



# A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament

The 2<sup>nd</sup> International Workshop on Electronic Voting  
Castle Hofen ► Bregenz ► Austria ► 2006.08.02-04

*JF Cunha\**, *MJ Leitão*, *JP Faria*, *MP Monteiro*, *MA Carravilla*

\* [jfcunha@fe.up.pt](mailto:jfcunha@fe.up.pt) ► +351-91-254 1104

Faculdade de Engenharia da Universidade do Porto





# Contents

## 1. Introduction

- Context
- The voting experiments

## 2. The Auditing Methodology

- Team composition
- Phases of the process
- The evaluation criteria and sub-criteria

## 3. The e-Voting Systems and Processes

- INDRA - Local Voting
- UNISYS/ESS - Local Voting
- MULTICERT - Local Voting with Mobility
- NOVABASE - Internet

## 4. Conclusions

# 1.

# Introduction

# Objectives

- Auditing criteria
  - Security
  - Transparency
  - Usability
  - Accessibility
- Compare several e-Voting systems.
- Independent Evaluation
- Provide information and guidelines, from the technical point of view, to the political actions about electronic ways of participation in the national decision processes in particular at elections.

# E-Voting Experiences

- Local Voting
  - Conceição - **Covilhã** (INDRA)
  - Santa Iria de Azóia - **Loures** (MULTICERT)
  - Coração de Jesus - **Lisboa** (INDRA)
  - Santos-o-Velho - **Lisboa** (UNISYS/ESS)
  - S. Sebastião da Pedreira - **Lisboa** (UNISYS/ESS)
- Internet Voting
  - Europe and other Continentes (NOVABASE)

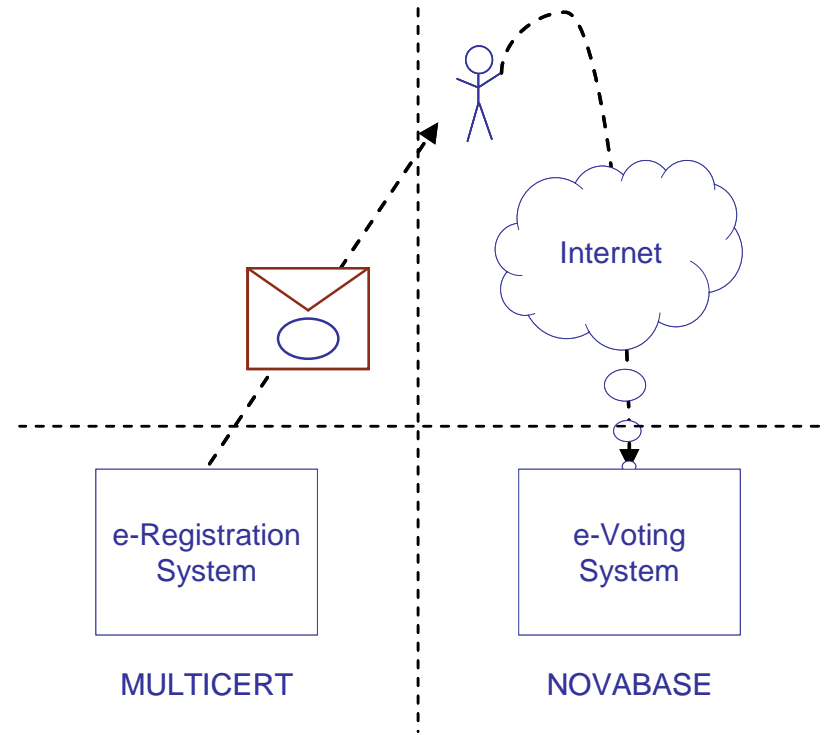
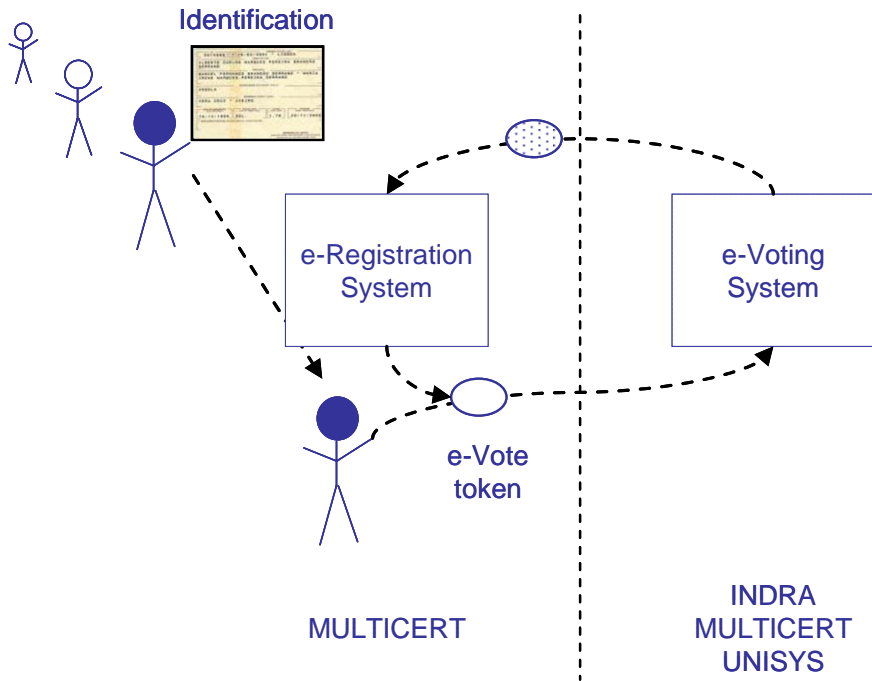
# Some numbers

- From a total of 26 515 electors who cast a valid paper vote, 8 824 also voted electronically (33%).
- From a total of 148 159 electors outside Portugal who were registered to vote by mail, 36 391 voted by mail (25%) and 4 367 voted through the Internet (12% of mailed votes).
- After voting, each citizen was personally interviewed by an independent organization in order to collect an opinion about the experience.
- In the Internet case, the voter could fill in a questionnaire for the same purpose.

# User Evaluation

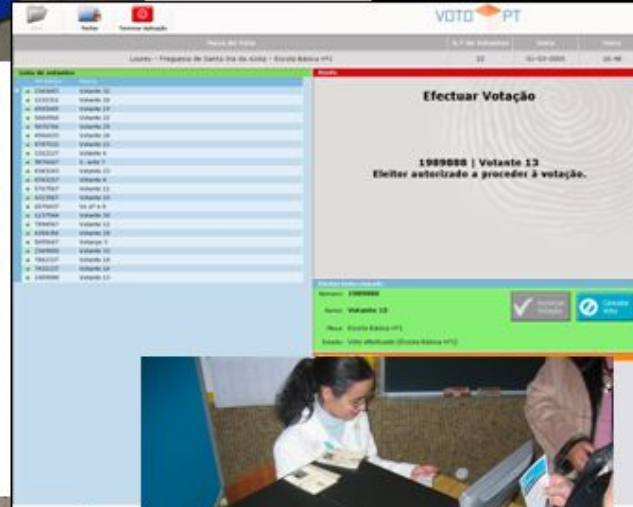
- According to the exit interviews:
  - 99.2% of the citizens that voted electronically enjoyed the experience
  - 98.1% said they would vote electronically in future elections
  - 80.5% trust the security of the EVS
  - 84.5% of the voters that had a paper trail option in the EVS used, consider important that the vote had been printed in paper and automatically inserted into a box
  - 86.3% consider that if such systems allow people to vote from other places then more people would vote
- For people voting through the Internet:
  - 99.2% enjoyed the experience
  - 98.3% said they would vote in this way in future elections
  - 57.8% trust the security of the EVS
  - 7.9% think it is not secure
  - 34.3% do not know or do not answer the question
  - 1.7% thought it is totally secure against attacks from hackers, while 54.3% do not know or do not answer

# Set-up for the experiments



LVP - Local Voting Process

IVP - Internet Voting Process



# 2.

## The Auditing Methodology

# Phases and Tasks

- Phases: Before, During and after the Election Day
- Before Election Day
  - Elaboração de pedidos de esclarecimento a enviar às empresas fornecedoras.
- Election Day
  - Presença nos locais de voto no dia das eleições, analisando:
    - Abertura das mesas de voto electrónicas
    - Processo de votação electrónica
    - Fecho das mesas de voto electrónicas
    - Contagem / Comunicação / Contagem de votos na UMIC.
- After Election Day
  - Realização de reuniões com as empresas fornecedoras.
  - Redacção dos Relatórios de Auditoria.
  - Apresentação e discussão dos resultados intercalares e das sugestões com a UMIC e outros especialistas nacionais ou internacionais.
  - Redacção do Relatório Final de Auditoria.

# Methodology

- Criteria:
  - **Security** (15 factors or sub-criteria)
  - **Transparency** (14)
  - **Usability** (5)
  - **Accessibility** (6)
- Define an index of viability for each technology:
  - Comparative relevance of sub-criteria - using Analytical Hierarchy Process (AHP)
  - Rate alternative systems (and rank if possible).

# Pairwise comparison of the sub-criteria of Accessibility using AHP

Accessibility	A1 Convenience	A2 Right to vote	A3 Documentation for the elector	A4 Flexibility	A5 Mobility
A1 Convenience	1	1/7	6	9	1/6
A2 Right to vote	7	1	9	9	8
A3 Documentation for the elector	1/6	1/9	1	1/6	1/8
A4 Flexibility	1/9	1/9	6	1	1/7
A5 Mobility	6	1/8	8	7	1

# Criteria and sub-criteria

SECURITY (S)		100,0%
S1	Audit-ability	10,3%
S2	Operator authentication	4,4%
S3	Certify-ability	9,0%
S4	Reliability	9,8%
S5	Detect-ability	4,6%
S6	Availability of system	5,4%
S7	Immunity to attack	8,1%
S8	Integrity of votes	14,4%
S9	Invulnerability	9,3%
S10	Traceability	3,8%
S11	Recoverability	5,3%
S12	Fault tolerance	4,6%
S13	Isolation	2,6%
S14	Security of communications	8,3%

USABILITY (U)		100,0%
U1	Easiness of use	38,4%
U2	Speed of use	10,1%
U3	Clarity of language in interface	23,4%
U4	Localisation of interface	11,1%
U5	Emotional satisfaction	17,0%

TRANSPARENCY (T)		100,0%
T1	Anonymity	11,3%
T2	Atomicity	7,0%
T3	Authenticity	11,5%
T4	Trust	6,2%
T5	Technical documentation	2,2%
T6	Integrity of personal	2,8%
T7	Integrity of system	6,0%
T8	Non-coercion-ability	10,5%
T9	Precision of system	7,6%
T10	Privacy	7,6%
T11	Singularity (non reuse)	10,7%
T12	Transparency of process	3,5%
T13	Transparency of system	3,9%
T14	Verifiability	6,5%
T15	Separation of roles	2,9%

ACCESSIBILITY (A)		100,0%
A1	Convenience	14,4%
A2	Right to vote	47,0%
A3	Documentation for the elector	7,6%
A4	Flexibility	11,9%
A5	Mobility	19,1%

# Summary Rating (Evaluation) of Systems

	UNISYS	INDRA	MULTICERT	NOVABASE
Security	4,2	4,1	2,6	3,6
Transparency	4,2	4,3	3,2	3,0
Usability	4,2	3,9	2,7	3,8
Accessibility	3,7	3,3	3,5	3,6

# 3.

## The e-Voting Systems and Associated Processes

# INDRA - Local Voting



# INDRA's Point&Vote

- The system consists of special purpose equipment based on a standard PC platform equipped with a touch screen with side view protection, a smart card reader and an internal printer for reports
- Two alternative versions were available, one with headphones and mouse for physically impaired voters, and another with a printer, where votes could be seen for a few seconds by the voter, but could not be removed from the collecting basket.
- In order to vote, each citizen receives a smartcard. This token is required to enable the use of the actual voting machine where votes are cast (and counted at the end of the ED). After being used the smartcard is returned to the e-registration and is not used again at the current election.
- At the end of the voting period, each machine is closed with the operator (supervisor) smartcard and password. Results from each machine can be locally printed and transmitted over the internal modem via a secure communications link to a computer of the Central Election Authority.

# UNISYS/ESS - Local Voting



# UNISYS/ESS's iVotronic

- The system can be generally characterised as a touch screen voting unit, portable and configurable (height and orientation), with good privacy protection. These features, plus an optional audio interface, allow good support to visually impaired and wheelchair locomoting voters.
- The PEB (Personal Electronic Ballot) is the token that gives access to vote. It's a sealed unit communicating (within a very short range) through an infrared technology and protocol that was designed to prevent communication with standard IrDA transceivers. After each use the PEB must be regenerated.
- Some special operations can be performed using a different supervisor PEB requiring explicit password validation. During the voting session results are accumulated internally and redundantly recorded. All operations, including the supervisor actions, are also timed and logged.
- At the end of the session the voting units must be closed and its accumulated results transferred and added to the supervisor PEB memory, allowing several units to be combined in a single one. This PEB is then read in another machine. This machine can now print the results (totals and partials) and transmit them to a computer of the Central Election Authority using a modem and a phone line.

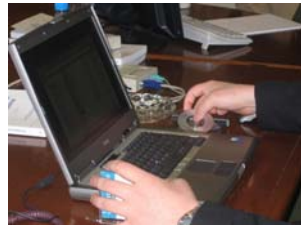
# MULTICERT - Local Voting with Mobility



# MULTICERT's EBBS

- Differently from the previous systems, the MULTICERT voting system allowed citizens to vote electronically in a place different from their traditional one, within the same borough. This was achieved by a distributed e-registration system, based on a central database remotely accessed by client applications located in each place.
- Another distinguishing feature of this system was the existence of an electronic ballot box system (EBBS) that actually stored the electronic ballots, separated from the electronic voting units where the electronic ballots were filled in. Small i-button devices were used to carry authorizations (similar to empty ballots) from the EBBS to the electronic voting units, and carry back filled in ballots to the EBBS.
- Besides a touch screen, each electronic voting unit had a small printer to print and store paper ballots corresponding to the electronic ballots, with the purpose of enabling non-electronic ballot recounting and improving the confidence on the process.
- Special operations could be done in the EBBS using supervisor i-buttons.

# NOVABASE - Internet



# NOVABASE - Internet

- The Internet voting system was aimed at all the citizens registered to vote outside of Portugal using postal vote. Two separate mailings were sent to voters abroad: one containing the valid ballots and another one with the information and keys to allow the vote using the Internet system.
  1. The system generates individual credentials, a unique code of a username and a password.
  2. Voter Information is registered together with the credential in the Active Directory.
  3. Credentials are posted. The message does not include the elector number.
  4. Pairs of encryption keys are generated. The public key is send to Novabase to be stored in the Database. The private key is divided into 7 parts, one for each political party represented.
  5. The vote process is open, allowing browsers to access the server.
  6. The elector receives the credentials. He/She can use any computer with a browser, able to accept some JavaScript and cookies, to access [www.votoelectronico.pt](http://www.votoelectronico.pt). He/She has to introduce the elector number and the credential.
  7. The confirmed vote is registered in a database table, using two key encryption. The public key is used to encrypt. During the same transaction it is stored that the citizen has voted in the credentials table and in the Active Directory.
  8. At closure of the election the information in the Active Directory is printed and sent to CNE. The Active Directory is erased. A copy of the database is stored and sealed in a CD with a MD5 seal.

# 4.

## Conclusions

# Evaluation of e-voting systems: rating

		Unisys	Indra	Multicert	Novabase	
<b>SECURITY (S)</b>		100,0%	4,22	4,14	2,57	3,63
S1	Audit-ability	10,3%	x	x	x	x
S2	Operator authentication	4,4%		x	x	x
S3	Certify-ability	9,0%	x	x	x	x
S4	Reliability	9,8%	x	x	x	x
S5	Detect-ability	4,6%		x	x	x
S6	Availability of system	5,4%		x	x	x
S7	Immunity to attack	8,1%	x	x	x	x
S8	Integrity of votes	14,4%	x	x	x	x
S9	Invulnerability	9,3%	x	x	x	x
S10	Traceability	3,8%	x	x	x	x
S11	Recoverability	5,3%		x	x	x
S12	Fault tolerance	4,6%	x	x	x	x
S13	Isolation	2,6%		x	x	x
S14	Security of communications	8,3%	x	x	x	x
<b>TRANSPARENCY (T)</b>		100,0%	4,22	4,32	3,15	3,03
T1	Anonymity	11,3%		x	x	x
T2	Atomicity	7,0%	x		x	x
T3	Authenticity	11,5%		x	x	x
T4	Trust	6,2%		x	x	x
T5	Technical documentation	2,2%	x	x	x	x
T6	Integrity of personal	2,8%	x	x	x	x
T7	Integrity of system	6,0%	x	x	x	x
T8	Non-coercion-ability	10,5%		x	x	x
T9	Precision of system	7,6%		x	x	x
T10	Privacy	7,6%		x	x	x
T11	Singularity (non reuse)	10,7%	x	x	x	x
T12	Transparency of process	3,5%	x	x	x	x
T13	Transparency of system	3,9%	x	x	x	x
T14	Verifiability	6,5%	x	x	x	x
T15	Separation of roles	2,9%	x	x	x	x
<b>USABILITY (U)</b>		100,0%	4,23	3,89	2,68	3,76
U1	Easiness of use	38,4%	x	x	x	x
U2	Speed of use	10,1%	x	x	x	x
U3	Clarity of language in interface	23,4%		x	x	x
U4	Localisation of interface	11,1%	x	x	x	x
U5	Emotional satisfaction	17,0%	x	x	x	x
<b>ACCESSIBILITY (A)</b>		100,0%	3,69	3,35	3,50	3,63
A1	Convenience	14,4%		x	x	x
A2	Right to vote	47,0%	x	x	x	x
A3	Documentation for the elector	7,6%	x	x	x	x
A4	Flexibility	11,9%	x	x	x	x
A5	Mobility	19,1%	x	x	x	x

# How many votes?

- $N_v$  is the number of total electronic votes (as counted by the EVS)
- $C_v$  is the total number of citizens that were given tokens to vote (as counted by the e-Registration system)
- The three situations below occurred. This could be a problem of the EVS, of the procedures people used, or both:
  - $N_v > C_v$ . At least one citizen voted twice. It could have happened that one citizen was given more than one chance to vote (e.g.; claimed token was faulty).
  - $N_v < C_v$ . At least one citizen did not vote. It could have happened that one citizen actually did not vote at the EVS (not a problem, if voluntary).
  - $N_v = C_v$ . All was fine, or pairs of the above happened at the same EVS.
- Do traditional system suffer from this problem?
- What can be done to improve this?

# Conclusions

- Non-valid experiments are required and relevant for several reasons:
  - Public awareness
  - Training of officials
  - Training of Auditors
  - ...
- Valid e-voting involves risks of security as well as does traditional voting.
- Independent auditing is essential for widespread trust by electors.



# Acknowledgments

- Auditing team: Gabriel David, J. Correia Lopes, A. Carvalho Brito, J. Magalhães Cruz, Sérgio R. Cunha, R. Moreira Vidal, Henriqueta Nóvoa, J. Vila Verde, Miguel Gonçalves, L. Miguel Silva, and J. Fernando Oliveira.
- Diogo Vasconcelos, Sara Piteira and João Vasconcelos, from UMIC.
- Fernando Silva, from CNPD.
- Officials from CNE and STAPE
- Representatives of enterprises involved in the experiments.

# Thank you!

- ... Questions?