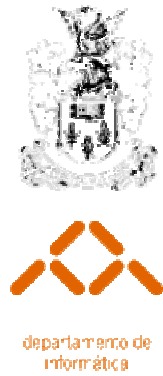
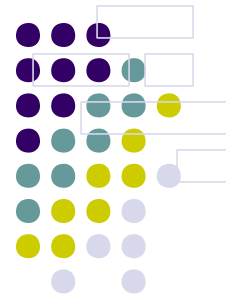


**Universidade do Minho**



## **Análise de um sistema comercial de votação electrónica**

**Filipe Campos**



# votação electrónica

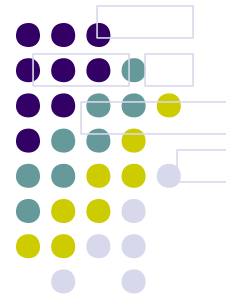
## Principais Vantagens

- Modernizar o sistema eleitoral.
  - reduzir os custos.
  - aumentar a eficiência.
  - Aumentar a segurança.
- Aumentar a conveniência para os eleitores.
  - Reduzir a abstenção.

## Problemas de implementação

### Ambientes de votação

- Votação num ambiente controlado
- Votação remota através de um maquina publica controlada
- Votação remota.



# votação electrónica

**Um sistema tem normalmente as seguintes fases:**

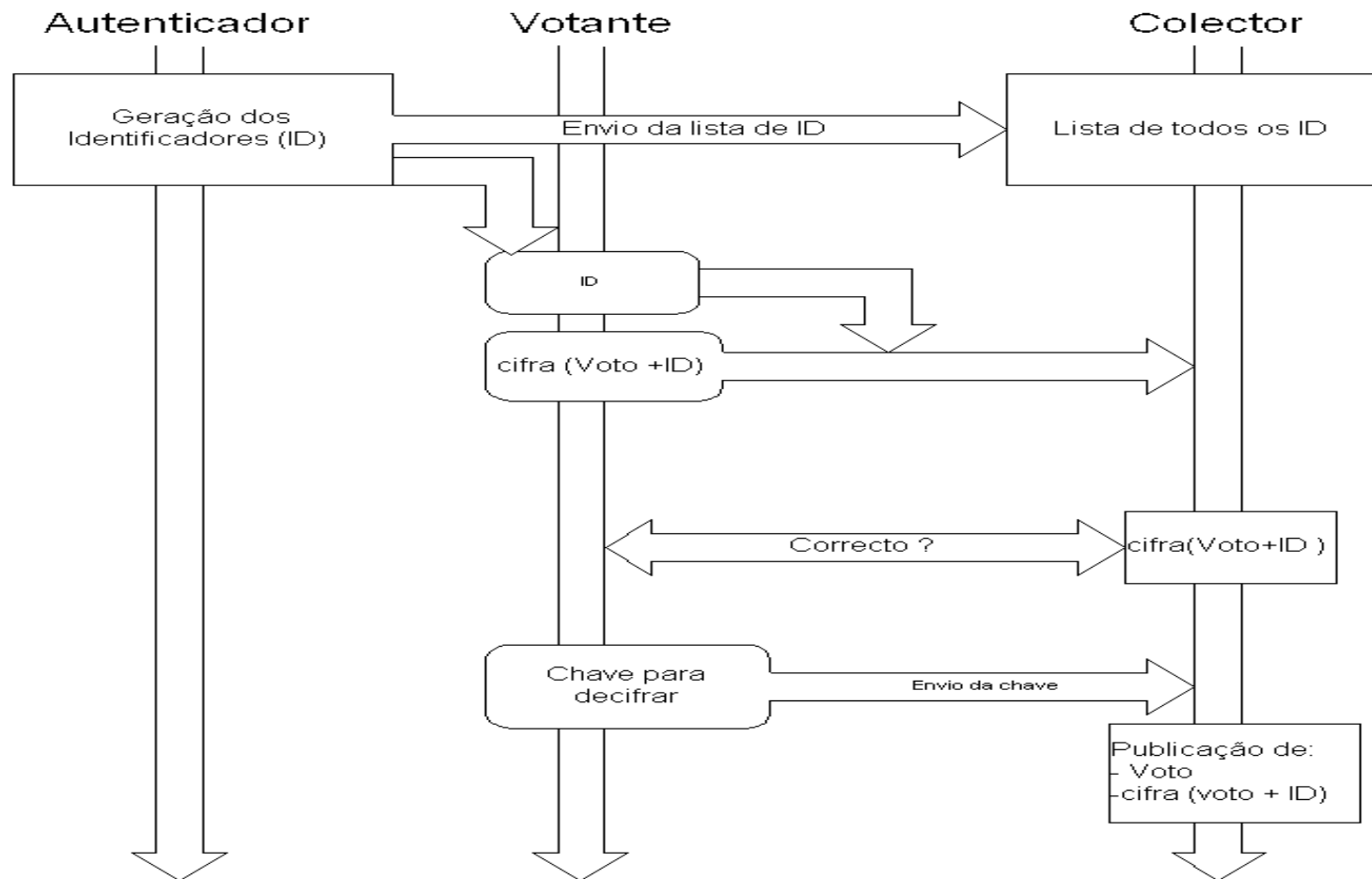
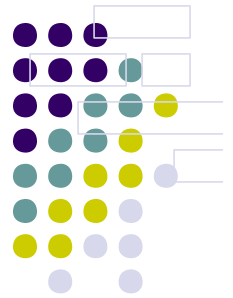
- Inicialização
- Votação
- Contagem
- Verificação
- Reclamação

## **Propriedades desejadas:**

- Exactidão
- Democracia
- Imparcialidade
- Verificação individual
- Verificação universal
- Privacidade
- Não coercibilidade

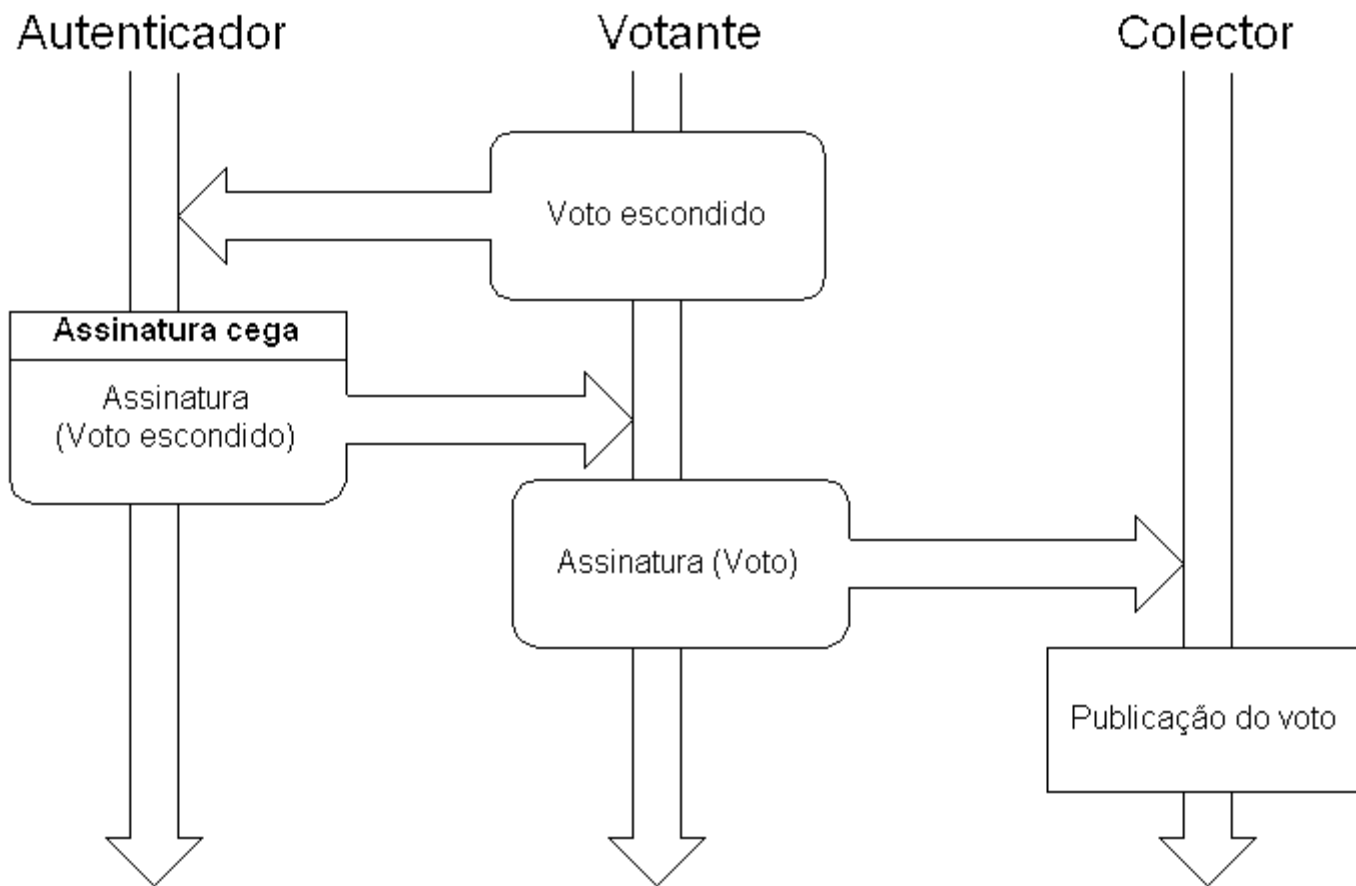
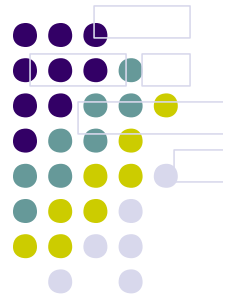
# Votação electrónica

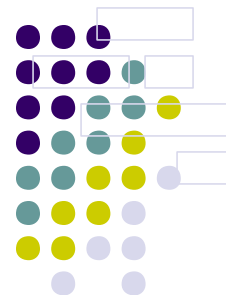
## (Protocolos de duas autoridades)



# Votação electrónica

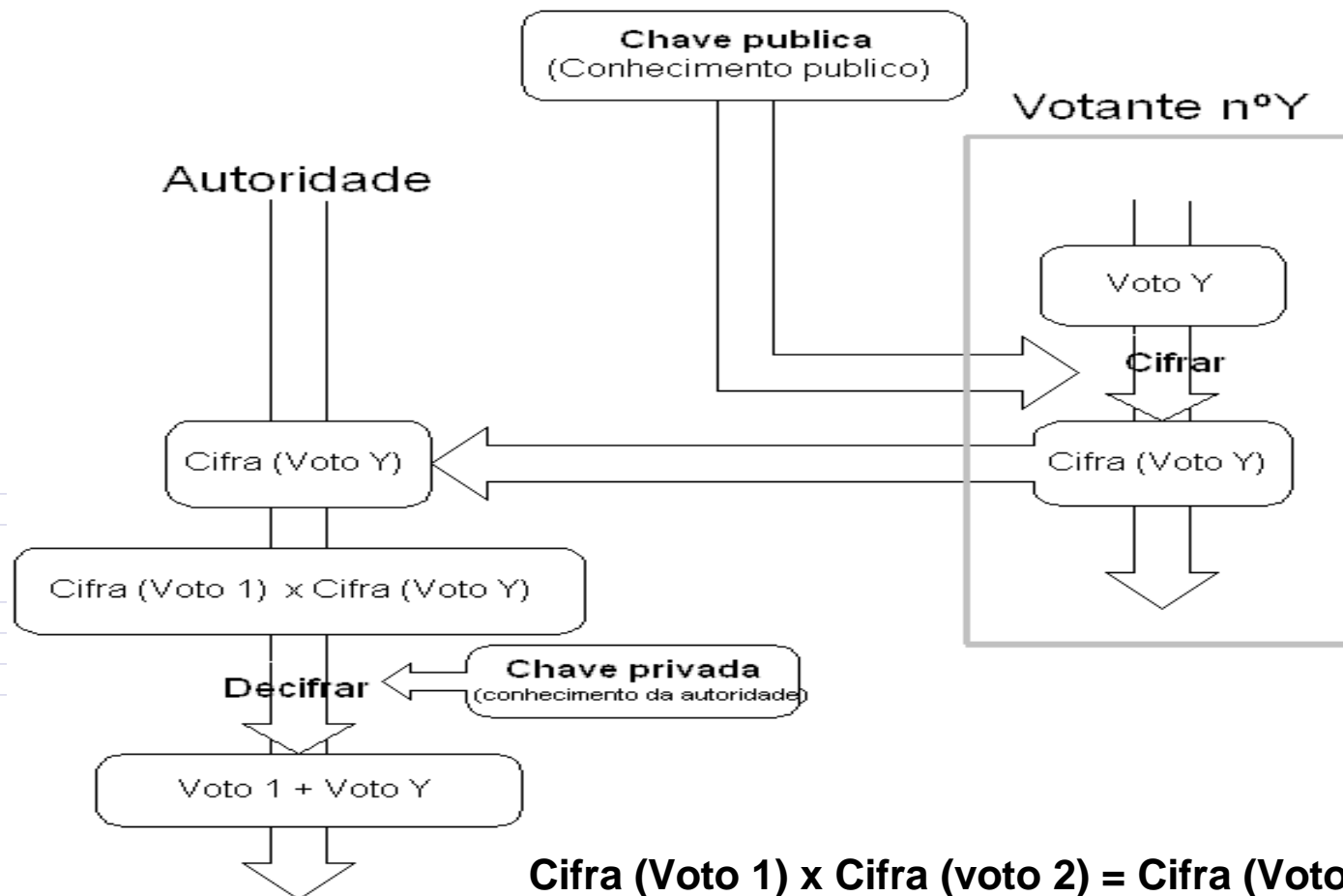
(Protocolos baseados em assinaturas cegas)





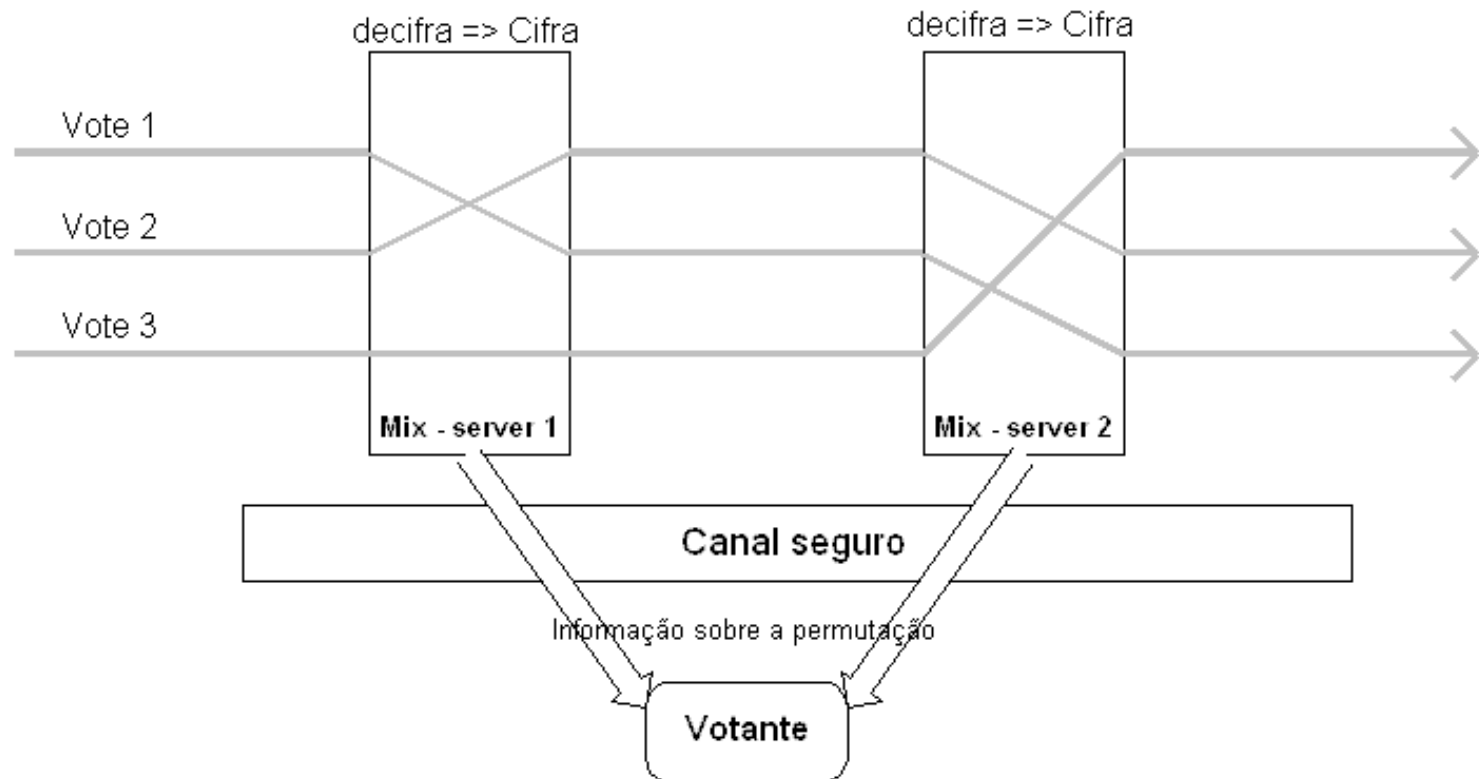
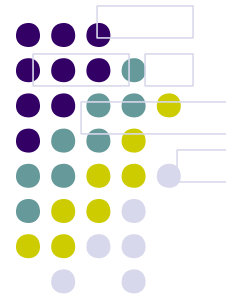
# Votação electrónica

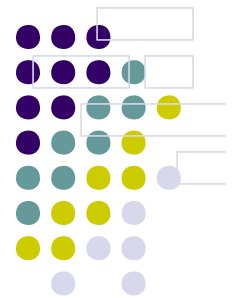
(Protocolos baseados em cifra *homomorphic*)



# Votação electrónica

(Protocolos baseados em canais anónimos)



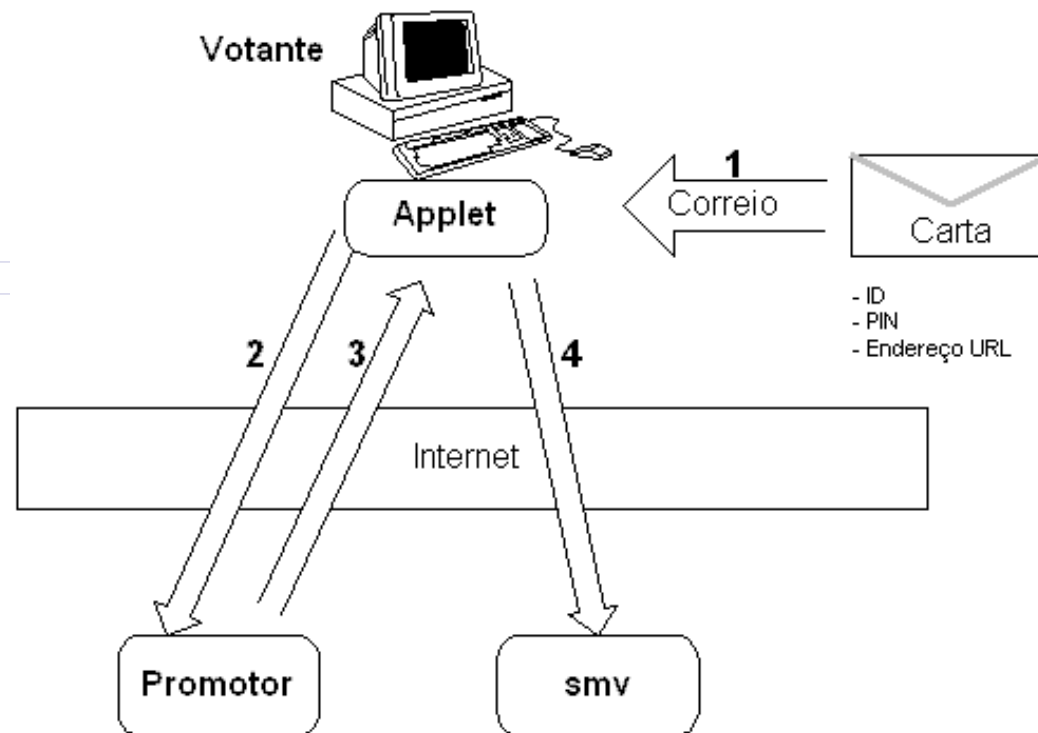


## SMV

Este sistema é constituído por duas autoridades:

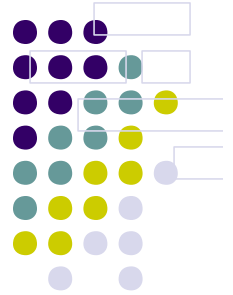
- **smv**: Tem a função de validar dos votos e os coleccionar
- **Promotor**: verifica a validade dos votantes.

Para o votante, a votação é realizada da seguinte forma:





# SMV - Fases de votação (Inicialização)



- Definido um janela temporal de votação em que a eleição vai decorrer
- São definidos os boletins e possíveis respostas.
- É feito uma lista do votantes validos.
- Para cada votante é criado um identificador (ID) e um PIN único.
- Cada votante vai receber em casa uma carta com um endereço Internet e as suas credenciais (ID e respectivo PIN).

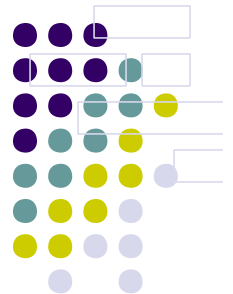
## Inicialização do promotor:

- É criado uma base de dados com todos os ID's dos votantes e respectivas datas de nascimento.
- Um par de chaves criptográficas.
- Um certificado com uma chave publica.

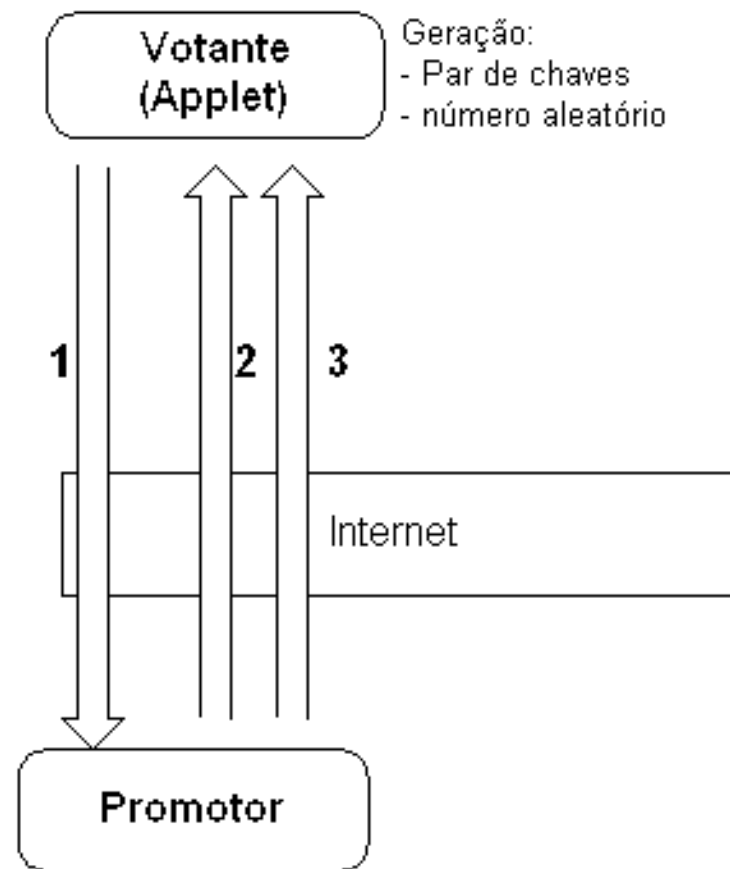
## Inicialização do smv:

- É criado uma base de dados com todos os ID's dos votantes e respectivos valor hash do PIN.
- Um par de chaves criptográficas.
- Um certificado com uma chave publica.

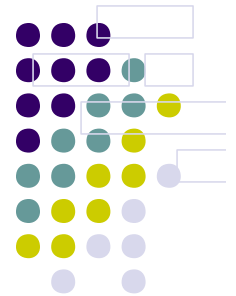
## SMV - Fases de votação (Registo)



- 1 O votante envia: Chave publica do votante, o seu ID e data de nascimento
- 2 O promotor envia: Um token assinado por ele. O token vai conter um identificador para um boletim de voto, um identificador interno do votante (pseudónimo), uma janela temporal de votação e a chave pública do votante.
- 3 O promotor envia: informação do boletim.



# SMV - Fases de votação (Votação)

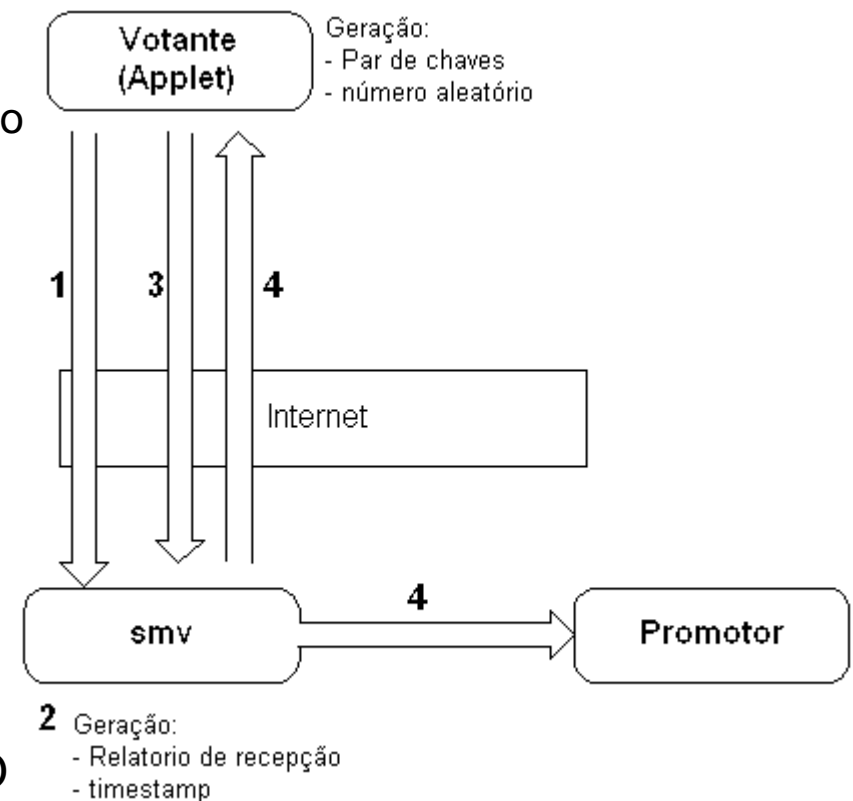


- 1 O votante envia:
  - o seu voto e o numero aleatório; cifrado com a chave publica do promotor e assinado com a chave privada do votante.
  - Hash do PIN e o token.

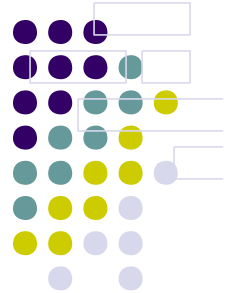
2 O promotor verifica se esta tudo correcto. O promotor envia: informação do boletim. o smv gera um relatório de recepção e um respectivo comprovativo temporal (timestamp).

3 O votante confirma o seu voto.

4 Caso afirmativo; o relatório e o timestamp são enviado ao votante. O smv envia uma mensagem ao promotor a indicar que o votante já votou.



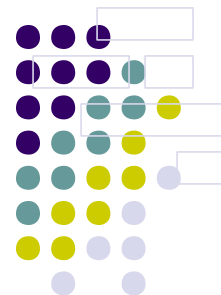
## SMV - Fases de votação (Contagem)



**Nesta fase é feito a contagem final da votação.**

- O promotor recebe um meio físico de armazenamento de dados (exemplo CD) com a lista de todos os votos cifrados com a chave pública do promotor e assinado com a chave privada do smv. Para cada voto a assinatura do votante foi substituída pela do smv.
- O promotor também recebe uma segunda lista com todos os token's válidos recebidos pelo smv.
- A geração destas duas listas é da responsabilidade do smv.
- A chave privada do promotor é usada para decifrar todos os votos.
- O promotor publica a contagem final.

# SMV - Fases de votação (Verificação e Reclamação)



## Verificação:

O promotor tem a lista de todos os token's validos, e o smv tem todos os votos cifrados e a lista dos token's validos recebidos durante a votação.

A verificação pode ser efectuada da seguinte forma:

- A duas listas de token's tem que ser iguais.
- Duas auditorias independentes têm de ser realizadas; Uma ao promotor e outra ao smv. As duas auditorias permite detectar se ocorreu alguma fraude, mas é necessário que assumir que pelo menos uma das autoridades não é corrupta.

## Reclamação:

- O votante pode usar o relatório de recepção e o timestamp retornado na fase de votação para provar que o seu voto foi erradamente excluído na contagem, e que participou na eleição.

# SMV

## (Propriedades obtidas)



**Exactidão:** Não possível alterar um voto. Não permitir um voto valido ser eliminado na fase de contagem. Não permitir um voto invalido ser cotado na fase de contagem.

**Democracia:** Só votantes validos podem votar. Cada votante pode votar só uma vez.

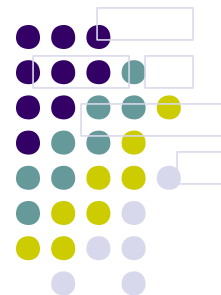
**Imparcialidade:** Nenhuma entidade pode obter conhecimento sobre o resultado (parcial) da votação antes da contagem final. Este conhecimento poderia afectar o voto de quem ainda não votou.

**Verificação individual:** Cada votante pode verificar se o seu voto foi cotado correctamente.

**Verificação universal:** Qualquer entidade pode verificar que todos os votos foram contados correctamente.

**Privacidade:** Nenhuma entidade pode efectuar uma ligação entre o votante e o seu voto.

**Não coercibilidade:** O votante não pode convencer um observador é quem votou. Isto propriedade evita a compra de votos.



## Conclusão

O SMV é um sistema que pode ser usado em diversos tipo de votação e que não usa nenhuma restrição física.

A maior parte dos problemas de segurança são resolvidos, mas é necessário considerar que:

- O smv e promotor não podem conspirar (serem desonestas ao mesmo tempo)
- Depois da eleição, é necessário efectuar duas honestas e separadas audições, uma ao smv e outra ao promotor.