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

Margaret McGaley and J. Paul Gibson
Computer Science Department, NUI Maynooth, Ireland
{*mmcgaley,pgibson*}*@cs.nuim.ie*

Abstract

In September 2004, the Council of Europe's *Committee of Ministers* officially adopted a set of standards recommended by the *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting* [7].

This paper puts the standards in their historical context, examines them according to established software engineering principles, and finally suggests how they could be restructured.

1 Introduction

E-voting is an idea with a lot of potential, for good and for harm. Improving access for voters with disabilities, eliminating accidental spoiling of votes, and so on are all laudable goals. On the other hand, a flawed e-voting solution could have disastrous results if it were used in a legally binding election.

An important step in ensuring that any system behaves correctly is laying down what *behaving correctly* means for that system. In other words, we must identify the system's requirements.

The Council of Europe standards document is a step in the right direction, but the document itself is seriously flawed. This paper consists of a discussion of the flaws, and a proposal for improving the document.

1.1 Council of Europe

The Council of Europe (CoE) is an organisation of 46 member states, from in and around Europe. It is not directly connected to the European Union (EU), though all current EU member-states are members of the CoE. According to its statute, the CoE aims 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."

With respect to voting the CoE has a clear purpose in protecting democracy, the rule of law, and human rights.

1.2 The Standards

The *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting* [7] was set up by the CoE in early 2003

> "...to 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." [9]

It is their recommendations that are the subject of this paper.

The document they produced (from now on referred to as "the standards") acknowledges that it cannot be judged in isolation. It states that it should respect:

> "the obligations and commitments as undertaken within existing international instruments and documents, such as [...]"

The list of 12 instruments that follows — though it is clearly not meant to be exhaustive — covers a diverse range of documents, including the *Universal Declaration of Human Rights*, the *European Charter of Local Self-Government* and the *Convention on Cybercrime*. It also includes the *Code of Good Practice in Electoral Matters* [10], which was produced by the Venice Commission [1].

This inter-related set of complex documents is analagous to a software system which has evolved over time, in response to ever changing sets of requirements. The system depends on a large number of other systems, and the environment of the system (the context in which it is being used) is not clearly understood. With such

legacy systems, one often reaches a stage where the system's operation can only be maintained through a restructuring (re-engineering) of the system and its architecture. Many techniques exist for this task, one of which is known as reverse engineering. We propose reverse engineering of the e-voting standards, with focus on arriving at a set of documents that can be usefully applied at the requirements capture stage of e-voting development.

1.3 Further analysis of standards - motivation

To strengthen our argument that the standards should be re-engineered, we analyse whether they – as they are stated – adhere to good practice with respect to system analysis and requirements engineering. Our goal is not to say whether we agree or disagree with the standards. Our aim is to show that the way in which the standards are expressed is very poor, in the sense that it makes it almost impossible for them to achieve both their objectives, as defined by the CoE, and our objectives, as outlined in this paper. The second part of our technical work will be to analyse the possibility of re-engineering the standards in order to improve the way in which they are expressed. We demonstrate that a simple restructuring is an inexpensive first step in the reverse engineering process.

1.4 Structure of paper

In the sections that follow, we will first give an overview of e-voting from a European perspective. We argue that the standards show a lack of ambition and propose how they could play a much more ambitious role in upholding the principles of freedom and democracy across Europe. In section 4, we argue that a requirement for the standards to successfully meet this new ambition is the incorporation of software engineering good practice into the drafting of the documentation. In section 5 we demonstrate one alternative for restructuring the document based on the right that each standard is aiming to uphold. In section 6 we analyse the restructuring work done with reference to examples. In our conclusions, we make recommendations to the CoE regarding the management and maintenance of these standards, and emphasise that they need to broaden their membership to include experts in technology, science, engineering and mathematics.

2 E-voting: the European context

2.1 Past, present and future

E-voting has been used in Europe, for legally binding elections, since at least 1982 [21]. Its use is still not widespread, though interest has increased. The Netherlands was a very early adopter, and it was almost a decade later (1991) that Belgium started experimenting with e-voting. Just a few years later, in the mid-nineties, France did the same. By the early 2000's, experiments or pilots had been run in the United Kingdom, Italy, Spain and the Republic of Ireland [3], among others.

In places, the pace seems to be slowing. In the UK some of the more ambitious proposals, such as SMS- and Internet-voting, will not be included in trials this year [17]. In Ireland, the introduction of e-voting was halted in 2003 by the publication of a report by the Commission on Electronic Voting [6]. The Irish government has not yet made a commitment as to whether or when the system they purchased will be used in the future.

2.2 Problems: public perception, government communication and reality

The difficulty of implementing e-voting is not generally obvious to the public. At first glance, e-voting seems to be a simple case of counting. Conflicting requirements [20] and the differences between implementing e-voting and, say, electronic banking are not immediately obvious, particularly to people with no experience of developing mission- or safety-critical systems.

In the absence of controversy, surveys of voter attitudes usually reflect satisfaction and trust (for example [22]). When concerns are raised by experts and in the media, however, public opinion can change dramatically. For example: in Ireland in 2003 a survey by Amarach Consulting found that a majority of Irish citizens were in favour of the introduction of e-voting [15]. Less than a year later, after controversy over the system had led to the establishment of the Commission on Electronic Voting, a Red C survey found that 58% of respondents felt that "...the [e-voting] proposal should be scrapped until such time as a paper back-up is incorporated into the system ..." and "one third of all voters were unconvinced that their choices will be registered properly" [1].

This instinctive trust of e-voting systems also appears to exist amongst officials. When government representatives speak about e-voting it tends to be in very positive terms. Their statements emphasise the benefits of e-voting; the largest obstacle, from their point of view, is usually gaining the voters' trust. The idea that the system in question might not deserve such trust is given little or no attention, except where it overlaps with "allay[ing] public concern" about the security of the system [4]. Two prime examples of this are the webpages for the voting systems of the Irish Government and the Swiss state of Geneva [12, 11].

In reality, implementing e-voting is not so simple. Mercuri identified one of the most significant obstacles

– the conflict between the requirements for secrecy and accuracy [20]. Serious problems also arise from the way in which voting systems are currently developed. To our knowledge there is still no voting system that has been treated as safety-critical in its development and deployment [18]. The components of the systems are, in general, proprietary [24, 19]. These and other factors have combined to create serious issues in legally binding elections. Examples of worrying incidents in real elections in the US have been gathered by the Verified Voting Foundation's *Election Incident Reporting System* [25].

2.3 Europe and America: contrasting approaches

There are three significant differences between the approaches taken towards e-voting standards in the CoE and at a Federal level in the US: timing, takeup and size.

The first two are naturally related. The US has had (nominally) voluntary standards since 1990. However, many states have passed laws requiring conformance [16]. The CoE standards remain voluntary. In fact, to our knowledge, the "certification processes" called for in standard 111 have not yet been developed in any European country . No doubt this is largely due to the fact that the document is less than two years old. It is likely that this is also influenced by the difficulties of certification against the standards, discussed below, and by the fact that e-voting remains less widespread in Europe than in the US. Where e-voting is used in Europe it is generally on an experimental or pilot basis.

Comprising two volumes of 12 and 10 documents respectively, totalling almost 300 pages, the latest US standards (developed by the Election Assistance Commission – EAC) are clearly much larger than the document produced by the CoE, which totals 21 pages (the explanatory memorandum is a further 67 pages long). As might be expected, considering the difference in size, the American standards aim for a much finer granularity than the CoE standards do. For example: whereas the CoE standards make a passing reference to testing in standard 111, the EAC standards list and elaborate on five categories of testing.

2.4 CoE Recommendations: lack of ambition

The CoE standards, as they stand, are not ambitious in the sense that they do not aim to meet particularly challenging quality criteria. In fact, the specific role (requirements, if you like) of the recommendations are stated in a generic form. Consequently it is difficult to answer the question of whether they are doing a "good" or "bad" job, since we have only a poor statement of the job that they are supposed to do.

3 CoE Recommendations: an ambitious proposal

A more ambitious approach would be to first identify the criteria against which the standards can be judged – to more explicitly state what "job they are supposed to be doing" – and then to re-write the standards in order to better meet these criteria. We propose that a good starting point would be to consider the requirements that the standards should meet, and to orient this analysis towards alleviating the main problems that have arisen because such standards were not in place when many of the e-voting systems were first developed and adopted.

3.1 Standards, Analysis and Requirements Capture

Analysis is the process of maximising *problem domain understanding*. Only through complete understanding can an analyst comprehend the responsibilities of a system. The modelling of these responsibilities is a natural way of expressing system requirements. The simplest way for an analyst to increase understanding is through interaction with the customer and potential users of the system, where one of the most common problems is that an interrelated set of requirements must be incorporated into one coherent and consistent framework. Interaction with the customer is an example of informal communication. It is an important part of analysis and, although it cannot be formalised, it is possible to add rigour to the process. A well-defined analysis method can help the communication process by reducing the amount of information an analyst needs to assimilate. By stating the type of information that is useful, it is possible to structure the communication process. Effective analysis for building requirements models is dependent on knowing the sort of information that is required, extracting it, and recording it in some coherent fashion.

Clearly, a document which proposes a set of standards for a general problem domain has a key role to play in the analysis and requirements capture during the development of a particular system within that domain. The nature of the standards dictates how they should be used in improving analysis and requirements capture, and hence in addressing the major issues that often arise when building any complex computer system: will the user trust it enough to use it, will the customer be able to ensure that the system being procured meets the needs of the users, will a delivered system be amenable to independent verification (test) against that which was agreed

during procurement, and will the manufacturers be able to better design their product based on the shared knowledge of the common required standards?

We propose that the CoE standards should be judged on how well they answer the questions posed above.

3.2 Public and Trust

There is no doubt that there is significant public mistrust of e-voting systems across the world. The largest number of users of the systems will be the voting public, and it is not reasonable to suggest that such systems should be employed without the public's trust. The standards should address the issue of trust in a number of ways. Firstly, through their very existence and their association with the CoE, we would argue that public trust would – perhaps foolishly – immediately increase if they knew that the voting systems had been measured against the recommended practices and found to meet them. More importantly, if the standards were written in a way that directly addressed specific issues of mistrust that had been explicitly stated by the public, and there was evidence to suggest that the standards were being enforced, then the degree of trust would rise, provided that the evidence put forward was from a trusted source. Thirdly, if the standards were to be seen to have contributed towards an "inadequate" e-voting system being rejected for use then voters would be even more convinced of their value and this would increase their trust in systems which had not been rejected in the same way.

3.3 Governments and Procurement

Requirements capture is one of the most difficult and critical stages of the development of any computer system. Governments should be assisted in the procurement of all such systems by expert advisers from the areas of information technology, software engineering, computer security, and so on. The CoE standards should embody this expertise in a re-usable form so that each time an e-voting system is to be procured (or an existing system modified) there is an accepted body of knowledge about what the requirements for such systems should incorporate.

The standard should evolve as our collective understanding of e-voting systems improves, and as technological advancements introduce new implementation possibilities. The standards should – at the very least – be able to guide a government in deciding what sort of requirements they need to consider and in making sure that they do not overlook some critical aspects. They should also help governments in writing requirements specifications that form part of the procurement contract with the system vendors. In particular, they should provide guidelines with respect to the structuring of such requirements, and advice concerning alternative implementation technologies that have proven themselves in meeting particular requirements.

Without this advice, the risk of the procurement process failing to result in a trustworthy e-voting system will increase dramatically.

3.4 International Standards and Independent Testing

Most governments require that their procured e-voting systems are "inspected" by an objective, competent agency and that their suitability for use be verified before they can be deployed. There are many international standards, and standards bodies responsible for documenting and enforcing these standards, in a wide range of disciplines such as telecommunications, medicine and transport. Additional rigour can be added to this process by requiring that the agencies responsible for the testing have themselves been accredited. Such accreditation will increase confidence in the agencies being competent and independent only if the standards are expressed in such a way that there is no doubt that the agencies are able to measure any given e-voting system against them, without risk of a system that does not meet the standards expected being passed as having met the standards.

Clearly then the CoE recommendations must not only say what standards are to be met, but must also state the minimum requirements expected of any agency that can be authorised to test a system against these standards. Without this additional safeguard one increases the risk that an e-voting system is procured, and that it is passed for use by an independent agency, and it subsequently fails to meet the required standards. In such a scenario it is very difficult to identify which actor is responsible for the system failing after deployment.

3.5 Manufacturers and Design Decisions

It is important to remember that e-voting system manufacturers are not the opposing team in the e-voting development game. We should all be playing for the same team! Manufacturers, in general, appreciate any assistance that is available where it is likely to improve the quality of their product, or make it easier to identify and maintain a customer base. They understand that the e-voting systems that they are attempting to sell are open to criticism and that this criticism could impact on sales and revenue. They also understand that the design of their systems is a result of a number of decisions with respect to complicated trade-offs involving cost, quality, time-to-market, marketability, maintainability, reputation, risk of failure, and so on.

Design decisions need to be driven by the needs of the customer and targeted towards leveraging the technology available to the manufacturer. Clearly, the CoE standards should assist e-voting machine manufacturers in making design decisions that help to bridge the gap between what is required and how the requirement is to be met. A well-structured standard should help manufacturers in structuring their own design models in such a way that they can have more confidence that the design decisions they are making (or have already made) are good ones, both for them and for their customers.

Furthermore, manufacturers should be able to provide feedback into the standards documentation (process) by highlighting where the standards did not help them in the decision making process, and where this resulted in poor design decisions being made.

4 A Software Engineer's View

In the section that follows we introduce the key properties that a good requirements model should exhibit, and we demonstrate – with a small number of examples – how the current set of standards does not adhere to them. We first examine consistency: does the standards document use (interpret and give meaning to) notation and terminology in a consistent way, do they have contradictory standards, and do the standards contradict the other set of instruments that precede the document? Next we ask if the standards are complete: are there some existing e-voting systems whose adherence to the standards cannot be ascertained because the standards are not broad enough, and are there some aspects of e-voting system behaviour, in general, that the users are interested in but are not mentioned in the document? We also ask if there are some aspects that really don't need to be included as they are either outside the scope of e-voting, or they are in the scope of e-voting but adequately addressed by the other instruments. The next property that we address is that of the level of abstraction of the standards: if the standards are too concrete (over-specified) then they will exclude potentially good e-voting systems (that meet user requirements) because they are not implemented in a particular way or using a particular technology; similarly, if they are too abstract (under-specified) then there is no obvious mechanism for deciding if a system meets the requirement and so the standard will fail to exclude systems that appear not to meet a requirement due to uncertainty. Next, we examine whether the standards embody a clarity of expression – where the goal is to say things as simply as possible – and so we ask if there is too much repetition. Finally, we ask if the document is easily changed and updated. Are there some things that are likely to change in the future, that will require changes to the standards, but whose change will be very difficult and costly to manage? If so, the standards are not maintainable.

4.1 Consistency

The CoE recognises that consistent use of terminology is key, and states:

> "In this recommendation the following terms are used with the following meanings: [...]"

The terms that it chooses to define are: authentication, ballot, candidate, casting of the vote, e-election or e-referendum, electronic ballot box, e-voting, remote e-voting, sealing, vote, voter, voting channel, voting options and voter's registrar.

However, even in this short set of "definitions", fundamental terms are used inconsistently. For example, the voter's register is not defined as a list of voters, it is defined as a list of persons entitled to vote (electors). Consequently, in some instances, later in the document, the term elector is used inconsistently to refer to a voter; which may lead to confusion between a person who is entitled to vote and a person who actually does vote. Another potential problem arises because the term 'vote' can be used inconsistently as both a verb and a noun. This can lead us to two different, yet reasonable, interpretations of some of the standards.

A different type of inconsistency arises when undefined terms are used in the definitions and these terms appear to be inconsistently used. For example, the "casting of a vote" definition refers to the ballot box. Only "electronic ballot box" is defined and its definition does not refer to a "ballot box". However "ballot" is defined. Thus, in the standards, the term "ballot box" can be interpreted as being "electronic" or otherwise when the difference between them is not made explicit.

The definitions that the CoE provide demonstrate that they realised that consistent use of terminology is important. However, they also suggest that they did not get adequate expert advice as to how these definitions would have been handled during analysis and requirements capture of an e-voting system. Surprisingly, one of the most common expressions in the standards is that of "e-voting system", yet "system" is never defined!

To conclude, the poor specification of the fundamental concepts actually increases the likelihood of *internal* inconsistency in the standards document. A quick reading of the other standards instruments shows the same inconsistent use of terminology and so it is also unlikely that the standards document will be *externally* consistent with these other documents.

4.2 Completeness and Scope

Many e-voting systems allow for multiple elections to be run concurrently and for a voter to make more than one vote when attending a voting station. This aspect of the system-voter behaviour is not well covered by the standards and is just one example of how they are incomplete.

In contrast, many of the standards address issues that are not specific to e-voting and have already been addressed in other "instruments". For simplicity, these should have been left out of the document. For example, standard 39 states:

> "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."

This requirement is adequately covered in the CoE's own *Code of good practice in electoral matters* [10] which is a much more appropriate document.

In particular, the inconsistent use of terminology means that keeping such standards within the document increases the risk of introducing ambiguity into their interpretation.

4.3 Over Specification — too concrete

Over-specification is easy to identify as it usually manifests itself in a sentence of the form: "you must use X because X does Y". Clearly, a requirements document would be better saying "you must do Y", and it could even state "and X is an alternative way of guaranteeing Y". Otherwise, if we had a machine that "uses Z to do Y" then this machine would be rejected even though it met its requirements.

An example of this is standard 66:

> "Open standards shall be used to ensure that the various technical components [...] interoperate"

4.4 Under Specification — too abstract

Under-specification is easy to identify as it usually corresponds to the expression of an idealistic goal, leaving the reader with no idea of how one could check whether a given system actually meets the goal, or even if such a system could exist.

An example of this is standard 65:

> "The presentation of the voting options shall be optimised for the voter.'"

4.5 Redundancy and Repetition

In the restructuring of the standards proposed in the following section, it becomes clear that many of the requirements are repeated across many of the sections. This is one of the biggest weaknesses of the document. Where terms are used unambiguously, and interpretation of terms made consistently, then a certain amount of redundancy can strengthen a requirements document due to a type of internal self-verification and intuitive error correction. However, in the standards document, as presented, this redundancy and repetition increases the risk of the underlying requirements model being misunderstood. See section 6.2 for an example.

4.6 Maintainability and Extensibility

A good requirements document that exhibits all the desirable qualities that we mention above is very likely to be easy to maintain. We argue that the CoE standards document will be difficult to maintain and extend for two main reasons. Firstly, the faults described above make it difficult to use, and if it is not actually used in the day-to-day process of maintaining e-voting systems then it is likely that no-one will see the need to maintain it. Subsequently — as it becomes more and more outdated — the cost of maintenance will rise dramatically.

Secondly, the document is almost impossible to maintain because its structure is such that small advances in technology or small changes to our understanding of e-voting machine requirements will almost certainly require large changes to the document. Furthermore, this will make it very difficult to manage the conflict that arises when manufacturers want to introduce new technology, governments want to adopt it, and voters do not trust it.

5 Proposal for restructuring

We propose that the CoE standards document can be restructured as a first step towards rooting-out the faults described above.

The committee began by classifying their standards according to the particular rights they aim to uphold: Universal, Equal, Free, Secret and Direct suffrage.[2] They could have taken this classification further, however, and divided all the standards according to those categories.

This approach has several advantages. First, the five rights have been developed over a long period of history to capture all the high-level requirements of fair elections; by structuring lower-lever requirements according to these categories we enhance our ability to cover all requirements. Second, if lower-level requirements

are grouped together in a simple, logical and systematic manner, we reduce the risk of inconsistency and redundancy. This conclusion is supported by the fact that restructuring the document helped uncover inconsistencies, redundancies and gaps in the requirements. Third, a well-structured document is easier to understand, to maintain, and to use.

The one requirement that we were unable to fit into any of these categories was the need for the electorate to trust the system. An election must not only be fair, but also seen to be fair. We have placed this requirement last, since the trust*worthiness* of the system is more important than the trust*edness*. In fact the latter is undesirable in the absence of the former.

Terms used below have the following meanings:
ballot – voting options available in a particular race/referendum/poll
cast – to commit to a particular set of preferences, equivalent to putting one's completed paper ballot into the ballot box in a traditional paper-based voting system
eligible voter – a person who is entitled to cast one or more votes
e-voting system – any voting system which makes use of an electronic device
polling period – period of time when polls are open, ie votes can be cast
vote (noun only) – the expression of an individual voter's preferences
voter – a person in their role as caster of a vote
voter register – list of eligible voters
voting channel – communication channel by which votes can be cast
voting system – a system (set of devices and methods) for the collection and tabulation of votes

In the text below, italicised numbers in parentheses refer to standards in the CoE standards document [7]. Where a standard in the original document was deemed to cover more than one concept, it was split into sub-standards (see section 6.1); these are referred to by letters (eg *(61b)*), with the division taken along natural lines.

5.1 Universal suffrage

Since universal suffrage is the right that "all human beings have . . . to vote and to stand for election subject to certain conditions, for example age and nationality" [8], under this category we will include requirements that the system be universally *available* and universally *usable*.

1) The e-voting system shall be universally available, that is: every eligible voter shall have access to at least one voting channel. *(4)*

1. A contingency procedure shall be drawn up to prepare for the possibility that one or more voting channels become unavailable, and to provide alternative voting channels where necessary. *(61b, 70a, 71a)*
2. The contingency procedure shall include measures for physical disaster recovery. *(75b)*
3. Staff shall be trained to follow the contingency procedure. *(71b)*
4. The e-voting system shall be protected against threats to its availability including: malfunction, breakdown and denial of service attacks. *(30)*
5. The availability of each voting channel shall be subject to regular checks. *(79b)*
6. The timetable for voting channel availability shall be designed to maximise voter access and shall be made public well in advance of the start of the polling period. *(37, 45)*

2) User interface design (for all interfaces, including vote-casting, registration *(2)* and administration) shall follow best practice to maximise usability *(1b, 61a, 65)*, in particular:

1. Interfaces shall be understandable. It shall be made clear to voters whether they are participating in a genuine election, and whether their vote has been recorded correctly. *(1a, 14, 50)*
2. Voters shall be consulted during the design and testing of vote casting and registration interfaces. *(62)*
3. The needs of voters with disabilities shall be taken into account in the design of the interface. Appropriate advocacy groups shall be consulted, and compatibility with relevant products and compliance with relevant standards maximised, to that end. *(3, 63, 64)*

3) Voters shall be educated in the use of the vote-casting interface and regarding any steps required in order to participate. *(38)*

1. Voters shall be given the opportunity to practice using the interface. *(22)*
2. Support and guidance shall be available to voters through widely available communication channels. *(46)*
3. Where there may be doubt (such as with remote voting) voters shall be educated as to how they may confirm that they are using an authentic voting channel and that the authentic ballot has been presented. *(90b)*

5.2 Equal suffrage

Since equal suffrage guarantees that each voter shall have the same number of votes, this category includes measures that prevent fraudulent or erroneous votes from being recorded.

4) Only votes cast by eligible voters shall be counted, and only the permitted number of votes for that voter.

(5a, 94) Note: this will require special attention where voters are allowed to cast provisional votes.

5) An authentication system shall exist to distinguish eligible voters from others, and those who have successfully cast votes from those who have not. Note: this may require special attention where multiple voting channels exist, and where voter registers may not be up-to-date. *(5b, 6, 41, 44, 82)*

6) Votes shall not be recorded outside the polling period. However, provision shall be made for latency in voting channels. *(91, 96)*

5.3 Free suffrage

7) The free formation and expression of the voter's opinion shall be secured, as – where required – shall the personal exercise of the right to vote. *(9)*

8) The vote-casting interface shall be free from any information, other than that strictly required for casting the vote. The e-voting system shall *prevent*[3] the display of other messages that may influence the voters' choice. *(48)*

9) The e-voting system shall not permit any manipulative influence to be exercised over the voter during vote-casting. *(12)*

10) Information on voters' options shall be presented with equality and shall be widely available. *(43, 47, 49)*

11) Voters shall not have access to information which may prejudice their decision, such as the number of votes already cast for a particular option. *(53)*

12) Voters shall be free to participate without expressing a preference, for example by casting a blank vote. *(13)*

5.4 Secret suffrage

Secret suffrage, or voter anonymity, is not always implemented the same way. In the Republic of Ireland, for instance, voter anonymity is absolute. Any marks on the ballot paper which identify the voter invalidates the vote. In the United Kingdom, on the other hand, voter anonymity is conditional. The identity of voters can be discovered using the unique codes on ballot papers; this information is considered a state secret. The decision between absolute and conditional anonymity was not made explicit in the original CoE document, and this led to inconsistency between requirements [14].

13) The e-voting system shall, to the extent allowed by law, protect the secrecy of the vote. Note that this may be endangered by processing votes in small groups.*(18, 54)*

1. Where the law requires absolute anonymity, it shall be impossible to reproduce the link between voter and vote. Where the law requires conditional anonymity, it shall be impossible to reproduce such a link without the permission of the relevant authority. *(contrast with 17)*
2. At no stage shall the voter's identity and vote be available together in unencrypted form to any person (other than the voter) or system *(16, 19, 34b, 35, 93a, 106)*, except where required by law and sanctioned by the relevant authority.
3. The voter shall not be allowed to retain possession of anything which could be used as proof to another person of the vote cast. *(51, 52)*
4. Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person. *(11)*
5. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained. *(78)*
6. The audit system shall not endanger the secrecy of the vote *(contrast with 103a)*

5.5 Direct suffrage

The committee did not categorise any of their standards under "direct suffrage" saying that it "does not call for special attention" [7]. We contend that, since direct suffrage (as defined by the CoE) requires that "the ballots cast by the voters directly determine the person(s) elected" [7], any measure used to protect the votes from tampering falls into this category, as does any measure to ensure that the results are tabulated correctly.

14) The e-voting system shall accurately record votes *(95)*

1. It shall be ensured that the voter is presented with an authentic ballot *(90a)*
2. The vote cast by a voter shall be the vote recorded within the system *(92)* [10, guideline 42]

15) The e-voting system shall prevent recorded votes from being changed or deleted *(15, 34a, 92)*

16) The e-voting system shall accurately calculate the result based solely on the votes cast *(7, 98)*

1. There shall be a secure and reliable method to aggregate all votes. *(8)*

In order to support these requirements:

17) Provision shall be made for the observation of all stages of elections to the extent permitted by law. *(23, 56)*

1. Reliable, accurate, detailed observation data shall be produced. *(83)*
2. Observers shall be educated about the expected behaviour of the system and its operators so that they can make informed judgements about the reliability of election results [14]

18) There shall be a comprehensive audit system designed into the e-voting system to provide information about the functioning of the system at all levels. *(59, 100, 101, 102, 103, 104, 107, 108)* Audit information recorded shall, at a minimum, include:

1. The number of votes cast,
2. Count information (including personnel involved, and enough information to reproduce the count results),
3. Any suspicious activities which may indicate some kind of attack on the system (including votes affected, if applicable),
4. System failures and malfunctions,
5. Logs of authorised access to the system (including user identity and activities undertaken). *(57, 58)*

19) Software engineering best practice shall be followed, including:

1. A comprehensive risk assessment shall underpin the decision to introduce e-voting in general, and any system in particular. This assessment shall be carried out by individuals with a suitable level of expertise. *(III)* [4]
2. Components' access to time sources shall be strictly limited on a "need to know" basis [14, 20]. *(contrast with 84, see section 6.4)*
3. Change management for the system shall be open and transparent. In particular:
   (a) All components of the system shall be subject to version control. *(69b)*
   (b) It shall be possible to accurately and reliably determine whether a given component is the version tested and approved for use.
   (c) Any updates of software, including third-party software such as operating systems, shall be justified before installation [14].
   (d) There shall be a bug-tracking system.
   (e) All of these measures shall follow best practices.
4. Compliance with suitable open standards is recommended. *(66)* [5]
5. At least one competent, independent body (certification authority) shall be appointed to assess and certify the system's operation and compliance with these standards. *(111)*
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. *(25, 31, 73)*
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. *(contrast with 24, 69a, 105, 110)*
8. The system shall be fault tolerant and fail safe.
   (a) Any backup system shall conform to the same standards and requirements as the original system. *(70b)*
   (b) Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system. *(27 – see point 65 in* [8] *, 77)*

20) Security measures shall be employed *(28)* to protect the system from fraud and error. *(29)*

1. Where data must be transmitted and/or stored electronically its origin shall be verifiable and its integrity shall be protected. Currently this is likely to require the use of cryptography. *(26, 75c, 89, 97, 99, 109)* (Such data may include votes, voter registers, lists of candidates *(86)*, and audit information.)
2. Where access to data must be restricted (for example authentication data), its secrecy shall be protected. Currently this is likely to require the use of cryptography. *(81)*
3. The system shall be monitored during operation for compliance with requirements. *(72a, 79a)*
4. Security arrangements shall ensure that, for the duration of operation, each component is the version tested and approved for use.
5. Incident levels shall be defined and appropriate responses identified. *(76)*
6. All technical operations shall be subject to a formal control procedure. *(74a)* In particular:
   (a) The principle of separation of duty shall be applied wherever applicable. [2]
   (b) Physical and electronic access to equipment used in elections shall be limited via a comprehensive authentication system which complies with best practice, including the principle of least privilege. *(32a, 80)*
   (c) Clear rules shall be developed for determining access privileges of individuals, and for the appointment of personnel to sensitive po-

sitions. *(32a)*

(d) All personnel who have been assigned a cryptographic key for authentication shall be educated about key management.

(e) The physical security of equipment used in elections shall be protected during *(75a)* and between elections. Access shall be restricted according to the formal control procedure.

(f) Any changes to key equipment shall be notified to the authorities identified in the control procedure. *(74b)*

(g) Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. All such activities shall be the subject of a report. As far as possible, such activities shall be carried out outside election periods. *(32b, 33a)*

(h) Where such activities must be undertaken during an election period, they shall be monitored by election observers. *(33b)*

5.6 Voter assurance

The results of an election produce no mandate if the electors don't trust them. Therefore, if for no other reason, voter trust is vital.

21) Steps shall be taken to maximise voter confidence in the system *(20)* including:

1. Voters shall be educated about how the system works, and the measures taken to protect its integrity *(21)*.

6 Analysis of restructuring

Space does not permit a detailed discussion of all decisions made during the restructuring process, but the following sections highlight certain categories of decision, giving examples of each. Due to the faults discussed in section 4, we found it necessary to split, merge, rephrase, contradict and leave out standards from the original document, as well as add standards that should have been included but were not. In the following we cite examples of each type of change; the last section is the most comprehensive, referencing (though not quoting) all standards left out completely.

For the sake of clarity, we will continue to refer to standards in the original CoE document using parenthesised numbers in italics (eg *(39)*). We will refer to standards in our restructured set using numbers in bold (eg **19) 3d.**).

6.1 Split

There were multiple cases where a single standard actually covered several concepts. For example:

> *(69)* "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. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time."

Its length alone is an indication that it covers more than one concept. Such standards were broken up for consideration in the restructuring process, and sub-standards referred to using letters. *(69)* was split into *(69a)* ("The competent ... description.") and *(69b)* ("A procedure ... any time"). In many cases, these sub-standards were then merged with other standards, rephrased, contradicted or left out. See below.

6.2 Merged

Because the document did not have a single over-arching structure, many concepts were dealt with in a somewhat piecemeal fashion. Different aspects of the same concept appeared in various parts of the document. Grouping these aspects together should help prevent inconsistencies.

In our restructured set we included:

> **5)** "An authentication system shall exist to distinguish eligible voters from others, and those who have successfully cast votes from those who have not. Note: this may require special attention where multiple voting channels exist, and where voter registers may not be up-to-date."

This incorporates the following five standards from the original document:

> *(5b)* "A voter shall be authorised to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box."

> *(6)* "The e-voting system shall prevent any voter from casting a vote by more than one voting channel."

> *(41)* "In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made."
>
> *(44)* "It is particularly important, where remote e-voting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once."
>
> *(82)* "Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured."

6.3 Rephrased

Many of the standards were rephrased, for diverse reasons. This example is overly verbose and refers to "[t]he level of incident" which is not defined anywhere else in the document.

> *(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."

We rephrased it as follows:

> **20) 5.** "Incident levels shall be defined and appropriate responses identified."

6.4 Contradicted

There were certain of the original standards deemed to be just plain wrong. For example:

> *(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."

As Doug Jones [14] and Rebecca Mercuri [20] have discussed elsewhere, access to clocks can be a source of security risk (for instance, they might be used to trigger a Trojan Horse, or may endanger voter anonymity). Therefore *(84)* is contradicted in our standards:

> **19) 2.** "Components' access to time sources shall be strictly limited on a 'need to know' basis."

6.5 Added

Several standards which should have been included were not. Two examples of standards we had to add are:

> **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."

6.6 Not included

(10, 36, 39, 40, 42, 55, 60, 67, 68, 72b, 85, 87, 88, 93b, 112) were not included in the restructured requirements for the following reasons.

(36, 39, 60, 87, 88 and 112) were deemed to be outside the scope of the document. For example:

> *(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."

This is not directly related to the design or use of e-voting systems. It would neither help a manufacturer to develop a better system, nor help a government determine whether a given system was 'good' or 'bad'.

(10) is "paternalistic" [14]. There is no reason why interface designers should attempt to ensure deliberation on the part of the voter, and attempts to do so would likely only make the interface annoying. The traditional paper ballot does not have any measures to "...prevent [the voters'] voting precipitately or without reflection".

The registration of candidates and voters online *(40, 42)* is extremely inadvisable at this time. The difficulties associated with effective authentication on the Internet are well known [13, 5].

The reason for the inclusion of

> *(55)* "Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period."

is unclear, particularly in light of the presence of

> *(34)* "The e-voting system shall ... keep [the votes] sealed until the counting process."

(67 and 68) refer specifically to the use of EML. While the use of open standards can be advantageous (see point 120 in [8]) it is not advisable to support a particular standard in a requirements document beyond citing it as an example.

(72b) "The backup services shall be regularly supplied with monitoring protocols." is indecipherable.

The assignment of responsibility for compliance with standards is complex, and

> *(85)* "Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies."

risks reducing the responsibility of vendors of e-voting systems.

Since voter anonymity is a responsibility as well as a right, we should never rely on the voter to delete evidence of their vote *(93b)*.

7 Conclusions

As the above analysis has shown, the CoE standards document is flawed. The inconsistency, incompleteness, over- and under-specification, redundancy and repetition that have been demonstrated could lead to 'bad' systems being certified against these requirements, and/or 'good' systems failing. These flaws were identified using standard software engineering practices, and their presence indicates inadequate involvement of experts in the development of the document.

E-voting systems are computer systems, and so the successful development of standards for e-voting systems will require the input of experts in technology, science, engineering and mathematics.

In the explanatory memorandum that accompanies the standards, the possibility is raised that "[t]he CoE may look again at this issue two years after the adoption of this recommendation…". This paper is therefore timely, since this September will see the second anniversary of the adoption of the recommendation.

We recommend that the committee takes advantage of the experience of experts for the restructuring and maintenance of their standards document. If a broadly applicable document were developed, it could be genuinely useful both to governments procuring e-voting systems, and to vendors developing and maintaining such systems.

Acknowledgments

Funding for Margaret McGaley's research is provided by the Irish Research Council for Science, Engineering and Technology (IRCSET) through the EMBARK initiative.

Paul Gibson thanks the NUI, Maynooth and the CNRS for their support of his sabbatical leave which allowed him to contribute to this research.

References [6]

[1] Poll majority want e-voting put on hold. *The Sunday Business Post* (March 14th 2004).

[2] BARR, E., BISHOP, M., DEFIGUEIREDO, D., GONDREE, M., AND WHEELER, P. Toward clarifying election systems standards. Tech. Rep. CSE-2005-21, Department of Computer Science University of California at Davis, September 2005.

[3] BENOIT, D. K. Experience with voting overseas. Appendix 2J to the first report of Ireland's Commission on Electronic Voting, December 2004.

[4] BRENNOCK, M. Cabinet to press ahead on e-voting in EU and local polls. *The Irish Times* (February 25th 2004).

[5] CALIFORNIA INTERNET VOTING TASK FORCE. final report. `http://www.ss.ca.gov/executive/ivote/`, 2000. Appendix a3 section 3.2.3.

[6] COMMISSION ON ELECTRONIC VOTING. first report. `http://www.cev.ie/htm/report/download_first.htm`, December 2004.

[7] COUNCIL OF EUROPE. Recommendation on legal, operational and technical standards for e-voting. Rec(2004)11, September 2004. `http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/`.

[8] COUNCIL OF EUROPE. Recommendation on legal, operational and technical standards for e-voting - explanatory memorandum. Rec(2004)11, September 2004.

[9] COUNCIL OF EUROPE. Specific terms of reference (IP1-S-EE) of the multidisciplinary ad hoc group of specialists on legal, operational and technical standards for e-enabled voting. IP1(2003)3 e, February 2004.

[10] EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION). Code of good practice in electoral matters. Opinion no. 190/2002, October 2002. `http://www.venice.coe.int/docs/2002/CDL-AD(2002)023rev-e.asp`.

[11] GENEVA GOVERNMENT WEBSITE. E-Voting: informations [sic] about eVoting. `http://www.geneve.ch/evoting/english/welcome.asp`.

[12] IRISH GOVERNMENT WEBSITE. Electronic voting: it's easier for everyone. `http://www.electronicvoting.ie/english/index.html`.

[13] JEFFERSON, D., RUBIN, A. D., SIMONS, B., AND WAGNER, D. A security analysis of the secure electronic registration and voting experiment (SERVE). `http://www.servesecurityreport.org/`, January 2004.

[14] JONES, D. W. The european 2004 draft e-voting standard: Some critical comments. `http://www.cs.uiowa.edu/~jones/voting/coe2004.shtml`, 2004.

[15] LEATHAM, S. Most irish citizens approve of e-voting:. *electricnews.net* (August 6th 2003).

[16] MARK GONDREE, PATRICK WHEELER, D. D. A Critique of the 2002 FEC VSPT E-Voting Standards. Tech. Rep. CSE-2005-20, Department of Computer Science University of California at Davis, September 2005.

[17] MCCUE, A. E-voting tech trials ditched by government.

[18] MCGALEY, M., AND GIBSON, J. P. E-Voting: A Safety Critical System. Tech. Rep. NUIM-CS-TR-2003-02, NUI Maynooth, Computer Science Department, 2003. `http://www.cs.may.ie/research/reports/2003/index.html#02`.

[19] MCGALEY, M., AND MCCARTHY, J. Transparency and e-Voting: Democratic vs. Commercial Interests. In Prosser and Krimmer [23], pp. 153 – 163.

[20] MERCURI, R. *Electronic Vote Tabulation Checks & Balances*. PhD thesis, University of Pennsylvania,School of Engineering and Applied Science, Department of Computer and Information Systems, 2000.

[21] NIEMOLLER, D. K. Experience with voting machines in the Netherlands and Germany. Appendix 2K to the first report of Ireland's Commission on Electronic Voting, December 2004.

[22] OOSTVEEN, A.-M., AND DEN BESSELAAR, P. V. Security as Belief: User's Perceptions on the Security of E-Voting Systems. In Prosser and Krimmer [23], pp. 73–82.

[23] PROSSER, A., AND KRIMMER, R., Eds. *Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, July, 7th-9th, 2004, in Schloß Hofen / Bregenz, Lake of Constance, Austria, Proceedings* (2004), vol. 47 of *LNI*, GI.

[24] SIMONS, B. Is it true that politics and technology don't mix? DREs: Direct Recording Electronic Systems. *ACM Queue 2*, 7 (2004).

[25] VERIFIED VOTING FOUNDATION. Election incident reporting system. `https://voteprotect.org/`.

Notes

[1]The *European Commission for Democracy through Law* is an advisory body appointed by the CoE. As it meets in Venice, it is commonly called the Venice Commission.

[2]By Universal suffrage, each person shall have access to vote except where restricted by law (for example because of citizenship/age). By Equal suffrage, each voter shall have the same number of votes, usually one. By Free suffrage, voters shall be free to form and express their choice without undue influence. By Secret suffrage, the voter's identity shall not be linked to their vote except to the extent required by law (for example in the UK); where the law does not require that the link be retained, it is preferable that the relationship be impossible to reconstruct. By Direct suffrage, results shall be based on, and only on, the exact votes cast by eligible voters.

[3]Italics are used here to highlight the change from 'avoid' to 'prevent'.

[4]The very important requirement for a full risk assessment is not included as a standard by the committee, but is mentioned in the introduction to Appendix III

[5]The authors are not satisfied that the EML standard recommended by the committee is useful, however discussion of the suitability of EML is outside the scope of this paper.

[6]All websites listed were accessed on May 31st, 2006