Auditoria ao Projecto de Voto Electrónico

Eleições Legislativas de 20 de Fevereiro de 2005

Relatório Final

Sistema MULTICERT

Faculdade de Engenharia da Universidade do Porto

Porto, 15 de Abril de 2005

FEUP Rua Dr. Roberto Frias
4200-465 Porto
jfcunha@fe.up.pt
Tel.: 22 508 1639
Fax: 22 508 1538

Auditoria ao Projecto de Voto Electrónico

Conteúdos

Página

1 Introdução

Este relatório apresenta os resultados preliminares da auditoria efectuada por uma equipa de auditoria da FEUP ao sistema de voto electrónico (SVE) da Multicert, utilizado em 7 locais de voto na freguesia de Santa Iria de Azóia na experiência piloto das eleições legislativas de 20 de Fevereiro de 2005.

1.1 Comissões de auditoria envolvidas

A auditoria ao SVE da Multicert envolveu os seguintes elementos da equipa:

- Prof. João Pascoal Faria - relator
- Prof. Raul Moreira Vidal
- Eng. Miguel Barbosa Gonçalves
- Prof. Gabriel David
- Prof. Mário Jorge Leitão
- Prof. António Carvalho Brito
- Prof. Maria Henriqueta Nóvoa
- Prof. António Pimenta Monteiro
- Prof. Sérgio Reis Cunha

A experiência de votação electrónica com sistemas Multicert na freguesia de Santa Iria de Azóia no dia das eleições de 20 de Fevereiro de 2005 foi acompanhada pelos elementos das comissões de auditoria da FEUP indicados na tabela seguinte.

Local de Voto	**Período**	**Auditor**
Grupo Desportivo de Pirescoxe	7h30-11h15 (abertura)	Gabriel David
Casa da Cultura de Santa Iria de Azóia	7h30-11h15 (abertura)	Raul Moreira Vidal
Atlético de Via Rara AVR	11h30 - 13h15	Mário Jorge Leitão
Sociedade Recreativa 1º de	13h30 – 14h00	Mário Jorge Leitão

Agosto Santairiense		
AMUPA	12h15 - 13h45	António Carvalho Brito
Escola Básica nº 2	14h30 - 16h	Maria Henriqueta Nóvoa
Escola Básica nº 1	13h30 - 15h30	António Pimenta Monteiro
Grupo Desportivo de Pirescoxe	17h - 20h (fecho)	João Pascoal Faria

1.2 Fontes de informação

Este relatório foi elaborado com base nas seguintes fontes:

- observações efectuadas pelos auditores da FEUP nos 7 locais de voto electrónico em Santa Iria de Azóia no dia das eleições;
- reunião com técnicos da Multicert, nas suas instalações na Rua Engº Ferreira Dias, 433, 1º, no Porto, no dia 1 de Março de 2005, entre as 10h00 e as 13h00, em que estiveram presentes, pela Multicert, Pedro Borges e Luis Félix, e pela FEUP, João Pascoal Faria, Raul Vidal, Miguel Gonçalves e Sérgio Reis Cunha;
- os seguintes elementos fornecidos gentilmente pela Multicert: resultados nos vários locais de voto em Santa Iria de Azóia e "screen shots" das aplicações;
- folheto de apresentação do voto electrónico (da UMIC, STAPE e CNE), de onde foi adoptada alguma nomenclatura;
- informação diversa facultada pela UMIC;
- mensagens de correio electrónico trocadas com técnicos da Multicert, para obtenção de esclarecimentos adicionais.

De notar que, em mensagem de 24 de Fevereiro de 2005, foi solicitada à Multicert "documentação que eventualmente tenham sobre o sistema", mas essa documentação não foi fornecida à comissão de auditoria até à data da escrita deste relatório. A ausência dessa documentação levou-nos a detalhar um pouco mais o capítulo 2 deste relatório.

1.3 Acrónimos e abreviaturas

CVE - Cabine de Voto Electrónico, mesmo que PVE

PVE - Posto de Votação Electrónica, mesmo que CVE

SVE - Sistema de Voto Electrónico

2 Apresentação do SVE – Sistema de Voto Electrónico

Na experiência de votação electrónica na freguesia de Santa Iria de Azóia com sistemas Multicert esteve em causa, para além da votação electrónica presencial, a mobilidade dos eleitores, ainda que apenas dentro de uma freguesia.

2.1 Arquitectura do SVE

Em termos de arquitectura física, pode considerar-se o SVE da Multicert subdividido em três sub-sistemas relativamente independentes entre si:

- caderno eleitoral electrónico, para identificar os eleitores e autorizar a sua votação, funcionando em rede por forma a suportar a mobilidade dos eleitores;
- cabines ou postos de voto electrónico [1], para os eleitores registarem as suas opções de voto;
- urnas electrónicas, para armazenar os votos dos eleitores.

A comunicação entre estes sub-sistemas ocorre apenas através de pequenos dispositivos de armazenamento (*i-buttons*) que, em certa medida, fazem as vezes dos boletins de voto em papel no sistema tradicional.

A Multicert, em parceria com a PT Inovação, desenvolveu também um protótipo de um sistema de votação por telemóvel, pensado para eleitores com necessidades especiais, que será analisado separadamente.

Segue-se uma descrição detalhada de cada um dos elementos do SVE.

2.1.1 Caderno eleitoral electrónico

Para suportar a mobilidade dos eleitores, ainda que apenas na vertente de identificação, a Multicert desenvolveu uma nova versão do caderno eleitoral electrónico (em relação à

[1] Mantém-se a designação "cabines de voto electrónico" que aparece no folheto publicado pela UMIC, apesar de os postos de votação electrónico não estarem protegidos por qualquer tipo de painéis como numa cabine tradicional.

versão desenvolvida para as eleições de 13 de Junho de 2004 [2]), funcionando em rede, e assentando numa base de dados central. Esta nova versão foi experimentada nos 7 locais de votação electrónica da freguesia de Santa Iria de Azóia.

Em cada secção de voto electrónico, para utilização pela mesa de voto, é instalado um computador cliente (ao centro na Figura 1), com sistema operativo Windows, no qual executa a aplicação cliente do caderno eleitoral electrónico, desenvolvida pela Multicert em tecnologia Microsoft .NET.

Num local central apropriado (em Santa Iria de Azóia foi escolhida a Casa da Cultura), é instalado um computador servidor, com sistema operativo Windows, contendo a base de dados central do caderno eleitoral (em SQL Server) e software servidor (apenas o SQL Server).

Durante o período eleitoral, os computadores clientes estão conectados ao computador servidor através da rede telefónica fixa (por ADSL) ou móvel (por UMTS), sendo as comunicações cifradas através de um túnel VPN IPSec. Nesta experiência de votação, 3 secções de voto estavam conectadas ao servidor por ADSL e 4 por UMTS. A ligação por UMTS, previsivelmente menos fiável, foi utilizada, não por ausência de telefone fixo, mas por uma questão de experimentação.

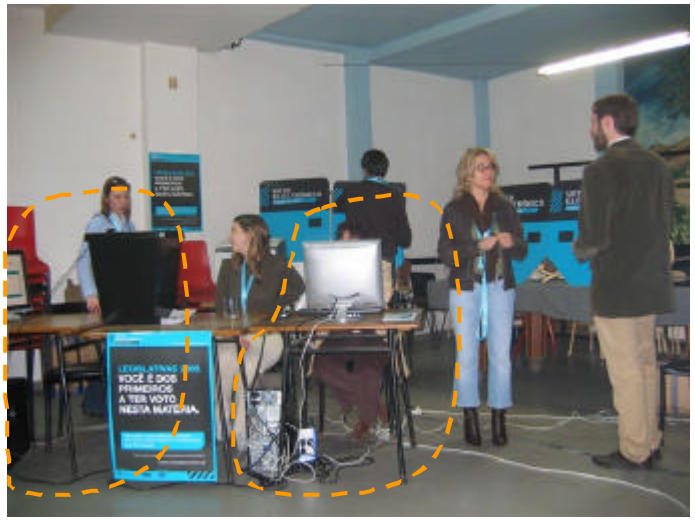

Figura 1- Pormenor da mesa de voto num dos locais de voto em Santa Iria de Azóia, vendo-se ao centro o sistema de acesso ao caderno eleitoral electrónico e do lado esquerdo o sistema da urna electrónica.

[2] De notar que a versão antiga do caderno eleitoral electrónico, desenvolvida pela Multicert para as eleições de 13 de Junho de 2004, foi usada nestas eleições (de 20 de Fevereiro de 2005) nos locais de voto com postos de votação Unysis e Indra.

Arquitectura de dados

A base de dados central do caderno eleitoral electrónico, para além de conter a lista de eleitores recenseados (neste caso, todos os eleitores recenseados pela freguesia de Santa Iria de Azóia), tem também, para cada eleitor recenseado, a indicação se já votou e em que local (mesa). Esta base de dados está localizada apenas no computador servidor, tendo os computadores clientes (localizados nas secções de voto) de se conectar ao computador servidor sempre que é necessário aceder ao caderno eleitoral. Em cada computador cliente, é mantida apenas uma pequena base de dados (em tecnologia MSDE) dos eleitores que já votaram nessa secção, para facilitar a apresentação ao utilizador da lista de eleitores que já votaram (lista de votantes no lado superior esquerdo da Figura 2) e detectar localmente tentativas de segunda votação, poupando essa comunicação com a base de dados central. Em caso de falha de comunicação com o computador servidor, não é possível autorizar nenhum eleitor a votar (apenas é possível negar a autorização a eleitores que porventura já tenham votado na mesma secção). A aplicação cliente comunica com a base de dados remota (mais precisamente com o motor SQL Server localizado na máquina servidora) por ADO.NET, usando uma conta (login/password) específica da aplicação para efeito de autenticação.

Mecanismos de protecção

Não foram implementados mecanismos de armazenamento redundante dos dados do caderno eleitoral electrónico no servidor (nomeadamente a indicação de quem já votou). Em caso de perda da base de dados com essa informação antes de terminado o acto eleitoral, as eleições poderiam ter de ser repetidas, a não ser que se conseguisse recuperar a indicação de quem já votou a partir das bases de dados residentes em cada máquina cliente com a informação dos eleitores que votaram nessa secção de voto (esta última hipótese não foi adiantada pela Multicert).

Numa configuração definitiva, a intenção é que tanto o servidor como as máquinas clientes do caderno eleitoral electrónico, assim como os routers/modems usados na comunicação, estejam equipados com UPS.

Utilização do caderno eleitoral electrónico

A aplicação cliente do caderno eleitoral é usada pelos membros da mesa de voto durante o período eleitoral para autorizar os eleitores a votar e assinalar os eleitores que já votaram, de acordo com o Procedimento 1 a seguir descrito. Uma imagem da aplicação é apresentada na Figura 2.

Procedimento 1 - Validação de um eleitor no caderno eleitoral electrónico

1. Quando um eleitor se dirige à mesa de voto com os seus documentos de identificação, um membro da mesa começa por procurar o seu registo no caderno eleitoral electrónico, usando um dos critérios de pesquisa disponíveis (Figura 2 - canto inferior direito).
2. O sistema mostra então uma lista de eleitores que obedecem ao critério de pesquisa, assinalando de forma diferente os eleitores que já votaram.
3. O membro da mesa selecciona o eleitor pretendido da lista apresentada pelo sistema, e selecciona a opção "Autorizar Votação" (Figura 2 - lado direito centro).
    a. Se o eleitor já tiver votado, a opção "Autorizar Votação" está desactivada.
4. Nesse momento, o sistema muda o estado do eleitor na base de dados central do caderno eleitoral electrónico (através da chamada remota a uma *stored procedure*) para "Voto efectuado" (apesar de na realidade o eleitor ainda não ter concretizado o seu voto), registando também o local em que o voto foi efectuado.
    a. No caso de o eleitor não chegar a concretizar o seu voto ou ocorrer algum engano (o que se espera seja muito raro), está disponível uma operação de "Cancelar voto" (Figura 2 - lado direito centro), que exige uma autenticação especial (a inserção dos *i-buttons* de 2 membros da mesa) e só está disponível na mesma secção em que o voto foi autorizado.
    b. Segundo os técnicos da Multicert, no caso de duas mesas tentarem simultaneamente autorizar a votação do mesmo eleitor (por engano ou por tentativa de fraude), apenas uma o conseguirá fazer com sucesso, recebendo a outra uma mensagem de erro. No entanto, esta situação não foi testada pelos auditores, nem foi inspeccionado o código da *stored procedure* em causa.

De notar que, na versão antiga do caderno eleitoral electrónico (experimentada nas eleições de 13 de Junho de 2004, bem como nestas eleições de 20 de Fevereiro de 2005 nos locais de voto com postos de votação Unysis e Indra), os eleitores eram colocados numa lista de eleitores pendentes enquanto não concluíam a sua votação, o que obrigava a um segundo acesso ao caderno eleitoral electrónico para confirmar a votação ou cancelar. Nesta nova versão, para tornar os procedimentos da mesa mais expeditos e minimizar os acessos ao servidor, a Multicert optou pela solução acima descrita.

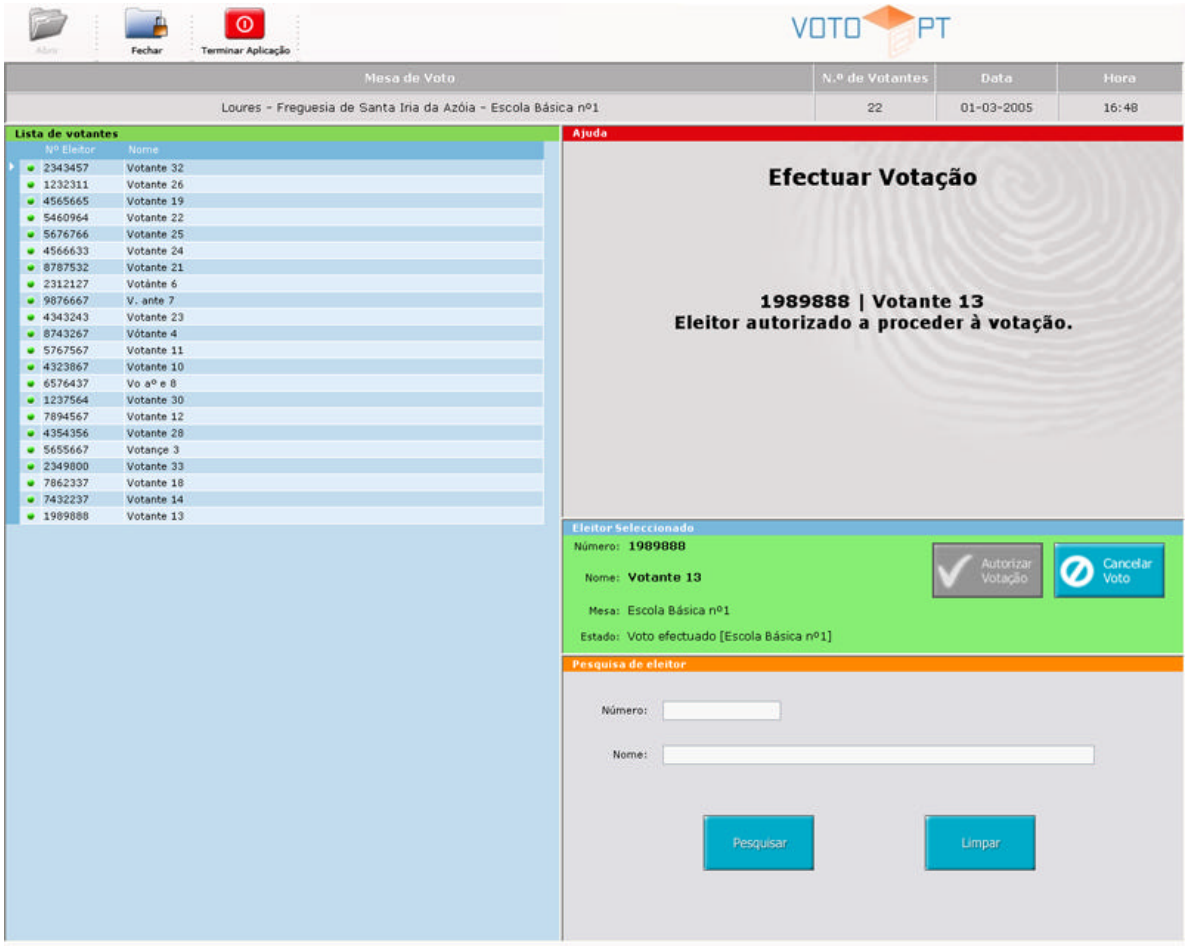

Figura 2 - Imagem do ecrã da aplicação cliente do caderno eleitoral electrónico com dados de teste, no momento imediatamente a seguir a pressionar o botão "Autorizar Votação".

Abertura do caderno eleitoral em cada secção de voto electrónico

A aplicação cliente do caderno eleitoral tem ainda opções para iniciar (Abrir) e encerrar (Fechar) o acto eleitoral em cada secção de voto (Figura 2 - canto superior esquerdo).

A operação de abertura pede a inserção sucessiva dos 3 *i-buttons* destinados aos 3 elementos da mesa (presidente e dois escrutinadores), para a sua formatação e inicialização. Estes *i-buttons* serão mais tarde necessários para a realização de algumas operações críticas. Só a partir desse momento é possível autorizar a votação dos eleitores.

Fecho do caderno eleitoral em cada secção de voto electrónico

A operação de fecho requer a inserção dos 3 *i-buttons* do presidente e dois escrutinadores preparados na abertura. A partir desse momento, a aplicação permite

continuar a consultar o caderno eleitoral electrónico, mas as opções de "Autorizar Votação" e "Cancelar Voto" estão desactivadas.

No final do acto eleitoral, a base de dados local tem a informação dos eleitores que votaram nessa secção de voto. Os procedimentos a seguir para salvaguardar e arquivar esta informação não foram reportados aos auditores nem foram analisados pelos auditores.

Importação do caderno eleitoral para a base de dados central

O primeiro passo para o arranque do acto eleitoral é a importação do caderno eleitoral, de um ficheiro em formato previamente definido, para a base de dados central do caderno eleitoral. Este ficheiro foi fornecido pelo representante da UMIC presente, que introduziu a palavra-chave de acesso.

A importação é realizada através de uma aplicação desenvolvida para o efeito pela Multicert, a qual é executada localmente no computador que aloja a referida base de dados. Esta aplicação não tem mecanismos de autenticação próprios, sendo apenas necessária a autenticação como utilizador com privilégios adequados ao nível do sistema operativo.

Salvaguarda dos dados da base de dados central no final do acto eleitoral

No final do acto eleitoral, a base de dados central do caderno eleitoral tem a indicação dos eleitores que votaram e do local em que votaram.

Os procedimentos a seguir para salvaguardar e arquivar esta informação não foram reportados aos auditores nem foram analisados pelos auditores.

2.1.2 Cabines de voto electrónico

Em cada local de voto estavam disponíveis três cabines de voto electrónico[3], destinadas aos eleitores para "preencherem" o seu voto.

[3] Devido a falhas técnicas, na Escola Básica nº 1 só duas estiveram de facto operacionais.

Uma cabine de voto electrónico é um sistema baseado em computador equipado com ecrã táctil, leitor de *i-buttons* e impressora compacta com receptáculo vedado (Figura 3).

Figura 3- Pormenor de dois tipos de cabines de voto electrónico usadas em secções de voto em Santa Iria de Azóia.

Na votação em Santa Iria de Azóia foram experimentadas cabines de voto electrónico de diversos tipos (Figura 4). Em geral, as caixas de sistema e cablagens estavam visíveis, embora a intenção é que tal não aconteça numa configuração definitiva.

Figura 4 - Três tipos de cabines de voto instaladas numa das secções de voto em Santa Iria de Azóia.

As cabines de voto electrónico funcionam isoladamente durante o período eleitoral, necessitando apenas de alimentação eléctrica.

Utilização das cabines de voto electrónico

As cabines de voto electrónico permitem aos eleitores efectuar as suas opções de voto, de acordo com o Procedimento 2 a seguir descrito e as imagens da Figura 5.

Procedimento 2 - Votação de um eleitor numa cabine de voto electrónico.

1. O eleitor dirige-se a uma cabine de voto electrónico livre, e insere o *i-button* que lhe foi previamente fornecido pela mesa (e que contém uma autorização para votar em qualquer uma das cabines de voto) no leitor respectivo.
2. A cabine de voto verifica a autorização de voto e apresenta ao eleitor o boletim de voto a que tem acesso (Figura 5b).
3. O eleitor selecciona a sua opção de voto pressionando no quadrado de voto (ou no símbolo ou na designação) no ecrã e, de seguida, pressiona no botão "Votar" (o qual só fica activo depois de um quadrado da voto estar seleccionado, nem que seja a opção de "Voto em Branco) (Figura 5c).
4. A cabine de voto pede ao eleitor para confirmar a sua opção de voto (Figura 5d).
5. O eleitor confirma a sua opção pressionando o botão "Sim, Confirmo".

   Se pressionar o botão "Alterar Voto", volta ao ecrã anterior com o boletim de voto.
6. A cabine de voto grava a escolha do eleitor no *i-button* (número da opção de voto e código identificativo do boletim de voto [4]), imprime um talão de voto ou *paper trail* com o número da autorização e a escolha do eleitor (Figura 6), o qual fica por breves momentos visível para o eleitor (sem que este o possa manipular) sendo de seguido cortado, e apresenta indicação ao eleitor para retirar o *i-button* (Figura 5e, Figura 5f).
7. O eleitor retira o *i-button* do leitor respectivo, devendo seguidamente dirigir-se à mesa para "depositar" o seu voto na urna electrónica.

[4] O código do boletim de voto é gravado para suportar um cenário em que existam diferentes boletins de voto, como aconteceria num cenário de mobilidade entre círculos eleitorais.

(a)

(b)

(c)

(d)

Imagens em falta, em que apareceriam mensagens de progresso, primeiro (extremamente rápido, enquanto grava)

BOTÃO EM ACTUALIZAÇÂO ...

AGUARDE UM MOMENTO POR FAVOR

e depois (mais demorado)

IMPRIMINDO O SEU VOTO ...

AGUARDE UM MOMENTO POR FAVOR

(e)

(f)

Figura 5 Sequência de imagens da aplicação que executa nas cabines de votação electrónica (em modo de demonstração, mas que é em tudo semelhante ao modo de funcionamento normal).

Figura 6 Exemplos de talões de voto (o do lado direito foi emitido em modo de demonstração).

Mecanismos de segurança

Quando o eleitor insere o *i-button* no leitor respectivo da cabine de voto, esta apenas verifica se o *i-button* tem uma autorização com formato válido (não verifica o conteúdo), e se não tem um voto (por depositar na urna electrónica).

Na implementação actual, a autorização de voto que é transportada no *i-button* (gerada pela urna electrónica) não é cifrada nem assinada com o certificado da urna electrónica. O mesmo acontece com a opção de voto do eleitor (gerada pela cabine de voto), que não é cifrada nem assinada com o certificado da cabine de voto.

Foram duas as razões apontadas pela Multicert para esta situação: por um lado, da solução anterior para a nova solução, mudaram de tecnologia Java (em que tinham grande controlo sobre as bibliotecas relacionadas com as questões de segurança) para tecnologia Microsoft .NET (em que ainda não amadureceram o controlo das bibliotecas relacionadas com as questões de segurança); por outro lado, quiseram minimizar a quantidade de informação transferida e consequentemente os tempos de transferência (na experiência de votação anterior, os tempos de transferência aproximavam-se dos 20 segundos com cartões, no entanto os *i-buttons* serão muito mais rápidos e essa é uma das razões por que foram escolhidos).

Abertura das cabines de voto electrónico

Inicialmente (antes da abertura) as cabines de voto estão em modo de demonstração. No modo de demonstração, consegue-se usar a aplicação sem inserir um *i-button* (mas obviamente, também não se consegue gerar um voto que possa ser transportado para a urna), aparecendo uma menção "DEMONSTRAÇÃO" no fundo do ecrã (ver Figura 5). A impressora funciona, mas os talões de voto têm a menção "DEMO" em vez de um número de autorização (Figura 6 à direita).

Para que os eleitores possam efectuar as suas opções de voto conforme descrito anteriormente, é necessário proceder à abertura de cada cabine, através da inserção do *i-button* de inicialização (contendo o certificado da urna electrónica) que é gerado durante a cerimónica de inicialização da mesma. Quando se insere este *i-button*, aparece um menu com uma opção para abrir o posto de votação. Executando essa opção, passa-se do modo de demonstração para o modo de votação. O certificado da urna electrónica é nesse momento lido pelo posto de votação.

Fecho das cabines de voto electrónico

Inserindo o *i-button* do presidente da mesa com a cabine em modo de funcionamento normal, aparece um menu com duas opções de administração, que devem ser executadas em sequência para "fechar" a cabine:

- Reinicializar - passa ao modo de demonstração já descrito;
- Terminar - desliga o sistema (*shutdown*) de forma controlada.

Note-se no entanto que o fecho das cabines de voto não é crítico, o que é crítico é o fecho das urnas electrónicas e do caderno eleitoral electrónico.

Recuperação de falhas e resolução de problemas

Não foram descritos aos auditores nem analisados mecanismos ou procedimentos de recuperação de falhas e resolução de problemas, nomeadamente em caso de falha da impressão (encravamento, fim da fita) e corte de energia (por desligamento acidental de cabos de alimentação, etc.).

2.1.3 Urnas electrónicas

Em cada mesa de voto existe uma "urna electrónica", destinada a armazenar os votos.

Uma urna electrónica não é mais do que um sistema baseado num normal computador (parcialmente visível no lado esquerdo da Figura 1) equipado com um monitor e um leitor de *i-buttons*, sendo este colocado junto à ranhura de uma urna tradicional, para tornar mais evidente a sua função (Figura 7). Este sistema executa uma aplicação desenvolvida pela Multicert em tecnologia Microsoft .NET, sobre sistema operativo Windows, sendo os dados guardados de forma persistente numa base de dados MSDE. O monitor da urna electrónica está normalmente posicionado de forma a ser visível tanto pelo eleitor como pelos elementos da mesa.

Figura 7 - Pormenor de urna electrónica usada em Santa Iria de Azóia (apenas é visível o leitor de *i-buttons* colocado sobre uma urna tradicional, e não o computador a que o leitor está ligado).

Utilização da urna electrónica

Depois de "preencher" o seu voto electrónico numa cabine de voto electrónico, o eleitor deve dirigir-se para a urna electrónica, para aí "depositar" (ou descarregar) o seu voto electrónico, de acordo com o Procedimento 3 a seguir descrito.

Procedimento 3 - Depositar o voto na urna electrónica

1. Depois de preencher o seu voto numa cabine de voto electrónico, o eleitor dirige-se à urna electrónica, em cujo monitor deve encontrar a mensagem "Introduza um Token de votação!". [5]
2. O eleitor insere o *i-button* (contendo o seu voto) no leitor respectivo da urna electrónica (o leitor está posicionado por cima de uma urna física, que tem uma função meramente decorativa).
3. A urna electrónica verifica se o *i-button* tem uma autorização de voto e um voto válidos. Mais precisamente, verifica se o número de autorização está na lista de números de autorização pendentes, isto é, que foram emitidos pela urna e ainda não foram depositados na urna, e verifica se o *i-button* tem também registado um voto. No futuro, pretende-se que o voto venha cifrado e assinado pela cabine de voto.
    a. Se o *i-button* tiver uma autorização válida, mas não contiver um voto (o que pode acontecer se o eleitor não tiver chegado a concluir a sua

[5] O *i-button* é designado "token" na aplicação da urna electrónica, enquanto que nas cabines de voto electrónico é designado "botão".

votação numa cabine de voto), é apresentada uma mensagem de erro (a autorização anterior contida no *i-button* continua válida).

b. Se o *i-button* tiver um voto válido, mas a autorização não for válida (o que pode acontecer se o voto tiver sido lido pela urna numa tentativa anterior, tendo o eleitor retirado o *i-button* antes de a urna reinicializar o *i-button*), é apresentada uma mensagem de erro. Na realidade, o sistema está preparado para que cada número de autorização só possa ser usado uma vez.

4. A urna electrónica armazena o voto (em conjunto com o número de autorização).
5. A urna electrónica reinicializa o *i-button* (apaga o voto e grava um novo número de autorização).
6. A mensagem "Voto aceite" fica visível por alguns instantes no monitor (Figura 8), após o que aparece uma mensagem para o utilizador retirar o *i-button*. No entanto, o eleitor pode retirar o *i-button* assim que aparece a primeira mensagem. [6]
7. O eleitor retira o *i-button* do leitor respectivo e entrega-o a um elemento da mesa, que o deve juntar ao conjunto de *i-buttons* disponíveis para votar, e deve devolver ao eleitor os documentos de identificação.

[6] Não vê sê nenhuma razão para surgirem estas duas mensagens em sequência, poderiam com vantagem ser reunidas numa única mensagem.

Figura 8 Imagem que aparece no monitor do sistema da urna electrónica.

Cancelamento de autorizações

No caso de se pretender cancelar um voto antes de o depositar na urna, a urna tem uma opção especial de "Reiniciar Token" (ver Figura 8), que deve ser seleccionada antes de inserir o *i-button* que se pretende reinicializar. Esta operação cancela a número de autorização na base de dados interna da urna electrónica, ignora e limpa o voto eventualmente contido no *i-button*, e emite nova autorização. Esta operação também serve para formatar um *i-button* por utilizar (carregando-o com uma autorização de votação). Se o *i-button* inserido for de um elemento da mesa, a operação não é realizada.

Se um *i-button* se avariar, no caso de ainda ser possível efectuar a leitura do *i-button*, a autorização poderá ser cancelada usando a operação anterior; caso contrário, actualmente não é possível anular tal autorização. Contudo, a única consequência é que, no final, existirá na base de dados uma autorização não consumada. No futuro, a Multicert poderá vir a diponibilizar uma operação que permita invalidar uma autorização através de uma associação entre o nº de série do *i-button* e a autorização.

Opções para abertura e fecho da urna e apuramento de resultados

A urna tem ainda as seguintes opções (Figura 8 - lado superior):

- Abrir - Primeira operação a realizar no dia das eleições, exige a inserção sucessiva dos 3 *i-buttons* do presidente e dos dois escrutinadores (previamente inicializados no sistema do caderno eleitoral electrónico), e torna disponíveis as restantes opções. Inicializa também um *i-button* de inicialização das cabines de voto electrónico, o qual é carregado com o certificado da urna electrónica. Inicializa também um conjunto de *i-buttons* de votação (neste caso, foram inicializados cerca de 6 a 10 *i-buttons* em cada secção de voto), carregando cada um deles com uma autorização de voto (número de autorização único).
- Adicionar Cabine - Esta operação ainda não estava disponível. No futuro, deveria ser utilizada para proceder à inicialização de uma cabine a qualquer momento durante o acto eleitoral (por exemplo, no caso de haver a necessidade de substituir uma cabine avariada). Para poder ser executada irá exigir a inserção do *i-button* do presidente.
- Adicionar Token - Esta operação ainda não estava disponível. É semelhante à operação "Reiniciar Token", diferindo apenas no caso de se estarem a utilizar (registar / validar) os números de série dos i-button's.
- Fechar - exige a inserção dos *i-buttons* do presidente e dos dois escrutinadores, imprime documento de fecho de mesa, não permite depositar mais votos, e activa as opções de "Apurar" e "Exportar";
- Apurar - mostra gráfico com os resultados (número total de votos obtidos por cada candidato e número de votos em branco);
- Exportar - Exporta para CD ficheiros com os votos (cifrados e em claro), as autorizações emitidas, a lista de eventos registada na urna (assinada digitalmente), o certificado da urna e um ficheiro XML com os resultados apurados assinado digitalmente em XMLDSIG.

<u>Conteúdo da base de dados da urna electrónica</u>

Cada sistema de urna electrónica tem uma base de dados MSDE.

As tabelas e colunas mais relevantes são:

- Tabela "Votes" - guarda os votos depositados
    - coluna "Vote" - codificação em base 64 de texto XML com a opção escolhida, isto é, com a identificação do boletim de voto (neste caso é sempre igual) e o nº da opção escolhida, devendo no futuro ser cifrado;

- coluna "VoteID" - nº sequencial, actualmente gerado por ordem cronológica pela aplicação, mas que no futuro deve ser gerado por ordem não cronológica para evitar a associação entre votos e votantes;
- coluna "ElectionID" - identificador da eleição (neste caso é sempre igual).

- Tabela "Authorizations" - guarda as autorizações emitidas
  - coluna "Serial"
  - coluna "ElectionID" - identificador da eleição (neste caso é sempre igual);
  - coluna "VoteAuthorization" - codificação em base 64 de texto XML com a autorização de voto, isto é, com a identificação do boletim de voto (neste caso é sempre igual) e o nº de autorização;
  - coluna "AuthorizationState" - estado da autorização, que pode ser "Idle" (autorização emitida mas ainda não votou), "Used" (já votou), "Cancelled" (autorização foi cancelada).
- Tabela "OperationLogs" - seria destinada a gravar "log" das operações críticas, mas neste caso não chegou a ser usada.

Mecanismos de armazenamento redundante

Não foram descritos mecanismos de armazenamento redundante. Em caso de falha do disco, ou se repetem as eleições, ou se consideram os talões de voto impressos nas cabines de voto.

A intenção é que o sistema da urna electrónica (assim como os sistemas do caderno eleitoral electrónico) esteja equipado com UPS, para proporcionar estabilidade de corrente em caso de falha de energia e impedir a corrupção da base de dados. No entanto, isso não protege contra falhas do disco.

2.1.4 i-buttons

Em cada secção de voto, são utilizados dois conjuntos de *i-buttons* (Figura 9):

- um conjunto de 3 *i-buttons* para os 3 membros da mesa (presidente e 2 escrutinadores), os quais são inicializados aquando da abertura do caderno eleitoral electrónico e são depois usados para efeito de autenticação em diversas operações críticas (encerramento do caderno eleitoral electrónico, abertura e encerramento da urna electrónica, abertura das cabines de voto electrónico e cancelamento de voto, pelo menos);

- um conjunto de cerca de 6 a 8 *i-buttons*, reutilizáveis, destinados aos eleitores, para transportar a autorização de voto (da urna electrónica até à cabine de voto electrónico) e o voto electrónico (da cabine de voto electrónico até à urna electrónica).

Figura 9 - Pormenor de um "i-button" (esquerda) e de um leitor/gravador de *i-buttons* (direita).

Todos os *i-buttons* são inicializados no início do período eleitoral, conforme já descrito.

Estes dispositivos foram escolhidos pela Multicert, em vez dos cartões utilizados na experiência de votação anterior, pela sua fiabilidade e robustez (capazes de suportar ciclos de leitura/gravação frequentes e manipulações menos cuidadosas), e velocidade de transferência de dados.

Os i-buttons são lidos e gravados por dispositivos de leitura e gravação, funcionando quer por contacto quer por encaixe, sendo o segundo modo o mais apropriado para evitar erros de leitura ou gravação.

Na implementação actual, as autorizações de voto e os votos são transportados de forma não cifrada nem assinada. Numa implementação futura, seguir-se-ia um circuito em tudo semelhante ao já experimentado na experiência de votação anterior:

- Na inicialização da urna electrónica, seriam gerados 2 certificados: um para cifra (exportável para a cabine, que na volta devolve o seu certificado para a urna), e outro para assinatura (não exportável).
- O *i-button* levaria a autorização de voto assinada pela urna com o seu certificado.
- De volta, ao *i-button* é acrescentado o voto (identificador do boletim mais nº da opção escolhida) cifrado duplamente (primeiro cifrado com chave assimétrica, e depois com chave simétrica aplicacional) e por fora assinado pela cabine.

Para segurança acrescida, existem modelos de *i-buttons* criptográficos disponíveis no mercado, contudo não foram usados nesta eleição. Os modelos criptográficos suportam a criação de assinaturas digitais (há um modelo em que os pares de chaves são gerados no próprio *i-button* e outro em que os pares de chaves têm que ser importados via software) e permitem guardar certificados digitais. Estes modelos poderiam ser

utilizados para o presidente e escrutinadores assinarem digitalmente algumas operações. No entanto, ainda não estão suficientemente estáveis.

2.1.5 Sistema de votação por telemóvel

A Multicert, em parceria com a PT Inovação, desenvolveu também um protótipo de um sistema de votação por telemóvel, destinado a eleitores com necessidades especiais. Este sistema começou por ser desenvolvido para suportar a votação dos invisuais, seguindo exigências da UMIC, sendo aliás a única possibilidade que um invisual tinha de experimentar o voto electrónico em Santa Iria de Azóia. Ainda que tal não tenha sido explorado nesta experiência, o sistema também poderia ser usado para suportar a votação de acamados e outros eleitores "em ambulatório" (em que a mesa eleitoral se deslocaria junto do eleitor, em vez do inverso).

A identificação do eleitor no caderno eleitoral electrónico processa-se como no sistema normal. O eleitor dirige-se a uma secção de voto (a votação "em ambulatório" não foi explorada), onde é identificado no caderno eleitoral electrónico e assinalado como tendo votado. Na implementação actual, não fica nenhuma indicação no caderno eleitoral a indicar que o voto se processou por telemóvel.

A primeira diferença em relação ao sistema normal é que, em vez de um *i-button* com a autorização de voto, é entregue ao eleitor um envelope fechado contendo um código de votação ou PIN único de 5 dígitos, a usar na votação por telemóvel (Figura 10). O código de votação não está relacionado com a identificação do eleitor, pois o envelope é retirado de um monte de envelopes previamente preparados. Cada código de votação só pode ser usado uma vez.

A segunda diferença em relação ao sistema normal é que, em vez de efectuar o seu voto através de uma cabine de voto electrónica e da urna electrónica, o eleitor efectua o seu voto por intermédio de uma chamada de voz para o número do "serviço de voto electrónico" a partir de um telemóvel que lhe é facultado pela mesa, e cujo número foi previamente registado junto do serviço de voto electrónico (por razões de segurança, o serviço de voto electrónico só aceita chamadas de números previamente registados).

Uma vez estabelecida a comunicação, o eleitor (ou alguém por ele, se for invisual [7]) deve digitar o código de votação. O sistema começa por pronunciar todas as opções de

[7] Dado que o sistema foi inicialmente concebido para suportar a votação de invisuais, por exigência da UMIC, era suposto que todo o procedimento, inclusive a digitação do código secreto, pudesse ser feita

voto (nomes de partidos/coligações) sem qualquer pausa. De seguida, volta a pronunciar as opções de voto, com uma pausa a seguir a cada opção, permitindo ao utilizador seleccionar a última opção ditada carregando numa tecla qualquer. No final há um diálogo de confirmação da opção escolhida.

A terceira diferença em relação ao sistema normal é que, em vez dos votos serem depositados e contabilizados na urna electrónica da secção de voto a que o eleitor se dirigiu, os votos são contabilizados no servidor do serviço de voto electrónico, que funciona como se fosse mais uma urna.

---

por cidadãos invisuais. No entanto, tal acabou por não ser possível uma vez que o referido código de votação não estava disponível em Braille, exigindo deste modo a intervenção de uma segunda pessoa, nomeadamente o presidente da mesa.

Figura 10 - Pormenor de um envelope com um código de votação.

2.1.6 Configuração dos locais de voto electrónico

Local de Voto	**Nº de secções de voto normal**	**Nº de postos de votação**	**Ligação a servidor**
Grupo Desportivo de Pirescoxe	2	3	ADSL
Casa da Cultura de Santa Iria de Azóia	2	3	ADSL
Atlético de Via Rara AVR	2	3	UMTS
Sociedade Recreativa 1º de Agosto Santairiense	2	3	ADSL

AMUPA	3	3	UMTS
Escola Básica nº 2	2	3	UMTS
Escola Básica nº 1	3	3 (*)	UMTS

(*) Na Escola Básica nº 1 estavam previstas três cabines de voto. No entanto, por dificuldades técnicas, apenas duas acabaram por estar disponíveis aos eleitores.

2.2 Procedimentos do SVE

2.1.7 Abertura da mesa e dos postos de votação

Abertura da mesa central (servidor do caderno eleitoral electrónico)

Foi acompanhada a abertura da mesa central na Casa da Cultura, tendo-se observado o procedimento já descrito na secção 2.1.1.

Abertura de cada mesa local e dos postos de votação

Foi acompanhada a abertura na Casa da Cultura e em Pirescoxe.

A abertura compreendeu, por ordem:

- abertura do caderno eleitoral electrónico, conforme procedimento já descrito na secção 2.1.1;
- abertura da urna electrónica, conforme procedimento já descrito na secção 2.1.3, e que incluiu a inicialização de diversos *i-buttons* para serem usados pelos eleitores no processo de votação;
- abertura dos postos de votação - depois de indicar na aplicação da urna o número de postos de votação que iam ser usados, o presidente da mesa dirigiu-se a cada um dos postos procedendo à sua abertura.

Conforme já foi referido, tanto a abertura do caderno eleitoral como a abertura da urna electrónica exigem a apresentação dos *i-buttons* dos três elementos da mesa, enquanto que a abertura dos postos de votação exige a apresentação do *i-button* do presidente da mesa.

2.1.8 Votação

Foi acompanhado o desenrolar da votação em todos os 7 locais, mas apenas uma parte do tempo em cada um. Segue-se uma descrição dos procedimentos observados.

a. operador do caderno eleitoral electrónico

O operador do caderno eleitoral executou durante a visita os seguintes passos, na sua interacção com os eleitores:

1. Recebimento dos documentos de identificação dos eleitores e pesquisa, através do número de eleitor (também poderia ser o nome) (o número de eleitor inclui uma letra designativa do seu local de votação), da sua existência no caderno eleitoral (aqui de toda a freguesia) e indicação de que ainda não tinha votado.
2. Feita esta verificação era feita a entrega dos documentos a um escrutinador, que por sua vez entregava o dispositivo de armazenamento (*i-button*) ao eleitor.
3. Validação de imediato da votação deste eleitor, sem esperar pelo seu voto, antes de atender o eleitor seguinte.

Em muitos dos locais de votação electrónica de Sta. Iria, e em períodos de maior afluência, a entrega do *i-button* e validação do eleitor só era feita quando houvesse pelo menos uma cabine de voto disponível.

Para mais detalhes ver o Procedimento 1 já descrito.

b. votantes

Os eleitores, para efectuar o seu voto, tiveram de efectuar os seguintes passos:

1. O eleitor dirige-se à mesa com a sua identificação, tendo ocasionalmente de esperar numa pequena fila.
2. Após a validação no caderno eleitoral, o eleitor recebe um pequeno dispositivo de armazenamento (*i-button*) pré-preparado, e é convidado a dirigir-se a uma das cabines de votação (mais uma vez, poderia ocasionalmente ser necessário esperar numa pequena fila).
3. Na cabine de votação, o dispositivo de armazenamento tinha de ser inserido no leitor/gravador correspondente (ranhura circular com cerca de 1 cm de diâmetro), o que por vezes apresentou algumas dificuldades, necessitando o eleitor de auxílio.
4. Após a inserção correcta do dispositivo aparecia ao eleitor o écran com a lista de partidos/coligações concorrentes. Feita a escolha da sua preferência (tocando o nome, símbolo, ou quadrado) o eleitor teria de confirmar a sua escolha no mesmo écran. Num segundo écran, apenas o partido/coligação escolhido era apresentado,

possibilitando-se a confirmação final ou voltar atrás para uma nova escolha. Após a confirmação final faz-se a impressão de um pequeno talão que o eleitor pode ver cair para um depósito inferior. No entanto esta impressão é feita com bastante rapidez, seguindo-se imediatamente o corte e queda, não sendo muito fácil o eleitor ler o partido/coligação votado no talão. Embora, segundo nos foi reportado, estivesse previsto que entre a finalização da impressão do registo do voto e o corte do papel houvesse um espaço de tempo de 5/6 segundos, tal nem sempre sucedeu (nomeadamente em Pirescoxe).

5. O eleitor retira o dispositivo de armazenamento do seu leitor/gravador e regressa à mesa onde o insere no sistema de leitura de votos com um leitor/gravador idêntico ao do posto de votação. Um écran permitia ver a confirmação da leitura do seu voto (indicação "voto aceite"). O dispositivo é então recolhido por um membro da mesa (tendo sido novamente preparado para reutilização numa nova votação) e os documentos do eleitor são devolvidos.

Para mais detalhes, ver também o Procedimento 2 já descrito.

c. operador da urna electrónica

Um segundo elemento da mesa assistia os eleitores na leitura dos seus votos, após o retorno dos postos de votação.

A rotina de operação deste 2º elemento da mesa foi então a seguinte:

1. Recebimento dos documentos dos eleitores do colega que fez a verificação no caderno, e entrega do dispositivo de armazenamento ao eleitor. Estes dispositivos eram guardados num recipiente e retirados daí aleatoriamente.

2. Auxiliar o eleitor a inserir o dispositivo no leitor/gravador e devolver os respectivos documentos. O dispositivo era então retirado e guardado no recipiente onde já se encontravam outros pré-preparados para a próxima votação. No total o recipiente deveria conter 6 a 8 dispositivos.

Para mais detalhes, ver também o Procedimento 3 já descrito.

2.1.9 Fecho da mesa e dos postos de votação

Foi acompanhado o encerramento da secção de voto localizada no Grupo Desportivo de Pirescoxe.

Foi inicialmente encerrado o caderno eleitoral electrónico, através da opção existente para o efeito na aplicação cliente, que requereu a inserção dos *i-buttons* dos 3 membros da mesa (presidente, 1º escrutinador e 2º escrutinador).

De seguida, foi encerrada a urna electrónica, através da opção existente para o efeito na respectiva aplicação, que requereu igualmente a inserção dos *i-buttons* dos 3 membros da mesa (presidente, 1º escrutinador e 2º escrutinador). A partir desse momento, ficaram disponíveis opções de imprimir os resultados e visualizar no ecrã um gráfico com os resultados (número de votos obtidos por cada partido/coligação).

Nas cabines de voto, não foi efectuada qualquer operação específica de encerramento, tendo-se apenas reunido os talões de voto das várias cabines, que foram depois depositados na urna física associada ao sistema da urna electrónica.

2.1.10 Apuramento de resultados

Foi acompanhado o apuramento de resultados no Grupo Desportivo de Pirescoxe.

O apuramento de resultados (número total de votos obtidos por cada partido/coligação, e número total de votos brancos) foi apenas efectuado localmente, em cada secção de voto electrónico, não se tendo procedido à comunicação dos resultados para um servidor central, para efeito de acumulação dos resultados das várias secções de voto electrónico. A UMIC não queria, por uma questão de confidencialidade, que os resultados finais fossem transmitidos, e os mecanismos de transmissão não estavam implementados pela Multicert. [8]

Numa implementação futura, os resultados seriam assinados com o certificado da urna e transmitidos sobre uma ligação HTTPS segura para um servidor. Segundo a Multicert, isso obrigaria a dotar os sistemas das urnas electrónicas de conectividade, o que não aconteceu nesta experiência (apenas o sistema do caderno eleitoral electrónico tinha conectividade).

No Grupo Desportivo de Pirescoxe, a pedido do auditor presente, foram contados manualmente os talões de voto (não se efectuou a contagem por cada partido/coligação, mas apenas o número total de votos). Uma vez que a primeira contagem deu um valor diferente do número total de votos indicado pela urna electrónica (643 talões contra 639 votos na urna electrónica), a contagem foi repetida duas vezes, tendo em ambas as vezes sido contados 647 talões (mais 4 do que na primeira contagem, possivelmente porque os talões estavam "colados"), pelo que se considerou este valor fiável. Durante a contagem manual não se detectaram talões em branco.

[8] Mesmo que não se pretendesse efectuar a transmissão de resultados nesta experiência concreta, a auditoria seria beneficiada se já estivesse implementado um mecanismo de transmissão dos resultados.

Não se apresentam aqui os votos obtidos por cada partido/coligação, por razões de confidencialidade, mas apenas os totais de votos e votantes por secção de voto (Tabela 1).

Tabela 1 Resumo dos contagens de votos e votantes (dados gentilmente cedidos pela Multicert, à excepção da contagem de talões de voto em Pirescoxe, que foi dirigida pelo auditor da Feup aí presente, que também verificou os restantes dados de Pirescoxe).

	1º de Agosto	Casa da Cultura	Escola Básica nº 1	Pirescoxe	Escola Básica nº 2	Via Rara	AMUPA	**Total**
a) Nº de votos na urna electrónica	438	572	579	639	537	691	487	3943
b) Nº de votos por telemóvel	0	7	3	1	0	0	4	15
c) Nº total de votos (a+b)	438	579	582	640	537	691	491	**3958**
d) Nº de votantes segundo caderno eleitoral electrónico	416	577	556	632	511	689	489	**3870**
e) Diferença (c-d)	22	2	26	8	26	2	2	**88 (2,3%)**
f) Nº de talões de voto	(por contar)	(por contar)	(por contar)	**647**	(por contar)	(por contar)	(por contar)	-
g) Diferença (f-a)	-	-	-	**8**	-	-	-	-

Conforme se pode constatar na Tabela 1, em todas as secções a urna electrónica tinha mais votos do que o número de votantes registados no caderno eleitoral electrónico (em média, mais 2,3%), o que, dependendo da causa, pode significar que diversos votantes votaram mais do que uma vez, pondo em causa o princípio da unicidade do voto.

Esta discrepância poderá dever-se a alguns eleitores terem, inadvertidamente, votado mais do que uma vez. Passando a explicar: A mesa e os técnicos presentes sabiam que, se um eleitor não completasse devidamente o sua voto na cabine de voto electrónico (por exemplo, por retirar o *i-button* antes do tempo), a urna electrónica daria uma mensagem de erro quando o eleitor tentasse aí depositar o voto (inserindo o *i-button*). Nesse caso, a mesa instruía o eleitor para se dirigir de novo a uma mesa de voto. Segundo foi admitido pelos elementos da mesa e técnicos presentes (e de acordo com o que foi percebido pelo auditor da Feup presente no fecho), tal terá ocorrido diversas vezes ao longo do dia. Isto só por si não seria motivo de erro. Mas acontece que, se um

eleitor com um *i-button* transportando um voto válido, inserir duas vezes seguidas de forma rápida o seu *i-button* no leitor da urna electrónica (o que é plausível dada a dificuldade demonstrada por muitos eleitores no manuseio dos *i-buttons*), o voto pode ser transferido e o *i-button* reinicializado na 1ª vez (o que é plausível dada a elevada velocidade de transferência de dados), dando um erro da 2ª vez que o mesmo é inserido, sem que ninguém (o eleitor ou a mesa) se chegue a aperceber da mensagem de voto aceite apresentada aquando da 1ª inserção. Nesse caso, o eleitor é instruído erradamente para se dirigir de novo a uma mesa de voto (o segundo voto é possível porque o *i-button* foi reinicializado). Em favor desta explicação, está também o que foi observado pelo auditor da mesa presente na abertura em Pirescoxe, e que está relatado mais à frente neste relatório (secção 3.2, ponto O9 - Erros a descarregar o voto para a urna electrónica).

Outra explicação teoricamente possível para a discrepância observada, resultante unicamente de erro humano, é a mesa ter permitido a votação de eleitores, sem chegar a proceder a essa autorização na aplicação do caderno eleitoral electrónico. Segundo informação da Multicert e UMIC, pelo menos em Pirescoxe membros da Mesa terão admitido que, por esquecimento, algumas vezes apenas seleccionaram o votante no caderno mas não carregaram no botão de autorização de votação. No entanto, não foi isso que percebeu o auditor da FEUP presente, pelo que conviria indagar de novo a presidente da Mesa. Mesmo que algum caso de excesso de votos em relação a votantes possa ter esta causa, não parece plausível que explique a maioria dos casos, pois devia originar discrepâncias semelhantes em locais de voto em que foram usados sistemas de voto electrónico doutras empresas, o que não aconteceu.

A Tabela 1 mostra que a discrepância entre votos e votantes teve grande variação entre diferentes locais de voto. Essa variação pode estar relacionada com diferenças nos procedimentos seguidos e cuidados tomados pela Mesa nos vários locais de voto.

Verificou-se também uma discrepância entre o número de talões de voto em papel e o número de votos na urna electrónica. Na altura, aventou-se a hipótese de esta discrepância corresponder a casos em que o eleitor terá retirado o *i-button* depois de a cabine de voto electrónico começar a impressão do talão em papel, mas antes de gravar a opção de voto no *i-button*. Mais tarde, na reunião com os técnicos da Multicert, essa hipótese foi posta de lado, pois o sistema grava primeiro o voto no *i-button* e só depois imprime o voto. Duas hipóteses de justificação aceitáveis foram adiantadas pela Multicert: podem ter sido impressos votos em modo demonstração (o que seria fácil averiguar, pois os talões têm a menção "DEMO" em vez de um nº de autorização), ou pode tratar-se de votos que foram cancelados (pode-se averiguar analisando os números de autorização em estado cancelado na base da dados da urna electrónica).

Observando os talões de voto em papel, verificou-se também que os mesmos não se encontravam impressos de forma uniforme. Normalmente, cada talão devia ter três linhas espaçadas entre si (Figura 6): (a) uma primeira linha com a designação do partido/coligação escolhido, (b) uma segunda linha com uma sequência de "#" e (c) uma terceira linha com o número de autorização. Ora acontece que diversos talões tinham a sequência b-c-a, em vez da sequência a-b-c. A dimensão dos talões também era variável. Segundo nos foi indicado por responsáveis da Multicert, tal terá sido devido a uma má configuração do tamanho de página de impressão.

A tabela seguinte (Tabela 2) fornece alguns indicadores indirectos de mobilidade. Os poucos casos de mobilidade que terão ocorrido correspondem a pessoas (nomeadamente membros das mesas de voto) que propositadamente experimentaram o voto electrónico numa secção diferente daquela em que tinham de efectuar o voto tradicional. Dadas as condições específicas em que ocorreu (dentro da mesma freguesia, e os eleitores tinham também de votar de forma tradicional sem mobilidade), o cenário de mobilidade montado serviu para um primeiro ensaio, mas não para medir a adesão real que poderá ter da parte dos eleitores.

Tabela 2 Indicadores de mobilidade, conforme dados do caderno eleitoral electrónico (dados gentilmente cedidos pela Multicert).

	1º de Agosto	Casa da Cultura	Escola Básica nº 1	Pirescoxe	Escola Básica nº 2	Via Rara	AMUPA	**Total**
a) Nº de eleitores que votaram nessa secção, provenientes de qualquer das 7 secções (*)	416	577	556	632	511	689	489	**3870**
b) Nº de votantes provenientes dessa secção que votaram em qualquer das 7 secções (*)	432	574	575	617	506	685	481	**3870**

(*) Seria mais interessante ter, para cada secção, o nº de eleitores que votaram nessa secção provenientes da mesma secção e o nº de eleitores que votaram nessa secção provenientes doutras secções, mas não foi possível obter essa informação.

3 Apreciação do SVE

3.1 Apreciação da arquitectura e desempenho do sistema

3.1.1 Afluência e atitude dos eleitores

Em geral, o processo de votação decorreu de forma organizada, sendo notória a satisfação das pessoas com todo o processo. No entanto, foi constatada alguma relutância e mesmo receio por parte de um número razoável de eleitores, particularmente alguns mais idosos, em efectuarem a experiência da votação electrónica.

Não se observaram filas significativas (com mais de 3/4 pessoas), à excepção dos períodos de falha do sistema.

A maioria da população votante parecia encontrar-se na faixa etária dos 40/60, sendo relativamente escassa a população jovem.

A tabela seguinte (Tabela 3) mostra alguns números recolhidos pelos auditores relativos à afluência de eleitores.

Tabela 3 Alguns dados recolhidos relativos à afluência de eleitores.

	1º de Agosto	Casa da Cultura	Escola Básica nº 1	Piriscoxe	Escola Básica nº 2	Via Rara	AMUPA	**Total**
Nº de votantes por via electrónica / nº de votantes por via tradicional (hora)		190 (11:35)	340 (13:30) 380 (15:30)		127 / 398 (11:30)		190 / 420 (11:30) 221 (13:15)	
Nº de votantes finais por via electrónica (conforme Tabela 1)	416	577	556	632	511	689	489	3870

3.1.2 Indicadores de desempenho

Foi seguido o percurso de alguns eleitores e medido o tempo despendido no acto de votação, nomeadamente:

- tempo de pré-votação: tempo de permanência na fila + identificação e entrega do dispositivo + tempo de espera por um posto livre (que ocorreu muito raramente);
- tempo de votação: tempo de permanência no posto de votação;
- tempo de pós-votação: tempo de descarga do voto + entrega de documentos;
- tempo total: soma dos três tempos anteriores.

Foi também contado o número de pessoas à frente na fila, quando o eleitor chegou.

A tabela seguinte (Tabela 4) mostra os tempos medidos numa amostra de votantes num dos locais de voto electrónico.

Tabela 4 Tempos (em segundos) medidos numa amostra de 13 pessoas a votar na Escola Básica nº 1,.

	Tempo de pré-votação	Tempo de votação	Tempo de pós-votação	Tempo total	Pessoas à frente na fila
Média	48s	52s	13s	114s	0,85
Mínimo	12s	30s	10s	52s	0
Máximo	240s	85s	20s	345s	4

Tempos semelhantes foram observados nos outros locais de voto pelos auditores presentes (em amostras de reduzida dimensão):

- Escola Básica nº 2: tempo total com valores médios entre 60 e 90 segundos.
- Casa da Cultura: tempo de votação médio de 65 segundos, tendo-se registado como valores extremos, 30 segundos e 87 segundos;
- AMUPA: valores semelhantes aos registados na Escola Básica nº 1;
- Pirescoxe: tempo de votação apresenta valores médios entre 6 0 e 90 segundos.

De notar que todas ou quase todas as pessoas foram assistidas na votação, embora nem todas o solicitassem, o que concerteza contribuiu para os tempos de votação relativamente curtos que foram observados.

Relativamente à votação por telemóvel, o processo foi considerado muito lento pelos poucos eleitores que o utilizaram (na presença dos auditores), nomeadamente 3 utilizadores na Casa da Cultura e um invisual em Pirescoxe (este teve dificuldade significativa em concretizar o voto, talvez pela falta de experiência, tendo demorado vários minutos a concluir o processo).

3.1.3 Aspectos positivos a realçar

S1: Fluidez do processo [9]

Em geral, e a menos dos problemas de conectividade, o processo de votação decorreu de forma fluída, particularmente em comparação com a experiência de votação electrónica com sistemas Multicert nas eleições Europeias de 2004.

Para isso terão contribuído os seguintes factores:

- supressão do segundo acesso ao caderno eleitoral electrónico, para registar a conclusão do acto de votação de cada eleitor;
- maior rapidez das operações de leitura/escrita de/para os *i-buttons*, por comparação com o que se passou nas Europeias de 2004 (em que foram usados *smartcards*, muito mais lentos, além de que a quantidade de informação transferida era maior);
- a menos dos problemas de conectividade, o funcionamento em rede da aplicação com o caderno eleitoral parecia ter uma resposta perfeitamente aceitável.

S2: Transparência

S2a: A separação física entre o sistema do caderno eleitoral electrónico e o sistema da urna electrónica (que não se verificava na solução apresentada pela Multicert para as eleições europeias de 2004), contribui para aumentar a transparência do processo, e dar aos eleitores maior confiança de que o seu voto é anónimo. Os próprios *i-buttons* usados pelos eleitores circulam apenas entre o sistema da urna electrónica e os postos de votação electrónica, sem ligação com o sistema do caderno eleitoral electrónico. O facto do *i-button* usado por cada eleitor ser escolhido de forma aleatória de um grupo de cerca de uma dezena, também contribui para aumentar a confiança no anonimato do voto.

S2b: O facto de se ter virado o monitor da urna electrónica de forma a que o eleitor pudesse verificar que o seu voto foi aceite quando encosta o *i-button* ao sistema de leitura, é um facto que aumenta a transparência do sistema para o eleitor.

[9] *S - Strength* (ponto forte).

S2c:A impressão de talões de voto, ao permitir ao eleitor verificar a materialização do seu voto e possibilitar a recontagem dos votos por qualquer pessoa, contribui também para aumentar a transparência do processo.

S2d: No capítulo da transparência, é ainda de realçar a disponibilidade e abertura manifestada pela Multicert para prestar todos os esclarecimentos sobre o sistema e dar acesso aos elementos considerados necessários para efeito da auditoria.

S3: Fiabilidade e robustez dos i-buttons

Os *i-buttons* mostraram suportar com maior fiabilidade ciclos de leitura-gravação intensivos ao longo do dia das eleições, e manuseamento menos cuidadoso (caíram ao chão várias vezes), comparativamente com os *smarcards* usados nas Europeias de 2004.

S4: Suporte de mobilidade

Apesar das limitações já descritas, a solução da Multicert permitiu a realização e análise de uma primeira experiência de mobilidade dentro de um círculo eleitoral.

S5: Dificuldade de forjar votos

Mesmo sem alguns mecanismos de segurança implementados (assinatura e cifragem das autorizações de voto e dos votos), o facto de se usar um número de autorização único gerado pela urna e validado depois pela mesma urna, praticamente impede forjar votos.

3.1.4 Constrangimentos detectados no sistema e na sua configuração nos locais de votação

W1: Solução muito incompleta e inacabada [10]

W1a: Não estavam implementados os mecanismos de transmissão dos resultados finais.

- Mesmo que, para a experiência concreta realizada, não fosse necessária a comunicação dos resultados (pois, como já foi referido, a UMIC não pretendia que se efectuasse a transmissão de resultados por uma questão de confidencialidade), o sistema não se pode considerar completo, nem pode ser avaliado plenamente, sem este mecanismo de grande importância.

W1b: Não estavam implementados diversos mecanismos de segurança (conforme descrito no capítulo 2), que a própria Multicert reconhece ser necessário introduzir no futuro.

[10] W - *Weakness* (ponto fraco).

- A auditoria fica prejudicada, pois a introdução desses mecanismos de segurança pode ter efeitos negativos noutros factores (velocidade, etc.), ficando por avaliar o equilíbrio conseguido entre os vários factores.

W2: Suporte limitado de mobilidade

Na sua versão actual, e por acordo entre a UMIC e a Multicert face ao escasso tempo disponível para o seu desenvolvimento, a solução apresentada pela Multicert suporta a mobilidade apenas na vertente de identificação dos eleitores no caderno eleitoral electrónico, através do funcionamento em rede do caderno eleitoral electrónico.

No caso de eleições em que existem diferentes boletins de voto para diferentes círculos eleitorais (como é o caso das presentes Eleições Legislativas) e/ou é necessário contar separadamente os votos provenientes de diferentes círculos eleitorais, para suportar a mobilidade a nível nacional será também necessário veicular nas autorizações de voto e nos próprios votos a identificação do boletim de voto e/ou círculo eleitoral de origem de cada eleitor (devendo as cabines de voto estar preparadas para apresentar a cada eleitoral o boletim de voto apropriado). Se bem que, no sistema auditado, as autorizações de voto e os votos tenham associado um código de boletim de voto para suportar cenários em que existem diferentes boletins de voto, falta definir e implementar mecanismos para gerar essa informação (identificação do boletim de voto e/ou do círculo eleitoral) em função do eleitor, bem como para agrupar e contar os votos de forma apropriada, salvaguardando o anonimato do voto e a transparência do processo.

W3: Montagem artesanal

Do ponto de vista físico, o sistema ainda apresentava um ar muito experimental, com muitos cabos e componentes à vista, dando um aspecto de "montagem artesanal". Por exemplo a ligação ao telemóvel UMTS, exibia em alguns casos enorme fragilidade.

W4: Dificuldade de manipulação dos *i-buttons* pelos eleitores

O sistema de *i-buttons* (devido aos *i-buttons* em si, aos seus suportes ou aos leitores/gravadores) revelou-se um fracasso em termos de usabilidade, pela dificuldade de inserção sem apoio dos assistentes, e pela facilidade com que são retirados antes do tempo.

De facto, a principal dificuldade manifestada pelos eleitores no processo de votação electrónica pareceu ser a colocação correcta do dispositivo de armazenamento no respectivo leitor/gravador. Caíram várias vezes, ficaram mal colocados e presume-se que tenham sido a fonte de várias situações de erro registadas.

A pequena dimensão dos *i-buttons* e o facto de não se assemelharem a nada familiar para a maioria dos eleitores, pode ter contribuído para a sua dificuldade de manuseamento.

O facto de o *i-button* ter que ser encaixado no posto de votação e de bastar um toque na mesa de voto para que o voto fosse aceite, cria confusão (encaixar ou tocar).

W5: Controlo deficiente da conclusão do voto, com possibilidade de duplicação ou perda de votos

A dificuldade de manipulação dos *i-buttons* pelos eleitores, combinada com o insuficiente controlo aplicacional e a falta de procedimentos de actuação da mesa bem definidos, levaram a uma deficiente percepção do conclusão efectiva do voto pelo eleitor e pela mesa, podendo ter originado a repetição indevida de votos em número significativo de casos e a consequente quebra do princípio da unicidade do voto (ver análise mais detalhada na secção 2.1.10).

Como já foi referido, ao contrário da aplicação de votação anterior, a nova aplicação de acesso ao caderno eleitoral não incluía o estado de "em votação" (isto é, o eleitor estava validado, mas não tinha concluído a votação). Nesta nova solução, o eleitor é imediatamente dado como tendo votado à entrada, o que evita alguma confusão no posto de verificação do caderno (aliás o sistema até é mais próximo do tradicional).

No entanto, para que este sistema funcione, é necessário que a mesa se aperceba claramente se o eleitor conclui efectivamente o seu voto. No sistema da Multicert, existe essa possibilidade, mas deveria ser mais explícita e robusta, não apenas um ecrã que ou está virado para o eleitor ou para a mesa.

É de salientar que, no próprio dia das eleições, o responsável da Multicert identificou uma alteração do sistema, fácil de implementar, que poderia tornar o sistema mais robusto: quando se tenta depositar um voto na urna electrónica (encostando o *i-button* ao leitor respectivo), sem que o *i-button* tenha um voto pronto a ser depositado, a urna electrónica deve apresentar mensagens diferenciadas, de acordo com o tempo decorrido desde a última vez que se depositou um voto com esse *i-button* (e o mesmo recebeu uma nova autorização de voto). Se o tempo decorrido for muito curto (inferior ao tempo necessário para votar numa cabine de voto), isso significa que o voto do eleitor já foi depositado na urna electrónica com sucesso.

W6: Anonimato do voto comprometido

Ainda que não seja essa a intenção futura, os votos são identificados por ordem cronológica na urna electrónica (ver a descrição do conteúdo da base de dados da urna electrónica na secção 2.1.3), e o sistema do caderno eleitoral electrónico mantém a

ordem dos votantes (pois apresenta aos membros da mesa a lista de votantes ordenada com o mais antigo à cabeça), o que pode permitir a associação entre votos e votantes, comprometendo o anonimato.

Este problema é de fácil resolução, bastando para tal numerar os votos por ordem aleatória. Se forem implementados *logs*, não devem ser sequenciais, pelo menos num dos lados (votos ou votantes).

W7: Falta de autonomia dos eleitores

Foi óbvia a necessidade de apoio em todos os passos no processo de votação electrónica. Os eleitores eram assistidos na votação quer pelos representantes da UMIC quer pelos técnicos da Multicert presentes em cada local.

Apesar de ter sido efectuada a recomendação na auditoria anterior, a não disponibilização de um posto de teste teve consequências negativas na votação, e dificulta a avaliação. Por exemplo, teria sido interessante averiguar até que ponto um eleitor que tivesse experimentado previamente o sistema de teste com ajuda, seria depois capaz de votar sozinho.

W8: Insuficiente autonomia da Mesa

As pessoas que constituíram as mesas eleitorais electrónicas não tiveram uma formação adequada, mas apenas uma formação muito sumária da utilização dos vários aspectos do sistema e possuíam apenas um pequeno manual de procedimento.

A abertura das mesas e dos postos de votação foram normalmente lideradas pelo técnico da empresa e não pelo Presidente da Mesa.

W9: Falta de sigilo (ou privacidade)

O posicionamento indevido de alguns assistentes em alguns dos locais de voto (do mesmo lado do eleitor), e o facto dos PVE não estarem suficientemente separados ou com protecções visuais, comprometeram o sigilo (ou privacidade) do voto.

W10: Paradigma confuso

A combinação de uma arquitectura do SVE pensada inicialmente para imitar o sistema tradicional, com a posterior inclusão das impressoras nas cabines de voto, perde coerência.

De facto, pode ser confuso para os eleitores verem o talão do voto a ser impresso e guardado na cabine de voto (que assim funciona também como urna), e terem ainda de levar e depositar o voto electrónico na urna electrónica.

A resolução deste problema pode passar por prescindir da impressão dos votos em papel ou por prescindir da urna electrónica (funcionando cada posto de votação também como urna electrónica).

De facto, a ideia de simular uma "entrega" do voto na mesa (na urna electrónica) acrescenta um passo eventualmente desnecessário (os votos poderiam ficar nos Postos de Votação até ao fecho) e em qualquer caso retardador do processo. A regeneração do *i-button* poderia ser assegurada pela Mesa.

De ressalvar que o modelo do SVE desenvolvido pela Multicert resulta de requisitos formulados pela UMIC para esta experiência piloto.

W11: Falta de maturidade do sistema de impressão de talões de voto

As impressoras dos votos e respectivos depósitos estavam ainda num estádio de desenvolvimento muito preliminar:

- O corte de papel era de tamanho variável.
- O papel ficava frequentemente encravado e mesmo quando caía era por vezes fácil ver o voto do eleitor anterior.
    - Segundo nos foi reportado, este problema ficou a dever-se a um problema detectado cerca de três dias antes das eleições, não havendo tempo para a remediar: o mau dimensionamento das urnas do registo de voto em papel.
- O circuito do voto estava protegido mas era facilmente destapável.
- Em diversos locais auditados, não havia praticamente tempo para confirmar o voto nem nada na interface apontava para isso. Aliás poucas pessoas olhavam para o papel.
- Não havia um procedimento devidamente consolidado para fazer face à eventualidade de algum eleitor reclamar que o papel não coincidia com a escolha que tinha feito no monitor.
    - No caso dessa eventualidade ocorrer (eventualidades “inesperadas” podem ocorrer num sistema de votação electrónica como num sistema tradicional), os coordenadores da UMIC estavam informados que a mesma devia ficar registada em acta, sendo necessário a identificação do eleitor queixoso.

W12: Votos em papel não permitem efectuar recontagem totalmente independente

Podem existir votos em papel que não valem porque foram cancelados posteriormente na urna electrónica. Assim, os talões de voto em papel não permitem efectuar uma

recontagem totalmente independente dos votos (a informação dos votos cancelados tem de ser obtida na urna electrónica).

W13: Falta de mecanismos de armazenamento redundante

A ausência de mecanismos de armazenamento redundante dos votos em cada urna electrónica pode implicar a repetição das eleições em caso de falha de disco, ainda que apenas para os eleitores que votaram nessa secção de voto (conforme registos no caderno eleitoral electrónico), a não ser que os talões de voto em papel permitam efectuar uma recontagem de votos totalmente independente.

Mais crítica, é a ausência de mecanismos de armazenamento redundante da informação de quem já votou na base de dados central do caderno eleitoral electrónico, pois pode implicar a repetição das eleições para todos os eleitores em caso de falha do disco do servidor. Mesmo que as bases de dados locais com a lista de pessoas que já votaram sejam fiáveis, permitindo em teoria recuperar a informação de quem já votou para o sistema central, a realização prática dessa recuperação seria problemática.

W14: Falta de fiabilidade das comunicações pela rede móvel

Num cenário de mobilidade, a solução de ligação via rede telefónica móvel não se revelou suficientemente fiável (por exemplo, 2 falhas durante o período de 2 horas de uma visita).

W15: Falta de mecanismos e procedimentos de recuperação de falhas

A seguir a uma perda de conectividade, a aplicação do caderno eleitoral não tinha capacidade para recuperar automaticamente a ligação.

W16: Falta de documentação

Não nos foi fornecida documentação sobre o sistema.

W17: Deficiências no desenho da interface do caderno eleitoral electrónico

Numa configuração definitiva à escala nacional, e em modo de operação normal, a possibilidade de seleccionar todos os eleitores (sem qualquer filtro) na interface do caderno eleitoral electrónico devia ser inibida, por se afigurar desnecessária e poder ser usada inadvertidamente prejudicando o desempenho do sistema.

A lista de eleitores que tinham votado mostrava permanentemente os primeiros votantes quando deveria estar por ordem inversa, mostrando sempre os últimos votantes, alguns dos quais ainda em fase de votação.

W18: Nomenclatura não uniforme

O *i-button* é designado "token" na aplicação da urna electrónica, enquanto que nas cabines de voto electrónico é designado "botão".

3.2 Ocorrências imprevistas observadas no dia do acto eleitoral

A percepção presencial do processo de votação permitiu detectar um conjunto de ocorrências imprevistas que deverão ser evitadas no futuro.

O1 - Perda de conectividade e posterior dificuldade de recuperação

Em diversos locais de voto, principalmente nos conectados por UMTS, ocorreram episódios de perda de conectividade do sistema do caderno eleitoral electrónico. Após o aparecimento da mensagem de erro da aplicação do caderno eleitoral, era necessário procurar restabelecer manualmente a ligação, o que nem sempre resultou. Em alguns casos, como último recurso, foi efectuado o *reboot* do sistema. Em diversos casos, o responsável da Multicert presente teve de efectuar uma consulta telefónica com um técnico da empresa. A recuperação demorava sempre pelo menos 2/3 minutos, principalmente em virtude do tempo de estabelecimento da VPN.

Segue-se uma lista com informação mais detalhada de alguns episódios de perda de conectividade observados pelos auditores ou a eles reportados.

- AMUPA (UMTS): Aquando da visita do auditor, a coordenadora da UMIC presente no local, referiu a existência de duas interrupções, que foram restabelecidas em alguns minutos. Posteriormente, a mesma coordenadora da UMIC reportou interrupções constante do sistema durante a tarde. Apesar de serem resolvidas de forma relativamente rápida pelo representante da Multicert e pelo próprio presidente da mesa, os referidos problemas explicam de forma significativa a fraca afluência ao Voto Electrónico (em termos percentuais) aí registada. Durante a tarde, entre as 16h e as 17h, registou-se uma falha do sistema UMTS que se prolongou durante cerca de 45 minutos. Ou seja, ao longo do dia, o sistema esteve em baixo entre duas e três horas. A AMUPA revelou-se o caso mais critico de toda a Freguesia.
- Escola Básica nº 2 (UMTS): Foram observados pelo auditor da FEUP presente dois episódios de perda de conectividade praticamente seguidos, às 15 e 15:05, que demoraram poucos minutos a resolver. O representante da Multicert contactou telefonicamente outro técnico da empresa e a ligação for restabelecida manualmente. A 2ª falha provocou alguma acumulação de pessoas em espera (8 a 9). Foi reportada pelo representante da UMIC uma falha de conectividade da abertura até às 9h, que fez com que o processo de votação só começou a decorrer

normalmente a partir das 10h30m (com perdas de conectividade pontuais), bem como outras falhas correspondendo a mais de duas horas de interrupção do processo normal de votação.

- Escola Básica nº 1 (UMTS): Foram observados pelo auditor da FEUP presente dois episódios de perda de conectividade, às 13h51m (por 15 minutos) e às 15h00m (por 7 minutos). O restabelecimento manual da ligação falhou sucessivamente, tendo sido necessário efectuar o *reboot* do computador nas duas vezes. O representante da Multicert consultou telefonicamente outro técnico da empresa da 1ª vez. Na 1ª falha, duas pessoas desistiram de esperar e, durante o período da falha, não foram convidados mais eleitores a efectuarem a experiência. Na 2ª falha, verificou-se uma acumulação de 7 a 8 pessoas à espera de votar (que continuaram a ser convidadas à experiência). Segundo foi reportado posteriormente pelo representante da UMIC, o problema mais grave de perda de conectividade ocorreu às 16h30m, quando a bateria do telemóvel que estava a assegurar a conectividade acabou, tendo-se perdido nesse momento as configurações de rede bem como o *user* que estava a ser utilizado no telemóvel. Após três tentativas frustradas de inserir um *login* e *password* predefinidos, o sistema bloqueou definitivamente. A falta de um *user* de reserva levou a que fosse necessário gerar um novo *user* / *password* na PT, processo que demorou cerca de uma hora e meia. Durante este tempo não foi possível aos eleitores votar electronicamente, mas foram realizadas demonstrações a todos os que se dirigiam à mesa electrónica. Os eleitores que queriam realmente votar electronicamente foram convidados a dirigirem-se à Casa da Cultura. De referir que a PT não estava preparada para este tipo de problemas em virtude de ter demorado muito tempo a apresentar uma solução. Devido à tentativa de geração de um novo *user* e *password* na EB1, a PT acabou por suspender a ligação UMTS em toda a freguesia durante cerca de 45 minutos, prejudicando os quatro locais ligados através da referida tecnologia e acarretando uma perda significativa de eleitores para o projecto.
- Atlético de Via Rara AVR (UMTS): Durante o período da visita, foram observadas diversas falhas de conectividade, que demoraram alguns minutos a resolver. Foi reportado pelo pessoal da Multicert que uma falha de conectividade UMTS numa altura crítica criou uma inconsistência entre a lista local de eleitores que votaram naquele posto e a situação real na base de dados central.
- Grupo Desportivo de Pirescoxe (ADSL): Verificaram-se algumas interrupções das comunicações no período da manhã.
- Sociedade Recreativa 1º de Agosto Santairiense (ADSL) : Não foram detectados episódios de perda de conectividade no curto tempo da visita (30 m).

O2 - Violação do princípio da independência na montagem das experiências

Registe-se ainda que o princípio da independência na montagem das experiências, para reduzir as interferências indesejáveis, foi violado pelas razões a seguir apontadas.

- Em Santa Iria de Azóia, a PT estava simultaneamente a experimentar a tecnologia de comunicações UMTS que aparentemente causou alguns períodos de indisponibilidade.
- Em Pirescoxe, ao lado da mesa de voto electrónico, foi montada (com autorização da UMIC) uma banca de demonstração de produtos da PT úteis num posto de votação electrónica para eleitores com necessidades especiais, desde invisuais a tetraplégicos ou doentes neurológicos, tendo sido efectuada uma demonstração de cerca de 45 minutos durante a visita do Secretário Geral do PCP. Dado o seu efeito perturbador sobre a experiência de votação electrónica, o coordenador da UMIC presente constatou nessa altura que a autorização não devia ter sido concedida.

O3 - Problemas no arranque do sistema do caderno eleitoral

A representante da UMIC presente na AMUPA, Paula Ávila, referiu que a votação electrónica só teve início pelas 9h devido a problemas no arranque do sistema com o caderno eleitoral.

O4 - Problemas no arranque dos postos de votação

Em Pirescoxe, dois dos três postos de votação não concluíram com sucesso o procedimento de abertura, o que só veio a acontecer após um *reboot* das máquinas, pelo que a votação electrónica só pôde começar às 8h30m.

O5 - Problemas com as impressoras

Verificaram-se diversos problemas de configuração e operação das impressoras.

- Escola Básica nº 2: Embora tal não se tenha verificado durante o tempo de visita, foi referido o facto de se terem verificado alguns encravamentos da impressora, bem como o facto dos talões de voto terem tamanho diferente.
- Casa da Cultura: Na altura da inicialização do sistema foi detectado um erro de configuração de uma das impressoras. Por diversas vezes registou-se o encravamento do papel dos votos impressos, devido ao pequeno tamanho do recipiente usado para o efeito.

O6 - Problemas com os leitores/gravadores de *i-buttons*

Casa da Cultura: Numa das cabines de votação, a votação só se iniciou por volta das 9h05m (e não pelas 8h15m como nas outros duas cabines), devido a problemas no

leitor/gravador de *i-buttons*. Foi necessário proceder por 2 vezes à substituição do leitor/gravador num dos postos de votação, havendo necessidade de reinicializar o sistema local.

O7 - Confusão na inserção do *i-button* na urna electrónica

Casa da Cultura: Em ocasiões distintas, 2 eleitores tentaram introduzir o dispositivo de armazenamento na ranhura da urna tradicional colocada em cima da mesa eleitoral.

O8 - Erro a utilizar o *i-button* na cabine de votação

Casa da Cultura: Em 2 ocasiões, eleitores tentaram exercer o seu voto na cabine de votação, tendo o sistema dado uma mensagem de erro. Nessas ocasiões, a mesa resolveu testar os respectivos dispositivos de armazenamento, inserindo-os na urna electrónica, tendo sido "surpreendida", nas 2 ocasiões, com a indicação "voto aceite". Uma explicação plausível para o sucedido é a seguinte: o *i-button* tinha um voto de um eleitor anterior, que não o chegou a descarregar devidamente na urna electrónica.

O9 - Erros a descarregar o voto para a urna electrónica

Pirescoxe (erros similares foram reportados noutros locais):

Os erros mais comuns na entrega do voto na urna electrónica foram:
a) a indicação de que o *i-button* (ou *token*) não possuía voto válido;
b) ultrapassagem do tempo definido para a votação;
c) erro interno.

A reacção da mesa (e do técnico da Multicert) foi variando com o tempo, o que denota uma falta de definição de procedimentos em caso de erro. O caso mais grave foi o primeiro, porque se identificaram duas razões principais para o seu aparecimento que ditavam respostas opostas.

Uma hipótese para o *i-button* não possuir um voto válido era o eleitor não ter concluído todos os passos da votação na cabine de voto, retirando o *i-button* antes da confirmação final. Esta situação é indetectável pela Mesa (não é emitido qualquer sinal luminoso ou sonoro). Quando se suspeitava dessa razão para o erro, a indicação a dar era a de o eleitor repetir o processo até ao fim na cabine de voto, para não se perder um voto relativamente ao que estava no caderno eleitoral.

A outra razão para o erro é a de o encaixe do botão no leitor da urna electrónica ser difícil, sendo no entanto o processo de leitura do conteúdo relativamente rápido. Era assim possível que a informação do voto fosse lida na primeira tentativa de encaixe (na realidade bastava encostar) e, quando o eleitor carregava melhor, a máquina respondia com o erro, porque entretanto o *i-button* já tinha sido regenerado. Neste caso, o voto já teria sido registado e não haveria lugar a repetição do processo.

Ficou assim a dúvida, relativamente a vários eleitores, sobre se o seu voto foi ou não efectivamente registado. Embora as duas situações associadas a este erro tenham efeitos que se cancelam, é de prever a existência de discrepâncias entre o número de votantes no caderno eleitoral e o número de votos na urna electrónica, como se veio a confirmar no final.

A interface da cabine de voto electrónico devia tornar claro que não se deveria retirar o *i-button* antes da segunda confirmação de que o voto era o pretendido, para evitar perdas de votos. O dispositivo de leitura dos *i-buttons* deveria ter manuseamento mecânico, temporizações e métodos de leitura que o tornem menos sujeito a interpretações erradas das mensagens.

O10 - Desligamentos inadvertidos

Casa da Cultura: Numa ocasião, um eleitor ao tentar manusear o monitor do posto de votação tocou inadvertidamente no botão de "On/Off", desligando-o.

O11 - Extravio de i-buttons

Grupo Desportivo de Pirescoxe: desaparecimento de um *i-button*, entre a abertura e as 11h30m.

O12 - Problemas de *layout*

- Pirescoxe: O *layout* da Mesa foi ajustado durante o processo, no sentido de ter um maior afastamento entre o Caderno Eleitoral e o Posto da Mesa, o que é bom no sentido de clarificar a independência informática das duas actividades. Notou-se, ainda assim, alguma confusão em torno da Mesa, em particular nos momentos de maior afluência. Pensa-se que esta situação poderia ser melhorada se o Caderno Eleitoral se encontrasse no topo da Mesa mais próximo da entrada dos eleitores, os quais poderiam assim fazer fila sem interferir com os que estavam a entregar o voto.
- Casa da Cultura: Registaram-se alguns atritos de alguns representantes dos partidos políticos presentes nas mesas de voto regulares em relação aos membros da mesa do sistema de votação electrónico, motivados pela disposição relativa do sistema de votação electrónica e das secções de voto tradicionais.

O13 - Discrepâncias significativas entre números de votos e de votantes

Pirescoxe: No apuramento de resultados, foram observadas as discrepâncias já relatadas em secção anterior.

Para mais detalhe, ver a secção 2.1.10 (apuramento de resultados).

O14 - Inconsistência entre a base de dados local e a base de dados central do caderno eleitoral

AVR: Foi reportado pelo pessoal da Multicert que uma falha de conectividade UMTS numa altura crítica tinha criado uma inconsistência entre a lista local de eleitores que votaram naquele posto e a situação real na base de dados central.

O15 - Votos ilegíveis

Na reunião com técnicos da Multicert, foram-nos reportados 2 casos de votos com erro nas urnas electrónicas. Num caso o voto era ilegível, noutro caso o número da opção de voto não era válido.

O16 - PIN incorrecto

Casa da Cultura: Numa das 3 votações por telemóvel observadas pelo auditor presente, a votação teve que ser repetida uma vez que o PIN (código) utilizado foi considerado incorrecto, havendo necessidade de recorrer a outro PIN (foi aberto um novo envelope).

3.3 Aspectos não auditados

Falta verificar se pode ser impresso mais do que um talão de voto no caso de alguma falha (ficamos com a impressão que isso podia acontecer, mas não foi possível verificar no decorrer do processo).

Os eleitores tinham alguma dificuldade em interagir com o ecrã táctil. Não foi possível verificar a origem deste problema, se resultante do próprio ecrã, se terá origem na área sensível de escolha dos partidos.

Falta analisar com mais detalhe a segurança das comunicações, que são um ponto vulnerável do sistema.

4 Análise das características do SVE

As características dos Sistemas de Voto Electrónico, ao nível da Segurança, Transparência, Usabilidade e Acessibilidade (referidos nos pontos seguintes), serão objecto de apreciação detalhada de seguida. A atribuição de pesos relativos aos vários atributos de Segurança, Transparência, Usabilidade e Acessibilidade, permitirá ainda definir o «Índice de viabilidade tecnológica», a incluir no relatório final.

4.1 Segurança (S)

O quadro apresentado mais adiante analisa de forma qualitativa e quantitativa os vários atributos considerados no capítulo da segurança.

Em resumo, os aspectos mais positivos a salientar são:

- a dificuldade de forjar votos (ver atributo "Imunidade a Ataques");
- a necessidade da inserção dos *i-buttons* dos membros da mesa (1, 2 ou 3, dependendo do grau de criticidade) para a realização de operações críticas (ver atributo "Autenticação do Operador").

Há, no entanto, diversos aspectos negativos que precisam de ser corrigidos para a solução poder ser considerada aceitável, de que se salientam os seguintes:

- verificaram-se discrepâncias significativas entre o número de votos e votantes, com mais 2,3 % votos do que votantes, muito superiores às verificadas em locais em que foram usados sistemas doutras empresas, pelo que não é de crer que se devam apenas a falhas humanas (este relatório aponta essencialmente para falhas ao nível da usabilidade dos *i-buttons* e falhas ao nível do controlo aplicacional);
- não existem mecanismos apropriados de armazenamento redundante e recuperação de falhas no servidor do caderno eleitoral electrónico, que é crítico num cenário de mobilidade à escala nacional;
- os votos são guardados nas urnas electrónicas de forma não cifrada nem assinada, o que pode permitir a contagem dos votos antes de terminado o período eleitoral (por não serem cifrados), e a alteração indevida dos votos (por não serem assinados);
- o sistema de impressões dos votos não é suficientemente fiável para permitir uma recontagem totalmente independente dos votos;

- verificou-se uma baixa disponibilizada do sistema, devida não só a causas externas ao sistema (problemas de conectividade da rede UMTS), como a dificuldade de recuperação do sistema e no arranque de diversos equipamentos;
- o sistema estava montado de forma artesanal, sem garantir o necessário isolamento dos equipamentos (dando acesso apenas aos dispositivos de interface estritamente necessários) e a privacidade dos eleitores.

		-				+	
SEGURANÇA (S)							**Comentários**
S	**Auditabilidade**			x			
	O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.						(+) Multicert disponibiliza-se para facultar acesso a código fonte para efeito de auditoria. (-) Processo de desenvolvimento não documentado. (-) Software não selado com *checksum*.
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.						(+) Operações críticas exigem inserção de *i-buttons* de um ou mais elementos da mesa. (-) Servidor do caderno eleitoral só tem autenticação a nível do sistema operativo.
S	**Certificabilidade**			x			
	O sistema deve poder ser testado e certificado por agentes oficiais.						(+) Sistema em princípio certificável, mas (-) de selagem mais problemática por se basear em máquinas Windows não dedicadas.
S	**Fiabilidade**		x				
	O SVE deve funcionar de forma fiável, sem perda de votos.						(-) Discrepâncias significativas entre números de votos e de votantes, com mais 2,3 % de votos do que votantes (O13), (-) 2 votos ilegíveis na urna electrónica (O15) e (-) votos em papel a rever, tanto por deficiência do sistema como dos procedimentos. (+) Fiabilidade e robustez dos i-buttons (S3).
S	**Detectabilidade**			x			
	O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.						(.) Não são conhecidos mecanismos deste tipo.
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.						(-) Disponibilidade prejudicada seriamente devido a falhas nas comunicações por UMTS alheias ao sistema (O1, W14), dificuldade de recuperação do sistema (O1, W15), e dificuldade a arrancar diversos equipamentos (O3, O4).
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.						(-) Segurança nos i-buttons (assinatura, cifragem) por implementar (W1), mas (+) o facto de usar um nº de autorização único gerado e validado pela urna praticamente impede forjar votos (S5). (+) Comunicação com o servidor do caderno eleitoral sobre VPN.

S	**Integridade dos Votos**		X				
	Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.						(-) Votos guardados não cifrados (W1), mas (+) o sistema da urna electrónica está isolado (pelo menos enquanto não comunica resultados).
S	**Invulnerabilidade**		X				
	A invulnerabilidade do SVE é a garantia de que não se pode aceder e alterar o sistema indevidamente.						(-) Mais difícil garantir por hardware não ser dedicado.
S	**Rastreabilidade**		X				
	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).						(-) Tabelas de *logs* previstas mas não foram usadas (2.1.3).
S	**Recuperabilidade**		X				
	O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.						(-) Base de dados local do caderno eleitoral ficou inconsistente aquando de falha de comunicação (O14). (-) Dificuldade de recuperação após perda de conectividade (O1, W15).
S	**Tolerância a Falhas**		X				
	Caso ocorra uma falha no sistema é possível recuperar o estado anterior e o funcionamento regular, assegurando um serviço aceitável.						(-) Não há redundância de bases de dados - caderno eleitoral e votos electrónicos (W13).
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.						(+) Cabines de voto e urna funcionam autonomamente, mas (-) montagem artesanal (W2).
S	**Segurança das comunicações**			X			
	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.						(+) Comunicação com servidor do caderno eleitoral por VPN. (-) Os resultados finais não foram comunicados (W1), mas (+) seria por HTTPS.

4.2 Transparência (T)

O quadro da página seguinte analisa de forma qualitativa e quantitativa os vários atributos considerados no capítulo da transparência.

Em resumo, os aspectos mais positivos a salientar são:

- garantia da propriedade de não-coercibilidade, dada intrinsecamente pelo voto presencial (electrónico ou não);
- transparência e verificabilidade proporcionada intrinsecamente pela impressão dos votos em papel (apesar das limitações apontados à solução concreta apresentada).

A maioria dos pontos negativos identificados são consequência de deficiências já apontadas no capítulo da segurança sobre atributos como singularidade, atomicidade, confiabilidade e precisão.

É ainda valorizada negativamente a ausência (ou pelo menos não disponibilização) de documentação técnica do produto, que se considera fundamental em sistemas de maior criticidade.

	-				+	
TRANSPARÊNCIA (T)						**Comentários**
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).						(-) Ordenação de votos e votantes pode permitir alguns cruzamentos (W6), mas (+) o problema é de fácil correcção.
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)?						(-) Difícil percepção de conclusão efectiva do voto (W5). (-) Discrepâncias significativas entre votos e votantes (O13) são sintoma de não atomicidade.
T **Autenticidade (método de autenticação do utilizador)**					x	
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.						(+) Aparentemente, sujeito apenas a falhas humanos na identificação presencial do eleitor.
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.						(-) Montagem artesanal (W3). (-) Falhas de conectividade (O1) e outras (O8, O9) visíveis para os eleitores.
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.						(-) Não foi fornecida embora tenha sido pedida (W16).

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.						(.) Não são conhecidos procedimentos especiais de selecção do pessoal.
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.						(-) Software não selado com *checksum*. Teoricamente (+) será possível correr um programa que verifica se a configuração actual do sistema corresponde ao que foi certificado, mas (-) é mais difícil garantir por hardware não ser dedicado.
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.						(+) Garantido intrinsecamente por voto presencial privado, não podendo o eleitor levar consigo um documento comprovativo do seu voto.
T	**Precisão do SVE**		x				
	O sistema deve garantir que todos os votos são adequadamente registados e contabilizados.						(-) Discrepâncias significativas entre números de votos e de votantes, com mais 2,3 % de votos do que votantes (O13). (-) Dois votos ilegíveis na base de dados da urna electrónica (O15).
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.						(-) Falta de sigilo devido a ausência de separadores e interferência de assistentes (W9), mas (+) o problema é de fácil correcção. Ver também anonimato e não coercibilidade.
T	**Singularidade (Não Reutilização)**		x				
	O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.						(-) Discrepâncias entre números de votos e votantes indiciam quebra de singularidade (O13), correcção pode passar por melhor controlo aplicacional e melhor usabilidade dos *i-buttons*.
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.						(-) Falta de informação, novidade. (+) Separação visível entre urna e caderno eleitoral (S2a). (+) Impressão em papel (S2c).
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.						(.) Sistemas operativo standard Windows (sem código aberto), bases de dados standard, equipamento standard.

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.						(+) Votos impressos em papel (S2c) , mas (-) ficam visíveis por tempo insuficiente, não há chamada de atenção suficiente, possibilidade de entupimento (W11, O5), (-) e não permitem efectuar rectontagem totalmente independente (W12). (-) Não há gravação redundante dos votos (W13) (a menos dos votos em papel, que não são ainda fiáveis). (+) Contagem separada de votos e votantes.
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.						(-) Falta de autonomia da mesa (W8) e dos eleitores (W7).

4.3 Usabilidade (U)

O quadro da página seguinte analisa de forma qualitativa e quantitativa os vários atributos considerados no capítulo da usabilidade.

Em resumo, o principal aspecto negativo a salientar neste capítulo, é a deficiente usabilidade do sistema de i-buttons (i-buttons, suportes e/ou leitores/gravadores).

De resto o sistema tem características perfeitamente aceitáveis.

	-				+	
USABILIDADE (U)						**Comentários**
U **Facilidade de uso**		X				
O sistema deve ser de uso fácil, quer para eleitores quer para operadores (membros da mesa de voto).						(-) Má usabilidade de i-buttons (W4, O7).
U **Rapidez de uso**			X			
O sistema deve ser de uso rápido, quer para eleitores quer para operadores (membros da mesa de voto).						(+) Razoável (S1), muito melhor que na versão anterior, mas (-) mais lento que sistema tradicional (1 minuto com apoio).
U **Clareza da Linguagem na Interface**			X			
A interface do SVE (linguagem e 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.						(+) Relativamente clara, mas (-) termos como *token* e *i-button* não são familiares, além de que são usados diferentes termos (W18). Necessidade/imposição de ajuda sistemática (W7).
U **Localização da Interface**		X				
A localização, orientação e altura do monitor, bem como dos restantes dispositivos de interacção, devem ser apropriadas ao eleitor.						(-) Localização dos leitores-gravadores de i-buttons nas cabines de voto electrónico (W4), montagem artesanal (W3).
U **Satisfação emocional**				X		
O sistema deve ser atraente e agradável de usar.						(+) Eleitores em geral satisfeitos (3.1.1).

4.4 Acessibilidade (A)

O quadro da página seguinte analisa de forma qualitativa e quantitativa os vários atributos considerados no capítulo da acessibilidade.

Em resumo, o principal aspecto positivo a salientar é o suporte (ainda que limitado) de mobilidade que, uma vez alargado à escala nacional, se espera poder contribuir para tornar o voto mais conveniente para os eleitores e reduzir a abstenção.

O principal aspecto negativo a salientar tem a ver com o suporte insuficiente da solução apresentada (nomeadamente a solução baseada em telemóvel) para a votação por invisuais e outras pessoas com necessidades pessoais.

	-				+	
ACESSIBILIDADE (A)						**Comentários**
A **Conveniência**				x		
O sistema só será útil se permitir a todos os votantes exercerem o seu direito de voto de forma rápida, com o mínimo de equipamento, treino e sem necessidades específicas adicionais.						(+) Tempo de votação aceitável (-) mas ainda significativamente maior que no sistema tradicional (de voto em papel). (-) Necessidade de apoio em todos os passos no processo de votação electrónica (W7).
A **Direito de Voto**				x		
O direito de voto deverá poder ser efectivamente exercido se um eleitor verificar simultaneamente as propriedades de Autenticidade e Singularidade.						(-) Voto electrónico com suporte de mobilidade é intrinsecamente mais sensível a falhas de comunicações.
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.						(+) Disponibilizado folheto. (-) Não houve simulador.
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, analfabetas, etc.						(-) Sistema de votação por telemóvel destinado a pessoas com necessidades especiais (nomeadamente invisuais) é difícil de usar.
A **Mobilidade**			x			
O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.						(+) Suporte de mobilidade (S4), mas apenas dentro do mesmo círculo eleitoral (W2).

4.5 Características transversais e outros aspectos (O)

O quadro da página seguinte analisa de forma qualitativa e, se possível, quantitativa alguns atributos que não se enquadram nos grupos anteriores.

	-				+	
CARACTERÍSTICAS TRANSVERSAIS E OUTROS ASPECTOS (O)						**Comentários**
O **Viabilidade (Custo/Beneficio)**						
O SVE deve ser eficiente e viável economicamente.						Não existem dados suficientes para avaliar este aspecto. No entanto no relatório final global de auditoria da FEUP serão apresentadas algumas considerações sobre o assunto. (+) A utilização de hardware de uso genérico (não dedicado), pode permitir reduzir os custos. (+) A utilização de *tokens* reutilizáveis (*i-buttons*) pode ser mais económica do que a utilização de *tokens* não reutilizáveis. (-) Voto electrónico presencial é intrinsecamente mais caro do que o voto pela Internet.
O **Escalabilidade do Sistema**				X		
A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.						(-) Não se fez a concentração de resultados, onde se poderiam verificar problemas de estrangulamento e escalabilidade do sistema. (-) Voto com suporte de mobilidade, com acesso remoto *online* a caderno eleitoral, pode intrinsecamente causar problemas de estrangulamento e escalabilidade do sistema.

4.6 Quadro Resumo da Apreciação

			Multicert					
SEGURANÇA (S)		100,00%			**2,57**			
S1	**Auditabilidade**	10,29%			x			3
S2	**Autenticação do Operador**	4,43%				x		4
S3	**Certificabilidade**	9,02%			x			3
S4	**Fiabilidade**	9,77%		x				2
S5	**Detectabilidade**	4,59%			x			3
S6	**Disponibilidade do Sistema**	5,44%		x				2
S7	**Imunidade a Ataques**	8,13%				x		4
S8	**Integridade dos Votos**	14,39%		x				2
S9	**Invulnerabilidade**	9,28%		x				2
S10	**Rastreabilidade**	3,82%		x				2
S11	**Recuperabilidade**	5,30%		x				2
S12	**Tolerância a Falhas**	4,59%		x				2
S13	**Isolamento**	2,58%		x				2
S14	**Segurança das comunicações**	8,35%			x			3
TRANSPARÊNCIA (T)		100,00%			**3,15**			
T1	**Anonimato**	11,25%			x			3
T2	**Atomicidade**	7,00%	x					1
T3	**Autenticidade** (método autenticação utilizador)	11,46%					x	5
T4	**Confiabilidade**	6,22%		x				2
T5	**Documentação técnica**	2,16%	x					1
T6	**Integridade do Pessoal**	2,83%				x		4
T7	**Integridade do Sistema**	5,96%		x				2
T8	**Não-Coercibilidade**	10,48%					x	5
T9	**Precisão do SVE**	7,61%		x				2
T10	**Privacidade**	7,57%				x		4
T11	**Singularidade (Não Reutilização)**	10,75%		x				2
T12	**Transparência do Processo**	3,46%				x		4
T13	**Transparência do Sistema**	3,93%			x			3
T14	**Verificabilidade**	6,46%				x		4
T15	**Separação de papéis**	2,87%			x			3
USABILIDADE (U)		100,00%			**2,68**			
U1	**Facilidade de uso**	38,39%		x				2
U2	**Rapidez de uso**	10,06%			x			3
U3	**Clareza da Linguagem na Interface**	23,38%			x			3
U4	**Localização da Interface**	11,13%		x				2
U5	**Satisfação emocional**	17,04%				x		4
ACESSIBILIDADE (A)		100,00%			**3,50**			
A1	**Conveniência**	14,42%				x		4
A2	**Direito de Voto**	46,96%				x		4
A3	**Documentação para eleitor**	7,63%			x			3
A4	**Flexibilidade**	11,86%		x				2
A5	**Mobilidade**	19,13%			x			3
A6	**Viabilidade (Custo/Beneficio)**							x
S15	**Escalabilidade do Sistema**					x		4

5 Conclusões e Recomendações

5.1 Conclusões

O modelo do SVE apresentado pela Multicert caracteriza-se genericamente pelas seguintes opções (ainda que não completamente implementadas ou implementadas de forma não satisfatória), "herdando" por isso as vantagens e desvantagens intrínsecas a essas opções:

- voto electrónico (por oposição a voto tradicional);
  - facilita e torna mais fiável a contagem de votos;
  - impede a ocorrência de votos nulos;
  - possibilita a votação com maior privacidade das pessoas com necessidades especiais, nomeadamente invisuais;
  - reduz a logística dos boletins de voto;
  - aumenta a logística dos equipamentos;
- voto presencial (por oposição a voto pela Internet);
  - garante a propriedade de não-coercibilidade;
  - é mais dispendioso que o voto pela Internet;
  - para algumas pessoas é mais conveniente que o voto pela Internet, enquanto que para outras pessoas se passa o contrário (o que quer dizer que a combinação dos dois sistemas maximiza a conveniência para o eleitor);
- suporte de mobilidade, isto é, possibilidade de um eleitor votar em qualquer secção de voto, e não apenas naquela em que está recenseado;
  - torna o voto mais conveniente para os eleitores, e pode contribuir para reduzir as taxas da abstenção;
  - aumenta a vulnerabilidade do sistema a ataques e falhas de comunicação, pois obriga a conectar as secções de voto durante o período eleitoral;
  - reduz a garantia de anonimato, pois pode ser necessário associar a autorização de voto concedida ao eleitor com o seu local de recenseamento;
- impressão de voto em papel, para além do registo do voto em formato electrónico;

  - permite a contagem dos votos por qualquer pessoa (como acontece no voto tradicional), ainda que não se espera que isso seja feito de forma sistemática (mas apenas por amostragem e em caso de anomalias);
  - permite ao eleitor ver o seu voto e assim aumentar a confiança no sistema;
  - complica a logística e custo do processo de votação;
- as cabines de voto electrónico não são urnas electrónicas (por oposição ao modelo em que as cabines de voto electrónico são também urnas electrónicas);
  - torna o processo de votação mais complicado para o eleitor;
  - aproxima-se mais do sistema tradicional;
  - pode permitir proteger melhor os votos;
  - é confuso quando as cabines de voto também imprimem os votos;
- separação física entre caderno eleitoral e restantes sub-sistemas (cabines de votação electrónica + urnas electrónicas);
  - dá maior garantia de anonimato;
  - possibilita a ocorrência de discrepâncias entre número de votantes (marcados no caderno eleitoral electrónico) e número de votos (armazenados nas urnas electrónicas), nem que seja por erro humano;
- utilização de hardware não dedicado (por oposição a hardware dedicado);
  - pode reduzir o custo e a logística do processo (se forem usadas instalações já equipadas e também usadas com outras finalidades);
  - pode colocar problemas de segurança e dificuldade de verificação dos sistemas.

No que se refere à implementação e configurações concretas apresentadas pela Multicert, e à forma como decorreu o processo de votação, são de salientar as seguintes conclusões:

- O SVE desenvolvido pela Multicert encontra-se ainda numa fase embrionária (solução incompleta e inacabada, solução de mobilidade reduz-se essencialmente à vertente de identificação, falta de maturidade do sistema de impressão dos votos, falta de documentação, montagem rudimentar, etc.).
- A usabilidade do sistema de *i-buttons* revelou-se claramente insatisfatória.

- Verificaram-se discrepâncias significativas entre o número de votos e votantes, com mais 2,3 % votos do que votantes, muito superiores às verificadas em locais em que foram usados sistemas doutras empresas, pelo que não é de crer que se devam apenas a falhas humanas. As discrepâncias verificadas terão a ver essencialmente com problemas de usabilidade do sistema de *i-buttons* e deficiente controlo aplicacional.
- O processo de votação pareceu bastante fluido, principalmente em ocasiões de pouca afluência de votantes. No entanto, praticamente todas as pessoas foram assistidas na votação, embora nem sempre o solicitassem.
- O cenário de mobilidade montado nesta freguesia poderá ser importante uma vez alargado a nível nacional. Neste cenário de mobilidade, o ponto mais fraco foi claramente a questão das comunicações. A solução de ligação via UMTS revelou-se fortemente inviável, em virtude da imaturidade tecnológica demonstrada (alheia ao SVE em si). Em contrapartida, as ligações via ADSL revelaram um comportamento aceitável.

5.2 Recomendações

Podem-se apontar as seguintes recomendações genéricas relativas ao modelo de SVE a usar e à condução de próximas experiências de votação electrónica:

- Num cenário de mobilidade, não utilizar a tecnologia UMTS enquanto esta não estiver suficientemente amadurecida e com provas dadas em Portugal.
- Garantir a formação atempada das pessoas que vão constituir as mesas eleitorais electrónicas.
- Garantir a disponibilização atempada para os eleitores e o público em geral de informação sobre os sistemas de votação electrónica a usar em próximas experiências de votação electrónica (vinculativas ou não vinculativas).

Relativamente ao SVE apresentado especificamente pela Multicert, recomenda-se a revisão e amadurecimento do mesmo, por forma a ultrapassar os vários problemas apontados ao longo deste relatório, mantendo as suas melhores características. Em particular:

- Revisão ou substituição do sistema de *i-buttons*, por forma a melhorar a usabilidade do sistema.

- Introdução de mecanismos que tornem mais evidente a conclusão efectiva do voto, tanto para o eleitor como para a Mesa.
- Desenvolvimento de uma solução completa de mobilidade, suportando a mobilidade dos eleitores à escala nacional.
- Revisão de todo o sistema de impressão, não só ao nível da sua implementação, como também ao nível da sua concepção, por forma a poder servir para a recontagem dos votos de forma fiável e totalmente independente.
- Melhorar o suporte para eleitores com necessidades especiais.
- Repensar e eventualmente eliminar a separação entre cabines de voto electrónico e urnas electrónicas.