E-voting:

an Immature Technology

in a Critical Context

Margaret McGaley

Department of Computer Science

National University of Ireland, Maynooth

Supervisor: Dr. J. Paul Gibson

NUI MAYNOOTH

Ollscoil na hÉireann Má Nuad

September 29, 2008

Abstract

E-voting has been introduced prematurely to national elections in many countries worldwide. There are technical and organizational barriers which must be resolved before the use of e-voting can be recommended in such a critical context.

Two fundamental requirements for e-voting systems are in conflict: ballot-secrecy and accuracy. We describe the nature and implications of this conflict, and examine the two main categories of proposed solutions: cryptographic voting schemes, and Voter Verified Audit Trails (VVATs). The conflict may permanently rule out the use of remote e-voting for critical elections, especially when one considers that there is no known way to reproduce the enforced privacy of a voting booth outside the supervision of a polling station.

We then examine the difficulty faced by governments when they procure Information and Communication Technology (ICT) systems in general, and some mitigation strategies. We go on to describe some legal implications of the introduction of e-voting, which could have serious consequences if not adequately explored, and discuss the evaluation and maintenance of systems.

In the final chapters we explore two approaches to the development of requirements for e-voting.

Dedication

I am dedicating this thesis to my wonderful husband Cian (in the active voice!). Without you, it could never have happened.

I want to thank Melanie Volkamer, Paul Gibson, Claire Guider, Paul McGaley, Tim Storer and everyone else who gave helpful comments and corrections. Thanks also to Joe McCarthy, Colm MacCarthaigh, Adrian Colley, and everyone at ICTE.

Naturally, any errors or omissions that remain are my own.

Contents

List of Tables

List of Figures

List of Abbreviations

BWahlG Bundeswahlgeräteverordnung – German Regulations for Voting Devices

C&AG Comptroller and Auditor General – A government official responsible for assuring that public money is properly administered

CC Common Criteria – an international standard (ISO/IEC 15408) for computer security

CoE Council of Europe – see section 5.1

DRE Direct Recording Electronic – e-voting systems in which *·votes·* are recorded directly on *·voting devices·*

DRE+VVAT DRE systems that incorporate a VVAT, usually by printing a ballot at the time the vote is cast

E-voting Electronic voting – any voting system which includes an electronic device in the vote-collection or result-tallying stage

EAC (US) Election Assistance Commission

EML Election Markup Language

EU European Union

ICT Information and Communication Technology

ITA Independent Testing Authority

Mark-sense E-voting systems in which paper ballots are scanned in for counting (the scanning is not necessarily in the optical range, so the term 'optical scan' may be misleading)

NIST (US) National Institute of Standards and Technology

PR-STV Proportional Representation Single Transferable Vote – the electoral system used in the Republic of Ireland, sometimes known as Instant Runoff Voting (IRV)

PTB Physikalisch-Technische Bundesanstalt – (German) national metrology institute providing scientific and technical services

PPARS Personnel, Payroll and Related Systems – software developed for use in the Irish health system

ROS Revenue Online Service

TD Teachta Dála – member of Dáil Éireann (the Irish National Parliament)

VVAT Voter Verified Audit Trail – also known as VVPB, see section 3.5 for details

VVPB Voter Verified Paper Ballots– also known as VVAT, see section 3.5 for details

Chapter 1

Introduction

Elections are a critical component of any democracy, whether they are considered 'safety' or 'mission' critical [1, 2, 3]. Elections decide the fate of countries and their citizens, so while the introduction of e-voting may seem like a natural step in the modern world, it is one that should be taken with caution. This thesis takes a software engineering approach to answer the question "What, if any, are the barriers to using e-voting in critical elections?".

1.1 Terminology

Election terminology is prone to ambiguity – some words may be used as both verb and noun (e.g. 'vote'), some words can have subtly different meanings (e.g. 'ballot' as piece of paper, or 'ballot' as set of voting options). We developed a glossary (appendix A) which gives unambiguous meanings to terms used in our requirements (see chapters 5 and 6). Words and phrases from the glossary appear ·*like this*· wherever we mean the glossary definition to apply.

In the interest of consistency, throughout this thesis "he" will be used as the gender neutral pronoun to refer to voters (and others) of unspecified gender.

In this thesis we use the term "e-voting" to mean the use of technology in the collection and/or counting of votes. We use the term "catalogue" to refer

to a set of requirements, or a requirements specification.

As a further defence against ambiguity, the key words SHALL and SHOULD (where they appear in small capitals) are used as described in RFC 2119 [4], i.e.: SHALL means that the definition is an absolute requirement of the specification, while SHOULD means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. In the case where a different course is chosen, all reasoning must be made explicit.

1.2 Scope of Research

1.2.1 Critical Elections

This thesis is concerned with what might be termed "critical elections": elections which are as important as general elections, presidential elections and referenda. There are of course many contexts in which (for instance) ballot secrecy is not essential, or the stakes are not high enough to be concerned about attacks on the system. Many of the arguments presented here will not be applicable in those contexts. It is beyond the scope of this thesis to attempt to draw a line between "critical" and "non-critical" elections. However, it is clear that elections of national importance (such as those mentioned above) do fit within the "critical" category.

1.2.2 The Electoral Process

Despite the variety of ways in which modern democracies implement elections, the following high-level view of the electoral process applies almost (if not actually) universally.

Voter Registration: a list of ·*eligible voters*· must be kept so that voting can be restricted to ·*eligible voters*·.

Voter Authentication: when a person attempts to ·*cast*· a ·*vote*·, they must be authenticated against the list mentioned above.

Vote Collection: the votes of authenticated ·*eligible voters*· must be recorded in a way which preserves secret suffrage (see section 1.6).

Vote Tabulation: results must be calculated based on the ·*votes*· ·*cast*· by authenticated ·*eligible voters*· according to the appropriate algorithm.

This thesis is concerned with the vote collection and tabulation phases of the electoral process. While other aspects of the electoral process have seen the introduction of technology, and may be fruitful areas for research, we chose to focus on e-voting: the use of technology to collect and count votes.

1.2.3 Technology

Technology might be introduced into this process in numerous ways, and for various reasons. Here we give a brief summary of the main technologies that have been used so far with the aim of putting the scope of this thesis in context.

Computerized management of the electoral register

It may be desirable to allow voters the opportunity to vote from whatever polling place they find most convenient. The best way to do this – without compromising voter anonymity or adding an excessive administrative burden – is likely to be the introduction of an accurate, up-to-date, computerized voter-register that can be securely accessed and modified from any polling place. An assessment of one such system (run on a pilot basis) is available in [5].

Voter authentication by digital signature

Jurisdictions that have the infrastructure in place may choose to implement computerized authentication of voters. This requires some kind of electronic record of voters identities, as well as a means of identifying the voter against

that record (such as an e-identity card). A description of a system which uses this kind of technology is available in [6].

Electronic vote collection and tabulation

The introduction of technology for these phases of the electoral process is what is generally known as 'e-voting'. Though a natural understanding of the term 'e-voting' might only include vote collection, e-voting systems inevitably also count votes. There are two main types of systems used: Direct Recording Electronic (DRE) systems collect votes directly from the voter through a *·vote-casting interface·*, Mark-sense systems (also known as Optical Scan systems) convert paper ballots into electronic records for tabulation. (Mark-sense systems introduce a new phase into their electoral process, between vote collection and tabulation, which might be termed 'vote format conversion').

The introduction of technology for vote collection (as in DRE systems) introduces a requirements conflict between vote secrecy and the accurate recording of votes (discussed in detail in chapter 3).

Remote voting systems

These systems generally use technology for all stages of the electoral process. They incorporate an electronic voter register, authenticate the voter remotely, collect the vote electronically and then calculate the results centrally.

We consider remote e-voting (such as via the Internet) to be outside the scope of this thesis, because we are concerned here with critical elections. As Adida says, the enforced privacy of the polling booth is the "only known way to establish a truly private interaction that prevents voter coercion" [7]. The most foolproof of security measures is only meaningful if we can prevent someone from standing beside the voter and watching as he casts his vote.

Besides this fundamental barrier to the use of remote e-voting, there are many immediate and practical obstacles such as the risk of viruses and trojan horses on the client computer. See [8, 9, 10] for thorough analyses. For a detailed

discussion of the political implications of remote e-voting, see [11].

1.3 A Short History of Voting Technology

The history of democracy is usually traced back to ancient Greece, but the form it took then would be barely recognizable as democracy to us today. Suffrage was extremely restricted, and those few members of society who did have votes cast them by dropping stones or clay shards into pots. They voted directly on the topics at hand rather than electing representatives to make those decisions.

While the secret ballot did exist in ancient Greece and was used for certain kinds of *·polls·*, in the modern era viva voce (by voice) voting was normal until the late 18th or early 19th century. Voters had to publicly declare their votes, which were written down by election clerks. When the secret ballot was first introduced ballots were hand-written by voters, cut from newspapers, or handed out by representatives of candidates.

In 1856, the "Australian ballot" was first introduced in the state of Victoria, Australia. Votes could only be cast on official ballots which were pre-printed by the electoral authority bearing all valid voting options. The idea spread gradually until it became the norm in democracies worldwide.

From the late 1800s, lever and punched card voting machines were introduced in various places around the US. Lever machines increment internal counters with each vote cast, keeping no record of individual votes. Punched card machines read cards that have been punched by individual voters, and those cards are retained and can be re-read where need arises. In a sense, these two types of voting machines are predecessors of the two main types of modern voting machines: DRE (direct recording electronic) and Mark-sense (ballot scanning) systems respectively. After the problems in Florida during the 2000 US presidential election, many of these lever and punchcard systems were replaced by DRE and Mark-sense systems. For a more detailed look at the history of voting technology in the US see [12, 13].

The use of mechanical voting has never been widespread in Europe, and e-voting has so far generally taken the form of DRE systems. By European standards, the Netherlands was a very early adopter (1982), 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 [14], among others.

Opposition to e-voting is growing in many places including Ireland [15], the UK [16], the Netherlands [17] and the US [18, 19]. These campaigns have, directly or indirectly, resulted in:

- the suspension of e-voting in Ireland since 2004 (see section 4.2.2)
- recommendations by the UK electoral commission that no further pilots of voting are undertaken until a comprehensive plan is in place, a central process is implemented and sufficient time is allocated for planning [20]
- the suspension of all e-voting in the Netherlands for the foreseeable future [21]
- de-certification in California of e-voting systems from four companies [22]
- new laws in many US states requiring a Voter Verified Audit Trail (VVAT – see section 3.5) [23].

1.4 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 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 (see chapter 3).

In the absence of controversy, surveys of voter attitudes usually reflect

satisfaction and trust (for example [24]). 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 Amárach Consulting found that a majority of Irish citizens were in favour of the introduction of e-voting [25]. 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" [26].

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 emphasize 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 [27]. Two prime examples of this are the webpages for the voting systems of the Irish Government [28] and the Swiss state of Geneva [29], both of which list advantages of their respective systems without making any mention of the real security concerns.

In reality, implementing e-voting is not so simple. Mercuri identified [30] one of the most significant obstacles – the conflict between the requirements for secrecy and accuracy (discussed in chapter 3). Serious problems also arise from the way in which voting systems are currently developed (discussed in chapter 4). To our knowledge there is still no voting system that has been treated as safety-critical in its development and deployment [1]. The components of the systems are, in general, proprietary [31, 32]. 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 *Election Incident Reporting System* set up by Verified Voting Foundation and Computer Professionals for Social Responsibility (CPSR) [33].

1.5 International Standards for E-voting

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. Despite the widespread and longterm use of e-voting in many places around the world, there does not yet exist a satisfactory requirements specification for e-voting.

E-voting is a problem that requires multidisciplinary input. Computer experts are unlikely to understand the social implications of the technology they design without input from those who have direct experience of running elections. Civil servants and political and social scientists are unlikely to understand the complexities and difficulties of designing technology to meet their needs. Requirements engineering is a vital step in system design and it always requires input from those for whom the system is being designed (clients – both buyers and users[1]) as well as those designing the system.

This thesis does not present a set of requirements based on this type of cross-disciplinary collaboration. However, many of the existing catalogues appear to have been developed without adequate requirements engineering expertise. This has produced requirements that are too abstract or too concrete, and documents that are internally inconsistent or incomplete (see analysis done in chapter 5 and [35]). Some catalogues are very much tied to the context for which they were developed (e.g. [36]). Many of the requirements are impossible to evaluate, leaving testers with no option but to say 'maybe'. Most of the requirement catalogues have not yet been used to evaluate real systems. This thesis does present two sets of requirements developed with software engineering needs in mind. Hopefully these requirements catalogues can be a building block for cross-disciplinary work to produce a valuable set of requirements for e-voting.

International standards exist in many disciplines. They clarify minimum

[1]The National Institute of Standards and Technology (NIST) in the US developed information security standards for the federal government. Ron Ross of NIST has identified the "open, public vetting process that involves significant review and public and private comment" as ensuring that "the standards and guidelines are technically sound, cost-effective, state of the practice, and can be implemented as required." [34]

general requirements, they provide a baseline from which requirements can be developed for more specific contexts and they pool international expertise. The need for such international standards for e-voting is one of the primary motivations for this thesis, and we make some proposals towards the development of such standards.

Various 'local' standards documents have been developed around the world. In the US the standards were developed originally by the Federal Election Commission (they are now maintained by the Election Assistance Commission – EAC). In Europe, the first trans-national e-voting standards were developed by the Council of Europe (CoE) (see chapter 5 for more details). There are also numerous standards documents developed for more specific contexts (e.g. [37, 38]).

However, no catalogue of requirements exists which:

- is generally applicable
- is developed with adequate software engineering expertise
- is useful for the design and evaluation of real systems
- takes evaluation techniques and certification procedures into account.

Of the existing catalogues, the two with the broadest intended scope must be those developed by the Council of Europe (CoE – see chapter 5) and the voluntary standards developed at a federal level in the US. There are three significant differences between the approaches taken towards e-voting standards in the CoE and 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 [35]. The CoE standards remain voluntary. In fact, to our knowledge, the "certification processes" they call for have not yet been developed in any European country. It is likely that this is influenced by the difficulties of certification against the standards (discussed in chapter 5) 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 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.

A standards document must be relevant to system developers and policy makers. It must be useful in weeding out "bad" systems without rejecting "good" systems. Unfortunately, neither approach has produced a standards document that meets these criteria (see the critiques of US standards in [39, 35] and of the CoE standards in chapter 5).

Despite the variety of ways in which democratic mechanisms are implemented around the world, there is enough commonality to make international standards feasible and worthwhile. Clearly this thesis cannot propose a complete set of such standards; their development requires input from experts in many disciplines. This thesis does, however, demonstrate the need for software engineering expertise in the development of standards (see especially the analysis of the CoE standards document in section 5.3).

1.6 Election Principles

Five principles are well established legally as necessary components of free and fair elections [40] (the need for suffrage to be 'trusted' has, until recent times, been left implicit; here it is included as a fundamental principle). Some of the following definitions are based on those in [40], though they have been rephrased in light of the glossary mentioned above (appendix A). These principles will be used later (chapters 5, 6) to categorize the requirements for e-voting.

Suffrage must be:

Universal: All human beings have the right to *·cast·* a *·vote·* subject to certain conditions, for example age and nationality.

Equal: Each *·eligible voter·* has the same number of *·votes·*[2].

Free: The *·voter·* has the right to form and to express his opinion in a free manner, without any coercion or undue influence.

Secret: The *·voter·* has the right, and the duty, to *·cast·* his *·vote·* secretly as an individual, and the state has the duty to protect that right.

Direct: The results of the *·poll·* shall be determined by the *·votes·* *·cast·* by the *·voters·*.

Trusted: The *·eligible voters·* must trust that these principles have been upheld.

1.7 Structure

This thesis is structured as follows: chapter 2 describes the research questions approached and the methodologies used. Chapter 3 examines the requirements conflict between secrecy and accuracy; we discuss the ways in which e-voting is different to paper voting with respect to that conflict. We then describe the two main approaches to resolving the conflict for e-voting. Chapter 4 describes some of the organizational issues with the introduction of e-voting. These issues include under-use of best practice in the public sphere and legal implications for electoral rules, results and vendors. Chapters 5 and 6 discuss the development of international requirements for e-voting, the former taking a top-down, and the latter a bottom-up approach. Chapter 7 lists the contributions made by the thesis, and chapter 8 discusses future work.

[2]In certain *·elections·*, some *·voters·* may have the right to *·cast·* more *·votes·* than others (e.g. stock corporations). Such elections are not considered here.

1.8 Acknowledgements

Some of the material in this thesis has previously been published elsewhere. Chapter 4 contains sections of "Transparency and e-Voting: Democratic vs. Commercial Interests" a paper written with Joe McCarthy [32]. Modified versions of "A Critical Analysis of the Council of Europe Recommendations on e-voting" co-authored with J. Paul Gibson [41] and "Requirements and Evaluation Procedures for e-Voting" written with Melanie Volkamer [42] form a large part of the thesis, mainly in chapters 5 and 6 respectively.

Chapter 2

Research Questions

The main research question in this thesis is: "What, if any, are the barriers to using e-voting in critical elections?". In the introduction, the term 'critical elections' is examined. In the following chapters, several barriers are identified and discussed. As this is a software engineering thesis the barriers examined are either software engineering problems, or discussed from the perspective of a software engineer.

2.1 Analysis

2.1.1 Secrecy versus Accuracy

The first barrier discussed was originally identified by Dr. Rebecca Mercuri [30], that is the conflict between the requirements for secrecy and accuracy. The sub-question here could be phrased:

> 1) "What solutions have been proposed to the secrecy-accuracy conflict, and are any of those solutions satisfactory for a critical context?"

In answering this question we asked the following: what is the nature of the conflict itself? What are the consequences for e-voting specifically (as opposed

to traditional paper-only elections), especially in dealing with fraud, error and usability issues? What solutions to the conflict have been proposed, and how do they resolve the conflict? Are they complete solutions, or mitigation strategies? Are they easily understood by voters? Are they easy to use? Do they rely too heavily on trusting individuals? What kind of procedural burdens to they entail?

Interesting questions which were not addressed include: what would be the financial cost of implementing these solutions? Do they place an unreasonable burden on election staff? What is their long-term viability (are they vulnerable to future scientific or technical breakthroughs)? What is the relationship between the solutions and international standards (are they compatible with/required by such standards)? What balance do they strike between secrecy and accuracy? Can this balance be 'tuned'? Many of these questions cannot be answered yet. For instance, since few of these solutions have been implemented in critical elections, it is very difficult to estimate their financial cost.

2.1.2 Organizational Barriers

The second sub-question relates to the broader political and organizational context of e-voting as an information technology system:

> 2) "What organizational barriers exist in the way that public bodies procure, use, and otherwise interact with e-voting systems? What mitigation strategies might prove useful?"

Here we focused on the following questions: given the existence of technical barriers to the safe use of e-voting in critical elections, why has e-voting been introduced so widely? Is e-voting an unusual case, or is there a pattern of difficulty in procuring high-quality ICT (Information and Communication Technology) systems by public bodies? In the Irish context, what high-profile examples of procurement success/failure would be useful for comparison? What

elements of ICT procurement/development best practice were implemented or not in each case? How did that affect the project outcome? What work has been done on the problem of procurement in the public sphere? Has that work suggested useful mitigation strategies? What legal barriers exist to the successful introduction of e-voting in critical elections? What are the considerations for the *·responsible election authority·* with respect to the maintenance and verification of systems? How can Independent Testing Authorities (ITA) help governments procure quality systems? What new challenges are posed by the selection of ITAs and the work that they do?

The limited availability of information in this area (as discussed in chapter 4) restricted the questions that could be asked here. It would have been interesting to examine a greater number of projects, in greater detail. Another investigation worth undertaking (but obviously beyond the scope of this thesis) would be to attempt to quantify the effects of mitigation strategies over a large number of projects.

2.1.3 Requirements

The third and most important sub-question encompasses the majority of the technical work of the thesis:

> 3) "Are there deficiencies in existing specifications of requirements for e-voting systems in critical elections? What can be done to address any such deficiencies?"

In answering that question we asked the following: what requirements catalogues exist? Are there any international standards? How suitable are such catalogues for the design, development and testing of e-voting systems? Do they express all the pertinent concepts? Taking the Council of Europe recommendations as an example, does that specification exhibit common requirements engineering errors? Can we modify it to reduce the number of such errors? If we were to propose a new catalogue of requirements for e-voting

for critical elections, what requirements would we include? How can we make use of the knowledge encapsulated in existing catalogues to improve our own requirements? How good are our requirements, and how can we assess their quality? How can systems be validated against our requirements?

Further questions in this area include: how can the requirements catalogue be modified and extended to include a broader range of e-voting systems? What modifications would be recommended or required by election officials and other interested parties? What are the political implications of the individual requirements, and what effect might they have on the establishment of a standards document based on them? What other existing catalogues could be usefully compared to our requirements?

2.2 Methodologies

We undertook an extensive literature review as a basis for answering all of the sub-questions under consideration.

Proposed solutions to the secrecy-accuracy conflict form a large part of the e-voting literature (though not all such authors describe their work that way explicitly). As a result, this was a theme that ran through much of the research for this thesis. With respect to sub-question 1) above we analysed the conflict itself, drawing on the extensive discussion available in the literature. From this discussion we identified the most important proposed solutions, which fell into two broad categories – cryptographic, and voter verification. We then examined each category for fitness-for-purpose for critical elections.

The secrecy-accuracy conflict is one of the "hot-topics" in e-voting. The analysis included here serves to elucidate the conflict as context for the rest of the chapter, rather than introducing new ideas. Our description is framed to highlight why the conflict arises in electronic rather than paper elections, and why the conflict increases the risk from both malice and error.

It became clear during our research that existing descriptions of crypto-

graphic schemes for e-voting were very difficult to read for non-cryptographers. Therefore we included a high-level description of the concepts behind the main schemes, and simple descriptions of three example schemes, summarizing the fundamental concepts expressed in the literature in more generally accessible language. We did not examine cryptographic schemes in greater detail, or compare their technical merits (in terms of metrics used in cryptography), since that research is already being undertaken by those with the relevant expertise.

We determined that a discussion of the strengths and drawbacks of proposed solutions to the conflict would be a useful contribution. Neither cryptographic schemes nor voter verification proved to be entirely satisfactory solutions; we identified specific issues with both categories. We did not propose our own solution to the secrecy-accuracy conflict, however much we would like to be able to offer an answer to this interesting and difficult problem.

We identified the broader context of e-voting as an ICT system procured by public bodies as an interesting and under-examined area. However, the lack of publicly available information on that type of procurement was disappointing, and limited the possible discussion. In answering sub-question 2) above, we derived a list of best practice principles from existing work in the area of public procurement of information technology. Since the available information was so limited, we did not seek to develop this list particularly rigorously – instead we sought practices which were common to the three documents we considered (and therefore well-attested). We identified three case studies from the Irish public sphere. For each case study we attempted to discover which of the aforementioned principles were implemented during the project's lifetime. In the case of the Revenue Online Service, this required direct contact with some of the staff involved. We included a summary of mitigation strategies suggested by extensive research in the UK context for informational purposes.

The publication of the Council of Europe's standards document for e-voting prompted our interest in standards and requirements for e-voting. We began our work in that area by examining that document for common requirements

engineering errors, and then developing a proposal for improvement. Since some of the requirements covered more than one concept, the first step was to split them into sub-requirements (see appendix B). We then rearranged the whole catalogue to group similar and related concepts together which helped to reveal inconsistencies, repetitions and gaps in the specification. The requirements were rephrased to increase clarity and to further reduce the number of common requirements engineering errors (see section 5.3). Some were deemed to be incorrect, and were therefore contradicted or left out. Some concepts not covered by the original specification were considered vital, and were therefore added. The resulting specification is a step towards the development of the requirements catalogue called for by sub-question 3).

As a further step towards answering that question, we developed a new catalogue in a bottom-up manner. The process of developing requirements involves: elicitation, analysis and negotiation, documentation and validation [43].

As Sommerville and Kotonya put it "structured methods are not very useful for requirements elicitation" [43, page 57]. Therefore we relied on the expertise encapsulated in existing requirements and literature, our own domain knowledge and methodical, iterative checking during this phase.

We used a modified version of the normal process of analysis and negotiation, since we did not have direct access to a "client" with whom to negotiate. Instead we analysed the requirements by re-checking them against existing catalogues and each other for classic requirements engineering mistakes (see section 5.3). Those other catalogues encapsulate a great deal of the relevant stakeholder needs, and therefore went some way towards making up for the lack of direct negotiation.

Documentation is the process of expressing requirements. It is important to find "an appropriate level" of expression for a given context. For e-voting it is necessary that requirements be comprehensible to many people including lawmakers and election officials, but they must also be useful to

system designers. We chose to express our requirements in well-defined natural language (for which we produced the glossary included in appendix A) but with a formalized structure (see section 6.3).

For validation, we again compared the latest version of our requirements against existing catalogues (producing the comparison tables in appendix C). We also developed an "interaction matrix" [43] to discover conflicts and highlight dependencies between requirements.

As discussed in [44], testing for completeness of requirements specifications is extremely difficult since "there is no other 'model' against which the specification can be tested; it is only through repeated validation cycles that one can gain some confidence of completeness." [44, page 13] Indeed the steps described above were not undertaken in a strictly separate way, and the results from one often fed back into another. We can confidently state that our requirements are more complete than any of the sets against which they were compared, however, since our catalogue includes necessary requirements not covered by any of them (see table C.6 in appendix C).

Chapter 3

Secrecy versus Accuracy

Where technology is introduced during the vote-collection phase of the electoral process, a requirements conflict can arise. This conflict poses a major barrier to the use of e-voting for critical elections. In this chapter we discuss the conflict itself, in particular why it does not arise in traditional paper systems. We go on to examine the two main types of proposed solutions to the conflict, and discuss their applicability to critical elections.

3.1 The Conflict

At the heart of e-voting there is a requirements conflict, between the need for accuracy and the need for secrecy [30]. If elections were public events, where every vote could be clearly traced to its originating voter, e-voting would become trivial. Take, for example, the voting system used in Dáil Éireann (the Irish Parliament). TDs (members of parliament) cast their vote by pressing a button at their seat. A large display board shows the votes as they are cast, as well as results. If a TD's vote is recorded incorrectly he/she is free to stand up and say so, and have the error corrected. Everyone can see how everyone else has voted, and everyone can see that his own vote has been recorded accurately. The secret ballot is not used in such situations because citizens have a right to

know how their representative votes.

Public elections are very different. Each voter has a right, and a duty, to a secret ballot. The introduction of the secret ballot was a very important innovation in the history of democracy; it enforces (in conjunction with effective voter registration) the rule: one voter, one vote. Since voters must successfully identify themselves before voting, and since they vote in the "supervised-privacy" of the voting-booth, each voter can vote the way he chooses to. Potential vote-buyers or coercers cannot gain extra votes because of their wealth or power, and their potential victims do not lose their votes because of their poverty or weakness.

It has been proposed that the secrecy of the ballot is no longer necessary and should be done away with in favour of more verifiability [45]. This proposal is flawed. The secret ballot exists more for the benefit of the system as a whole than for an individual voter; it prevents coercers and buyers from getting "more than their fair share" of votes. Developed countries with stable economies and governments must also take two more factors into account: first, other countries are probably watching and emulating, and second, the stability we enjoy is not as unassailable as it seems.

Here is where the conflict arises: in any other computer system, transaction accuracy is ensured by auditability. Online banking is feasible because any given transaction is recorded along with amounts and identities of all parties involved. The transaction can be checked for accuracy at a later date. E-voting does not allow this kind of auditability, because one party to the transaction (namely the voter) must remain anonymous[1]. When examining the election for accuracy, we cannot be certain about the accuracy of the *recording* of votes, since it cannot be audited [11].

[1]In a limited sense, the UK is an exception to this rule. Votes can be traced back to their originating voter via identifying numbers on ballot papers. This information is considered a state-secret however, and is only accessible in limited circumstances. For the purposes of this discussion let us consider the situation in the UK to be effectively equal to other jurisdictions with stricter definitions of the word "secret".

3.2 The Paper System

In the paper system this conflict doesn't arise. This is thanks in part to the advent of the Australian Ballot, another significant innovation in the development of our current democratic structures. The Australian Ballot is pre-printed by the organizing authority bearing the names of all candidates/ballot options. The idea is that access to an authentic ballot should only be granted to authorized voters, and those involved in the count should be able to easily identify an authentic ballot[2]. Since the voter has seen the actual record of his vote that will later be used to calculate results, and since he can be confident that "pencil doesn't fade overnight" [46, page 8], he can be sure his vote was recorded correctly. Similarly, since counters can identify authentic ballots, and they know that each authentic ballot was seen (and marked) directly by its respective voter, they can be sure that the votes they are counting were recorded accurately.

One significant weakness of paper voting systems is that they rely on a chain of custody to safeguard the integrity of ballot boxes after the close of polls. Often representatives of various interested parties as well as police officers supervise the transport and/or storage of the sealed boxes until they are opened for counting. Unfortunately, this chain of custody is not 100% reliable [47], though it is certainly better than no chain of custody at all (as we have in e-voting systems that do not incorporate some mechanism to solve the secrecy-accuracy conflict).

3.3 What's Changed?

With the introduction of a computer between voter and vote, we introduce doubt. A voter cannot see the computations performed within a computer, and therefore never sees the actual record of his vote. Assurances from the

[2] A similar system is used in certain European countries where access to the ballot-box is limited instead of access to authentic ballots.

computer that "your vote has been recorded", and even displays of the vote it claims to have recorded, make no difference. The display of information is a separate operation from the recording of information, so what is displayed does not necessarily bear any resemblance to what is recorded [48].

It could be argued that adequate testing would reduce the risk of accidental error below the risk of accidental error in the paper system, and that therefore e-voting should be more reliable than paper voting, but there are four important objections to that argument:

- we must concern ourselves with malice as well as error
- we cannot expect any testing regime to uncover all errors and weaknesses.

  > "Program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence." – Edsger W. Dijkstra [49, page 864]

  Those errors that do occur in e-voting systems will be more difficult to detect and deal with than those that occur in the paper system
- usability is a more complex question for computer systems than for paper
- the assumption that adequate testing will be carried out is not always justified (see section 4.2.2).

3.3.1 Malice

Unfortunately, elections have high stakes, and accidental error is not the only thing we need to test for. It would not be paranoid to say that there are numerous individuals and organizations that might want to alter the behaviour of voting computers to suit their own purposes [47], as recent experience with postal voting in the UK has proven yet again [50]. The single point of attack offered by an e-voting system provides a tempting target.

Attacks on the paper system certainly do happen, but the distributed nature of paper elections limits their scope. In order to affect an election without being

blatant one would have to spread any attack over many ballot boxes. Each new ballot box requires new members of the conspiracy.

A successful attack on an e-voting system, on the other hand, could have very far-reaching implications.

> "E-voting machines potentially make electoral fraud unprecedentedly simple. An election saboteur need only introduce a small change in the master copy of the voting software to be effective." [51, page 44].

An insider within the vendor company could hide "cheating behaviour" inside the proprietary and secret source code for voting computers. Someone could subvert the machine which calculates results. It has even been demonstrated that some systems are vulnerable to virus attacks which are spread from voting computer to voting computer [52], potentially subverting the behaviour of most of the computers in use on election day. Any of these could affect all or most of the voting computers simultaneously, in all elections in which the devices were used.

This also applies to attacks on the secrecy of votes. Certainly such attacks exist in paper systems. Chain voting is a classic example [47]. Early on polling day the attacker acquires a blank ballot. He then fills in that ballot according to his preferences. Vote-sellers are given the already filled-in ballot on their way into the polling place, and paid when they return to the attacker with a blank ballot (which they were given by polling staff). Of course the scope of such an attack is limited, the resources required are significant, and vigilance on the part of election staff should make it difficult in practice. Because of the centralized nature of e-voting systems, successful attacks on their secrecy are likely to have much more far-reaching effects.

3.3.2 Error

Errors in the paper voting system are similarly limited in scope. If one ballot box is misplaced the effects are limited to that constituency. An error which

caused voting computers to lose all votes of a certain type is likely to affect all computers, in all constituencies, every time they are used.

Potential errors in counting paper are also limited. Where ballots are hand-counted there is an assumed margin of error, and facilities for recounts are standard. However, since we are talking about random error, all candidates should be equally affected (statistically speaking) and the effects should balance one another out. Each recount should reduce this margin of error. An e-voting system, in contrast, cannot offer the facility of a recount without a completely separate ballot counting implementation. There are applications where one would expect a computer program to return different results when it is re-run, but the tallying of election results is not one of them.

In other words, we can assume that hand-counting gives results which are always at least slightly wrong, but the more times we calculate the results, the closer we get. E-voting systems give a result which *may* be 100% accurate, but which *may* be wildly wrong (resulting in the wrong candidate being elected) without being detected. Re-running a hand count should help uncover mistakes, re-running counting software will only repeat any mistakes. Schneier discusses these issues in [53].

3.3.3 Usability

E-voting systems have *the potential* to be more usable than paper, especially for people with disabilities such as visual impairment or reduced motor control. Indeed, paper voting systems are not free of usability problems [54]. However, designing a user interface for a voting computer is a much more difficult task than designing a good paper ballot. Paper ballots are based on a technology (paper and pen) that is extremely familiar to people of all ages. They also interact very simply with the user. In contrast, the very flexibility of e-voting interfaces that makes them so powerful also makes them much more complex to design well. It is also worth noting that e-voting systems cannot afford to have a steep learning curve [55]; citizens in most jurisdictions vote rarely and don't

have much opportunity to become familiar with the interface.

A good user-interface must be designed with its users in mind. For voting, the users are immensely diverse: age, abilities (physical and mental), language, familiarity with computers, and many more attributes may all be relevant to a given voter's ability to use the interface.

A poorly designed voting interface disenfranchises those who cannot use it (some of whom may believe they have used it correctly). It also jeopardizes the ballot secrecy of those who need help using it. There is a risk that voters may stay at home rather than attempt to use a system they are not comfortable with. Indeed, as the "butterfly ballot" incident in Florida [54] showed, a poorly designed voting interface can change the outcome of an election.

See Sarah P. Everett's doctoral thesis [56] for a more detailed analysis of the problem of usability in e-voting systems.

3.4 Proposed Solution: Cryptographic Voting Schemes

In this section we discuss the use of cryptographic voting schemes as a means of overcoming the requirements conflict as a barrier to the use of e-voting in critical elections. We summarize the design of these schemes, giving a high-level outline of three example schemes, and then discuss their suitability for use in critical elections at their current stage of development.

In the long term, cryptography offers the exciting possibility of improving election verifiability beyond even that offered by tried-and-trusted paper systems, removing the reliance on chain of custody for security. Though many cryptographic protocols have been proposed for remote e-voting (e.g. [57, 58, 59]), polling stations remain an essential part of any voting system for critical elections, including those that make use of cryptography (see section 1.2.3). In general, the cryptographic systems proposed so far aim for:

- *ballot casting assurance* – whereby each voter can be certain that his

vote has been recorded accurately (also known as "voter verifiability")

- *coercion resistance* – whereby no voter can prove to anyone else how he voted (also known as "receipt freeness")
- *universal verifiability of the tally* – whereby any observer can verify that the recorded votes match the published tally.

These aims are achieved by a fundamental design that underlies all the major polling-site cryptographic voting protocols. The voter casts his vote in a polling booth. He receives a token (usually a piece of paper) which proves to him that his vote was recorded correctly, but cannot be used to prove to others how he voted (*coercion resistance*). This 'proof' is achieved differently in different protocols, but always involves the publication of votes on a secure, reliable, accessible 'bulletin board' in an encrypted form. The voter can check (or allow someone to check on his behalf) that the token he received is represented on the bulletin board (combined with verification that his token accurately represents his vote this gives *ballot casting assurance*). There is also always some mechanism for ensuring that the published encrypted votes do indeed tally to the published result (*universal verifiability of the tally*).

In these schemes, cryptography is used to maintain the secrecy of the ballot, and "[a]ccuracy is ... verified by statistical means." [60, page 61] using the concept of "cut and choose". If Alice and Bob have a cake to share, Alice *cuts* the cake and Bob *chooses* his half. Alice cannot do better than cutting the cake evenly in two because if one part is larger Bob will choose that part. In the voting context, cut and choose is usually implemented as follows: someone (preferably the voter [7]) chooses between two ballot papers, one of which they use to vote, the other of which they check to see that it would have accurately recorded a vote. The reasoning is that since the "powers that be" (voting machine vendors, ballot printers, etc.) could not predict which of the two would be checked for accuracy, they cannot hope to cheat the system undetected.

Many cryptographic e-voting protocols use mixnets to decrypt votes while preserving privacy (Adida calls mixnets "shaking the virtual ballot box" [7, page

38]). Mixnets spread trust over several mutually antagonistic trustees (such as representatives of the different political parties) to provide certain guarantees such as: "given that at least one trustee is not corrupt, the secrecy of the ballot has not been broken" and "no ballots were modified during the mixing process". The latter is not provided by all types of mixnet; it may be required, for instance, that each trustee provide a zero-knowledge proof (proof of an assertion without giving away any more information than the assertion itself) that his contribution to the mixnet did not modify any ballots.

For a thorough discussion of the foundational concepts in cryptographic voting systems (including *zero-knowledge proofs* and *mixnets*) see Adida's doctoral thesis [7].

To give a better idea of this booth/token/bulletin board design concept, let us briefly describe three examples: Prêt à Voter (Ryan [61]), Punchscan (Chaum [62]) and Scratch & Vote (Adida [7]). The interested reader may wish to see two of the earliest such schemes [63] and [64] and Rivest's ThreeBallot voting system [65][3].

3.4.1 Prêt à Voter

In Prêt à Voter [61], ballot options are listed in a random order (which varies from ballot to ballot) on a detachable tab on the ballot paper (figure 3.1). The part of the ballot on which the voter fills in his preferences also contains encrypted information which, in combination with certain secret information, allows the candidate ordering to be reconstructed. It has been noted that randomized ballot ordering may adversely affect voters who have pre-planned their voting [67], and in many jurisdictions the law requires that all voting options appear in a fixed order.

The voter is assured that the encrypted information does actually represent the correct ordering (and therefore that his vote will be decrypted correctly)

[3]ThreeBallot is a work-in-progress attempt to provide the same end-to-end assurances as these schemes, with similar reasoning, but without the use of encryption (the system has unresolved security and usability issues [66]).

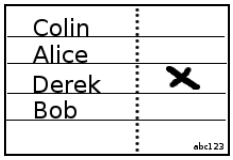


Figure 3.1: Prêt à Voter ballot with vote cast for Derek

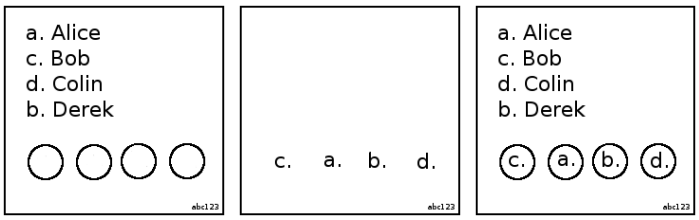
by use of cut and choose. Auditors randomly select half the printed ballots to be decrypted before polling begins. The chances of an adversary successfully planting faulty ballots without being detected by this audit are negligible, especially if they want to plant enough ballots to affect the election. As explained in [7], however, it would be preferable for the voter to do the choosing in the cut-and-choose protocol; otherwise the voter must trust whomever makes the choice.

The detachable part of the ballot (which shows candidate ordering) is removed and destroyed, and then the part of the ballot paper on which the voter has expressed his preferences is scanned and marked in some way by election officials as a valid ballot (this prevents voters producing fake ballots in order to claim that their vote was not recorded). The official cannot see what the voter's preferences are, since the ballot paper no longer indicates candidate ordering. The voter can take the scanned part of the ballot home as a kind of receipt (though not one he could use to prove to others how he voted).

Once all ballots have been cast, they are published in their encrypted form to a public bulletin board where voters (or their representatives) can check that their receipt is included. Before being decrypted for tallying, the votes are anonymized via a mixnet and zero knowledge proofs produced to guarantee that the set of anonymized encrypted ballots corresponds exactly to the set of published decrypted ballots.

3.4.2 Punchscan

Punchscan [62] ballots are also formed of two parts, but in this case one overlays the other (figure 3.2).



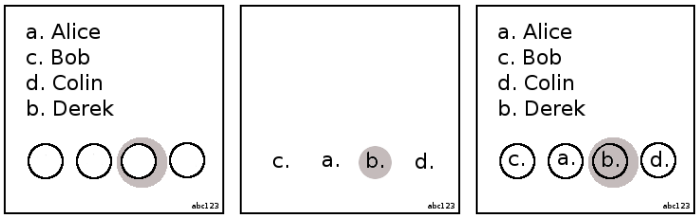
(a) top (b) bottom (c) both together

Figure 3.2: Punchscan ballot: top, bottom, both pieces together

The top part has holes in it, through which the lower ballot is visible. The top part has a list of voting options, each with an associated symbol (usually a letter). The association between options and letters is randomized and differs from ballot to ballot. On the bottom part, visible through the holes in the top part, these symbols are printed (again in a randomized order - independent of the order on the top part). These ballots go through a similar pre-election auditing process, where half the ballots are selected at random and checked for correctness.

To cast his vote the voter finds the letter associated with his preferred voting option (in the list on the top part), then finds that symbol among the symbols on the bottom part (visible through the holes). He then uses a "bingo dauber" or similar device to mark his choice. The dauber should be wider than the hole so that it marks both the top and bottom parts of the ballot (figure 3.3).

The voter then chooses which part – top or bottom – to keep, and which to destroy (a second, voter-based, 'cut and choose'). The former is scanned before the voter leaves the polling place so that the vote can be included in the tally, and published on the bulletin board for voters and their representatives to check. This arrangement would be difficult to adapt to more complex ballots, such as those where voters express preferences in order. For example, a Punchscan



(a) top (b) bottom (c) both together

Figure 3.3: Punchscan ballot: top, bottom, both pieces together, with vote cast for Derek

ballot for PR-STV would have to represent the ballot options in a grid with preference number on one axis and ballot options on the other (or something similarly complex) (figure 3.4).

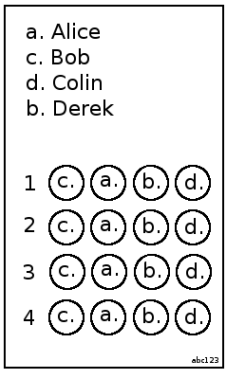


Figure 3.4: Possible Punchscan ballot for PRSTV

Both parts of the ballot have the same unique ID number printed on them. This ID number is associated with a row in a special table which allows for the result to be calculated. Again, this result has an associated zero-knowledge proof, but this time based on a simplified mixnet [7].

3.4.3 Scratch & Vote

Scratch & Vote [7] is a voting method which can be used with multiple ballot designs. The basic idea is that the ballot has a scratch surface on it (similar

to scratch surface lottery tickets). Beneath the scratch surface is enough information to decrypt the ballot. For example: if Scratch & Vote were used on a Prêt à Voter ballot (figure 3.5), the information under the scratch surface would allow you to reproduce that ballot's candidate ordering without requiring access to secret information (unlike standard Prêt à Voter ballots, which cannot be decrypted by individual voters).

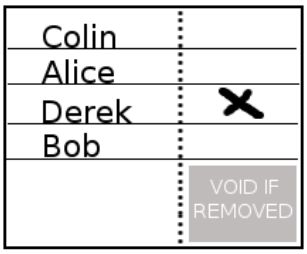


Figure 3.5: Scratch & Vote on a Prêt à Voter ballot

Obviously, if the surface has been scratched, the ballot becomes void for use in the election. It can be used for auditing purposes, however. This modification has the advantage of bringing the auditing phase into the hands of voters (and their chosen 'helper organizations' [7]) rather than requiring them to trust election officials to do the audit properly.

In order to create these ballots that can be individually decrypted in this way, Scratch & Vote uses a special type of encryption called 'homomorphic encryption' [68, 57] which has the powerful advantage of allowing votes to be tallied without decrypting individual votes. Tallying can be reproduced by anyone using only the public key, eliminating the need for the trustees required by mixnet-based protocols.

One disadvantage of homomorphic encryption is that a zero-knowledge proof is required for each individual vote, to ensure that it will be correctly tallied. This forces voters to check that a proof has been provided for their ballot. (Adida proposes that, since these proofs would be too large to include on the ballots themselves, polling places should be provided with electronic copies that

voters can check before casting their vote [7]).

A more significant, and indeed insurmountable, problem is that homomorphic encryption cannot be used for some of the more complex tallying systems such as PR-STV (which is non-monotonic [69]), nor can it handle write-in candidates (which are commonly allowed in the US). While modifications may be developed for other voting schemes to enable them to handle non-monotonic electoral systems and write-in candidates, voting schemes which rely on homomorphic encryption cannot be made to accommodate such systems (without added-on mechanisms not based on homomorphic encryption) because of theoretical limitations.

3.4.4 Limitations

Unfortunately, the cryptographic protocols that have been proposed so far have not yet overcome all of the barriers to their use in critical elections.

Understandability

The most significant of these barriers, and the one that affects all current cryptographic voting protocols, is the fact that they are so hard to understand. Voters must be able to trust that their vote has been recorded correctly, kept secret, and counted correctly. This trust should be based on understanding, not faith. In the end, asking a voter to trust cryptographers is not any different to asking him to trust e-voting system vendors. The voter is only protected from coercion if his vote is secret *and he believes* that his vote is secret. If the voter doesn't understand the protocol, he may be at risk of being convinced by a coercer that his vote is not secret.

> "Democracy not only means an equal right to vote, it also means an equal right to understand the techniques of voting procedures and an equal right to prove the results. Democracy includes full transparency in all its procedures. Thus, in a democracy, all elements of the voting process (including the software) must – at least in principle – be easy to follow and to understand for all citizens. Citizens who agree to give up that right, and to put

> all their confidence in technicians who will judge the security of computer software in their place, have already agreed to transfer all power to an aristocracy of a handful of people."
>
> – Hubertus Buchstein [11, page 50]

Usability

As discussed in section 3.3.3, usability is a major concern in e-voting system design. Though detailed usability studies are lacking[4] it is clear that many of these systems may pose difficulties for voters. Many of these systems place an unreasonable burden on the voter, requiring that he complete several steps in order to cast his ballot. Usability is also related to understanding, since a voter may find a system more difficult to use if he doesn't understand how it works.

Reliance on auditors

Most of the systems require that an audit be carried out before polling by trusted auditors. The level of trust required may be excessive, though it could be argued that similar levels of trust are required in certain players in a paper system.

Flexibility

To be broadly useful, these protocols must be compatible with many different voting methods. Protocols that rely on homomorphic encryption, for instance, cannot be used for non-monotonic systems such as Ireland's PR-STV. Nor are they capable of taking write-in candidates.

The Bulletin Board

The bulletin board (where encrypted votes are available to voters for checking) must be secure, reliable and accessible. It is "effectively a robust, authenticated broadcast channel" [7, page 76]. Though it is possible to implement such a bulletin board (for example, using public-key cryptography), it is an essential

[4] This lack is acknowledged, in the case of Punchscan, in [70].

part of these systems, and must not be neglected. Many proposals for cryptographic voting protocols simply assume the existence of such a channel. The implementation of this channel could disenfranchise voters (see Usability above). Indeed, it has been argued that reliance on such technology might leave certain demographics at a disadvantage when it comes to verifying that their votes have been correctly recorded [71].

Theoretical limitations

Certain protocols rely on concepts that have profound theoretical limitations. The democratic implications of these limitations are not always fully understood by the cryptologists who propose the schemes. An example of this is the continuing emergence of schemes based on homomorphic encryption (see the discussion in section 3.4.3 above).

3.5 Proposed Solution: Voter Verification

Unless and until a suitable cryptographic protocol is developed we shall have to rely on other methods to ensure the verifiability of elections. Perhaps the most commonly proposed solution is what is known as Voter Verified Paper Ballots (VVPB) or a Voter Verified Audit Trail (VVAT) [30]. This consists of a tangible record of each vote cast which has been verified as correct by the voter at the time he cast it. Effectively, this is an attempt to reuse the solution that works for paper voting systems: create a record of each vote which is both verified by the voter and clearly genuine, thus bridging the authentication/secrecy gap.

There are various ways in which this can be implemented. DRE (Direct Recording Electronic) systems may have printers added such that each voter views a printout of his vote before the vote is irrevocably cast (DRE+VVAT). An alternative is so-called “mark-sense” ballots where voters cast their votes on ballot papers which are scanned.

A correctly implemented VVAT must:

- comprise ballots verified by individual voters, which must be treated the same as ballots in the paper system (chain of custody). Where inconsistencies are detected these ballots must take precedence, since they have been verified by voters.
- not retain ballot-casting order. Some VVAT systems in use print ballot details onto a roll of paper. An observer who took note of the order in which voters entered the booth, and who then had access to the paper trail, could identify individual's votes. See [72] for an extreme example.
- be counted and compared to the electronic result in a mathematically calculated, statistically significant [73], number of randomly selected constituencies at every election (there would be no point in creating such a paper trail if it were not checked in a meaningful way).
- have adequate procedures in place to handle any discrepancies between electronic and VVAT results that do arise, as well as other problems.

There are numerous procedural issues that arise with the use of VVAT. For instance, where DRE+VVAT is used authorities must decide what should happen if a voter claims that the voting computer printed the wrong vote. The claim must be taken seriously, since the computer may be "trying to cheat", but the voter may also be lying or simply mistaken. Mark-sense systems have their own vulnerabilities; for instance, improper calibration of the devices (accidental or deliberate) could have a significant effect on the outcome of a *·poll·* [74].

Above all, the paper trail must be examined in a meaningful way. Whatever way the record is created, it is clear that it serves no purpose unless it is checked and its results compared to those from the electronic system. There is ongoing discussion about how often these records should be checked [73].

Amongst other practical issues with VVAT is the concern that voters will not actually check the paper records for accuracy. Recent research suggests that voters do not even check confirmation screens on voting computers for so-called "vote-flipping" [56]. This is an area that merits further study. How many ballots are likely to be checked by voters and how many voters would need to check

their ballots to make an attack statistically non-viable?

Despite these problems, a properly implemented VVAT could raise an e-voting system's trustworthiness to the level of existing paper voting systems. As will become clear in the following chapters, however, it seems unlikely that governments will be able to procure e-voting systems of high quality and hence systems with a properly implemented VVAT. It would be wise to concentrate on improving the way they procure ICT in general (chapter 4) and deciding what exactly they want their e-voting system to do (chapters 5 and 6) before introducing new risks into such a sensitive and important area as elections.

3.6 Summary

The requirements conflict between secrecy and accuracy is a significant barrier to the use of e-voting in critical elections. It increases the risk of undetected, and uncorrectable, modifications of results by malice or error. It also raises usability issues.

In the long term, the most attractive solution to this conflict may be the introduction of cryptographic voting schemes. These schemes have the potential to improve the accuracy of elections beyond that of traditional paper voting systems without compromising secrecy. However, they have not yet overcome all of the limitations which make their use in critical elections undesirable.

In the short term the use of techniques which allow for voter verification, where properly implemented, may raise the accuracy of e-voting elections without compromising secrecy. There are important procedural issues, however, which must be overcome if voter verification is to be used in critical elections.

Chapter 4

Organizational Issues

There are several organizational issues which act as a barrier to the successful introduction of e-voting for critical elections. In this chapter we highlight the difficulty faced by public bodies in procuring Information and Communication Technology (ICT) systems in general. We also discuss the best practice techniques and mitigation strategies that might help to improve the situation. We then describe some of the legal issues which arise with the introduction of e-voting. Finally we look at questions arising for the *·responsible election authority·* because of the need for verification and maintenance of e-voting systems and the standards that govern them.

4.1 The Problem of Procurement

Why have so many governments introduced e-voting in the face of such – if not insurmountable, un-surmounted – technical barriers? The answer may lie in a general difficulty amongst governments in procuring ICT systems. The discussion below will focus on projects undertaken in Ireland and proposed mitigation strategies from the UK, but it is unlikely that these problems are restricted to those two countries – especially considering the widespread adoption of e-voting without even basic attempts to address the conflict between

secrecy and accuracy.

ICT procurement is notoriously difficult. According to the Standish group's "CHAOS Report" (quoted in [75]) 18% of the private-sector ICT projects they surveyed in 2004 were "cancelled prior to completion or delivered and never used". A further 53% were categorized as 'challenged', meaning that they were delivered "late, over budget and/or with less than the required features and functions". Just 29% of the projects they surveyed were categorized as having succeeded - "delivered on time, on budget, with required features and functions" (figure 4.1).

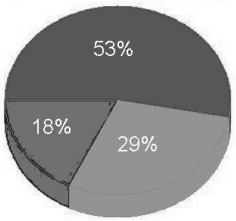


Figure 4.1: 53% challenged, 29% succeeded, 18% cancelled [75]

Though there does not seem to be an equivalent to the Standish report for governmental agencies, there is reason to believe that the situation is even worse in public institutions. Among other things, projects tend to be large, there is no threat of bankruptcy to encourage the abandonment of failed projects, and the requirement for public accountability is far greater [76].

4.2 Best Practice

In this section we compare three high profile Irish ICT projects. The aim is to illustrate the effect of best practice principles on real-world projects in the public sphere. We begin by enumerating an illustrative (but not exhaustive) list of best practice principles derived from various sources, including [77, 78, 79]. We then ask which of the listed practices were followed for each project, and how

successful the project was. The lack of available data (as discussed in more detail below) limited this exercise, and the results are therefore illustrative rather than comprehensive.

Our conclusion – that following best practice appears to have a positive effect on project outcome – indicates that more widespread use of such principles in the public sphere would be appropriate.

4.2.1 List of Best Practice Principles

1. At the very earliest stages, a clear *Vision* for the project must be developed. If the general goals, aspirations and concerns for the project are not outlined in the beginning, it makes all the later stages considerably more vulnerable.
2. A *Business case* can then be developed, including a detailed and realistic *Cost/benefit* analysis and *Risk analysis*. This should be developed with an open mind to the possibility that the project may have to be abandoned if the cost/benefit ratio is not satisfactory, or the risks are deemed too high.
3. At this point it should be ensured that there is adequate *Buy-in from all stakeholders*. Without this the project may never meet the needs of the users for whom it is intended, and/or it may have necessary resources pulled before completion.
4. *Requirements* for the project can now be formally defined. This is a process which requires considerable expertise (if the requirements document is to be any use to developers) but also requires the input of future users of the system to ensure that the project built is that which is required and not simply that which the developers know how to make.
5. The *Clarification of the roles and responsibilities of key players* ensures that no one party is left dealing with all the consequences in the event of project failure.

6. The statistics cited above from the Standish report make the need for *ICT project management expertise* clear. If these projects could be run without the support of experts, they would be more successful. This principle may be particularly difficult for the public sphere, as governments find it difficult to retain skilled staff in this area [80].
7. A *Single responsible owner* must be identified to maintain consistency and direction and to ensure that disputes amongst interested parties can be resolved, one way or another.
8. It is well established that taking a *Modular and incremental approach* to system development and deployment is a useful strategy. Modular and incremental development allow for unit-testing, can aid bug-fixing (by helping pin-point the origin of errors) and can provide some functionality to users before the system is complete. Similarly, incremental deployment helps "iron-out" unexpected issues that arise in the real world before large-scale deployment where they might have more serious consequences.
9. During development the project must be subject to *Regular oversight*, including gateway reviews (see section 4.2.6). This helps to identify problems early and prevent projects spiralling out of control.
10. *Contingency arrangements* must be developed to cope with the possibility of system failure. This is especially important in mission/safety critical systems – as many government ICT projects are.

4.2.2 Example Project: E-voting

E-voting was first proposed for use in Irish elections in the late 90's by the then Minister for the Department of the Environment, Heritage and Local Government (Minister for the Environment)[1], Noel Dempsey TD. The Nedap/Powervote system was chosen through a tender process to eventually be

[1]For historical reasons, the Minister for the Environment has responsibility for the running of Irish elections

used nationwide for all elections in the Republic of Ireland. Two pilots were held in 2002 in local elections and the re-run of the Nice treaty referendum. They were described at the time as being highly successful, but it was later revealed that the number of votes recorded varied significantly from the number of voters marked on the register as having voted. This was attributable to clerical errors, but the fact that it went unremarked is indicative of some of the problems with the project.

In 2003 a lobby group called Irish Citizens for Trustworthy Evoting (ICTE) was formed as opposition was growing to the introduction of e-voting without adequate safeguards. Pressure from ICTE, opposition parties and others led to the creation, in 2004, of the Commission on Electronic Voting (CEV). The CEV was asked to examine the secrecy and accuracy of the chosen system and concluded in April 2004 (just one month before the system was to be used nationwide) that it could not advocate the use of the system for the upcoming elections – citing the fact that deciding in favour of the system's use had a much higher threshold than deciding against, and that threshold had not been reached. They asked for more time to further examine the system, and their second report was released at the end of 2006 [81]. In that report they outlined the changes they would require to the system before they could endorse its use for Irish elections. A notable absence from this list is the requirement that a VVAT (see section 3.5) be added to the system, even though the report clearly states that

> "**Since the chosen electronic system does not have this facility [VVAT]**, and while it does provide features to facilitate a degree of independent audit in its vote counting function, together with features that facilitate audit at the administrative level and confirmation of statutory compliance, **it is not subject to any meaningful independent audit of its vote recording function**. Thus the paper system is superior in this respect."
> (emphasis added) [81, page 154]

After the release of the final report of the CEV, statements from the then Minister for the Environment Dick Roche TD indicated that he intended the

system to be used for Irish elections at some point in the future (though it was unclear whether he intended to implement all of the changes indicated in the report). The current Minister for the Environment John Gormley TD has not declared his plans for the system (the Green party, of which he is a member, has expressed strong opposition to the system [82]) but the Fianna Fail/Green Party program for government did include the establishment of a permanent Electoral Commission (as recommended by the Council of Europe [83]) which would presumably be responsible for such decisions.

Here we evaluate the procurement of e-voting in Ireland against the list of best practices laid out in section 4.2.1:

1. The introduction of e-voting did not begin with a clear *Vision*. Reasons cited publicly for the use of e-voting have repeatedly changed. In the beginning the system was supposed to save money (this argument was not based on any actual evidence) and improve Ireland's image as a technologically advanced country. It was later argued that the system would help voters to accurately record their votes. If indeed this had been part of the original vision it is likely that more care would have been taken to procure a system with a good user interface.
2. The Comptroller and Auditor General's report of 2003 indicates that a *business case* was developed, but that "the project should have been subject to a more rigorous cost/benefit analysis in view of the scale of the financial commitments involved." [84, page 66] There is no evidence that any *risk assessment* was developed before the one produced for the CEV [85] (which itself is not a formal risk assessment – it does not clearly define the terms used, nor does it justify assessments made).
3. The existence of ICTE and the resistance to the project from opposition parties makes it clear that the project did not have *Buy-in from all stakeholders*. Every voter and every politician is a stakeholder in election administration. While one cannot expect the support of 100% of voters (and therefore it is difficult to determine what buy-in from voters looks

like) it is hardly too much to expect that such a project would have cross-party support.

4. The *Requirements* laid out in [86] were totally inadequate for the development (or procurement) of an e-voting system which would safeguard Irish democracy. In fact, the requirements for e-voting have never been satisfactorily defined. See chapters 5 and 6.
5. The *Clarification of roles and responsibilities of key players* for this project can certainly be described as failed. The contracts which were signed between the vendor and the Minister for the Environment give the Irish Government no comeback from the vendor should anything go wrong with the system, amongst other issues [32].
6. There appears to have been a significant lack of *ICT project management expertise*. The e-voting project was run by civil servants within the franchise section of the Department of the Environment. Such organizations have notorious difficulty retaining trained and experienced ICT staff [80]. This forced the staff involved to rely on information and advice from the vendors of the system. Some of the pitfalls of this are discussed below (section 4.3.3). Another serious consequence was the lack of adequate testing of the system. For example, prior to the work of the CEV no end-to-end testing was carried out on the system, and there was no examination of risks posed by authorized personnel. The Department staff did not understand what constituted adequate testing, because they lacked the necessary expertise.
7. *Single responsible owner*: Unknown.
8. From reports about the counting software it appears that it was not developed modularly; in fact, even code for different countries seems to be mixed up together [87]. The incremental approach taken for deployment – running ever expanding pilots – was a good one, but it was cut short when the Minister for the Environment decided to move from using the system in 3 and then 7 constituencies straight to using

it in all 43. It is important that one is not blinded by the success of early increments. For instance, the system was never used for more than one election type simultaneously before the proposed use nationwide in 2004.

9. *Regular oversight* of the project could have highlighted some of the other errors that occurred in time for something to be done. Instead, a sense that the project could not be halted or slowed down seemed to prevail [88].

10. The lack of *Contingency arrangements* for the project [84] is indicative of the excessive level of trust officials had in the system. A total of 7,321 machines were bought [84], which is not even enough to cater for normal usage, never mind the need for spares. It also appears that there was no adequate planning for how spares would be transported to the polling station where they were needed. Planning should also have been in place for the eventuality of needing to return to paper (e.g. catastrophic system failure, contract/legal issues with vendor). Paper ballots were successfully used in the 2004 elections, at short notice, but it was to be the first use of the system for most constituencies. Returning to paper after several years of e-voting, even for one election, would be considerably more difficult. Much of the existing expertise and knowledge amongst election officials, and the processes in place to run elections, could be quickly lost.

4.2.3 Example Project: PPARS

The procurement of PPARS (Personnel, Payroll and Related Systems) began in 1997. It was intended to provide a centralized system for the administration of human resources within the health services. After several years of exceeding its budget without providing expected functionality, the project was examined by the Comptroller and Auditor General (C&AG) in 2005. It was suspended in October 2005 pending a review. The report of the C&AG describes some of the

failures that led to the serious problems encountered by the project. All quotes and data in this section are from that report [77].

Here we evaluate the PPARS project against the list of best practices laid out in section 4.2.1:

1. There was a "failure to develop a clear vision of what strategic human resource management actually meant for the health service as a whole and for its individual operational units" [77, page 9].
2. Two appraisals carried out on the system in 1998 and 2002 "fell short of the requirements for a full business case for the project." [77, page 11] "The first did not adequately address the costs and benefits of the proposed approach while the second was seriously deficient with regard to its analysis of costs" [77, page 11] and "the [C&AG's] examination found that estimates prepared in the course of the project were not supported by detailed cost analysis and were mostly framed in the context of funding requests." [77, page 11] It does not appear that a *risk analysis* was developed in the early stages of the project. Risks were identified in a report in 2002 "which do not seem to have been taken on board sufficiently." [77, page 88]
3. There was a "lack of readiness in the health agencies to adopt the change management agenda." [77, page 9]
4. There was an "inability to definitively 'freeze' the business blueprint or business requirements at a particular point in time in accordance with best practice." [77, page 9]
5. "The manner in which external consultants and contractors were engaged to work on this project was unsatisfactory." [77, page 90] For example: the "arrangements with Deloitte did not incorporate an appropriate sharing of risk. In practice, the state carried all the risk. There is evidence of a lack of clarity regarding the role of Deloitte." [77, page 12]
6. The over-reliance of the project on consultants indicates a distinct lack

of internal expertise. Between 1998 and 2005 €57 million was spent on consultants and contractors out of a total of €131 million (43.5%). A budget drawn up in 1998 had allocated €20 million to consultants out of €109.5 million (18.3%).

7. The C&AG's report also cited "[a] complex governance structure defined by a consensus style of decision-making." [77, page 9] There was a nominal *single responsible owner* but "this person did not have the power to make and enforce decisions across the range of autonomous agencies" [77, page 11] involved.
8. There was a "failure to comprehensively follow through on its pilot site implementation strategy before advancing with the roll out to other [Health Service Executive] areas." [77, page 9]
9. "The project was reviewed by external consultants on five occasions. None of the reviews provided a meaningful challenge to the case for continuing with the project. In fact, the reviews tended to justify the continuation of the project although a wider review scope might have focused attention on the escalating cost, reduced scope and the risks to timeliness and coherence." [77, page 13]
10. Since the project was suspended in 2005 pending a review, we must assume that it was possible to function without it. It is not clear, however that *contingency arrangements* were a part of the project.

4.2.4 Example Project: Revenue Online Service

The Revenue Online Service (ROS) is certainly a success-story amongst ICT projects in the Irish public sector. The project won numerous awards, and has attracted delegations from many parts of the world [89, 90]. It is a system which allows businesses and individuals to file and pay their taxes securely online.

In their paper called "Revenue On-Line Service (ROS), Ireland's eGovernment Success Story", Sean Cosgrove and Conor Hegarty outline some of the factors they see as having played an important role in that success. [90]

Throughout the (ongoing) life of the project the maxim 'Think Big, Start Small, Scale Fast' has been used as a guiding principle. The vision for the project was always ambitious, but early development focused on getting basic functionality working correctly. Since then, the project has rapidly expanded to cover more and more transactions.

As discussed in section 4.2.5, this project is the least well described of the three simply because it was the most successful. More than half of the data points listed below were acquired through direct contact with ROS staff.

Here we evaluate the ROS project against the list of best practices laid out in section 4.2.1:

1. An ambitious, but clear *Vision* was developed at a very early stage (figure 1 [90]) in the project.
2. A *business plan* was prepared including a *risk analysis* and a *cost/benefit* analysis.
3. Buy-in from all stakeholders and corporate commitment (which "involves making the best resources available on request") are listed by Cosgrove and Hegarty as key to the project's success.
4. *Requirements*: Unknown.
5. *Roles and responsibilities* were clearly defined from the start.
6. *ICT project management expertise*: Unknown.
7. One of the first steps taken in the project was the appointment of an ROS Strategy Manager.
8. *Modular and incremental approach*: "additional taxes and duties are added to the service regularly with two or three major releases every year."
9. *Regular oversight* : Unknown.
10. *Contingency arrangements* were in place to ensure that reverting to paper remained an option.

4.2.5 Comparison

Table 4.1 gives a summary of these reviews.

Table 4.1: Best practice use in three public sector ICT projects

	Principle	E-voting	PPARS	ROS
1	Vision	✗	✗	✓
2	Business case	✓	✗	✓
	Cost/benefit	✗	✗	✓
	Risk analysis	✗	✗	✓
3	Buy-in from all stakeholders	✗	✗	✓
4	Requirements	✗	✗	?
5	Clarification of roles and responsibilities of key players	✗	✗	✓
6	ICT project management expertise	✗	✗	?
7	Single responsible owner	?	✗	✓
8	Modular and incremental approach	✗	✗	✓
9	Regular oversight	✗	✗	?
10	Contingency arrangements	✗	?	✓
	Success?	Postponed	Postponed	Award winning

Unfortunately this data can only hint at the significance of these elements of best practice; it cannot tell us which are necessary and which sufficient nor can it give us any idea of the importance of these principles relative to one another. Our survey is limited in scope, both in terms of the number of projects and in terms of the selected principles.

The data is further limited by the information that is publicly available on these projects. It is notable that the most successful project of the three examined (ROS) is the least well described. Both PPARS and the e-voting system were scrutinized by the Comptroller and Auditor General [77, 84] because they had in some sense failed, and the results of that examination are publicly

available. ROS on the other hand has been successful, and therefore never subjected to such scrutiny. A survey of public sector ICT procurement along the lines of the Standish Group's survey of commercial projects [75] could be extremely useful in mitigating this dearth of information. Data gathered could be anonymized to prevent embarrassment where projects have failed, while allowing others to learn from those failures.

4.2.6 Mitigation Strategies from the UK

In addition to the use of best practice, what other strategies might be used to reduce the effect of this barrier to the successful use of ICT by public bodies (and hence to the successful use of e-voting)?

As part of an extensive program to investigate and improve governmental procurement of ICT systems, the UK set up a centralized body called the Office of Government Commerce (OGC) to oversee the process [91]. Its responsibilities included "Measurement and benchmarking of procurement performance across Government", "Undertaking periodic procurement reviews of procurement performance, skills and capabilities with Departments" and "Catalysing the spread of best in class procurement practice", amongst others [91]. Three of the most broadly applicable and useful strategies are described below. For a more detailed description of these measures, and a description of the positive effects they have had on ICT procurement in the UK, see [79].

Centres of Excellence

Centres of Excellence were set up in the UK "as a means of establishing the 'right structures and culture' for successful programme and project delivery within departments", with a target for all departments to have one by June 2003 [79, page 30]. A centre of excellence that has the resources to be able to attract a high calibre of staff [80] provides a focal point for comprehensive oversight and a repository for knowledge and expertise. It can also assist in embedding key practices within the department [79].

Gateway Reviews

Gateway Reviews are one way of implementing regular oversight (see section 4.2). They were introduced in the UK by the OGC in 2001. The National Audit Office (NAO) define Gateway reviews as "Reviews of civil Central Government procurement projects and programmes at key decision points by a team of trained reviewers, independent of the project team" [79, page 74].

The six gateway reviews used by the OGC (as defined in [78]) are:

Gateway review 0 $\longrightarrow$ Strategic assessment

Gateway review 1 $\longrightarrow$ Business justification

Gateway review 2 $\longrightarrow$ Procurement strategy

Gateway review 3 $\longrightarrow$ Investment decision

Gateway review 4 $\longrightarrow$ Readiness for service

Gateway review 5 $\longrightarrow$ Benefits evaluation (repeated as required).

A project is not allowed to proceed beyond a given gateway until reviewers are satisfied with its progress. This is a useful strategy for preventing projects from spiralling out of control. It also enforces certain other aspects of best practice; for example, a project must have a viable business case in order to pass gateway 1.

Gateway reviews are also recommended by the C&AG in his report on the PPARS system, stating "Gateway reviews need to be built into the approval process for major ICT projects and should be independent of the project team." [77, page 89]

Red-Amber-Green

In 2002, colour coding was introduced into the gateway review process in the UK. The meanings [79] of the three colours used are:

Red – To achieve success the project team should take action immediately.

Amber – The project should go forward with actions on recommendations to be carried out before the next OGC Gateway Review of the project.

Green – The project is on target to succeed but may benefit from the uptake of recommendations.

This gives a clear indication of the level of concern held by reviewers of the project.

4.3 Legal Implications

The introduction of technology is often seen as necessary to progress, and therefore in some way unstoppable. All too often, however, little consideration is given to the new challenges – legal, political and sociological – posed by technology. Besides the outstanding fundamental technological issues discussed in the previous chapter, and the lack of compliance with best practice in the public sphere discussed above, there are also other very serious barriers to the successful use of e-voting.

The introduction of e-voting raises questions about the legal position of the electoral rules, the electoral results and the vendors of the system. It is vital that the law moves to meet the new challenges posed by introducing new technology. The legal position of Independent Testing Authorities (ITAs) is discussed in section 4.4.

4.3.1 Electoral Rules

The Irish Electoral Act [92] 1992 is the current legislation governing the rules by which votes should be counted in Irish elections. The act outlines the particular form of Proportional Representation - Single Transferable Vote (PR-STV) mandated in the Irish constitution, including the specific rules to be followed during counting. Thus the Irish Electoral system was completely described in law.

Since the introduction of enabling legislation for e-voting in 2001, the rules for deciding Irish elections are no longer necessarily dictated solely by the relevant law. Where e-voting is used, the software that counts the votes is in

fact the final arbiter. If the e-voting system chosen for use in Ireland were used, under current agreements between the Irish Government and Nedap/Powervote, this would lead to an extraordinary situation. The count rules would no longer belong to the Irish people, no longer be public and would be subject to change without legal procedures (when the software is modified or updated).

The Electoral Law has been interpreted by the Department of the Environment in a document called the "Count Rules" [93]. This document served as the user specification for the programmer of the Nedap/Powervote count-software. No other documentation exists except the application itself which is in some 150 to 200 modules of Borland Delphi code. The overall codebase is 200,000 lines of code originally established for use in the Netherlands [94, 95]. It has been modified for use in Germany, in Ireland, in the UK and in Brest, France. Reviewers' comments [87] indicate that there is no separation between the UK and the Irish code base for certain modules. This is a very dangerous practice since the electoral rules are completely different in the two countries – the UK uses first past the post whereas Ireland uses PR-STV.

4.3.2 Electoral Results

In most jurisdictions the law required that paper ballots be kept for a minimum period (in Ireland, six months) in provision for disputes arising. In such cases, a court could require that the paper ballots be re-examined. A similar provision has been made within the electronic system, but as the only records of votes cast would be electronic, the only evidence which could be presented in court would be electronic evidence (or a printout of electronic evidence, which is of course no more reliable). It is difficult to have electronic evidence admitted in a court of law [96] and rightly so, since it is so much more easily manipulated and tampered with.

The legal position of electronic ballots has not been tested in any Irish court, nor to our knowledge in any European court, but the possibility that results could be successfully appealed on this basis should certainly be considered.

4.3.3 Vendors

E-voting systems are different from other software and hardware products, because of the vital role they play in the democracies where they are used. It makes sense therefore that the vendors of such products should be treated differently. The commercial interests of those companies cannot be allowed to take precedence over democratic interests.

Perhaps the most obvious conflict between these interests is in the matter of trade secrets. Normal practice within the software industry is for software developers to keep the source code for their products secret. The same applies to all the documentation produced during the development process, including design documents, and test strategies and results.

If the public is to be satisfied that the system was well-developed and does what it is supposed to do, this documentation must be made publicly available, so that those with the skills to examine its quality have that opportunity. While this approach prioritizes public interests over private, it is not all negative for the company. There are many successful businesses today who use the open source model [97].

A further conflict of interest is this: if there is a flaw in the system it is very much in the public interest that such a flaw be discovered and corrected. This would be bad publicity for the vendor, however. Unfortunately it is not safe to assume that a business will put the correct working of democracy ahead of its own reputation. Therefore it must be made as difficult as possible for vendors to deny or ignore flaws in the system. Again, this requires the highest level of public scrutiny.

The ownership of source code and similar materials (such as design documentation) is another important issue where standard industry practice conflicts with the best interests of the public. Usually software vendors sell licences to use pre-compiled versions of their product and retain copyright of the code itself. However, if the source code were owned by the people instead of the vendors, we would be protected from at least two extremely undesirable

scenarios: the case where a vendor or vendors go out of business, and the possibility of vendor refusing to comply with the government's wishes. First, should the vendor go out of business, the future of our e-voting system would be considerably more secure. There being no doubt as to the ownership of the code, the government would be considerably freer in their choice of a replacement vendor. Second, since the government would be in a position to switch to a competitor, the vendor could not make unreasonable price increases or other undesirable policy changes, nor could they refuse to make alterations/updates to the software.

The contract between Nedap/Powervote and the Irish Government explicitly retains ownership of the embedded software in the voting machines for Powervote.

> *Clause 10.1.2 Notwithstanding the vesting of ownership of the Ordered Equipment in the Customer, the Customer and Returning Officers acknowledge that the Embedded Software remains subject to a licence granted by the Suppliers and no transfer of ownership of the Embedded Software shall occur, including but without limitation any Intellectual Property Rights in the Embedded Software. The Customer and Returning Officers acknowledge that the Embedded Software is the Confidential Information of the Suppliers. [98]*

This is a reversal of the position laid out in the original request for tenders.

> *Clause 8.4 All software paid for and developed to Department's specification will be the property of the Department. [86]*

The Irish Government had to provide an indemnity to the Commission on Electronic Voting in case the source code it examined fell into the hands of competitors [99]. To have allowed such a situation to develop shows a significant failure on the part of the Department of the Environment to set out clear expectations that it should own any software developed for elections. The cost of the software is estimated to be €467,000 for the counting system.

It is vital that these potential conflicts of interest are recognized and addressed by those introducing e-voting. It is not good enough for a government

to rely solely on the advice, opinions and information provided by vendors. These must all be scrutinized by experts with no personal or commercial interest in the system.

The establishment of Centres of Excellence should provide decision making bodies with enough expertise to ensure that their own interests (and thereby the interests of those they serve) are not secondary to the interests of vendors. As illustrated by the PPARS experience, hiring consultants to advise does not necessarily solve this conflict of interest.

4.4 Verification and Maintenance

The final organisational issue discussed here is the verification of e-voting systems against requirements, and the maintenance of both the systems themselves, and the standards where those requirements are defined. We discuss the considerations that arise for the *·responsible election authority·* with respect to evaluation (section 4.4.1), maintenance (section 4.4.2) and Independent Testing Authorities (section 4.4.3).

The problem of defining requirements for e-voting will be discussed in detail in chapters 5 and 6, but identifying requirements is not enough. Those requirements must be fit for purpose: they must meet users' needs, and they must be genuinely useful for improving and validating the systems in question.

One serious failing of many existing requirements catalogues for e-voting is the lack of provision for verification and maintenance. For instance, of the catalogues mentioned in chapter 6, the CoE requirements call for "certification processes" [40, page 20] without going into any detail about those processes. They make no mention of maintenance other than a brief note stating that the CoE "may look again at this issue two years after the adoption [of these requirements]". (The requirements were adopted in 2004). The PTB requirements [38] explicitly avoid the evaluation process. Again, the only reference to maintenance is brief: "[f]uture technical developments and new

experience gathered in general as well as from particular threats may lead to amendments or extensions of this catalogue."

The development of a standards document should never be considered "complete" since technology is constantly changing, as is our understanding and expectation of that technology. Standards documents must make provision for their own maintenance in such a way that the verification based on them is not compromised. They must also make provision for the maintenance of the *·e-voting systems·* covered (such as identifying under which circumstances recertification becomes necessary) as vulnerabilities come to light, requirements change, and new technology becomes available.

4.4.1 Evaluation

In [42] we presented an earlier version of the requirements in chapter 6. In that paper we proposed that the security and assurance requirements could be evaluated according to the Common Criteria (CC) methodology. However, as Mercuri has pointed out [30], the CC does not provide a mechanism for dealing with conflicts within requirements such as the conflict between the need for secrecy and accuracy in e-voting (see chapter 3). Further, the CC has recently come under criticism for being costly, slow, and focusing too much on documentation rather than the product itself, among other things [100]. Here, instead, we attempt to identify appropriate testing methodologies. In table C.6 at least one of the following testing methodologies is assigned to each of the requirements developed in chapter 6.

Usability Testing

Usability is a concept that is difficult to define precisely. Usability requirements are at risk of being defined vaguely, and therefore inadequately tested (see subsection 4.4.3). This is the reason that terms such as user-friendly and understandable have been marked as *·responsible election authority·* variables in their respective requirements (meaning they must be defined within a specific

context). In fact, usability cannot be defined without reference to the users themselves. Therefore evaluation against usability requirements necessitates the use of sociology-style experimentation with suitably representative test subjects [101]. Usability testing is an established discipline in its own right [102].

1. The *·e-voting system·* SHALL be subjected to usability testing.

Election Observation

Organizational requirements are unusual, in that they cannot be met by the system outside the context of an actual election. They do not describe properties of the system in the abstract, but properties of the system as it is implemented on election day. However, they are more than mere guidelines for the *·responsible election authority·*; they are very important assumptions about the environment which must be met to ensure that the system as a whole meets the broad election principles (see section 1.6). Therefore someone must check that these requirements are being met while the election is being run. We propose that the work of existing election observation organizations [103, 104] can be extended to cover these requirements, though teams will have to include computer science experts in order to make judgement calls on certain requirements. For example, a minimum level of expertise would be required to judge the adequacy of the cryptographic key management policy called for by Org_2. The Carter Center has recently published a draft methodology for the observation of new voting technologies [105].

2. Election observers SHALL check that organizational requirements and relevant assurance requirements have been met. Where a VVAT is implemented, observers SHALL check that VVAT-requirements have been met.

Manufacturer Compliance

Certain requirements seem simple to evaluate since the ·*manufacturer*· either complies or does not comply. However, it is vital that the quality of the documentation produced by the ·*manufacturer*· is also evaluated. For example, the ·*manufacturer*· cannot truly be said to have met requirement Assur_7 unless the testing conducted meets accepted best practice. We have assigned the responsibility for ensuring compliance to the ·*independent testing authority*·.

3. The ·*independent testing authority*· SHALL ensure that the ·*manufacturer*· complies with all relevant requirements and SHALL assess the quality of all documentation produced.

Other Tests

There are many other types of testing that should be carried out on an ·*e-voting system*· beyond that testing undertaken by the ·*manufacturer*· (Assur_7). These include:

Code reviews - examining the source code of the various software components of the system for adherence to accepted best practice (e.g. readability and modularity).

Functionality testing - testing the functionality of components to ensure they meet individual requirements.

End-to-end testing - testing the whole system as it will be used during elections. This kind of testing is vital to ensure that all components interact as expected and that the system as a whole is working correctly.

Environmental testing - testing the ·*election devices'*· resistance to being dropped from a height and to extremes of temperature, humidity, and so on.

4. The ·*independent testing authority*· SHALL conduct code reviews, functionality testing, end-to-end system testing and environmental testing to ensure that security, functional and audit requirements are met.

Red Team Testing

The term "Red Team" originates from the name for the opposing force in military simulations. These simulations allow commanders the opportunity to test plans and concepts against an opponent that poses no actual threat. The Red Team's objective is to beat the commander's strategy so that the strategy can be improved before being tested against a real enemy. The term has come into common use in computer security for a type of testing also known as penetration testing. The objective is similar: the Red Team must have access to the system in a realistic scenario and attempt to break its security. It must be noted that the failure of a Red Team to break the security of a system does not necessarily mean that a real attacker would also fail [106]. To paraphrase Dijkstra [49], testing can only show the presence, never the absence of vulnerabilities. However, Red Team testing can be a very effective way of discovering vulnerabilities, and if the Red Team is competent, can increase confidence in the system.

5. Red Team testing SHALL be employed to attempt to discover security flaws in the *·e-voting system·*.

SHOULD Requirements

As discussed in section 6.3, some of the requirements allow for a certain amount of flexibility. They use the keyword SHOULD to recognize that it may be undesirable or infeasible to meet that requirement in certain circumstances. Those circumstances must always be made explicit, however, since the requirements have been included for a reason, and should not be simply dropped because they are inconvenient.

6. For each requirement containing the keyword SHOULD where the SHOULD clause is not met, the *·responsible election authority·* SHALL ensure that an explicit justification is provided. The *·responsible election authority·* and election observers SHALL assess those justifications for validity.

4.4.2 Maintenance

Error Correction: Procedures and Responsibilities

Since the whole development process is in human hands, it is prone to human-error. This applies to both the requirements and the systems they describe. Errors will almost certainly be found (and will certainly exist) in the requirements themselves, and in design, implementation, testing and use of systems. Therefore we must design procedures for dealing with these errors, including the identification of responsible parties.

Timing is very important. If a grievous error is discovered between elections, there may be time to deal with it before the system must be used again. There may be much more serious consequences if it is discovered just before an election, or worse, just after an election has been completed. Someone must decide how serious a given error is, and how it should be dealt with in the short, medium and long term. The question of who must make those decisions is discussed in section 4.4.3 below.

Other Types of Change

Error discovery is not the only agent of change for requirements and systems. For example, the introduction of new legislation (national, transnational or international), or new elections types, may have direct consequences. The fact that so many types of legislation and sources of requirements exist raises the possibility of conflicts and inconsistencies arising (apart from the fundamental requirements conflict identified in chapter 3). The development of

new technologies may also necessitate the modification of requirements and/or systems.

A Long Term View of Testing

Whenever a system changes, whatever the surrounding circumstances, it must be tested and certified again. If the system of evaluation and testing has been well-engineered, however, it may not be necessary to "begin again" with every modification. If the *·e-voting system·* under examination has been subjected to critical-system development methods, we should be able to make use of test re-use and regression testing (testing for unintended consequences of software changes) to shorten the re-certification process.

The design of the evaluation process must make provision for the ownership, legal status, and expected lifetime of the system and its components as well as the expected frequency of use and time between tests.

4.4.3 Independent Testing Authorities

The responsibility for these questions will ultimately rest with the *·responsible election authority·* and their nominated Independent Testing Authority (ITA). International standards exist in a wide range of disciplines such as telecommunications, medicine and transport. These standards are documented and enforced by their respective standards bodies. Additional rigour can be added to this process by requiring accreditation for the responsible agencies themselves.

However, for such accreditation to be meaningful it must be possible for these agencies to do their job – to measure systems against their requirements. That means that the requirements must be expressed in a testable way. Jones has identified two weaknesses in the ITA process as used in the US [107]: first, requirements that are vague or subjective are more difficult to test, and ITAs may give them minimal attention; and second, if a requirement is not made explicit in the specification, no matter how obvious it may seem, the ITA cannot be expected to test for it.

It must also be possible to determine whether a given agency can do the job. Clearly then requirements documents must not only say what standards are to be met, but must also state the minimum requirements expected of any testing agency. Without this additional safeguard one increases the risk that a system is procured, is passed for use by an independent agency, and 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. ITAs must be competent, independent and objective, and they must be seen to be so.

The whole system of testing and accreditation must be designed in such a way that ITAs have more incentive to fail bad systems than to pass them, and to pass good systems than to fail them. The results of their tests should be made public, to increase public confidence in those results. It is also vital that provision be made for de-certification of systems that have been shown to be faulty [108].

It is worth noting that cost may have a direct effect here. If certification is expensive for vendors, and maintenance of their systems requires recertification, there is a risk that vendors will not make necessary changes to their systems (to avoid recertification) or will make changes without having the systems re-certified.

4.5 Summary

Public bodies appear to have particular difficulty in procuring high quality ICT systems. There are various reasons for this situation, and various strategies which might help. The use of best practice techniques appears to have a positive effect on project outcome (though the evidence presented here is observational). The techniques proposed by the UK's Office of Government Commerce are based on more available evidence and appear to be having positive effects since their introduction there. Any success in improving ICT procurement in general should naturally increase the chances of successful procurement of a high quality

e-voting system.

There are legal implications specific to the introduction of e-voting (as opposed to ICT systems in general) that result from the nature of both the technology in question and the electoral system. The legal implications for the electoral rules, electoral results and system vendors must be carefully examined by the responsible electoral authority when procuring an e-voting system.

Finally, standards for e-voting must make provision for verification and maintenance (both of the systems and of the standards themselves). Otherwise, the natural evolution of technology and law will become a barrier to the successful use of e-voting.

Chapter 5

Requirements for E-voting: Top-down

Before we can ensure that any system behaves correctly, we must define what "behaving correctly" means for that system. In other words, we must identify our requirements for that system. The lack of an adequate requirements definition for e-voting prevents us from determining the quality of a given system, and is therefore a barrier to the use of e-voting for critical elections.

There are certain types of errors that are common in requirements specifications, and that have a negative effect on their usefulness for developing and testing systems (see section 5.3). In this chapter we analyse a specific e-voting requirements specification for the presence of such errors, and make a proposal for how the number of those errors could be reduced. For that purpose, we took a top-down approach (described in section 5.5 below). The resultant requirements specification is not proposed as a finished product, rather it is intended to highlight specific examples of the type of problems encountered in existing requirements specifications. Chapter 6 will broaden the discussion to other requirements catalogues, and propose another set of requirements developed in a bottom-up fashion.

5.1 The Council of Europe Standards for E-voting

The Council of Europe (CoE) is an organization 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." [109]

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

The *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting* [110] 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." [110]

The document they produced [40] (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 then enumerated — 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* [83], which was produced by the Venice Commission [1].

[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.

This inter-related set of complex documents is analogous 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 standards, with focus on arriving at a document that can be usefully applied at the requirements capture stage of e-voting development.

In September 2004, the CoE's *Committee of Ministers* officially adopted the standards. This trans-national effort was a step in the right direction, but the set of standards developed is seriously flawed.

5.2 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 chapter. 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.

The 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.

5.3 A Software Engineer's View

In [111] Meyer lists the "seven sins of the specifier" – common requirements engineering mistakes that have a negative effect on the usefulness of specifications that exhibit them. In this section we introduce the same concepts phrased positively as 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, does it have contradictory standards, and do the standards contradict the other set of instruments that precede the document? (Meyer's "sins" against consistency are 'contradiction' and 'ambiguity'.)

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. (Meyer's "sin" against completeness is 'silence'.)

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. (Meyer's "sins" against correct levels of abstraction are 'over-specification' and 'wishful thinking'.)

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. (Meyer's "sin" against clarity is 'noise'.)

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. (Meyer's "sins" against maintainability are all those listed above, plus 'forward-reference'.)

5.3.1 Consistency

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

> "In this recommendation the following terms are used with the following meanings: [...] [40, page 8]"

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 register.

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; this 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 realized 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 related standards instruments (mentioned in section 5.1) 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.

The glossary of election terms in appendix A was developed to help avoid this kind of confusion and inconsistency.

5.3.2 Completeness and Scope

Many e-voting systems allow for multiple *·polls·* to be run concurrently and for a voter to *·cast·* 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." [40, page 13]

This requirement is adequately covered in the CoE's own *Code of good practice in electoral matters* [83] 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.

5.3.3 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." [40, page 15]

5.3.4 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." [40, page 15]

5.3.5 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 5.6.2 for an example.

5.3.6 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.

5.4 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.

5.4.1 Standards, Analysis and Requirements Capture

Analysis is the process of maximizing *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 formalized, 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?

5.5 Restructured Requirements

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 election principles they aim to uphold: Universal, Equal, Free, Secret and Direct Suffrage. (See section 1.6 for our definitions of these principles). They could have taken this classification further, however, and divided all the standards according to those categories. That is how the requirements catalogue that follows was first developed; changes were then made as necessary (see section 5.6).

This approach has several advantages. First, the five principles have been developed over a long period of history to capture almost 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. For this reason we added "trusted suffrage" to the list of election principles. However, 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.

The following sections contain our modified and restructured version of the CoE standards. In the text below, italicized numbers in parentheses refer to requirements in the standards document [40] (the original requirements have been included here as appendix B). Where a requirement in the original document was deemed to cover more than one concept, it was split (see section 5.6.1); these sub-requirements are referred to by letters (e.g. *(61b)*) and the divisions are made explicit in appendix B with annotations in the requirements themselves. Each section begins with the definition of the election principle under consideration as per section 1.6.

5.5.1 Universal Suffrage

> All human beings have the right to ·*cast*· a ·*vote*· subject to certain conditions, for example age and nationality.

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 maximize ·*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 interface*·, registration *(2)* and administration) shall follow best practice to maximize 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 interface*· 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 maximized, 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 practise 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)*

5.5.2 Equal Suffrage

> Each ·*eligible voter*· has 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 ·*voters' 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)*

5.5.3 Free Suffrage

> The ·*voter*· has the right to form and to express his opinion in a free manner, without any coercion or undue influence.

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*[2] 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

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

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)*

5.5.4 Secret Suffrage

> The *·voter·* has the right, and the duty, to *·cast·* his *·vote·* secretly as an individual, and the state has the duty to protect that right.

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 [112].

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 *·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).*

5.5.5 Direct Suffrage

> The results of the *·poll·* SHALL be determined by the *·votes· ·cast·* by the *·voters·*.

The committee did not categorize any of their standards under "direct suffrage" saying that it "does not call for special attention" [40, page 26]. 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" [40, page 25], 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)* [83, 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 [112]

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 authorized 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)* [3]

[3]The very important requirement for a full risk assessment is not included as a standard by

2. Components' access to time sources shall be strictly limited on a "need to know" basis [112, 30]. *(contrast with 84, see section 5.6.4)*
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 [112].
   (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. 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

the committee, but is mentioned in the introduction to Appendix III of the CoE document. See footnote on page 156.

requirements as the original system. *(70b)*

(b) Technical and organizational 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* [40, page 37] *, 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·*, *·voters' 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. [113]
   (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 positions. *(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)*

5.5.6 Trusted Suffrage

> The *·eligible voters·* must trust that these principles have been upheld.

The results of a *·poll·* 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 maximize *·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)*.

5.6 Analysis of Restructuring

Rather than giving a detailed discussion of all decisions made during the restructuring process the following sections highlight certain categories of decision, giving examples of each. Due to the faults discussed in section 5.3, 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 parenthesized numbers in italics (e.g. *(39)*). We will refer to standards in our restructured set using numbers in bold (e.g. **19.3d**).

5.6.1 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." [40, page 16]

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. The example above 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.

5.6.2 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 ·*voters' 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." [40, page 9]

> *(6)* "The e-voting system shall prevent any voter from casting a vote by more than one voting channel." [40, page 9]

> *(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." [40, page 13]

> *(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." [40, page 13]

> *(82)* "Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured." [40, page 17]

5.6.3 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." [40, page 17]

We rephrased it as follows:

> **20.5** "Incident levels shall be defined and appropriate responses identified."

5.6.4 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." [40, page 18]

As Jones [112] and Mercuri [30] 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."

5.6.5 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."

5.6.6 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." [40, page 12]

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" [112]. 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 [9, 114].

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" [40, page 14]

is unclear, particularly in light of the presence of

> *(34)* "The e-voting system shall ... keep [the votes] sealed until the counting process." [40, page 12]

(67 and 68) refer specifically to the use of EML. While the use of open standards can be advantageous (see point 120 in [40, page 48]) 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" [40, page 18]

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)*.

5.7 Evaluation

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.

The revised requirements presented in this chapter are not intended as a replacement for the CoE standards, however they do contain improvements. Each requirement encapsulates a single concept which reduces the risk of contradiction and ambiguity, and makes the task of testing against the requirements easier. The requirements are organized in a logical and consistent manner, under the election principles defined in section 1.6. Grouping them together like this helps to reduce the risk of repetition, redundancy and contradiction because any clashing requirements should be close to one another and so easier to spot. It also makes the whole document more human-readable, and therefore more easily maintained.

Our glossary of terms is more extensive than the one included in the CoE document. Highlighting the use of glossary-terms typographically has made it easier to check that they are used consistently. Requirements were added where we discovered incompleteness (e.g. **19.3d**), and removed where they were deemed to be outside the scope of the document (e.g. *(36)*). Cases of over- and under-specification (e.g. *(66)* and *(65)* respectively) were removed or rephrased. Cases of redundancy and repetition were reduced by merging requirements (e.g. **5** summarizes *(5b)*, *(6)*, *(41)*, *(44)* and *(82)*).

However, our specification also exhibits some undesirable traits. For instance: there are still some requirements that are quite aspirational (e.g. **7**); it is not always clear where responsibility lies for ensuring compliance with a given requirement; the specification has not been subjected to the more rigorous checks used on the requirements presented in the next chapter. The intention in presenting this restructured requirements catalogue is to give examples of the kind of flaws common in requirements specifications, and to indicate one method that might be used to reduce the number of those flaws. In the following chapter we present a requirements catalogue developed in a bottom-up manner, and propose that it might form the basis for a future standard.

Chapter 6

Requirements for E-voting: Bottom-up

In the previous chapter we developed a set of requirements from an existing catalogue in a top-down fashion (abstract to specific). Another approach we could take is to develop a new set of requirements from scratch, and then categorize those requirements according to several abstract concepts (see section 6.3). This chapter presents a catalogue of requirements developed in this way. As with the requirements in chapter 5 this catalogue is not intended to fulfill the role outlined in section 1.5 but rather to demonstrate one method of development, though it might form the basis of a generally useful requirements catalogue.

6.1 Terminology

As discussed in section 1.1, words and phrases from the glossary (appendix A) appear ·*like this*· wherever we mean the glossary definition to apply. There were other terms used in these requirements which can only be defined within a given context, they appear underlined throughout the specification (see section 6.4.8).

The numbering of requirements is formed from a reference to the category

in which the requirement belongs (e.g. Sec_ for security requirements), and a number indicating where in the list it appears.

The key words SHALL and SHOULD (where they appear in small capitals) are used as described in RFC 2119 [4], i.e.: SHALL means that the definition is an absolute requirement of the specification, while SHOULD means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. In the case where a different course is chosen, all reasoning must be made explicit.

We use a shorthand to refer to the election principles discussed in section 1.6: universal [un] , equal [eq] , free [fr] , secret [se] , direct [di] , trusted [tr] suffrage.

6.2 Limitations of Specification

As these requirements were developed for critical elections, remote e-voting systems are not considered (see section 1.2.3). We exclude voter-registration and voter-authentication from our current analysis, since they are outside the scope of this thesis; we assume that they are implemented as per paper-only elections. Indeed, we assume that the whole system is protected by the same organizational measures used in standard paper-only elections. Therefore requirements for such measures are generally left out (e.g. we do not include a requirement that poll-workers must satisfy themselves of a voter's identity before authorizing him to vote).

The requirements in their current form are not flexible enough to cover non-DRE *·e-voting systems·*. For example, the following requirements assume the existence of a *·voting device·* as part of the *·e-voting system·*: Sec_10, Sec_12, Sec_23, Funct_1, Funct_2, Funct_3, Funct_4, Funct_5, Funct_6, Funct_7, Funct_9, Funct_10, Usab_4, Org_3, Org_4, Org_8, Org_11, Assur_1. Therefore this catalogue excludes, for example, Mark-sense (also known as optical-scan)

and digital pen election systems.

6.3 Development of Requirements

We developed the first draft of these requirements from our own experience and understanding of e-voting systems. We then iteratively compared them to various existing catalogues to incrementally improve the requirements (see section 6.5).

We developed them to have a clear, consistent phraseology. Each requirement identifies:

- The responsible entity (such as the *·manufacturer·* in Assur_2 or the *·election device·* in Sec_9)
- The degree of flexibility (requirements with the keyword SHALL are absolute, whereas for requirements with the keyword SHOULD exceptions may be reasonable. Such exceptions must be explicitly justified – see section 4.4.1)
- The action required

The majority of requirements are in the inflexible SHALL form. Of the SHOULD requirements several go on to identify a minimum SHALL clause; that is, where for whatever reason the SHOULD clause cannot be met, at least the SHALL clause must be. This is intended to identify the core requirement, while recognizing the need for flexibility in some circumstances. For example, Sec_13 states:

> The *·election devices·* SHOULD not store any data which could link the *·voter·* with his *·vote·* either during normal operation (all election phases – see figure 6.1), or in the case of exception, malfunction or system breakdown. Where such data is stored the *·e-voting system·* SHALL ensure that it is only accessible to those with appropriate authorization.

This acknowledges that in certain jurisdictions (notably the UK) the link between a *·voter·* and his *·vote·* must be retained for legal reasons. In that case, however, the information must be carefully guarded.

We have divided our requirements (section 6.4) into the following categories: security, functional, usability, organizational, assurance and audit system requirements. To make the value of the requirements clear (especially to those without technical background) each is associated with at least one election principle (universal [un] , equal [eq] , free [fr] , secret [se] , direct [di] , trusted [tr] suffrage – see section 1.6).

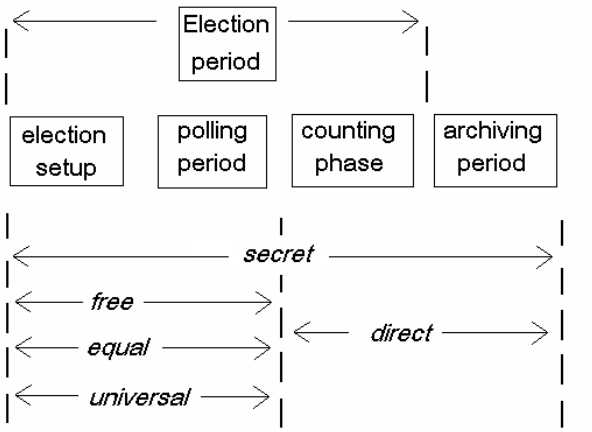


Figure 6.1: Election phases

In the process of assigning these principles to the requirements we found that many could be said to be upholding both *free* and *direct* elections, or both *equal* and *direct*. After all, it could be said that all the other principles exist to ensure *direct* elections. We decided that the best way to clarify this was to apply the principles of *free, equal* and *universal elections* to individual voters, and *direct* to collections of votes. Figure 6.1 illustrates this difference; the election phases in this diagram are further explained in the glossary (appendix A).

Some of the requirements are interconnected. Where we considered it useful to the reader's understanding of the requirements as a whole, we have made these connections explicit; cross-references in the requirement definitions are shown with the name of the connected requirement in braces (e.g. {Sec_13}).

Certain terms can only be defined within a given context, for example appropriate authorization (Sec_2) or election data (Sec_17). We have called

these *·responsible election authority· variables*. They appear underlined throughout the requirements. They must be defined by the *·responsible election authority·* before their respective requirements can be assessed. See section 6.4.8 for a list of all *·responsible election authority· variables*.

6.4 Requirements

6.4.1 Security Requirements

Sec_1 [eq] [tr] The *·e-voting system·* SHALL implement a solution to the conflict between the need for ballot secrecy {Sec_13} and the need for accuracy {Funct_6}.

Sec_2 [eq] The *·election devices·* SHALL ensure that, during the *·polling period·*, *·e-votes·* can only be added through the *·vote-casting interface·*, and only with appropriate authorization.

Sec_3 [di] The *·election devices·* SHALL prevent loss of *·election·* data during normal operation (all election phases – see figure 6.1), and in the case of exception, malfunction or system breakdown.

Sec_4 [all] The *·election devices·* SHALL implement the access control policy defined by the *·responsible election authority·* {Org_2}.

Sec_5 [all] The *·election devices·* SHALL be capable of producing comprehensive audit data.

Sec_6 [eq] The *·election devices·* SHALL provide the functionality to check that the *·e-ballot box·* is empty.

Sec_7 [eq] The *·election devices·* SHOULD provide the functionality to completely delete all *·election·* data from previous *·elections·*.

Sec_8 [un] The *·election devices·* SHALL be robust {Sec_3} against

1. power outage

2. unexpected ·*user*· activity
3. environmental effects (mechanical, electromagnetic, climatic, etc.)
4. etc.

Sec_9 [un] The ·*election devices*· SHALL provide feedback in the form of error messages in the case of exceptions and malfunctions.

Sec_10 [un] The ·*voting device*· SHALL prevent ·*voter*· interaction in the case of unresolved exceptions and malfunctions of the ·*voting device*·.

Sec_11 [un] The ·*e-ballot box*· SHALL provide the functionality to determine whether the ·*e-vote*· of the last ·*voter*· was successfully stored in the case of exceptions, malfunctions and breakdowns.

Sec_12 [se] When a ·*voter*· completes the ·*voting process*· (by ·*casting*· his ·*vote*· or cancelling) the ·*voting device*· SHALL delete any record of his ·*selections*· from display.

Sec_13 [se] The ·*election devices*· SHOULD not store any data which could link the ·*voter*· with his ·*vote*· either during normal operation (all election phases – see figure 6.1), or in the case of exception, malfunction or system breakdown. Where such data is stored the ·*e-voting system*· SHALL ensure that it is only accessible to those with appropriate authorization.

Sec_14 [se] The ·*e-ballot box*· SHALL store the ·*votes*· in a history independent way. The ·*e-ballot box*· SHALL prevent determination of ·*casting*· order, and SHALL not store any timestamp with the ·*e-vote*·.

Sec_15 [se] [eq] [tr] Components of the ·*e-voting system*· (other than the ·*audit system*·) SHOULD not have access to any time source.

Sec_16 [se] [fr] The ·*e-voting system*· SHALL prevent the calculation of results during the ·*polling period*·.

Sec_17 [di] The ·*e-voting system*· SHALL protect the integrity and authenticity

of ·*election*· data {Sec_24}.

Sec_18 [all] The ·*election devices*· SHALL be tamper-resistant and tamper-evident.

Sec_19 [all] The ·*e-voting system*· SHALL provide the functionality to accurately and reliably determine whether a given component (hardware or software) is the version evaluated and approved for use.

Sec_20 [di] The ·*e-ballot box*· SHALL be tamper-resistant and tamper-evident.

Sec_21 [se] Where more than one ·*poll*· is run in parallel, the ·*e-voting system*· SHALL prevent anyone from linking the ·*e-votes*· of a particular ·*voter*· to one another.

Sec_22 [di] The ·*counting software*· SHALL accurately calculate results using the appropriate algorithm based on all ·*e-votes*· ·*cast*· during the ·*polling period*· and only such ·*e-votes*·.

Sec_23 [di] The ·*counting software*· SHOULD run isolated from the ·*voting device*·.

Sec_24 [di] The ·*counting software*· SHALL verify the integrity and authenticity of ·*votes*· {Sec_17}.

Sec_25 [di] The ·*counting software's*· operations and data SHALL be unaffected by other applications.

6.4.2 Functional Requirements

Funct_1 [se] The ·*voting device*· SHALL not display any information about the ·*voter's*· ·*selections*· outside the ·*vote-casting interface*·.

Funct_2 [se] The ·*voting device*· SHALL prevent any emissions which might endanger the secrecy of the ·*vote*·.

Funct_3 [fr] The ·*voting device*· SHALL ensure equality of presentation of ·*ballot*·

options.

Funct_4 [di] The ·*voting device*· SHALL indicate to the ·*poll-worker*· the number of ·*votes*· ·*cast*· so far.

Funct_5 [eq] The ·*poll-worker interface*· SHALL indicate to the ·*poll-worker*· whether the ·*voting device*· is in an ·*active state*· or an ·*inactive state*·.

Funct_6 [fr] [eq] The ·*voting device*· SHALL ensure that the ·*voter's*· ·*selections*· are accurately represented in the ·*e-vote*·.

Funct_7 [fr] The ·*voting device*· SHALL accurately display the authentic ·*ballot*·.

Funct_8 [tr] The ·*e-voting system*· SHALL not obstruct the use of alternative ·*counting software*· to calculate results.

Funct_9 [un] The ·*voting device*· SHALL be capable of recording an adequate number of ·*votes*·.

Funct_10 [fr] The ·*voting device*· SHALL support an adequate number of ·*ballot*· options.

Funct_11 [un] All ·*election devices*· SHOULD be compatible with other devices (such as those used by people with disabilities) where appropriate.

Funct_12 [fr] The ·*vote-casting interface*· SHOULD provide the functionality for the ·*voter*· to:

1. change his ·*selection(s)*· before ·*casting*·
2. ·*spoil*· his ·*vote*·
3. cancel his ·*voting process*·
4. clear all his ·*selections*·.

Funct_13 [fr] The ·*vote-casting interface*· SHOULD warn the ·*voter*· when he is about to ·*spoil*· his ·*vote*· in one or more ·*polls*· {Funct_12}.

Funct_14 [all] The ·*poll-worker interface*· SHALL provide the functionality to check that the ·*election devices*· have been set up, and are functioning, correctly.

6.4.3 Usability Requirements

Usab_1 [un] The *·manufacturer·* SHALL ensure that all *·user·* interfaces on all *·election devices·* are user-friendly.

Usab_2 [un] The *·manufacturer·* SHALL ensure that all system messages provided by all interfaces are understandable.

Usab_3 [un] The *·vote-casting interface·* SHALL make provision for *·voters·* with disabilities.

Usab_4 [fr] [un] The *·vote-casting interface·* SHALL clearly indicate to the *·voter·* whether the *·voting device·* is in an *·active state·* or an *·inactive state·*.

Usab_5 [tr] The *·vote-casting interface·* SHALL provide immediate feedback to the *·voter·* regarding the status of his *·vote·* (for example, that his *·vote·* has been stored successfully in the *·e-ballot box·*).

Usab_6 [fr] The *·vote-casting interface·* SHOULD protect the *·voter·* from accidentally *·casting·* his *·vote·*.

Usab_7 [all] All *·poll-worker interfaces·* SHALL protect *·poll-workers·* from taking any action accidentally.

6.4.4 Organizational Requirements

Org_1 [tr] The *·responsible election authority·* SHALL define all *·responsible election authority· variables* (listed in section 6.4.8), prescribe the certification process (including decertification and recertification), and appoint the *·independent testing authority·*.

Org_2 [tr] The *·responsible election authority·* SHALL define (for all election phases - see figure 6.1):

1. *·user·* roles
2. an access control policy that restricts all activities to particular *·user·*-roles (taking account of the principle of separation of duties)

3. necessary administration activities
4. a cryptographic key management policy
5. incident levels
6. reporting procedures
7. provisions for election observation
8. etc.

Org_3 [tr] The *·responsible election authority·* SHALL develop procedures covering all stages of the *·election·* including:

1. secure storage of *·election devices·* at all times
2. system maintenance including software updates (from the *·manufacturer·* or from third party suppliers)
3. logistics (transport of *·election devices·*, spare *·election devices·*, accessories, etc.)
4. configuration of all *·election devices·* (including *·ballot·* details and order on *·voting devices·* and *·counting software·*)
5. checking *·election devices·* (including their configuration and that the *·e-ballot box·* is empty)
6. response to *·election device·* breakdown (including level of access allowed to representatives of the *·manufacturer·*)
7. recording of *·poll-worker·* activities, *·manufacturer·* representatives' activities, *·voting device·* state changes, system restarts, etc.
8. ensuring that any transferable-proof of the *·vote·* (that is, proof which can be used to show other people how he *·voted·*) provided to the *·voter·*, is deposited in the *·ballot box·*
9. ensuring that, during an *·election·*, *·voting devices·* are only ever in an *·active state·* during the *·polling period·*
10. closing the *·poll(s)·* including disabling *·voting devices·*
11. counting and recounting
12. comparing number of *·votes·* recorded with number of *·electors·* {Org_4}
13. *·archiving period·* including data deletion at the end {Sec_7}

14. examining audit data, and checking for evidence of tampering {Sec_18, Sec_20, Audit_5}
15. redundant storage of data
16. system breakdown
17. etc.

Org_4 [tr] The *·responsible election authority·* SHALL develop a contingency plan describing appropriate responses to the following circumstances:

1. results produced by recount or alternative *·counting software·* do not agree with original result
2. number of *·votes·* recorded does not match number of *·electors·*
3. *·voter·* leaves a *·voting device·* in an *·active state·*
4. etc.

Org_5 [tr] Before the *·election·* the *·responsible election authority·* SHOULD publicly disclose all technical information about the *·election devices·* (including design, configuration, version numbers for all software, etc.). The *·responsible election authority·* SHALL provide a detailed justification for every document not so disclosed.

Org_6 [di] The *·responsible election authority·* SHALL ensure that *·election·* data is stored, and its integrity and authenticity preserved {Sec_17, Audit_6}, for the prescribed *·archiving period·*.

Org_7 [tr] The *·responsible election authority·* SHOULD procure alternative *·counting software·* to check results {Org_4}.

Org_8 [fr] [tr] The *·responsible election authority·* SHALL educate *·voters·* in the use of the *·voting devices·* and SHALL ensure that the information provided to them is understandable {Assur_5}, providing translations where appropriate.

Org_9 [un] The *·responsible election authority·* SHALL educate *·poll-workers·* in the use of the *·election devices·* and about the procedures they must follow and SHALL ensure that information provided to them is understandable {Assur_5,

Org_10, Assur_5, Org_3}.

Org_10 [all] The *·poll-workers·* SHALL follow the procedures described by the *·responsible election authority·* {Org_3} and SHALL respond to system messages in accordance with the user-guide {Assur_5, Org_9}.

Org_11 [un] The *·responsible election authority·* SHALL ensure that adequate spare *·voting devices·* are available.

6.4.5 Assurance Requirements

Assur_1 [eq] The only interfaces to the *·voting device·* SHOULD be the *·vote-casting interface·* (including those designed for *·voters·* with disabilities) and *·poll-worker interfaces·*. Where other interfaces exist they SHALL be disabled.

Assur_2 [tr] The *·manufacturer·* SHALL develop the *·election devices·* according to software engineering best practice, including use of version control and bug tracking for all documents and source code.

Assur_3 [un] The *·manufacturer·* SHALL build the *·e-voting system·* from reliable components.

Assur_4 [eq] [tr] [di] The *·manufacturer·* SHALL limit the functionality of the *·election devices·* to that necessary for *·elections·*.

Assur_5 [tr] The *·manufacturer·* SHALL produce the following documents ensuring that they are exhaustive, consistent, unambiguous, appropriate, comprehensible and concise

1. system specification including at least:
   (a) high-level design system architecture
   (b) functional specification
   (c) engineering specification
2. requirement conformance claim
3. component list
4. environmental assumptions

5. testing record
6. development security measures
7. user-guide - containing
   (a) normal use instructions for all *·users·* for all phases (including: maintenance instructions, system and functional checks, system setup, election preparation, system configuration, storage, transport, sealing)
   (b) appropriate responses to all system messages {Sec_9}
8. bug tracking record
9. version control record
10. etc.

Assur_6 [tr] The *·manufacturer·* SHOULD publicly disclose all: documentation listed in Assur_5, executable programs and source code. The *·manufacturer·* SHALL disclose these data to the *·independent testing authority·*.

Assur_7 [tr] [un] The *·manufacturer·* SHALL test the *·election devices·*, these tests SHALL include unit, integration, end-to-end functionality and usability tests.

Assur_8 [un] The *·manufacturer·* SHOULD involve *·users·* in the interface development process {Usab_1}.

Assur_9 [tr] The *·independent testing authority·* SHALL do a risk analysis and develop a threat model.

Assur_10 [all] The *·independent testing authority·* SHALL evaluate the *·election devices·* against the requirements (including national and international legislation). Tests SHALL include penetration, usability and end-to-end functionality tests.

Assur_11 [all] The *·independent testing authority·* SHALL examine documentation provided by the *·manufacturer·* (including source code and details of version control and bug tracking) for compliance with requirements and software

engineering best practice {Assur_5, Assur_2}.

Assur_12 [all] The *·independent testing authority·* SHALL examine the delivery procedures for the *·election devices·* and the identified development security measures (including their application) {Assur_5}.

6.4.6 Audit System Requirements

Audit_1 [tr] The *·audit system·* SHALL record system configuration (including software version numbers) and *·election·* configuration (including *·ballot·* options) on all *·election devices·* at least at the following points:

1. end of *·election setup·*
2. beginning and end of *·polling period·*
3. before and after counting.

Audit_2 [tr] For every action performed by *·poll-workers·* the *·audit system·* SHOULD record a timestamp, the nature of the action, and *·poll-worker·* authentication data.

Audit_3 [tr] The *·audit system·* SHALL record (with timestamps, where appropriate) all system breakdowns, exceptions, malfunctions and results of any self-checks.

Audit_4 [tr] The *·audit system·* SHALL implement the access control policy defined by the *·responsible election authority·* {Org_2}.

Audit_5 [tr] The *·audit system·* and its records SHALL be tamper-resistant and tamper-evident.

Audit_6 [tr] The *·audit system·* SHALL protect the integrity and authenticity of audit records.

Audit_7 [tr] The *·audit system·* SHOULD have access to a reliable time source.

Audit_8 [tr] The *·audit system·* SHALL not record any information which might endanger the secrecy of the *·vote·*.

6.4.7 VVAT Requirements

Where a Voter Verified Audit Trail is implemented:

VVAT_1 [tr] [eq] The VVAT SHALL comprise tangible, human-readable ballots verified by individual *·voters·*.

VVAT_2 [tr] [di] The *·responsible election authority·* SHALL ensure that VVAT-ballots are protected with adequate safeguards (including chain of custody).

VVAT_3 [tr] [se] The VVAT SHALL not retain ballot-casting order.

VVAT_4 [tr] [di] Where results of a *·poll·* are close, the *·responsible election authority·* SHALL tally the VVAT-results.

VVAT_5 [tr] [di] The *·responsible election authority·* SHALL tally the VVAT-results in a statistically significant number of randomly selected constituencies at every election. The *·responsible election authority·* SHALL calculate the number of constituencies to be checked according to established statistical principles before the election, and SHALL make the random selection after the end of the *·polling period·*.

VVAT_6 [tr] [eq] For the purposes of VVAT_4 and VVAT_5, VVAT-results SHALL be tallied by hand.

VVAT_7 [tr] [di] Where inconsistencies are detected between the results produced by the *·e-voting system·* and the VVAT-results, the *·responsible election authority·* SHALL give precedence to the VVAT-results.

VVAT_8 [all] The *·responsible election authority·* SHALL develop procedures to handle

1. voter complaints (in DRE+VVAT systems)
2. discrepancies between results produced by the *·e-voting system·* and VVAT-results (including rules governing how many constituencies must have their VVAT-results tallied when such discrepancies arise, and how they are to be chosen)

3. etc.

6.4.8 Responsible Election Authority Variables

The following table lists the *·responsible election authority· variables* used in the above specification. These terms require further definition based on the particular context in which the system is to be used.

Table 6.1: REAvars

Variable	Note
appropriate authorization Sec_2 Sec_13	Requires definition of both who can access the data/functionality in question, and how their identity will be checked.
·election· data Sec_3 Sec_7 Sec_17 Org_6	This term covers at least: *·votes·*, results and audit data, but may include other data in some contexts.
comprehensive Sec_5	This term must be defined within the context of both the electoral setting, and system design.
etc. Sec_8 Org_2 Org_3 Org_4 Org_5 Assur_5 VVAT_8	This term is used where a representative list is included. Other elements may be added to the list depending, for instance, on what technology is used in the e-voting system.
adequate/adequate number Funct_9 Funct_10 Org_11	Dependant on electoral context: number of voters expected in an average constituency, number of constituencies, and so on.
user-friendly Usab_1	This term must be defined for specific users in the context of their familiarity with given interfaces and technology as well as other sociological factors.

reliable components Assur_3	The definition of this term must take into account international standards for reliability in electronic components (such as resistance to extremes of temperature).
requirements Assur_10 Assur_11	The requirements that a given e-voting system is subject to must be determined by the *·responsible election authority·* and the applicable laws.
close VVAT_4	The definition of this term will depend on the electoral system in use. It should be based on sound mathematical/statistical argument.

6.5 Evaluation

The limitations of this specification were discussed in section 6.2 and future work that might be valuable is described in section 8.3. The requirements do offer some improvements over the other catalogues we examined, however.

Our requirements bring together all of the concepts covered by those other catalogues that are relevant to our scope (as discussed in section 6.2). Those concepts we did not include were given one of the following labels: "as per paper-only elections"; "not applicable to the systems under consideration"; "over specification in this context"; "outside the scope of these requirements". We introduced requirements covering important concepts that are not included in any of those other catalogues. We identified the election principle(s) that each requirement exists to uphold, which should make the specification more comprehensible. We also identified the evaluation technique(s) (as described in section 4.4.1) applicable to each requirement. Concepts which are necessary for the requirements but can only be properly defined within a given context

are explicitly identified, and associated with explanatory notes (see section 6.4.8); this increases the flexibility of the specification without causing under-specification. See the tables in appendix C for comparisons between our requirements and other catalogues, as well as a summary table for our catalogue.

The tools we used to increase the quality of our requirements included the following four techniques. Repeated validation cycles, where our current draft was iteratively checked against other catalogues, produced a catalogue covering all the relevant concepts. Developing the tables in appendix C made the relationships between the catalogues explicit, showing where concepts are included in our catalogue and reasons for leaving out requirements (this process also uncovered oversights from the validation cycles). Developing the summary table C.6 made explicit the principles being upheld, which requirements introduce new concepts, appropriate evaluation techniques and which requirements contain *·responsible election authority·* variables. We produced an interaction matrix [43] which involved the comparison of each of our requirements with every other for conflicts and dependencies. Again, this was an iterative process; conflicts between requirements were identified, requirements were changed, and checks were repeated. The final interaction matrix has not been included (except as cross-references between requirements – see section 6.3) because the information is difficult to display and much less useful than the process of developing the matrix.

Other requirements engineering techniques which might prove useful in the future, but which were not used in the development of this catalogue, include: risk driven specification [115], data-flow modelling [43] within specific electoral contexts, and formal methods [115].

Risk driven specification requires a detailed risk-assessment which, while called for by our requirements (Assur_9), we did not develop for this thesis; many relevant risks may also be context specific. Data-flow modelling would require context-specific information, in particular details about the electoral system in use. Formal methods can produce very high-quality specifications, but

they require expertise and a significant investment of time and other resources. They should also be based on a quality natural language specification. These factors combine to make formal methods beyond the scope of this thesis.

A comparison between the quality of the requirements in the previous chapter and that of the requirements in this chapter would not be particularly useful in determining the relative value of the two approaches taken. The requirements in chapter 5 were written first, with the aim of highlighting some of the problems in the CoE's standards document and suggesting improvements. They have not been modified in light of the work contained in this chapter. The requirements in this chapter, on the other hand, did benefit from that previous work. This set of requirements has also been written in a more standardized form (see section 6.3) and has benefited from the influence of multiple existing catalogues (whereas the previous set were only influenced by the CoE standards).

As already stated, the requirements presented here are not a "finished product". An international standard for e-voting should be technology independent (some of the above requirements are currently only applicable to DRE systems), it should discuss evaluation and maintenance (see section 4.4) and it should cover the introduction of technology to other parts of the democratic process (such as ·*voter*· registration and authentication).

Chapter 7

Contributions

This thesis makes several contributions to the field of e-voting. The most important is the requirements catalogue in chapter 6 [1]. The requirements have several noteworthy attributes:

- they are written to be unambiguous, using an extensive glossary of election terminology;
- each requirement encapsulates a single concept (as opposed to several closely related concepts);
- all of the requirements follow the same format which shows who/what is responsible for ensuring that a requirement is met, and what it is that they must ensure;
- the use of SHALL/SHOULD (as defined in section 1.1) indicates the difference between requirements that must be met in all circumstances and those that may be set aside provided that adequate justification has been provided;
- they were developed to be useful in a technical context, for the development, procurement, testing and maintenance of e-voting systems. With respect to testability, each is associated with a testing methodology (as described in section 4.4.1, see table C.6);

[1] These requirements were developed from a set of requirements produced in collaboration with Melanie Volkamer and published in [42].

- despite their technical focus, they are easy to read;
- the catalogue has been carefully reviewed several times to check for internal consistency. This process was aided by the consistent use of terminology, consistent formulation of the requirements and the development of an interaction matrix;
- the requirements were repeatedly compared to existing catalogues to ensure that all relevant concepts captured by those other catalogues were covered by the new requirements (this comparison is summarized in appendix C).

These requirements do not constitute a definitive catalogue of requirements for e-voting, since such a catalogue would require the input and buy-in of stakeholders from many different disciplines. However, they could form the basis of a definitive catalogue (see section 8.3).

There are also several more minor contributions made by this thesis:

- the glossary mentioned above (appendix A) is necessary because election terminology is particularly vulnerable to ambiguity (see section 1.1). The terms defined cover general election terminology, election phases, actors/entities, and devices/components. These terms were originally selected to cover the concepts needed for requirements definitions, but also proved useful throughout the text of the thesis;
- the description of cryptographic voting schemes (section 3.4) provides an introduction to the area for readers with little or no familiarity with cryptography in general, whereas most descriptions tend to assume a certain amount of knowledge of that field on the part of the reader;
- the examination of the procurement of e-voting systems within the context of procurement of ICT by public bodies (section 4.1) gives new insight into the problems experienced with many e-voting systems that have been used for real elections;
- the discussion of verification and maintenance (section 4.4) is missing

from existing standards and recommendations for e-voting. [2];

- the critique of the Council of Europe requirements (chapter 5) highlights some flaws in that document which would significantly reduce its usefulness in the design, verification and maintenance of e-voting systems, and suggests one route which might be taken to improve the specification.

Overall the thesis identifies several major barriers to the use of e-voting in critical elections and suggests routes by which those barriers might be overcome. Aspects of this thesis would be useful to legislators and election officials as an introduction to some of the technical issues involved in the use of e-voting, while other parts would be useful to technologists, particularly those attempting to develop a definitive set of requirements for e-voting in critical elections.

[2]This section has now been developed into a joint paper with Paul Gibson called "Verification and Maintenance of e-voting systems and standards" [116].

Chapter 8

Future Work

In each of the three main topics covered by this thesis, and identified in chapter 2, there remain unanswered questions and unexplored areas. Some of these could not be answered due to a lack of available data, some would be premature in the current context, some are simply outside our area of competency. In the following sections we discuss the most interesting outstanding questions and consider the skills that would be required to approach them.

8.1 Secrecy versus Accuracy

As discussed in chapter 3, the conflict between secrecy and accuracy is a major barrier to the use of e-voting for critical elections. That chapter also discusses some of the weaknesses in the solutions to that conflict that have been proposed so far. Therefore an important area of future work in e-voting is the search for a satisfactory remedy to the conflict. Such a solution must not itself violate any of the election principles identified in section 1.6 (universal, equal, free, secret, direct and trusted suffrage). It must also: be understandable by individual voters; not disenfranchise voters; be user-friendly (both in vote casting and vote checking); not rely to an unreasonable degree on trusting a small number of auditors; and be implemented under real-world assumptions (e.g. if a robust,

authenticated broadcast channel is required, the scheme must be explicit about how such a channel could be implemented).

In section 2.1.1 we identified several questions which were not answered in this thesis for various reasons, but which might be fruitful for future research. These questions mainly pertain to points of comparison between proposed solutions to this conflict, such as: financial cost, level of extra effort required from election staff, ease of use for voters, voters' reactions and "comfort" levels, balance struck between secrecy and accuracy, vulnerability of system to future technological developments, compatibility with international standards. So far, many of these systems have only been trialled on a very small scale (such as university elections), if at all. This research might be more usefully carried out at a future time when more of these solutions have been implemented under realistic circumstances.

This type of comparison would be useful to decision makers when choosing an e-voting system for their context. The priority given to each of these points of comparison will vary from context to context, so the research is unlikely to pinpoint a "best" solution. It would, however, help policy makers to determine the best solution for their context given their priorities.

Since the information sought by this research is quite diverse, it would require a broad range of skills. For instance, comparing the usability (for both voters and election staff) of the various systems fairly would require well-designed usability testing (see section 4.4.1); testing voters' satisfaction with the systems would require knowledge of good survey design; discussion of compatibility with international standards would require a close familiarity with those standards; and so on. As with so many aspects of the field of e-voting, the ideal team to carry out this research would be cross-disciplinary and would include: cryptographers, usability experts, and researchers familiar with financial analysis, survey design, and international standards.

8.2 Organizational Barriers

One of the most striking results of the research for chapter 4 was that there is a lack of available information on procurement of ICT within the public sector. This hinders the ability of public bodies to learn from their own and others' successes and mistakes, and makes it unlikely that the quality of systems procured will increase. It is also clear that strategies for increasing and retaining internal expertise need to be developed, so that knowledge of best practice can be used by individuals representing the public body's interests. This would reduce the reliance of public bodies on external information from vendors and consultants.

One approach to resolving this lack of information would be to introduce a regular survey of ICT projects in the public sector similar to the one carried out in the private sector by the Standish Group [75]. Useful data to collect would include: project cost breakdown (including projections), project success in terms of delivery time and features, level of involvement of internal staff, level of involvement of external actors (such as consultants), acceptance of final project amongst users, techniques applied to the project (with rationale), organizational structures and rules, and so on. This survey would have to be organized in such a way that it protected the anonymity of those involved. This would encourage participation and help participants to see the project as an information-gathering rather than a blame-laying exercise. The anonymised data could be analysed quantitatively – giving information about what techniques and best practices are most effective under what circumstances – as well as qualitatively – giving anecdotal evidence to help practitioners learn directly from specific experiences of their peers. The Irish Comptroller and Auditor General recently released a report on work of this kind [117] though its scope was limited to projects undertaken within the Republic of Ireland, and under the Government's definition of "eGovernment" projects.

Such a survey would require the co-operation of public bodies, perhaps

enforced from above. The team producing the report would require expertise in survey design and analysis, as well as familiarity with current best practice in both the public and private spheres.

Mitigation strategies could be another fruitful area for study. A survey of strategies for the improvement of ICT procurement (such as those discussed in section 4.2.6), used in both the public and private sectors around the world, could yield useful information. It would be particularly useful if the use of these strategies could be shown to be related to project success.

8.3 Requirements

This thesis identifies the need for a set of requirements for e-voting that is useful to legislators, election officials and technology developers. While the requirements proposed here go some way towards meeting that need, there remains significant work to be done.

The requirements presented here could be further developed to deal with the limitations already identified in section 6.2. One of the major restrictions on this work was the lack of input from experts in other disciplines; future work would require cross-disciplinary participation. A research team – perhaps within a supra-national organization rather than an academic context – composed of experienced requirements engineers, legislators, legal experts, election officials and others could develop a full international standard that met the needs of the various interested parties and improved the quality of procured e-voting systems. This standard should include an improved set of requirements (as discussed below) and also cover: how systems can and should be evaluated against those requirements; maintenance of the standard itself and of the systems it describes; and the role of ITAs (see section 4.4). It must be flexible enough to apply to all existing technologies used in critical elections, and not prevent the certification of valid new technologies. It is vital that the development process is not subverted by commercial or political (as opposed to democratic) interests

(see section 4.3).

The requirements presented here could also be improved in several ways by such a research team. For example:

- Requirements could be developed to cover stages of the electoral process (section 1.2.2) not dealt with here,
- Assumptions about system design (e.g. that the system incorporates a *·voting device·* – section 6.2) should be removed, perhaps by including optional sections in the specification,
- A multi-disciplinary review and revision (requirements-engineer-led negotiation [43]) could ensure that the requirements meet the needs not only of technologists, but also of legislators, election officials, and others,
- The use of requirements engineering techniques which were not practical (see section 6.5) in the preparation of this thesis could lead to further improvements. For example: risk driven specification [115], data-flow modelling [43] within specific electoral contexts, and formal methods [115].

Chapter 9

Conclusions

This thesis identifies several barriers to the use of e-voting in critical elections. Having examined each in turn, we conclude that there are several such barriers which have not been satisfactorily overcome.

The requirements conflict between secrecy and accuracy increases the risk of undetected, and uncorrectable, modifications of results by malice or error. Proposed solutions to that conflict have unresolved problems such as: usability issues (both cryptographic schemes and voter verification), reliance on trusted auditors (cryptographic schemes) and procedural burdens (voter verification).

Procurement of ICT systems is a difficult problem, and particularly so in the public sphere. This reduces the chances of a public body successfully procuring a high-quality e-voting system. There are legal implications which must be adequately addressed with regard to the underlying technological issues. These include the legal position of electoral rules, electoral results and vendors of e-voting systems.

A requirements catalogue must be developed that adequately captures the expected behaviour of e-voting systems. Without a clear definition of what e-voting systems should do, it is impossible to ensure that they do it correctly. The requirements presented here should prove useful in the development of such a catalogue, but the current draft retains certain limitations.

9.1 Analysis of Work Done

9.1.1 Secrecy Versus Accuracy

Chapter 3 presents an analysis of the requirements conflict between secrecy and accuracy framed to highlight why the conflict arises in electronic rather than paper elections, and why the conflict increases the risk from both malice and error. It serves to elucidate the conflict as context for the rest of the chapter, rather than introducing new ideas. We then discuss two approaches to resolving this conflict, with emphasis on the barriers to using each approach in critical elections. As part of the discussion on cryptographic voting schemes we include a description of the underlying design (as well as three example schemes) aimed at a non-cryptographer audience.

A more in-depth comparison between proposed solutions to the conflict could be very useful to authorities introducing e-voting. Points of comparison might include: financial cost, level of extra effort required from election staff, ease of use for voters, voters' reactions and "comfort" levels, balance struck between secrecy and accuracy, vulnerability of system to future technological developments, compatibility with international standards. See future work section 8.1.

9.1.2 Organizational Barriers

Chapter 4 puts e-voting in the broader context of ICT procurement in the public sphere. The discussion of best practice illustrates the effect these techniques have on ICT project outcome. In the interest of offering a solution to an identified problem, we include a summary of some mitigation strategies developed from UK research into public procurement. We identified several areas where the legal implications of introducing e-voting must be considered, as well as some of the considerations resulting from the need for verification and maintenance.

The lack of available data on public procurement severely limited our

discussion on that subject. While our work does illustrate the likely effects of best practice on project outcome in the public sphere, it was not as rigorous as we had hoped. All of the areas addressed in chapter 4 could be better addressed in a multi-disciplinary environment since none of them are computer science topics, but in this context all require in-depth knowledge of the technological issues. See future work section 8.2.

9.1.3 Requirements

Chapters 5 and 6 present our work on developing a catalogue of requirements for e-voting. We use the Council of Europe's standards document as an example to highlight the types of errors that can exist in requirements specifications. We then present a catalogue of requirements developed from scratch. This catalogue has many positive attributes (see chapter 7). We developed a glossary of election terminology (appendix A) as part of this work.

Our requirements are limited in several ways: they only cover part of the electoral process (vote collection and tabulation), they make some design assumptions (such as the existence of a *·voting device·*) and they do not cover remote e-voting. They could be further developed to deal with these limitations. This work could most effectively be done by a multi-disciplinary team. See future work section 8.3.

9.2 Final Remarks

The introduction of e-voting in critical elections constitutes a major change in a highly sensitive apparatus of democracy. The increased potential for negative impact from fraud and error must be taken seriously. We hope that the work presented here will be useful to *·responsible election authorities·* in their decisions regarding the introduction of e-voting, and to researchers in the field – particularly in the development of a requirements catalogue that is useful to legislators, election officials and technology developers.

Bibliography

All URLs in this bibliography were checked on July 4th 2008.

[1] Margaret McGaley and J. Paul Gibson. E-Voting: A Safety Critical System. Technical Report NUIM-CS-TR-2003-02, NUI Maynooth, Computer Science Department, 2003.

[2] Commission on Electronic Voting. Summary and Conclusions – Part 7 of the second report of Ireland's Commission on Electronic Voting, July 2006.

[3] Dominique Cansell, J. Paul Gibson, and Dominique Méry. Refinement: A Constructive Approach to Formal Software Design for a Secure e-voting Interface. *Electronic Notes Theoretical Computer Science*, 183:39–55, 2007.

[4] Scott Bradner. RFC2119 – Key words for use in RFCs to Indicate Requirement Levels. Network Working Group, March 1997.

[5] Alexandros Xenakis and Ann Macintosh. The UK Deployment of the E-Electoral Register. In Prosser and Krimmer [118], pages 143–152.

[6] Epp Maaten. Towards Remote E-Voting: Estonian case. In Prosser and Krimmer [118], pages 83–100.

[7] Ben Adida. *Advances in Cryptographic Voting Systems.* PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2006.

[8] Aviel D. Rubin. Security Considerations for Remote Electronic Voting. *Communications of the ACM*, 45(12), December 2002.

[9] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), January 2004.

[10] Joe Mohen and Julia Glidden. The case for internet voting. *Commun. ACM*, 44(1):72–ff., 2001.

[11] Hubertus Buchstein. *Electronic Voting and Democracy: A Comparative Analysis*, chapter Online Democracy, Is it Viable? Is it Desirable? Internet Voting and Normative Democratic Theory, pages 39–58. palgrave macmillan, 2004.

[12] Douglas W. Jones. A Brief Illustrated History of Voting. `http://www.cs.uiowa.edu/~jones/voting/pictures/`, 2001 (updated 2003).

[13] Roy G. Saltman. *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*. Palgrave Macmillan, January 2006.

[14] Dr. Kenneth Benoit. Experience with Voting Overseas – Appendix 2J to the first report of Ireland's Commission on Electronic Voting, December 2004.

[15] Irish Citizens for Trustworthy Evoting (ICTE) homepage. `http://evoting.cs.may.ie`.

[16] Open Rights Group (ORG) homepage. `http://www.openrightsgroup.org/`.

[17] Wij Vertrouwen Stemcomputers Niet (We Don't Trust Voting Computers) homepage (English). `http://www.wijvertrouwenstemcomputersniet.nl/English`.

[18] VotersUnite.Org homepage. `http://www.votersunite.org/`.

[19] The Verified Voting Foundation homepage. http://www.verifiedvotingfoundation.org/.

[20] UK Electoral Commission. Electronic voting: May 2007 electoral pilot schemes, August 2007.

[21] E-voting plans hit by decision in Dutch court. *Irish Independent*, October 3rd 2007.

[22] Decertification/Recertification Decisions Issued August 3, 2007, by California Secretary of State Debra Bowen. http://www.sos.ca.gov/elections/elections_vsr.htm.

[23] Robert Kibrick (VerifiedVoting.org Legislative Analyst). Voter-Verified Paper Record Legislation. http://www.verifiedvoting.org/article.php?list=type&type=13.

[24] Anne-Marie Oostveen and Peter Van den Besselaar. Security as Belief: User's Perceptions on the Security of E-Voting Systems. In Prosser and Krimmer [118], pages 73–82.

[25] Sylvia Leatham. Most Irish citizens approve of e-voting. ENN, August 6th 2003.

[26] Poll majority want e-voting put on hold. The Sunday Business Post, March 14th 2004.

[27] Mark Brennock. Cabinet to press ahead on e-voting in EU and local polls. *The Irish Times*, February 25th 2004.

[28] Irish Government website. Electronic voting: it's easier for everyone. http://www.electronicvoting.ie/english/index.html.

[29] Geneva Government website. E-Voting: informations [sic] about eVoting. http://www.geneve.ch/evoting/english/welcome.asp.

[30] Rebecca Mercuri. *Electronic Vote Tabulation Checks & Balances*. PhD thesis, University of Pennsylvania, School of Engineering and Applied Science, Department of Computer and Information Systems, October 2000.

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

[32] Margaret McGaley and Joe McCarthy. Transparency and e-Voting: Democratic vs. Commercial Interests. In Prosser and Krimmer [118], pages 153 – 163.

[33] Verified Voting Foundation and Computer Professionals for Social Responsibility (CPSR). Election Incident Reporting System. `http://voteprotect.org/`.

[34] Ron Ross. Managing Enterprise Security Risk with NIST Standards. *Computer*, 40(8):88–91, 2007.

[35] Mark Gondree, Patrick Wheeler, and Dimitri DeFigueiredo. A Critique of the 2002 FEC VSPT E-Voting Standards. Technical Report CSE-2005-20, Department of Computer Science University of California at Davis, September 2005.

[36] Melanie Volkamer and Roland Vogt. Digitales Wahlstift-System (Common Criteria Protection Profile for Internet Voting for the City of Hamburg). BSI-PP-0031, 2006.

[37] BMI Bundesministerium des Inneren. Bundeswahlgeräteverordnung (bwahlgv), April 1999. (German Regulations for Voting Devices) Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Paralments aus der Bundesrepublik Deutschland. Vom 03.09.1975 (BGBl S. 2459) zuletzt geändert am 20.04.1999 (BGBl I S. 749).

[38] Physikalisch-Technische Bundesanstalt Braunscheig/Berlin PTB. Online Voting Systems for Nonparliamentary Elections - Catalogue of Requirements, May 2004.

[39] P.L. Vora, B. Adida, R. Bucholz, D. Chaum, D.L. Dill, D. Jefferson, D.W. Jones, W. Lattin, A.D. Rubin, M.I. Shamos, and M. Yung. Evaluation of voting systems. *Commun. ACM*, 47(11):144, 2004.

[40] Council of Europe. Recommendation on legal, operational and technical standards for e-voting Rec(2004)11, September 2004.

[41] Margaret McGaley and J. Paul Gibson. A Critical Analysis of the Council of Europe Recommendations on e-voting. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2006.

[42] Melanie Volkamer and Margaret McGaley. Requirements and Evaluation Procedures for e-Voting. In *Dependability and Security in e-Government? - DeSeGov 2007*, 2007.

[43] Ian Sommerville and Gerald Kotonya. *Requirements Engineering: Processes and Techniques*. John Wiley & Sons, Inc., 1998.

[44] Pericles Loucopoulos and Vassilios Karakostas. *System Requirements Engineering*. McGraw-Hill, Inc., New York, NY, USA, 1995.

[45] Lynn Landes. Scrap the "Secret" Ballot - Return to Open Voting. `http://www.thelandesreport.com/OpenVoting.htm`.

[46] Irish Citizens for Trustworthy Evoting. Submission to the Commission on Electronic Voting.

[47] Andrew Gumbel. *Steal This Vote: Dirty Elections and the Rotten History of Democracy in America*. Nation Books, July 2005.

[48] David L. Dill, Bruce Schneier, and Barbara Simons. Voting and technology: who gets to count your vote? *Commun. ACM*, 46(8):29–31, 2003.

[49] Edsger W. Dijkstra. The humble programmer. *Commun. ACM*, 15(10):859–866, October 1972.

[50] Barnaby Mason. Voting scandal mars UK election. BBC news online, April 5th 2005.

[51] Anthony Di Franco, Andrew Petro, Emmett Shear, and Vladimir Vladimirov. Small vote manipulations can swing elections. *Commun. ACM*, 47(10):43–45, 2004.

[52] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2007.

[53] Bruce Schneier. Schneier on Security: The Problem with Electronic Voting Machines. `http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html`.

[54] Jonathan N. Wand, Kenneth W. Shotts, Jasjeet S. Sekhon annd Walter R. Mebane Jr., Michael C. Herron, and Henry E. Brady. The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida. *American Political Science Review*, 95(4):793–810, 2001.

[55] Bruce Schneier. Talk at Defcon 15. `http://www.schneier.com/blog/archives/2007/10/my_talk_at_defc.html`. time 31:46 - 36:45.

[56] Sarah P. Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. PhD thesis, Rice University, Houston, TX, 2007.

[57] Josh C Benaloh and Moti Yung. Distributing the power of a government to enhance the privacy of voters. In *PODC '86: Proceedings of the fifth annual ACM symposium on Principles of distributed computing*, pages 52–62, New York, NY, USA, 1986. ACM Press.

[58] K.R. Iversen. A cryptographic scheme for computerized general elections. *Advances in Cyptology-CRYPTO*, 91:405–419, 1992.

[59] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. Multi-authority Secret-Ballot Elections with Linear Work. *Lecture Notes in Computer Science*, 1070:72, 1996.

[60] Josh Benaloh. Towards Simple Verfiable Elections. In *IAVoSS Workshop On Trustworthy Elections (WOTE 2006) – Pre-Proceedings*, Robinson College, University of Cambridge, England, June 2006.

[61] P.Y.A. Ryan and T. Peacock. Prêt à Voter: a systems perspective. Technical Report CS-TR-929, University of Newcastle, 2005.

[62] K. Fisher, R. Carback, and A. Sherman. Punchscan: Introduction and System Definition of a High-Integrity Election System. In *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 06)*, Cambridge, UK, June 2006.

[63] C. Andrew Neff and Jim Adler. Verifiable e-Voting. Indisputable electronic elections at polling places. White paper, August 2003.

[64] David Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Security and Privacy*, 02(1):38–47, 2004.

[65] R. Rivest and W. Smith. Three Voting Protocols: ThreeBallot, VAV, and Twin. *Proceedings of USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, 2007.

[66] Harvey Jones, Jason Juang, and Greg Belote (Instructor: Ronald L. Rivest). ThreeBallot in the Field. Term paper for MIT course 6.857, December 2006.

[67] Benjamin B. Bederson, Bongshin Lee, Robert M. Sherman, Paul S. Herrnson, and Richard G. Niemi. Electronic voting system usability issues. In *CHI '03: Proceedings of the SIGCHI conference on Human factors*

in computing systems, pages 145–152, New York, NY, USA, 2003. ACM Press.

[68] Josh D. Cohen and Michael J. Fischer. A Robust and Verifiable Cryptographically Secure Election Scheme (Extended Abstract). In *FOCS*, pages 372–382, 1985.

[69] Helmer Aslaksen and Gary McGuire. Mathematical Aspects of Irish Elections. *Irish Mathematics Teachers Association Newsletter*, 105:40–59, 2006.

[70] Aleks Essex, Jeremy Clark, Rick Carback, and Stefan Popoveniuc. Punchscan in practice: an E2E election case study. Workshop on Trustworthy Elections (WOTE) 2007.

[71] Pippa Norris. *Electronic Voting and Democracy: A Comparative Analysis*, chapter Will New Technology Boost Turnout? Evaluating Experiments in UK Local Elections, pages 193–225. palgrave macmillan, 2004.

[72] Declan McCullagh. E-voting predicament: Not-so-secret ballots. CNET News.com, August 20th 2007.

[73] Javed A. Aslam, Raluca A. Popa, and Ronald L. Rivest. On Estimating the Size and Confidence of a Statistical Audit. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2007.

[74] Douglas W. Jones. Optical Scan Calibration. National Institute of Standards and Technology (NIST) Workshop – Threats to Voting Systems, October 7th 2005.

[75] Stephen P. Masticola. A Simple Estimate of the Cost of Software Project Failures and the Breakeven Effectiveness of Project Risk Management. In *ESC '07: Proceedings of the First International Workshop on The Economics of Software and Computation*, page 6, Washington, DC, USA, 2007. IEEE Computer Society.

[76] The Comptroller and Auditor General (UK). Better Public Services through e-government. National Audit Office HC 704-III, April 2002.

[77] The Comptroller and Auditor General (Ireland). *Development of Human Resource Management System for the Health Service (PPARS)*. Stationary Office, Government of Ireland, December 2005. Report No. 51.

[78] Parliamentary Office of Science and Technology (UK). Government IT projects, July 2003.

[79] National Audit Office (UK). Improving IT procurement: The impact of the Office of Government Commerce's initiatives on departments and suppliers in the delivery of major IT-enabled projects, November 2004.

[80] Office of Government Commerce. Successful IT: Modernising Government in Action – Cabinet Office Review of Major Government IT Projects, May 2000.

[81] Commission on Electronic Voting. Second Report, July 2006.

[82] Green Party calls on Cullen to resign over e-voting fiasco (Press Release), April 30th 2004.

[83] European Commission for Democracy Through Law (Venice Commission). Code of good practice in electoral matters – Opinion no. 190/2002, October 2002.

[84] The Comptroller and Auditor General (Ireland). *Annual Report of the Comptroller and Auditor General*, volume 1. Stationary Office, Government of Ireland, 2003.

[85] Commission on Electronic Voting. Comparative Assessment: Assessment of Risks – Appendix 5B to the second report of Ireland's Commission on Electronic Voting, December 2004.

[86] Department of the Environment, Heritage and Local Government. Request for Tenders: Electronic Voting and Counting System, June 2000.

[87] Nathean Technologies. Code Review of IES Build 0111 for the Department of the Environment, Heritage and Local Government - page 25.

[88] Margaret McGaley. True democracy needs a voting trail. Online magazine openDemocracy, December 2004.

[89] Revenue On-Line Service (ROS). Submission to eEurope awards – Winner Impact category. (received from Conor Hegarty, Revenue Commissioner), 2005.

[90] Sean Cosgrove and Conor Hegarty, Revenue Commissioners. Revenue On-Line Service (ROS), Ireland's e-Government Success Story. In *International Conference on E-Governance ICEG06*, December 2006.

[91] Peter Gershon. Review of Civil Procurement in Central Government. Technical report, HM Treasury, April 1999.

[92] Electoral Act 1992 (Ireland).

[93] Department of the Environment, Heritage and Local Goverment. Electronic Voting and Counting System : Request for Tenders Count Requirements and Commentary on Count Rules, June 2000.

[94] Nathean Technologies. Electronic Voting and Counting System Information Paper, January 2004.

[95] Minutes of a meeting of the Joint Committee on Environment and Local Government, December 18th 2003.

[96] Paul Lambert. Who has their eye on your online activities? The Sunday Business Post, May 2002.

[97] Josh Lerner and Jean Tirole. The open source movement: Key research questions. *European Economic Review*, 45(4-6), May 2001.

[98] Agreement: Powervote Ireland Ltd and Nedap NV -and- The Minister for the Environment, Heritage and Local Government, December 2003.

[99] Mark Brennock. Last-minute indemnity for e-voting commission agreed. *The Irish Times*, April 2004.

[100] William Jackson. Under attack: Common Criteria has loads of critics, but is it getting a bum rap? Government Computer News, August 13th 2007.

[101] Kristen K. Greene, Michael D. Byrne, and Sarah P. Everett. A Comparison of Usability Between Voting Methods. In *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2006.

[102] Joseph S. Dumas and Janice C. Redish. *A Practical Guide to Usability Testing*. Intellect Ltd, October 1999.

[103] OSCE Office for Democratic Institutions and Human Rights (ODIHR). Election observation - a decade of monitoring elections: the people and the practise, 2005.

[104] The Carter Center Democracy Program. `http://www.cartercenter.org/peace/democracy/index.html`.

[105] The Carter Center. Developing a Methodology for Observing Electronic Voting, October 2007.

[106] Aviel D. Rubin. *Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting*. Morgan Road Books, September 2006.

[107] Douglas W. Jones. *The Machinery of Democracy: Protecting Elections in an Electronic World*, chapter Appendix E: Voting Machine Testing. Brennan Center Task Force on Voting System Security, 2007.

[108] Rebecca T. Mercuri and L. Jean Camp. The code of elections. *Commun. ACM*, 47(10):52–57, 2004.

[109] Statute of the Council of Europe, Chapter I, Article 1a.

[110] 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.

[111] B. Meyer. On Formalism in Specifications. *IEEE Softw.*, 2(1):6–26, 1985.

[112] Douglas W. Jones. The European 2004 Draft E-Voting Standard: Some critical comments. `http://www.cs.uiowa.edu/~jones/voting/coe2004.shtml`, 2004.

[113] Earl Barr, Matt Bishop, Dimitri DeFigueiredo, Mark Gondree, and Patrick Wheeler. Toward Clarifying Election Systems Standards. Technical Report CSE-2005-21, Department of Computer Science University of California at Davis, September 2005.

[114] California Internet Voting Task Force. Final Report, 2000. Appendix a3 section 3.2.3.

[115] Ian Sommerville. *Software Engineering (8th edition).* Addison Wesley, 2006.

[116] Paul Gibson and Margaret McGaley. Verification and Maintenance of e-Voting Systems and Standards. In *8th European Conference on e-Government*, 2008.

[117] The Comptroller and Auditor General (Ireland). *eGovernment.* Stationary Office, Government of Ireland, October 2007. Report No. 58.

[118] Alexander Prosser and Robert Krimmer, editors. *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*, volume 47 of *LNI*. GI, 2004.

[119] Michael Ian Shamos. Electronic Voting - Evaluating the Threat. *Third Conference on Computers, Freedom and Privacy, CPSR*, March 1993.

Appendix A

Glossary

The terms below have the following meanings in this thesis where they appear highlighted *·like this·*.

A.1 Election Terminology

·ballot·

: voting options available in a particular *·poll·*

·cast· (verb)

: to commit to a particular set of *·selections·*, equivalent to putting one's completed paper *·vote·* into the *·ballot box·* in a traditional paper-based voting system

·election·

: the proceedings accompanying the formal choosing of the winner(s) of one or more *·polls·*

·poll·

: a decision between options – such as candidates for a position, or choices in a referendum – which is determined by *·votes·* *·cast·* by *·eligible voters·*

·selection·

an indication by a *·voter·* of some subset of his preferences

·spoil·

to *·cast·* a *·vote·* which will not be counted for some legitimate reason (e.g. incorrectly filled-in, or blank)

·vote· (noun only)

the expression of an individual *·voter's·* preference(s)

·voters' register·

list of *·eligible voters'·* details, including whether they have *·cast·* their *·vote·*

A.2 Phases of the Election (see figure 6.1)

·archiving period·

period after the *·election period·* for which *·vote·* records must be retained

·counting phase·

calculation of *·poll·* results. This may entail the collection of votes for tabulation

·election period·

the period from the beginning of the *·election setup·*, through the *·polling period·*, to the completion of the *·counting phase·*

·election setup·

preparation of devices and personnel for *·polling period·*

·polling period·

period of time when polls are open, i.e. ·*votes*· can be ·*cast*·

·*voting process*·

all interactions of an authorized ·*voter*· with the ·*voting device*·. The ·*voting process*· begins when the ·*voting device*· is put in an ·*active state*· and ends when the voter has cast his ·*vote(s)*· or cancels the ·*voting process*·

A.3 Actors/Entities

·*certification authority*·

body nominated by the ·*responsible election authority*· which certifies the ·*election devices'*· compliance with requirements

·*elector*·

an ·*eligible voter*· who has ·*cast*· his ·*vote(s)*·

·*eligible voter*·

a person who is entitled to ·*cast*· one or more ·*votes*·

·*manufacturer*·

the body responsible for the development and maintenance of ·*election devices*· (hardware and software)

·*poll-worker*·

a person in his role as an official facilitator in the running of an ·*election*·

·*responsible election authority*·

the organization responsible for running the ·*election*·

·*independent testing authority*·

body (or bodies) nominated by the *·responsible election authority·* which tests the *·election devices'·* compliance with requirements

·user·

anyone who is authorized to interact with an *·election device·* during the *·election period·*

·voter·

a person in his role as *·caster·* of a *·vote·*

A.4 Devices and Components

·system·

a set of devices and methods

·audit system·

sub-system of the *·e-voting system·* which allows the actual behaviour of the *·e-voting system·* to be audited

·ballot box·

physical box in which tangible *·vote·* records (usually paper) are stored

·counting software·

software which calculates *·poll·* results

·election device·

any hardware and/or software component involved in the *·e-voting system·* e.g., *·voting devices·* and *·counting software·*

·e-ballot box·

·system· in which *·e-votes·* are stored

·e-voting system·

a *·system·* for the electronic collection of *·votes·* and calculation of results, including e.g. the *·election devices·* and *·poll-workers·*

·e-vote·

an electronic copy of a *·vote·*

·poll-worker interface·

user-interface to *·election devices·* which enables *·poll-workers·* to carry out their duties

·vote-casting interface·

user-interface through which an authenticated *·voter·* may cast his *·vote(s)·* or cancel the *·voting process·*

·voting channel·

a medium through which *·voters·* can *·cast·* *·votes·*

·voting device·

the device on which *·voters·* *·cast·* their *·votes·* in the polling booth

·active state·

the *·voting device·* is in an *·active state·* if it is capable of accepting a *·voter's·* *·selections·* and *·votes·* can be *·cast·* (or the *·voting process·* cancelled)

·inactive state·

the *·voting device·* is in an *·inactive state·* if it is incapable of accepting a *·voter's·* *·selections·* and no *·votes·* can be *·cast·* (nor the *·voting process·* cancelled)

Appendix B

Council of Europe Requirements for E-voting

This appendix quotes verbatim from Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 – Legal, Operational and Technical Standards for E-voting (with additional annotation, described below). The copyright for the quoted text is held by the Council of Europe, and it is included with permission.

The requirements are arranged in that document under three appendices: Principles, Operational Standards, and Technical Requirements; the original nomenclature is retained here. For the full text of the recommendation, including an explanatory memorandum, see [40]. For the sake of ease of reference from chapters 5 and 6, divisions have been added to some of these requirements; they are indicated by boldface letters in square brackets (e.g. **[a]**).

Legal standards

Appendix I

A. Principles

I. Universal suffrage

1. **[a]** The voter interface of an e-voting system shall be understandable **[b]** and easily usable.

2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.

3. E-voting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.

4. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

II. Equal suffrage

5. **[a]** In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. **[b]** A voter shall be authorized 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.

7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.

8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.

III. Free suffrage

9. The organization of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.

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.

11. **[a]** 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, **[b]** without their previous choices being recorded or made available to any other person.

12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.

13. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.

14. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.

15. The e-voting system shall prevent the changing of a vote once that vote has been cast.

IV. Secret suffrage

16. E-voting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.

17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.

18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.

19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

B. Procedural safeguards

I. Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

21. Information on the functioning of an e-voting system shall be made publicly available.

22. Voters shall be provided with an opportunity to practise any new method of e-voting before, and separately from, the moment of casting an electronic vote.

23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.

II. Verifiability and accountability

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.

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.

26. **[a]** There shall be the possibility for a recount. **[b]** Other features of the e-voting system that may influence the correctness of the results shall be verifiable.

27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

III. Reliability and security

28. The member state's authorities shall ensure the reliability and security of the e-voting system.

29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.

30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.

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.

32. **[a]** Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. **[b]** Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.

33. **[a]** While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and **[b]** any election observers.

34. **[a]** The e-voting system shall maintain the availability and integrity of the votes. **[b]** It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. **[c]** If stored or communicated outside controlled environments, the votes shall be encrypted.

35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be

separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

Appendix II

Operational standards

I. Notification

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.

37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e-voting, the period shall be defined and made known to the public well in advance of the start of voting.

38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organized, and any steps a voter may have to take in order to participate and vote.

II. Voters

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.

40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.

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.

III. Candidates

42. The possibility of introducing online candidate nomination may be considered.

43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.

IV. Voting

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.

45. Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.

46. **[a]** For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. **[b]** In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.

47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.

48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice.

49. If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.

50. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.

51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.

52. **[a]** In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. **[b]** Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.

V. Results

53. **[a]** The e-voting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. **[b]** This information shall not be disclosed to the public until after the end of the voting period.

54. The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.
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.

56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.

57. A record of the counting process of the electronic votes shall be kept,

including information about the start and end of, and the persons involved in, the count.

58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.

VI. Audit

59. The e-voting system shall be auditable.

60. The conclusions drawn from the audit process shall be applied in future elections and referendums.

Appendix III

Technical requirements

The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks[1] involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified. Service failure or service degradation shall be kept within pre-defined limits.

A. Accessibility

61. **[a]** Measures shall be taken to ensure that the relevant software and services can be used by all voters **[b]** and, if necessary, provide access to alternative ways of voting.

62. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

63. Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as

[1]The need for a risk assessment is not identified within the CoE requirements other than in this paragraph. We refer to this paragraph from chapters 5 and 6 as III.

personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).

64. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.

65. The presentation of the voting options shall be optimized for the voter.

B. Interoperability

66. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.

67. At present, the Election Markup Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this recommendation, and supporting documentation are available on the Council of Europe website.

68. In cases which imply specific election or referendum data requirements, a localization procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.

C. Systems operation

(for the central infrastructure and clients in controlled environments)

69. **[a]** 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. [**b**] 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.

70. [**a**] Those responsible for operating the equipment shall draw up a contingency procedure. [**b**] Any backup system shall conform to the same standards and requirements as the original system.

71. [**a**] Sufficient backup arrangements shall be in place and be permanently available to ensure that voting proceeds smoothly. [**b**] The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.

72. [**a**] Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. [**b**] The backup services shall be regularly supplied with monitoring protocols.

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.

74. [**a**] All technical operations shall be subject to a formal control procedure. [**b**] Any substantial changes to key equipment shall be notified.

75. [**a**] Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. [**b**] During the election or referendum period a physical disaster recovery plan shall be in place. [**c**] Furthermore, any data retained after the election or referendum period shall be stored securely.

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.

D. Security

I. General requirements

(referring to pre-voting, voting, and post-voting stages)

77. Technical and organizational 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.

78. **[a]** The e-voting system shall maintain the privacy of individuals. **[b]** Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.

79. **[a]** The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications **[b]** and that its services are available.

80. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.

81. The e-voting system shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.

82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.

83. **[a]** E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. **[b]** The time at which an event generated observation data shall be reliably determinable. **[c]** The authenticity, availability and integrity of the data shall be maintained.

84. The e-voting system shall maintain reliable synchronized 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.

85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies. II. Requirements in pre-voting stages (and for data communicated to the voting stage)

86. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.

88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

III. Requirements in the voting stage
(and for data communicated during post-election stages)

89. The integrity of data communicated from the pre-voting stage (e.g. voters' registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

90. **[a]** It shall be ensured that the e-voting system presents an authentic ballot to the voter. **[b]** In the case of remote e-voting, the voter shall be informed about

the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.

91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.

92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.

93. **[a]** Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. **[b]** In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.

94. **[a]** The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and **[b]** shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.

95. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.

96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.

IV. Requirements in post-voting stages

97. The integrity of data communicated during the voting stage (e.g. votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.

99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.

E. Audit

I. General

100. The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application.

101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.

II. Recording

102. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

103. The audit system shall record times, events and actions, including:

a. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;
b. any attacks on the operation of the e-voting system and its communications infrastructure;
c. system failures, malfunctions and other threats to the system.

III. Monitoring

104. The audit system shall provide the ability to oversee the election or

referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.

105. Disclosure of the audit information to unauthorized persons shall be prevented.

106. The audit system shall maintain voter anonymity at all times.

IV. Verifiability

107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.

108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.

V. Other

109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.

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.

F. Certification

111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.

112. In order to enhance international co-operation and avoid duplication

of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Co-operation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.

Appendix C

Requirements Catalogues Compared

Our requirements were greatly improved by comparison with existing catalogues. The development of each one of the following tables (indicating the mapping between these catalogues and ours) resulted in further modifications to our requirements.

C.1 Council of Europe Requirements

The Council of Europe requirements catalogue is discussed at length in chapter 5.

Table C.1: Mapping from Council of Europe requirements to ours

1a	Usab_2, Org_8, Org_9
1b	Usab_1
2	not applicable to the systems under consideration
3	Usab_3, Funct_11
4	not applicable to the systems under consideration

5a	Sec_2
5b	as per paper-only elections
6	not applicable to the systems under consideration
7	Sec_22
8	not applicable to the systems under consideration
9	as per paper-only elections
10	Usab_6
11a	Funct_12
11b	Sec_12
12	Funct_3
13	Funct_12
14	Usab_5
15	Sec_20
16	Sec_13, Sec_14
17	Sec_13, Sec_14
18	as per paper-only elections
19	Sec_13, Sec_14
20	Org_5, Org_8
21	Org_5
22	Org_8
23	Org_2, Audit_4
24	Assur_6, Org_5
25	Assur_7, Assur_10, Assur_11
26a	Funct_8
26b	Sec_1
27	Funct_8
28	Org_2, Org_3, Org_4, Org_5, Org_7, Assur_9, Assur_10, Assur_11, Assur_12

29	Sec_18, Org_3
30	Sec_8
31	Sec_19, Org_3
32	Sec_4, Org_2
33	Sec_4, Org_2
34a	Sec_24, Sec_17, Sec_3, Sec_20
34b	Sec_13, Sec_14
34c	over specification in this context
35	Sec_13, Sec_14
36	as per paper-only elections
37	as per paper-only elections
38	Org_8
39	as per paper-only elections
40	not applicable to the systems under consideration
41	not applicable to the systems under consideration
42	not applicable to the systems under consideration
43	not applicable to the systems under consideration
44	not applicable to the systems under consideration
45	not applicable to the systems under consideration
46a	Org_8
46b	not applicable to the systems under consideration
47	Funct_3
48	as per paper-only elections
49	not applicable to the systems under consideration
50	not applicable to the systems under consideration
51	not applicable to the systems under consideration
52a	Sec_12
52b	Org_3

53a	Sec_16
53b	as per paper-only elections
54	as per paper-only elections
55	over specification in this context
56	Org_2, Audit_4
57	Sec_5
58	Sec_5
59	Sec_5
60	outside the scope of these requirements
III	Assur_9
61	Org_8, Usab_3, Funct_11
62	Assur_8
63	Usab_3, Funct_11
64	Funct_11
65	Usab_1
66	Assur_7 (over specification in this context)
67	over specification in this context
68	over specification in this context
69a	Org_5
69b	Org_3
70	Org_4
71a	Org_4
71b	Org_10
72a	Assur_10, Assur_11
72b	indecipherable
73	Org_3, Org_10
74	Org_3, Org_2, Sec_4
75a	Org_3

75b	Org_4
75c	Org_6
76	Org_2
77	Sec_3, Org_3, Org_10
78a	Sec_13
78b	not applicable to the systems under consideration
79	Org_3
80	Org_2, Sec_4
81	Org_2, Sec_4
82	as per paper-only elections
83a	Sec_5
83b	Audit_7
83c	Audit_6
84	Audit_7 (see also section 5.6.4)
85	outside the scope of these requirements
86	not applicable to the systems under consideration
87	not applicable to the systems under consideration
88	outside the scope of these requirements
89	not applicable to the systems under consideration
90a	Funct_6
90b	not applicable to the systems under consideration
91	as per paper-only elections
92	Sec_18, Sec_20
93a	Sec_12
93b	not applicable to the systems under consideration
94a	as per paper-only elections
94b	Sec_2
95	Funct_6

96	Funct_6, Sec_22
97	Sec_17
98	Sec_22, Funct_8
99	Sec_20, Org_6
100	Sec_5
101	Sec_5
102	Sec_5
103	Audit_1
104	Org_2, Audit_4
105	Audit_4
106	Audit_8
107	Sec_5
108	Sec_5
109	Audit_5
110	outside the scope of these requirements
111	Org_1
112	outside the scope of these requirements

C.2 Requirements from Chapter 5

The requirements in chapter 5 (originally published in [41]) were developed as part of a critical analysis of the CoE standards in an attempt to overcome some of the faults identified.

Table C.2: Mapping from requirements in chapter 5 to those in this chapter

1	Org_4
1.1	Org_4

1.2	Org_4
1.3	Org_9
1.4	Sec_8
1.5	not applicable to the systems under consideration
1.6	not applicable to the systems under consideration
2	Usab_1
2.1	Usab_2, Usab_5
2.2	Assur_8
2.3	Usab_3, Funct_11
3	Org_8
3.1	outside the scope of these requirements
3.2	outside the scope of these requirements
3.3	not applicable to the systems under consideration
4	Sec_2
5	outside the scope of these requirements
6	Sec_22
7	as per paper-only elections
8	as per paper-only elections
9	as per paper-only elections
10	Funct_3
11	Sec_16
12	Funct_12
13	Sec_13
13.1	Sec_13
13.2	Sec_13
13.3	Org_3
13.4	Funct_12, Sec_12
13.5	not applicable to the systems under consideration

13.6	Audit_8
14	Funct_6
14.1	Funct_7
14.2	Funct_6
15	Sec_20, Sec_1
16	Sec_22
16.1	Sec_22
17	Org_2
17.1	Sec_5
17.2	Org_2
18	Sec_5
18.1	Audit_1, Audit_2
18.2	Audit_1
18.3	Audit_4
18.4	Audit_3
18.5	Audit_2
19	Assur_2, Assur_11
19.1	Assur_9
19.2	Sec_15
19.3	Org_3
19.3(a)	Assur_2
19.3(b)	Sec_19
19.3(c)	Org_3
19.3(d)	Assur_2
19.3(e)	Assur_2
19.4	over specification in this context
19.5	Org_1
19.6	Org_1

19.7	Org_5
19.8	Sec_8, Org_4
19.8(a)	Org_4
19.8(b)	Sec_3, Org_4
20	Sec_1 – Sec_25
20.1	Org_6, Sec_17, Audit_6
20.2	Org_2, Sec_4, Audit_4
20.3	Org_3, Org_2
20.4	Sec_19, Org_3
20.5	Org_2
20.6	Org_3, Org_2, Sec_4
20.6(a)	Org_2
20.6(b)	Org_2
20.6(c)	Org_2
20.6(d)	Org_2
20.6(e)	Org_3, Sec_4
20.6(f)	Org_2
20.6(g)	Org_3, Sec_4
20.6(h)	Org_3
21	Sec_1, Org_7
21.1	Org_8, Org_5

C.3 German Regulations for Voting Devices

The newest version of the German Regulations for Voting Devices [37] dates back to 1999. These requirements are very specific and in some points even over specified. The regulations distinguish between organizational and technical

requirements and they define the responsibilities for (re) evaluation, certification and revocation, but not the evaluation process itself.

Table C.3: Mapping from German Regulations for Voting Devices (BWahlGV) to our requirements

BWahlGV	
1	Org_1
2(1)	outside the scope of these requirements
2(2)	outside the scope of these requirements
2(3,4)	Org_1
2(5)	Org_5
2(6)	Org_1
3	Org_1
4(1)	Org_5
4(2)	as per paper-only elections
5	as per paper-only elections
6a	outside the scope of these requirements
6b	Org_5
7(1)a	Assur_5
7(1)b	Org_10
7(2)	Org_3
7(3)	Org_9
8(1)	Org_3
8(2)	Org_3
8(3)	Org_9
8(4)	Org_9
8(5)	Org_9
8(6)	Org_1

9(1)	as per paper-only elections
9(2)	as per paper-only elections
10(1)	Org_3
10(2)a	over specification in this context
10(2)b	Org_2, Org_10
11(1)	as per paper-only elections
11(2)	as per paper-only elections
11(3)	Sec_2
11(4)	Org_4
11(5)	Org_3
12	Org_3
13	Org_3
14	Org_3
14(1)	Org_3
14(2)	outside the scope of these requirements
14(3)	Org_3
14(4)	over specification in this context
14(5)	Org_3
14(6)	removed by catalogue authors
15(1)	Org_3
15(2)	Org_4
15(3)	Org_3
16(1)	Org_3
16(2)	Org_3
17(1)	Org_3
17(2)	Org_6
17(3)	Org_3
18	not applicable to the systems under consideration

19	removed by catalogue authors
20	not applicable to the systems under consideration

BWahlGV Appendix 1	
A a-e	outside the scope of these requirements
A f	Assur_4
B 1	Assur_5
B 2.1a	Assur_2
B 2.1b	Sec_18
B 2.2	Sec_8, Assur_3, Org_3, Assur_5
B 2.3	Sec_3, Sec_8
B 2.4a	Sec_2, Sec_20, Assur_1, Funct_2
B 2.4b	Sec_21
B 2.5	Sec_8
B 2.6a	outside the scope of these requirements
B 2.6b	Org_3
B 3.1a	outside the scope of these requirements
B 3.1b	Sec_2, Funct_12
B 3.1c,d	Usab_1
B 3.2a	over specification in this context
B 3.2b	Sec_9
B 3.3a,b	Funct_3
B 3.3c	Funct_6
B 3.3d	Funct_12
B 3.3e	Funct_6
B 3.3f	Funct_10
B 3.4a	Funct_9
B 3.4b	over specification in this context

B 3.4c	over specification in this context
B 3.4d	Sec_22
B 3.4e	Funct_4, Sec_3
B 3.4f	Sec_16, Sec_17, Funct_1
B 3.4g	Funct_1, Sec_13
B 3.4h	Funct_8
B 3.5a	Sec_6, Sec_7, Usab_1
B 3.5b	Assur_1
B 3.5c	Sec_17
B 3.5d	Sec_2
B 3.5e	Org_3, Sec_17
B 3.6a,b	Sec_2
B 3.6c	Funct_1
B 3.6d	Funct_12, Sec_9, Usab_6
B 3.7a	Usab_2
B 3.7b	over specification in this context
B 3.7c	Sec_8
B 4	Assur_5

C.4 PTB Requirements

Requirements for "Online-Voting Systems for Non-parliamentary Elections networked polling-station elections" were developed by the PTB (Physikalisch-Technische Bundesanstalt) [38]. The catalogue contains technical and organizational requirements and is based on an analysis of other available requirement catalogues. The requirements are classified according to election phases (Preparation of election = *·election setup·*, Voting phase = *·polling period·*, Determination of election result = *·counting phase·*, Wrap-up and safe-keeping

= ·*archiving period*·). Where requirements apply across multiple phases or to the whole ·*election*· they are classified as "cross-sectional functions"

Table C.4: Mapping from PTB Requirements to ours

Preparation of election (PE)	
PE 1-1	as per paper-only elections
PE 1-2	Usab_1
PE 2 (1-6)	not applicable to the systems under consideration
PE 3-1	Usab_1, Assur_5
PE 4-1	Assur_5
PE 4-2	Assur_5, Org_8
PE 4-3	Org_2, Sec_4, Org_3
PE 4-4	Org_2
PE 4-5	as per paper-only elections
PE 4-6	not applicable to the systems under consideration
PE 4-7	as per paper-only elections
PE 4-8	Assur_7, Assur_10, Assur_11
PE 4-9	Assur_7
PE 4-10	over specification in this context
PE 4-11	Org_11, Org_4
PE 4-12	Org_4

Voting phase (VP)	
VP 1-1	as per paper-only elections
VP 1-2	Sec_13
VP 1-3	not applicable to the systems under consideration
VP 1-4	not applicable to the systems under consideration
VP 1-5	not applicable to the systems under consideration

VP 1-6	Sec_2
VP 1-7	Funct_5, Usab_1
VP 2 (1-5)	not applicable to the systems under consideration
VP 3-1	Funct_7
VP 3-2	Funct_7
VP 3-3	Org_3
VP 3-4	Funct_3
VP 3-5	Funct_3
VP 3-6	Org_8
VP 3-7	Funct_1, Funct_2
VP 3-8	Funct_6
VP 3-9	Sec_3, Sec_9, Sec_10
VP 3-10	Funct_12, Sec_9
VP 3-11	Funct_12
VP 3-12	Usab_1
VP 3-13	Sec_2
VP 3-14	Usab_6
VP 3-15	Sec_13
VP 3-16	Sec_12
VP 3-17	Sec_2
VP 3-18	Usab_5
VP 3-19	Usab_5
VP 4-1	Funct_6
VP 4-2	Funct_6
VP 4-3	Sec_16, Sec_20
VP 4-4	Sec_17
VP 4-5	Org_3
VP 4-6	Sec_22

VP 4-7	Org_4
VP 5-1	Sec_22
VP 5-2	Sec_20
VP 5-3	Sec_3
VP 5-4	not applicable to the systems under consideration
VP 5-5	Org_4, Assur_5
VP 5-6	Sec_16

Determination of election result (DR)	
DR 1-1	Org_3
DR 1-2	Sec_3
DR 1-3	Org_3
DR 1-4	Org_3
DR 1-5	Usab_1
DR 2-1	Sec_16
DR 2-2	Sec_22
DR 2-3	Sec_22
DR 2-4	Usab_1
DR 2-5	Funct_8
DR 2-6	Funct_8
DR 2-7	Sec_17

Wrap-up and safe-keeping (WS)	
WS 1-1	Org_6
WS 1-2	Sec_7, Org_3
WS 2-1	Org_3
WS 2-2	Org_6
WS 2-3	Org_2

WS 2-4	Org_3
WS 2-5	Org_6
WS 2-6	Org_3

Cross-sectional functions (CF)	
CF 1-1	Assur_6
CF 1-2	Sec_25, Assur_4
CF 1-3	Assur_10, Assur_11
CF 1-4	Assur_2, Assur_5
CF 1-5	Assur_2
CF 1-6	Assur_5
CF 1-7	Sec_8
CF 1-8	Assur_3
CF 1-9	Sec_3, Sec_8, Sec_20, Sec_13
CF 1-10	not applicable to the systems under consideration
CF 1-11	Org_4
CF 1-12	Sec_10
CF 1-13	Org_4
CF 2-1	not applicable to the systems under consideration
CF 2-2	Sec_17, Sec_24, Audit_6
CF 2-3	Org_4
CF 2-4	Org_4
CF 2-5	Org_4
CF 2-6	Sec_17, Sec_24, Audit_6
CF 3-1	Sec_13
CF 3-2	Sec_13
CF 3-3	Assur_6
CF 3-4	Assur_11, Assur_10

CF 3-5	not applicable to the systems under consideration
CF 3-6	Org_2
CF 4-1	Sec_5
CF 4-2	Audit_8
CF 4-3	Sec_5, Audit_2
CF 4-4	Audit_5

C.5 Michael Shamos' "Commandments"

In 1993 Michael Shamos presented a paper titled Electronic Voting - Evaluating the Threat [119] which contained the following "commandments". Though somewhat tongue-in-cheek, they capture the high-level requirements of e-voting.

Table C.5: Mapping from Michael Shamos' "Commandments" to our requirements

I. Thou shalt keep each voter's choices an inviolable secret.	Sec_13
II. Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote.	Sec_2
III. Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.	Sec_18, Sec_20
IV. Thou shalt report all votes accurately.	Funct_6
V. Thy voting system shall remain operable throughout each election.	Org_4
VI. Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I.	Sec_1, Sec_5, Audit_8

C.6 Summary Table

Table C.6: Summary of our requirements: principles upheld; whether covered by other catalogues; evaluation technique(s); whether contains *·responsible election authority·* variable

Req.	[un]	[eq]	[fr]	[se]	[di]	[tr]	New [1]	Eval. [2]	Var. [3]
Sec_1		✓			✓			4	
Sec_2		✓						4	✓
Sec_3					✓			4	
Sec_4	✓	✓	✓	✓	✓	✓		4	
Sec_5	✓	✓	✓	✓	✓	✓		4	✓
Sec_6		✓					✓	4	
Sec_7		✓						4 6	
Sec_8	✓							4	✓
Sec_9	✓							4	
Sec_10	✓							4	
Sec_11	✓						✓	4	
Sec_12				✓				4	
Sec_13				✓				4, 6	
Sec_14				✓				4	
Sec_15		✓		✓		✓		4	
Sec_16			✓	✓				4	
Sec_17					✓			4	✓
Sec_18	✓	✓	✓	✓	✓	✓		4	
Sec_19	✓	✓	✓	✓	✓	✓		4	

[1] Not covered by other catalogues
[2] Evaluation technique(s) – see section 4.4
[3] Requires definition of *·responsible election authority·* variable – see section 6.3

Req.	[un]	[eq]	[fr]	[se]	[di]	[tr]	New	Eval.	Var.
Sec_20					✓			4	
Sec_21				✓				4	
Sec_22					✓			4	
Sec_23					✓		✓	4 6	
Sec_24					✓			4	
Sec_25					✓			4	
Funct_1				✓				4	
Funct_2				✓				4	
Funct_3			✓					4	
Funct_4					✓			4	
Funct_5		✓						4	
Funct_6		✓	✓					4	
Funct_7			✓					4	
Funct_8						✓		4	
Funct_9	✓							4	✓
Funct_10			✓					4	✓
Funct_11	✓							4, 6	✓
Funct_12			✓					4, 6	
Funct_13			✓				✓	4, 6	
Funct_14	✓	✓	✓	✓	✓	✓	✓	4	
Usab_1	✓							1	✓
Usab_2	✓							1	✓
Usab_3	✓							1	
Usab_4	✓		✓					1	
Usab_5						✓		1	
Usab_6			✓					1, 6	
Usab_7	✓	✓	✓	✓	✓	✓	✓	1	
Org_1						✓		2	

Req.	[un]	[eq]	[fr]	[se]	[di]	[tr]	New	Eval.	Var.
Org_2						✓		2	✓
Org_3						✓		2	✓
Org_4						✓		2	✓
Org_5						✓		2 6	✓
Org_6					✓			2	
Org_7						✓		2, 6	
Org_8			✓			✓		2	
Org_9	✓							2	
Org_10	✓	✓	✓	✓	✓	✓		2	
Org_11	✓							2	
Assur_1		✓						4 6	
Assur_2						✓		3	
Assur_3	✓							3	✓
Assur_4		✓			✓	✓		4	
Assur_5						✓		3	✓
Assur_6						✓		3 6	
Assur_7	✓					✓		3	
Assur_8	✓							3 6	
Assur_9						✓		2	✓
Assur_10	✓	✓	✓	✓	✓	✓		2	✓
Assur_11	✓	✓	✓	✓	✓	✓		2	✓
Assur_12	✓	✓	✓	✓	✓	✓		2	
Audit_1						✓		4	
Audit_2						✓		4, 6	
Audit_3						✓		4	
Audit_4						✓		4	
Audit_5						✓		4	
Audit_6						✓		4	

Req.	[un]	[eq]	[fr]	[se]	[di]	[tr]	New	Eval.	Var.
Audit_7						✓		4, 6	
Audit_8						✓		4	
VVAT_1		✓				✓	✓	2	
VVAT_2					✓	✓	✓	2	
VVAT_3				✓		✓	✓	2	
VVAT_4					✓	✓	✓	2	✓
VVAT_5					✓	✓	✓	2	
VVAT_6		✓				✓	✓	2	
VVAT_7					✓	✓	✓	2	
VVAT_8	✓	✓	✓	✓	✓	✓	✓	2	✓