A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

NUI Maynooth

1st August 2006

mmcgaley@cs.nuim.ie
Structure

- Introduction
A Critical Analysis of the Council of Europe Recommendations on e-voting

Introduction

What is the Council of Europe?
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction

- What is the Council of Europe?
- E-voting in Europe

Structure

- Introduction
- Standards
- Examples
- Conclusion
Structure

- Introduction
  - What is the Council of Europe?
  - E-voting in Europe
  - Europe and the US - contrasting approaches
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction
- What is the Council of Europe?
- E-voting in Europe
- Europe and the US - contrasting approaches

The standards
Introduction
- What is the Council of Europe?
- E-voting in Europe
- Europe and the US - contrasting approaches

The standards
- Software engineering analysis
Structure

- Introduction
  - What is the Council of Europe?
  - E-voting in Europe
  - Europe and the US - contrasting approaches

- The standards
  - Software engineering analysis
  - Proposal
Introduction

- What is the Council of Europe?
- E-voting in Europe
- Europe and the US - contrasting approaches

The standards

- Software engineering analysis
- Proposal

Examples
Structure

- Introduction
  - What is the Council of Europe?
  - E-voting in Europe
  - Europe and the US - contrasting approaches
- The standards
  - Software engineering analysis
  - Proposal
- Examples
- Conclusions
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction

Standards

Examples

Conclusion

(CoE)
Council of Europe

- (CoE)
- 46 member states
Council of Europe

- (CoE)
- 46 member states
- Founded 1949
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Council of Europe

- (CoE)
- 46 member states
- Founded 1949
- Not directly connected with EU

Introduction
Standards
Examples
Conclusion
(CoE)  
46 member states  
Founded 1949  
Not directly connected with EU  
Open to countries that:
Council of Europe

- (CoE)
- 46 member states
- Founded 1949
- Not directly connected with EU
- Open to countries that:
  - follow principle of rule of law
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction

Standards

Examples

Conclusion

Council of Europe

- (CoE)
- 46 member states
- Founded 1949
- Not directly connected with EU
- Open to countries that:
  - follow principle of rule of law
  - uphold fundamental human rights
Council of Europe

- (CoE)
- 46 member states
- Founded 1949
- Not directly connected with EU
- Open to countries that:
  - follow principle of rule of law
  - uphold fundamental human rights
  - provide freedom for citizens
Council of Europe

- (CoE)
- 46 member states
- Founded 1949
- Not directly connected with EU
- Open to countries that:
  - follow principle of rule of law
  - uphold fundamental human rights
  - provide freedom for citizens
- Statute - “The aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and realising the **ideals and principles** which are their **common heritage** and facilitating their economic and social progress.”
CoE recommendations

- CoE created committee to develop standards doc.
CoE recommendations

- CoE created committee to develop standards doc.
- Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting
CoE created committee to develop standards doc.
Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting
Terms of reference
CoE recommendations

- CoE created committee to develop standards doc.
- Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting
- Terms of reference
  - “develop an intergovernmentally agreed set of standards for e-enabled voting, that reflect Council of Europe member states differing circumstances, and can be expected to be followed by the ICT industry.”
Use in Europe

- Netherlands - 1982
Use in Europe

- Netherlands - 1982
- Belgium - 1991
Use in Europe

- Netherlands - 1982
- Belgium - 1991
- UK, Italy, Spain, Ireland - 2000’s
Use in Europe

- Netherlands - 1982
- Belgium - 1991
- UK, Italy, Spain, Ireland - 2000’s
- experimental, or limited scope
Use in Europe

- Netherlands - 1982
- Belgium - 1991
- UK, Italy, Spain, Ireland - 2000’s
- experimental, or limited scope
- UK, Ireland pulling back
Contrasting approaches

- US standards effort is older
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
  - US standards nominally voluntary, legally required in many states
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
- Size
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
- Size
  - US standards – 2 volumes = 22 documents = almost 300 pages
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
- Size
  - US standards – 2 volumes = 22 documents = almost 300 pages
  - CoE doc 21 pages (explanatory memorandum 67 pages)
Contrasting approaches

- US standards effort is older
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- Result – wider use
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
- Size
  - US standards – 2 volumes = 22 documents = almost 300 pages
  - CoE doc 21 pages (explanatory memorandum 67 pages)
- EAC doc. has much finer granularity
Contrasting approaches

- **US standards effort is older**
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- **Result – wider use**
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
- **Size**
  - US standards – 2 volumes = 22 documents = almost 300 pages
  - CoE doc 21 pages (explanatory memorandum 67 pages)
- **EAC doc. has much finer granularity**
  - eg CoE doc. passing reference to testing (standard 111)
Contrasting approaches

- **US standards effort is older**
  - CoE doc. is now two years old
  - First FEC standards were produced in 1990
- **Result – wider use**
  - US standards nominally voluntary, legally required in many states
  - To my knowledge only Belgium is using CoE doc
- **Size**
  - US standards – 2 volumes = 22 documents = almost 300 pages
  - CoE doc 21 pages (explanatory memorandum 67 pages)
- **EAC doc. has much finer granularity**
  - eg CoE doc. passing reference to testing (standard 111)
  - EAC standards list and elaborate on 5 categories of testing
Analysis - maximising problem domain understanding
Standards, analysis, requirements capture

- Analysis - maximising problem domain understanding
- Interaction w/customer, potential users
Standards, analysis, requirements capture

- Analysis - maximising problem domain understanding
- Interaction w/customer, potential users
- General analysis makes specific analysis easier
Standards, analysis, requirements capture

- Analysis - maximising problem domain understanding
- Interaction w/customer, potential users
- General analysis makes specific analysis easier
- Standards doc in general problem domain
  - useful in requirements capture for a specific system
Standards and the public

- Standards could increase trust
Standards and the public

- Standards could increase trust
  - Associations with CoE alone could increase trust (rightly or wrongly)
Standards and the public

- Standards could increase trust
  - Associations with CoE alone could increase trust (rightly or wrongly)
  - If written to address specific concerns ...
Standards and the public

- Standards could increase trust
  - Associations with CoE alone could increase trust (rightly or wrongly)
  - If written to address specific concerns...
  - Standards used to reject inadequate systems
Standards and government

- Govs need expert advise
Standards and government

- Govs need expert advise
- Standards are reusable expertise
Standards and government

- Govs need expert advise
- Standards are reusable expertise
- Should help procure better systems
Standards and manufacturers

- Improve quality of product
Standards and manufacturers

- Improve quality of product
- Maintain, identify customer base
Standards and manufacturers

- Improve quality of product
- Maintain, identify customer base
- Aid design decisions - by making priorities clear
Standards and manufacturers

- Improve quality of product
- Maintain, identify customer base
- Aid design decisions - by making priorities clear
- Feedback to improve standards
Original Standards Themselves

- First glance
Original Standards Themselves

- First glance
  - Clearly written by committee
Original Standards Themselves

- First glance
  - Clearly written by committee
  - Vague and ill-defined, or overly technical, or nonsensical
Soft/eng view of original standards

- Consistency
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction

Standards

Examples

Conclusion

Soft/eng view of original standards

- Consistency
- Completeness, scope
Soft/eng view of original standards

- Consistency
- Completeness, scope
- Over specification
Soft/eng view of original standards

- Consistency
- Completeness, scope
- Over specification
- Underspecification
Soft/eng view of original standards

- Consistency
- Completeness, scope
- Over specification
- Underspecification
- Redundancy, repetition
Soft/eng view of original standards

- Consistency
- Completeness, scope
- Over specification
- Underspecification
- Redundancy, repetition
- Maintainability, extensibility
Proposal: reverse engineering, restructuring

- Categorised according to five rights
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
  - any measure used to protect the votes from tampering
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
  - any measure used to protect the votes from tampering
  - any measure to ensure that the results are tabulated correctly.
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
  - any measure used to protect the votes from tampering
  - any measure to ensure that the results are tabulated correctly.
- Organising reqs like this helps
Proposal: reverse engineering, restructuring

- Categorised according to five rights
  - Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
  - any measure used to protect the votes from tampering
  - any measure to ensure that the results are tabulated correctly.
- Organising reqs like this helps
  - prevent inconsistency and redundancy
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
  - any measure used to protect the votes from tampering
  - any measure to ensure that the results are tabulated correctly.

- Organising reqs like this helps
  - prevent inconsistency and redundancy
  - maximise cover - prevent underspecification
Proposal: reverse engineering, restructuring

- Categorised according to five rights
- Universal, equal, free, secret, direct suffrage
- Original began like this, but didn’t follow it through
- Direct suffrage
  - “the ballots cast by the voters directly determine the person(s) elected”
  - any measure used to protect the votes from tampering
  - any measure to ensure that the results are tabulated correctly.
- Organising reqs like this helps
  - prevent inconsistency and redundancy
  - maximise cover - prevent underspecification
  - easier to understand and use
New structured reqs

- About 80
New structured reqs

- About 80
- Most needed rewording
New structured reqs

- About 80
- Most needed rewording
- Many covered more than one idea
  - Divided with letters (a, b, ...)
New structured reqs

- About 80
- Most needed rewording
- Many covered more than one idea
  - Divided with letters (a, b, ...)
- Many could be grouped together
New structured reqs

- About 80
- Most needed rewording
- Many covered more than one idea
  - Divided with letters (a, b, ...)
- Many could be grouped together
- 15 left out
  - Irrelevant, inadvisable, undecipherable, unjustifiable
New structured reqs

- About 80
- Most needed rewording
- Many covered more than one idea
  - Divided with letters (a, b, ...)
- Many could be grouped together
- 15 left out
  - Irrelevant, inadvisable, undecipherable, unjustifiable
- Phrase “competent electoral authorities”
19 (3d)
- There shall be a bug-tracking system.
Requirements added

- 19 (3d)
  - There shall be a bug-tracking system.

- 20 (4)
  - Security arrangements shall ensure that, for the duration of operation, each component is the version tested and approved for use.
Requirements rephrased

- (original)

- 76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the *competent electoral authorities*, who will take the necessary steps to mitigate the effects of the incident. The **level of incident** which shall be reported shall be specified in advance by the electoral authorities.
(original)

76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.

(our revision)

20 (5). Incident levels shall be defined and appropriate responses identified.
Requirements rephrased

- (original)
  - 74b. Any substantial changes to key equipment shall be notified.
Requirements rephrased

- (original)
  - 74b. Any substantial changes to key equipment shall be notified.

- (our revision)
  - 20 (6f). Any changes to key equipment shall be notified to the authorities identified in the control procedure.
Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.

Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.

Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.
25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.
25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.

31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.
(original)

- 25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is **working correctly** and that all the necessary security measures have been taken.
- 31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is **genuine and operates correctly**.
- 73. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it **complies with technical specifications**. The findings shall be submitted to the competent electoral authorities.
19 (6). The certification authority shall develop a test plan which covers testing to be carried out: before the system is introduced, at regular intervals, and triggered by specific events (for example software updates, upcoming elections) as well as the timing of such tests.
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction

Standards

Examples

Conclusion

Requirements merged

- (original)
72a. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements.
A Critical Analysis of the Council of Europe Recommendations on e-voting

Margaret McGaley and J. Paul Gibson

Introduction
Standards
Examples
Conclusion

Requirements merged

- (original)
  - 72a. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements.
  - 79a. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications.
(original)

- 72a. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements.
- 79a. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications.

(our revision)

- 20 (3). The system shall be monitored during operation for compliance with requirements.
84. The e-voting system shall maintain reliable synchronised *time sources*. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.
84. The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

19(2). Components’ access to time sources shall be strictly limited on a “need to know” basis.
Requirements contradicted

- (original)
Requirements contradicted

- (original)
  24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.
(original)

- 24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.
- 69a. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description.
Requirements contradicted

- (original)
  - 24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.
  - 69a. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description.
  - 105. Disclosure of the audit information to unauthorised persons shall be prevented.
Requirements contradicted

- (original)
  - 24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.
  - 69a. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description.
  - 105. Disclosure of the audit information to unauthorised persons shall be prevented.
  - 110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.
19(7). All components of the system and software used, and all audit information, shall be publicly disclosed. Exceptions to this rule shall only be allowed where it can be shown that such a disclosure would either: endanger the security of the system or, genuinely endanger the intellectual property of the vendor. In either of these cases, full disclosure shall be made to the certification authority for verification and certification purposes.
39. There shall be a voters register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections. (covered by other CoE documents)
39. There shall be a voters register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections. (covered by other CoE documents)

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum. (outside scope)
10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.
10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.

72b. The backup services shall be regularly supplied with monitoring protocols.
After writing, developed list of terms (in an effort to follow our own advice :))
Note

- After writing, developed list of terms (in an effort to follow our own advice :) )
- Uncovered inconsistent use of terminology in our own req.s
Note

- After writing, developed list of terms (in an effort to follow our own advice :)
- Uncovered inconsistent use of terminology in our own req.s
- Small example of the value of this kind of analysis
Conclusion

- CoE standards flawed, but have potential
Conclusion

- CoE standards flawed, but have potential
- Terms of reference
Conclusion

- CoE standards flawed, but have potential
- Terms of reference
  - “develop an intergovernmentally agreed set of standards for e-enabled voting, that reflect Council of Europe member states differing circumstances, and can be expected to be followed by the ICT industry.”
Conclusion

- CoE standards flawed, but have potential
- Terms of reference
  - “develop an intergovernmentally agreed set of standards for e-enabled voting, that reflect Council of Europe member states differing circumstances, and can be expected to be followed by the ICT industry.”
- Fails second point
Conclusion

- CoE standards flawed, but have potential
- Terms of reference
  - “develop an intergovernmentally agreed set of standards for e-enabled voting, that reflect Council of Europe member states differing circumstances, and can be expected to be followed by the ICT industry.”
- Fails second point
- Examples of inconsistency, incompleteness, over- and under-specification, redundancy and repetition
Conclusion

- CoE standards flawed, but have potential
- Terms of reference
  - “develop an intergovernmentally agreed set of standards for e-enabled voting, that reflect Council of Europe member states differing circumstances, and can be expected to be followed by the ICT industry.”
- Fails second point
- Examples of inconsistency, incompleteness, over- and under-specification, redundancy and repetition
- Potentially bad systems certified and good systems failed
Conclusion

- Computer systems, need computer experts advise
Conclusion

- Computer systems, need computer experts advise
- Recommend:
Conclusion

- Computer systems, need computer experts advise
- Recommend:
  - Take advantage of expertise
Conclusion

- Computer systems, need computer experts advise
- Recommend:
  - Take advantage of expertise
  - Develop broadly applicable doc.,
Conclusion

- Computer systems, need computer experts advise
- Recommend:
  - Take advantage of expertise
  - Develop broadly applicable doc.,
  - Useful to Governments, vendors, citizens
Questions?

- Recommendations -
  http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/

- Our full redrafted version is in the paper
  http://www.usenix.org/events/evt06/tech/full_papers/mcgaley/mcgaley_html

- Research funded by Irish Research Council for Science, Engineering and Technology (IRCSET) through the EMBARK initiative.