Voto Electrónico · Eleições Europeias 2004
Resultados do Processo de Auditoria

José Manuel Valença, Manuel Bernardo Barbosa, José Bacelar Almeida [1]

9 de Agosto de 2004

[1]Departamento de Informática · Escola de Engenharia · Universidade do Minho

Conteúdo

Capítulo 1

Principais resultados

Um dos argumentos apresentados para a adopção de um sistema de votação electrónica é a mobilidade dos eleitores, isto é, a possibilidade de votar numa assembleia de voto diferente daquela onde normalmente se votaria. Este tipo de mobilidade implica a transferência de boletins, encerrados, entre as diversas assembleias de voto, para que a contagem possa ser efectuada correctamente. Em alternativa, a contagem poderá ser efectuada apenas centralmente, sendo os boletins dos eleitores de cada assembleia de voto abertos simultaneamente, independentemente da sua proveniência geográfica. **Nenhum dos sistemas analisados permite, no modo de utilização que foi auditado, implementar este tipo de funcionalidade.**

Das três soluções que foram analisadas, **apenas a solução Multicert apresenta integração entre o sistema de gestão de cadernos eleitorais e o sistema de recolha de votos**, pelo que está mais perto de poder fornecer mobilidade. Provavelmente por ter sido desenvolvido especificamente para este acto eleitoral, este sistema necessita ainda de algum amadurecimento em termos de implementação.

Os sistemas Indra e Unisys são muito semelhantes em termos da funcionalidade que oferecem, estando limitados à recolha de votos. A gestão dos cadernos eleitorais tem de ser feita manualmente ou, como foi o caso, através de uma aplicação desenvolvida para o efeito. **Ambas as soluções se encontram numa fase de desenvolvimento estabilizado, tendo já sido utilizadas em votações oficiais noutros países.** Em termos comparativos, e excluindo factores económicos, a solução Unisys apresenta algumas vantagens relativas, nomeadamente o facto de usar HW e SW específico, o facto de os tokens utilizados serem verificados pela mesa depois de utilizados para depositar um voto.

De acordo com a informação que foi possível recolher, é possível concluir que **todas as soluções analisadas permitiriam levar a cabo uma votação electrónica com um nível de segurança adequado, desde que a sua utilização seguisse um conjunto de procedimentos que garantisse a sua correcção**.

Há no entanto aspectos que deixam algumas preocupações:

- As garantias quanto à segurança das componente fundamentais dos vários sistemas (anonimato do voto, unicidade e integridade do voto, correcção na contagem, etc.) derivam essencialmente da confiança de que a funcionalidade

do sistema é aquela que está expressa; não existem, porém, mecanismos externos que permitam validar essas garantias sem recorrer à auditoria do código fonte.

- Nesta experiência não foi possível avaliar cabalmente a fiabilidade dos sistemas analisados, por forma a ser possível extrapolar algum tipo de garantia de funcionamento normal numa votação a nível nacional.
- Ficou patente nas visitas que efectuamos que um dos aspectos mais importantes para o sucesso de um processo de votação electrónica, será a capacidade de os membros das assembleias de voto garantirem a correcção do processo. A formação dos elementos das assembleias de voto será um dos grandes problemas a resolver no caso da evolução para um sistema de votação electrónica.

Capítulo 2

Resultados do processo de auditoria

2.1 Sistema Indra

Este sistema não inclui nenhum tipo de funcionalidade de gestão de cadernos eleitorais. Isto é uma falha assinalável, no caso de a mobilidade dos votantes ser importante. O objectivo deste sistema é apenas o de eliminar a votação em papel, e de acelerar o processo de contagem dos votos. Por outro lado, isto simplifica enormemente o funcionamento do sistema e torna muito mais fácil a implementação de mecanismos de segurança adequados.

A documentação fornecida pela Indra para a elaboração desta auditoria, revela algum cuidado, mas é omissa no que diz respeito ao aspecto mais importante: a natureza e o formato da informação armazenada em cada componente do sistema: smartcards e cabine (incluindo a memória flash).

2.1.1 Recursos necessários (estimativa de custo)

1. Recursos Materiais
    - É necessário um conjunto de cabines adequado ao número de votantes da assembleia de voto, um número razoável de smartcards (que permita que a formatação daqueles que são utilizados não implique tempo de espera para os votantes), e equipamento para formatação dos cartões utilizados.
    - Todo o equipamento é propriedade da própria empresa, e não tem de ser adquirido pelo Estado.
    - Não foi fornecida nenhuma indicação dos custos associados.
2. Recursos Humanos
    - Na experiência realizada, o número de técnicos presente no local era claramente exagerado e incomportável numa eleição real.
    - Não foi fornecida uma estimativa do que seria uma equipa de suporte razoável, e dos custos associados.

3. Infraestruturas

    - Apenas são necessárias ligações de alimentação correntes, e uma linha telefónica para ligação das cabines ao servidor central no final da votação.

2.1.2 Requisitos funcionais (adequação do sistema à estrutura clássica da Assembleia de Voto)

1. Inicialização

    - O tempo de instalação, realizada tipicamente pelos técnicos, é razoavelmente baixo.
    - Não parece viável deixar este procedimento a cargo dos elementos da mesa, a não ser com um esforço considerável de formação.
    - A impressão de um relatório no instante da abertura de cada cabine é um elemento importante para assegurar que os elementos da mesa são capazes de assegurar que a inicialização decorreu correctamente.

2. Votação

    - O processo é simples: um eleitor identificado recebe um smartcard que lhe permite aceder à cabine, no final da votação esse smartcard é devolvido à mesa para ser formatado.
    - Uma evolução para este sistema não traria problemas para o caso Português, desde que a gestão dos Cadernos Eleitorais permanecesse inalterada.
    - Um aspecto menos bom deste sistema, é o facto de ser difícil aos membros da mesa de voto verificarem que os eleitores depositam os seus votos correctamente.

3. Contagem

    - O processo de encerramento, contagem dos votos, e impressão de resultados é simples e rápido, e poderia facilmente ser levado a cabo pelos elementos da mesa.

4. Exportação dos resultados

    - A funcionalidade de transferência dos resultados para um servidor central por ligação dial-up é eficaz.
    - Não parece viável deixar este procedimento a cargo dos elementos da mesa, a não ser com um esforço considerável de formação.
    - É, no entanto, razoável assumir que os elementos da mesa serão capazes de controlar o correcto desenrolar dos procedimentos.

2.1.3 Requisitos de segurança

1. Ligação ao exterior

    - O único contacto electrónico com o exterior ocorre já no final da votação, e por uma ligação dial-up.

- Os cuidados de segurança nesta transferência parecem adequados, principalmente tendo em conta que existe uma contagem em papel impresso pelas cabines, que fica registada nas actas, e que funciona como garante da integridade dos resultados.

2. Identificação do eleitor
   - Presencial.
3. Caderno Eleitoral (gestão das listas de eleitores)
   - Manual.
   - A autorização de voto é representada pela posse de um smartcard formatado.
4. Cabine de voto
   - A privacidade física do votante é satisfatória.
   - Não há riscos de perda do anonimato, a não ser em cenários improváveis de inspecção da BD interna de cada cabine e extracção da sequência de votação.
   - Partindo do princípio que o sistema de smartcards funciona correctamente, e que não há lugar a furtos, também não há riscos de votação dupla, ou de eleitores não autorizados.
   - Note-se que o facto de o token utilizado ser um smartcard, com formato standardizado e muito disseminado, há riscos de um votante mal intencionado inserir numa cabine um cartão diferente daquele que lhe é fornecido da mesa. As possíveis consequências deste tipo de ataque não podem ser avaliadas com a informação disponível.
   - A utilização de hardware e software desenvolvidos por terceiros é um factor de risco, nomeadamente no que diz respeito ao sistema operativo. No entando, o ambiente controlado em que o equipamento é utilizado deverá ser suficiente para eliminar esses riscos.
   - Não foram fornecidos elementos técnicos suficientemente detalhados sobre o tipo de informação que é armazenado nas cabines. Por esta razão não é possível avaliar as possíveis consequências de uma análise intrusiva do conteúdo de uma cabine no final de uma votação.
   - O SGBD utilizado nas cabines é reconhecidamente uma solução para aplicações de muito pequena dimensão, e é importante avaliar qual número de votos a partir do qual a sua performance se deteriora.
   - Uma avaliação das garantias fornecidas relativamente à não manipulação de resultados dentro das cabines apenas seria possível através de um processo de creditação do código fonte.

2.2 Sistema Unisys

Este sistema não inclui nenhum tipo de funcionalidade de gestão de cadernos eleitorais. Isto é uma falha importante, no caso de a mobilidade dos votantes ser importante. O objectivo deste sistema é apenas o de eliminar a votação em papel, e de acelerar o processo de contagem dos votos. Por outro lado, isto simplifica enormemente o funcionamento do sistema e torna muito mais fácil a implementação de mecanismos de segurança adequados.

A documentação fornecida pela Unisys para a elaboração desta auditoria é satisfatória, sendo no entanto omissa omissa no que diz respeito ao aspecto mais importante: a natureza e o formato da informação armazenada em cada componente do sistema: cabines e tokens.

2.2.1 Recursos necessários (estimativa de custo)

1. Recursos Materiais
    - É necessário um conjunto de cabines adequado ao número de votantes da assembleia de voto, um número razoável de tokens (que permita evitar que um votante fique retido por não haver um token disponível).
    - Todo o equipamento é propriedade da própria empresa, e não tem de ser adquirido pelo Estado.
    - Não foi fornecida nenhuma indicação dos custos associados.
2. Recursos Humanos
    - Na experiência realizada, o número de técnicos presente no local seria difícil de replicar numa eleição real.
    - Não foi fornecida uma estimativa do que seria uma equipa de suporte razoável, e dos custos associados.
3. Infraestruturas
    - Apenas são necessárias ligações de alimentação correntes, e uma linha telefónica para ligação da base-station a um servidor central no final da votação.

2.2.2 Requisitos funcionais (adequação do sistema à estrutura clássica da Assembleia de Voto)

1. Inicialização
    - O tempo de instalação, realizada tipicamente pelos técnicos, é razoavelmente baixo.
    - Não parece viável deixar este procedimento a cargo dos elementos da mesa, a não ser com um esforço considerável de formação.
    - A impressão de um relatório no instante da abertura das cabines é um elemento importante para assegurar que os elementos da mesa são capazes de assegurar que a inicialização decorreu correctamente.
2. Votação
    - O processo é simples: um eleitor identificado recebe um token que lhe permite aceder à cabine, no final da votação esse token é devolvido à mesa para ser formatado.
    - A possibilidade de detectar anomalias no conteúdo destes tokens assim que o votante os devolve é uma mais valia no que diz respeito ao controlo do desenrolar do processo por parte dos elementos da mesa.
    - Uma evolução para este sistema não traria problemas para o caso Português, desde que a gestão dos Cadernos Eleitorais permanecesse inalterada.

3. Contagem

   - O processo de encerramento, contagem dos votos, e impressão de resultados não é demasiado complicado, mas parece difícil assumir que pode ser levado a cabo pelos elementos da mesa sem formação adequada.
   - É, no entanto, razoável assumir que os elementos da mesa serão capazes de controlar o correcto desenrolar dos procedimentos.

4. Exportação dos resultados

   - A funcionalidade de transferência dos resultados para um servidor central por ligação dial-up é apropriada.
   - Não parece viável deixar este procedimento a cargo dos elementos da mesa, a não ser com um esforço considerável de formação.
   - É, no entanto, razoável assumir que os elementos da mesa serão capazes de controlar o correcto desenrolar dos procedimentos.

2.2.3 Requisitos de segurança

1. Ligação ao exterior

   - O único contacto electrónico com o exterior ocorre já no final da votação, e por uma ligação dial-up.
   - Os cuidados de segurança nesta transferência parecem adequados, principalmente tendo em conta que existe uma contagem em papel impresso pela base-station, que fica registada nas actas, e que funciona como garante da integridade dos resultados.

2. Identificação do eleitor

   - Presencial.

3. Caderno Eleitoral (gestão das listas de eleitores)

   - Manual.
   - A autorização de voto é representada pela posse de um token formatado.

4. Cabine de voto

   - A privacidade física do votante é satisfatória.
   - Não há riscos de perda do anonimato. O sistema em questão foi desenvolvido com o cuidado de não armazenar a informação com base na sequência de inserção dos votos.
   - Existe a possibilidade de "marcar"votos, para que numa fase posterior o administrador indique se devem ou não ser aceites. A utilização desta funcionalidade teria de ser cuidadosamente estudada para o caso Português.
   - Os cuidados depositados na gestão dos tokens que funcionam como autorizações de voto, fornecem garantias concretas contra riscos de votação dupla, ou de eleitores não autorizados.
   - Note-se que o facto de os token utilizados serem desenvolvidos para utilização exclusiva neste tipo de sistema, reduz significativamente o risco de ataques.

- A não divulgação de resultados antes do tempo é assegurada pela utilização de temporização interna, e por uma configuração adequada do sistema na altura da inicialização.
- A utilização de hardware e software específicos, nomeadamente a utilização de memórias estáticas, com redundância e mecanismos de controlo de erros apurados, são o pontos forte deste sistema.
- Uma avaliação das garantias fornecidas relativamente à não manipulação de resultados dentro das cabines apenas seria possível através de um processo de creditação do código fonte.

2.3 Sistema Multicert

Dos três sistemas avaliados, este é o único que inclui uma componente de gestão dos cadernos eleitorais. Esta componente foi desenvolvida especificamente para este acto eleitoral, de acordo com uma especificação funcional fornecida pela UMIC, e que se ajusta à realidade do sistema eleitoral Português. Pelo facto de incluir este tipo de funcionalidade, este sistema está mais próximo do que seria necessário para possibilitar a mobilidade dos votantes. Por outro lado, os cuidados de segurança necessários para cumprir os requisitos para um sistema de votação são muito mais complexos, e introduzem um peso computacional adicional não negligenciável.

A implementação revelou, no entanto, estar ainda numa fase de estabilização, tendo sido registados diversos problemas, nomeadamente:

- Demora na inicialização e votação, essencialmente devido a problemas com os smartcards.
- Impossibilidade de obter alguns resultados devido a uma deficiente configuração das cabines de voto.

A justificação fornecida para estes problemas foi o pouco tempo disponível e a escassez de recursos para o desenvolvimento do sistema, nomeadamente para a fase de testes. Tendo em conta que o sistema foi desenvolvido de raiz, e os moldes em que esta experiência foi levada a cabo, esta justificação parece razoável.

A documentação fornecida pela Multicert no contexto desta auditoria revelou-se suficiente e ajustada ao que foi solicitado.

2.3.1 Recursos necessários (estimativa de custo)

1. Recursos Materiais
   - É necessário um conjunto de cabines (PCs com touch screen e leitor de smartcards) adequado ao número de votantes da assembleia de voto, um número razoável de smartcards (que evitar tempos de espera para os votantes), e um PC com dois monitores e um leitor de smartcards para a aplicação da mesa.
   - A propriedade do equipamento (Estado, Multicert ou terceiros) é deixada em aberto, existindo apenas restrições de compatibilidade.

- O custo estimado é de 1260? por mesa, e de 2900? por cabine.

2. Recursos Humanos

   - Na experiência realizada, a Multicert destacou um elemento técnico no local, sendo o custo estimado de 75?/hora.
   - Não foi fornecida uma estimativa do que seria uma equipa de suporte razoável, e dos custos associados, no caso de uma eleição a nível nacional.

3. Infraestruturas

   - Apenas são necessárias ligações de alimentação correntes, e uma linha telefónica para ligação das cabines ao servidor central no final da votação.

2.3.2 Requisitos funcionais (adequação do sistema à estrutura clássica da Assembleia de Voto)

1. Inicialização

   - O sistema foi implementado e documentado com o objectivo de serem os elementos da mesa a efectuarem a inicialização mas, na prática, isso foi feito por pessoal técnico.
   - O processo de inicialização é relativamente simples, mas foram registados alguns problemas de ordem técnica que introduziram atrasos significativos nesta fase.
   - O funcionamento do sistema incorpora muitos elementos do funcionamento de uma mesa de voto tradicional, nomeadamente pelo facto de contemplar papéis diferentes para Presidente e escrutinadores, o que é uma grande vantagem no caso de se pretender evoluir neste sentido.
   - A impressão de um relatório no instante da abertura das cabines é um elemento importante para assegurar que os elementos da mesa são capazes de assegurar que a inicialização decorreu correctamente.

2. Votação

   - O processo é simples: um eleitor identificado recebe um smartcard que lhe permite aceder à cabine, no final da votação esse smartcard é devolvido à mesa para ser formatado.
   - O facto de a gestão dos eleitores que estão a exercer o seu direito de voto em cada instante ser feita de forma automática, bem como a possibilidade de detectar anomalias no conteúdo dos tokens assim que o votante os devolve, são uma mais valia no que diz respeito ao controlo do desenrolar do processo por parte dos elementos da mesa.
   - Uma evolução para este sistema não traria problemas para o caso Português.

3. Contagem

   - O sistema foi implementado e documentado com o objectivo de serem os elementos da mesa a efectuarem a inicialização mas, na prática, isso foi feito por pessoal técnico.
   - O processo de encerramento e impressão do relatório final é relativamente simples, mas foram registados alguns problemas de ordem técnica que introduziram falhas significativas nesta fase.

- Os cuidados de segurança colocados no armazenamento e transferência dos boletins de voto durante a votação tornam a abertura dos votos um processo relativamente demorado.

4. Exportação dos resultados

   - A funcionalidade de transferência dos resultados para um servidor central por ligação dial-up, utilizando canais seguros e autenticação criptográfica, é apropriada.
   - A possibilidade de gravar os resultados, com autenticação criptográfica, num CD-ROM pode ser um elemento muito positivo para a auditabilidade do sistema.
   - Não parece viável deixar estes procedimentos a cargo dos elementos da mesa, a não ser com um esforço considerável de formação.
   - É, no entanto, razoável assumir que os elementos da mesa serão capazes de controlar o correcto desenrolar dos procedimentos.

2.3.3 Requisitos de segurança

1. Ligação ao exterior (transferência de dados para o exterior quer por ligações de rede, quer por suportes digitais)

   - Os cadernos eleitorais são recebidos em CD-ROM, sendo a sua integridade e autenticidade asseguradas por meios não electrónicos.
   - Os resultados eleitorais são impressos em papel, sendo esse documento incluído nas actas da mesa de voto. Este documento serve como garante último da integridade dos resultados exportados em formato electrónico.
   - Os resultados podem ser exportados via CD-ROM ou via ligação dial-up. A integridade e autenticidade dos ficheiros é assegurada utilizando assinaturas digitais e certificados digitais.
   - No caso de eleições a nível nacional, a utilização de certificados digitais e a implantação de uma PKI de suporte seria um dos pontos fundamentais para permitir a implementação de mecanismos que possibilitem a mobilidade dos votantes com um nível adequado de segurança.

2. Identificação do eleitor

   - Presencial.

3. Caderno Eleitoral (gestão das listas de eleitores)

   - A autorização de voto consiste num ficheiro, assinado digitalmente pela mesa de voto, armazenado dentro do smartcard. Este ficheiro não contém informação relativa ao votante.
   - A aplicação de gestão das listas eleitorais garante que apenas uma autorização de voto é emitida para cada eleitor.
   - As garantias de isolamento entre o sistema de gestão dos cadernos eleitorais e o sistema de armazenamento dos votos, implementadas no sistema, teriam de ser auditadas por análise do código fonte.
   - A utilização de hardware e software desenvolvidos por terceiros é um factor de risco, nomeadamente no que diz respeito ao sistema operativo. No entanto, o ambiente controlado em que o equipamento é utilizado deverá ser suficiente para eliminar esses riscos.

4. Cabine de voto

    - A privacidade física do votante é satisfatória.
    - Não há riscos de perda do anonimato, uma vez que as cabines não recebem nem armazenam qualquer informação relativa aos votos ou aos votantes.
    - Os cuidados depositados na gestão das autorizações de voto, fornecem garantias concretas contra riscos de votação dupla, ou de eleitores não autorizados.
    - Os boletins gerados são cifrados duplamente, e assinados digitalmente. Uma cifragem exterior assegura a confidencialidade dos resultados até ao final da votação. O restante processamento assegura a integridade e confidencialidade dos boletins de voto quando são transferidos entre as cabines e a mesa.
    - Uma avaliação das garantias fornecidas relativamente à não manipulação de boletins dentro das cabines apenas seria possível através de um processo de acreditação do código fonte.
    - Note-se que o facto de o token utilizado ser um smartcard, com formato estandardizado e muito disseminado, há riscos de um votante mal intencionado inserir numa cabine um cartão diferente daquele que lhe é fornecido da mesa. As possíveis consequências deste tipo de ataque não podem ser avaliadas com a informação disponível.
    - A utilização de hardware e software desenvolvidos por terceiros é um factor de risco, nomeadamente no que diz respeito ao sistema operativo. No entanto, o ambiente controlado em que o equipamento é utilizado deverá ser suficiente para eliminar esses riscos.

5. Urna (armazenamento de boletins durante a votação)

    - A autenticidade dos boletins é assegurada através de assinaturas digitais.
    - Não há riscos de perda do anonimato, a não ser em cenários improváveis de inspecção das BDs internas e extracção da sequência de votação. Mesmo este tipo de análise implicaria o conhecimento das chaves criptográficas que protegem os boletins enquanto estão armazenados na base de dados, o que aumenta o grau de complexidade do ataque.
    - Uma avaliação das garantias fornecidas relativamente à não manipulação de resultados dentro do sistema apenas seria possível através de um processo de acreditação do código fonte.
    - A utilização de hardware e software desenvolvidos por terceiros é um factor de risco, nomeadamente no que diz respeito ao sistema operativo. No entanto, o ambiente controlado em que o equipamento é utilizado deverá ser suficiente para eliminar esses riscos.

Capítulo 3

Relatórios das visitas efectuadas

3.1 Freguesia de Santa Maria de Belém (Lisboa)

Solução Indra

A visita decorreu durante a tarde, desde a 15 horas, até ao encerramento da mesa. Durante toda a tarde a adesão dos eleitores aparentava ser muito boa, e o processo de votação decorria sem problemas. Havia no entanto alguma confusão devido às condições em que estavam instaladas as mesas de voto electrónico, numa zona de passagem. Este enquadramento, bem como a constituição das mesas de voto (constituídas na sua totalidade por jovens com idades muito próximas dos 20 anos) e o grande número de elementos da organização presentes, tornou difícil a avaliação de como decorreria a votação numa situação real.

A equipa que acompanhava os eleitores era constituída por elementos da UMIC e da Indra. As pessoas inquiridas foram Sara Piteira (UMIC) e Luisa Graça (Indra). Nenhuma das pessoas presentes conhecia o funcionamento do sistema de votação electrónica em detalhe, pelo que a visita serviu apenas para observação do modo comum de utilização e inspecção exterior do equipamento.

Informação recolhida sobre o sistema utilizado:

- O sistema abrange apenas o processo de recolha de votos e é completamente independente do processo de gestão dos cadernos eleitorais, que poderia ser feito de qualquer forma, inclusivamente de forma manual.
- O sistema é constituído por equipamento desenhado especificamente para este tipo de aplicação, sendo propriedade da empresa.
- O sistema era composto 14 cabines de voto, e uma provisão de smartcards utilizados de forma descartável, num regime de um cartão por votante.
- A instalação parece ser bastante simples, sendo o design do sistema optimizado para a rapidez de instalação. As cabines necessitam apenas da ligação de um cabo de alimentação.

- Cada cabine apresenta como interface um touch-screen, sendo a privacidade do votante protegida através do posicionamento da própria cabine num ambiente em que não seja possível a observação por parte de outras pessoas.
- A inicialização do sistema foi levada a cabo pelos técnicos da Indra, que instalaram todas as cabines e as inicializaram em modo de administração. A abertura de cada cabine é assinalada através da impressão de um documento que comprova a inexistência de votos, documento esse que é fornecido à mesa de voto.
- O modo de administração é activado através de um conjunto de passwords, e da apresentação de um smartcard próprio.
- Durante o processo de votação, cada eleitor identificado pela mesa e autorizado a votar, recebe um smartcard que lhe permite aceder a uma qualquer cabine disponível, e depositar apenas um voto. Uma vez registado o voto, o smartcard é descartado. Aparentemente é possível um outro modo de funcionamento em que os smartcards são reutilizados, sendo necessário para esse efeito equipamento adicional.
- A votação é feita utilizando o touch-screen para navegar através de um GUI aparentemente fácil de utilizar. A usabilidade do sistema tornou-se difícil de avaliar, uma vez que praticamente todos os eleitores que o experimentaram foram auxiliados por elementos da organização.
- Os votos ficam armazenados na cabine onde são depositados. As cabines incluem baterias que permitem suportar falhas de energia temporárias.
- A contagem é efectuada no momento em que se encerra a votação. Os técnicos da Indra acedem às cabines em modo de administração e encerram a votação. Cada cabine imprime os totais dos votos que recolheu. Através da ligação de um cabo telefónico, cada cabine é também capaz de enviar os dados da votação para um servidor remoto através de uma ligação dial-up.

3.2 Freguesia de Monte Belo (Setubal)

Solução Unisys

O número de votantes até à altura da visita, ao fim da manhã, era superior a 500. A adesão dos eleitores aparentava ser muito boa, e o processo de votação decorria sem problemas.

A equipa que acompanhava os eleitores era constituída por elementos da UMIC e da Unisys. As pessoas inquiridas foram Nuno Santos (UMIC) e Rui Martinho (Unisys). Nenhuma das pessoas presentes conhecia o funcionamento do sistema de votação electrónica em detalhe, pelo que a visita serviu apenas para observação do modo comum de utilização e inspecção exterior do equipamento.

Estava presente também uma equipa de auditores da FEUP, que presenciou a abertura da mesa de voto. Esta equipa anotou algumas dificuldades no arranque da aplicação de gestão dos cadernos eleitorais.

Informação recolhida sobre o sistema utilizado:

- O sistema abrange apenas o processo de recolha de votos e é completamente independente do processo de gestão dos cadernos eleitorais, que poderia ser feito de qualquer forma, inclusivamente de forma manual.
- O sistema é constituído por equipamento desenhado especificamente para este tipo de aplicação, sendo propriedade da empresa.
- O sistema era composto por uma estação de controlo, 8 cabines de voto, e um conjunto 8 tokens de formato proprietário que funcionam como autorização de acesso às cabines de voto, e um token especial, com o mesmo formato, que permite o acesso ao sistema para operações de administração.
- A instalação parece ser bastante simples, sendo o design do sistema optimizado para a rapidez de instalação. As cabines necessitam apenas da ligação de um cabo de alimentação.
- Cada cabine apresenta como interface um touch-screen posicionado horizontalmente, sendo a privacidade do votante protegida por um conjunto de painéis plásticos opacos posicionados à volta do écran.
- A inicialização do sistema foi levada a cabo pelo responsável da Unisys, utilizando o token de administração, priimeiro para o arranque da base-station, e depois para a activação de todas as cabines.
- Durante o processo de votação, cada eleitor identificado pela mesa e autorizado a votar, recebe um token que lhe permite aceder a uma qualquer cabine disponível, e depositar apenas um voto. Uma vez registado o voto, o token é devolvido à mesa, que o reformata para ser reutilizado.
- A votação é feita utilizando o touch-screen para navegar através de um GUI aparentemente fácil de utilizar. A usabilidade do sistema tornou-se difícil de avaliar, uma vez que praticamente todos os eleitores que o experimentaram foram auxiliados por elementos da organização. Um aspecto menos positivo da interface é o facto de o voto em branco ser indicado pela selecção do botão "Seguinte", sem assinalar nenhuma opção de voto.
- Os votos ficam armazenados na cabine onde são depositados, aparentemente com redundância no armazenamento, utilizando memórias estáticas. As cabines incluem baterias que permitem suportar falhas de energia temporárias.
- A contagem consiste é efectuada no momento em que se encerra a votação: o token de administração é utilizado para encerrar cada cabine, recolhendo os resultados parciais. Os resultados totais são obtidos na estação central, que permite imprimir os resultados, ou transferi-los por dial-up para um servidor remoto. Este procedimento é levado a cabo por técnicos.
- Auscultados os membros da mesa de voto, estes revelaram-se contentes com o sistema, achando-o melhor que o tradicional. No entanto, manifestaram também algumas reservas quanto à sua capacidade de garantir que os resultados apurados não foram de alguma forma manipulados.

3.3 Freguesia de Mirandela (Bragança)

Solução Multicert

A visita iniciou-se cerca das 12 horas e para o levantamento da informação aqui descrita foram entrevistados o representante da UMIC, do STAPE, da empresa Multicert, o presidente da mesa de voto electrónico e alguns dos seus colaboradores.

Na altura da entrevista registavam-se 711 votantes dos quais 213 tinham participado no processo de votação electrónica. Como observação imediata nota-se uma fila bastante extensa de votantes a aguardar o voto electrónico, indicativa da lentidão do processo, o que contrastava com a rapidez e ausência de filas nas mesas de voto tradicionais.

3.3.1 Instalação

O equipamento usado era do tipo genérico (computadores pessoais) com dois postos de voto activos em cabines de voto, um posto na mesa de voto e um posto sobressselente. O tempo de instalação foi aproximadamente 4 horas e requereu a presença de técnicos da empresa; o nível técnico exigido para a instalação foi avaliado pelos entrevistados como "médio".

Para apoio aos votantes a mesa contava com três elementos e existia um elemento adicional para apoio aos votantes em cada cabine de voto.

3.3.2 Inicialização

A inicialização do sistema de voto é da responsabilidade da mesa de voto mas não existia qualquer documentação de apoio acessível aos elementos da mesa. Fomos informados que tinha sido produzida documentação e entregue à UMIC mas essa informação não estava disponível na mesa de voto.

3.3.3 Funcionamento

Uma análise mais pormenorizada do funcionamento da solução Multicert é apresentado na secção 2.3.

Sob os vários sub-processos é de referir:

Caderno Eleitoral

O uso da aplicação de gestão do caderno eleitoral (CE) revelou-se demorado; não se detectaram mecanismos de controle da aplicação por parte dos membros da mesa e, genericamente, o processo era lento quando comparado com o processo manual. A ausência de apoio documental (e.g. baixas no caderno eleitoral actualizadas nas listagens) foi considerado importante.

Autorização de Voto

A passagem da autorização de voto (AV), produzida na mesa de voto, e a cabine de votos era efectuada por "smart-cards"; estavam disponíveis um número reduzido

destes cartões que eram sistematicamente usados pelos diferentes votantes. Os cartões usados dispunham de capacidade criptográfica local e a informação da AV era assinada digitalmente e acompanhada pelo certificado de chave pública da mesa.

Garantias de segurança específicas dadas aos votantes e/ou aos membros da mesa quanto à ligação entre a gestão do CE e a criação da AV (uma AV deve corresponder a uma baixa no CE; uma AV só permite a realização de um voto) não são implementadas.

Garantias de segurança específicas da AV são satisfatórias quanto ao anonimato da AV, à capacidade de anular uma AV e à exigência de uma AV para produzir um voto válido; porém não é possível garantir que uma dada AV origina eventualmente um voto.

Eventualmente todos os requisitos de segurança assentam na confiança dos vários agentes em relação à funcionalidade da aplicação.

Cabine de Voto

Os votantes dispunham de bastante informação e apoio directo no acto de votação; no entanto, talvez devido a esse apoio, a privacidade de voto foi quase inexistente; num regime normal de funcionamento isto será alterado, com certeza. A aplicação "cabine de voto" (CV) era simples de utilizar. O voto é armazenado no mesmo cartão onde consta a AV e não existe provimento para armazenamento redundante.

Urna e Contagem

O voto é depositado (via "smart-card") e contado na mesa não ficando qualquer registo centralizado do mesmo. A informação específica de cada voto não é enviada pela mesa e qualquer outro sistema; a mesa limita-se a comunicar informação agregada e anónima.

Uma vez mais as garantias de segurança assentam na confiança sobre a funcionalidade da aplicação e não existem garantias especificamente fornecidas aos votantes sobre:

- o anonimato do voto; o facto de o voto vir no mesmo suporte onde foi gerada a AV e ser contado no mesmo local onde a AV foi gerada, não impede (em princípio) uma ligação entre estes dois actos,
- a correcção da contagem; o votante não pode verificar se o seu voto foi contado e se foi contado correctamente; o papel dos delegados no sistema actual não tem aqui equivalente.

Cenários de falha

Em termos de "sustentabilidade" do sistema em caso de situações anómalas verificou-se que:

- Existe uma UPS para suporte da mesa e cabines de voto em caso de falha de corrente eléctrica.

- Não existe qualquer documentação que descreva procedimentos em situações anómalas.
- Não existem cenários de recuperação no caso de avarias na mesa de voto (questão da coerência do CE), na cabine de votos (coerência nos votos realizados) ou na comunicação entre ambos (coerência das autorizações de votos e votos armazenados).

3.3.4 Opinião dos votantes/representantes na mesa

Uma oscultação rápida de opiniões pelos elementos presentes permitiu concluir que, na opininião dos membros da mesa, a informação fornecida era pouca mas que o processo de votação era simples e tão fácil de usar como o tradicional.

Quanto às questões de segurança foi referido que os votantes eram sensíveis ao anonimato e privacidade do voto.

Os votantes contactados não receavam eventuais fraudes mas não gosram do comprimento da fila e das demoras no voto.