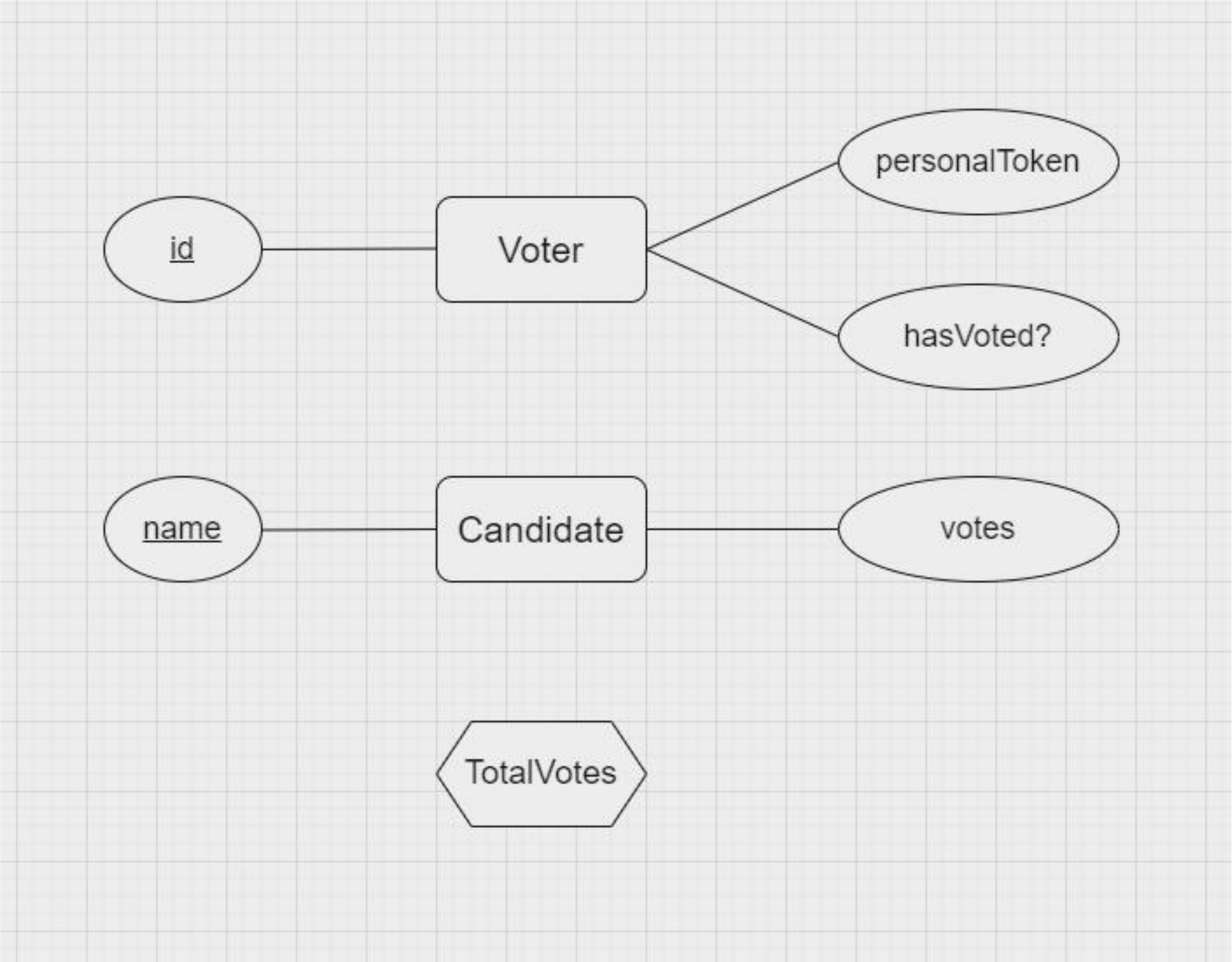
About localhost:3001

Connection is secure

GHENT UNIVERSITY

Data Storage

EER-diagram



GHENT
UNIVERSITY

PostgreSQL

- ACID / access control / TDE / TLS
- Anonymity
- WAL

Remaining Security Issues

Remaining Security Issues

- Stolen device with hacker knowing password
- Privacy during voting
- Physical interference with (central) counting server(s)
- Large scale DDoS attacks
- The problems coming with all of the used technologies