INSTITUTO SUPERIOR DE CIÊNCIAS DO TRABALHO E DA EMPRESA

Departamento de Ciências e Tecnologias de Informação

VOTO ELECTRÓNICO:

ESTUDO DA UTILIZAÇÃO DO EML NO CASO PORTUGUÊS

Paulo Jorge Tavares Bastos

Tese submetida como requisito parcial para obtenção do grau de Mestre em Engenharia Informática e de Telecomunicações

Orientador:

Prof. Doutor Carlos J Costa

Janeiro, 2008

(esta página foi deixada em branco propositadamente)

Resumo

A *Election Markup Language* (EML) é uma linguagem de comunicação para ser utilizada entre os diversos subsistemas que constituem o Sistema de Votação Electrónica (SVE).

Esta dissertação tem como objectivo contribuir para o estudo do Voto Electrónico em Portugal, analisando a lei do processo eleitoral e utilizando as recomendações do Conselho da Europa sobre a adopção do EML, propõe-se apresentar uma arquitectura de SVE que possa ser utilizado para as eleições e referendos.

Palavras-chave: Voto Electrónico, EML, Votação Remota, *Web Services*

Abstract

Election Markup Language (EML) is a communication language to be used between the diverse subsystems that compose the Electronic Voting System (EVS).

This thesis has the objective to contribute for the study of the Electronic Vote in Portugal. Analyzing the voting process law and using the recommendations of the Council of the Europe about the adoption of the EML, and porpoise system's architecture for EVS that can be used for elections and referenda.

Keywords: Electronic Vote, EML, Remote Voting, Web Services

Índice

Índice de Figuras

Índice de Tabelas

(esta página foi deixada em branco propositadamente)

1 Introdução

A votação é a fase crucial [OASIS, 2007] e fulcral das democracias, o conceito de democracia não existe se não houver o acto de votar. É através desse acto que os eleitores demonstram a confiança [Internet Policy Institute, 2001] nos governantes, nas suas políticas e que se faz a transferência de poder.

Nas democracias actuais, estudos [Internet Policy Institute, 2001] argumentam que os métodos tradicionais de votação não encorajam a participação dos eleitores, por implicações de tempo, localização e acessibilidade.

Para combater essas tendências, um pouco por todo o mundo efectuam-se estudos e projectos-piloto de voto electrónico. Faz parte de um conjunto de medidas do chamado *e-governament*, a pôr em prática pelos governos nacionais para modernizar os processos governamentais.

A adopção de Sistema de Votação Electrónica (SVE) acaba por ser uma oportunidade para modernizar todo o processo eleitoral, desde a manutenção dos cadernos eleitorais actualizados, permitir a mobilidade dos eleitores e, claro, conseguir um aumento da rapidez no apuramento dos resultados.

O SVE também pode contribuir para diminuir os níveis de abstenção [Houston, et al., 2005] e aumentar a participação dos eleitores, uma vez que, corrige os inconvenientes da deslocação aos tradicionais locais de voto. O aumento da participação dos eleitores trará mais legitimidade ao processo eleitoral e poderá contribuir para aumentar o interesse na política. O SVE poderá ser o elemento chave para ajudar a reverter as tendências de apatia perante a governação que caracterizam as actuais democracias.

A adopção de um SVE é sempre um processo complexo, que envolve muito mais do que tecnologia. Para garantir que são compridos os direitos fundamentais (CM(2005)56) [Council of Europe - Ministers' Deputies, 2005] (Rec(2004)11) [Council of Europe - Committee of Ministers, 2004] dos cidadãos: segurança, privacidade, anonimato, que as eleições são livres, válidas e justas, e que o SVE consegue a confiança dos eleitores.

Para isso, mesmo existindo auditorias durante o desenvolvimento/implementação do SVE e durante o acto eleitoral, o SVE deve ser desenvolvido de acordo com *standards* públicos [European Communities, 2004] de modelos e de código aberto, e deverá estar disponível publicamente [Schneier, 2004] para análise e estudo pelos cidadãos interessados.

O Conselho da Europa recomenda a utilização de *standards* abertos [European Communities, 2004] na elaboração de SVE. Um desses *standards* recomendados para adopção é o EML [Cover, 2004] nas normas para a elaboração de SVE nacionais. O EML [OASIS, 2007] [Aas, 2005] [Mertz, 2004] é uma linguagem de comunicação *standard* para as comunicações entre os subsistemas que constituem o SVE. Por ser um *standard*, o SVE pode perfeitamente ser dividido em diversos subsistemas, desenvolvidos por diferentes entidades e mesmo assim possuir uma total integração nas comunicações e troca de dados.

O objectivo [OASIS, 2007] [Aas, 2005] do EML é não entregar todo o sistema eleitoral a apenas uma organização, deve-se subdividi-lo em diversos subsistemas independentes que através de um conjunto de interfaces claros fazem uma integração transparente através de um conjunto de regras e objectos definidos no EML.

O EML parte de um princípio [Aas, 2005] democrático, não existe uma dependência a uma só companhia, permite que facilmente se possa mudar um subsistema, mantendo toda a estrutura em funcionamento.

1.1 Objectivos

No trabalho de investigação desta dissertação pretende-se conseguir alcançar os seguintes objectivos:

- Adaptação do *standard* EML a uma situação concreta;
- Desenho de um sistema distribuído de apoio à votação que utilize EML;
- Desenvolvimento do sistema proposto;
- Utilização do sistema num cenário concreto e respectiva avaliação.

1.2 Motivação / Utilidade

O contributo desta dissertação no estudo do voto electrónico (*e-voto*) em Portugal é a proposta de um sistema de votação remoto distribuído, que cumpra as recomendações do Concelho da Europa [Cover, 2004] sobre a utilização de *standards* como o EML e que possa ser utilizado nas mais diversas aplicações, como por exemplo, eleições nacionais, referendos e votações públicas ou privadas.

1.3 Estrutura da Dissertação

No **capítulo 2** são analisados os problemas e requisitos dos SVE em geral através uma revisão de a literatura e do estudo de alguns casos onde já se implementaram SVE.

No **capítulo 3** é feito um estudo do sistema de votação português, através de uma análise da legislação Portuguesa e da criação de diagramas UML de alguns processos do sistema eleitoral.

No **capítulo 4** é feita uma abordagem aos conceitos tecnológicos utilizados para a elaboração da proposta.

No **capítulo 5** são apresentados uma arquitectura e um protótipo baseados no estudo do EML e das conclusões da revisão da literatura.

No **capítulo 6** é exposta uma avaliação do sistema proposto no capítulo anterior.

No **capítulo 7** é apresentada a conclusão e as propostas de trabalho futuro.

2 Sistemas de Votação Electrónicos

2.1 Introdução

Designa-se por SVE [UMIC, 2005] "*um sistema de votação que utilize meios electrónicos nas fases de votação ou contagem dos resultados de determinado acto eleitoral ou referendário. Os votos podem ser recolhidos através de interfaces mecânicos, ópticos ou electrónicos. O sistema poderá também transmitir os resultados da votação para uma unidade central de apuramento através de redes de telecomunicações*".

Esta definição de SVE considera que o SVE abrange as fases de votação e contagem dos votos, no entanto o conceito de SVE pode considerar todas as operações essenciais para a realização de eleições, desde o recenseamento, passando pela fase de votação propriamente dia, a contagem e transmissão dos resultados, bem como a sua publicação e divulgação. Isto indica que é possível conceber um SVE totalmente electrónico, apesar do que na prática isso ainda não existir. O que existe em vários países são sistemas parcialmente electrónicos, em que se mantém o carácter de processamento tradicional de algumas operações juntamente com a utilização de meios electrónicos para a realização de outras. Em geral os SVE empregam meios electrónicos apenas na fase de votar ou na recolha e/ou contagem e/ou apuramento dos votos.

Neste capítulo é feita uma abordagem aos SVE numa vertente concepcional e casos práticos de projectos ou SVE utilizados em algumas regiões do mundo. Para realizar esse estudo divide-se em dois grandes tópicos:

- **Conceito dos Sistemas de Votação Electrónicos**: estudo dos aspectos teóricos na concepção dos SVE, tais como, as propriedades dos SVE, tipos e

arquitecturas, princípios e salvaguardas, problemas, requisitos e as fases do processo de votação;

- **Casos de Estudos**: análise de três casos práticos de projectos-piloto ou de SVE já implementados noutros países, de arquitecturas distintas.

2.2 Propriedades dos SVE

Um SVE deve transpor as mesmas características e funcionalidades para o meio electrónico que o sistema de votação tradicional oferece. Um SVE deve ter as seguintes propriedades [Cranor, et al., 1997]:

1. **Exactidão**

   Um SVE é exacto quando:
   - Não é possível alterar um voto válido;
   - Não permite um voto válido ser eliminado na fase de contagem;
   - Não permite um voto inválido ser contado nos resultados.
2. **Democracia**

   Um SVE é democrático quando:
   - Só votantes válidos podem votar;
   - Cada votante pode votar só uma vez.
3. **Privacidade**

   Um SVE é privado quando:
   - Nenhuma autoridade de voto, nem ninguém, consegue estabelecer ligação entre um boletim de voto e o eleitor que nele exerceu o seu direito de voto;
   - Ninguém pode provar que votou de uma determinada maneira.
4. **Verificável**

   Um SVE é verificável quando:
   - **Verificação individual:** Cada votante pode verificar se o seu voto foi contado correctamente;
   - **Verificação universal:** Qualquer entidade pode verificar que todos os votos foram contados correctamente.

5. **Conveniência**

   Um SVE é conveniente quando:

   - O votante puder exercer o seu direito de voto rapidamente numa só sessão com o mínimo de equipamento e competências.

6. **Flexibilidade**

   Um SVE é flexível quando:

   - Se não restringe o formato dos boletins de voto.

7. **Mobilidade**

   Um SVE é móvel quando:

   - Não impõe restrições de natureza logística ao local onde cada eleitor pode exercer o seu direito de voto.

2.3 Fases do Processo de Votação

Um SVE tem várias fases [Gritzalis, 2002] durante todo o processo eleitoral. Na Tabela 1 estão descritas as principais operações de cada uma dessas fases e os principais problemas (no capítulo 2.5 serão estudados esses problemas) associados. Por uma questão de organização decompõe-se as fases de acordo com a sua ocorrência temporal perante o acto de votar propriamente dito.

Tabela 1 – Fases da Votação

Ocorrência	**Fase**	**Operações**	**Problemas**
Antes	Preparação	Definir os Eleitores; Definir os Candidatos; Criar os Boletins de Voto; Criar os meios para a autenticação.	Erros na preparação das eleições; Erros no registo de votantes: falsificação e anulação de eleitores; Confidencialidade.

Durante	Autenticação	Colocar as credenciais de acesso	Confidencialidade
	Votação	Escolha do candidato	Erros na votação
	Recolha do Voto	Selar o Voto; Garantir a confidencialidade do voto.	Integridade: alteração do voto válido
Após	Contagem	Validar os votos	Fuga de resultados parciais; Alteração de votos.
	Verificação	Verificar a integridade dos Votos; Consolidar os Votos.	Confidencialidade

2.4 Arquitecturas de SVE

Existem duas grandes arquitecturas distintas no voto electrónico [Svensson, et al., 2003] [The Risk of e-Voting, 2004], a primeira e a mais implementada é a arquitectura *Direct Recording Electronic Voting System* (DRE) [Dill, et al.] e a segunda é o Voto Remoto (voto usando a *Internet*, ou voto pela *Web*) [Safevote Inc., 2006] que ainda é pouco implementada.

2.4.1 Direct Recording Electronic

Os DRE são sistemas electrónicos colocados em locais específicos, normalmente nos mesmos locais onde decorrem o método tradicional de votação, como escolas e juntas de freguesia. Tal como acontece no sistema tradicional de votação, nesses locais existem oficiais destacados pela comissão de eleições para monitorizar e garantir que

são cumpridos os requisitos de segurança e confidencialidade do processo de votação, bem como prevenir actos de fraude e vandalismo que possam de alguma forma comprometer a integridade do processo.

Os sistemas de votação DRE consistem [Dieterich, 2004] num computador com um monitor *touch-screen* ou um outro dispositivo de *input,* um dispositivo de memória permanente, software e, em alguns casos, uma impressora para o comprovativo do voto. O software é constituído por: (i) o sistema operativo que suporta o sistema de votação e que faz o controlo directo do monitor, da memoria e dos outros dispositivos que constituem o computador; (ii) o sistema de votação, propriamente dito, é executado como uma aplicação no sistema operativo e gere o interface do votante, processa os votos, controla os erros do votante (votos nulos, duplicação de votos, votar em mais do que um candidato).

Existem vários fabricantes (i.e. *Sequoia Voting Systens, Diebold Election Systems, ES&S, Nedap*) mas os princípios básicos de funcionamento são comuns. Para além do computador com o sistema operativo e software de votação, existe um dispositivo de *input* para o interface com o votante, como um monitor *touch-screen* ou um teclado com um conjunto de botões. Os sistemas DRE também contêm um mecanismo para transmitir os votos e/ou resultados totais da votação para um sistema central. O funcionamento destes sistemas é em geral *off-line*, desligado de qualquer rede e apenas no final do exercício eleitoral é que poderá estabelecer uma ligação *vpn*[1] (ou *pptp* e *vpn*) para fazer a comunicação dos resultados para um ponto central de processamento.

Alguns autores [Mercuri, 2007] [Kitcat, 2006] recomendam a utilização de sistemas DRE que possam ser auditáveis, e que possa criar um comprovativo físico (em papel) do voto. Através da utilização de uma impressora ou um *scanner* óptico para os boletins electrónicos. Que em caso de dúvidas perante os resultados pode-se recorrer aos métodos tradicionais de contagem dos votos.

[1] Do inglês *Virtual Private Network* - Rede privada virtual

2.4.2 Voto Remoto

Os Sistemas Remotos de Votação Electrónica, também designados por "*voto electrónico não presencial*" ou "*voto electrónico à distância*", surgem naturalmente da evolução e da banalização do acesso à Internet e da evolução das tecnologias de informação e comunicação, principalmente no campo da segurança (certificados digitais, leitores de cartões, algoritmos de cifras forte).

Estes sistemas funcionam ligados à rede pública, utilizando o canal já existente: – a Internet. Normalmente recorrem à utilização de um simples *Web browser*[2], disponível em todos os dispositivos com acesso à Internet, ou de *Java applets*[3]. A principal característica desta arquitectura é a mobilidade, permite que o votante no conforto da sua casa ou num outro local onde exista um ponto de acesso à rede Internet ou através da utilização de um dispositivo móvel, como um telemóvel ou PDA, possa exercer o direito de voto.

Estes tipos de sistemas de votação são muito mais cómodos e resolvem o problema da mobilidade, principalmente para votantes com dificuldades de motricidade ou com necessidades especiais. Por outro lado, estão mais expostos, tanto a nível de segurança do sistema, como outros aspectos para além do factor segurança [Rubin, 2001] como a coação, venda do voto, solicitação do voto, que tornam-se mais difíceis de gerir pela facto do voto não ser realizado num ambiente controlado.

As experiências com sistemas de votação não presenciais estão a surgir como forma de permitir uma maior comodidade no acto de votar, procurando atacar o problema da abstenção ao tornar o sufrágio mais apelativo e apetecível, principalmente para os mais jovens que habitualmente já são utilizadores de sistemas *Web*.

Estes sistemas de voto à distância foram utilizados pela primeira vez a nível nacional na Estónia [Maaten, 2006] [The National Election Committee, 2005], a 16 de Outubro de 2005, por cerca de 10.000 pessoas, correspondendo a 1% dos votantes.

---

[2] Programa que permite a navegação em documentos HTML, como o Mozilla, Opera, Safari, Internet Explorer.

[3] Aplicações desenvolvidas na linguagem de programação Java que são executados a partir de um *Web browser*.

2.4.3 Comparação das arquitecturas

Na Tabela 2 apresenta-se as principais vantagens e desvantagens que caracterizam as duas principais arquitecturas dos SVE.

Tabela 2 - Quadro comparativo das vantagens e desvantagens dos tipos de SVE

	Vantagens	**Desvantagens**
DRE	Segurança; Acessibilidade; Funcionamento *off-line* e/ou em rede privada virtual (*vpn*); Rapidez no apuramento dos resultados;	Obrigam a deslocação das votantes; Não resolve o problema da mobilidade e da abstenção; Custo da infra-estrutura; Sistemas fechados ("caixa preta");
Votação Remota	Comodidade: Voto a qualquer hora em qualquer lugar; Centralizado: Rapidez na contagem dos votos; Barato: utiliza os canais e sistemas já existentes; Mobilidade dos votantes; Período de voto alargado.	Facilidade de vender o voto; Coação e solicitação do voto; Problemas nas comunicações; Ataques informáticos; Infoexclusão.

Na tabela seguinte,

Tabela 3, apresenta-se as principais características que os SVE devem responder e as funcionalidades que duas arquitecturas apresentam, baseado nas propriedades [Cranor, et al., 1997] apresentadas em 2.2 e no estudo das duas arquitecturas apresentado em 0.

Tabela 3 – Quadro de resumo das arquitecturas dos tipos de SVE

	DRE	**Remoto**
Privacidade	Maior privacidade	Risco acrescido
Verificável	Possibilidade do uso de comprovativos em papel de voto	
Conveniência	Obrigam a deslocação do votante	Voto a qualquer hora em qualquer lugar
Mobilidade	Não resolve o problema da mobilidade e da abstenção	Facilidade de votação
Custo	Custo mais elevado	Mais económico Utiliza canais já existentes
Segurança	Mais seguro Funcionamento *off-line*	Sujeito a maiores riscos e ataques informáticos

2.5 Recomendações do Concelho da Europa

O Concelho da Europa apresenta um conjunto de recomendações [Council of Europe - Committee of Ministers, 2004] sobre a adopção dos SVE. Em termos gerais recomendam que:

- Voto electrónico deve respeitar todos os princípios das eleições democráticas e deverá ser tão de confiança e seguro como as eleições que não usam meios electrónicos;
- A Interconexão entre os aspectos legais, operacionais e técnicos do voto electrónico deve ser levada em conta quando aplicadas as Recomendações do Concelho da Europa;

- Enquanto não for requerido para mudar os processos de eleição, os Estados Membros devem considerar rever a sua legislação à luz das Recomendações;
- Os Estados Membros devem manter sobre revisão as suas políticas e experiência sobre o voto electrónico. E reportar ao secretário do Concelho da Europa.

2.5.1 Avaliação

Os standards legais, técnicos e operacionais das Recomendações do Concelho da Europa compreendem 113 medidas de avaliação [Commission on Electronic Voting, 2006]. As medidas caracterizam-se por:

- Standards Legais (35 medidas)
    - Princípios (sufrágio universal, igual, livre, secreto)
    - Protecções processuais (transparência, verificável, responsabilidade, confiável, segurança)
- Standards Operacionais (25 medidas)
    - Notificação
    - Votantes
    - Candidatos
    - Votação
    - Resultados
    - Auditar
- Standards técnicos (53 medidas)
    - Gerais
    - Acessibilidade
    - Interoperabilidade
    - Sistemas
    - Segurança (geral, pré-votação, votação, pós-votação)
    - Auditar (geral, gravar, monitorizar, verificar, outros)
    - Certificação

2.6 Riscos e problemas de segurança

Os SVE estão expostos a diversos problemas técnicos e humanos, se os SVE têm potencial para muitos benefícios, também trazem muitos riscos [Shamos, 2004].

Estes sistemas, também apresentam novas questões: Como garantir a segurança e segredo do voto nesse novo ambiente? Como garantir que o *e-voto* está acessível para todos?

As máquinas de voto são "caixas pretas", cujo funcionamento é obscuro para o público e o *feedback* para o votante é também gerado pela máquina. Quer se encontrem, ou não, a funcionar correctamente, isso não pode ser independentemente verificado. Para resolver estes problemas, algumas empresas permitem o acesso ao código fonte [Hall, 2006]. Por outro lado, nenhuma quantidade de código auditado pode detectar *software* malicioso ou erros no *software*.

A indústria dos sistemas DRE é dominada por um número pequeno de empresas [Shamos, 2004], alguns dos quadros executivos dessas empresas são militantes de alguns partidos americanos. Um executivo pode ordenar aos programadores para adicionar código a cada máquina, desenvolvida pela empresa, para mover os votos para o candidato desejado, o que pode determinar uma viragem nos resultados eleitorais.

Nas duas arquitecturas ou tipos de SVE (DRE e Remoto) existem riscos e problemas mais ou menos visíveis. A maioria dos problemas identificados nos sistemas DRE, podem ser amplificados na votação pela Internet [Svensson, et al., 2003]. De um modo geral todas as arquitecturas de SVE apresentam problemas como:

- Falta de confiança no SVE;
- Falta de transparência do sistema ("caixa preta");
- Fraude e erros humanos;
- Sabotagem;
- Falhas no sistema operativo, software intermédio (*Web browser*, *applets*, …) e no próprio SVE.

2.6.1 Votação Remota

Os sistemas de votação remotos são caracterizados pelo votante aceder remotamente ao SVE e pelo acto de votar ser realizado num ambiente não controlado. De modo geral a votação remota apresenta os seguintes riscos [Stephen, 2004]:

- Uso da Internet como meio de comunicação;
- Falta de fidedignidade das aplicações instaladas no computador ou nos noutros dispositivos (PDA, *WebTV*, *smartphone*) de acesso do votante – como vírus, *spyware*, *trojan horse*;
- Falhas no lado do servidor – vulnerabilidades no próprio SVE ou em outros serviços (i.e. no servidor *Web* que suporta o SVE) ou mesmo no Sistema Operativo;
- Possibilidade da coercibilidade: tanto física como com recurso a meios electrónicos, i.e. *pop-ups* com publicidade;
- Colisão entre a confirmação do voto, a privacidade e a possibilidade de venda de votos;
- Tolerância a falhas do próprio sistema;
- Infoexclusão.

A nível de ataques informáticos, estes tipos de sistemas estão expostos a três tipos de ataques fundamentais [Stephen, 2004]:

- **Acesso não autorizado**: utilizando informação de autenticação de um utilizador (nome de utilizador e palavra chave);
- **Ataques por imitação**: fazer passar um utilizador ou sistema por outro (*spoofing* ou *reply attacks*);
- **Negação do serviço** (DoS[4] ou DDoS[5]): impedir o funcionamento de um sistema com interrupção dos serviços disponibilizados. Este tipo de ataques é

[4] Denial of Service

[5] Distributed Denial of Service

conseguido através de muitos pedidos aos servidores que causam sobrecarga, fazendo com que fiquem impedidos de processar os pedidos normais.

2.6.2 Acessibilidade

Os SVE podem fornecer consideráveis mais-valias para os cidadãos com necessidades especiais face aos métodos tradicionais de votação. Nos casos dos sistemas baseados na arquitectura DRE poderão ser utilizados mecanismo como sintetizadores. Nos sistemas de voto remoto, ao utilizarem o canal Internet e não obrigarem à deslocação das pessoas, permitem chegar a mais pessoas, principalmente aos votantes com limitações de mobilidade. Por outro lado, pode-se diversificar o acesso e utilizar diversas plataformas:

- HTTP;
- WebTV (*set top box*);
- PDA/SmartPhone

No entanto, toda esta oferta tecnológica ainda não está presente em todo o lado e há aqueles que por razões socioeconómicas não possuem computador ou acesso à Internet. Para esses casos é necessário haver as seguintes preocupações de acessibilidade no desenvolvimento de um SVE:

- A votação Remota não deve ser obrigatória;
- Eleitores com necessidades especiais;
- Infoexclusão;
- Sistema compatível com a maioria dos sistemas (Web *browsers*).

Para alem disso, o prazo de voto deve ser alargado e deverá existir um tempo de aprendizagem, ou seja o sistema deverá estar disponível antes das eleições para o eleitor experimentar aceder ao sistema e votar.

É, também recomendado a continuação da existência, nos locais tradicionais de voto, de sistemas para permitir que aqueles que não possuem acesso a um dos canais de votação remota possam exercer o seu direito de voto.

2.7 Casos Práticos

Este tópico apresenta três abordagens bastante distintas de SVE utilizados em eleições de três Países.

Uma solução totalmente baseada em hardware, com máquinas tipo *quiosque* (tipo *Multibanco)* - uma arquitectura DRE; com outra que utiliza um sistema misto de hardware (*Smart Card*) e Votação Remota com recurso à Internet; com uma outra arquitectura de Votação Remota totalmente baseada em software.

2.7.1 Caso do Brasil

O projecto de Votação Electrónica Brasileiro [TRE-MG, 2006] [Unicamp, 2002] teve início em 1987, quando o Tribunal Superior Eleitoral do Brasil começou a construir uma base de dados central para o registo de eleitores. Em 1996, o Brasil tornou-se no primeiro país a informatizar todo o processo de votação.

O SVE Brasileiro consiste [TRE-SP] [Antunes, et al., 2001] [Unicamp, 2002] em sistemas DRE colocados nos locais tradicionais de voto, composto por um terminal com um monitor LCD, um teclado numérico com as teclas: *BRANCO*, *CORRIGE* e *CONFIRMA*.

O terminal possui dois cartões de memória flash, um com o sistema operativo e software de votação, e outro com os dados dos candidatos.

Os terminais (são chamados *urnas electrónicas*) são distribuídos pelos centros de voto e durante a votação encontram-se desligadas da rede informática, funcionando *off-line*.

Após o fim da eleição [TRE-SP], são impressos alguns boletins referentes à *urna* e são gravados em disquete os dados encriptados das tabelas, os eleitores, *logs* de eventos e é prepara a *urna electrónica* para ser recolhida. A *urna*, os documentos da eleição e disquete são encaminhados para a *Junta Eleitoral local* que irá atestar a validade da votação e enviará os dados para o sistema informático do TRE.

Ilustração 1 – Terminal do SVE Brasileiro

Ilustração 2 – Teclado do SVE Brasileiro

Passos do protocolo para votar [TRE-MG, 2006] [Antunes, et al., 2001]

1) O Eleitor desloca-se até ao local de voto acompanhado o cartão de eleitor e de um documento oficial com foto;
2) Após a identificação física face à lista dos eleitores é autorizado a votar;
3) Digita o número do candidato no teclado da urna. No ecrã LCD, aparecerá a foto, o número, o nome e a sigla do partido do candidato escolhido. Se as informações estiverem correctas, usa-se a tecla verde **CONFIRMA**. A cada voto confirmado, a urna emitirá um rápido sinal sonoro. Após o registo do último voto, a urna emitirá um sinal sonoro mais prolongado e aparecerá na tela a palavra **FIM**;
4) Após o fecho das urnas, os dados são transmitidos para os respectivos tribunais eleitorais regionais, através de uma rede privada.

2.7.2 Caso da Estónia

A Estónia começou o seu projecto de voto [The National Election Committee, 2005] pela Internet em 2001 e foi posto em prática nas eleições locais de 2005. A Estónia tornou-se no primeiro país a utilizar a Internet nas eleições.

Para ter acesso ao sistema é necessário ter um cartão nacional de identificação electrónica (ID-card) que é um *Smart Card* com uma assinatura digital, que pode ser utilizada para identificação remota ou como assinatura digital legalmente reconhecida.

Esse Cartão contém [Maaten, 2006]: (i) Dados Pessoais; (ii) Certificados para autenticação; (iii) Certificado para assinatura digital.

Ilustração 3 – Cartão de Eleitor na Estónia

A votação pela Internet é feita 4 a 6 dias antes do dia de votação e os eleitores podem votar sucessivamente durante esse período, é o chamado "voto reversível". E ainda no dia da eleição, presencialmente na Assembleia de voto e nesse caso, o voto "*presencial*" é que terá validade.

Passos do protocolo para votar [The National Election Committee, 2005]

1) Autenticação é feita colocando o cartão de eleitor no *smart card reader*;
2) Faz-se a escolha;
3) Ao confirmar a escolha, o voto é cifrado com a assinatura digital;
4) Os votos dos votantes válidos são separados da assinatura digital antes de se proceder à contagem dos votos;
5) Os votos e a chave privada da eleição entram para um contador e este gera como *output* os resultados finais e *logs* para auditoria onde só aparecem os resumos dos votos cifrados. Os votos em claro nunca saem do contador.

2.7.3 Caso de Genebra – Suíça

A Suíça segue de forma rigorosa a Rec(2004)11 do COE, sentindo como necessária a existência de mecanismos de certificação do *e-voto* [Council of Europe, 2007]. O projecto Suíço começou em fase piloto, utilizando uma implementação "passo a passo" em três cantões.

O projecto de voto pela Internet [Republique et Canton de Geneve] no cantão de Genebra, foi iniciado em 2000 e testado pela primeira vez em Janeiro de 2003, desde então tem sido usado com regularidade.

O SVE de Genebra dá ao eleitor a possibilidade de utilizar um dos três canais de voto: Internet, voto postal e assembleia de voto.

Na base do desenvolvimento do SVE baseado na Internet foi travar o declínio da participação dos eleitores. No âmbito do sistema de democracia directa vigente no país, os eleitores vão às urnas eleitorais várias vezes ao ano para decidir sobre questões tão diversas como a segurança nacional ou ambiente.

A SVE foi desenvolvido baseado no material existente e não requer nenhum software adicional para além do computador do eleitor.

Factores para o sucesso: (i) Na Suíça os cidadãos votam 4 ou 5 vezes por ano; (ii) Conforto é a palavra-chave no processo de votação.

Passos do protocolo para votar [Republique et Canton de Geneve]:

1) É enviado para casa do eleitor o cartão de eleitor, renovado sempre que há eleições;
2) Autenticação: Primeiro é necessário colocar o número do cartão. Esse número não é sequencial, por isso a probabilidade de ser descoberto é 1 em 5 biliões. Depois de autenticado o sistema faz uma ligação a um servidor seguro;
3) Vota;
4) O sistema faz uma recapitulação da escolha: confirma ou altera a escolha;

5) Confirma o voto através da data de nascimento, a naturalização e do *pin* que se encontra no cartão de eleitor;

6) O sistema confirma o voto, mostrando a data de registo;

7) O servidor coloca o voto numa aplicação de "urna electrónica" e marca o votante como já tendo votado;

8) Para proceder à contagem dos votos a "urna electrónica" é desligada da rede;

9) De seguida é introduzida a chave de eleição e os votos são baralhados e decifrados.

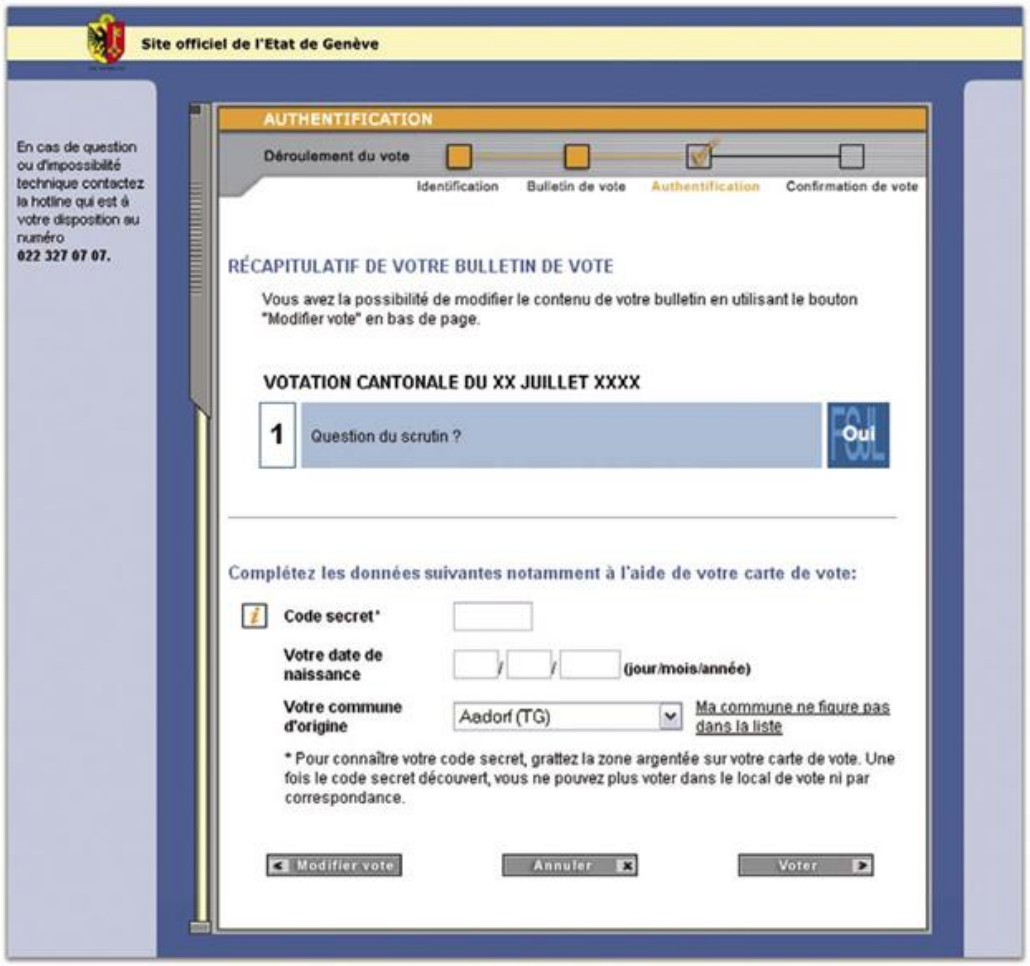


Ilustração 4 – SVE de Genebra

2.7.4 Quadro de Resumo dos Casos de Estudo

Na Tabela 4 em género de resumo verifica-se as características dos 3 SVE estudados.

Tabela 4 – Resumo dos casos de estudo dos SVE

	Brasil	**Estónia**	**Suíça – Genebra**
Arquitectura	Distribuída	Centralizada	Centralizada
Mobilidade	Presencial	Não Presencial	Não Presencial
Autenticação	Pessoal: Cartão de eleitor e documento com foto	Assinaturas digitais	Senha secreta e informação pessoal
Validade dos votos		Assinaturas digitais	
Usabilidade		Tecnologicamente complexo (leitor de cartões, instalação de *drivers*)	Não é necessário software adicional

2.8 Síntese

Neste capítulo abordou-se a nível concepcional dois conceitos de arquitecturas totalmente distintas sobre os SVE, de acordo com localização, DRE e Remotos (ou voto pela Internet).

A arquitectura DRE apresenta à primeira vista inúmeras vantagens perante a votação remota, por recorrerem a um ambiente controlado, com meios técnicos e humanos para prevenir a fraude. Por outro lado o conceito *remoto*, apesar dos riscos e da diversidade de meios e de possíveis problemas é sem duvida uma solução a ter em conta para substituir o actual voto postal (voto por correspondência), e uma considerável mais-valia para os votantes com dificuldades de mobilidade e, possivelmente, é a arma que falta para combater a abstenção ao resolver os principais problemas que se colocam aos SV: segurança, comodidade e mobilidade.

Estudou-se também três casos práticos de utilização de SVE:

- Brasil – DRE;
- Estónia – Remoto, com recurso a hardware: *Smart Card* e *Smart Card Reader*;
- Genebra (Suíça) – Remoto, totalmente baseado em software.

Chegou-se à conclusão que o sistema utilizado em Genebra, Suíça, compre notoriamente os princípios e garantias definidos pelo Concelho da Europa. Esse SVE, por ser um sistema remoto, sem a necessidade de equipamento adicional, torna-se sem dúvida a solução a ter em conta no desenvolvimento de SVE nacionais.

3 O Sistema Eleitoral Português

3.1 Introdução

Neste capítulo aborda-se o sistema eleitoral em Portugal, a nível legal, mais precisamente a fase de votação propriamente dita. Pretende-se também ser o mais generalista possível, descrevendo o sistema no global, tendo como objectivo primordial a descrição dos processos comuns aos vários tipos de eleições (legislativas, autárquicas, presidenciais, …) e referendos.

Partindo desta perspectiva, o estudo vai dividir Sistema Eleitoral Português em quatro subsistemas principais [Assembleia da Republica - Lei Eleitoral, 1979]:

1. Recenseamento Eleitoral;
2. Votação (autenticação, votação e depósito do voto);
3. Contagem;
4. Divulgação (dos resultados).

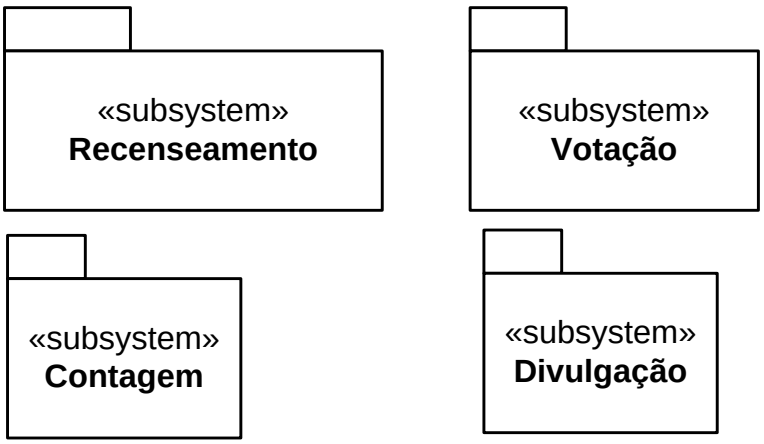


Ilustração 5 – Subsistemas do SV Português

3.1.1 Conceitos técnicos

3.1.1.1 Casos de Uso e Diagramas de Actividade

Os diagramas de casos de uso [Booch, et al., 1998] mostram como o sistema se encontra organizado. Os diagramas estão relacionados com a especificação de requisitos e descriminam o comportamento pretendido para o sistema. O estudo dos casos de uso, mais do que modelar os requisitos do sistema, destinam-se a dirigir todo o processo de desenvolvimento e avaliação do sistema [Silva, et al., 2001].

Diagramas de Actividade [Booch, et al., 1998] [Silva, et al., 2001] representam fluxos conduzidos por processamento interno.

3.1.1.2 Actores

Os actores representam todos os utilizadores ou conceitos (por exemplo publico em geral) que interagem com o sistema. No sistema de eleitoral Português existem os seguintes actores:

- **Recenseador:**
  Elementos, nomeados pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, com o objectivo de poderem aceder ao sistema para efectuar presencialmente o Recenseamento de Eleitores.
- **Potencial Eleitor:**
  Todo o cidadão que esteja em condições legais para participar no processo eleitoral e que pretenda registar-se como Eleitor, para posteriormente exercer o seu direito de voto.
- **Eleitor:**
  Todo o cidadão que esteja em condições legais para participar no processo eleitoral.
- **Mesa da Assembleia:**
  Órgão constituído por cinco eleitores que executa e dirige as operações de votação e de apuramento parcial em cada assembleia ou secção de voto. A mesa

é composta por um presidente, pelo seu suplente e por três vogais, sendo um secretário e dois escrutinadores.

- **Público em Geral:**
  Todos os interessados (órgãos de comunicação social, partidos políticos, candidatos, população, etc.) na obtenção dos resultados parciais/finais de um processo de votação.
- **Mesa da Assembleia:**
  Órgão constituído por cinco eleitores que executa e dirige as operações de votação e de apuramento parcial em cada assembleia ou secção de voto. A mesa é composta por um presidente, pelo seu suplente e por três vogais, sendo um secretário e dois escrutinadores.
- **Presidente da Câmara do Município:**
  Presidente da Câmara do Município da área de recenseado ou Presidente da Câmara onde se situe o estabelecimento hospitalar ou prisional
- **Delegados do Listas:**
  Representantes das listas de candidatos às eleições.

3.2 Recenseamento

O Recenseamento Eleitoral (RE) (Lei 13/99 de 22-Março) [Assembleia da República, 1999] é um direito constitucional fundamental que garante a concretização da participação política dos cidadãos através da votação em eleições e referendos.

Trata-se de conjunto de operações de inscrição, eliminação ou actualização de dados dos eleitores, com vista à elaboração dos cadernos de recenseamento contendo a lista de todos os cidadãos titulares do direito de sufrágio e respectivos ficheiros com os seus dados identificativos. A realização do RE é condição prévia imprescindível para o exercício do direito constitucional de sufrágio, activo e passivo, em eleições ou referendos.

3.2.1 Características do RE

De acordo com a lei nº 13/99 de 22-Março [Assembleia da República, 1999] o RE tem as seguintes características:

- **Obrigatório**

  O RE é, nos termos da Constituição, "*obrigatórios para os cidadãos nacionais residentes no território nacional maiores de 18 anos*" (art. 7 da lei nº 13/99, de 22-Março), sob pena de procedimento criminal, à excepção dos nacionais que residem no estrangeiro, para quem o recenseamento é voluntário ou para os cidadãos da União Europeia *não nacionais* do Estado Português, residentes em Portugal, mas necessário para votar nas eleições europeias e autárquicas, bem como para os cidadãos de outras nacionalidades com capacidade eleitoral nas eleições autárquicas.

- **Permanente**

  A Constituição Portuguesa refere também ser o RE *"tem efeitos permanentes*" (art. 5 da lei nº 13/99, de 22-Março), o que significa que ele é válido para todas as eleições, não sendo renovado cada vez que se realiza nova eleição, mas tão-somente actualizado pela contínua inscrição de novos eleitores, eliminação de eleitores falecidos ou que tenham sido privados do exercício de direitos políticos por sentença criminal, ou transferência resultante de mudança de residência.

- **Único**

  Nos termos da Constituição, o RE é único – "*ninguém pode estar inscrito mais do que uma vez no recenseamento*" (art. 7 da lei nº 13/99, de 22-Março), o que visa assegurar a existência de um só recenseamento, como garantia de um controlo da sua regularidade, uma das condições indispensáveis para que a cada eleitor corresponda um e só um voto nas eleições por sufrágio directo e universal.

3.2.2 Descrição do Processo RE

Os cidadãos eleitores devem estar recenseados (art. 9 da lei nº 13/99, de 22-Março) "*na entidade recenseadora correspondente à residência indicada no B.I."* ou ao domicílio

constante do título de residência emitido pela entidade competente, correspondendo, em regra, a unidade geográfica no continente e nas regiões autónomas à freguesia e no estrangeiro ao distrito consular ou ao país se nele houver apenas embaixada.

A inscrição no recenseamento eleitoral dos cidadãos residentes no território nacional e estrangeiro é realizada continuamente, excepto nos 60 dias que antecedem qualquer votação, ocasião em que o RE se suspende. É, no entanto, admitida a inscrição de eleitores com 17 anos (art. 35 da lei nº 13/99, de 22-Março) e que cumpram 18 até ao dia da votação, até ao 55º dia anterior à votação. Assim, podem inscrever-se no RE logo que completem 17 anos, embora a inscrição só se torne efectiva quando completam 18 anos.

Para se inscreverem (art. 34 da lei nº 13/99, de 22-Março) devem dirigir-se à Comissão Recenseadora correspondente à residência indicada no B.I. ou título de residência, e aí preencher um verbete de inscrição (branco para os nacionais, azul para os cidadãos da UE e amarelo para os restantes estrangeiros), recebendo em troca um cartão de eleitor de cor idêntica, contendo o respectivo nº de inscrição.

Na Ilustração 6 é representado no diagrama uma visão de alto nível do processo de recenseamento eleitoral utilizando o modelo UML Use Cases (ou casos de uso).

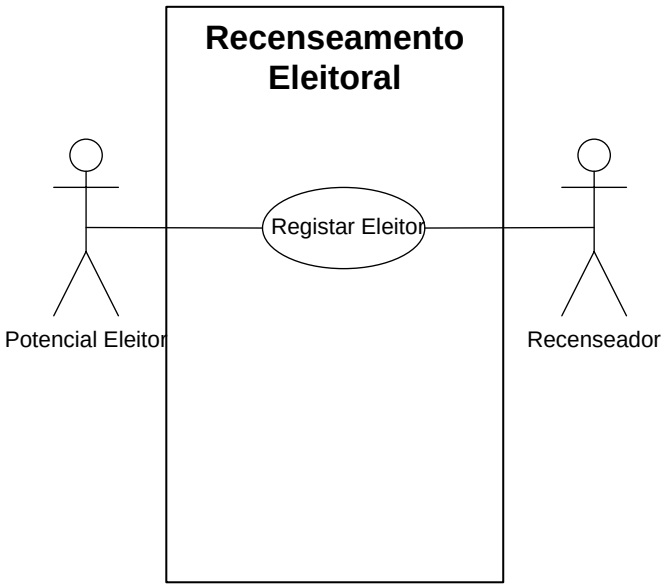


Ilustração 6 – Use Cases - Recenseamento Eleitoral

A Ilustração 7 representa-se num Diagrama de Actividades o processo de RE com os dois actores: “Potencial Eleitor” e “Recenseador”.

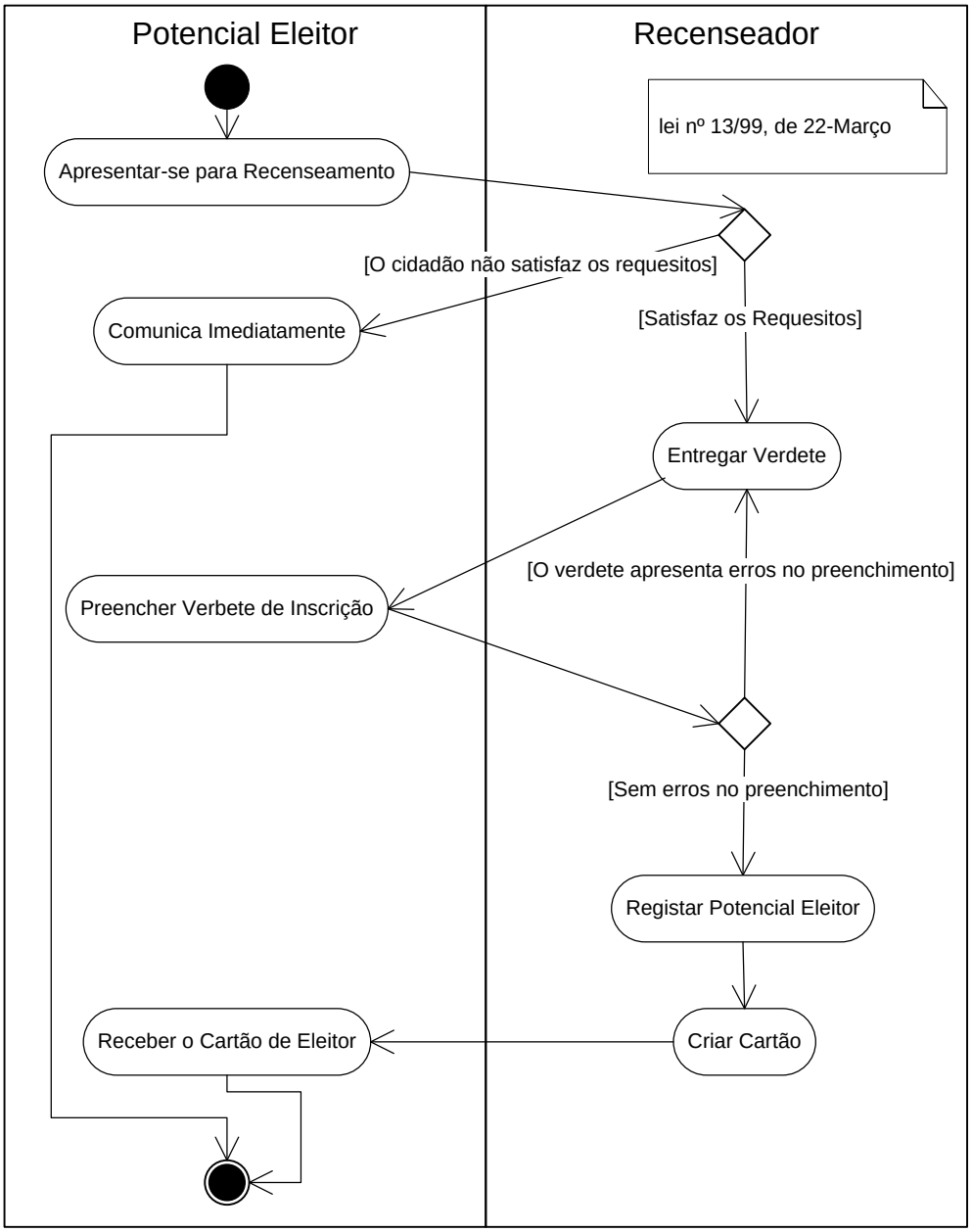


Ilustração 7 - Diagrama de Actividades - Processo de RE

3.3 Votação

No processo eleitoral Português, podem exercer o direito de voto:

- **Os cidadãos portugueses recenseados em território nacional**
  Os cidadãos portugueses recenseados em território nacional (art.º 2.º, nº 1, al. a e 4.º lei nº 13/99, de 22 Março).
- **Os cidadãos da U.E.**
  Não nacionais do Estado Português (art.º 2.º, nº 1, al. b) e 4.º da lei nº 13/99, de 22-Março).
- **Os cidadãos de países de Língua Oficial Portuguesa.**
  Com residência legal em Portugal há mais de dois anos – Brasil e Cabo-Verde (art.º 2.º, nº 1, al. c) e 4.º da lei nº 13/99, de 22-Março).
- **Outros cidadãos estrangeiros**
  Com residência em Portugal há mais de 3 anos, desde que nacionais de países que, em condições de reciprocidade, atribuam capacidade eleitoral activa aos portugueses nele residentes e que são, actualmente, Argentina, Chile, Estónia, Israel, Noruega, Peru, Uruguai e Venezuela (art.º 2.º, nº 1, alínea d) e 4.º da lei nº 13/99, de 22-Março).

3.3.1 Processo de Votação

O processo de votação divide-se em cinco fases devidamente ordenadas, como representado na Ilustração 8, com as actividades a ser realizadas no dia da votação. Essas fases decorrem pela ordem [Assembleia da Republica - Lei Eleitoral, 1979]: (i) Abertura das Urnas; (ii) Votação dos Elementos da Mesa; (iii) Processar os Votos antecipados (se existirem); (iv) Votação (presencial, por ordem de chegada); (v) Fecho das Urnas.

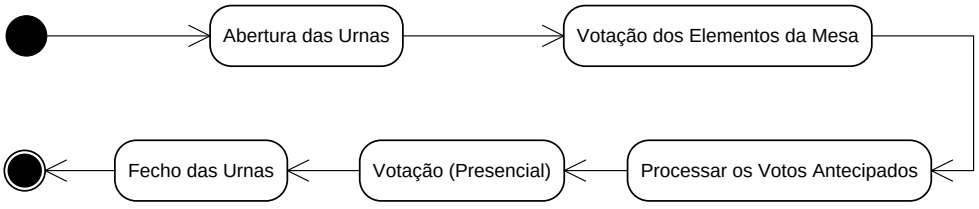


Ilustração 8 – Diagrama de Actividades da Votação

3.3.2 Votação Presencial

Os cidadãos eleitores devem dirigir-se aos locais de voto correspondente à residência indicada no B.I. ou ao domicílio [Assembleia da Republica - Lei Eleitoral, 1979] [Assembleia da República, 1999] constante do título de residência emitido pela entidade competente.

Ao chegar deverão apresentar um documento comprovativo de identidade e o respectivo cartão de eleitor aos membros da Mesa Eleitoral. Um dos elementos da Mesa Eleitoral irá verificar se o cidadão satisfaz todos os requisitos legais e regista a participação no acto eleitoral. Pretende-se desta forma assegurar que: (i) Só votam os cidadãos recenseados; (ii) Cada eleitor só vota uma vez.

O cidadão eleitor recebe o boletim de voto, desloca-se para uma área do recinto, criada para o efeito, para proceder à sua escolha. Posteriormente regressará à Mesa Eleitoral para depositar o seu voto, devidamente selado, para o depositar. Garante-se desta forma a **confidencialidade** do voto.

Na imagem Ilustração 9 utiliza-se o Modelo UML Use Cases para representar o processo de votação:

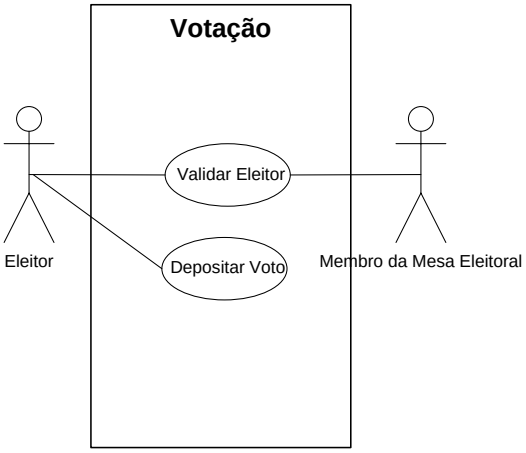


Ilustração 9 – Use Cases - Processo de Votação

Excepções: No caso do voto dos deficientes o artigo 97 da Lei 14/79, de 16 Maio, permite que o cidadão "*vota acompanhado de outro eleitor por si escolhido, que garanta a fidelidade de expressão do seu voto e que fica obrigado a sigilo absoluto*" [Assembleia da Republica - Lei Eleitoral, 1979].

Modo como vota cada eleitor:

"*O direito é exercido directamente pelo cidadão eleitor*" (Artigo 79º da Lei 14/79, de 16 Maio).

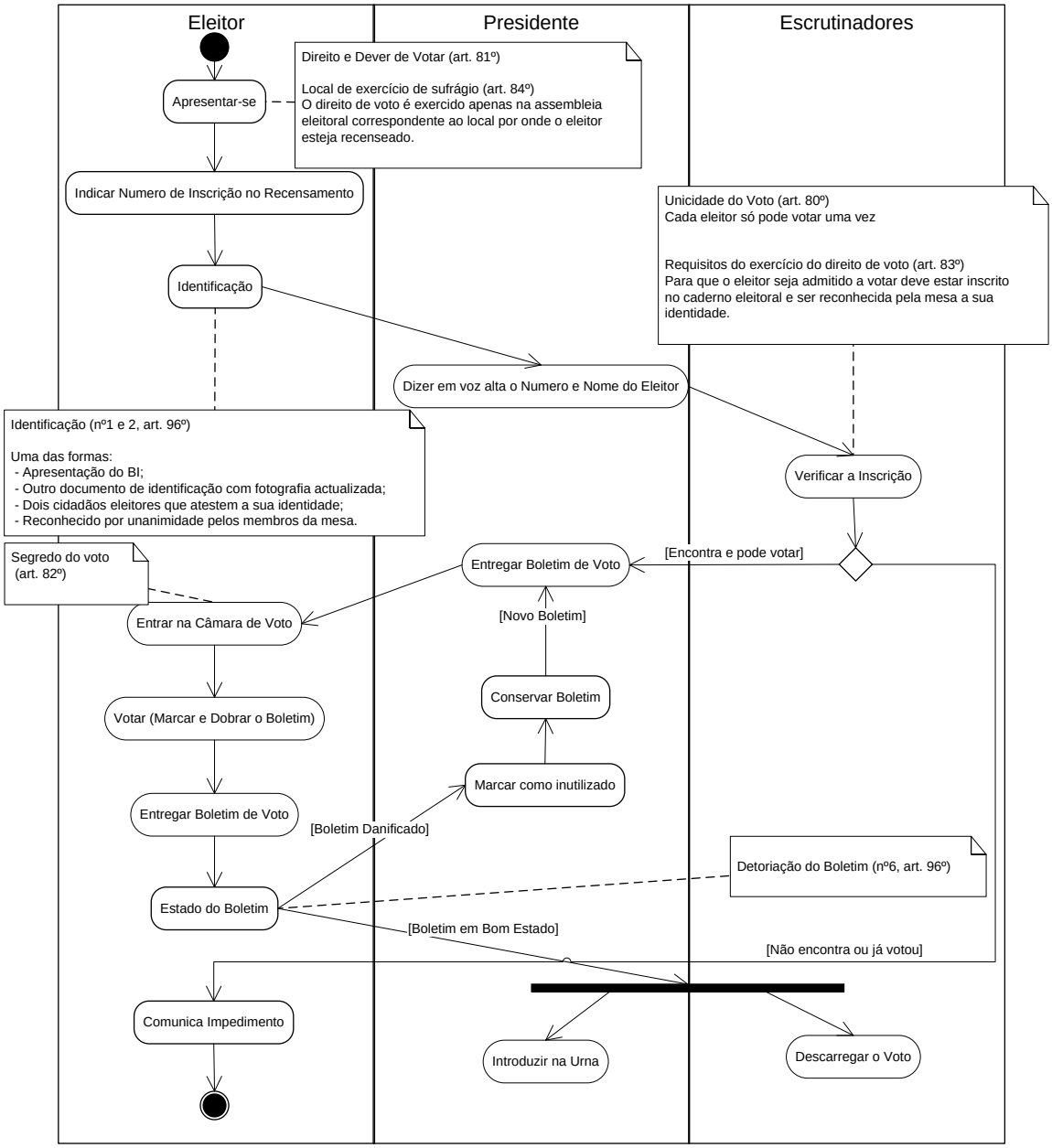


Ilustração 10 – Diagrama de Actividades – Processo de Votação

3.3.3 Votação antecipada

O conceito de voto antecipado reporta-se a determinadas grupos de eleitores como os citados pela Lei 14/79, de 16 Maio, art. 70.º-A.

3.3.3.1 Militares, agentes de segurança, trabalhadores dos transportes e desportistas.

Modo de exercício do direito de voto antecipado por militares, agentes de forças e serviços de segurança, trabalhadores dos transportes e membros que representem oficialmente selecções nacionais, organizadas por federações desportivas dotadas de estatuto de utilidade pública desportiva (artigo 79.º-B da lei 14/79, de 16 Maio).

Na Ilustração 11 representa numa linguagem formal, diagrama de actividades, as operações do processo de votação antecipado. Segundo o artigo 79.º da lei 14/79, de 16 Maio, o eleitor tem de tem de se encontrar numa das seguintes situações:

”*a) Os militares que no dia da realização da eleição estejam impedidos de se deslocar à assembleia de voto por imperativo inadiável de exercício das suas funções;*

b) Os agentes de forças e serviços que exerçam funções de segurança interna, nos termos da lei, e se encontrem em situação análoga à prevista na alínea anterior;

c) Os trabalhadores marítimos e aeronáuticos, bem como os ferroviários e os rodoviários de longo curso, que, por força da sua actividade profissional, se encontrem presumivelmente embarcados ou deslocados no dia da realização da eleição; (...)

f) Os membros que representem oficialmente selecções nacionais, organizadas por federações desportivas dotadas de estatuto de utilidade pública desportiva, e se encontrem deslocados no estrangeiro, em competições desportivas, no dia da realização da eleição.”

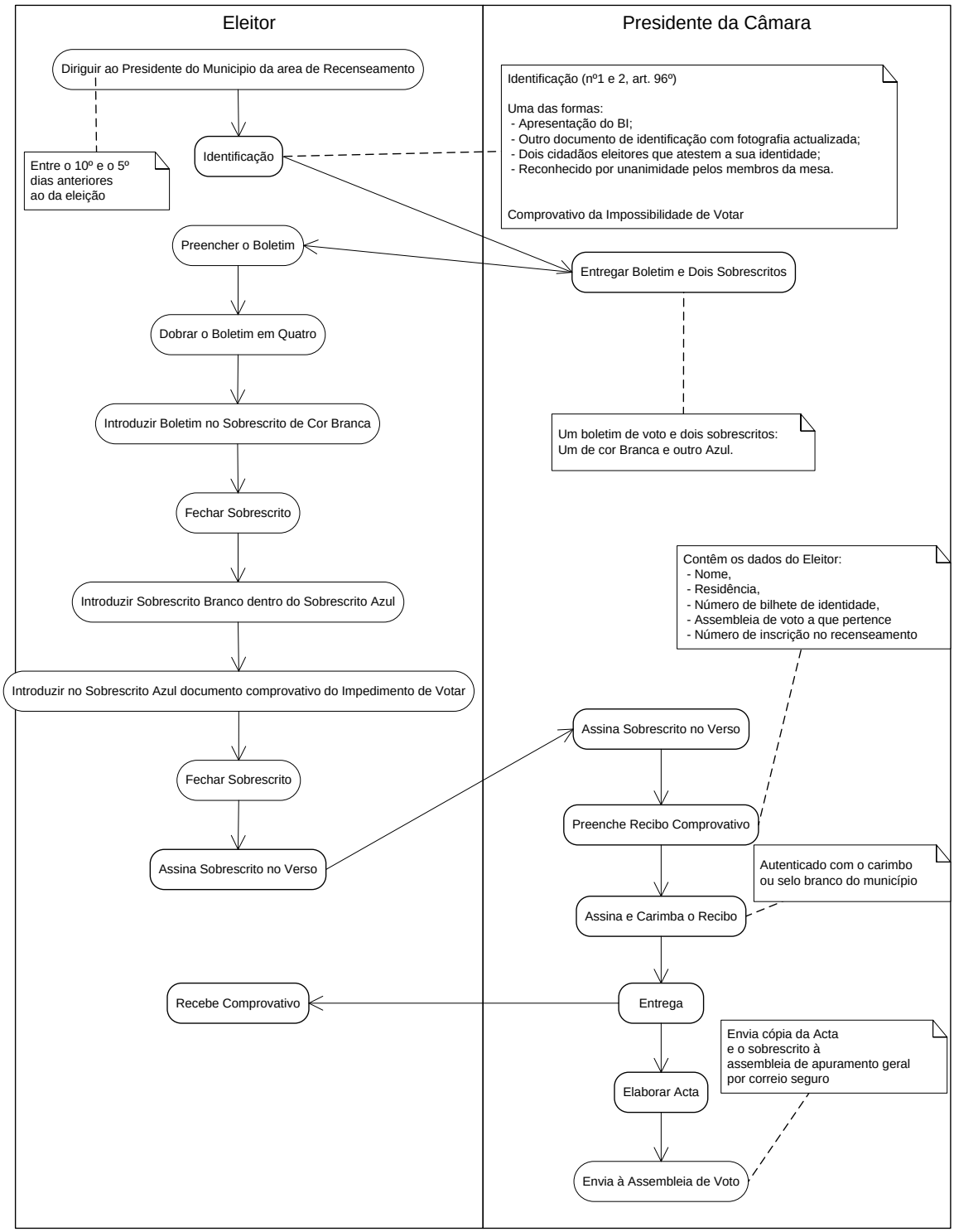


Ilustração 11 – Diagrama de Actividades – Voto Antecipado A

3.3.3.2 Doentes Internados e Presos

Modo de exercício do direito de voto antecipado por eleitores que por motivos de doença se encontrem internados e com a impossibilidade de deslocar e presos não privados de direitos políticos é descrito como diagrama de actividades na Ilustração 12 de acordo com o artigo 79.º-C da lei 14/79, de 16 Maio.

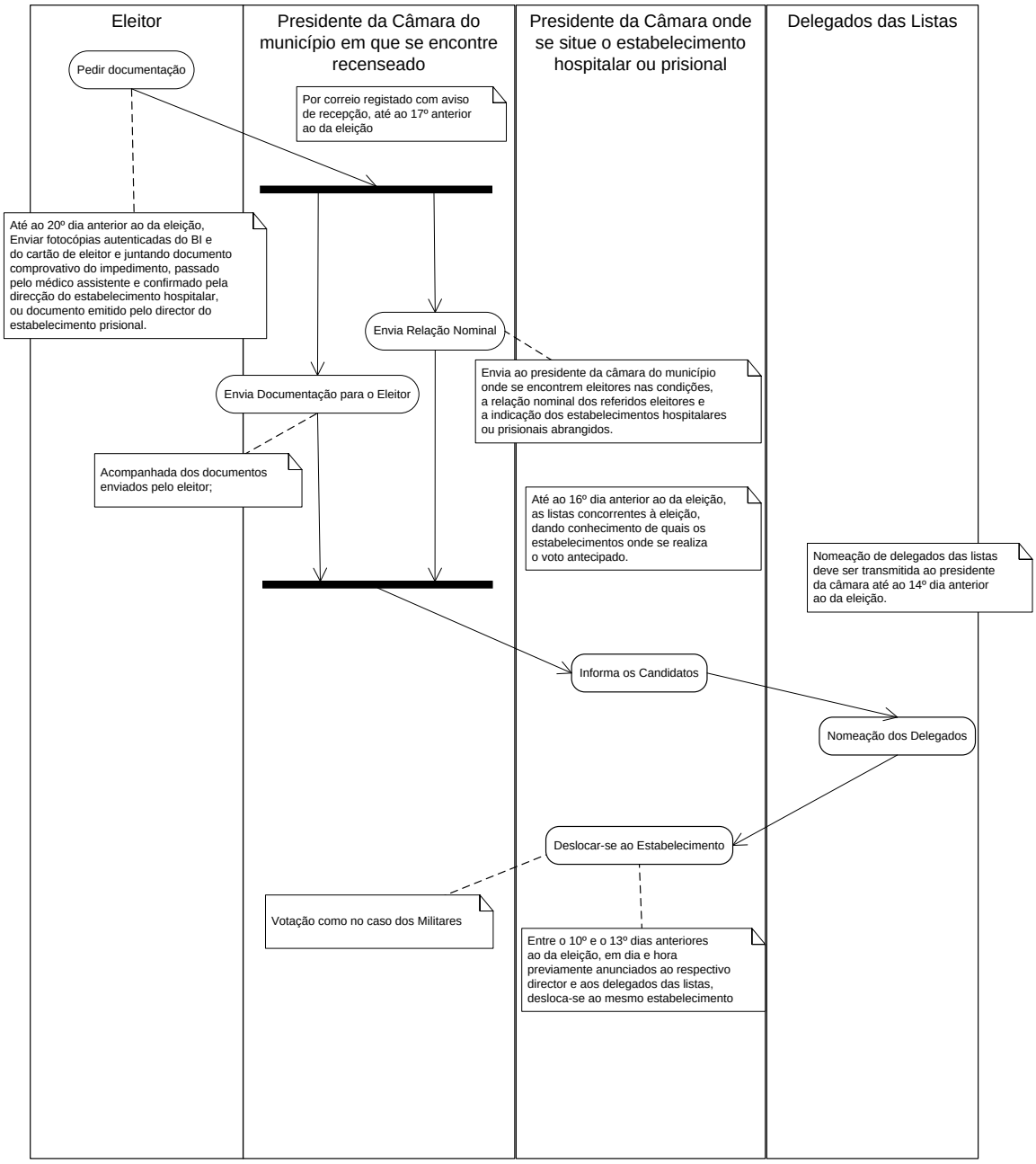


Ilustração 12 – Diagrama de Actividades – Voto Antecipado B

3.4 Contagem

O subsistema de contagem dos votos, também denominado de *escrutínio,* é a operação de contagem dos votos obtidos para a definição dos resultados dos actos eleitorais ou referendários A legislação eleitoral portuguesa optou pelo apuramento na assembleia de voto, no dia da eleição [Assembleia da Republica - Lei Eleitoral, 1979]. Tal solução confere, sem dúvida, grande celeridade ao apuramento e ao consequente conhecimento público dos resultados, embora se deva referir que existem no nosso país cerca de 12.500 assembleias eleitorais, sendo difícil assegurar que em todas haja uma eficaz fiscalização.

O processo de contagem começa logo após o fecho das urnas, em cada assembleia de voto, obtendo-se os resultados. Nesse processo pretende-se [Assembleia da Republica - Lei Eleitoral, 1979]:

- **Consolidar os Votos:** Consolidar os votos contados bem como a lista de pessoas que votaram no acto eleitoral. O processo é independente em cada centro eleitoral.
- **Verificar a Integridade:** É realizada se houver dúvidas de alguma parte sobre o modo como o processo decorreu. Nesse caso os responsáveis deverão demonstrar os registos para provar a validade dos resultados.
- **Verificação da não duplicação de votos:** Verificar que os votos foram contados correctamente, isto é, que o total de votos obtidos coincide com o número de votantes.

Os resultados das secções de voto são enviados para a Junta de Freguesia onde são somados para obtenção dos resultados a nível de Freguesia, os quais são depois transmitidos ao respectivo Governo Civil

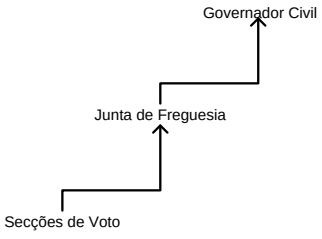


Ilustração 13 – Contagem

Podemos definir que existem quatro subsistemas de contagem:

- Apuramento por secções de voto;
- Apuramento por freguesia;
- Apuramento por distrito;
- Apuramento geral.

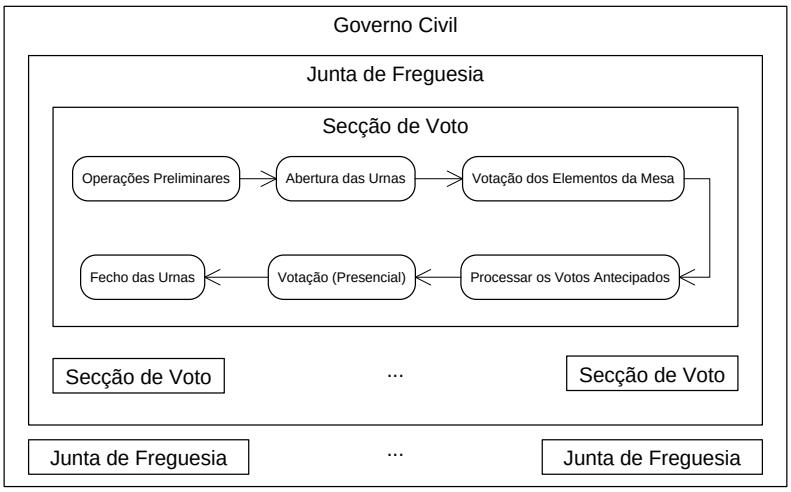


Ilustração 14 – Apuramento dos Resultados

Processo de Contagem Geral utilizando o Modelo UML Use Cases:

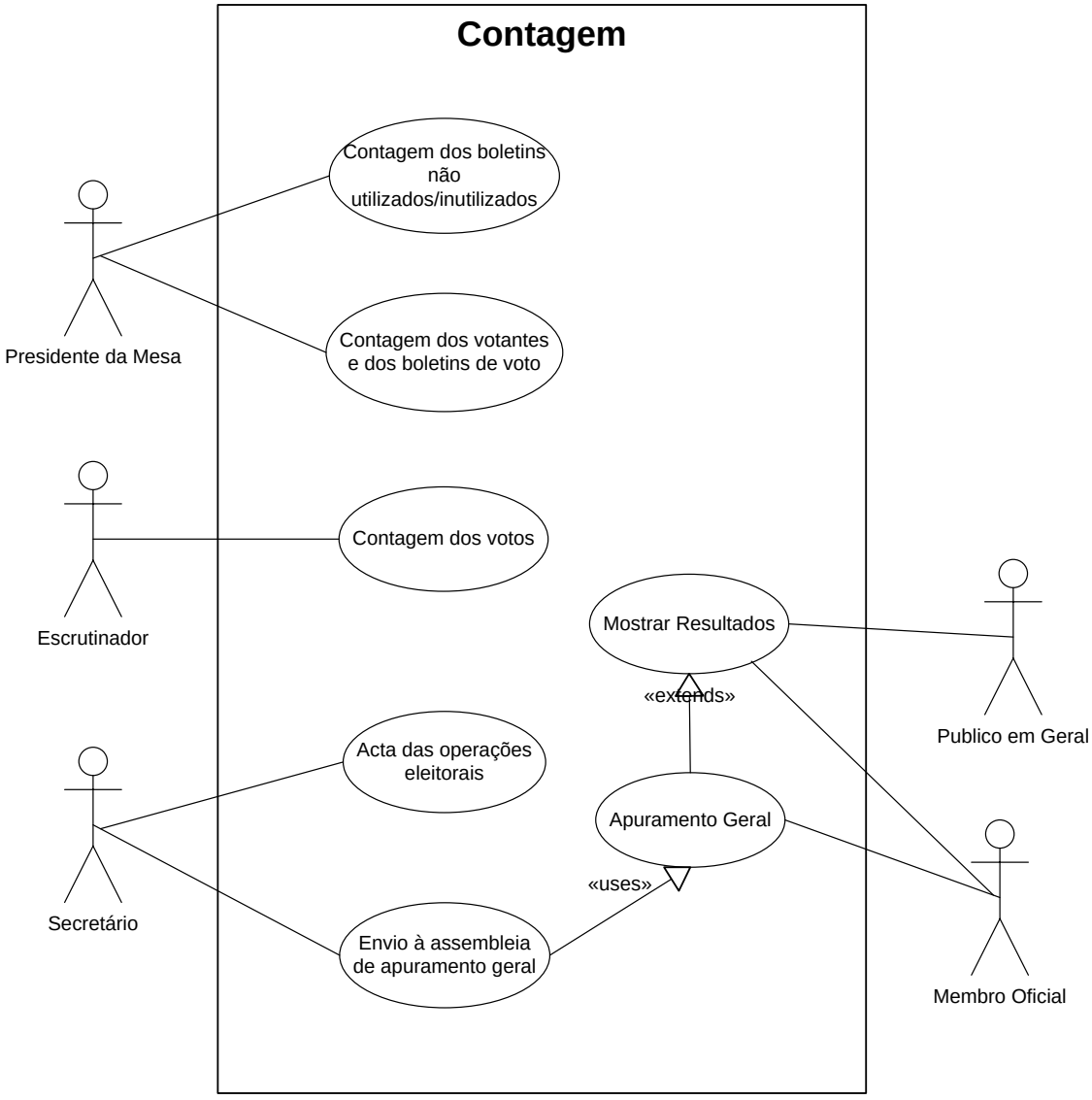


Ilustração 15 – Use Cases – Contagem

3.4.1 Descrição do Processo de Apuramento dos Resultados

Após o encerramento das urnas procede-se ao apuramento dos resultados na própria assembleia de voto.

É o seguinte o escalonamento das operações [Assembleia da Republica - Lei Eleitoral, 1979]:

1. **Contagem dos boletins de voto não utilizados e inutilizados** pelos eleitores (artigo 100.º).

Devem ser metidos em pacote com ofício (modelos **AR-31 e 32**), fechado e lacrado, sendo enviado ao Presidente da Câmara Municipal (artigo 95.º, n.º 7 da Lei 14/79, de 16 Maio);

2. **Contagem dos votantes** pelas descargas feitas nos cadernos (artigo 101.º, n.º 1 da Lei 14/79, de 16 Maio);
3. Abertura da urna e **contagem dos boletins de voto** nela entrados. Depois de contados devem ser de novo metidos na urna (artigo 101.º, n.º 2 da Lei 14/79, de 16 Maio); Se o número de votantes contados pelas descargas não for igual ao número de votos contidos na urna será o número de votos da urna que prevalecerá (artigo 101.º, n.º 3 da Lei 14/79, de 16 Maio);
4. **Publicação de edital** (modelo AR-33) em que se indicará o **número de boletins de voto entrados**, que, depois de lido em voz alta pelo presidente, será afixado à porta principal da assembleia de voto (artigo 101.º, n.º 4 da Lei 14/79, de 16 Maio);
5. **Contagem dos votos nas listas, brancos e nulos**.
6. De seguida, um dos escrutinadores desdobra os boletins de voto um a um e anuncia em voz alta qual a lista votada, enquanto o outro regista, numa folha branca ou nas folhas de descarga ou, se possível, num quadro bem visível, os votos atribuídos a cada lista, os votos em branco e os votos nulos (artigo 102.º, n.º 1 da Lei 14/79, de 16 Maio).
    a. Considera-se **voto em branco** o boletim de voto que não tenha qualquer tipo de marca.
    b. Considera-se voto nulo:
        i. Aquele que tenha uma cruz em mais de um quadrado;
        ii. Aquele que estiver assinalado numa lista que desistiu;
        iii. Aquele que contenha qualquer corte, desenho, rasura ou no qual tenha sido escrita qualquer palavra;
        iv. O voto antecipado quando o boletim de voto não chega nas condições legalmente previstas ou seja recebido em envelopes que não esteja devidamente fechado (v. ponto B4).

7. **Loteamento** dos votos: O presidente irá examinando e exibindo, auxiliado por um dos vogais, os boletins de voto agrupando-os por lotes que correspondam às listas votadas, aos votos em branco e aos votos nulos (artigo 102.º, n.º 2 da Lei 14/79, de 16 Maio).
8. A **conferência final** far-se-á do seguinte modo:
    - O presidente compara o número de votos de cada lote com o número de votos registados na folha ou no quadro (artigo 102.º, n.º 3 da Lei 14/79, de 16 Maio).
    - Os delegados das listas poderão examinar depois os lotes dos boletins de voto separados. Podem também apresentar dúvidas, reclamações ou protestos quanto à contagem ou quanto à qualificação dada ao voto de qualquer boletim; estas dúvidas, reclamações ou protestos deverão ser feitas perante o presidente e, se não forem atendidas, os delegados terão direito de, juntamente com o presidente, rubricar o boletim de voto em causa sendo estes separados dos restantes.
    - Deve realçar-se que a reclamação ou protesto não atendidos não impedem a contagem do respectivo boletim de voto para efeitos de apuramento (artigo 102.º, n. 4, 5 e 6 da Lei 14/79, de 16 Maio).

Publicitação dos resultados.

A mesa deverá afixar à porta da assembleia de voto um edital (modelo AR-34) contendo o número de votos atribuídos a cada lista, o número de votos em branco e o de votos nulos (artigo 102.º, n.º 7 da Lei 14/79, de 16 Maio).

O secretário da mesa deverá elaborar a acta das operações de votação e apuramento (modelo **AR-48**) (artigo 105.º da Lei 14/79, de 16 Maio) que terá obrigatoriamente de ser remetida à Assembleia de Apuramento Geral.

O **preenchimento da acta** é **obrigatório** e deve ser feito **integralmente**. O incumprimento total ou parcial desta obrigação é punível com multa (artigo 168.º da Lei 14/79, de 16 Maio).

Comunicação de resultados

Escrutínio provisório

No final das operações eleitorais é **indispensável** que o presidente da mesa **comunique** com a máxima celeridade, **pelos meios e para as entidades localmente determinadas**, os **resultados eleitorais obtidos** na respectiva assembleia/secção de voto.

A necessidade dessa rápida comunicação é devida aos trabalhos do Escrutínio Provisório organizado pelo STAPE, que se desenrola em Lisboa — para onde os resultados são encaminhados pelas entidades locais que os recolhem — e através do qual o País será informado, no próprio dia da eleição, do evoluir dos resultados eleitorais.

Para evitar qualquer tipo de perturbação, as mesas não deverão divulgar publicamente os resultados a nenhuma entidade ou indivíduo antes de os comunicarem às autoridades locais acima referidas e de afixarem o edital respectivo.

Assembleia de apuramento geral

O **apuramento geral** dos resultados da eleição em cada distrito/região autónoma compete à Assembleia de Apuramento Geral, que inicia os seus trabalhos às **9 horas** do **2.º dia posterior ao da eleição**, no local para o efeito designado pelo Governador Civil ou, nas Regiões Autónomas pelo Ministro da República (artigo 107.º da Lei 14/79, de 16 Maio).

Entre os elementos que a compõem figurarão seis presidentes de assembleia ou secções de voto designados pelo Governador Civil ou Ministro da República (artigo 108.º, n.º 1, alínea d) da Lei 14/79, de 16 Maio).

Processo de Contagem utilizando o Modelo UML Diagrama de Actividade:

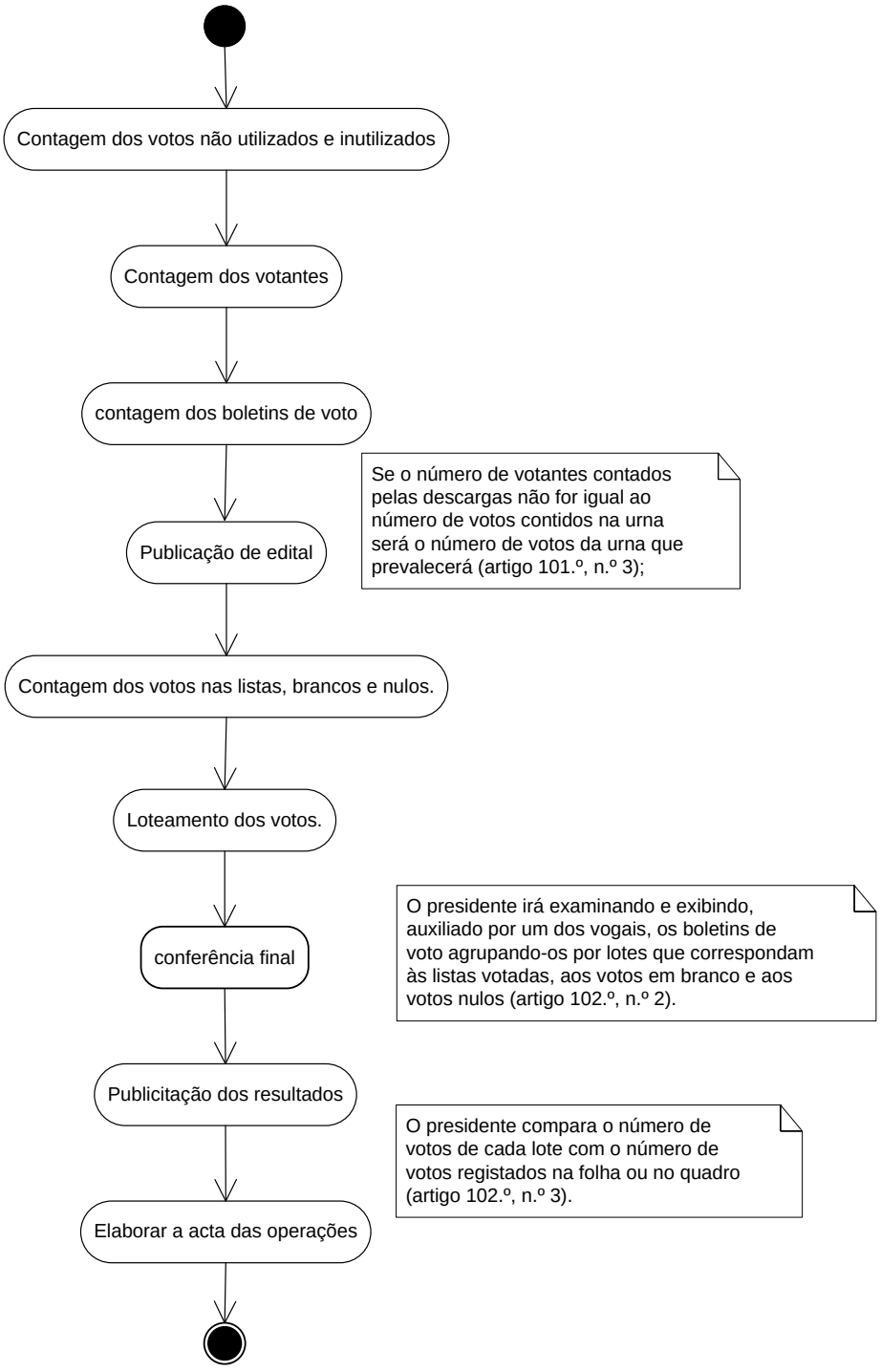


Ilustração 16 – Diagrama de Actividade - Contagem

3.5 Síntese

Neste capítulo descreveu-se o funcionamento do Sistema Eleitoral Português, é um sistema de votação tradicional que respeita a observância dos princípios eleitorais básicos. A Lei 13/99 de 22-Março estabelece o regime jurídico do recenseamento eleitoral e a Lei 14/79, de 16 Maio estabelece o regime jurídico para a realização de eleições e forma como se processa a votação, contagem e apresentação dos resultados.

A legislação portuguesa permite a votação antecipada nos casos definidos pela lei e o recurso a voto por correspondência.

Neste capítulo fez-se, também, a descrição das actividades, com base na legislação eleitoral, utilizando uma linguagem formal, o UML, para representar e descrever os principais processos (recenseamento, votação, contagem e divulgação dos resultados) que constituem o Sistema Eleitoral Português.

4 Tecnologias para e-Voto

4.1 Introdução

Neste capítulo são abordadas os conceitos e tecnologias utilizadas para o desenvolvimento do trabalho de investigação representado no protótipo e apresentado nesta dissertação, tais como o EML, *Web Services*, XML.

4.2 Election Markup Language

Election Markup Language (EML) é uma linguagem de comunicação [OASIS, 2007] desenvolvida pelo consórcio OASIS[6] (*Organization for the Advancement of Structured Information Standards*). No início do desenvolvimento desta dissertação a versão disponibilizada (*standard* desde Fevereiro de 2006) e recomendada pelo Concelho da Europa [Cover, 2004] [European Communities, 2004] é a 4.0. Em Maio de 2007 surgiu uma nova versão, a 5.0., e em Novembro de 2007 foi aprovada como *standard* OASIS.

O EML apresenta uma visão de alto nível dos fluxos de um sistema genérico de votação electrónica, através de um conjunto de XML *schemas*[7] bem elaborados, que tentam ser o mais completos e genéricos possíveis, e que servem para a interpolação entre os diversos subsistemas que constituem o SVE.

O EML permite que o SVE possa ser desenvolvido por diversas organizações, não estando todo o sistema dependente [OASIS, 2007] [Aas, 2005] de uma única organização, ao subdividi-lo em diversos subsistemas independentes que através de um conjunto de interfaces claros fazem uma integração transparente, utilizando um conjunto de regras e objectos definidos no EML. Ou seja, o EML parte de um princípio democrático [Aas, 2005], não existe uma dependência de uma só organização. Isto

[6] OASIS é um consórcio internacional, sem fins lucrativos, que conduz o desenvolvimento, a convergência e a adopção de padrões de e-*business*.

[7] XML *schema* é uma linguagem baseada no formato XML para definição de regras de validação em documentos no formato XML.

permite com que facilmente se possa mudar um subsistema, mantendo toda a actual estrutura do SVE.

O EML não defende que as diversas fases do processo de votação electrónica tenham um *schema* associado a cada *output*. O objectivo é que seja utilizado os respectivos documentos EML (definidos nos *schemas*) para a comunicação entre os diversos subsistemas que constituem o SVE no intercâmbio dos dados.

4.2.1 Características do EML

O EML foi criado com o objectivo de cobrir o maior número de possibilidades, é possível ser utilizado nas mais diversas situações, desde eleições públicas (nacionais, locais), referendos, votações privadas, utilizando canais diversos como a Internet, o voto postal, voto por *SMS*, voto por telefone, votação tradicional.

As principais características do EML são [Borras, 2002]:

- **Multinacional:** com criada com a possibilidade se ser utilizado globalmente;
- **Flexível:** possível de ser implementado sobre diferentes estruturas e canais de votação (tradicional, *SMS*, Internet, postal);
- **Multilingue:** flexível para suportar diversas línguas;
- **Adaptável:** pode ser utilizado para eleições públicas, privadas, referendos;
- **Seguro:** define medidas de segurança na interpolação dos dados.

O EML suporta todas as fases do processo eleitoral: (1) Preparação dos boletins, candidatos e eleição; (2) Votação e acessibilidade no dia da eleição; (3) Contagem; (4) Resultados; (5) Distribuição/apresentação e arquivo.

4.2.2 Estrutura do EML

A comunicação definida no EML é baseada num modelo que divide o sistema eleitoral em diversos subsistemas. O modelo pode ser visto na "Ilustração 17 – EML - Fluxo de Informação", que é uma simplificação do "*High-Level Modell – Technical View*" do documento "*EML Process & Data Requirements*" que acompanha os *schemas*.

Os subsistemas do modelo definem diferentes sistemas conceptuais: sistema de nomeação de candidatos, sistema de eleitores, sistema de listas de candidatos, sistema de votação, sistema de contagem e, além disso, o sistema de eleição. Estes sistemas são realmente apenas partes do sistema eleitoral como um todo.

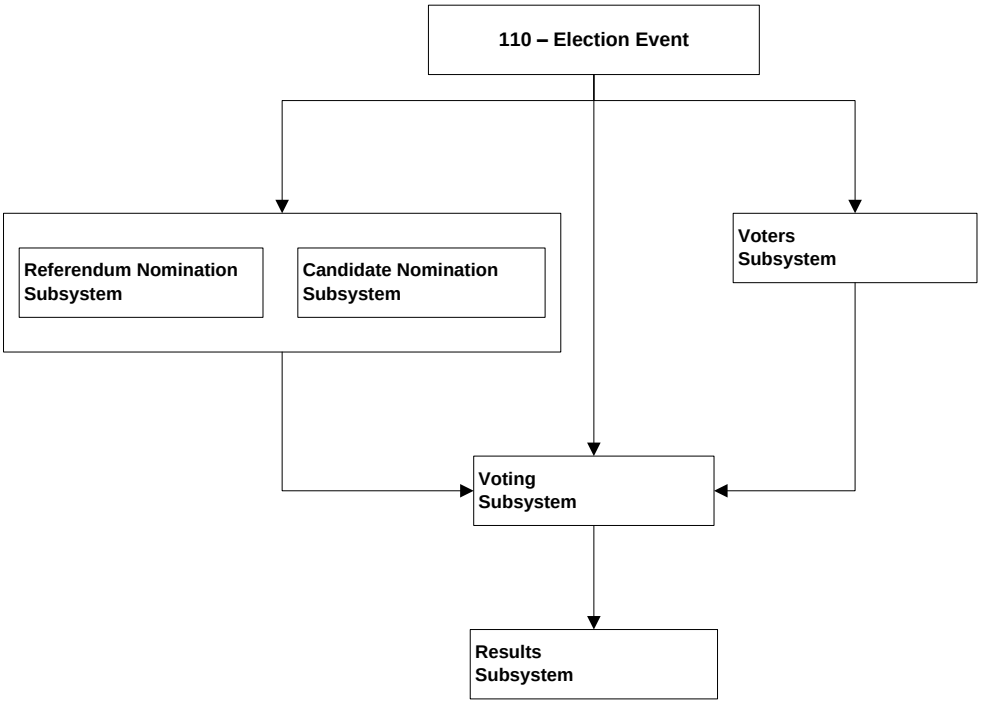


Ilustração 17 – EML - Fluxo de Informação[8]

O EML inclui especificações dos processos, definições dos dados e XML *schemas* para todas as fases que ocorrente antes, durante e após o acto eleitoral. Em seguinte indicam-se as principais operações suportadas pelo EML.

Pré-eleição:

- Nomeação de candidatos, resposta a nomeações e listas de candidatos aprovados;
- Opções de eleição;
- Informação de registo de eleitores;
- Varias comunicações entre eleitores e oficiais da eleição, tais como a informação da votação, as observações da eleição, etc.

[8] O evento eleição 110 – é a referência do schema xml

Eleição:

- Boletins;
- Autenticação de eleitores;
- Votação e confirmação do voto;

Pós-eleição:

- Contagem e resultados;
- Auditar.

A partir destas três grandes áreas (pré-eleição, eleição e pós-eleição) que constituem o processo eleitoral, representa-se na Tabela 5 os principais *schemas* EML utilizados.

Tabela 5 - Principais documentos do EML

Fase	**Schema**	**Descrição**
Pré-eleição	EML 110 – election event	Informação sobre a eleição ou conjunto de eleições.
	EML 210 – candidate nomination	Usado para nomear candidatos ou partidos
	EML 230 – candidate list	Detalhes dos candidatos
	EML 310 – voter registration	Usado para registo dos eleitores
	EML 330 – voter election list	Detalhes dos actuais eleitores de uma eleição
	EML 340 – polling information	Notificação ao eleitor de uma eleição, sua elegibilidade e como votar
Votação	EML 410 – ballot	Descreve o boletim que vai ser usado na votação
	EML 420 – voter authentication	Usado para a autenticação do votante durante a votação
	EML 440 – cast vote	Registo do voto actual

	EML 460 – votes group	Grupos de votos transferidos para contagem
Pós-eleição	EML 480 – audit log	Registos de actividades
	EML 510 – count	Contagem dos resultados das eleições
	EML 520 – result	Detalhes dos resultados das eleições

4.2.3 Validação das mensagens EML

A comunicação entre os diversos subsistemas que constituem o SVE é assente nas mensagens ou documentos especificados pelos *schemas* EML. Como esses subsistemas poderão ser desenvolvidos por diversos fabricantes é extremamente importante que as mensagens sejam válidas, para haver uma correcta comunicação e evitar dessa forma erros desnecessários.

As mensagens EML devem, portanto, ser construídas de acordo com as regras especificadas no *schema* EML, e, é face a esses *schemas* que serão validadas, recorrendo a uma validação da estrutura e conteúdo com o *Schematron*[9].

Por outro lado, as *schemas* EML representam especificações para a criação de um conjunto de documentos XML (eXtensible Markup Language) e essa definição é suficiente formal para tornar possível compilar esses *schemas* para código. Essa compilação é efectuada através de um *binding compiler*.

No capítulo 4.4 vai-se abordar com maior detalhe o processo de *bind* das mensagens XML.

[9] É uma linguagem para fazer declarações sobre padrões encontrados em documentos XML http://www.schematron.com

4.3 Open Source

Alguns autores [Schneier, 2004] definem que o software utilizado nos sistemas de votação deverá estar disponível para consulta pública e em vez dos actuais sistemas proprietários de "caixa preta".

Uma das formas de garantir a confiança dos SVE é recorrer à utilização de padrões e código aberto (*Open Source)* para dar confiança nas tecnologias utilizadas e lançar o código do SVE para o domínio público. Dessa forma garantem que o funcionamento do SVE é transparente, o que trará maior confiança no sistema.

Esta abordagem sobre a disponibilização do código do SVE já é posta em uso por alguns países. Por exemplo, o SVE australiano [Electronic voting and counting, 2006] encontra-se disponível para consulta pública

Open Source é o software que o código fonte é visível publicamente. O conceito não diz respeito apenas ao acesso, define também regras para a sua distribuição e utilização. Há muitas licenças *Open Source*, como o GNU *General Public License* (GPL), *Apache Software License*, *Mozilla Public License* (MPL), MIT *License*, etc. (não é objectivo deste trabalho abordar essas regras de distribuição).

No desenvolvimento deste protótipo recorreu-se a tecnologias robustas e sempre que possível *Open Source*, tais como:

- Linux: sistema operativo do servidor;
- PHP e Java: linguagens de programação;
- XMLBeans e JAXB: xml *binding*;
- Apache: servidor Web;
- MySQL: servidor de base de dados;
- Eclipse: IDE (*Integrated Development Environment*).

4.4 XML *binding*

A partir de um *schema* que especifica a estrutura do documento XML, o compilador gera um conjunto de classes contendo todo o código para criar e manipular os

documentos XML baseados no XML *schema*. Tudo isto sem requerer escrever muitas linhas de código para trabalhar com *schemas* complicadas.

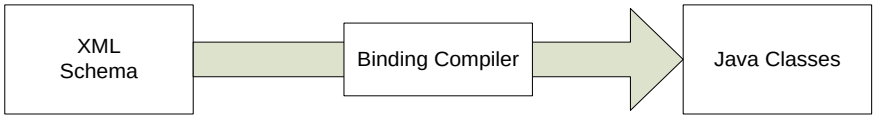


Ilustração 18 - Processo de criação de classes Java

Utilizar um *xml binding compiler* tem muitas inúmeras vantagens, garante-se que os documentos XML são validos, é rápido, fácil de usar e é extensível.

Neste trabalho de dissertação usou-se JAXB [Ort, et al., 2003] (Java Architecture for XML Binding) e o XMLBeans [Apache, 2007] do projecto Apache. Ambos fornecem uma maneira rápida de mapear XML documentos em objectos Java.

4.5 Web Services

Web services é uma solução utilizada para a integração de diversos sistemas e para a comunicação entre diferentes aplicações [Sumra, 2003]. Com o recurso a esta tecnologia é possível integrar novas aplicações com outras já existentes e que sistemas desenvolvidos em plataformas diferentes sejam totalmente compatíveis.

Os *Web services* podem ser vistos como componentes que permitem às aplicações enviar e receber dados. Cada aplicação tem a sua maneira característica de funcionar, com linguagens e estruturas próprias que são convertidas para estrutura universal no formato XML.

Para comunicar com o *Web Service*, é necessária uma implementação do protocolo SOAP (*Simple Object Access Protocol*) definido no W3C. Este protocolo é o responsável pela independência que o *Web Service* precisa. Actualmente já existem diversas implementações disponíveis em várias linguagens de programação.

Na Ilustração 19 encontra-se um diagrama mostrando as mensagens trocadas entre o cliente e o servidor numa comunicação SOAP. Para as duas aplicações poderem comunicar, um *Client Wrapper* e um *Server Wrapper* estão a disponibilizar

transparência para as aplicações. As mensagens são transferidas no formato XML, encapsulados pelo protocolo SOAP sobre o transporte HTTP.

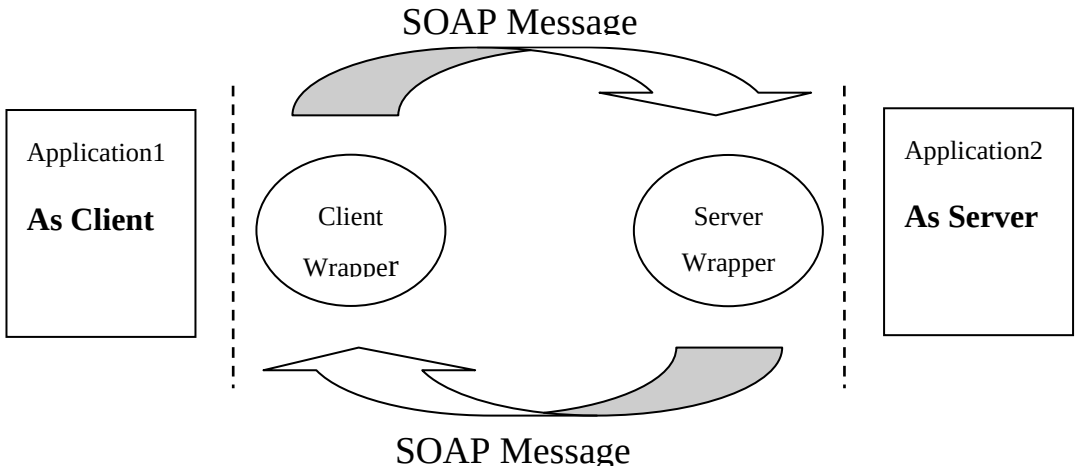


Ilustração 19 – Funcionamento de *Web Services* [10]

A proposta para a implementação do EML que se apresenta no próximo capítulo, divide o SVE em diversos subsistemas independentes e ao mesmo tempo torna-o distribuído, assenta sobre os conceitos de *Web Services*.

4.6 Síntese

Neste capítulo foram abordados numa forma concepcional as tecnologias que estão na base da proposta e protótipo deste trabalho de dissertação.

O recurso a *Web Services* e a tecnologia *Open Source*, como o *standard* EML para o desenvolvimento de sistemas de votação trará maior legitimidade e flexibilidade às arquitecturas de SVE.

[10] A ilustração é baseada na figura do artigo [Sumra, 2003].

5 Proposta

5.1 Introdução

Um sistema eleitoral é constituído por um conjunto de processos electrónicos ou manuais com diferentes tempos e propósitos de execução [Aas, 2005]. Alguns são utilizados antes, outros durante e outros no fim da votação. Esses subsistemas podem ser vistos como entidades autónomas que realizam tarefas claras, definidas na legislação eleitoral e que no seu conjunto constituem um sistema completo de votação.

O trabalho apresentado nesta dissertação pretende demonstrar a utilização do EML num ambiente de simulação de um sistema de voto electrónico. Ambiciona-se demonstrar a interpolação de alguns subsistemas que constituem o SVE através do recurso às mensagens XML definidas pelo respectivo *schema* EML.

A prototipagem corresponde aos subsistemas das fases *durante* e *após* a votação descritas na Tabela 1 do capitulo 2 , tais como: validação de eleitores, votação, recolha e contagem dos votos. Os restantes subsistemas e respectivos processos que antecedem o acto eleitoral, como o recenseamento, organização dos círculos eleitorais, apresentação das candidaturas (nomeação dos candidatos), preparação dos distritos eleitorais, ficam para um futuro desenvolvimento.

5.2 Requisitos do Protótipo

O SVE proposto deverá ser capaz de satisfazer os principais requisitos apresentados na secção 2.2 e cumprir os objectivos técnicos propostos em 1.1 . O protótipo irá ainda apresentar um SVE composto por vários módulos ou subsistemas independentes e a comunicação entre eles será efectuada com recurso a mensagens EML.

O sistema será desenvolvido tendo por base o XML (*eXtensible Markup Language*), o que irá permitir futuramente desenvolver a adaptação do *frontend* para diversos canais

(PDA, WebTV, *smartphone*), para além de todas as outras vantagens oferecidas pelo XML, como a transparência, simplicidade, flexibilidade e manipulação de dados.

5.3 Arquitectura do Protótipo

A arquitectura proposta pega nos conceitos e *workflow* do EML, divide o SVE em diversos subsistemas baseado no estudo do capítulo 2 , nomeadamente as fases de votação e contagem representadas na Tabela 1. Como objectivo primário é demonstrar a utilização do EML, apresenta-se um sistema distribuído, baseado em *Web Services* (capítulo 4.5), que irão desempenhar alguns dos subsistemas que constituem o SVE.

Na Tabela 6 são descritas as principais operações dos 5 subsistemas principais que compõem o protótipo.

Tabela 6 - Fases e Subsistemas do protótipo

Fases	**Sistemas/Servidores**	**Componentes/Operações**
Autenticação	Servidor de Autenticação (*Authentication Servers*)	Autenticação do votante.
Votação	Servidor de Votos (*Ballot Servers*)	Disponibilização do Boletim (XML); Confirmação do Voto.
Recolha do Voto	Repositório de Votos (*Votes Repository*)	Tornar voto anónimo; Guardar o Voto (XML e base de dados).
Contagem	Contadores (*Counters*)	Contagem dos Votos XML e validação dos resultados.

Esses subsistemas são autónomos, devem ser distribuídos em diversos servidores físicos independentes, como é apresentado na figura da arquitectura física[11].

[11] O nome dos servidores e das camadas está em inglês para haver uma correspondência com as classes (no código) do protótipo e para facilitar a sua divulgação.

A arquitectura física proposta para o SVE:

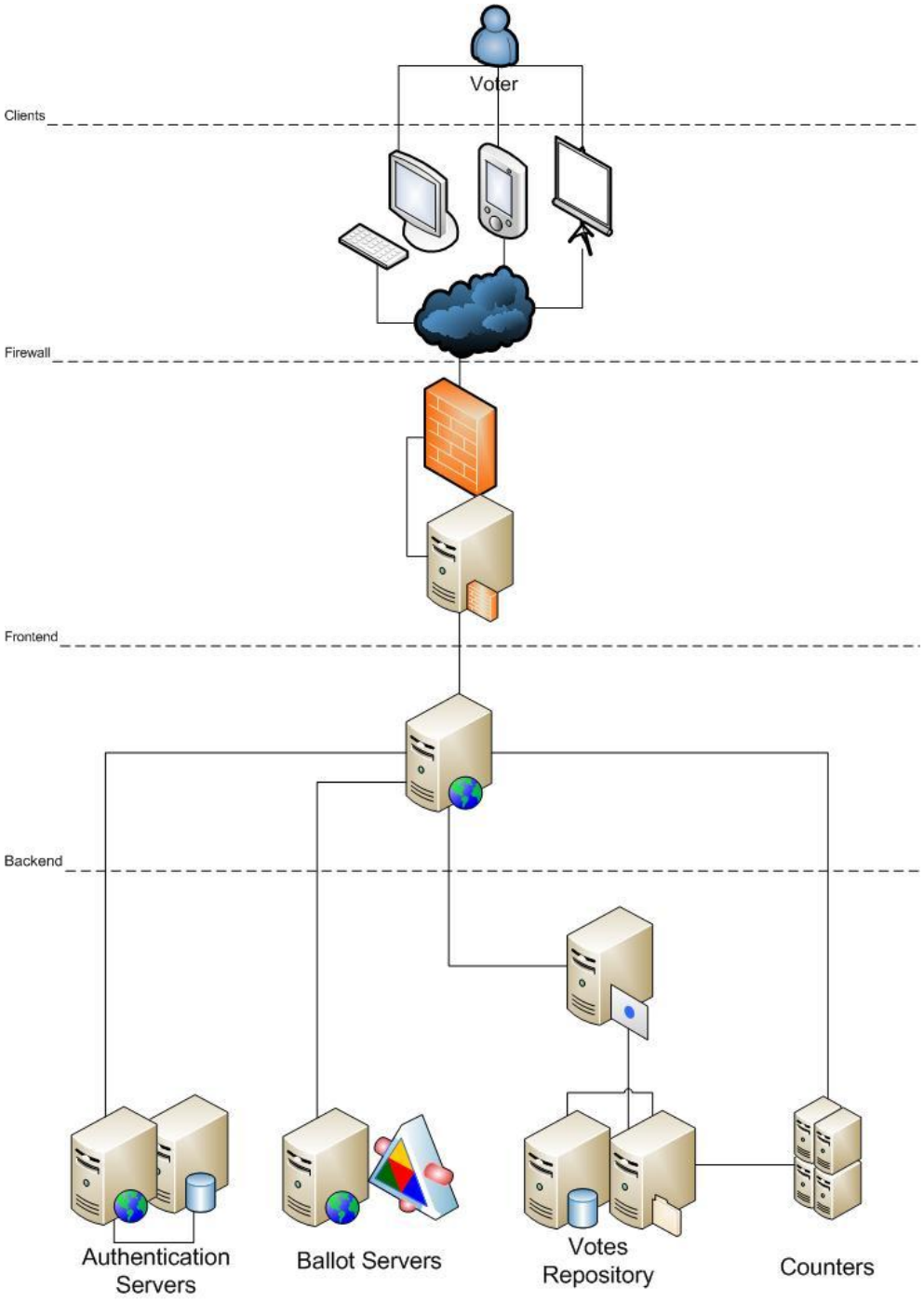


Ilustração 20 - Camadas da Arquitectura Física

Para fins de prototipagem, todos estes servidores aplicacionais serão concentrados num único servidor físico, no entanto o protótipo está preparado para ser distribuído em diversos servidores. Cada um desses servidores desempenha as tarefas definidas, como autenticação, boletins, registo dos votos e contadores, e, como já foi referido, a comunicação entre eles é baseada nas mensagens EML.

Do ponto de vista lógico, tentou-se aplicar parcialmente no desenvolvimento, a arquitectura aplicacional *n-tier*[12]. A arquitectura proposta para o funcionamento do protótipo é constituída por diversas camadas lógicas como exemplificado na Ilustração 21, baseada na arquitectura proposta em CEVS [Dessislava, et al., 2003]. Onde existem basicamente quatro camadas:

- Client: os diversos canais que podem ser utilizados para utilizar o SVE;
- WEB: responsável pela detecção e manipulação da informação para ser disponibilizada aos clientes;
- Business: conjunto de componentes de criptografia e XML;
- DATA: base de dados e templates gráficos para lidar com o XML.

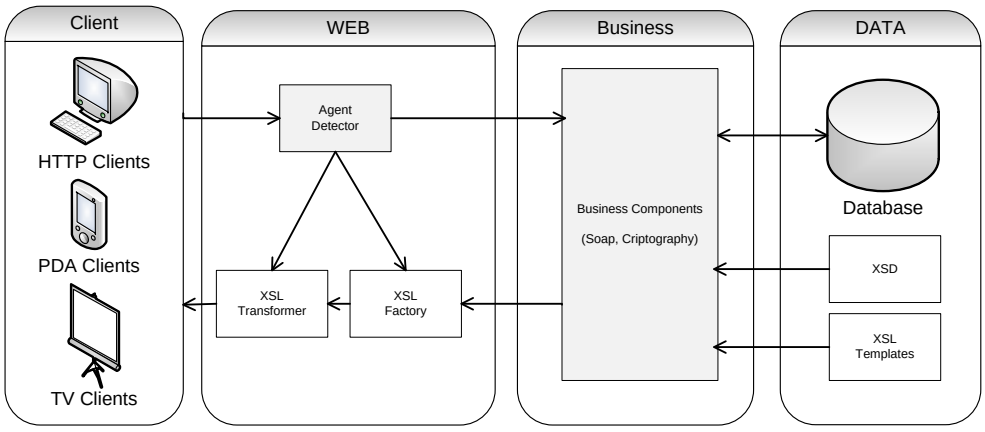


Ilustração 21 – Camadas da Arquitectura Lógica do Sistema

[12] Arquitectura de desenvolvimento multi-camadas

5.4 Proposta conceptual

5.4.1 Actores

Os actores representam todas as entidades que interagem com o SVE. Uma entidade pode ser um utilizador (pessoa) como um eleitor ou candidato, ou um equipamento informático, como um servidor (servidor de eleitores, boletins) ou qualquer outro componente do sistema de votação.

De seguida apresentam-se os principais actores que interagem no SVE:

- **Eleitor**: são as pessoas previamente registas no sistema e que possuem o direito de voto;
- ***FrontEnd***: é o componente que funciona como interface para o eleitor, cabe a este componente realizar todas as operações entre o eleitor e os restantes componentes;
- **Servidor de Autenticação (***Authentication Servers***)**: é o componente que valida o direito de voto de determinado eleitor para determinado acto eleitoral;
- **Servidor de Boletins (Ballot Server)**: é o servidor responsável pela disponibilização do boletim para o eleitor;
- **Repositório de Votos (Votes Repository)**: responsável pelo anonimato e arquivo dos votos.

A Ilustração 22 apresenta o diagrama UML de casos de uso do SVE proposto. Esse diagrama representa uma visão geral de alto nível dos casos de uso dos quatro actores e suas principais acções.

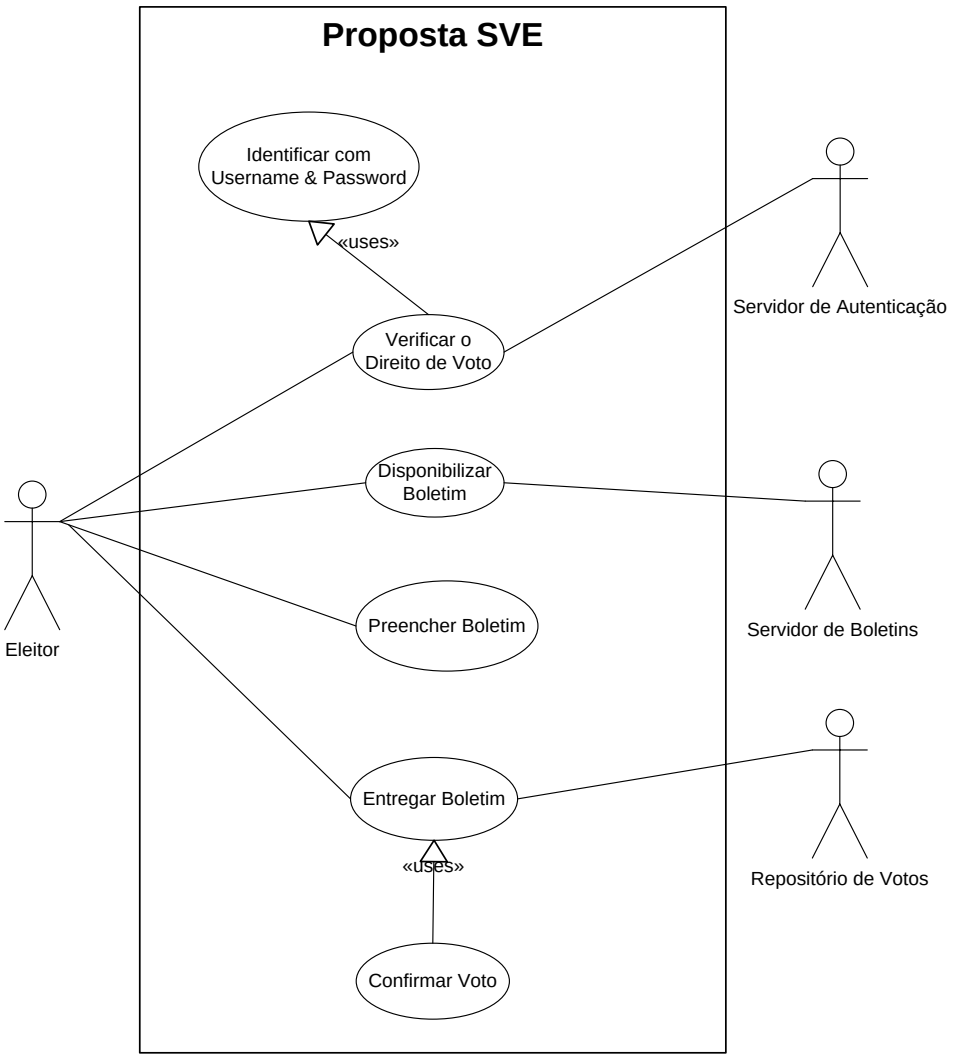


Ilustração 22 - Diagrama de Casos de Uso do protótipo

5.4.2 Diagrama de Classes

Os diagramas de classes permitem especificar a estrutura estática de um sistema segundo uma abordagem orientada a objectos [Ambler, 2001]. Em particular as entidades existentes, as suas estruturas internas e relações entre si.

Um diagrama de classes descreve um conjunto de instâncias compatíveis com determinado diagrama de classes. Permite ilustrar os detalhes de um sistema em determinado momento ao providenciarem cenários e possíveis configurações [Silva, et al., 2001].

A Ilustração 23 apresenta as classes do SVE proposto.

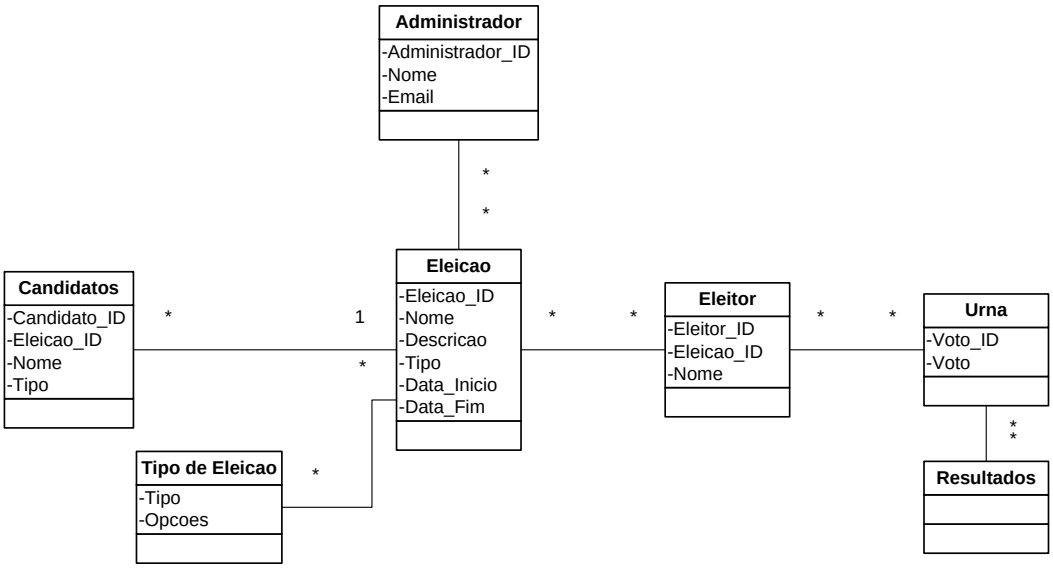


Ilustração 23 - Diagrama de Classes do protótipo

5.5 Análise e desenho do sistema

5.5.1 Diagrama de sequência

O diagrama de sequência [Booch, et al., 1998] descreve as interacções entre os elementos do SVE segundo uma visão temporal. Os elementos são representados pelas suas "linhas de vida" e interagem por troca de mensagens ao longo de um determinado período de tempo [Silva, et al., 2001].

De seguida apresenta-se os diagramas de sequência referente à implementação para a operação de votar propriamente dita. A Ilustração 24 representa o processo de autenticação no SVE, com a utilização do *Web Service authentication* para a validação do Eleitor.

Após o eleitor ter submetido os dados pedidos pelo *frontend* (*Username*, *Password* e *ValidNumber*) são submetidos para validação para o sistema de autenticação. Se os dados forem válidos é gerado um *token* (*vtoken*) e enviado para o *frontend*. O *token* é validado e se for válido, é registada a sessão e concedido o direito de acesso ao sistema de votação.

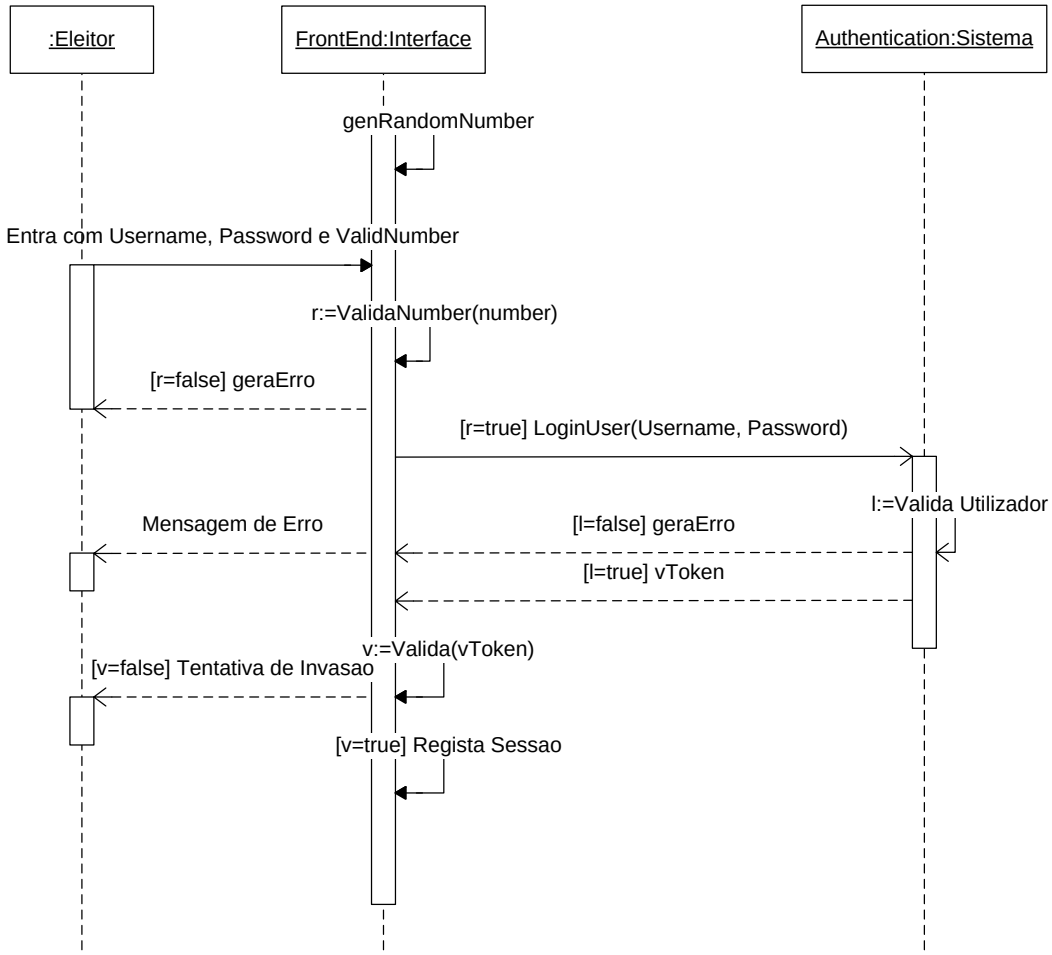


Ilustração 24 - Diagrama de Sequência da Autenticação

Na Ilustração 25 está representado o processo de votação com os diversos *Web Services* a desempenhar o seu papel de disponibilização, recolha e arquivo do voto. É nesta fase que é utilizado o código *PIN* entregue juntamente com o *Username* e *Password*. Esse PIN é requerido para confirmar a escolha no candidato.

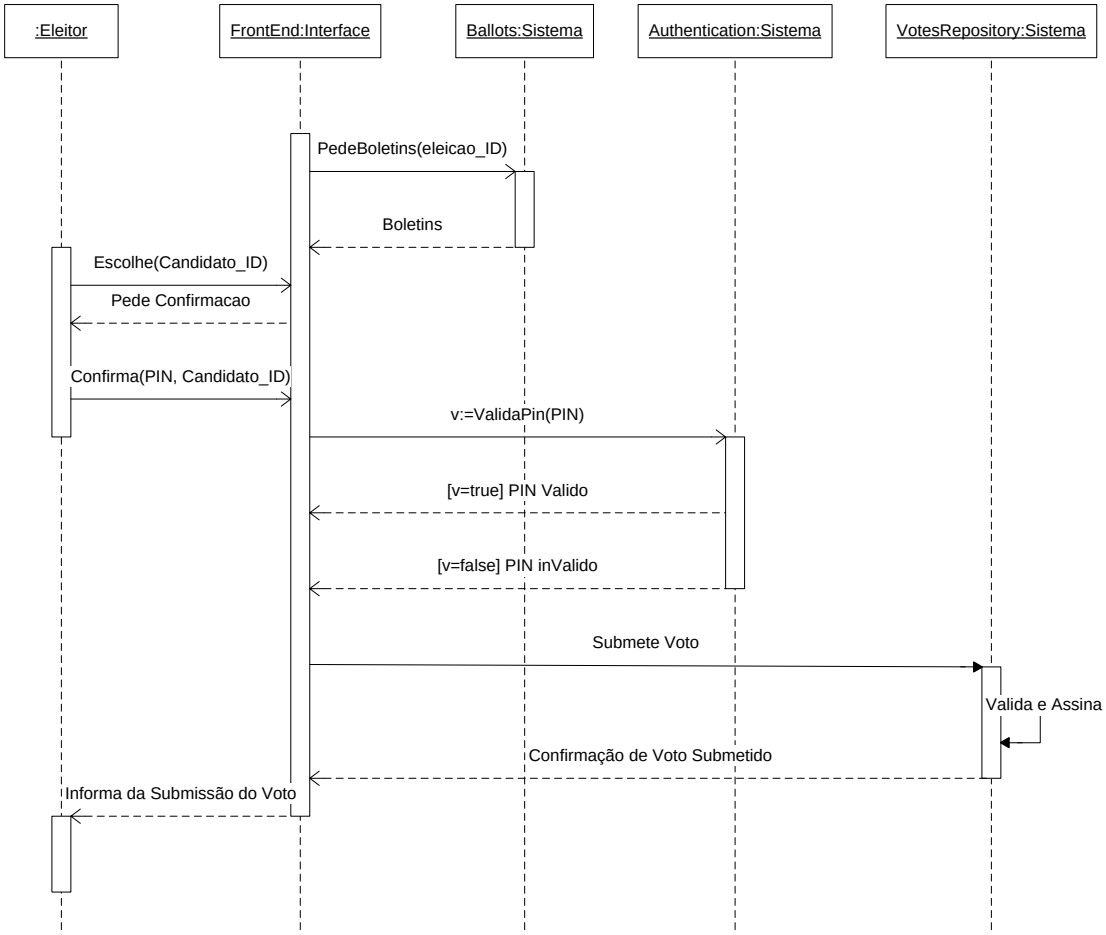


Ilustração 25 - Diagrama de sequência da Votação

5.5.2 Diagrama de Base de Dados

No desenvolvimento do protótipo recorre-se a três bases de dados (Elections_DB, Voters_DB, Votes_DB) relacionais [Codd, 1970] que deverão ficar distribuídas em servidores de base de dados distintos. Deve-se ainda utilizar *clusters* ou outros mecanismos de balanceamento de carga nesses servidores que irão estar as bases de dados, de modo a minimizar falhas.

Elections_DB:

A primeira base de dados "*Elections_DB*", representa no Ilustração 26, é a base de dados utilizada para criar a eleição e para o registo dos candidatos. É também nessa base

de dados que se define os parâmetros da eleição, como a data de abertura e fecho das urnas, bem como o tipo de eleição (i.e. uso de voto reversível).

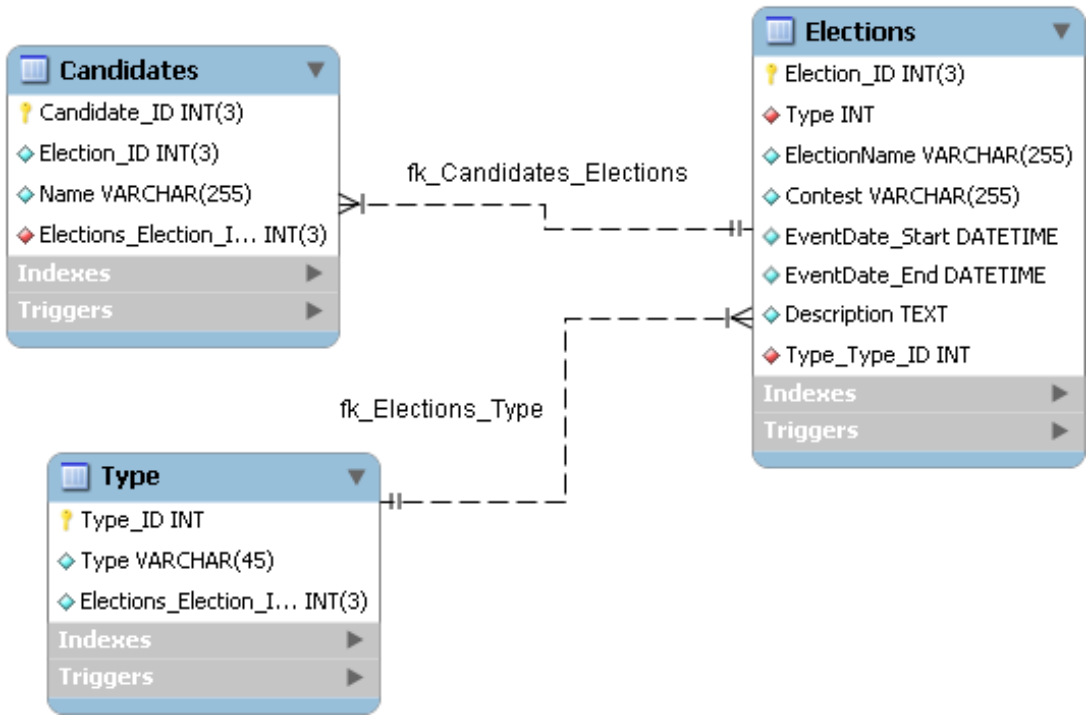


Ilustração 26 - *Schema* da Elections_DB

Votes_DB:

A base de dados "*Votes_DB*" é a base de dados onde ficam guardados os votos válidos submetidos durante a votação.

No processo de contagem, analisam-se e confrontam-se esses dados da base de dados com os votos guardados no repositório de dados no formato XML/EML. Para haver garantias que os votos não foram alterados, valida-se o *checksum* do documento EML e dos dados da base de dados, para além disso, o servidor de base de dados de votos e o repositório de votos deverão ser servidores distintos.

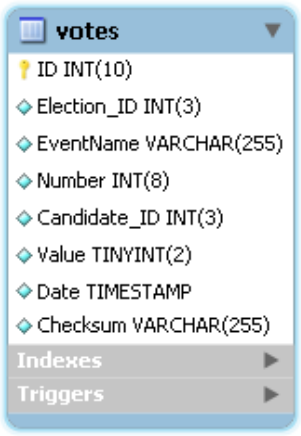


Ilustração 27 - *Schema* da Votes_DB

Voters_DB:

A base de dados "*Voters_DB*" é responsável pelo processo de autenticação do eleitor, é também através dessa base de dados que são definidos os mecanismos de tentativas ilegais de acesso.

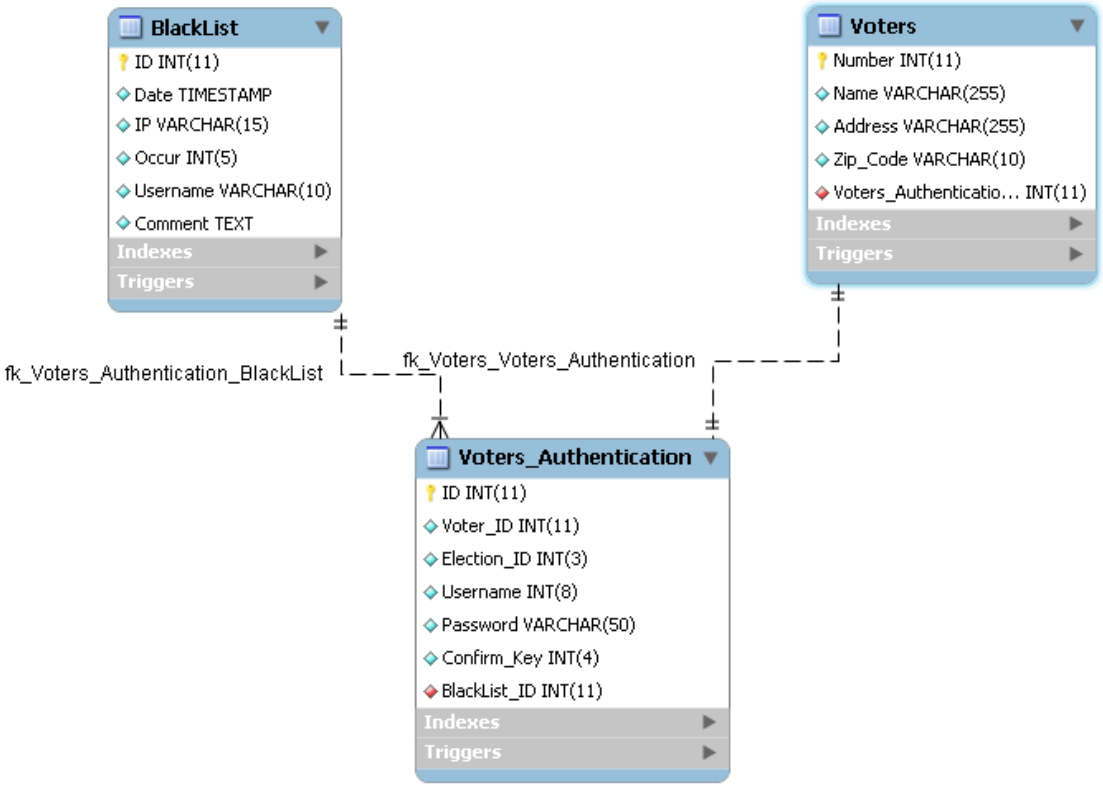


Ilustração 28 - *Schema* da Voters_DB

5.6 Descrição do Funcionamento

O protótipo funciona em três fases, a nível de *backoffice antes* e *após* a eleição, para a preparação das eleições e contagem dos votos, e a nível de *frontoffice, durante* a votação propriamente dita.

5.6.1 Antes da eleição

Antes da eleição, há trabalho de *backoffice* de preparação das eleições. São nessa fase criadas as eleições e definidos os meios para a autenticação.

Durante o processo de preparação das eleições, são criados os mecanismos de autenticação dos eleitores. Para os eleitores válidos para o acto eleitoral, que estão previamente registados no sistema através dos mecanismos de recenseamento eleitoral, são criados conjuntos aleatórios, de *username*, *password* e *pin*, não sequenciais. Esses conjuntos são enviados para a morada do eleitor e apenas permitem votar num acto eleitoral. Durante o acto de votar, não há nenhuma associação entre o *username* e a identificação real do eleitor.

É também nesta fase que se faz a escolha do tipo de eleição, o sistema permite dois tipos de eleição: voto "reversível" e votação única. O voto reversível permite que eleitor possa votar quantas vezes desejar, sendo válido o último voto, no entanto na utilização destes casos apenas é útil em cenários de votação antecipada, para não ser sobreposto ao voto presencial. No caso, do voto único, o eleitor apenas pode votar uma única vez por acto eleitoral.

5.6.2 Durante a Votação

O eleitor *navega* com um *Web browser* para uma página *Web*. Ao chegar à pagina do SVE, depara-se com um mecanismo de autenticação, Ilustração 29, onde terá que inserir o *username* e *password*, bem como um terceiro valor gerado aleatoriamente. O objectivo é bloquear tentativas de acesso ilegais ao sistema. Como o *username* é aleatório e não sequencial, associado a uma terceira validação numérica, torna-se bastante difícil ocorrer acessos indevidos por *força bruta*, pela descoberta das

combinações. O sistema também deverá registar todas as tentativas de acesso falhadas, de modo a que seja possível bloquear *usernames* e endereços IP que estejam a fazer várias tentativas de acesso ilegais.

Como o sistema estará disponível antes do acto eleitoral, propriamente dito, para ser experimentado pelos eleitores, minimiza-se o risco de erros causados pela aprendizagem do sistema e pelo bloqueio de contas por erros na introdução da *password*. Durante, essa fase ainda será possível requisitar novos dados para acesso, para os casos de extravio e bloqueio das contas.

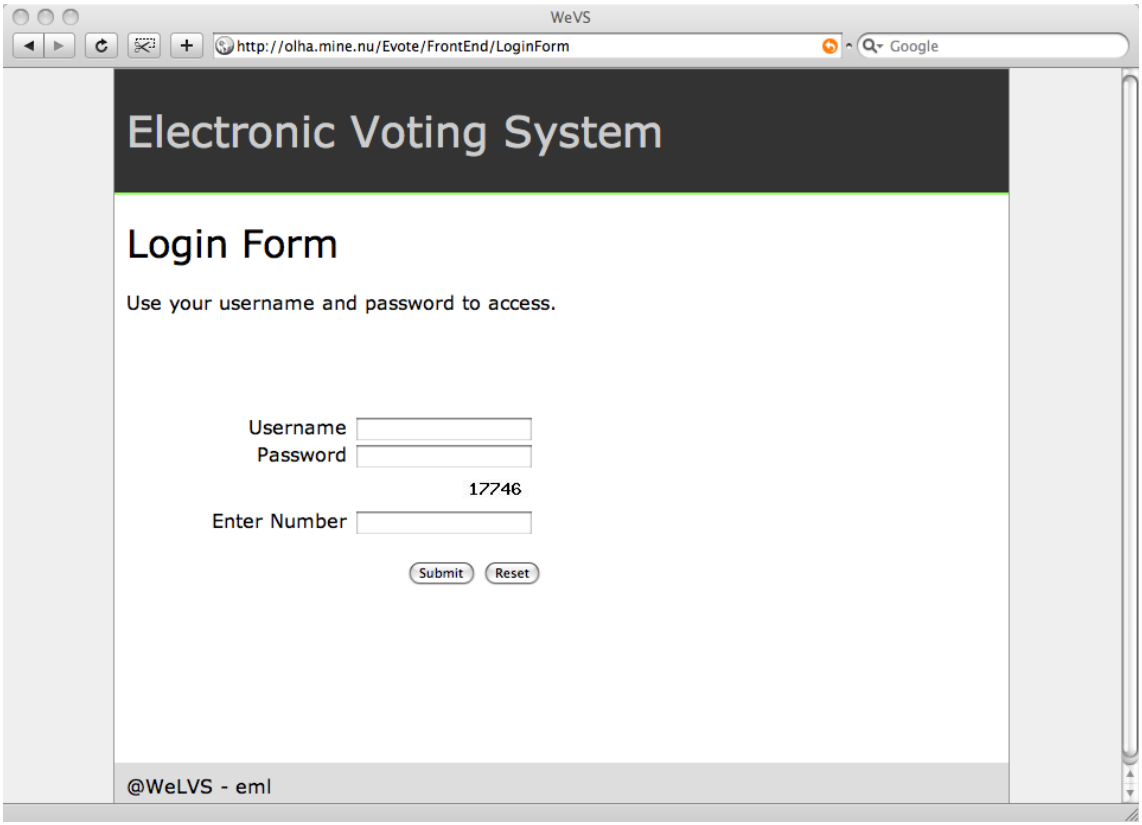


Ilustração 29 – *Snapshot* Autenticação

Depois de autenticado no *Web Service* responsável pela validação, o eleitor depara-se com a eleição e a escolha dos candidatos (Ilustração 30), faz a sua escolha e submete o voto. Seguidamente é pedido para confirmar o voto (Ilustração 31) com o *PIN*, que recebeu antes da eleição e apenas válido durante a eleição actual.

Se o *PIN* for válido, o voto é submetido e guardado num arquivo EML/XML devidamente assinado e também cifrado numa base de dados.

Na base de dados, guarda-se o *username* encriptado, o voto e um *checksum* de ambos os valores.

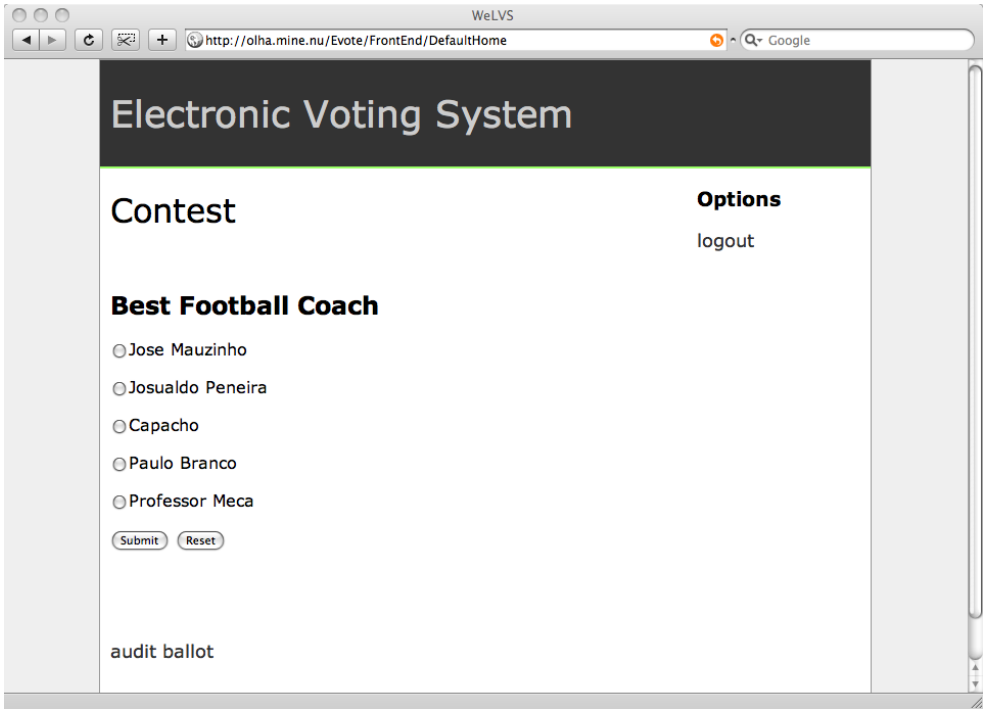


Ilustração 30 – *Snapshot* Eleição

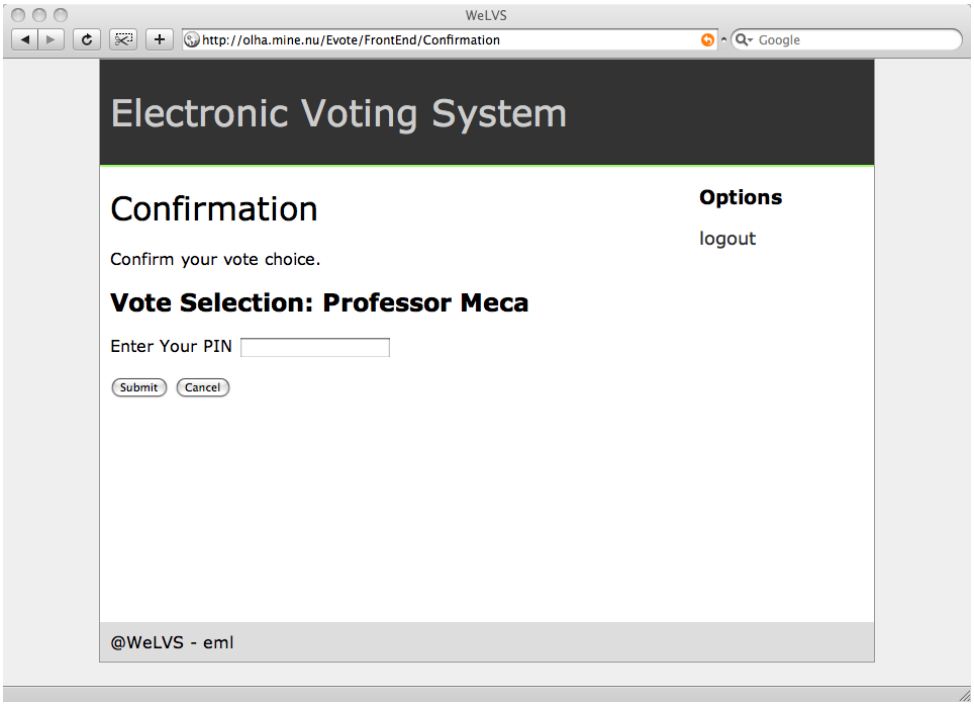


Ilustração 31 - *Snapshot* Confirmação do Voto

5.6.3 Após a eleição

Após o fecho das urnas, são calculados os resultados da eleição através da contagem dos votos válidos. Durante a contagem, validam-se os ficheiros XML, bem como os votos guardados na base de dados.

Seguidamente, os resultados são disponibilizados num ficheiro XML como mostra a Ilustração 32.

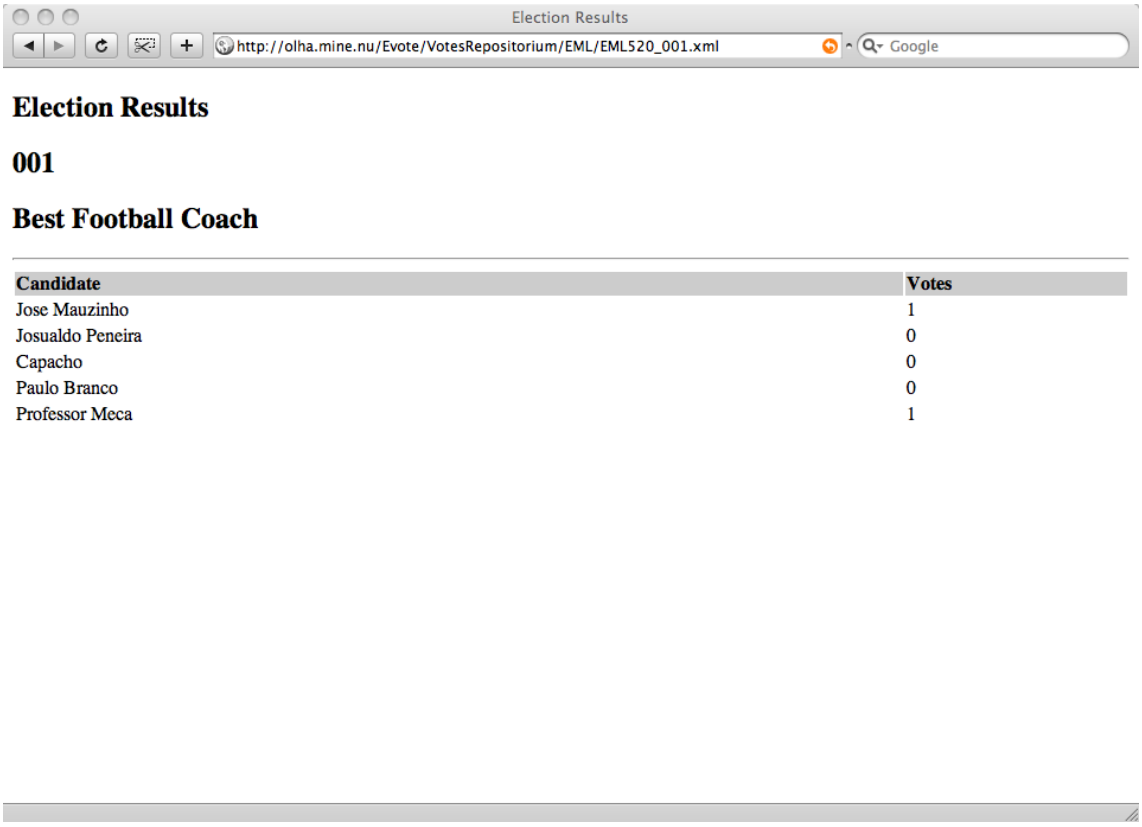


Ilustração 32 – *Snapshot* Resultados

5.7 EML

No inicio do desenvolvimento deste trabalho, recorreu-se a *bind compilers* para a criação das mensagens EML, com o decorrer do desenvolvimento optou-se por usar o *DOM API*. A utilização de *bind compilers* estava a mostrar-se complexa devido a erros no *bind* dos *schemas* com o JABX. Por esse motivo optou-se por programar todas as mensagens EML, sem recorrer a *xml binding*, para além disso, abandonou-se todo o

trabalho desenvolvido em Java e recomeçou-se tudo com a linguagem PHP. A linguagem PHP não possui mecanismos para lidar com *xml Schemas*.

De seguida apresentam-se algumas das principais mensagens EML utilizadas no protótipo do SVE:

Autenticação: Exemplo da mensagem devolvida após serem submetidos as credenciais de acesso e essas terem sido aceite pelo *Web Service* de autenticação:

<Authenticationxmlns="urn:oasis:names:tc:evs:schema:eml">
<VToken>
<ComponentType="PersonalIdNumber"/>
</VToken>
</Authentication>

Boletim: Exemplo do boletim disponibilizado depois de o eleitor estar autenticado

Source of http://olha.mine.nu/Evote/BallotServerWS/createBallot?election_ID=001

```
<?xml version="1.0" encoding="UTF-8"?>
<EML Id="410" SchemaVersion="5.0" xmlns="urn:oasis:names:tc:evs:schema:eml" xmlns:p1="http://www.w3.org/2000/09/xmldsig#"
xmlns:p2="urn:oasis:names:tc:ciq:xsdschema:xAL:2.0" xmlns:p3="urn:oasis:names:tc:evs:schema:eml:ts" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="xsi:schemaLocation=&amp;quot;urn:oasis:names:tc:evs:schema:eml ../../EML-v5/410-ballots-v5-0.xsd">
  <TransactionId Id="001"/>
  <Ballots>
    <EventIdentifier Id="001"/>
    <BallotChoices>
      <Candidate>
        <CandidateIdentifier Id="001"/>
        <CandidateName>Jose Mauzinho</CandidateName>
      </Candidate>
      <Candidate>
        <CandidateIdentifier Id="002"/>
        <CandidateName>Josualdo Peneira</CandidateName>
      </Candidate>
      <Candidate>
        <CandidateIdentifier Id="003"/>
        <CandidateName>Capacho</CandidateName>
      </Candidate>
      <Candidate>
        <CandidateIdentifier Id="004"/>
        <CandidateName>Paulo Branco</CandidateName>
      </Candidate>
      <Candidate>
        <CandidateIdentifier Id="005"/>
        <CandidateName>Professor Meca</CandidateName>
      </Candidate>
    </BallotChoices>
  </Ballots>
</EML>
```

Confirmação do Voto: Exemplo da confirmação do Voto

Source of http://olha.mine.nu/Evote/VotesRepositorium/CastVote?ID=12

```
<?xml version="1.0" encoding="UTF-8"?>
<EML xmlns="urn:oasis:names:tc:evs:schema:eml" Id="440" SchemaVersion="5.0" xmlns:p1="http://www.w3.org/2000/09/xmldsig#"
xmlns:p2="urn:oasis:names:tc:ciq:xsdschema:xAL:2.0" xmlns:p3="urn:oasis:names:tc:evs:schema:eml:ts" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="xsi:schemaLocation=&quot;urn:oasis:names:tc:evs:schema:eml ../../EML-v5/440-castvote-v5-0.xsd">
  <TransactionId Id="12"/>
  <CastVote>
    <EventIdentifier Id="001">
      <Contest>
        <ContestIdentifier Id="001">
          <Selection>
            <CandidateIdentifier Id="005"/>
          </Selection>
        </ContestIdentifier>
      </Contest>
    </EventIdentifier>
  </CastVote>
</EML>
```

Resultados: Exemplo dos resultados de uma votação

Source of http://olha.mine.nu/Evote/VotesRepositorium/EML/EML520_001.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet href="EML520_Result.xsl" type="text/xsl"?>
<EML Id="520" SchemaVersion="5.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="xsi:schemaLocation=&quot;urn:oasis:names:tc:evs:schema:eml ../../EML-v5/520-result-v5-0.xsd">
  <TransactionId Id="2008.01.15"/>
  <Result>
    <Election>
      <ElectionIdentifier Id="001">
        <Contest>
          <ContestIdentifier Id="Best Football Coach"/>
          <Selection>
            <CandidateIdentifier Id="001">
              <CandidateName>Jose Mauzinho</CandidateName>
            </CandidateIdentifier>
            <Votes>1</Votes>
          </Selection>
          <Selection>
            <CandidateIdentifier Id="002">
              <CandidateName>Josualdo Peneira</CandidateName>
            </CandidateIdentifier>
            <Votes>0</Votes>
          </Selection>
          <Selection>
            <CandidateIdentifier Id="003">
              <CandidateName>Capacho</CandidateName>
            </CandidateIdentifier>
            <Votes>0</Votes>
          </Selection>
          <Selection>
            <CandidateIdentifier Id="004">
              <CandidateName>Paulo Branco</CandidateName>
            </CandidateIdentifier>
            <Votes>0</Votes>
          </Selection>
          <Selection>
            <CandidateIdentifier Id="005">
              <CandidateName>Professor Meca</CandidateName>
            </CandidateIdentifier>
            <Votes>1</Votes>
          </Selection>
        </Contest>
      </ElectionIdentifier>
    </Election>
  </Result>
</EML>
```

5.8 Web Services

Os *Web Services* juntamente com o XML desempenham um papel fundamental no SVE ao tornar possível a comunicação entre os subsistemas e ao mesmo tempo tornam possível criar um sistema distribuído e transparente (assente em mensagens claras).

Cada um dos subsistemas que constitui o SVE proposto tem pelo menos um *Web Service* associado, existem *Web Services* para autenticação dos votantes, para disponibilizar boletins, para a confirmação do voto e para submissão e registo do voto.

De seguida apresenta-se o WSDL[13] do *Web Service* responsável pela autenticação, os restantes WSDL dos *Web Services* encontram-se disponíveis no sítio da Web do SVE: ver nos anexos.

Source of http://olha.mine.nu/Evote/AuthenticationWS/login.wsdl

```
<?xml version='1.0' encoding='UTF-8'?>

<!-- WSDL file generated by Zend Studio. -->

<definitions name="auth" targetNamespace="urn:auth" xmlns:typens="urn:auth" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns="http://schemas.xmlsoap.org/wsdl/">
        <message name="doLogin">
                <part name="username" type="xsd:string"/>
                <part name="password" type="xsd:string"/>
        </message>
        <message name="doLoginResponse">
                <part name="doLoginReturn" type="xsd:string"/>
        </message>
        <portType name="LoginUserPortType">
                <documentation>
                        this is a AuthenticationWS
                </documentation>
                <operation name="doLogin">
                        <documentation>
                                The LoginUser function
                        </documentation>
                        <input message="typens:doLogin"/>
                        <output message="typens:doLoginResponse"/>
                </operation>
        </portType>
        <binding name="LoginUserBinding" type="typens:LoginUserPortType">
                <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
                <operation name="doLogin">
                        <soap:operation soapAction="urn:LoginUserAction"/>
                        <input>
                                <soap:body namespace="urn:auth" use="encoded" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
                        </input>
                        <output>
                                <soap:body namespace="urn:auth" use="encoded" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
                        </output>
                </operation>
        </binding>
        <service name="authService">
                <port name="LoginUserPort" binding="typens:LoginUserBinding">
                        <soap:address location="http://olha.mine.nu/Evote/AuthenticationWS/wsLogin.php"/>
                </port>
        </service>
</definitions>
```

Ilustração 33 - WSDL do *Web Service* autenticação

5.9 Síntese

A solução apresentada neste trabalho apresenta um protótipo de um SVE de votação remota, desenvolvido tento por base a linguagem XML e assente sobre uma plataforma

[13] WSDL (Web Services Description Language) – são as especificações do *Web Service* escritas em XML. W3C sobre o WSDL: http://www.w3.org/TR/wsdl

de *Web Services.* Utiliza o *workflow* e as mensagens definidas pelas *schemas* EML para a comunicação entre os diversos subsistemas que constituem o SVE.

Esta proposta apresenta vantagens pela utilização dessas tecnologias tais como:

- Sistema *Always On*: por ser distribuído;
- Balanceamento de carga: permite a distribuição de carga por diversos servidores;
- Transparente: baseado em *standards*, xml e ferramentas *Open Source*;
- Utilização Remota (via *Web browser*);
- Partilha do mesmo sistema por várias eleições (simultâneas ou não);
- Separação de papéis dos subsistemas e consequentemente a transparência.

6 Avaliação

Neste capítulo é apresentado a avaliação global do sistema proposto, primeiro pretende-se determinar se os objectivos propostos foram cumpridos e depois se as propriedades definidas no capítulo 2.2 são respeitadas.

Na segunda parte da avaliação, recorre-se à utilização de um cenário prático, simulado, com eleitores reais e com uma eleição fictícia. Os votantes utilizam o sistema desenvolvido e no final dá-se uma breve explicação do sistema e pede-se para darem uma apreciação global do sistema. Utiliza-se a avaliação desses indivíduos para avaliar se os objectivos foram cumpridos.

6.1 Avaliação das propriedades do Sistema

Na Tabela 7 representam-se as propriedades [Cranor, et al., 1997]que o SVE deverá cumprir e a abordagem do protótipo. Para realizar essa avaliação, foi-se o mais rigoroso possível e descreve-se o resultado dessa avaliação.

Tabela 7 - Avaliação do Protótipo

Propriedade	**Protótipo: cumpre**	**Descrição**
Exactidão	Sim	Existem mecanismos para impossibilitar a alteração de votos válidos;
Democracia	Sim	Cada eleitor apenas pode votar uma única vez;
Privacidade	Parcialmente	Ninguém consegue provar em quem votou, no entanto é possível recorrendo a sistemas de captura de ecrã gravar o acto de votar;
Verificável	Não	O voto após ser submetido e o

		utilizador ser informado que o voto foi contabilizado não existe maneira de o eleitor ter garantias que o voto foi contado durante o processo de contagem dos resultados. Ou seja, não existem mecanismos durante o processo de contagem para garantir que ao eleitor em particular que o seu voto foi contado correctamente.
Conveniência	Sim	O sistema é fácil de usar e não requer equipamento adicional para além do computador e acesso à rede.
Flexibilidade	Parcialmente	O boletim é um documento xml/eml e está optimizado para *Web*, no entanto é possível preparar o boletim para outros formados.
Mobilidade	Sim	O sistema funciona através da Web, a partir de qualquer lado com uma ligação à Web é possível votar;

6.2 Operacional

Para a realização da avaliação pegou-se na amostra de 3 indivíduos entre os 25 e 35 anos, da classe média, com formação superior (em áreas diversas como a engenharia física, engenharia informática e artes plásticas) para usarem o protótipo. Foi também explicado o funcionamento do SVE e, também, foi-lhes dado acesso ao código fonte da aplicação. No final, foi pedido para responderem se votariam através da *Web* e para darem uma opinião em relação ao sistema que utilizaram.

Claramente, esta amostra não representa o universo de eleitores portugueses, também não é esse o objectivo principal. Por outro lado, são excelentes candidatos, por representarem a faixa etária tradicionalmente desmotiva perante o acto eleitoral e por serem utilizadores com conhecimentos de tecnologias de informação.

O primeiro indivíduo, é licenciado em engenharia informática, trabalha como programador *Web*. Apesar dos potenciais riscos da Intranet, afirma que usaria o sistema para votar. Declara que como o "*sistema é distribuído e seria desenvolvido/mantido por pessoas diferentes, e, a possibilidade do código ser libertado para domínio público para análise são vantagens que dão confiança no sistema*".

O outro indivíduo, licenciado em engenharia física, trabalha como administrador de sistemas/redes, afirma que votaria pela *Web* "*pela comodidade de não ter de se deslocar à assembleia de voto*". Por outro lado, não considera importante o desenvolvimento do sistema por diversas organizações, desde que o usem *standards* e mecanismos de segurança, como "*sistemas robustos, firewalls e mecanismos de encriptação"*, afirma ainda que considera que o desenvolvimento por diversos organismos não traria vantagens, "*aumentaria o custo do sistema e não traria vantagens significativas*".

O terceiro indivíduo, licenciado em artes plásticas, trabalha como professora de artes e designer gráfica *freelancer*, possui conhecimentos básicos de informática na óptica do utilizador. Como é utilizadora de sistemas bancários (*home banking*) não vê problemas em usar a votação pela *Web*. Faz uma pergunta interessante: "s*e posso movimentar e fazer investimentos com o meu banco na Internet, porque é que não posso votar?*". Em relação à aplicação que utilizou, diz que deveria ter explicações dos passos a serem dados pelos utilizadores com menos conhecimentos de informática, bem como ter "*cores mais apelativas*". Também, não vê vantagens na utilização do terceiro valor aleatório inicial no mecanismo de autenticação, ou na disponibilização do código fonte para domínio público: "*a maioria as pessoas não percebem nada de programação*".

De modo geral, os objectivos propostos foram cumpridos, o SVE é móvel, distribuído, anónimo, utiliza *standards* como o EML e é está perfeitamente preparado para responder aos desafios do levantamento dos requisitos relativos à realidade Portuguesa, bem como o respeito pelos direitos fundamentais do homem e às recomendações do

Concelho da Europa perante o voto electrónico, uma vez que na base do seu desenvolvimento está o exemplo Suíço de Genebra.

7 Conclusão

A implementação e desenvolvimento de SVE é um processo bastante complexo, que envolve áreas multidisciplinares (sociologia, informática, antropologia, direito) e a sua utilização é processo que envolve alterações profundas de métodos e de conceitos já interiorizados.

Nesse processo de mudança do sistema de votação tradicional para o electrónico é necessário criar condições de modo a que os eleitores conheçam o SVE e tenham confiança nele e que sejam garantidos os direitos fundamentais das eleições livres e justas.

Uma das formas para criar a confiança nos SVE e garantir alguma independência é recorrer a *standards* e tecnologias *Open Source*. O Concelho da Europa recomenda a utilização de *standards* como o EML na implementação dos Sistemas de Votação Electrónicos. O EML permite não entregar todo o SVE a uma única organização, podendo ficar distribuído em diversos subsistemas desenvolvidos por diversas companhias e que interagem entre si através de interfaces claros definidos no EML. Por outro lado deve-se seguir uma estratégia de implementação passo-a-passo (como a Suíça) para o êxito duradouro do voto electrónico.

O investimento num SVE pode ser rentabilizado ao recorrer com maior frequência à opinião dos cidadãos para assuntos mais delicados, com referendos. Dessa forma aumenta-se a participação dos eleitores nas decisões políticas e consegue-se combater a apatia e desinteresse sobre a política que caracterizam as democracias ocidentais.

Existem inúmeras vantagens do uso de sistemas de votação electrónica fase aos tradicionais sistemas de votação, tais como:

- Rapidez no apuramento de resultados;
- Custo;
- Mobilidade;
- Período de voto alargado (a custo reduzido).

7.1 Trabalho Futuro

O objectivo proposto foi maioritariamente comprido, no entanto ainda há algum trabalho a ser feito para desenvolver um sistema de votação robusto, seguro e confiável.

Continuar o desenvolvimento do protótipo, incluindo o desenvolvimento de outros subsistemas que não foram contemplados nesta fase, como o recenseamento dos votantes, e a candidatura de candidatos e partidos.

O protótipo também deve ficar preparado para suportar integralmente diversos canais de voto e ser possível de parametriza-lo para ser utilizado em diversos cenários de votação: tais como eleições locais, nacionais, referendos e eleições privados.

Deverá ser incluído no desenvolvimento novas funcionalidades de segurança, com a adopção de dados pessoais na validação do voto, recurso a cartões matriz e a sistemas de certificação como assinaturas digitais.

Também é necessário implementar mecanismos para auditar o sistema, recorrendo aos *logs* gerados pelo *Web Server*, documentos EML trocadas e base de dados.

Bibliografia

Aas, Patricia. 2005. *Evaluating the suitability of EML4.0 for the Norwegian Electoral System.* s.l. : University of Oslo, 2005.

Ambler, Scott W. 2001. *The Object Primer 2 Edition.* s.l. : Cambridge University Press, 2001.

Antunes, Pedro; Monteiro, Américo; Soares, Natércia; Oliveira, Rosa Maria. 2001. *Sistemas Electrónicos de Votação.* [Portable Document Format] Lisboa : Departamento de Informática, Faculdade de Ciências da Universidade de Lisboa, 2001.

Apache. 2007. XMLBeans Schema Tools. *XMLBeans Schema Tools.* [Online] Apache, 08 28, 2007. [Cited: 08 2007, 30.] http://www.xmlbeans.org/.

Assembleia da Republica - Lei Eleitoral. 1979. *Lei Eleitoral.* [Portable Document Format] 1979.

Assembleia da República. 1999. *Regime jurídico do recenseamento eleitoral - Lei 13/99, 22 Março* . [Portable Document Format] Lisboa : s.n., 1999.

Booch, Grady, Rumbaugh, James and Jacobson, Ivar. 1998. *The Unified Modeling Language User Guide.* s.l. : Addison-Wesley Object Technology Series, 1998.

Borras, John. 2002. *Overview of the work on e-voting technical standards.* [Portable Document Format] s.l. : Cabinet Office, UK Government, 2002.

Codd, Edgar F. 1970. *A relational Model of Data for Large Shared Data Banks.* s.l. : Communications of the ACM, 1970.

Commission on Electronic Voting. 2006. *Second Report of the Commission on Electronic Voting.* s.l. : Government of Ireland, 2006.

Council of Europe - Committee of Ministers. 2004. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. *CoE.* [Online] CoE, 09 30, 2004. [Cited: 08 22, 2007.] https://wcd.coe.int/ViewDoc.jsp?id=778189.

Council of Europe - Ministers' Deputies. 2005. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society. *Council of Europe.* [Online] Council of Europe, 05 13, 2005. [Cited: 06 09, 2007.] https://wcd.coe.int/ViewDoc.jsp?id=849061&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

Council of Europe. 2007. *Council of Europe Symposium on e-democracy.* Strasbourg : s.n., 2007.

Cover, Robin. 2004. Election Markup Language (EML) Recommended to Member States by Council of Europe. *Cover Pages.* [Online] 11 10, 2004. [Cited: 06 05, 2007.] http://xml.coverpages.org/ni2004-11-10-a.html.

Cranor, Lorrie Faith and Cytron, Ron K. 1997. A Security-Conscious Electronic Polling. *Proceedings of the 30th Hawaii International Conference on System Sciences: Information System Track-Organizational Systems and Technology - Volume 3* . Washington, DC, USA : IEEE Computer Society, 1997.

Dessislava, Vassileva and Boyan, Bontchev. 2003. CEVS – A Corporative E-voting System Based on EML. *Computer and Information Sciences - ISCIS 2003.* s.l. : Springer Berlin / Heidelberg, 2003.

Dieterich, Ernie. 2004. Direct Recording Electronic Voting Systems. *League Issues.* [Online] 04 2004. [Cited: 08 14, 2007.] http://www.leagueissues.org/tutorial.html.

Dill, David L.; Mercuri, Rebecca; Neumann, Peter G.; Wallach, Dan S. Frequently Asked Questions about DRE Voting Systems. *Verified Voting.* [Online] [Cited: 07 17, 2007.] http://www.verifiedvoting.org/article.php?id=5018.

Electronic voting and counting. 2006. Electronic voting and counting. [Online] ACT Electoral Commission, 10 05, 2006. [Cited: 08 17, 2007.] http://www.elections.act.gov.au/Elecvote.html.

European Communities. 2004. EU: E-voting systems must be based on open standards, says Council of Europe. *IDABC.* [Online] European Communities, 10 20, 2004. [Cited: 06 10, 2007.] http://ec.europa.eu/idabc/en/document/3294/330.

Gritzalis, Dimitris A. 2002. *Principles and requirements for a secure e-voting system.* [Portable Document Format] s.l. : Elsevier Science Ltd, 2002.

Hall, Joseph Lorenzo. 2006. Transparency and Access to Source Code in E-Voting. s.l. : USENIX/ACCURATE Electronic Voting Technology Workshop Working Paper Available at SSRN: http://ssrn.com/abstract=909582 , 2006.

Houston, Houston L.; Yao, Yurong; Okoli, Chitu; Watson, Edward. 2005. *Will remote electronic voting systems increase participation?* [Portable Document Format] s.l. : Electronic Government, an International Journal, 2005.

Internet Policy Institute. 2001. *Report of Nacional Workshop on Internet Voting.* [Portable Format Document] 2001.

Kitcat, Jason. 2006. National Institute of Standards & Technology says e-voting machines cannot be made secure. *Jason Kitcat e-voting.* [Online] 10 30, 2006. [Cited: 08 18, 2007.] http://www.j-dom.org/?be_id=321.

Maaten, Epp. 2006. *Estonia 2005 the first practice of Internet voting.* [PowerPoint Presentention] Strasbourg : Councillor of the Elections Department, Chancellery of the Riigikogu, 2006.

Mercuri, Rebecca. 2007. Electronic Voting. *Notable Software.* [Online] Notable Software, Inc, 03 15, 2007. [Cited: 08 18, 2007.] http://www.notablesoftware.com/evote.html.

Mertz, David. 2004. XML Matters: OASIS Election Markup Language. [Online] Bean Counter, Gnosis Software, Inc, 10 15, 2004. [Cited: 05 06, 2007.] http://www-128.ibm.com/developerworks/library/x-matters38.html.

OASIS. 2007. *The Case for using Election Markup Language (EML).* [Portable Document Format] 2007. http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/00_e-voting_news/Case%20for%20EML.pdf.

Ort, Ed and Mehta, Bhakti. 2003. Java Architecture for XML Binding (JAXB). *Sun Developer Network.* [Online] Sun, 03 2003. [Cited: 06 18, 2007.] http://java.sun.com/developer/technicalArticles/WebServices/jaxb/.

Republique et Canton de Geneve. The Geneva Internet voting system. *Site officiel de l'Etat de Genève.* [Online] [Cited: 05 06, 2007.] http://www.geneve.ch/e-voting.

Rubin, Avi. 2001. Security Considerations for Remote Electronic Voting over the Internet. *Avi Rubin.* [Online] 2001. [Cited: 08 18, 2007.] http://avirubin.com/e-voting.security.html.

Safevote Inc. 2006. Internet Voting FAQ. *Safevote.* [Online] Safevote Inc., 2006. [Cited: 08 18, 2007.] http://safevote.com/internetvoting.htm.

Schneier, Bruce. 2004. The Problem with Electronic Voting Machines. *Schneier on Security.* [Online] 10 10, 2004. [Cited: 08 17, 2007.] http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html.

Shamos, Michael Ian. 2004. Paper v. Electronic Voting Records – An Assessment. *14th ACM Conf. on Computers, Freedom & Privacy, Berkeley, CA.* 2004.

Silva, Alberto and Videira, Carlos. 2001. *UML, Metodologias e Ferramentas Case.* s.l. : Edições Centro Atlântico, 2001. ISBN 972842636-4.

Stephen, Mason. 2004. Is there a future for Internet voting? s.l. : Science Direct (Elsevier), 2004.

Sumra, Rajesh. 2003. Developing JAX-RPC–Based Web Services Using Axis and SOAP. *developer.com.* [Online] 03 18, 2003. [Cited: 1 2008, 6.] http://www.developer.com/java/web/article.php/2237251.

Svensson, Jörgen and Leenes, Ronald. 2003. *E-voting in Europe: Divergent democratic practice.* s.l. : IOS Press, 2003.

The National Election Committee. 2005. *E-Voting System: Overview.* [Portable Document Format] Tallinn : s.n., 2005. http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf.

The Risk of e-Voting. **Lauer, Thomas W. 2004.** Issue 1, s.l. : Electronic Journal of e-Government, 2004, Vol. Volume 2.

TRE-MG. 2006. A Informatização do voto no Brasil. *Tribunal Regional Eleitoral.* [Online] Tribunal Regional Eleitoral, 2006. [Cited: 05 06, 2007.] http://www.tre-mg.gov.br/urna_eletronica/historico_voto_elet/voto_eletronico2.htm.

TRE-SP. Voto passo a passo. *Tribunal Regional Eleitoral de São Paulo.* [Online] Tribunal Regional Eleitoral de São Paulo. [Cited: 09 30, 2007.] http://www.tre-sp.gov.br/urna/voto.htm.

Tribunal Regional Eleitoral. Como votar na urna eletrônica . *Tribunal Regional Eleitoral.* [Online] Tribunal Regional Eleitoral. [Cited: 05 06, 2007.] http://www.tre-mg.gov.br/urna_eletronica/imagens_da_urna_eletronica2tri.htm.

UMIC. 2005. Projecto Voto Electrónico. *Voto Electrónico.* [Online] Agência para a Sociedade do Conhecimento, 2005. [Cited: 05 06, 2007.] http://www.votoelectronico.pt/.

Unicamp. 2002. *Avaliação do Sistema Informatizado de Eleições.* 2002.

Anexos

INSTALAÇÃO DO PROTÓTIPO E HIPERLIGAÇÕES ÚTEIS

No CD encontra um arquivo com o protótipo do SVE proposto, em alternativa poderá descarregar a última versão em http://webpages.fc.ul.pt/~pjbastos/Evote

No *Web Site* http://olha.mine.nu/Evote encontra-se uma versão de demonstração

Dados para acesso:
Username: guest
Password: mestrado

REQUESITOS

1. Apache

No httpd encontrar as referências e alterar para:

Options Indexes MultiViews

AllowOverride All

2. PHP (5)

O php precisa de ser compilado com o módulo *soap enable (--with-soap)* e DOMXML (normalmente vêm por omissão em todas as instalações)

Verificar o ficheiro php.ini para ficar assim:

[soap]

soap.wsdl_cache_enabled = "1"
; enables or disables WSDL caching feature
soap.wsdl_cache_dir = "/tmp"
; sets the directory name where SOAP extension will put cache files
soap.wsdl_cache_ttl = "86400"

; (time to live) sets the number of second while cached file will be used
; instead of original one

3. MySQL

A versão do MySQL deve ser a 4 ou superior

INSTALAÇÃO

1. Fazer download e extrair para um directório

2. Dar permissões de escrita nos directórios:

/Evote/BallotServerWS/EML

/Evote/VotesRepositorium/EML

3. Criar base de dados

É necessária uma base de para cada componente

4. Configurações

Alterar os ficheiros *Configuration/conf.inc.php* com os dados da base de dados e URL do servidor / *Web Services*

Alterar os ficheiros .*wsdl* com o url do *Web service*

Hiperligações úteis

Download da última versão do protótipo: http://webpages.fc.ul.pt/~pjbastos/Evote

Demonstração de uma eleição: http://olha.mine.nu/Evote

EXEMPLO DE UM ATAQUE:

De acordo com [Rubin, 2001] uma das formas para ataque é forçar o utilizar a usar um Web *proxy*. O servidor de *proxy* pode controlar todos os aspectos da experiencia de navegação.

Como a maioria dos utilizadores utiliza o sistema operativo Windows e o Web browser Internet Explorer, para alterar o proxy, é algo tão simples que pode ser feito apenas com recurso a uma chave no *regedit* do Sistema Operativo Windows.

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

"ProxyServer"="<your proxy IP address>:8080"

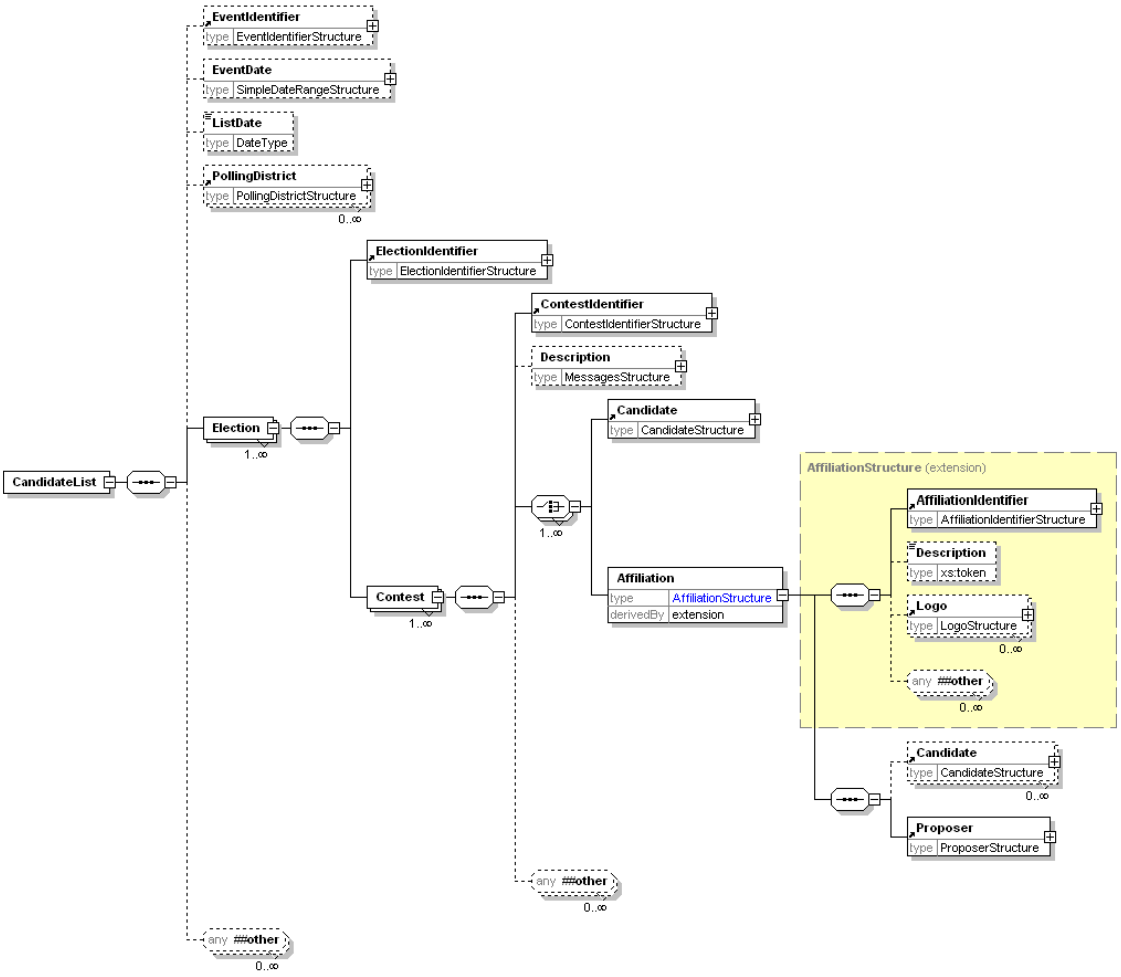
"ProxyEnable"=dword:00000001
"ProxyOverride"="<local>"

Uma das formas de prevenir que os *proxys* captem a informação confidencial é recorrer a ligações seguras SSL. No entanto, pode estar definido no *proxy* para reencaminhar o pedido do site para um site falso.

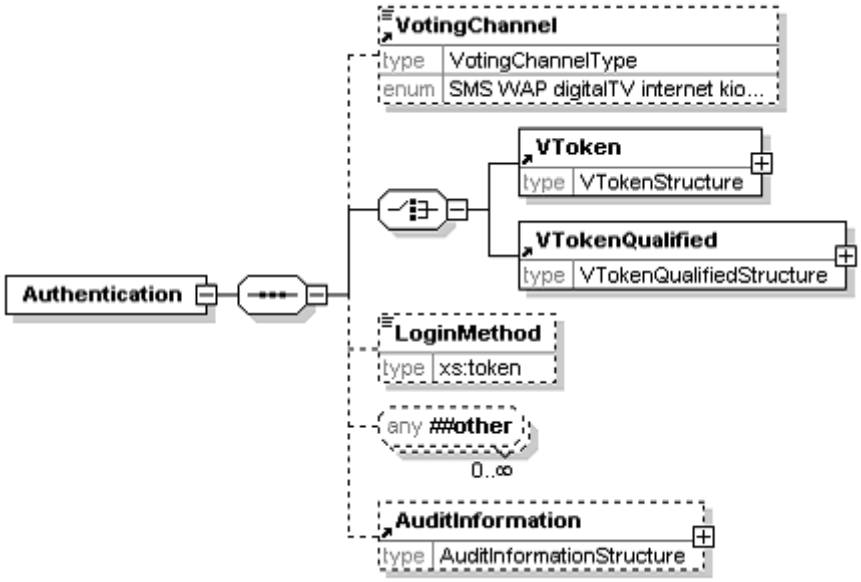
SCHEMAS EML

Alguns dos *schemas* EML utilizados no desenvolvimento do protótipo. As imagens foram retiradas do documento "*EML schema description*" que acompanha o EML.

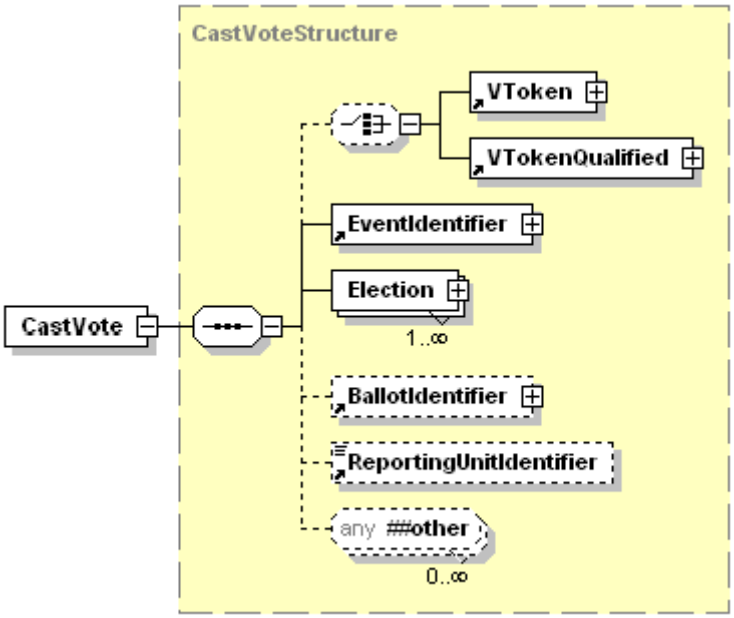
Candidate List (230)



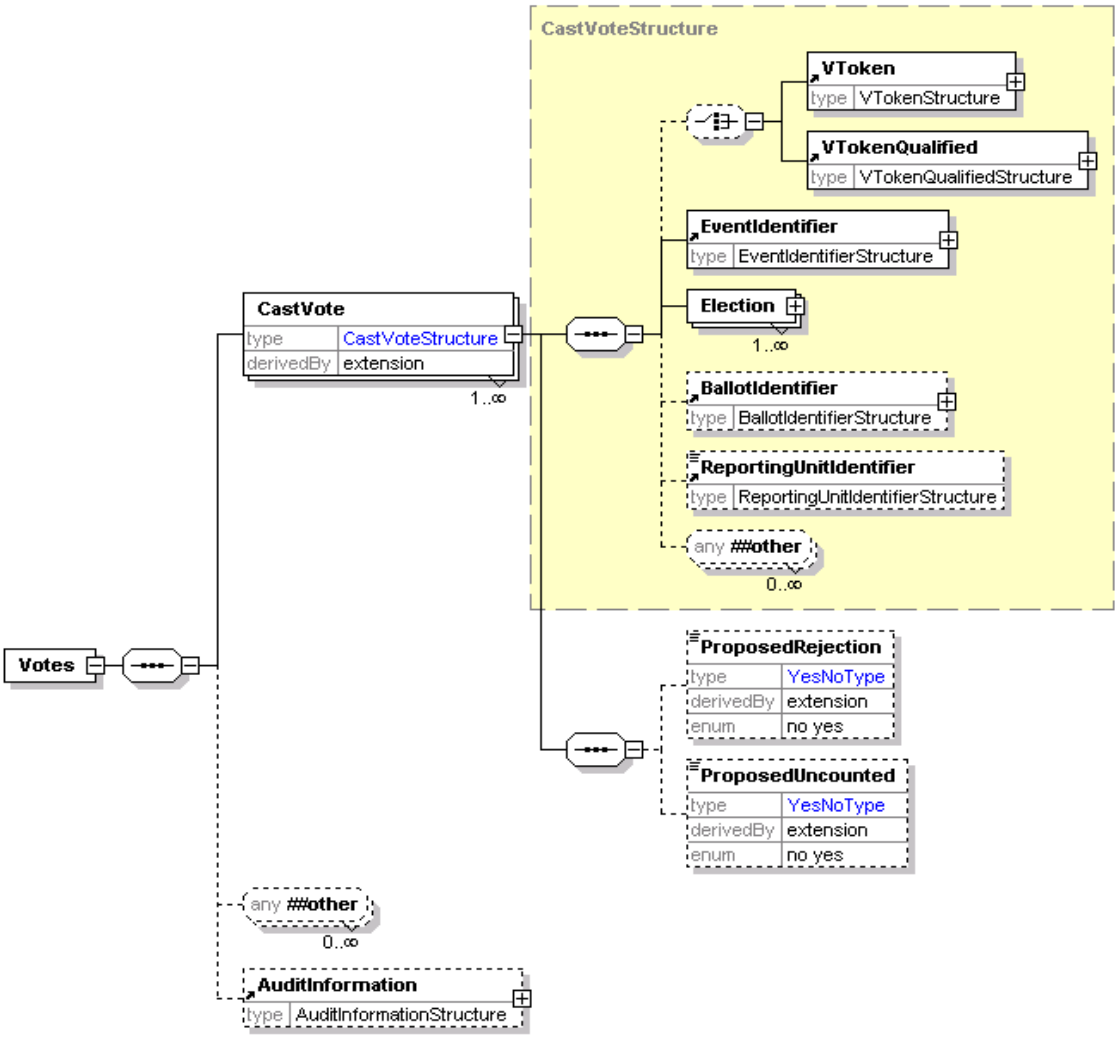
Authentication (420)



Cast Vote (440)



Votes (460)


CastVoteStructure
VToken
type VTokenStructure
VTokenQualified
type VTokenQualifiedStructure
EventIdentifier
type EventIdentifierStructure
Election
1..∞
BallotIdentifier
type BallotIdentifierStructure
ReportingUnitIdentifier
type ReportingUnitIdentifierStructure
any ##other
0..∞
CastVote
type CastVoteStructure
derivedBy extension
1..∞
Votes
ProposedRejection
type YesNoType
derivedBy extension
enum no yes
ProposedUncounted
type YesNoType
derivedBy extension
enum no yes
any ##other
0..∞
AuditInformation
type AuditInformationStructure

SIMULADOR SVE BRASILEIRO

Disponível em:

http://www.tse.gov.br/eleicoes/urna_eletronica/simulacao_votacao/UrnaApplet2.htm

Snapshot do simulador: