Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2010

JOÃO MANUEL SOUSA BAPTISTA TAVARES

VOTAÇÃO ELECTRÓNICA EM CABO VERDE

Universidade de Aveiro
2010

Departamento de Electrónica, Telecomunicações e Informática

JOÃO MANUEL SOUSA BAPTISTA TAVARES

VOTAÇÃO ELECTRÓNICA EM CABO VERDE

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações – Especialização em Sistemas de Informação, realizada sob a orientação científica do Doutor André Ventura da Cruz Marnoto Zúquete, Professor Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

Com o apoio da Cooperação Portuguesa

COOPERAÇÃO PORTUGUESA

Dedico este trabalho à minha esposa e filhas pela alegria proporcionada ao longo desta caminhada e pela compreensão das horas de ausência.

o júri

presidente	Prof. Doutor José Manuel Matos Moreira professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
arguente	Prof. Doutor Fernando Joaquim Lopes Moreira professor associado da Universidade Portucalense.
orientador	Prof. Doutor André Ventura Zúquete professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

Agradecimentos

Primeiramente à Deus pela vida que me concedeu e por mais esta conquista.

À minha querida família espalhada pelo mundo.

A todos os professores e colegas que com suas presenças e companheirismo me incentivaram e proporcionaram vários momentos de aprendizagem.

palavras-chave Sistema de votação electrónica, e-voto, voto electrónico.

resumo

A forma mais tradicional de exercício do direito ao sufrágio consiste em o próprio cidadão se dirigir às assembleias de voto, identificar-se e proceder à votação através de boletins em papel não identificados para garantir o secretismo do mesmo. As recentes tentativas de implementar um Sistema de Votação Electrónica (SVE) procuram igualmente garantir a unicidade, a autenticidade e o anonimato associados a este. Todavia, o processo de voto electrónico se revela extremamente complexo e exigente a nível de segurança.

O objectivo desse trabalho é de descrever e encontrar uma forma alternativa segura, mais eficaz e cómodo de voto, que permite aumentar a participação nos actos eleitorais Cabo-verdianos, i.e., diminuir o abstencionismo, dada a dispersão geográfica das nossas ilhas e da diáspora.

A aposta na comodidade e conforto dos cidadãos relativamente ao processo de votação através da votação electrónica, constitui uma mais valia e traduz-se em ganhos directos, proporcionados pela redução de custos dos processos eleitorais, permitindo também, de acordo com experiência internacional capitalizar a interacção com os cidadãos.

O actual código eleitoral já prevê a votação electrónica no seu Artigo 2º (Experiências de votação electrónica) que transcrevo a seguir:

"O Governo, ouvidos os partidos políticos legalmente constituídos, pode realizar experiências-piloto de votação electrónica, em um ou mais círculos eleitorais."

keywords Electronic Voting System, e-voting, electronic vote.

abstract

The most traditional form of exercise of the right to the suffrage consists of the own citizen to go to the vote assemblies, to identify and proceed to the vote through no identified paper bulletins in order to guarantee the secrecy of voting. The recent attempts to implement an Electronic Voting System seek equally to guarantee the agreement, the authenticity and anonymity related to that one. However, the process of electronic vote is revealed to be extremely complex and demanding at level of security.

The goal of that work is to describe and find a safe alternative form, more effective and suitable of voting, that allows to increase the participation in the electoral Capeverdean acts, that is, to reduce abstention, given the geographical dispersion of our islands and the community emigrated. Betting in the ease and the citizens´ comfort relatively to the voting process through the electric vote it constitutes a more value and translates direct gains, proportioned by the reduction of cost of the electoral processes, also allowing, in agreement with international experience to capitalize the interaction with the citizens.

The current electoral code already foresees the electronic voting in its Article 2nd (Experiences of electronic voting) that I transcribe in the below paragraph:

"The Government, after hearing the political parties legally constituted, can accomplish experience-pilot of electronic voting, in one or more electoral circles."

ÍNDICE GERAL

ÍNDICE DAS FIGURAS

ÍNDICE DAS TABELAS

1 – INTRODUÇÃO

1.1 - Contexto e Motivação

A construção de uma sociedade baseada na informação e no conhecimento, assim como a oposta na boa governação e dada a grande aceitação das novas tecnologias de informação e comunicação (NTIC), as mesmas podem ser vistas como facilitadores de práticas democráticas, nomeadamente no suporte ao exercício do voto.

A modernização do processo eleitoral é uma das prioridades da reforma administrativa. O projecto "ELE - Eleições [1], que permitiu o acesso centralizado às informações da base de dados nacional e o Sistema de Processamento Central de Dados Eleitorais, já está praticamente consolidado. O referido projecto foi ensaiado nas eleições autárquicas 2008 e tinha como objectivo evitar redundâncias no processo, garantir uma maior fiabilidade da informação introduzida e aumentar a confiança da sociedade no sistema eleitoral.

Em Cabo Verde, o actual governo tem implementado diversos sistemas no plano de Governação Electrónica. Verifica-se uma forte vontade política, de todos os quadrantes, para a implementação de Sistemas de Votação Electrónica uma vez que reconhecem as diversas vantagens, como dar resposta à forte abstenção, à morosidade dos processos de contagem, entre outras.

A introdução do voto electrónico, em Cabo Verde, tem que ser feita gradualmente, passando por várias fases que permitirão a aceitação do grande público e a aquisição de experiência no campo técnico da questão.

O tema "Sistema de Votação Electrónica em Cabo Verde", que irei descrever nesse trabalho, é hoje, como tal, alvo de investigação nas maiores universidades em todo mundo com ligação à ciência e tecnologia.

A motivação maior desse trabalho é de descrever e encontrar uma forma alternativa segura, mais eficaz e cómodo de voto, que permite aumentar a participação nos actos eleitorais Cabo-verdianos, i.e., diminuir o abstencionismo, dada a dispersão geográfica das nossas e da diáspora que, em eleições gerais, se têm vindo a acentuar.

1.2 - Potencialidades e Problemas

São inúmeras as potencialidades que os Sistemas de Votação Electrónica encerram sobre si. Após um investimento inicial, tais sistemas permitem uma enorme poupança de dinheiro, quer por parte da entidade organizadora da votação, quer por parte dos partidos políticos.

Para além dessa poupança, pode-se poupar-se tempo por parte da organizadora, pois, uma eleição suportada electronicamente pode ser organizada num menor intervalo de tempo do que uma eleição convencional. Por parte dos votantes, a poupança de tempo reflecte-se no facto

de não ser necessária a sua presença numa determinada assembleia de voto, uma vez que essa presença é, por vezes, sujeita a intermináveis filas de espera.

A mobilidade oferecida aos votantes é outro dos factores que constitui uma potencial vantagem considerando a insularidade das ilhas e contribuindo dessa forma pela diminuição da abstenção que se tem verificado ao longo das últimas eleições.

Contudo, existe ainda, uma falta de maturidade no desenho e desenvolvimento de sistemas de suporte à votação electrónica. Esta falta de maturidade prende-se com a complexidade inerente a um sistema deste tipo, complexidade essa que é reflectida por vários requisitos que são necessários assegurar, tais como auditabilidade, certificabilidade, confiabilidade, detectabilidade, integridade do sistema, disponibilidade, verificabilidade, privacidade, entre outros [2].

Outro dos problemas que se afigura é de natureza cultural. Numa eleição convencional, os votantes são confrontados, numa assembleia de voto, com documentos que os identificam (Bilhete de Identidade, normalmente), boletins de voto de papel, urnas de voto, representantes da entidade organizadora da eleição e de partidos políticos. No entanto, numa votação electrónica, os votantes deparam ainda com uma entidade física, um computador ou um outro qualquer dispositivo electrónico, com um inexpressivo software.

Há uma resistência social, havendo a necessidade de os votantes confiarem não só nas pessoas que implementaram o programa de software com o qual estão a interagir, mas também na própria rede de suporte, uma vez que o voto é transmitido através de uma rede de computadores insegura e susceptível de ataques.

Por outro lado, existe o problema da conveniência social. Infelizmente, muitas são as pessoas que não podem aceder às últimas tecnologias, apesar de, tal como os outros cidadãos, terem o direito a exercer o seu voto. Tal é um problema que cabe ao governo de Cabo Verde suprimir, investindo numa sociedade igual para todos e onde todos se possam sentir como uma parte da sólida democracia.

Resumindo os problemas apontados acima, posso dizer que a introdução das NTIC nos actos de cidadania levanta um conjunto de questões relacionadas com a privacidade e segurança digital [1].

A privacidade constitui um dos aspectos mais relevantes na implementação da democracia electrónica uma vez que condiciona os mais variados aspectos em termos de gestão da informação, nomeadamente a sua divulgação e partilha, e salvaguarda do uso abusivo dos dados.

A segurança digital, contempla ainda os aspectos relacionados com a integridade e confiabilidade dos dados individuais.

1.3 - Estrutura do Relatório

O presente documento, integrando um trabalho final de mestrado, encontra-se estruturado em dez grandes capítulos, sendo que no primeiro capítulo se encontra a parte introdutória que faz o enquadramento teórico, contexto e motivação, apresentando as potencialidades e os problemas de sistemas de votação electrónica.

No segundo capítulo, é apresentado uma breve revisão da literatura sobre o voto tradicional e o voto electrónico apresentando as vantagens, desvantagens e requisitos de um SVE.

No terceiro capítulo, Segurança na Votação Electrónica, é descrito algumas propriedades, ameaças e ataques assim como algumas tecnologias implementadas na segurança electrónica.

No quarto capítulo,Sistemas Actuais de Votação Electrónica, faz-se uma abordagem comparativa de alguns sistemas actuais de votação, tendo-se destacado o REVS desenvolvido em Portugal, o SENSUS no Brasil e o EVOX nos Estados Unidos.

No quinto capítulo é apresentada a Legislação Cabo-verdiana com alguns artigos do Código Eleitoral, revisto recentemente.

No sexto capítulo é apresentado um protótipo desenvolvido para as eleições presidenciais, explicando os passos necessários para o uso do mesmo.

No capítulo 7, Conclusões, é apresentado as considerações finais deste trabalho, onde são ressaltados os principais resultados e recomendações do trabalho de pesquisa realizado sobre SVE.

No capítulo 8 é apresentado as principais referências bibliográficas consultadas assim como as complementares visitadas na Internet.

Nos capítulos finais, nono e décimo, são apresentados, respectivamente, o glossário e os anexos que fazem parte desse trabalho.

2 – SISTEMA DE VOTAÇÃO ELECTRÓNICA EM CABO VERDE

O sistema que pretendo para Cabo Verde tem que permitir a máxima confiança não só aos autores políticos como também aos eleitores principalmente. O conceito de confiança tem evoluído significativamente ao longo do tempo, pelo que não tentarei dar uma definição precisa. Para a construção do referido sistema posso analisar a confiança sob as seguintes perspectivas [3]:

- Por via de instituições que garantam a confiança no sistema: autoridades legais, organizações independentes de inspecção, certificação e auditoria, empresas reputadas no desenvolvimento de sistemas.
- Pela geração de consensos na sociedade resultantes de testes, ensaios e experimentação directa do sistema.
- Pela capacidade do SVE em gerar confiança no seu funcionamento.

Descrevo aqui uma breve revisão da literatura sobre o voto tradicional e o voto electrónico apresentando as vantagens, desvantagens e requisitos de um SVE.

2.1 - Processo Eleitoral Tradicional em Cabo Verde

O processo eleitoral tradicional não tem conseguido dar resposta à forte abstenção que tem aumentando muito, em parte, devido à obrigatoriedade da votação ser feita no local de recenseamento e como podemos constatar, devido a dispersão geográfica das nossas ilhas, vários eleitores que são naturais de outras ilhas/concelhos são “obrigados” a votarem nos locais de residências.

Um dos objectivos de qualquer SVE é proporcionar um aumento das oportunidades de voto, ou seja, crie maior número de locais onde se torna possível exercer o direito de voto e não obrigatoriedade de o eleitor se apresentar nos locais de recenseamento.

Seguidamente, descrevo brevemente o processo do voto tradicional.

2.1.1 - Recenseamento

Como sabemos, o recenseamento consiste do registo, no caderno eleitoral, da pessoa que tenha as condições exigidas por lei para o processo de eleição em questão. Cada cidadão deveria receber um cartão de eleitor com um número único, no respectivo caderno, que serve de identificação, na altura da eleição. No entanto, essa entrega por parte das organizações de recenseamento, não se verificou no último recenseamento nacional o que sob ponto de vista da conformidade com a lei, constitui uma violação do artigo do Código Eleitoral [4].

2.1.2 - Validação da identificação do eleitor

A validação da identificação do eleitor é feita na altura em que o eleitor se dirige à mesa de voto e requisita o seu boletim de voto. O presidente da mesa pronuncia o nome em voz alta e

número do eleitor e os restantes elementos da mesa registam, na sua lista de eleitores, o votante. Esta fase acontece no decorrer da eleição, ao contrário da fase anterior.

O mesmo registo serve para evitar o voto múltiplo, isto é, serve para garantir a unicidade do voto (princípio democrático de uma pessoa votar uma única vez).

2.1.3 - Recolha de Votos

Após o levantamento do boletim de voto, o eleitor dirige-se à cabine de voto onde regista no boletim a sua votação para depois dobrar o boletim e dirige-se, novamente à mesa de voto onde introduz o seu boletim na urna. Termina nesta fase a participação do eleitor. Os elementos da mesa acompanham esta fase.

2.1.4 - Contagem dos votos

Esta tarefa fica a cargo dos elementos da mesa. Após o encerramento da votação, as urnas são abertas e os votos são validados, classificados e contados, sendo depois publicado o resultado da contagem.

2.2 - Votação electrónica

O voto electrónico consiste na utilização de sistemas informáticos que automatizem qualquer etapa ou processo de uma eleição (o recenseamento eleitoral, a votação, a transmissão do resultados e a publicação do resultados oficiais) [5]. Já existem várias implementações de sistemas de contagem de votos, sistemas de urnas automáticas, entre outros, nos países como Brasil, Portugal, Holanda, Suécia, etc.

O ideal para Cabo Verde, seria um sistema de votação completamente informatizado, com a possibilidade de se votar remotamente de qualquer parte (qualquer Ilha/Concelho) em que o eleitor se encontre, obviamente sem comprometer o conjunto de pressupostos que estão subjacentes a um processo eleitoral livre, não coercivo e livre de fraudes.

Posso apresentar as seguintes soluções para o processo electrónico em Cabo Verde [3]:

- Solução maximalista – consiste em replicar todos os componentes do processo tradicional em papel:
  - Mesa de Voto Electrónico – com tecnologia para a verificação do Direito de Voto recorrendo a lista de eleitores em formato digital.
  - Máquinas Electrónicas de Registo Directo – com tecnologia para permitir aos eleitores seleccionarem as suas preferências, garantindo a Privacidade.
  - Urna Electrónica – com tecnologia para registar o voto do eleitor.
- Solução intermédia – consiste em eliminar a urna:
  - Mesa de Voto Electrónico – como apresentada na solução anterior.
  - Quiosque de Votação – combinando as funcionalidades da máquina electrónica de registo directo e da urna.

- Solução minimalista – consiste em eliminar a mesa de voto electrónica, restando um único componente:
    - Quiosque de Registo do Votante e Votação – com tecnologia que combina as funcionalidades da mesa de voto, máquina de registo directo e urna.

Do ponto de vista das autoridades legais, a terceira solução é a melhor uma vez que destina-se a simplificar o processo de votação e reduzir os custos (tempo, dinheiro, logística). No entanto, esta solução pode apresentar algumas dúvidas sobre os requisitos de votação: Anonimato do voto (a autenticação do eleitor e a votação são realizados no mesmo dispositivo), Singularidade do voto (desaparecem os mecanismos visíveis que ajudem a verificar se alguém vota mais de uma vez).

Em jeito de conclusão nessa matéria de confiança, posso observar que a implementação de um SVE pode adoptar um funcionamento que se aproxima mais de caixa de vidro [2] (capaz de mostrar de forma clara quais os seus componentes internos e a forma como estes se relacionam e operam em conjunto por forma a transformar os dados de entrada nos dados de saída), ou que se aproxima mais da caixa negra (não oferece mecanismos que permitam aos seus utilizadores analisar, avaliar e predizer o seu funcionamento), eventualmente menos confiável.

2.2.1 - Tipos de voto electrónico

O sistema de voto tradicional, descrito anteriormente, implica a presença do eleitor no local de recenseamento. Na votação electrónica, essa presença pode não ser necessária, logo podemos distinguir dois tipos de voto electrónico: presencial e não presencial [6]:

- Presencial. É indispensável a presença do eleitor no acto de identificação. A validação poderá ser feita junto à mesa de assembleia (local controlado) ou num local público determinado previamente, ainda que sejam utilizados os meios electrónicos de identificação.
- Não presencial. Pela faculdade tecnológica (infra-estrutura de Internet, por exemplo) e, ao contrário da presencial, o eleitor pode votar remotamente, sem estar confinado ao seu local de recenseamento, ou seja, através de qualquer local onde seja possível o acesso ao sistema de votação.

2.2.2 - Vantagens de voto electrónico

As vantagens de um SVE, identificadas por diversos autores, prendem-se com os seguintes factores [13], [14], [15]:

1. Combate à forte abstenção, com tendência a aumentar;

2. Possibilitar a invisuais e pessoas com necessidades especiais poderem votar confortavelmente, sem necessidade de se deslocar, ou sem nenhum acompanhante até à cabina de voto;
3. Uma forte redução de custos a médio prazo, através da redução do destacamento de pessoas para o processo eleitoral devido a nossa dispersão geográfica;
4. Eliminação dos boletins de voto em papel.

Para além destes factores positivos, é notória uma forte vontade política em introduzir as Tecnologias de Informação e Comunicações (TIC) no processo eleitoral, o que já vem sendo notado no âmbito da Governação Electrónica.

2.2.3 - Desvantagens de voto electrónico

No entanto, a implementação destes sistemas em Cabo Verde pode gerar alguma controvérsia, como é notório pelas várias opiniões de autores políticos, pelas falhas identificadas em experiências efectuadas noutros países, com particular destaque para as da Alemanha, EUA, Holanda e Irlanda, onde a votação electrónica foi suspensa ou substancialmente reformulada e em Portugal, de acordo com as acções de auditoria realizadas por uma equipa de Faculdade de Ciências da Universidade de Lisboa (FCUL) durante a experiência de voto electrónico realizada em 13 de Junho de 2004 [8].

Posso descrever que as falhas de implementação que provocam renitência a estes sistemas, passam por:

1. Falta de fidedignidade das aplicações instaladas no computador do eleitor;
2. Uso da Internet como meio de comunicação entre os servidores de voto e o computador do qual os eleitores estão a votar;
3. A possibilidade da coercibilidade;
4. A colisão entre a confirmação do voto e em quem foi votado, e a possibilidade de venda de votos;
5. Tolerância à falha do próprio sistema;
6. Etc.

2.2.4 - Requisitos do processo eleitoral

Nas leis eleitorais estão patentes os requisitos necessários para que o processo eleitoral tradicional decorra com normalidade. São enunciados os mais relevantes [9]:

1. **Elegibilidade/Autenticação**

Numa eleição democrática apenas os eleitores constantes dos cadernos eleitorais e em condições de o fazer devem poder votar. Para tal, é necessário que o sistema de voto electrónico permita a identificação e autenticação dos mesmos, assim como a verificação da sua admissibilidade ao processo em questão.

2. **Singularidade (reutilização)**

A cada eleitor tem de ser permitido um voto. A regra democrática de “um eleitor, um voto”.

3. **Apuramento**

Todos os votos válidos têm de ser contabilizados no processo da eleição.

4. **Integridades**

Os votos têm de permanecer inalterados, mesmo após o término do processo eleitoral.

5. **Verificabilidade / Auditabilidade**

Em todos os tipos de eleições deverá ser possível verificar se todos os votos válidos foram contabilizados, especialmente perante o votante. Este requisito é particularmente importante no caso de um sistema de SVE.

6. **Transparente**

O sistema de SVE não pode ser uma caixa negra. O seu funcionamento deverá ser do conhecimento público e monitorizado por todas as partes envolvidas no processo eleitoral.

7. **Robustez / Tolerância a faltas**

Consiste na continuidade de disponibilidade, independentemente, de uma falha ou erro nos componentes do sistema. Existem vários métodos que permitem a tolerância a falhas, tais como: redundância – quando um disco duro falha ao ser acedido, sem o utilizador notar um disco redundante continua a fornecer o serviço; - o simples uso de um dispositivo acumulador de corrente, permite tolerar a falha de energia.

No caso do voto electrónico, o sistema deve ter um mecanismo de recuperação/tolerância a faltas, de forma a evitar a perda de votos e permitir o eleitor dar continuidade a partir da altura em que ocorreu a falha ou erro. No sistema de votação tradicional esse mecanismo pode passar pela realização de novas eleições numa data própria.

8. **Flexibilidade / conveniente**

Uma das vantagens que os autores defendem que o SVE vem trazer é a possibilidade de este ser flexível o suficiente para se adaptar à especificidade do leitor. Por exemplo, no caso de este ser invisual, o sistema deve adaptar a sua interface para uma forma sonora.

9. Usabilidade

O sistema SVE deve ser de interface amigável, de preferência intuitiva, e de fácil utilização por parte de todos os eleitores.

10. Rastreabiliade

Durante a votação o eleitor deverá ter a possibilidade de retomar o processo em caso de mau funcionamento, sem lhe ser negado o direito ao voto. Por outro lado, existe a necessidade da criação de registos de acções feitas perante o sistema, sem comprometer o direito à privacidade do eleitor. Este é, porventura, o requisito mais difícil de garantir, exigindo simultaneamente o registo de acções do eleitor para futura utilização e a privacidade desses mesmos registos, sob controlo exclusivo do eleitor.

11. Disponibilidade

O sistema deverá estar disponível a todos os eleitores, durante todo processo eleitoral evitando dessa forma a negação do direito ao voto.

2.3 - Descrição do Sistema

O sistema que irá ser implementado visa suportar as diversas eleições nomeadamente, autárquicas, legislativas e presidenciais.

O presente capítulo descreve a arquitectura do sistema na sua versão 0, contemplando as tecnologias de segurança propostas no capítulo 3.

Deparei com a necessidade de construir numa linguagem visual, o UML, a definição de requisitos que servirá de base desse trabalho. Toda definição, ou seja, os diagramas de caso de uso, diagramas de sequência e diagrama de classes, está descrita nos anexos 1 e 2.

2.3.1 - Fases do Sistema

Qualquer processo de votação contempla várias fases desde a criação da comissão eleitoral, passando pela fase de criação de uma eleição até a contagem e publicação dos votos.

A criação da eleição, das listas e restante do processo é da responsabilidade da Comissão Eleitoral. A Comissão Eleitoral acede ao sistema para criar a eleição, fornecendo todas as informações relativas à mesma. Esta fase dá origem ao caso de uso “CaU1 – Criar Eleição”.

Passo a descrever as seguintes fases para uma melhor análise:

1. Recenseamento;

2. Votação;
3. Contagem dos votos.

Recenseamento

É da responsabilidade da Comissão Eleitoral criar também o caderno eleitoral e recensear os eleitores (registo de eleitores) e criar as listas concorrentes (candidatos). O referido registo é obrigatório sendo fornecido aos respectivos eleitores um mecanismo de comprovação que poderá ser o Cartão Único do Cidadão (CUC) [10] (ver detalhes do cartão de português no anexo 3) contendo um chip, smartcard, com dados pessoais do eleitor, ou entrega de códigos (PIN). O eleitor poderá consultar as listas, através de uma publicação do sistema, momentâneo que o administrador do sistema disponibiliza. Esta fase da origem aos seguintes casos de uso: "CaU2 – Criar Caderno Eleitoral" e "CaU3 – Recensear Eleitor".

Votação

Esta fase é parte fulcral do sistema, ou seja, é a fase de votação propriamente dita. Para o eleitor poder votar, terá de identificar-se perante o sistema através do CUC ou de dados biométricos (no caso de votação presencial controlado ou presencial num local público), e essa identificação será confrontada com a base de dados de recenseamento devidamente preparada para o efeito, de forma a validar as condições de votação (Autenticação e Singularidade), ou seja, verifica-se o direito de voto. No caso de votação presencial no recinto controlado, o eleitor identifica-se junto do Presidente da Mesa Eleitoral ao qual compete verificar a identidade do mesmo.

Seguidamente, o eleitor acede ao sistema, através de uma interface específica, onde poderá ver a lista dos candidatos (disponibilização do boletim de voto) e submeter o seu voto ao sistema (preenchimento e entrega do boletim). O sistema estará preparado para manter o anonimato do eleitor, e guardará o voto sem qualquer identificação do eleitor. Esta fase dá origem ao caso de uso: "CaU4 - Votar".

Contagem dos votos

No final da votação, a Comissão Eleitoral poderá aceder ao sistema e proceder ao apuramento e à contagem dos votos. Será eficientemente elaborada uma acta da eleição onde constará todas as informações inerentes à eleição, bem como a publicação e a divulgação dos resultados. A Comissão poderá dar como encerrado o processo eleitoral, considerando duas

variantes da contagem: Contagem localizada[1] e contagem centralizada[2] [3]. Esta fase dá origem ao caso: "CaU5 – Contar os votos".

2.3.1.1 - Identificação de actores e processos chaves

Como é de conhecimento, os actores representam todos os utilizadores que interagem com o sistema. No entanto, um actor não é necessariamente um utilizador no sentido restrito de termo – pessoa que utiliza o sistema – podendo ser um equipamento informático, como por exemplo um servidor.

Para cada informação descrita no diagrama de classes, anexo 1, foram identificados os casos de uso que a suportam e os actores que a manuseiam.

Desde modo, identifiquei a seguinte tabela:

	Processos/Casos de Uso				
Actores	**CaU1**	**CaU2**	**CaU3**	**CaU4**	**CaU5**
Administrador					
Comissão Eleitoral	**X**	**X**	**X**		**X**
Eleitor				**X**	

Tabela 01 – Actores e seus processos

Existem ainda outros actores, como por exemplo, o auditor, que é o elemento responsável por auditar todas as transacções que estão a decorrer no sistema permitindo registar todas as informações na detecção de eventuais deficiências de funcionamento. Temos também o público em geral, que todos os interessados (órgãos de comunicação social, partidos políticos, candidatos, população, etc.) na obtenção dos resultados parciais/finais de um processo de votação.

Seguidamente, procedi com o mapeamento dos processos e actores com as propriedades de segurança que no caso de concretização de uma ameaça, podem ser afectadas, como ilustra a seguinte tabela.

Propriedades de Segurança	**Actores**			**Casos de Uso**				
	Adm.	**C.E.**	**Eleit.**	**CaU1**	**CaU2**	**CaU 3**	**CaU4**	**CaU5**
Confidencialidade	**X**	**X**	**X**		**X**		**X**	
Integridade	**X**	**X**	**X**	**X**	**X**		**X**	
Disponibilidade	**X**	**X**	**X**	**X**			**X**	
Autenticidade	**X**	**X**	**X**		**X**	**X**	**X**	**X**
Anonimato	**X**	**X**	**X**		**X**	**X**	**X**	

Tabela 02 – Relação de processos e actores com as propriedades de segurança

As propriedades apontadas na tabela acima serão detalhadas no capítulo 3 – Segurança na Votação Electrónica.

[1] Contagem localizada – realizada em recinto controlado, sendo os votos posteriormente transmitidos a uma autoridade superior.
[2] Contagem centralizada – onde os votos são enviados para uma central de contagem.

3 - SEGURANÇA NA VOTAÇÃO ELECTRÓNICA

3.1 - Introdução

Na construção de sistemas de suporte à votação electrónica, como em qualquer sistema distribuído que se pretenda seguro, são utilizadas diversas técnicas para atingir um nível de segurança desejado. Na prática, um sistema de suporte à votação electrónica constitui um aglomerado de técnicas de segurança que, coordenadamente, tentam garantir as propriedades de segurança: Confidencialidade, Integridade e Disponibilidade (ISO/IEC 1996; ISO/IEC 1999; ISO/IEC 2000; ISO/IEC 2005) [7].

3.2. - Propriedades de Segurança

Considerando os inúmeros trabalhos e normas publicados sobre Segurança dos Sistemas de Informação, são identificadas, normalmente, um conjunto de três propriedades que constituem os pilares dessa segurança: Confidencialidade, Integridade e Disponibilidade.

Na votação electrónica não é difícil reconhecer a importância destas propriedades, mas é necessário reforçar outras três: Autenticidade, Autorização e Anonimato.

3.2.1 - Confidencialidade

Confidencialidade significa que qualquer informação trocada é secreta e apenas as partes autorizadas conseguem aceder a estas. No caso do SVE, esta propriedade é basilar, dado que em todas as fases do processo eleitoral existe troca de informação crítica e que apenas deve ser perceptível para as entidades/actores devidamente autorizados pelo sistema. Não é possível manter a confidencialidade se a informação não for íntegra.

3.2.2 - Integridade

Manter a integridade da informação significa manter a sua veracidade, ou seja, garantir que a informação apenas é alterada intencionalmente por actores devidamente autorizados. Neste grande objectivo não é difícil encontrar três medidas complementares: não permitir a alteração por entidades não autorizadas; garantir que as entidades autorizadas têm sempre conhecimento de alterações; e garantir que a informação permanece coerente.

3.2.3 - Disponibilidade

A disponibilidade do SVE significa que os actores devem aceder à informação, íntegra e confidencial, de uma forma permanente e em qualquer altura que necessitem para que o processo decorre na normalidade.

3.2.4 - Autenticação/Identificação/Autorização

Autenticação está directamente relacionada com outra propriedade de segurança que é a identificação. Identificação significa que o eleitor se identifica de uma forma reconhecida pelo

sistema. Com base nestas duas propriedades e ao longo do processo eleitoral os eleitores podem ou não serem autorizados a aceder ao sistema.

No caso do SVE em Cabo Verde a identificação poderá ser através Cartão Único do Cidadão que tem como objectivos principais [10] (ver detalhes no anexo 3) ou de dados biométricos:

- Garantia de uma correcta identificação e unicidade de todos os cidadãos residentes em território nacional, assim como todos os cidadãos de nacionalidade cabo-verdiana, residentes no estrangeiro;

- Construção de um forte Sistema Nacional de Identificação e Autenticação Civil (SNIAC), que garanta as valências de identificação e autenticação garantindo a existência de informações relevantes do cidadão desde o seu nascimento

- Centralização da missão de gestão de identidade pelos Registos, Notariado e Identificação (RNI), deverão ser garantidos meios para que os diversos sectores se dediquem mais à sua missão utilizando, sempre que necessário, a infra-estrutura informacional instalada para a correcta identificação e autenticação dos cidadãos.

3.2.5 - Anonimato

A associação entre o voto e o eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam manutenção do sistema) quer após a votação (mesmo que por ordem judicial) [5].

3.3 - Ameaças de segurança

Os computadores foram construídos para executar processos repetitivos com grande rapidez. Naturalmente, o seu mau uso pode provocar uma falha de segurança em larga escala e com repercussões insustentáveis.

Qualquer ataque a uma votação electrónica bem sucedido teria uma mediatização e um impacto sem medidas. Por esta razão, a segurança no voto electrónico tem a maior relevância. Vejamos a seguir que cada fase do processo eleitoral (identificadas no capítulo), ao ser informatizado, atrai uma série de ameaças de segurança sobre a informação que trata:

1. **Recenseamento**. Nesta fase as ameaças estão relacionadas com o registo de pessoas inexistentes, ou com o registo de pessoas em vários círculos eleitorais, ou ainda com a possibilidade de anulação do registo de eleitores, entre outras. De acordo com a Auditoria Externa ao Recenseamento Eleitoral Geral realizada em Cabo Verde [4], o processo de recenseamento foi adequadamente estruturado e integrado com os devidos níveis de segurança e monitorização.
2. **Validação da identificação**. A informatização desta fase é um dos maiores entraves à implementação do voto electrónico. Na votação presencial esta fase poderá ser garantida

com a apresentação do Cartão Único do Cidadão ou com os dados biométricos. No entanto, na votação não presencialmente, temos uma série de questões que podem comprometer a segurança: venda de voto, coercibilidade, solicitação de voto, privação do voto, entre outras.

3. **Recolha de votos**. Nesta fase, os grandes problemas assimilados passam por:
   - Consentir ao eleitor ter a certeza de que o seu voto foi validado (garantir o direito do voto e a integridade);
   - Que não existe mais do que um voto por eleitor (singularidade do voto);
   - A integridade da informação (integridade do sistema);
   - Anonimato dos votos (A não violação da privacidade do eleitor.)
4. **Contagem dos votos**. Nesta fase os maiores receios demonstrados por diversos autores passam pela contabilização de todos os votos válidos, do número de votos corresponder com o número de votantes, integridade da informação dos boletins de voto, entre outros.

3.4 - Ataques de segurança

No decorrer do processo eleitoral, vários são os ataques de segurança que podem comprometer todo o processo. Exponho, de seguida, alguns destes ataques recolhidos na literatura [6] que requerem a frequente actualização dos sistemas operativos, de forma a tentar evitar mal funcionamento e acções indesejadas.

3.4.1 - Negação do serviço (DOS) - A1

Consiste no congestionamento do servidor central de tal forma que compromete o atendimento dos computadores localizados nas assembleias de voto. Este tipo de ataque não requer grandes conhecimentos por parte do atacante, a resposta do mecanismo de defesa é moroso, podendo por em causa o direito de voto dos eleitores, inclusivamente, pode ser feito de uma forma selectiva.

3.4.2 - Cavalo de Tróia – A2

Actualmente é muito comum este tipo de ataque. Não requer grandes conhecimentos e a sua origem é muito difícil de saber. Pode comprometer o acesso por parte dos eleitores ao sistema de voto electrónico, negando a possibilidade de voto ou ainda alterar o sentido de voto.

3.4.3 - “Spoofing” – A3

O “spoofing” consiste num atacante fazer-se reconhecer pelo sistema como um utilizador credenciado. Desta forma, é possível, votar-se por alguém que se abstivesse ou mesmo, negar o voto a alguém.

3.4.4 - Ataques internos ao sistema – A4

Este tipo de ataque pode acontecer quando alguém, do próprio sistema, credenciado provoca vulnerabilidades ou falhas de segurança. São extremamente perigosos e difíceis de detectar, com consequências desastrosas, podendo por em causa todo o processo eleitoral.

3.4.5 - Vírus – A5

A existência de um vírus, tanto no cliente como no servidor, pode provocar a alteração do boletim de voto, comprometer a privacidade, entre outros.

3.4.6 - Alterações de configuração – A6

O computador do votante pode ser manipulado através de código malicioso e provocar o desvio da página oficial do sistema de votação. Pode provocar falta de privacidade ou negação do direito ao voto.

3.4.7 - Comércio de votos automatizado – A7

Pode ser desenvolvida uma ferramenta que permita de uma forma remota a comercialização dos votos, o que pode comprometer a democracia implícita de uma eleição.

3.4.8 - Coercibilidade – A8

O eleitor pode ser sujeito, de uma forma coerciva, a votar em determinado sentido, comprometendo a democracia.

Na tabela desenhada a seguir, apresento a classificação das ameaças e a sua influência nas propriedades de segurança:

	Ameaças							
Propriedades	**A1**	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**
Confidencialidade		**X**		**X**		**X**		
Integridade		**X**		**X**	**X**	**X**		
Disponibilidade	**X**	**X**	**X**	**X**		**X**		
Autenticidade		**X**	**X**	**X**	**X**	**X**	**X**	**X**
Anonimato		**X**		**X**	**X**	**X**	**X**	**X**

Tabela 03 – Classificação das ameaças e as propriedades de segurança

3.5 – Tecnologias de Segurança

A tecnologia está em constante evolução e, com os recentes acontecimentos relacionados com actos de terrorismo, associados a um maior recurso às tecnologias de informação e

comunicações em diversos domínios da actividade económica e social, as tecnologias de segurança têm assumido, cada vez mais, um papel de destaque. Existem já diversas tecnologias desenvolvidas para funções que procuram garantir, com maior ou menor grau de flexibilidade e segurança, as propriedades de segurança e direitos a salvaguardar num sistema de votação electrónica.

Existem várias tecnologias de segurança mas seria cansativa descrever todas de modo que seleccionei as tecnologias que estão de acordo com um estudo "2005 CSI/FBI Computer Crime and Security Survey" (CSI/FBI 2005) consideradas as mais utilizadas no contexto das organizações [7];

3.5.1 – Firewall

Este pode ser implementado num dispositivo electrónico (Hardware) ou num programa (Software). Consiste em estabelecer num único ponto de passagem numa comunicação entre computadores. É utilizado nas empresas como interligação entre o acesso à Internet e a rede interna.

No Firewall é possível definir regras que permitem funcionar como filtros de comunicação, podendo-se proibir destinos, tanto internos como externos, de modo a salvaguardar informação crítica. Este tipo de tecnologia de segurança pode suster ataques do tipo DoS[3].

No caso do SVE esta tecnologia poderá ser profícua na filtração de computadores que acedem a servidores do sistema de voto electrónico. Por exemplo, depois do eleitor ser identificado e autenticado, pode a sua ligação ser feita a um outro servidor central que sirva de urna electrónica e este estar com um firewall activado de modo a só permitir comunicações a computadores já identificados e reconhecidos pelo sistema.

3.5.2 - Software Antivírus

Como sabemos, são aplicações residentes que permitem identificar vírus, "worms" e código maléfico. Estes, normalmente, são pequenos programas escondidos, residentes e de fácil propagação. A protecção contra este tipo de ataque tem de ser feita de várias formas: prevenção, detecção, isolamento e recuperação.

No caso concreto do SVE, esta tecnologia de segurança é tão relevante no lado do servidor, como no computador que o eleitor está a utilizar. Qualquer alteração de configuração conseguida por este tipo de ataque pode inviabilizar todo o processo eleitoral.

3.5.3 - Sistemas de detecção de intrusão

Este tipo de tecnologia de segurança consiste numa aplicação que analisa as acções tomadas perante o sistema e de acordo com os privilégios dos utilizadores determina se é uma ameaça ou não.

[3] DoS – Denial of Service – Negação do Serviço

No caso do SVE esta ferramenta de segurança é necessária para prevenir eventuais ataques de utilizadores internos do sistema.

3.5.4 - Lista de controlo de acesso

Lista de controlo de acesso consiste no registo de perfis de acções dos utilizadores autorizados e por cada acção requerida o sistema confronta-a com as acções autorizadas para aquele utilizador. Deste modo, é possível controlar o acesso de cada um dos utilizadores perante o sistema.

No caso do SVE esta ferramenta permite definir quem tem acesso e ao que tem acesso ao nível de informação e processos de suporte ao sistema.

3.5.5 - Cifra de dados em transporte

Por defeito as comunicações entre dois computadores é feita de modo aberta, ou seja, a informação contida nas mensagens é completamente aberta a qualquer ataque de intersecção da mensagem. Por esta razão é necessário o uso de sistemas de encriptação de forma a não revelar o conteúdo das mensagens, evitando o comprometimento do direito à privacidade, e as propriedades de integridade e confidencialidade.

3.5.6 - Contas de utilizadores/login

As contas de utilizadores são usadas para definir quem são os actores do sistema autorizados, para se proceder a acções de identificação e autenticação perante o sistema ao longo de todo o processo eleitoral.

3.5.7 - Cifra de ficheiros

Da mesma forma que existe a necessidade de cifrar a informação durante o seu transporte, também é necessário que esta seja cifrada durante o armazenamento. Esta tecnologia permite evitar que seja possível aceder a informação que não lhe é destinada.

3.5.8 - Smartcards

Os smartcards são cartões do tamanho de cartões de crédito, com um chip embebido, que podem ser programáveis ou não. Para o caso de votação em Cabo Verde, o Cartão Único de Cidadão (CUC), poderá ser utilizado como os smartcards que serão utilizados essencialmente na fase de identificação e autenticação perante o sistema (ver detalhes no anexo 3).

3.5.9 - Infra-estrutura de chaves públicas

Garantir segurança na votação electrónica requer mecanismos seguros para a troca de informações. A Infra-estrutura de Chaves Públicas (PKI) garante a segurança de comunicações em sistemas distribuídos através dos seguintes elementos, entre outros: a) Autenticação (verificar a identidade do eleitor e das máquinas torna-se crucial durante o processo de votação). b) Encriptação (Encriptação e algoritmos de integridade são utilizados para proteger comunicações e

garantir a privacidade durante do voto de um computador a outro). c) Não repúdio (Não repúdio significa que os remetentes de e-mails ou transacções assinadas digitalmente não podem alegar que não a transmitiram)

O CUC já usa uma PKI e a mesma deveria ser usada para autenticar as máquinas envolvidas no processo de votação

3.5.10 - Biometria

Biometria consiste na utilização de uma característica física ou comportamental humana como forma de identificação e autenticação perante o sistema. Poderá ser uma alternativa ao smartcard ou complemento. Pode ser usado para controlo de acesso físico, electrónico e monitorização.

3.6 – Politica de Segurança na Votação Electrónica em Cabo Verde

De acordo com os requisitos do sistema de voto electrónico apresentados no capítulo 2 e a política de segurança deste capítulo, tenho a seguinte redacção:

3.6.1 – Segurança Geral

O sistema de voto electrónico que se pretende para Cabo Verde tem de permitir a verificação de todos os processos, através de um sistema tipo convencional. Deve suportar as auditorias ao sistema. Deve ser robusto e suportar mecanismos de tolerância a falha, permitindo ao eleitor retomar o processo de votação, no caso de alguma anomalia ou falha o ter interrompido. O sistema deve estar durante todo o processo eleitoral disponível para todos os eleitores. O eleitor devidamente inscrito no caderno eleitoral, só poderá votar uma só vez no mesmo processo eleitoral.

3.7.1 – Segurança Funcional

Administrador

O administrador do sistema é responsável pela disponibilidade do sistema de voto electrónico, e pela atribuição da credencial à comissão eleitoral. Também deve ser responsável pelo manuseio das seguintes informações: Comissão Eleitoral, Caderno Eleitoral e Administrador.

O administrador está sujeito a todas as ameaças em todas as propriedades de segurança, em especial, as ameaças: Cavalo de Tróia, Ataques internos e Alterações de configuração. Todas as tecnologias de segurança devem ser tidas em consideração, sendo as mais abrangentes: Firewall, Detecção de Intrusão e Controlo de acesso.

Comissão Eleitoral

A Comissão Eleitoral é responsável por todo o processo eleitoral deste a sua criação até à contagem dos votos (sessão 2.3.1). Esta manuseia as seguintes informações: Eleição, Eleitor, Lista, Caderno Eleitoral, Dispositivo Electrónico (Urna, PC, etc.). Está sujeita a todas as ameaças, sendo as mais abrangentes em relação às propriedades de segurança, as seguintes: Cavalo de Tróia, Ataques internos e Alterações de configuração.

As ameaças afectam de uma forma, igualmente, abrangente os processos: Pedir Credencial, Verificar Caderno Eleitoral e Votação. Todas as tecnologias de segurança devem ser consideradas, sendo as mais abrangentes, face às propriedades de segurança, as seguintes: Firewall, Detecção de Intrusão, Controlo de acesso, Cifra de ficheiros, Smartcards, Chaves públicas e Biometria.

Eleitor

Os eleitores apenas têm contacto com o sistema nos processos: Verificar Caderno eleitoral e Votação. As informações que manuseiam são: Eleição, Eleitor, Lista, Caderno eleitoral, e Dispositivo Electrónico (Urna, PC, etc.).

As ameaças que os eleitores estão sujeitos são todas à excepção da: Negação do Serviço. As tecnologias de segurança devem ser todas consideradas, em especial as que protegem a privacidade e autenticidade.

Em relação às propriedades de segurança, são salientadas as seguintes tecnologias de segurança: Firewall, Detecção de Intrusão, Controlo de acesso, Cifra de ficheiros, Smartcards, Chaves públicas e Biometria.

A política de segurança apresentada aqui poderá estar sujeita a alteração, de acordo com: a evolução da tecnologia, o aparecimento de novas vulnerabilidades e auditorias à sua implementação.

4 - SISTEMAS ACTUAIS DE VOTAÇÃO ELECTRÓNICA

Nos últimos anos várias experiências foram administradas para facilitar o processo de votação nas eleições. Tais facilitações foram introduzidas por alguns sistemas de votação electrónica como: o REVS (Robust Electronic Voting System), o Sensus e o Evox.

4.1 – REVS (Robust Electronic Voting System)

O **REVS** é um sistema de votação electrónica desenvolvido por Rui Joaquim [11] com objectivo de:

- Ter disponibilidade, eliminando os pontos de fracasso;
- Reiniciar a votação, tanto por vontade do votante como devido a falhas de rede;
- Resistir a conspirações, não permitir que um ou mais servidores, até um número qualquer, interfiram numa eleição.

Este sistema é composto por quatro tipos de servidores, os quais desempenham os seguintes papéis**:**

• **Distribuidores de Boletins** – São responsáveis pela distribuição das informações relativas a uma dada eleição;

• **Administradores** – São os servidores responsáveis pela validação dos votos, neste caso existe um número mínimo de validações, dado pela fórmula **n/2 +1** em que **n** corresponde ao número total de Administradores, para que o voto seja aceite;

• **Anonimizadores** – A função destes servidores é a de proteger a identidade dos votantes, impossibilitando os Contadores de associarem o voto a uma determinada máquina;

• **Contadores** – o papel deste servidor é verificar se os votos possuem o número de assinaturas necessárias para ser considerado um voto válido e é o responsável pela realização da contagem no fim da eleição, eliminando os votos repetidos.

Existem também**:**

- Um *Módulo Eleitor*, que é usado pelos eleitores para suportar as suas votações executando todas as interacções necessárias com os servidores;
- Um módulo para preparar a eleição, o *Comissário*.

- **Comissário** – é o módulo usado para preparar a eleição: registar os eleitores, definir as configurações operacionais (par de chaves da eleição, boletim, endereços e chaves públicas dos servidores, número de assinaturas requeridas, etc.). O Comissário assina todos os dados relativos à eleição de modo a que qualquer pessoa possa verificar a sua autenticidade;

Na figura abaixo, pode ser observado esquematicamente a arquitectura do **REVS.**

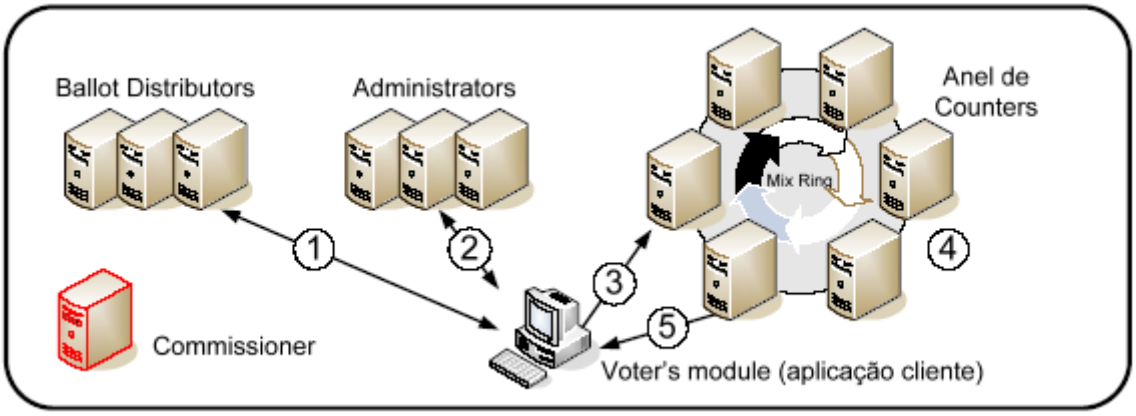


Figura 01 – Nova arquitectura de REVS

É um sistema que aposta numa arquitectura baseada na replicação de componentes, tendo em vista aumentar a tolerância a falhas [3].

4.2 – SENSUS

Desenvolvido no Department of Computer Science da Washington University por Lorrie Cranor e Ron Cytron, o Sensus assume-se como uma das mais divulgadas implementações de sistemas de suporte à votação electrónica a nível académico e científico, sendo uma das mais conhecidas variantes do protocolo de Fujioka, Okamoto e Ohta.

O Sensus usa assinaturas cegas para obter a privacidade dos votantes. Para tal o votante exprime o seu voto, cifra-o e aplica-lhe o factor de cegamento. O sistema é depois responsável por verificar a assinatura e, caso seja conforme, assinar cegamente o voto, devolvendo-o ao utilizador. O voto é depois enviado pelo votante, depois de decifrado, para o módulo responsável pela contagem de votos, sendo o módulo referido responsável por fazer todas as diligências para verificar a validade do voto. Em caso afirmativo, o voto é contabilizado na contagem dos mesmos.

Ao contrário da proposta de Fujioka, Okamoto e Ohta, o Sensus utiliza quatro módulos, em deterimento dos dois propostos anteriormente, sendo denominados por Registrar, Validator, Pollster e Tallier. Tais módulos repartem entre si a funcionalidade inerente a um sistema de suporte à votação electrónica, tendo como objectivo a obtenção das propriedades de segurança e implementação pretendidas. Como tal, a funcionalidade de tais módulos é a que abaixo se lista:

- **Registrar:** O módulo Registrar é, tal como o nome indica, responsável pelo prévio registo dos votantes. Tal é feito tendo como base a lista de pessoas habilitadas para votar e, com a referida lista, produzir um registo electrónico da mesma. São referidos como atributos

essenciais um número de identificação (número de eleitor), o nome, uma chave pública e, opcionalmente, o endereço de correio electrónico.

- **Pollster**: O módulo Pollster actua como uma interface entre o votante e o Sensus. Tal módulo é responsável por apresentar aos votantes as opções de voto e comunicar devidamente a resposta a tais opções ao módulo Validator.
- **Validator**: O módulo Validator assume responsabilidade idêntica à do Administrador proposto por Fujioka Okamoto e Ohta, sendo, portanto, responsável por verificar quais são os utilizadores habilitados para votar e certificando-os dessa hipótese, garantindo desde logo a propriedade de democracia.
- **Tallier**: O módulo Tallier é responsável pela colecção e posterior contagem dos votos, num procedimento idêntico ao do Contador proposto por Fujioka, Okamoto e Ohta. Ao receber os votos encriptados, o Tallier verifica a autenticidade da sua validação e verifica se tal voto é único. Caso surjam dois votos encriptados iguais, um deles é descartado, assumindo a hipótese que é muito difícil obter dois votos encriptados idênticos.

Genericamente, o Sensus é, como se pode observar, bastante idêntico ao protocolo que lhe serve de base. O votante começa por seleccionar o seu voto, encriptá-lo e aplicar-lhe um factor de cegamento.

O voto é então assinado e enviado ao módulo Validator, o qual verifica a validade da mesma e a habilitação do utilizador para exercer o direito de voto. Caso se trate de um votante habilitado para tal, o voto é assinado e reenviado ao votante. Obtido o voto assinado é então enviado para o módulo Tallier, através de um canal anónimo. O referido módulo verifica a validade do voto encriptado. Caso o seja, é então publicado numa lista, assinando-o e reenviando-o ao utilizador que assim obtém uma prova de voto.

Apesar de apenas constituir um protótipo, tal constitui, em caso de real utilização do Sensus, uma desvantagem. Tal é, inclusive, advertido pelos autores, referindo, contudo, a possibilidade de utilização de formulários HTML. Por outro lado, pelo facto de constituir uma transposição da teoria de Fujioka, Okamoto e Ohta para uma implementação real, tal protótipo apresenta, basicamente, as mesmas vantagens e desvantagens do referido protocolo.

4.3 – EVOX

Tal como o Sensus, o EVOX é uma das implementações de maior divulgação no meio académico e científico, tendo sido desenvolvido no Cryptographic and Information Security Group do Massachusetts Institute of Technology (MIT) por uma equipa coordenada por Ronald Rivest.

Os principais objectivos do EVOX são:

- Conseguir o voto assinado pelo Administrador e enviá-lo ao Contador;

- Verificar que o voto foi listado pelo Contador, confirmar as assinaturas e, eventualmente, enviar as chaves;
- Confirmar que os votos foram contados correctamente.

Ora, o desenvolvimento de tais passos não é, de todo, amigável ao utilizador, sendo que uma eleição nestes moldes pode levar mais tempo que o desejável. Segundo Rivest os dois últimos passos atrás referidos podem ser delegados. Uma entidade externa aos votantes. Existe, portanto, a tentativa de proporcionar uma mais fácil, intuitiva e agradável utilização do sistema.

Tal como todos os restantes protocolos, o EVOX assume um conjunto de assumpções, considerando que os métodos de criptografia utilizados são difíceis de quebrar e que não existem conspirações entre as entidades envolvidas no protocolo.

Em termos de autoridades de voto e tentando obter os seus objectivos, o EVOX considera três módulos, o Administrador, o Contador e o Anonimizador, sendo o Votante modelado por uma applet de Java. A funcionalidade de Administrador e de Contador são idênticas às propostas por REVS, sendo o Anonimizador responsável pela privacidade das votações, uma vez que o protocolo não considera a existência de canais anónimos no sentido referido por Chaum.

No protocolo EVOX, o votante começa, naturalmente por seleccionar o seu voto, sendo-lhe aplicado o factor de cegamento. Como é natural, depois de receber o voto, identificação e password de forma segura, o Administrador verifica a habilitação do utilizador para votar e, em caso afirmativo assina o voto e reenvia-o, seguramente para o utilizador. Ao receber o voto assinado pelo Administrador, o votante retira o factor de cegamento do voto, enviando o voto assinado pelo Administrador e o voto em claro para o Anonimizador, assim como as chaves para confirmação do voto. Tal procedimento é realizado de forma segura, sendo cada voto guardado num ficheiro separado sem qualquer informação relativa à sua origem. Após o “fecho das urnas” os votos são enviados do Anonimizador para o Contador de forma segura e aleatória, sendo posteriormente publicada a lista dos votos enviados para o Contador.

O Contador verifica a assinatura do Administrador, decifrando e contando os votos. Por fim, a lista é publicada.

A implementação concreta do EVOX requer, contudo, mais algumas entidades para além das atrás apresentadas. De forma a definir os contornos da eleição, nomeadamente as opções de voto, os autores do EVOX preconizam a utilização do Election Builder. Por outro lado, é também utilizado o módulo Registrar, em tudo idêntico ao utilizado pelo Sensus de Cranor e Cytron.

O EVOX contém, apesar de tudo algumas limitações. Uma delas é a forte possibilidade de conspiração entre as entidades envolvidas. Por outro lado, é reconhecida pelos autores a pouca optimização e eficiência do seu código. Na implementação do EVOX há, contudo, um aspecto que nos parece de grande importância que ultrapassa os limites teóricos inerentes a muitas propostas.

Tal prende-se com a linguagem escolhida para a implementação: o Java. Tal linguagem, pelas funcionalidades incorporadas revela-se de grande importância para obtenção dos objectivos propostos pelos autores do EVOX, oferecendo aos programadores uma vasta biblioteca

criptográfica incorporando os mais utilizados mecanismos de criptografia. Por exemplo, a cifra de mensagens utilizando RSA resume-se a duas linhas de código Java.

Genericamente**:**

- **RsaEncryption myRsa = new RsaEncryption(seed);**
- **Cyphertext = myRsa.encrypt (message);**

Além do mais, as facilidades inerentes obtidas pela modelação de algumas entidades como objectos assumem crucial importância na eventual facilidade de implementação. Por exemplo, o voto de cada votante pode ser modelado como uma classe. Tal classe constitui, inclusive, o centro da implementação do EVOX. Outro ganho potencial adquirido pela utilização do Java que, contudo ainda não é utilizado no EVOX, é a utilização do JDBC (Java Database Connectivity). Actualmente, os votantes no protótipo EVOX são modelados por ficheiros separados, o que limita o potencial número de votantes. Com a utilização do JDBC, o potencial número de votantes eleva-se bastante, sendo possível, com algumas adaptações ao protocolo, suportar eleições de carácter nacional. Tais modificações devem ter em conta a forma como os sistemas de votação convencional lidam com os votantes. Tal prende-se com o facto de o universo eleitoral ser dividido em pequenas áreas eleitorais com apenas alguns milhares de votantes em detrimento dos milhões de eleitores que compõem a totalidade do universo eleitoral.

Tais vantagens constituem uma eventual mais valia à construção de todo o tipo de sistemas distribuídos em geral e, em particular, de sistemas de suporte à votação electrónica, pelo que a sua utilização deve ser considerada pelos investigadores.

4.4 - Comparação entre os Sistemas

4.4.1 - Vantagens

Sistema	Vantagem
REVS	• Protecção configurável contra o conluio de entidades participantes no processo eleitoral; • Protocolo tolerante, a falhas nas comunicações, servidores e máquina cliente, maximizando a disponibilidade do sistema; • Protecção configurável contra o conluio de entidades participantes no processo eleitoral.
SENSUS	• Suficientemente flexível para permitir outros tipos de votação menos tradicionais; • Usa assinaturas cegas para obter a privacidade dos votantes.

EVOX	• Utiliza canais anónimos; • Permite a confirmação de que o seu voto foi entregue e contabilizado.

Tabela 04 – Comparação entre SVEs

4.4.2 - Diferença na implementação

A tabela abaixo apresenta de forma resumida as principais diferenças nas arquitecturas apresentadas [3].

	EVOX	**SENSUS**	**REVS**
Pré-registo	Election Commission		
Registo	Registrar	Registrar	
Validação	Admin	Validator	Administrator
Anonimização	Anon		Anonymizer
Votação	Voter	Pollster	Voter Engine
Contagem	Contador	Tailler	Contador
Verificação	Confirmation		

Tabela 05 – Diferença na implementação dos SVEs

Como se pode observar na tabela acima, o sistema EVOX propõe um componente que opera numa fase ainda anterior ao processo de votação (anterior mesmo à fase de registo do votante), chamada de Pré-registo. Nessa fase, no sistema EVOX são elaborados os boletins de voto.

Relativamente à fase de registo dos eleitores, apenas o sistema proposto por REVS parte do princípio de que a lista de eleitores já existe. Em todos os restantes se prevê o registo de votantes.

A validação do votante é tida em conta por todos os sistemas aqui apresentados.

O sistema REVS trata da anonimização do voto num componente independente e completa essa importante função com a capacidade muito específica de encobrir a origem e data dos votos. De notar que o sistema EVOX também se refere à anonimização de canais através de um componente específico mas com um papel mais restrito. Ainda que o outro sistema como o Sensus se refiram também à anonimização, esta fase é incluída no processo de tratamento do voto durante a fase de votação.

A fase de votação é uma fase que parece consensual em todos os sistemas.

A fase de verificação apresentada por estes sistemas pode ser considerada como uma primeira abordagem à auditoria do processo eleitoral num SVE.

O sistema EVOX, refere-se à fase de verificação como sendo da responsabilidade do próprio, através da confirmação/validação final de que os votos foram depositados.

4.4.3 - Países que desenvolveram ou utilizam esses sistemas

Sistema	País
REVS	Portugal
SENSUS	Brasil
EVOX	Desenvolvido no Cryptographic and Information Security Group do Massachusetts Institute of Technology (MIT).

Tabela 06 – Países que desenvolveram ou utilizam os SVEs mencionados.

4.5 - Sistema ideal para Cabo Verde

O sistema de votação electrónica que pretendo para Cabo Verde não deve munir-se de complexidade estrutural. No entanto, por natureza própria, um sistema desse porte é complexo, como já foi descrito anteriormente. Vejamos algumas fontes de complexidade que podemos deparar na implementação do sistema, segundo uma abordagem proposta por Kim Vicente [12]:

- Espaço do problema alargado

Vários são as questões que podem traduzir em problemas num SVE. As respostas eficientes para seguintes questões podem ser soluções para os respectivos problemas:

  - Como contar todos os votos?
  - Como garantir a comunicação de dados durante a votação?
  - Como garantir o anonimato dos votos?
  - Como garantir a total segurança na votação?
  - Como garantir a simplicidade do sistema garantindo a segurança?
  - Como garantir o acesso aos eleitores portadores de deficiências invisuais?
  - O que fazer quando um partido político põe em causa a eficiência do sistema?

Muitas outras questões podem ser aqui levantadas com objectivos claros de garantir a confiança não só das autoridades como, principalmente, dos eleitores.

- Natureza social

Um SVE tem uma componente de natureza social muito significativa, além da tecnológica, considerando que o objectivo principal é eleger pessoas para cargos políticos, ou seja, a função do sistema não é técnica mas política.

- Diversidade de visões sobre o sistema

Muitas fontes de informação envolvidas no processo eleitoral, tais como, os organismos reguladores, as instituições/organizações credenciadas que adquirem ou certificam e desenvolvem os sistemas, os partidos políticos, o público em geral, têm visões diferentes sobre a natureza e função dos sistemas. Dessas visões origina requisitos ambíguos e por vezes contraditórios que se tornam difíceis de clarificar, negociar e conciliar.

- Distribuição

Pela sua natureza, um SVE é um sistema distribuído e de grande escala que apresenta requisitos técnicos complexos. Complexidades tais como, disponibilidade, funcionamento em tempo real e afluxo dos utilizadores (vários eleitores simultaneamente acessando o sistema) são adicionadas.

- Acaso

Uma das fontes de complexidade associadas ao acaso está na dificuldade em aplicar a estratégica de teste e erro, uma vez que não é possível realizar ensaios gerais de eleições nacionais.

- Acoplamento

Na sua estrutura funcional, um SVE é composto por uma quantidade significativa de subsistemas interligados e interdependentes. Se acorrer uma falha em um subsistema pode comprometer o sistema todo.

Ambas arquitecturas vistas acima (REVS, SENSUS e EVOX) são interessantes. Apesar de possuírem as suas desvantagens, são importantes e contribuem para a minimização dos custos bem como a diminuição da abstenção nas eleições. Para Cabo Verde, o melhor sistema poderá ser o REVS, dado a sua facilidade na implementação e por ser um sistema sólido e de domínio público.

A utilização do sistema REVS para Cabo Verde poderá ter um custo muito mais reduzido do que o esperado, dado que este sistema parte do princípio de que a lista de eleitores já existe, e sendo assim utiliza a base de dados do recenseamento eleitoral que foi actualizada recentemente.

Cabo Verde deve acompanhar a evolução tecnológica na votação electrónica como em muitos países que estão tentando melhorar a tecnologia de votação actualmente utilizada para deixá-la mais segura. No entanto, há um longo caminho a ser percorrido pois, até agora o sistema está longe de ser perfeito, especialmente onde métodos electrónicos substituíram completamente o método tradicional.

É de todo interesse Cabo Verde obedecer um conjunto de recomendações na implementação de um SVE, entre as quais:

1. Monitorização do sistema por uma entidade independente com ampla competência técnica na matéria.

2. Testes de rotina das máquinas que suportam o sistema antes das eleições.

3. Realização de um estudo completo de vulnerabilidade de todo o sistema por peritos em segurança de tecnologias de informação.

4. Publicação dos resultados da votação por mesa de assembleia de voto, incluindo votos atribuídos a cada candidato, votos em branco.

5. Garantia de que as autoridades públicas têm capacidades de supervisão e compreensão adequadas, de forma a evitar uma excessiva dependência dos fornecedores de equipamentos.

6. A verificação do estado inicial do sistema antes da abertura do escrutínio deve ser pública.

5 – LEGISLAÇÃO CABO-VERDIANA

CÓDIGO ELEITORAL
LEI N.º 92/V/99, de 8 de Fevereiro
(na nova redacção dada pela Lei nº 118/V/2000, de 24 de Abril)[4]

Por mandato do Povo, a Assembleia Nacional decreta, nos termos da alínea i) do número 1, do artigo 187º da Constituição, o seguinte:

Artigo 1º

(Aprovação)

É aprovado o Código Eleitoral que faz parte integrante da presente lei e baixa assinado pelo Presidente da Assembleia Nacional.

Artigo 2º

(Experiências de votação electrónica)

O Governo, ouvidos os partidos políticos legalmente constituídos, pode realizar experiências-piloto de votação electrónica, em um ou mais círculos eleitorais.

Artigo 3º

(Recenseamento geral de eleitores estrangeiros e apátridas)

O Governo, ouvidos os partidos políticos legalmente constituídos, marca, por decreto-regulamentar, as datas de abertura e encerramento do recenseamento geral dos estrangeiros e apátridas residentes no país, possuidores de capacidade eleitoral activa.

Artigo 4º

(Pessoal da Comissão Nacional de Eleições)

O quadro de pessoal indispensável ao regular funcionamento da Comissão Nacional de Eleições é aprovado por resolução da Assembleia Nacional.

Artigo 5º

(Alterações)

As alterações que de futuro se fizerem sobre a matéria regulada no Código ora aprovado são inseridas no lugar próprio, devendo ser sempre efectuadas por meio de substituição dos artigos alterados, supressão dos revogados ou aditamento dos novos.

Artigo 6º

(Revogação)

1. São revogados:

- A Lei n.º 112/IV/94, de 30 de Dezembro;

- A Lei n.º 113/IV/94, de 30 de Dezembro;

- A Lei n.º 116/IV/94, de 30 de Dezembro;

[4] O Código Eleitoral, na versão que ora é apresentada, absorve na íntegra as alterações introduzidas pela Lei nº 118/V/2000, de 24 de Abril. Entretanto, as normas anteriormente em vigor são sempre transcritas no novo texto, em local apropriado, sob a forma de notas de rodapé, permitindo, assim, ao leitor e intérprete do Código a comparação do conteúdo e sentido das alterações

- A Lei n.º 117/IV/94, de 30 de Dezembro;

- A Lei n.º 118/IV 94, de 30 de Dezembro.

2. São ainda revogados todos os dispositivos legais que contrariem o estatuído no Código ora aprovado.

Artigo 7º

(Entrada em vigor)

Esta lei entra em vigor na data da sua publicação.

Aprovada em 16 de Janeiro de 1999

O Presidente da Assembleia Nacional,

ANTÓNIO DO ESPÍRITO SANTO FONSECA

Promulgada em 26 de Janeiro de 1999.

Publique-se.

O Presidente da República,

ANTÓNIO MANUEL MASCARENHAS GOMES MONTEIRO

Assinada em 26 de Janeiro de 1999

O Presidente da Assembleia Nacional,

ANTÓNIO DO ESPÍRITO SANTO FONSECA

6 – APRESENTAÇÃO DO PROTÓTIPO

Desenvolvi três protótipos para as respectivas eleições nomeadamente, autárquicas, legislativas e presidenciais.

Numa forma simplista, o protótipo a seguir apresentado é para as eleições presidenciais, na vertente presencial num recinto controlado.

O acesso ao sistema é garantido a partir de um código (login do eleitor) e a respectiva palavra-passe, apresentado nos subcapítulos seguintes.

No entanto, o acesso pretendido para o SVE em Cabo Verde deverá ser através do Cartão Único do Cidadão (ver anexo 3) ou de dados biométricos conforme explanado anteriormente. O subcapítulo 6.2 descreverá detalhadamente a interface de identificação.

6.1 – Interfaces Principais

O protótipo aqui descrito apresenta as seguintes interfaces:

Figura 02 – Interface Principal

O eleitor depara com a interface principal do sistema, que para exercer o seu direito de voto tem de clicar no botão **Votar**.

Ao clicar no botão **Votar** abre-se uma segunda interface.

Figura 03 – Interface de Acesso

Esta interface solicita ao eleitor o Código do Eleitor e a sua respectiva Palavra-Passe. O eleitor introduz os respectivos dados e clica no botão **Entrar** abrindo uma terceira interface com os dados informativos do eleitor. Caso o eleitor já tinha votado aparecerá a seguinte mensagem “O ELEITOR JÁ VOTOU”. Caso o eleitor não estiver inscrito e tentar votar aparecerá a mensagem “O ELEITOR NÃO ESTÁ INSCRITO”. Caso queira desistir de votar deve clicar no botão **Cancelar**. Se introduziu código correcto e palavra-passe errada aparecerá a mensagem “PALAVRA PASSE INVÁLIDA”.

Figura 04 – Interface de Identificação do Eleitor

Esta interface apresenta os dados do eleitor: código, nome completo, número de BI e outros dados necessários.

Nesse ponto, o eleitor deve pressionar o botão **Escolher Candidato** e aparece uma interface com uma lista de candidatos (Figura 05). Caso o eleitor pretenda desistir da votação deve então clicar no botão **Sair**.

Figura 05 – Interface de Apresentação dos Candidatos

O eleitor pode escolher o seu candidato pressionando os respectivos botões (**Votar Nesse Candidato**) ou escolher o Voto em Branco. Escolhendo qualquer um apresentado na lista abre uma nova interface (Figura 06) onde poderá corrigir ou confirmar o candidato escolhido.

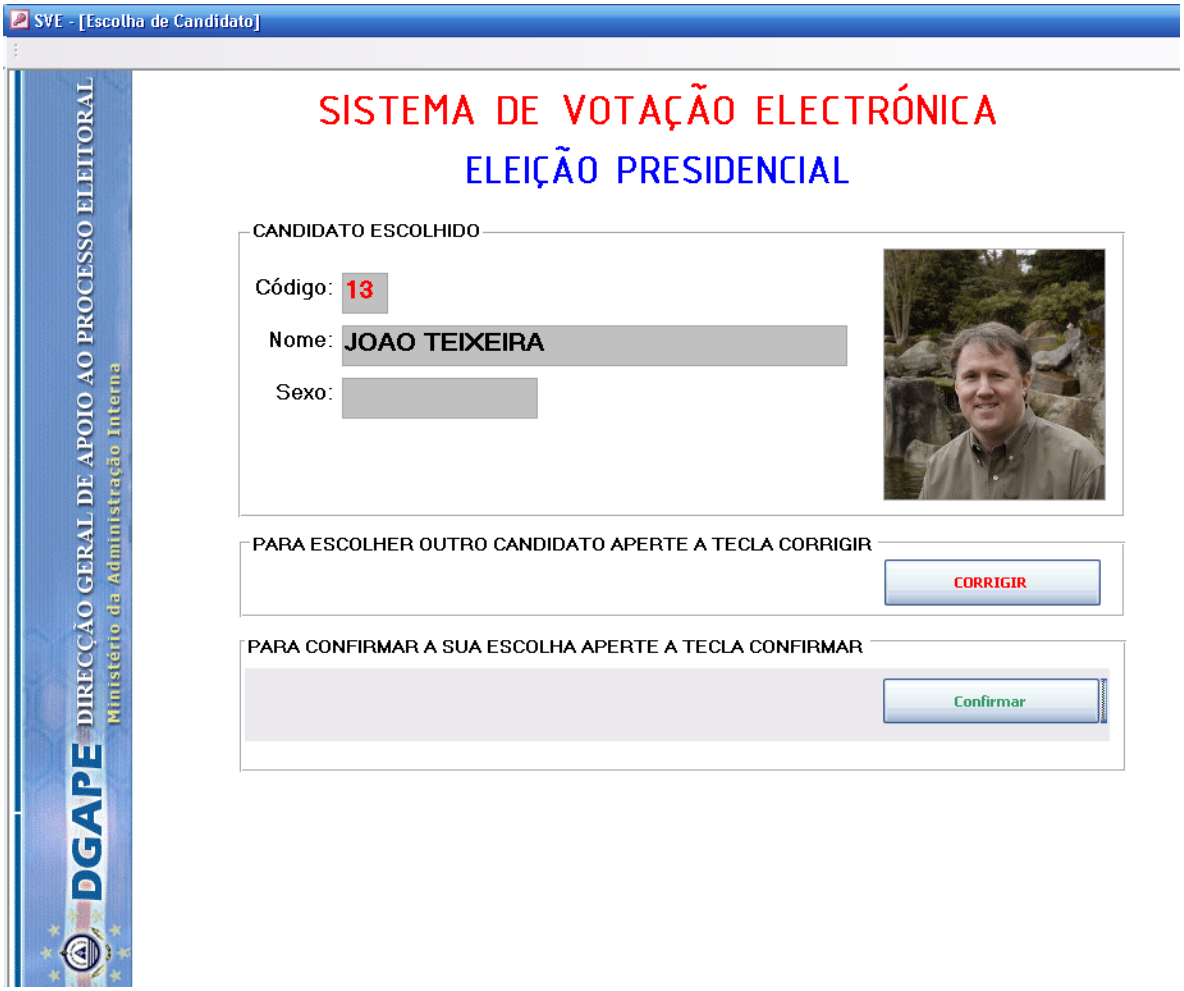


Figura 06 – Interface de Certificação de Escolha

O eleitor pode confirmar a sua escolha pressionando o botão **Confirmar** e aparecerá a caixa de diálogo de Confirmação do Voto, ou então poderá escolher outro candidato da sua preferência através do botão **Corrigir**.

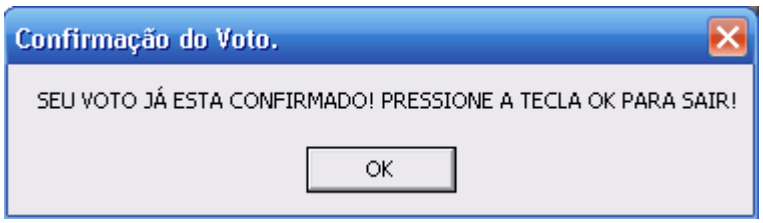


Figura 07 – Caixa de Dialogo de Confirmação do Voto

Pressionando o botão **OK** volta ao interface principal para a utilização do próximo eleitor.

6.2 – Interfaces do Cartão Único de Cidadão

6.2.1 - Físicas

A interface física dos leitores "conectáveis" (i.e. Leitores Desktop e Leitores All-in-One) com computadores pessoais, deverá ser USB (1.1 ou 2.0).

6.2.2 - Smartcard

A interface do leitor com o Cartão de Cidadão deverá:

- Suportar a norma ISO/IEC 7186 Class A, B e C (smarcards com voltagens de 5V, 3V, 1.8V);
- Suportar leitura e escrita para smarcards com microprocessadores alinhados com ISO/IEC 7816-1,2,3,4, protocolos T=0 e T=1;
- Suportar smartcards com frequências de relógio até 8Mhz;

6.2.3 – Interface de Identificação

O eleitor depara com a interface principal do sistema (Figura 02), que para exercer o seu direito de voto tem de clicar no botão **Votar.**

Ao clicar no botão **Votar** abre-se uma segunda interface que é a de Identificação através do Cartão de Cidadão.

A aplicação desenvolvida para o efeito (Microsoft ou não) deverá solicitar ao eleitor a introdução do respectivo cartão no leitor acoplado ao computador. Uma vez reconhecido o cartão, o sistema solicitará a introdução do PIN de Autenticação previamente entregue ao eleitor. Caso a validação tiver sucesso a seguinte interface deverá aparecer com os dados do eleitor:

Figura 08 – Interface de Identificação do Eleitor

Nessa interface temos os dados pessoais do eleitor fornecidos pelo smarcard embutido no cartão, que deverá garantir a viabilidade dos mesmos.

A partir desta interface, o leitor poderá seguir os outros passos descritos anteriormente.

6.3 – Ferramenta do Protótipo

A ferramenta utilizada para a implementação desse protótipo foi MS Access 2007, por ser uma ferramenta de fácil manuseio. O objectivo da demonstração desse protótipo é mostrar que, através de interfaces simples e intuitivas, o eleitor deve sentir seguro e confiante na votação.

Uma solução baseada na Internet assente na plataforma de desenvolvimento .Net, da Microsoft, e na sua tecnologia de bases de dados SQL Server, ficaria robusta a implementação, passando pela reengenharia das interfaces.

6.4 – Apresentação de Relatórios

O protótipo apresenta diversos relatórios desde listas de eleitores votantes, candidatos e os resultados da votação. A apresentação é desenhada não só em forma de tabelas com informações conduzentes ao tipo de relatório solicitado, como também em gráficos com as respectivas percentagens.

7 - CONCLUSÕES

A evolução das tecnologias de informação e a massificação do acesso a redes de comunicações tornam hoje o voto electrónico uma realidade possível e desejável para Cabo Verde, a par do desenvolvimento de plataformas de democracia electrónica com vista a uma futura generalização.

O desenvolvimento de sistemas de voto electrónico é um processo tecnologicamente complexo que depende de muitos factores sociológicos, culturais e políticos, i.é, é necessário um forte engajamento por parte de peritos das diferentes áreas envolvidas.

A Base de Dados de Recenseamento Eleitoral já está implementada e o projecto para criação de Cartão Único do Cidadão está em desenvolvimento possibilitando assim maior transparência na identificação dos eleitores (projectos do NOSi).

O próximo passo é a realização de projectos-piloto de voto electrónico, situação já prevista na legislação, e que trará benefícios quer em termos de eficiência e transparência de todo o processo, quer na promoção de uma maior proximidade e relacionamento dos cidadãos com as novas tecnologias da informação e comunicação e os processos electrónicos.

8 - REFERÊNCIA BIBLIOGRÁFICA

8.1 – Bibliográfias Principais

[1] PAGE, Plano de Acção para a Governação Electrónica: Uma Governação Mais Próxima dos Cidadãos. Novembro de 2005. Alfa Comunicações.

[2] Antunes, P. e. (Novembro de 2007). Sistemas de Votação Electrónica, Uma contribuição para a discussão dos seus problemas e oportunidades, Versão provisória - 2.3.

[3] Zúquete, A. et al. (2008). Voto Electrónico – Discussão técnica dos seus problemas e oportunidades. Lisboa: Edições Sílabo, Lda., 1ª Ed. .

[4] Martins, P. e. (25 de Junho de 2008.). Auditoria Externa ao Recenseamento Eleitoral Geral, Relatório Geral.

[5] Pinto, R. R. (Março de 2004). Estudo dos Requisitos para um Sistema de Votação Electrónica.

[6] Pereira, T. R. (2006). Tecnologias de segurança no e-vote, Mestrado em Sistemas de Informação. Universidade de Minho.

[7] Rubin, A. (2001). Security Considerations for Remote Electronic Voting over the Internet.". Florham Park, NJ.: AT&T Labs – Research.

[8] Antunes, P. N. (2004). Projecto de Avaliação de Sistemas de Votação Electrónica: Resultados da Auditoria. Faculdade de Ciências da Universidade de Lisboa.

[9] Mendes, M. d. (2005). LEI ELEITORAL DA ASSEMBLEIA DA REPÚBLICA - Anotada, Comissão Nacional de Eleições. Lei 14/79.

[10] Nosi. (n.d.). Cartão Unico de Cidadão. Retrieved Janeiro 2008, from Web site do Nosi: http://www.nosi.cv

[11] Joaquim, [. R. (Fevereiro 2005). A fault tolerant voting system for the Internet. Tese de Mestrado . IST/UTL.

[12] Vicente, K. (1999). Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work. Lawrence Erlbaum Associates, Inc.

[13] Malkhi, D., Rosner, G. (2002). Electronic Voting Protocols and Schemes, The Hebrew University of Jerusalem, Israel.

[14] Rivest, R. L. (2001). Electronic Voting. Financial Cryptography '01, Grand Cayman, BWI, International Financial Cryptography Association.

[15] Kitcat, J. (2004). "Electronic Voting: I want to understand the issues."

8.2 – Bibliográfias Complementares

1 - Almeida, Carlos Filipe. Anonimato em e-Voting. Tese de Mestrado, Universidade de Aveiro, Dep. Electrónica, Telecomunicações e Informática, Outubro 2006

2 - Joaquim, Rui; Zúquete, André; Ferreira, Paulo Revs – A Robust Electronic Voting System**.** IADIS International Journal on WWW/Internet, Vol. 1, No. 2, pp. 47-63, ISSN: 1645 – 7641

3 - Chaum, David. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 4(2), Fevereiro 1981.

4 - Burnside, Matthew and KEROMYTIS, Angelos D. Low Latency Anonymity with Mix Rings. Department of Computer Science, Columbia University.

5 - Brunazo Filho, Amílcar; Cortiz, Maria Aparecida - Fraudes e defesas no voto electrónico São Paulo: All Print Editora, 2006. ISBN 85-7718-030-1

6 – Gonçalves, Marco; Ramos, Marco - Sistemas de Suporte à Votação Electrónica – Trabalho final de curso LEIC-PSI, IST

7 - CÓDIGO ELEITORAL **–** Lei nº 92/V/99, de 8 de Fevereiro – (na nova redacção dada pela Lei nº 118/V/2000, de 24 de Abril)

8.3 – Bibliográfias Virtuais

1 - Página Ímpar: Estados d'Alma, Abstenção e voto electrónico,
Disponível em: http://paginaimpar.blogspot.com/2007/02/absteno-SVE-electrnico.html,
Visitado em Jan./2008

2 - Como exercer o Direito de Voto? Portal do Cidadão,
Disponível em: http://www.portaldocidadao.pt/como+exercer+o+direito+de+voto.htm
Visitado em Jan./2008

3 - UMIC, Agencia para a Sociedade de Conhecimento - Voto Electrónico,
Disponível em: http://www.umic.pt/index2.php.htm
Visitado em Jan./2008

4 – Sorumbático, Que é feito do voto electrónico?

Disponível em: http://sorumbatico.blogspot.com/que-feito-do-voto-electrnico.html
Visitado em Jan./2008

5 – Q u i n t u s, Sobre o "Voto Electrónico": Um atentado à Democracia?

http://movv.org/2007/10/09/sobre-o-voto-electronico-um-atentado-a-democracia/

Visitado em Jan./2008

6 – Comissão Nacional de Eleições, Glossário, Voto Electrónico,
http://www.cne.pt/index2.cfm.htm
Visitado em Jan. /2008

7 - http://www.gsd.inesc-id.pt/~revs/

Visitado em Jan. /2008

8 - http://ww.urnaelectronica.com

Visitado em Jan. /2008

9 - http://ww.votoelectronico.pt

Visitado em Jan. /2008

10 - Electronic Vote and Democracy Links page.
http://www.electronic-vote.org/link_tutti_en.php
Visitado em Fev. /2008

11 - Voting, Computers and the Human-Computer Interface
Website by the Voting Working Group of Computer Professionals for Social Responsibility (CPSR).
http://www.cpsr.org/issues/voting.html
Visitado em Mar. /2008

12 - CyberVote, A European project to allow Internet voting in a highly secure and verifiable way by using PC, palm computers and mobile phone.
http://www.eucybervote.org/
Visitado em Mar./2008

9 - GLOSSÁRIO

Sigla	Descrição
CaU	Caso de Uso
CNE	Comissão Nacional de Eleições
CUC	Cartão Único de Cidadão
DGAPE	Direcção Geral de Apoio ao Processo Eleitoral
DOS	Denial of Service – Negação do Serviço
EU	Urna Electrónica
JDBC	Java Database Connectivity
REVS	Robust Electronic Voting System
SIS	Subsistema de Instalação e Segurança
SVE	Electronic Voto – Voto Electrónico
SVE	Sistema de Votação Electrónica
NTIC	Novas Tecnologias de Informação e Comunicação
SNIAC	Sistema Nacional de Identificação e Autenticação Civil
RNI	Registo, Notário e Identificação

10 - ANEXOS

Anexo 1 – Casos de Uso

Anexo 2 – Diagrama de Casos de Uso

Anexo 3 – Cartão Único de Cidadão

Anexo 1 – Casos de Uso

CaU1 – Criar Eleição

Nome:	**CaU1 Criar Eleição**
Âmbito:	Sistema de Votação Electrónica – SVE.
Finalidade:	Criar a eleição, listas de concorrentes e restante do processo.
Actores:	Comissão Eleitoral.
Pré-condições:	O Administrador do sistema deve manter o sistema disponível.
Sequência típica dos eventos:	A Comissão Eleitoral acede ao sistema para criar a eleição, fornecendo todas as informações relativas à mesma.
Sequências alternativas e extensões:	
Requisitos especiais:	
Aspectos em aberto:	

CaU2 – Criar Caderno Eleitoral

Nome:	**Criar Caderno Eleitoral**
Âmbito:	Sistema de Votação Electrónica – SVE
Finalidade:	Criar o caderno eleitoral e criar as listas concorrentes.
Actores:	Comissão Eleitoral.
Pré-condições:	É da responsabilidade da Comissão Eleitoral criar o caderno eleitoral e criar as listas concorrentes (candidatos).
Sequência típica dos eventos:	O Eleitor consulta as listas, através de uma publicação do sistema, momentânea que o Administrador do sistema disponibiliza.
Sequências alternativas e extensões:	
Requisitos especiais:	
Aspectos em aberto:	

CaU3 – Recensear Eleitor

Nome:	**Recensear Eleitor**
Âmbito:	Sistema de Votação Electrónica – SVE.
Finalidade:	Recensear os cidadãos (eleitores).
Actores:	Comissão Eleitoral.
Pré-condições:	É da responsabilidade da Comissão Eleitoral recensear os cidadãos.
Sequência típica dos eventos:	A Comissão Eleitoral recenseia todos os cidadãos respeitando as condições estipuladas na legislação (Código Eleitoral).
Sequências alternativas e extensões:	O eleitor acede ao sistema para a verificação de seus dados.
Requisitos especiais:	
Aspectos em aberto:	

CaU4 – Votar

Nome:	**Votar**
Âmbito:	Sistema de Votação Electrónica – SVE
Finalidade:	Votar no candidato.
Actores:	Eleitor.
Pré-condições:	Para o Eleitor poder votar, terá de identificar perante o sistema.
Sequência típica dos eventos:	O Eleitor identifica-se perante o sistema através do Cartão Único do Cidadão ou de dados biométricos. O Eleitor acede ao sistema, através de uma interface desenhada para o efeito, onde poderá ver a lista dos candidatos e submeter o seu voto ao sistema.
Sequências alternativas e extensões:	O sistema estará preparado para manter o anonimato do Eleitor, e guardará o voto sem qualquer identificação do Eleitor.
Requisitos especiais:	A identificação do Eleitor será confrontada com a base de dados de recenseamento devidamente preparada para o efeito, de forma a validar as condições de votação.
Aspectos em aberto:	

CaU5 – Contar os Votos

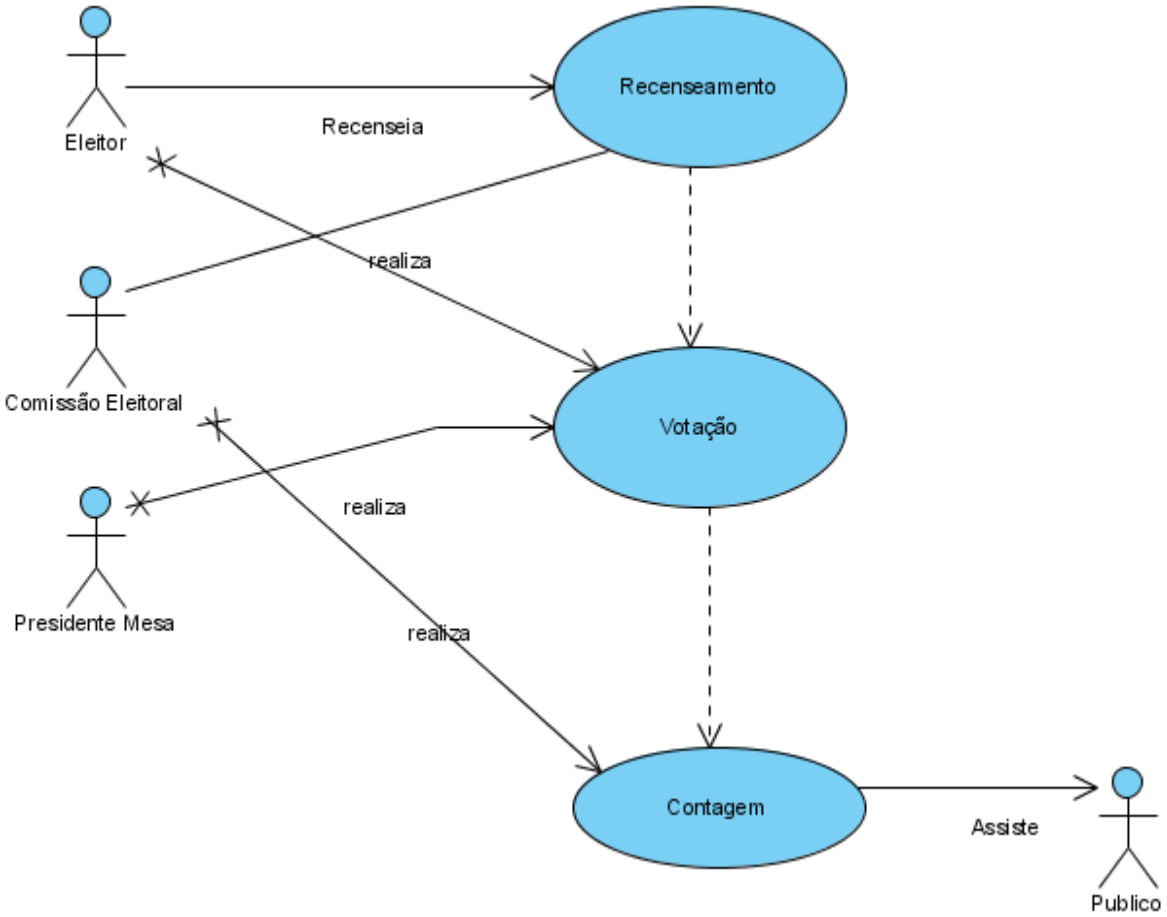
Nome:	**Contar os Votos**
Âmbito:	Sistema de Votação Electrónica – SVE
Finalidade:	Cotar todos os votos.
Actores:	Comissão Eleitoral, Presidente Mesa de Voto, Servidor Votação, Público.
Pré-condições:	A votação tem que estar encerrada.
Sequência típica dos eventos:	A Comissão Eleitoral acede ao sistema e procede ao apuramento e à contagem dos votos.
Sequências alternativas e extensões:	A Comissão Eleitoral elabora uma acta da eleição onde constará todas as informações inerentes à eleição, bem como a publicação e a divulgação dos resultados. A Comissão dá como encerrado o processo eleitoral.
Requisitos especiais:	
Aspectos em aberto:	

Anexo 2 – Diagramas

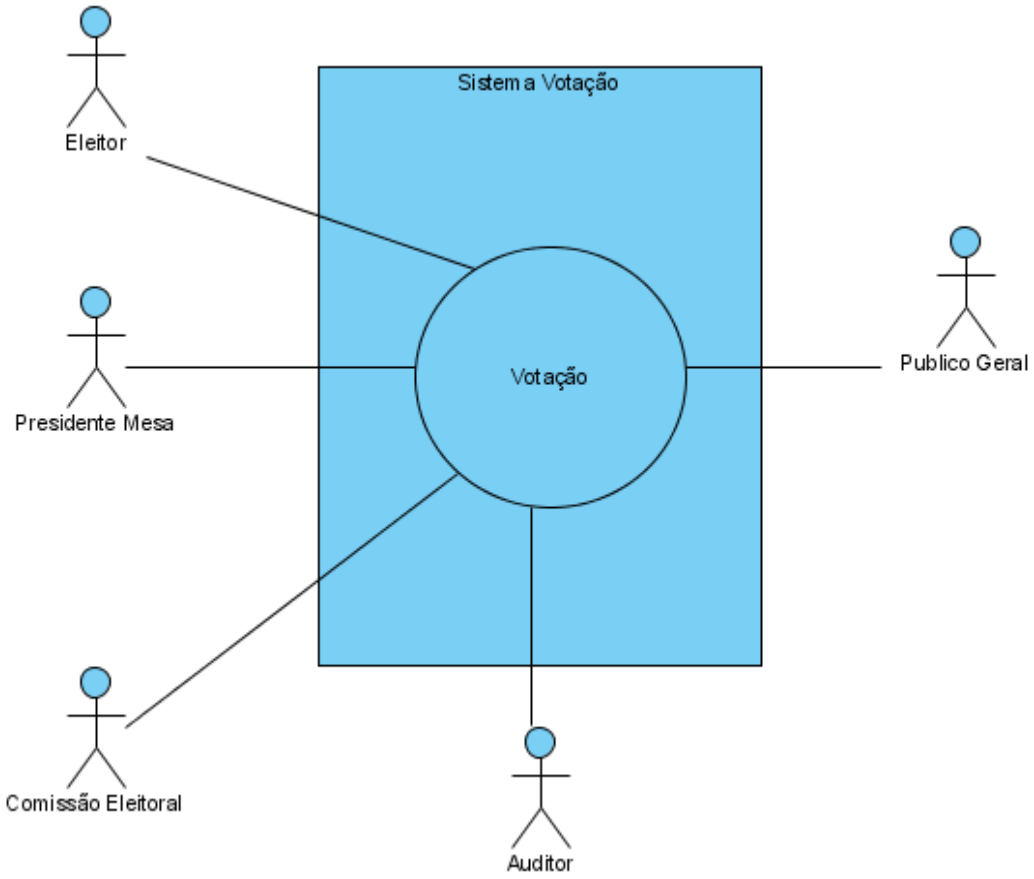
Diagramas de Casos de Uso

Os Diagramas de Casos de Uso são utilizados para identificar as fronteiras do sistema e descrevem quais os serviços que devem ser disponibilizados aos utilizadores (Actores). São apresentados os seguintes Diagramas de Casos de Uso:

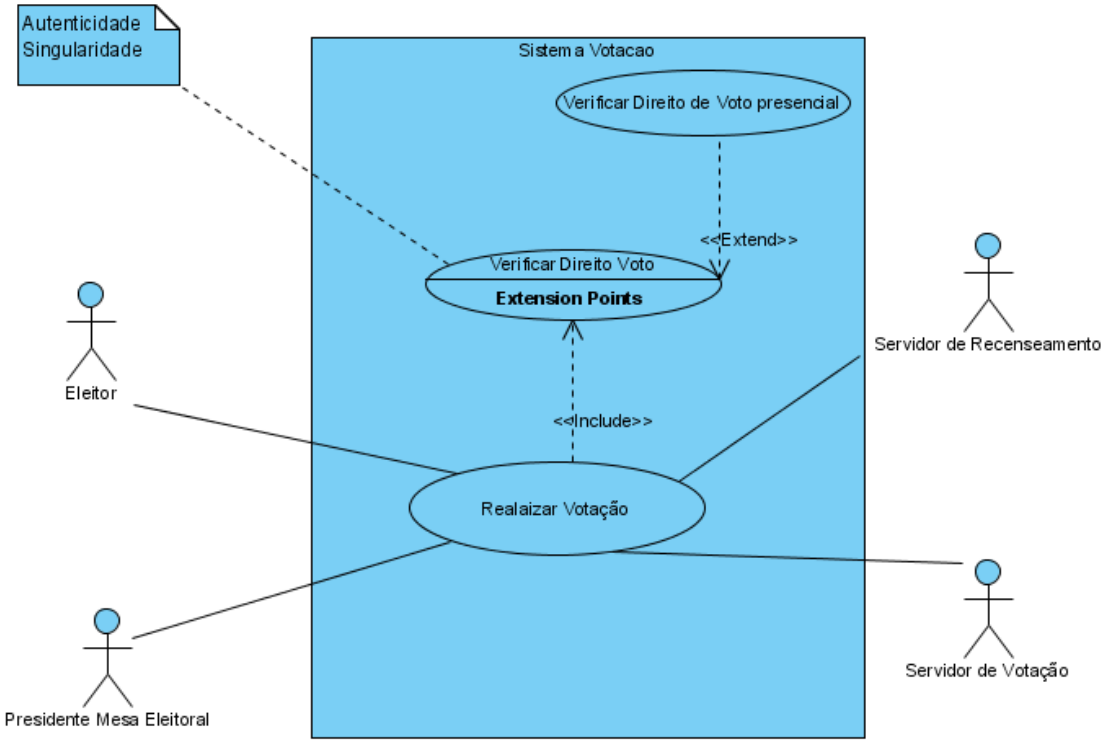
1 - Caso de uso – Nível geral



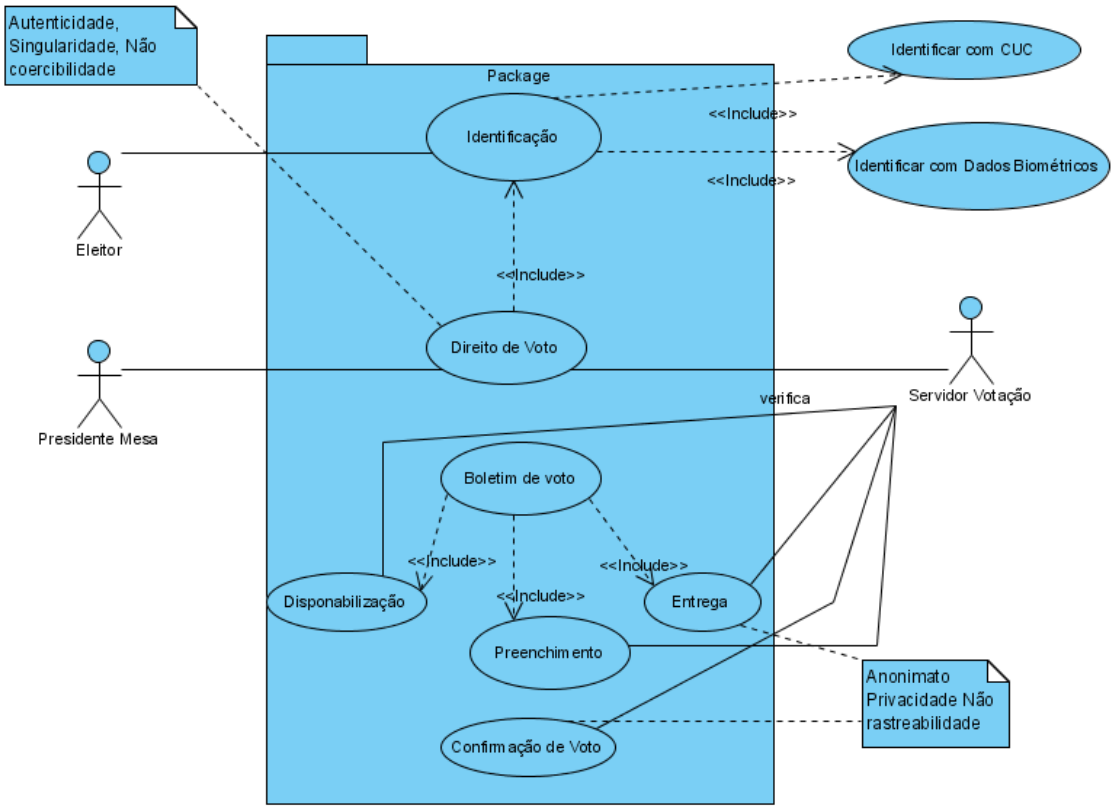
2 - Caso de uso – Votação (nível 1)



3 - Caso de uso – Votação (nível 2)



4 - Caso de uso – Votação (nível 3)



5 - Caso de uso – Contagem de Votos

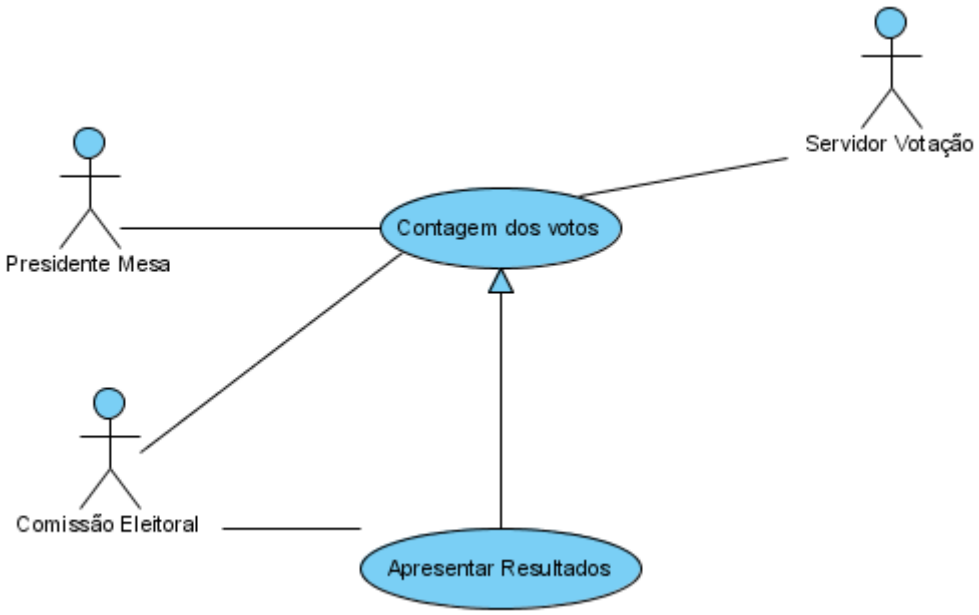


Diagrama de Classes

O diagrama de classes apresenta elementos conectados por relacionamentos. O diagrama desenhado abaixo representa o modelo da estrutura do sistema, demonstrando as classes, os tipos e os relacionamentos.

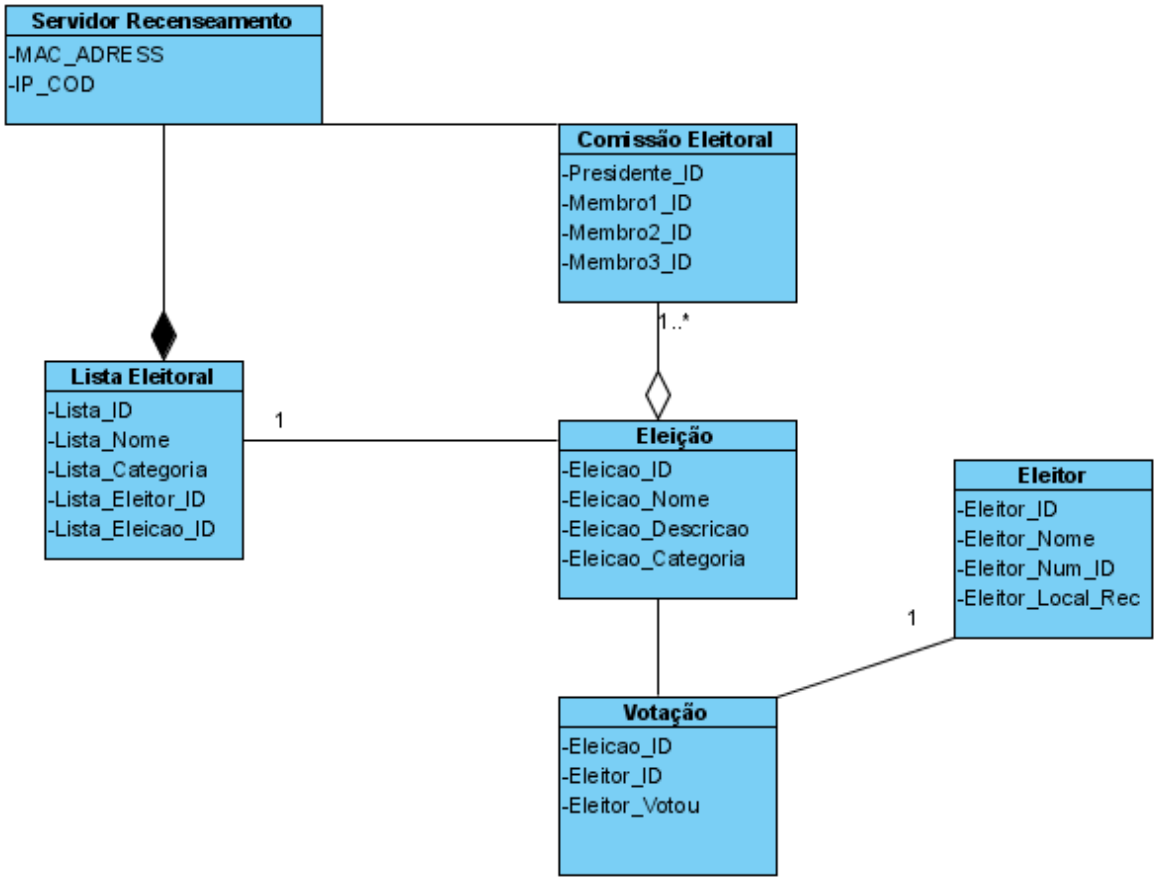
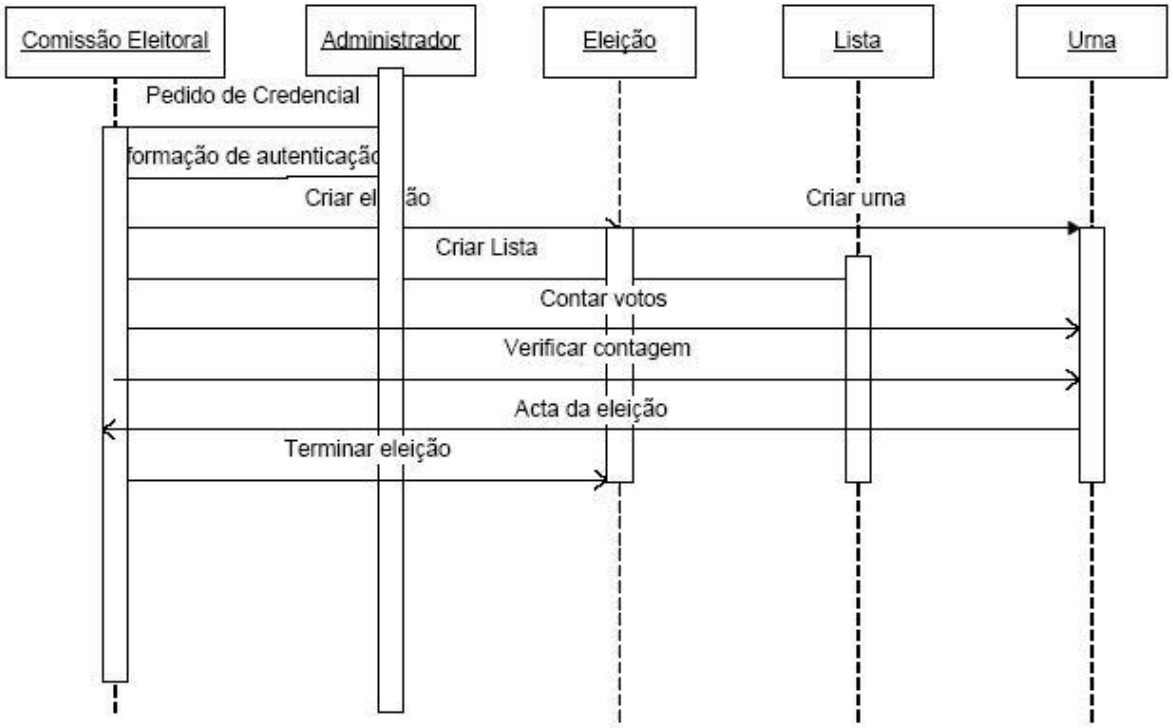


Diagrama de Sequência

O Diagrama de Sequência descreve as interacções entre os elementos do SVE segundo uma visão temporal. São apresentados os seguintes diagramas:

1 - Comissão Eleitoral



2 - Diagrama de Sequência – Eleitor

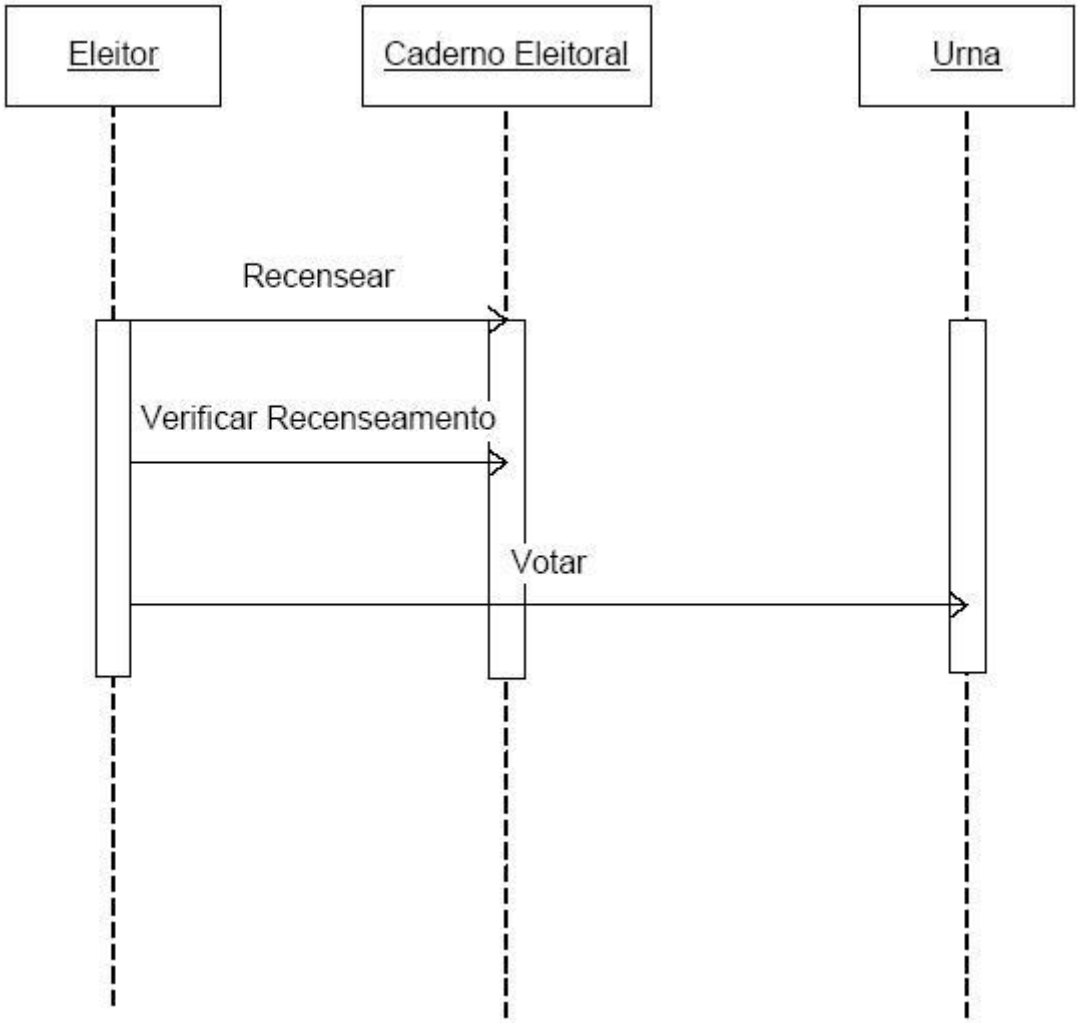


Diagrama de Instalação

O Diagrama de Instalação abaixo representa a configuração e a arquitectura do sistema de votação em que estarão ligados seus respectivos componentes.

1 - Votação Recinto Controlado

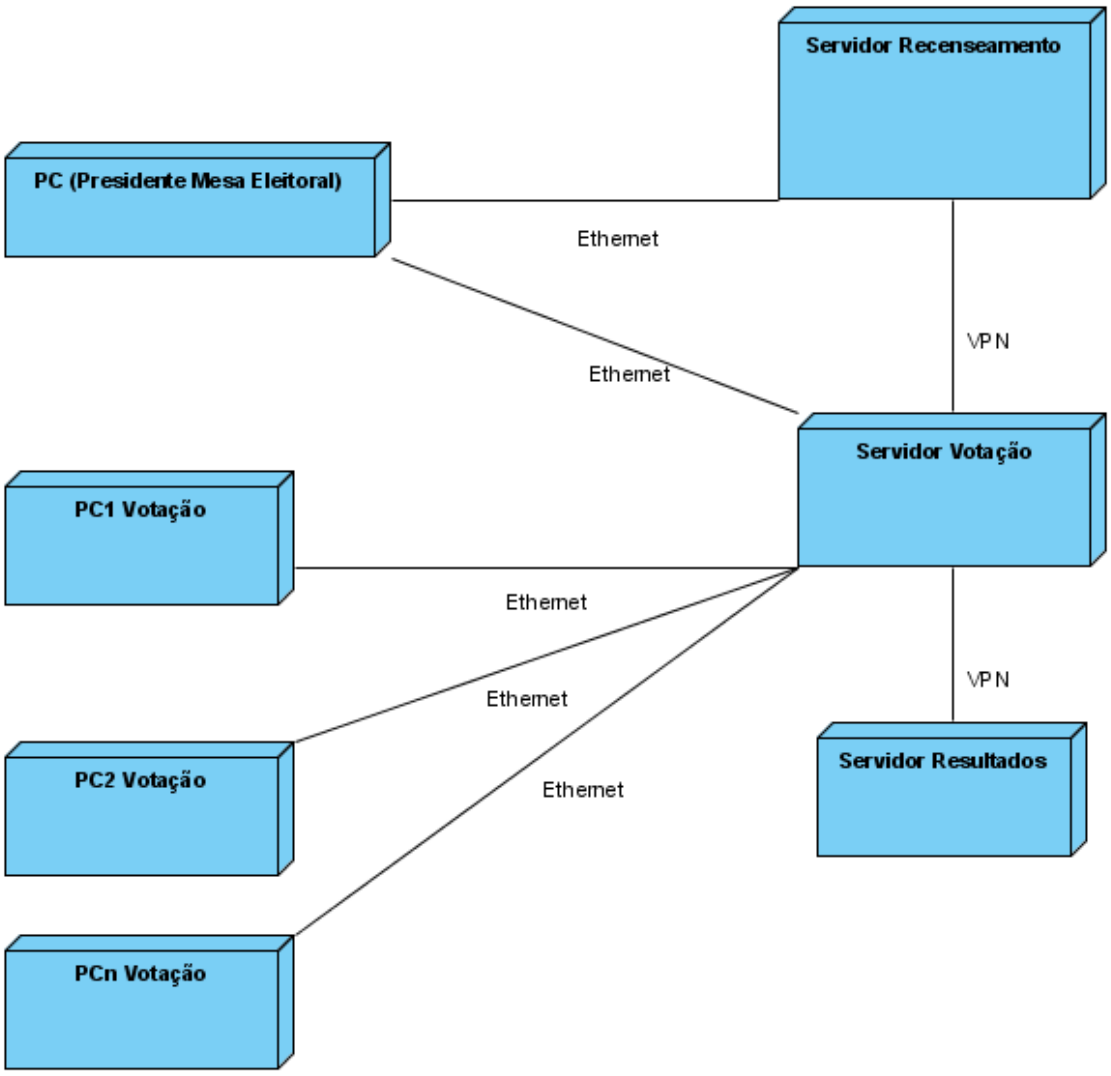
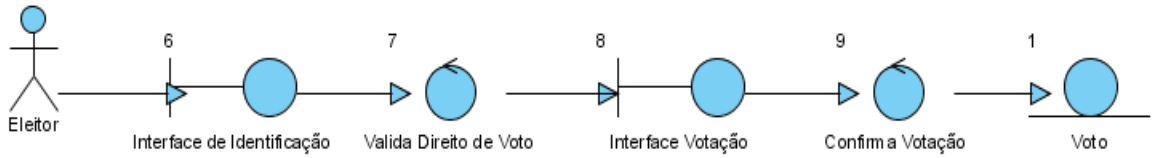


Diagrama de Comunicação

Diagrama de Comunicação mostra objectos, seus inter-relacionamentos e o fluxo de mensagens entre eles. É um dos diagramas de interacção que dá ênfase à organização estrutural dos objectos que colaboram entre si.



Anexo 3 – Cartão Único do Cidadão – CUC

1 - Introdução

O Cartão Único do Cidadão é um novo modelo de identificação que integra todas os componentes (Biometria, Identificação e Autenticação) e etapas do processo eleitoral num conjunto coerente e sistematizado de acções encadeadas entre si de forma a garantir a eficiência e transparência e transmitir confiança ao cidadão, aos partidos políticos e à sociedade cabo-verdiana.

Esse cartão provavelmente será semelhante ao Cartão de Cidadão de Portugal (CC), que já está a ser emitido para portugueses desde Fevereiro de 2007. O CC possui diversas características tais como: uma delas é o facto de ser um cartão que substitui cinco outros: bilhete de identidade, cartão de eleitor, cartão do contribuinte, cartão de beneficiário da Segurança Social e cartão de utente do Serviço Nacional de Saúde. Pretende-se, desta forma, evitar a dispersão de suportes físicos sem, no entanto, reduzir o universo de identificadores (números) afectos a cada cidadão – número de identidade civil, número de eleitor, número de identificação fiscal, número da Segurança Social e número de utente de saúde.

A frente do cartão de cidadão contém informação textual específica sobre a identificação do seu titular.

Figura 1 - Informação inscrita na frente do cartão

O verso do cartão de cidadão contém informação textual específica dos actuais documentos de identificação sectoriais (Finanças, Segurança Social e Saúde) do titular, bem como uma zona de leitura óptica – Machine Readable Zone (MRZ). A MRZ é formada por três linhas de texto, como ilustra a imagem esquerda da Figura 2.

Figura 2 - Informação inscrita no verso do cartão

Uma das características mais inovadoras do Cartão do Cidadão é que o mesmo é um smartcard (cartão inteligente) porque possui um micro-computador embebido. Este smartcard tem diversos fins, a saber:

Guardar informação privada. Informação privada é informação que o titular pode usar mas não divulgar. Concretamente, esta informação é constituída por três chaves criptográficas: (i) uma chave privada de um par de chaves assimétricas, que serve para produzir assinaturas digitais do titular, (ii) uma chave privada de outro par de chaves assimétricas, que serve para produzir autenticar o titular e (iii) uma chave simétrica de autenticação do titular.

1. Guardar informação pessoal para validação informática interna da identidade do titular. Concretamente, esta informação é constituída por elementos descritivos (*template*) da impressão digital do titular. Este *template* é usado apenas internamente ao *smartcard* para validar uma impressão digital comunicada ao mesmo.

2. Guardar informação reservada. Informação reservada é informação que o titular conhece mas que apenas disponibiliza de forma fidedigna, via *smartcard*, a quem desejar ou a quem tiver autorização para a obter, independentemente da vontade do titular. Concretamente, esta informação é constituída pela morada do titular.

3. Guardar informação pública de grande dimensão, não memorizável por humanos. Concretamente, esta informação é constituída por certificados X.509 de chaves públicas do titular, chaves essas que podem ser usadas para autenticar o titular ou a sua assinatura digital.

4. Guardar toda a informação do titular observável no Cartão do Cidadão (fotografia, nome, dada de nascimento, os diversos números de identificação, validade do cartão, etc.).

5. Efectuar operações criptográficas usando as chaves que fazem parte da sua informação privada.

As operações realizadas pelo *smartcard* em nome do seu titular necessitam que o mesmo indique um código secreto (PIN). Cada cartão possui três PIN (Personal Identification Number), cada um

com quatro algarismos: um para autorizar a indicação da morada, outro para autenticação do titular e um terceiro para produzir uma assinatura digital.

Os PIN são os elementos chave que tornam o *smartcard* pessoal. Por outras palavras, a perda do cartão não permite a quem o encontrar o usufruto das funcionalidades do *smartcard*. No entanto, existe um risco mínimo que quem o encontrar descubra, por acaso, um dos PIN antes de esgotar as tentativas erradas. Para evitar este problema, o Cartão do Cidadão é fornecido com um código de cancelamento. Este é um número de oito algarismos que pode ser comunicado às autoridades competentes para invalidar todas as funcionalidades do *smartcard* em caso de extravio ou furto.

2 - Autenticação com o *smartcard*

A autenticação com o *smartcard* é realizada de duas formas distintas.

Uma das formas destina-se a autenticar o titular sem recorrer a meios computacionais, usando o EMV-CAP (Europay, MasterCard e Visa *Chip Authentication Program*). Inserindo o cartão num leitor pessoal, semelhante a uma pequena calculadora (ver Figura 3), digita-se o PIN de autenticação no teclado do terminal e no ecrã do mesmo aparece uma senha única (*One-Time Password*, OTP). Esta OTP pode ser comunicada, por qualquer meio de comunicação (v.g., telefone, FAX, etc.) a quem precisar de autenticar o titular para uma dada operação remota. O autenticador valida a OTP comunicando-a, junto com a identidade do sujeito a autenticar, a uma Autoridade que sabe verificar a OTP. Essa Autoridade responderá afirmativamente se a OTP estiver correcta, e negativamente caso contrário.

Figura 3 - Exemplo de leitores de smartcard destinado à autenticação via EMV-CAP. O teclado serve para introduzir o PIN do titular do cartão, o ecrã serve para mostrar a senha única (OTP)

A OTP é gerada a partir de um algoritmo existente no *smartcard* e da chave simétrica secreta guardada no mesmo. A Autoridade que valida as OTP possui e usa os mesmos elementos, algoritmo e chave, para verificar se uma OTP apresentada é ou não válida.

A outra forma de autenticação destina-se a autenticar o titular em universos computacionais. Para esse efeito, o *smartcard* possui um par de chaves assimétricas de autenticação, as quais podem ser usadas por diversas aplicações (v.g. navegadores) e protocolos (v.g. HTTPS, HyperText Transfer Protocol Secure) para autenticar o titular. O PIN de autenticação do titular tem de ser

enviado para o *smartcard* de cada vez que for necessário usar a chave privada do par de chaves assimétricas para autenticação do titular.

O *smartcard* possui e disponibiliza um certificado X.509 com a chave pública de autenticação do titular. Este certificado pode ser comunicado aos interlocutores do titular para que os mesmos possam verificar a correcção e validade da chave privada de autenticação do titular.

3 - Assinaturas digitais com o *smartcard*

As assinaturas digitais são uma forma não repudiável de autenticação de documentos. Elas permitem simultaneamente garantir a inalterabilidade de um documento e indicar a sua autoria, que não é mais do que a identidade de quem as produziu. As assinaturas digitais podem ser validadas usando a chave pública correspondente à privada que a gerou. A divulgação fidedigna das chaves públicas aos validadores de assinaturas digitais é feita através de certificados digitais X.509 dessas mesmas chaves públicas.

O *smartcard* possui um par de chaves assimétricas de assinatura digital qualificada, as quais podem ser usadas por diversas aplicações para assinar documentos. O *smartcard* possui e disponibiliza um certificado X.509 com a chave pública de validação da assinatura digital qualificada do titular. Este certificado pode ser comunicado aos interlocutores do titular para que os mesmos possam verificar a correcção e validade das suas assinaturas.

O PIN de assinatura digital do titular tem de ser enviado para o *smartcard* de cada vez que for necessário usar a chave privada do par de chaves assimétricas de assinatura digital do titular.

Por omissão, a funcionalidade de assinatura digital não está activada quando o Cartão do Cidadão é entre ao seu titular. Tal é feito através da publicação de um certificado de revogação das credenciais de assinatura digital presentes no *smartcard*. Desta forma, o titular poderá produzir assinaturas digitais com o seu cartão, mas as mesmas não poderão ser validadas porque o validador receberá uma indicação que as credenciais usadas na geração da assinatura não estão válidas.

A activação da funcionalidade de assinatura digital tem de ser requerida presencialmente pelo seu titular numa instituição autorizada para esse efeito. A activação consiste na eliminação do certificado de revogação antes referido.

4 - Aplicação Cartão de Cidadão

A aplicação Cartão de Cidadão é suportada nos seguintes sistemas operativos:

- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows 2000 SP3
- Red Hat Enterprise Linux WS 4 Update 4
- OpenSuse 10.2

- Ubuntu 6.10
- Fedora Core 6
- Caixa Mágica 11

5 - Leitor do Cartão de Cidadão

Para usar o Cartão de Cidadão através do computador pessoal é necessário que este possua um dispositivo de leitura.

O Leitor do Cartão de Cidadão é um periférico de um computador pessoal, que lê (e escreve, sempre que aplicável), por contacto com o Chip, o seu conteúdo através de uma aplicação própria para o efeito. Tecnicamente é um leitor de SMARTCARDs, não sendo exclusivo o seu uso pelo Cartão de Cidadão.

O Chip do Cartão não tem bateria (energia própria) pelo que a energia necessária ao seu funcionamento é fornecida pelo Leitor, através do computador a que está ligado.

O Leitor é assim um instrumento de leitura e escrita (se permitido), de uso não exclusivo (pode ler outros cartões SMARTCARD) do Cartão de Cidadão do seu titular.

O Leitor é essencial para quem pretenda relacionar-se electronicamente com entidades públicas e privadas que disponibilizem ou venham a disponibilizar serviços electrónicos através da Internet, a partir dum computador pessoal. É igualmente essencial para que a aplicação do Cartão de Cidadão possa interagir localmente com o Cartão de Cidadão.

6 - **Votação com Cartão Único de Cidadão**

Futuramente o CUC passará a ser um documento de identidade que permitirá a identificação visual e presencial do cidadão nos actos eleitorais em Cabo Verde

Tratando-se de um documento seguro com garantias de segurança física que dificultem as possibilidades de usurpação da identidade (uma vez que é pessoal e intransmissível), o eleitor sentirá maior confiança na utilização do mesmo, sem falar das garantias de segurança electrónica que impossibilitem a violação da privacidade do cidadão, impedindo o acesso a quaisquer dos seus dados pessoais sem o seu consentimento expresso.