Voto Electrónico para um Portugal Moderno

Processo de Auditoria

Relatório de Auditoria ao Sistema de Votação Electrónica – Fase de Simulação

Freguesia de Paranhos

2004-07-26

Conteúdos

0. Introdução 2
0.1 Constituição da comissão de auditoria 2

1. Processo de votação 2
1.1 Configuração do local de voto electrónico 2
1.2 Abertura das mesas 2
1.3 Processo de votação 3
1.4 Encerramento das mesas 4

2. Ocorrências anormais e constrangimentos detectados no sistema 4
2.1 Abertura das mesas 4
2.2 Processo de votação 5
2.3 Encerramento das mesas 6

3 Análise das características do sistema 7
3.1 Segurança (S) 8
3.2 Transparência (T) 9
3.3 Acessibilidade (A) 11

4. Conclusões e Recomendações 11

ANEXO – Grelha para as Conclusões e Recomendações do Relatório de Auditoria ao Sistema de Votação Electrónica (RASVE) 14
Segurança 15
Transparência 16
Acessibilidade 17

0. Introdução

0.1 Constituição da comissão de auditoria

Prof. Doutor Mário Jorge Leitão

Prof. Doutor Sérgio Reis Cunha

Prof. Doutor António Carvalho Brito

Engº Miguel Barbosa Gonçalves

1. Processo de votação

1.1 Configuração do local de voto electrónico

A Escola Preparatória de Paranhos foi o local seleccionado para o teste do voto electrónico no Porto, sendo a solução avaliada da responsabilidade da empresa Multicert. Neste local estavam instaladas catorze secções de voto, correspondendo a cerca de 14000 eleitores inscritos. O local de voto electrónico estava devidamente assinalado e, de acordo com instruções da UMIC, só era solicitado aos eleitores para experimentarem esta nova forma de votação depois de votarem pelo processo tradicional, ficando também claro que esta segunda votação era apenas um ensaio, não tendo por isso qualquer valor oficial.

Para esse efeito foram instaladas duas mesas de voto electrónico, cada uma servindo metade dos eleitores inscritos. A equipa responsável por cada uma das mesas era constituída por um presidente e dois vogais. Cada mesa estava equipada com um computador, dois monitores, sendo um apenas uma réplica de apoio, e uma urna de voto contendo um leitor de cartões, sendo o conjunto alimentado através de uma UPS. Para apoio a cada mesa foram instaladas quatro cabinas de votação, estando cada uma equipada com um computador, um monitor de ecrã táctil e um leitor de cartões. Foram entregues três cartões, com assinaturas digitais, ao presidente e a dois vogais de cada mesa.

1.2 Abertura das mesas

Pelas 8h foi iniciado o processo de arranque das mesas pelos dois responsáveis da Multicert. O primeiro passo consistiu na importação do caderno eleitoral, para o que foi necessária a presença do representante da UMIC, que introduziu a palavra-chave de acesso. De seguida, procedeu-se à abertura da mesa através da introdução sucessiva dos cartões do presidente e dos dois vogais. Depois de indicar na aplicação o número de cabinas de voto que iam ser usadas, o presidente da mesa dirigiu-se a cada uma das cabinas procedendo à sua abertura. O processo de abertura era simples, exigindo a introdução do cartão do presidente de forma a garantir que a informação relativa aos votos da cabina pudesse ser assinada digitalmente, de maneira a que o acesso só pudesse ser feito através do cartão do presidente e fosse possível garantir que os dados eram originários daquela cabina.

A fase seguinte consistiu na inicialização de um conjunto de cartões para serem usados pelos eleitores no processo de votação. Para se dar início a esta fase e para a sua conclusão foi necessário, também, a introdução do cartão do presidente da mesa. Pelas 8h e 15min foi dado início ao processo de votação na mesa 3. Na mesa 1, devido a problemas de instalação da aplicação, os responsáveis da Multicert só conseguiram a sua abertura por volta das 10h45.

1.3 Processo de votação

O eleitor dirigia-se à mesa e apresentava o BI e o cartão de eleitor. Um elemento da mesa introduzia o número de eleitor na aplicação (que podia também pesquisar pelo nome) e, depois de confirmar a identidade do eleitor, este era adicionado à lista de eleitores em votação (lista de pendentes).

Era então entregue um dos cartões de voto ao eleitor, o qual não continha qualquer informação relativa ao votante ou a votos anteriores; apenas um certificado que garante que só os postos de votação assignados à mesa que providenciou o cartão o aceitam.

O eleitor dirigia-se à cabina de votação e introduzia o cartão, o qual é validado, dando início à sequência de votação através da escolha das opções apresentadas no ecrã táctil. O primeiro ecrã permitia a escolha da língua portuguesa ou inglesa. O ecrã seguinte, semelhante a um boletim de voto, permitia, pressionando o quadrado correspondente ao partido escolhido, marcar com uma cruz a escolha efectuada. Depois de carregar no botão de avançar, era mostrado um ecrã onde o eleitor podia confirmar a votação ou alterar o voto, regressando neste último caso ao ecrã anterior. No ecrã seguinte ao da confirmação era feito um pequeno inquérito com duas questões de resposta "sim"/"não": a primeira "se gostou desta forma de votar?"; e a segunda "se prefere esta forma de votar?".

Concluído o voto, este é cifrado com uma chave simétrica gerada pelo posto, para cada voto individual. A mesma chave é cifrada com a chave pública correspondente a uma chave privada apenas conhecida pela mesa de voto (definida durante a inicialização do sistema). Este conjunto é ainda cifrado com outra chave pública (desta feita a chave privada é conhecida da aplicação que corre no computador da mesa) e assinada com a chave privada do posto de votação (as chaves públicas dos postos de votação foram dadas a conhecer à mesa no acto de inicialização do sistema). Esta informação cifrada e assinada é gravada no cartão de voto, ocupando cerca de 8 Kbytes. Enquanto decorria este conjunto de operações, o eleitor devia aguardar a indicação no monitor para retirar o cartão do leitor.

Seguidamente, o eleitor levava o cartão para a mesa e inseria-o no leitor da urna. No ecrã da aplicação, uma das zonas apresentava os eleitores em votação (pendentes). Quando o cartão era inserido na urna, o elemento da mesa premia o botão "aceitar voto" correspondente ao nome do eleitor que se encontrava com o cartão inserido na urna. O voto é então descarregado no seu estado de cifrado e assinado para uma base de dados. Apesar de se identificar o eleitor a partir da lista de pendentes (com vista a lhe serem devolvidos os elementos de identificação), os elementos da Multicert garantem que não há qualquer associação entre o eleitor e o voto do cartão inserido na urna. Tão-pouco é associada qualquer marca temporal, nem a base de dados é ordenada por ordem de inserção, visando impedir a identificação do eleitor responsável por cada voto. Se o processo de leitura do cartão na urna não fosse bem sucedido, o elemento da mesa podia seleccionar o botão "recusar voto", ficando o eleitor novamente em condições de repetir o processo de votação.

Descarregado o voto do cartão para a base de dados, o cartão era limpo de qualquer informação relacionada com o voto. Era-lhe introduzido um novo certificado (gerado no momento) por forma a permitir que outro eleitor o possa usar. Este passava então para o lote de cartões disponíveis, enquanto que ao eleitor eram devolvidos os elementos de identificação. Visualmente, na lista de eleitores do ecrã, era possível confirmar através de um pequeno círculo, à esquerda do nome do eleitor, se este já tinha votado (cor verde) ou não (cor vermelha).

1.4 Encerramento das mesas

Terminado o processo de votação, a mesa de voto foi fechada por um processo semelhante ao de inicialização da mesma. São necessários os mesmos três cartões (na posse de cada um dos elementos da mesa). A aplicação impõe que este acto esteja devidamente concluído para permitir a contagem dos votos.

Fechada a mesa de voto, torna-se possível proceder ao apuramento de votos, bastando para tal seleccionar uma opção do programa. Neste processo, a base de dados de votos cifrados e assinados é lida. Cada voto é descodificado apenas nessa altura e inserido noutra base de dados. Segue-se a contagem de votos e apresentação de resultados no ecrã, com possibilidade de impressão.

Independentemente da contagem de votos, a base de dados de eleitores (que serviu de apoio à identificação de eleitores) pode ser destruída. Este processo de destruição teve que ser executado por intervenção directa do responsável da Multicert (e não de forma automática).

Fechadas as mesas de voto, pouco depois das 19h00 (após todos os eleitores presentes na sala, em espera desde antes das 19h00, terem concluído a votação), procedeu-se ao apuramento de resultados. Verificou-se então que a mesa 1 registou 406 eleitores/votos e que a mesa 2 registou 628. A diferença resulta do facto da mesa 1 apenas ter começado a operar mais tarde, conforme já descrito. Contudo, enquanto que a mesa 1 produziu resultados da votação conforme o esperado, no ecrã do computador da mesa 2 apareceu uma mensagem que indicava não ser possível concluir essa operação. Após diversas tentativas, não foi possível apurar os resultados (ver secção 2.3).

2. Ocorrências anormais e constrangimentos detectados no sistema

A percepção presencial do processo de votação permitiu detectar um conjunto de ocorrências anormais e identificar alguns constrangimentos do sistema que deverão ser resolvidos no futuro.

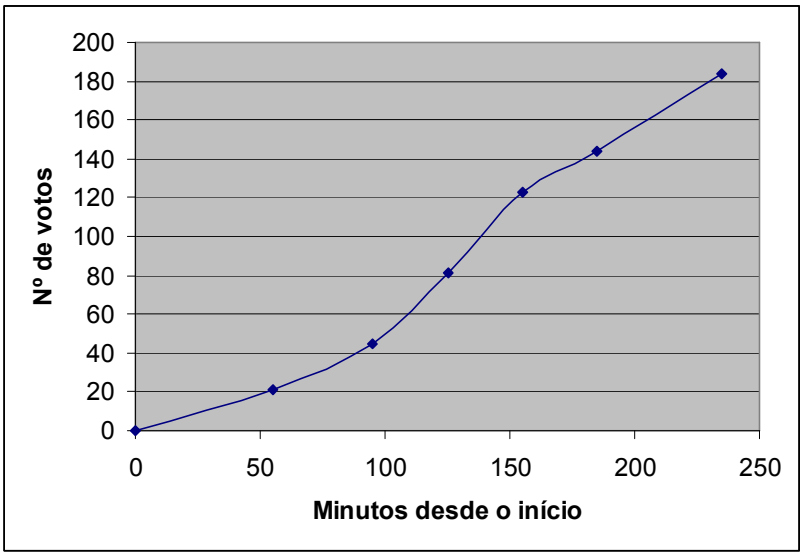
2.1 Abertura das mesas

Como foi referido, só foi possível abrir a mesa 1 cerca das 10h45. Como os eleitores estavam rigidamente distribuídos pelas duas mesas, este atraso penalizou muitos potenciais eleitores. Para colmatar esta eventualidade, sugere-se que, em ocasiões futuras, o processo de abertura possa ser feito com a devida antecedência de forma a garantir a abertura à hora marcada.

2.2 Processo de votação

Em relação ao processo de votação, a avaliação preliminar constatou períodos de tempo excessivos em certas operações e alguns pontos de bloqueio que reduziram significativamente o fluxo de votantes. De facto, tenha-se em conta que a mesa que esteve permanentemente aberta registou apenas 628 votos. Perante o facto de nenhuma das mesas ter estado em algum instante inactiva por falta de eleitores, pode concluir-se pela insuficiente capacidade do sistema. Acresce ainda que os eleitores esperavam em média cerca de 30 minutos para acederem pela primeira vez à mesa de voto. Se, por um lado, este valor é manifestamente exagerado, por outro mostra a adesão que o sistema teve junto da população, bem como o entusiasmo demonstrado no acolhimento desta iniciativa.

No gráfico seguinte representa-se a evolução da votação da mesa 2 nas primeiras 4 horas. Como se pode observar, há um período inicial mais lento, que correspondeu à existência de alguns problemas na leitura dos cartões de voto e também à pouca experiência na utilização do sistema por parte da mesa, que foi melhorando ao longo do dia.



Analisando com maior detalhe os tempos, verificou-se o seguinte:

- O processo de identificação do eleitor, desde a apresentação da identificação até à entrega do cartão de voto, demorou em média menos que 10 segundos.
- O processo de votação, incluindo deslocações entre a mesa e os postos de votação, demorava cerca de um a dois minutos.
- Já com o voto concluído e armazenado no cartão, o tempo médio que cada eleitor esperava junto da mesa até ser de novo atendido rondava os dois minutos. Não só este tempo se deve a outros eleitores a completar, à sua frente, o mesmo processo, como também ao atendimento de novos eleitores. Obviamente, os novos eleitores também sofriam severos atrasos derivados da necessidade de a mesa processar os votos.
- O número médio de eleitores em votação situava-se entre os 3 – 4.
- O processo de descarga do voto, re-identificação do eleitor e passagem deste do estado de pendente para o estado de ter efectuado a votação demorava cerca de 30 segundos. Durante

este tempo a mesa não podia efectuar outras operações em paralelo, o que limitou a capacidade do sistema.

Mantendo-se estas condições, dificilmente se conseguiria que mais do que 1 eleitor votasse em cada minuto. A esta taxa corresponderia, em 11h de abertura da mesa, um número estimado de cerca de 660 votantes, com tempos de espera inaceitáveis. Atendendo a que a uma mesa de voto tradicional estão atribuídos cerca de 1000 eleitores, a taxa estimada para este processo é manifestamente insatisfatória. Levantada esta questão junto dos responsáveis da Multicert, considerou-se que, alterando o sistema, não seria difícil reduzir os tempos de leitura de forma a eliminar estes estrangulamentos. Apesar desta melhoria, haveria igualmente que ajustar o processo do ponto de vista da disposição física dos vários componentes do sistema.

Há ainda outros aspectos que terão de ser revistos:

- Até o voto cifrado e assinado ser gravado decorrem alguns segundos. Ainda que este tempo seja reduzido, pode sempre gerar-se uma situação em que os eleitores retiram os cartões da respectiva ranhura antes da gravação estar concluída, o que resulta em cartões com informação inconsistente, inviabilizando a sua posterior leitura na urna (problema resolúvel com inicialização do cartão e repetição do processo de voto). Para evitar esta debilidade, os leitores deverão ser de retenção, e não de inserção.
- Seria melhor, até por uma questão de transparência, que não houvesse a possibilidade de criar a suspeição de que se possa associar o cartão na urna com o correspondente eleitor. Ou seja, o processo de recolha de voto deveria ser independente do processo de autenticação do eleitor. Adicionalmente, o eleitor deveria ser capaz de acompanhar a evolução do processo de votação, o que não acontecia, uma vez que os ecrãs se encontravam virados para os elementos da mesa, situação que fere igualmente a imagem de transparência do acto.
- A lista de eleitores votantes e não votantes era só visível aos elementos da mesa. Seria desejável que o eleitor pudesse ter também alguma indicação de que o seu voto tinha sido aceite - por exemplo, a visualização do incremento unitário do número de votos entrados, após a leitura do seu voto.
- Será necessário disponibilizar pontos de experimentação à entrada das mesas de voto, e não no seu interior, onde o eleitor poderá testar todas as fases do processo e solicitar apoio quando necessário.

2.3 Encerramento das mesas

Verificou-se o potencial problema de não se poderem apurar os resultados por falta, na altura do fecho da votação, de qualquer dos cartões (por extravio ou este estar em más condições).

A ocorrência mais grave foi a impossibilidade de apurar os resultados da mesa 2, que criou um verdadeiro cenário de crise, visto que a incapacidade de recuperação de resultados após a conclusão de um acto eleitoral é um dos piores pesadelos de um sistema eleitoral.

As primeiras tentativas para resolver o problema passaram pela substituição de versões de software. Se, por uma lado, numa situação real tal implicasse naturalmente a anulação dos resultados dessa

mesa, permitiu por outro constatar virtudes do sistema ser relativamente aberto, centrado na cifragem dos votos, o que gera confiança perante algum grau de intervenção sobre o sistema.

Tendo estas tentativas fracassado, passou-se à análise dos conteúdos das bases de dados. Verificou-se que a base de dados de votos cifrados estava preenchida, enquanto que a de votos já interpretados estava vazia. Pôde constatar-se então que o problema de apuramento de resultados residia na interpretação dos elementos cifrados. Verificou-se também que o sistema permite que haja acesso aos votos cifrados e às chaves que os permitem decifrar através de processos alternativos à aplicação que suporta o processo de votação. Com efeito, apenas o facto do computador não estar ligado em rede durante o acto eleitoral e ter estado sempre sob a alçada da mesa permite assegurar que tal não aconteceu.

Não existindo capacidade de decifrar os votos no local de votação, procedeu-se do seguinte modo:

- As bases de dados com informação sobre os eleitores foram destruídas e foi garantido que não restava informação latente sobre o conteúdo das mesmas nos discos dos computadores.
- Foram feitas cópias para CDs do conteúdo das bases de dados dos votos e das chaves. Essas cópias foram entregues à Multicert (para permitir analisar o problema), à equipa da FEUP, à mesa de voto, ao representante da CNPD e à UMIC.
- O computador da mesa foi fechado na sua caixa, a qual foi tornada inviolável com o material disponível na altura, tendo a UMIC procedido à sua entrega na Junta de Freguesia.

Posteriormente, no dia 16 de Junho, veio a Multicert, em reunião ocorrida na FEUP com a presença de representantes da UMIC, expor sobre o problema de apuramento de resultados. Um erro durante o processo de inicialização conduziu a que alguns votos tenham sido cifrados com uma chave pública correspondente a uma chave privada da mesa entretanto substituída. Tal conduziu à impossibilidade de recuperar esses votos. No caso de Paranhos, tal apenas afectou entre 2 e 3 votos. Perante a conclusão pela pouca relevância dos resultados eleitorais em si e por não ser necessária qualquer outra análise ao conteúdo do computador da mesa 2, este, até à altura à guarda da Junta de Freguesia de Paranhos, foi no fim dessa reunião entregue à Multicert.

Para evitar que esta situação se repita no futuro é necessário:

- Verificar que o voto é consistente relativamente às chaves necessárias para o interpretar no momento da sua entrega à mesa de voto. Doutro modo, não é possível garantir que qualquer erro de procedimento não conduza à anulação do acto, ainda que localmente. Tal verificação não pode comprometer, contudo, as premissas sobre as quais se sustentam o acto eleitoral.
- Proceder ao armazenamento da informação sobre os votos de forma segura e robusta, nomeadamente por processos redundantes e distintos.

3 Análise das características do sistema

Nesta secção faz-se uma análise detalhada do sistema de votação electrónica, em função de um conjunto de parâmetros especificados na grelha anexa

3.1 Segurança (S)

3.1.1 Auditabilidade

A implementação actual não exibia características satisfatórias em termos de auditabilidade. Contudo, tem potencial para vir a ser no futuro auditável, dado que se baseia em componentes criptográficas, o que permite, no limite, tornar o código completamente aberto sem perda de segurança.

3.1.2 Autenticação do Operador

A autenticação dos membros da mesa é efectuada por cartão (três em simultâneo). O sistema é seguro, embora possa perder operacionalidade na circunstância de extravio ou avaria de qualquer dos cartões.

3.1.3 Certificabilidade

O sistema tem potencial para certificação pelas razões apontadas em 3.1.1.

3.1.4 Fiabilidade

O sistema é globalmente complexo por forma a satisfazer um conjunto vasto de requisitos, dos quais se destaca a segurança. Em contrapartida, requer esforço adicional de desenvolvimento para adquirir a necessária robustez. Esse objectivo não foi atingido com a implementação actual, o que se compreende face ao tempo que a empresa dispôs para implementar o sistema.

3.1.5 Detectabilidade

Esta questão não se coloca nesta fase, uma vez que o sistema não operava em rede.

3.1.6 Disponibilidade do Sistema

Os problemas de indisponibilidade numa das mesas no início da votação são justificáveis pelo facto de o sistema estar na fase de protótipo, ainda sujeito a alterações de última hora.

3.1.7 Imunidade a Ataques

A arquitectura criptográfica do sistema assegura uma adequada protecção contra ataques relativos a adulteração de votos, com excepção da possibilidade de eliminação de votos numa configuração de ligação de rede dos computadores das mesas.

3.1.8 Integridade dos Votos

Como referido no ponto anterior, o único risco é a eliminação de votos.

3.1.9 Invulnerabilidade

A implementação actual do sistema é demasiado aberta, na perspectiva de que os administradores de sistema podem aceder a toda informação contida nas bases de dados, ainda que cifrada.

3.1.10 Rastreabilidade

Nesta etapa de desenvolvimento do sistema, ainda na fase de protótipo, não foram identificados eventos que fosse necessário registar para posterior análise.

3.1.11 Recuperabilidade

O sistema funcionou sem problemas perante dois episódios que exigiram o rearranque do computador da mesa.

3.1.12 Tolerância a Falhas

A total dependência do sistema em mecanismos de criptografia, que não recorrem a redundância, gerou um sério problema de recuperação de votos já relatado em 2.3. Este aspecto requer revisão.

3.1.13 Isolamento

Verificou-se que todos as máquinas envolvidas no processo, sendo computadores pessoais, apresentam todas as interfaces típicas dos mesmos, ainda que visivelmente desconectadas.

3.1.14 Segurança das comunicações

Não foi testada na instalação de Paranhos.

3.1.15 Escalabilidade do Sistema

O sistema mostrou ser escalável desde que utilizado em regime de voto local com replicação total do sistema para mais unidades (quer postos de votação quer mesas).

3.2 Transparência (T)

3.2.1 Anonimato

O sistema não faz prova de anonimato porque o caderno eleitoral e o sistema de recolha de votos encontram-se suportados na mesma máquina. Acresce o facto de o eleitor ser identificado no acto de depósito do seu voto.

3.2.2 Atomicidade

Não se detectaram problemas de atomicidade a não ser os resultantes de incorrecto procedimento dos elementos da mesa em termos de troca de eleitores.

3.2.3 Autenticidade (método de autenticação do utilizador)

Identificação presencial semelhante ao processo tradicional.

3.2.4 Confiabilidade

Os problemas de juventude do sistema limitaram a confiabilidade no sistema na sua forma actual.

3.2.5 Documentação técnica

Não foi apresentada documentação técnica relativamente ao sistema.

3.2.6 Integridade do Pessoal

O sistema dependeu do comportamento íntegro dos elementos da mesa e da Multicert, que o mostraram ser. Ficou evidente a necessidade de qualquer sistema de votação electrónico depender exclusivamente da integridade dos elementos da mesa.

3.2.7 Integridade do Sistema

Verificaram-se alterações de última hora nas versões do *software* utilizado o que compromete qualquer teste de integridade.

3.2.8 Não-Coercibilidade

Garantida pelo facto de o voto ser presencial, tal como no voto tradicional.

3.2.9 Precisão do SVE

O sistema falhou no aspecto da robustez o que limita a sua precisão. No caso de Paranhos não foi possível determinar o conteúdo de dois ou três votos.

3.2.10 Privacidade

O sistema garante privacidade. Inclusive, os votos são armazenados sem correspondência com a sequência de entrada dos mesmos.

3.2.11 Singularidade (Não Reutilização)

O sistema garante a singularidade do voto.

3.2.12 Transparência do Processo

Os factos de o posto da mesa ser único para processar o caderno eleitoral e armazenar votos e de se identificar o eleitor no momento em que ele descarrega o voto na urna fragiliza fortemente a percepção de transparência do processo.

3.2.13 Transparência do Sistema

Devido à possibilidade de todo o código poder ser tornado público este sistema apresenta excelentes qualidades no que se refere à sua transparência.

3.2.14 Verificabilidade

O sistema permite verificar se os votos foram devidamente armazenados e contados.

3.2.15 Separação de papéis

Havia possibilidade e houve necessidade de elementos da Multicert intervirem sobre o sistema durante a votação (vide 3.1.11). O mesmo se passou no processo de fecho das mesas e posterior contagem dos votos.

3.3 Acessibilidade (A)

3.3.1 Conveniência

O elevado tempo de descarga dos votos na urna gerou, tal como exposto em 2.2, tempos de espera inaceitáveis. Esta situação é passível de ser facilmente corrigida.

3.3.2 Direito de Voto

O sistema funcionou sem limitações inerentes ao mesmo.

3.3.3 Documentação para eleitor

O folheto explicativo revelou ser insuficiente. Sugere-se a instalação de um equipamento de demonstração funcionalmente análogo ao sistema real.

3.3.4 Flexibilidade

Não foi disponibilizado equipamento específico para pessoas com necessidades especiais.

3.3.5 Mobilidade

Esta propriedade não constitui um requisito do sistema. Contudo, a arquitectura deste sistema tem características adequadas para o futuro suporte de mobilidade.

3.3.6 Usabilidade

O sistema é globalmente satisfatório em termos de facilidade de utilização. No entanto, apresentou deficiências significativas em termos de rapidez já descritas na secção 2 e que poderão ser supridas em futuras evoluções.

3.3.7 Viabilidade (Custo/Benefício)

Só se obterá uma relação custo/benefício que supere o processo tradicional se for suportada a mobilidade. Este é o benefício que pode justificar o custo.

4. Conclusões e Recomendações

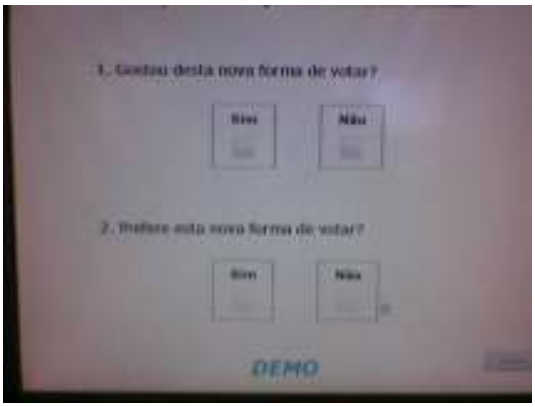
Seguem-se as conclusões e recomendações mais importantes relativamente ao sistema apresentado pela Multicert:

- O sistema apresentava alguns problemas de juventude ao nível da implementação. Tal é perfeitamente compreensível, atendendo ao pouco tempo que esta empresa teve disponível para o efeito.

- O facto de o eleitor ser identificado no acto do seu voto ser descarregado para a urna gera um sério problema de transparência. É necessário demonstrar ao eleitor que não fica registado (nem pode ficar) qualquer associação entre eleitor e voto. Embora a existência de uma lista de eleitores pendentes tenha sido uma imposição da UMIC, o tratamento dado a este problema pelas outras empresas, ainda que imperfeito, atenuava este problema.
- A não separação entre processo de identificação e descarga dos votos gerou problemas operacionais e pequena capacidade de processamento de eleitores.
- O armazenamento dos votos num único ponto por mesa de voto (em vez de o ser no posto de votação) tem vantagens operacionais, especialmente num cenário futuro em que se pretenda a mobilidade dos eleitores entre várias possíveis mesas de voto.
- A segurança providenciada por um sistema de chaves e em métodos de domínio público tem a enorme vantagem de permitir abrir o sistema. Tal advoga em favor da transparência, da facilidade de evolução da infraestrutura de suporte e consequentemente da escalabilidade da solução.
- A segurança do sistema implica grande robustez e cuidado no armazenamento e processamento da informação, sob o perigo constatado desta se perder. Tais características de robustez são ainda muito insuficientes.
- O sistema apresentado apresenta características compatíveis com a evolução do sistema para um cenário de mobilidade presencial (possibilidade dos eleitores votarem em mesas de voto que não necessariamente aquelas onde estão inscritos, mas presencialmente). Neste cenário, as mesas de voto terão que estar ligadas em rede, nem que seja apenas para garantir que cada eleitor apenas vota uma vez. A necessidade de transporte do voto por forma a que este seja contabilizado no local de inscrição do eleitor (exigível para, pelo menos, eleições autárquicas) faz com que a criptografia tenha, neste cenário, um papel fundamental.

Ecrã da aplicação da mesa:

Sequência de ecrãs na cabina de votação:



ANEXO – Grelha para as Conclusões e Recomendações do Relatório de Auditoria ao Sistema de Votação Electrónica (RASVE)

Apresenta-se de seguida a classificação resumo da Grelha de Avaliação usada na auditoria efectuada.

Segurança

		-				+
SEGURANÇA (S)						
S	**Auditabilidade**			X		
	O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.					
S	**Autenticação do Operador**				X	
	Os utilizadores autorizados a operar o sistema devem ter mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjunção de alguns dos tipos de autenticação existentes. Por exemplo: cartão inteligente («Smartcard»), PIN ou senha, ou ainda autenticação bio-métrica – impressões digitais, retina ocular e voz.					
S	**Certificabilidade**			X		
	O sistema deve poder ser testado e certificado por agentes oficiais.					
S	**Fiabilidade**			X		
	O SVE deve funcionar de forma fiável, sem perda de votos.					
S	**Detectabilidade**					
	O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.					
S	**Disponibilidade do Sistema**				X	
	Durante o período eleitoral, o SVE deve estar sempre disponível para todos os actores legítimos, em particular para os eleitores votantes, para que o processo decorra normalmente.					
S	**Imunidade a Ataques**					X
	Medidas de defesa contra fraudes, inclusive vindas dos próprios agentes que projectaram e desenvolveram o sistema, devem ser rigorosas e redundantes. Um SVE, tal como outros sistemas de alto risco, pode ser alvo privilegiado de ataques mal intencionados.					
S	**Integridade dos Votos**				X	
	Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.					
S	**Invulnerabilidade**		X			
	A invulnerabilidade do SVE é a garantia de que não se pode aceder e alterar o sistema indevidamente.					
S	**Rastreabilidade**					
	O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir registos ("logs") de entrada e saída de utilizadores não eleitores ou de quaisquer outros acessos, bem como registos do envio e recepção de dados, que obviamente não comprometam as restantes propriedades (anonimato e privacidade do eleitor).					
S	**Recuperabilidade**					X
	O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.					
S	**Tolerância a Falhas**		X			
	É desejável a existência de métodos de detecção de falhas no equipamento. A troca de um bit num total de um candidato pode ser a diferença entre ganhar ou perder a eleição.					
S	**Isolamento**		X			
	Só devem existir no SVE os dispositivos de interface externos absolutamente essenciais para o acto eleitoral, sendo todos os componentes certificados e iguais a um padrão, incluindo o software.					
S	**Segurança das comunicações**					
	As comunicações entre as assembleias de voto e o sistema central utilizam mecanismos de validação de identidade de ambos (assembleia e sistema central), de não adulteração da informação e de cifragem da mesma para garantir a confidencialidade, integridade e autenticidade.					
S	**Escalabilidade do Sistema**				X	
	A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.					

Transparência

	TRANSPARÊNCIA (T)	-				+
T	**Anonimato**		X			
	A associação entre o voto e a identidade do 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).					
T	**Atomicidade**					X
	Garantia de que, em caso de falha a meio do processo, não permanecem registos ou percepções inconsistentes relativos ao mesmo. Por exemplo: registos no caderno eleitoral de votantes, mas sem registos de voto no computador; o eleitor e a mesa ficaram com a percepção de que o voto se concretizou, quando na realidade não ficou nenhum registo no computador; falha de alimentação quando o votante confirma a opção de voto no computador, como se sabe se o voto foi concretizado (por forma a tornar os registos consistentes entre si e consistentes com a percepção das pessoas envolvidas)?					
T	**Autenticidade (método de autenticação do utilizador)**					
	Autenticar o indivíduo é o meio pelo qual a identificação de um votante é validada e confirmada. Apenas os eleitores autorizados devem poder votar. Exemplos de tipos de autenticação são: presencial, PIN, senha, certificado digital, cartão inteligente ou bio-métrica.					
T	**Confiabilidade**			X		
	O SVE deve funcionar de forma fiável e robusta, tornando-se confiável aos olhos dos diversos actores envolvidos, em particular o eleitor.					
T	**Documentação técnica**	X				
	Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema, devem estar documentados, devendo não conter ambiguidades e ser coerente.					
T	**Integridade do Pessoal**					X
	O pessoal envolvido no projecto, implementação, administração e operação do SVE deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.					
T	**Integridade do Sistema**	X				
	Deve ser possível garantir em qualquer momento que o SVE que está a ser usado é o mesmo que foi validado e certificado por auditores externos, pela Comissão Nacional de Eleições e pelos membros da mesa de voto, eventualmente por um processo de amostragem.					
T	**Não-Coercibilidade**					X
	O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.					
T	**Precisão do SVE**		X			
	As eleições podem ser decididas por apenas um voto. O sistema não pode tolerar margens estatísticas de erro durante a sua operação.					
T	**Privacidade**				X	
	O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.					
T	**Singularidade (Não Reutilização)**					X
	O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.					
T	**Transparência do Processo**		X			
	Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.					
T	**Transparência do Sistema**					X
	Todo o software, documentação, equipamento, micro-código e circuitos especiais devem poder ser abertos para inspecção e auditoria a qualquer instante. Deve ser conhecido o formato dos dados registados e transmitidos.					
T	**Verificabilidade**				X	
	O sistema deve permitir verificar que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a autenticidade dos registos dos votos, sem no entanto quebrar outras propriedades como o anonimato ou a privacidade do votante.					
T	**Separação de papéis**			X		
	O fabricante do SVE, o instalador e o operador não devem ser da mesma instituição ou empresa. Os únicos operadores do SVE durante o acto eleitoral devem ser elementos da mesa de voto ou elementos previamente acreditados pela Comissão Nacional de Eleições.					

Acessibilidade

		-				+
ACESSIBILIDADE (A)						
A	**Conveniência**		X			
	O sistema só será útil se permitir aos votantes exercerem o seu direito de voto de forma rápida, com o mínimo de equipamento, treino e sem necessidades específicas adicionais.					
A	**Direito de Voto**					X
	O Direito de Voto será atribuído a um eleitor sempre que ele verifique simultaneamente as propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de ele poder votar.					
A	**Documentação para eleitor**			X		
	O eleitor deve ter acesso com a antecedência adequada a informação de compreensão simples sobre o SVE e as suas características.					
A	**Flexibilidade**	X				
	Os equipamentos de votação que fazem parte do SVE devem suportar uma variedade de questões relacionadas com o processo de votação, com por exemplo a utilização por pessoas com necessidades especiais, etc.					
A	**Mobilidade**					
	O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.					
A	**Usabilidade**				X	
	O sistema deve ser de uso fácil e rápido, quer para eleitores quer para operadores (membros da mesa de voto). A interface do SVE, a linguagem e os termos utilizados, deve ser acessíveis aos eleitores e aos elementos que participam no processo eleitoral, não devendo ser necessário que estes tenham conhecimentos informáticos especializados. A localização, orientação e altura do monitor devem ser apropriadas ao eleitor. Um erro involuntário de um eleitor, mal treinado para votar em dado equipamento, pode inverter ou modificar o resultado eleitoral.					
A	**Viabilidade (Custo/Beneficio)**					
	O SVE deve ser eficiente e viável economicamente.					