# Arquitecturas de SVE

Revisão da Literatura e Comparação

**Pedro Antunes**
paa@di.fc.ul.pt
www.di.fc.ul.pt/~paa

## Fujioka, Okamoto & Ohta

- Componentes
  - Voting - prepara, assina e envia boletins
  - Administrator - oculta votos e assina boletins
  - Counter - publicita boletins recebidos e conta votos depois de libertados pelo votante
  - Opening - liberta boletins no Counter

# Fujioka, Okamoto & Ohta

- Fases
  - Preparação - votante preenche boletim, assina e envia para Administrator
  - Validação - Administrator oculta voto e assina boletim, devolvendo-o ao votante
  - Votação - votante envia boletim duplamente assinado ao Counter
  - Contagem - Counter publicita boletins recebidos e pede verificação
  - Verificação - votante verifica e liberta boletim
  - Apresentação - Counter publicita contagem de votos

# EVOX

- Mesmos componentes do Fujioka
- Novos componentes
  - Election Comission - criação de boletins
  - Registrar - lista de votantes
  - Anonimizer – canal colocado entre Voting e Counter, para garantir anonimato do votante

# EVOX

- Novas fases
  - Pré votação - criação de boletins e listas de votantes

# Sensus

- Componentes
  - Registrar - registo dos votantes
  - Validator - verifica registo dos votantes
  - Pollster - interacção com votante, colecciona e entrega boletins
  - Tailler - conta votos e apresenta resultados

# REVS

- Componentes
  - Ballot Distributor - distribuição do boletim ao votante
  - Administrator - assina boletins
  - Anonymizer- garante anonimato do votante
  - Vote Engine - comunica boletins
  - Counter - verifica validade das assinaturas e conta votos

# Kofler, Krimmer & Prosser

- Componentes
  - Registration - registo dos votantes, anterior à votação
  - Trust Center - verifica direito de voto
  - Ballot Box - acumulação de votos

# Oasis

- Componentes
  - Candidates - listagem dos candidatos
  - Voters - registo dos votantes, anterior à votação
  - Voting - autenticação dos votantes, voto e confirmação
  - Results - contagem de votos
  - Audit - verificação de boletins e votos

# Cybervote

- Componentes
  - Client Repository - registo dos dispositivos de votação
  - Registration Server - registo dos votantes
  - Vote Server - recepção de boletins
  - Tabulation - contagem, verificação e apresentação de resultados
  - Audit and Validation - verificação do processo

# Resumo

| | Pré-registo | Registo | Validação | Anonimização | Votação | Contagem | Verificação |
|---|---|---|---|---|---|---|---|
| Fujioka | | | ★ | | ★ | ★ | ★ |
| EVOX | ★ | ★ | | | ★ | ★ | ★ |
| Sensus | | ★ | | | ★ | ★ | |
| REVS | | | ★ | ★ | ★ | ★ | |
| Kofler | | ★ | ★ | | ★ | | |
| Oasis | ★ | ★ | | | ★ | ★ | ★ |
| Cybervote | ★ | ★ | | | ★ | ★ | ★ |

# Verificação

| | Verificação |
|---|---|
| Fujioka | ★ |
| EVOX | ★ |
| Sensus | |
| REVS | |
| Kofler | |
| Oasis | ★ |
| Cybervote | ★ |

| | Verificação |
|---|---|
| Fujioka | confirmação pelos próprios |
| EVOX | confirmação pelos próprios |
| Sensus | |
| REVS | |
| Kofler | |
| Oasis | recontagem de votos |
| Cybervote | análise de logs |

# Discussão

- Verificação
  - Relativamente limitada no tempo e no modo
    - Confirmação pelos próprios (mas não por outros)
    - Recontagem de votos (por membros oficiais)
    - Análise de logs
  - Falta componente de auditoria ao sistema

# Auditoria ao sistema

- Misuse-cases
  - Ameaças ao funcionamento do sistema
  - Ameaças à segurança do sistema
- Tipos de misuse-cases
  - Comprometem fase de preparação e/ou registo
  - Comprometem fase de votação e/ou validação
  - Comprometem fase de contagem
  - Comprometem um componente
  - Comprometem a interligação entre componentes

# Como?

| | Funcionamento | Segurança |
|---|---|---|
| Preparação e registo | Controlo do registo dos dispositivos de votação | Marcar e verificar alterações aos registos durante a votação |
| Votação e validação | Verificar percursos dos boletins | Votos provisórios |
| Contagem | Replicação | |
| Componente | Simular uso do componente | Auditar logs |
| Interligação de componentes | Simular partes do processo de votação | Monitorizar percursos dos boletins |

# Auditoria ao sistema

| Fases | Preparação | Validação | Anonimização | Votação | Contagem | Verificação |
|---|---|---|---|---|---|---|
| Componentes | Registrar | Administrator | Anonymizer | Voting | Counter | Confirmation |
| Auditoria | Autenticidade do votante<br>Direito de voto<br>Singularidade | | Anonimato | Privacidade<br>Não coercibilidade | Integridade dos votos<br>Precisão | |