

Procedural Security in Electronic Voting

Alexandros Xenakis and Prof. Ann Macintosh
International Teledemocracy Center, Napier University, Edinburgh
a.xenakis@napier.ac.uk a.macintosh@napier.ac.uk

Abstract

In this paper we explore the security related procedures that are required for the successful development and deployment of electronic voting in legally-binding government elections. Initiating our research on the theoretical basis, which justifies the necessity for security in deploying electronic elections, we further explore the question of who and what should be safeguarded in the course of the e-electoral process. Based on our research study, we suggest that security in e-voting has two aspects, the technical and the procedural one. It is recognised that from the technical perspective further research is necessary to ensure full and complete voter authentication and voting security to enable an e-election. However, we argue that e-voting security can also be enhanced through providing procedural security measures at specific points in the e-electoral process.

Our analysis of the Electoral Commission's evaluation reports on the 2002 UK local government e-voting pilots identified past cases of procedural security issues. Interviews and observations conducted during the 2003 UK e-voting pilots further confirmed these issues. We have established the need to further explore the re-design of the electoral process and consider procedural security as primarily applicable to agent-related processes. In view of the increased complexity of the e-voting processes, which can involve multi-channel e-voting options, and the increase in the number of agents involved in the administration of e-elections, we relate procedural security to the need for transparent allocation of responsibilities among the different agents. In concluding we argue that existing procedural security should be enhanced, that there is a clear need for better monitoring of compliance to such procedures and that further security procedures need to be put in place at specific points in the e-election process.

1. Introduction

The issue of security in the context of the electoral process is referenced as one of the most important constraints in the implementation of electronic voting. The Caltech-MIT Voting Technology Project [1], in their report quote:

"Security is as important as reliability in guaranteeing the integrity of the voting process and public confidence in the system. People do not use things in which they have no confidence. Losing confidence in elections means losing confidence in our system of government."(p. 42)

Coleman [2], as chair of the ICAVM (The UK Independent Commission on Alternative Voting Methods) accordingly argues that:

"The probity, accuracy, and security of electoral arrangements are integral to the vitality and credibility of democracy" noting *"One thing is for certain: public confidence in democratic elections takes decades to develop and far less time to destroy"* (p. 6)

We can therefore establish that the introduction of electronic voting has to be implemented in a secure form so as not to jeopardise the existing public confidence in the electoral procedures.

Security is a problem because, to date, the commercially available technology does not provide a completely secure e-transaction environment. Security can therefore, primarily be considered as a technological problem. It is not the aim of this research to address the future technical advances of security in electronic voting, but rather, in the course of this paper, we will explore, how we can improve the level of security of the e-voting procedures, given the established limitations of technology in addressing the issue in question. We will primarily present the set of concepts related to the issue of security as well as the factors on which security measures depend.

The context of this research paper lies in the experience gained through the 2002 and 2003 UK Local Authority e-voting pilots. All pilot schemes formed part of legally binding elections on a local authority level. For each pilot project, a special order

of law was passed by the Parliament, allowing the experimentation of e-voting technologies in real election circumstances. Sixteen e-voting pilot projects took place in May 2002 followed by another 18 in May 2003. These involved Local Authority elections, experimenting with Internet, touch-tone IVR (interactive voice response), SMS text messaging, kiosk and digital television voting, along with e-counting of paper ballots and the use of smart cards for voter identification purposes. Detailed evaluation of all 2002 pilots has been produced by the Electoral Commission. At the time of writing this paper the 2003 evaluation reports have still to be published.

In summer 2002 the UK Government published a consultation paper on a strategy for e-democracy [25]. This stated that the Government's aim was to put "robust systems in place for an e-enabled General Election after 2006" (p.47).

2. Research methodology

The research presented in this paper forms part of a doctoral programme concerned with the identification of the emerging constraints in re-designing the electoral process in relation to ICTs. The first half of this research has involved an extensive literature search on e-voting and some empirical work. The main material for the empirical work comes from the UK e-voting pilots. The research methodology is outlined in figure 1.

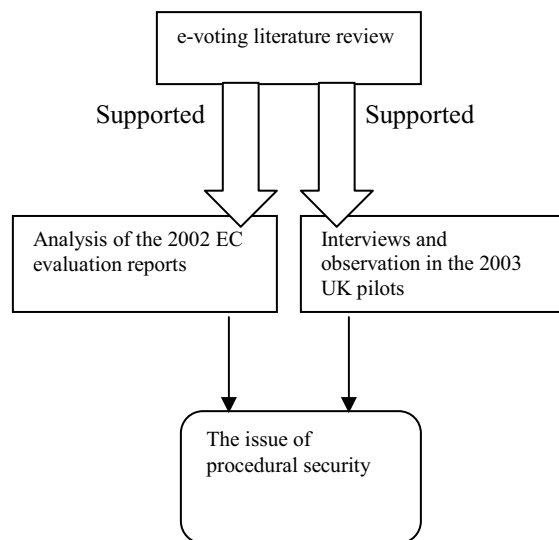


Figure 1. **Research methodology**

The results from our research indicate that the issue of procedural security has emerged as an important

constraint in the re-design of the electoral process to an e-voting/e-enabled one.

3. Security elements in electronic voting

Different emphasis is given to the concept of security in existing literature. The Caltech-MIT [1] report refers to two broad types of security problems; manipulation of voters and tampering with the recording of votes and counting mechanisms. From their point of view secrecy, as in the principle of the secret ballot, is a procedure to prevent voter manipulation. In the ICAVM report [2] security is defined as: "protection against voter impersonation and tampering" (p.6). The UK Government in its response to the Electoral Commission's strategic evaluation [3] of the 2002 e-voting pilots [29] acknowledges two aspects of security; maintaining the secrecy of the vote and providing a secure infrastructure to transport, collect, count and audit votes. The OASIS Election and Voter Services Technical Committee take a system design perspective relating to security a set of requirements such as voter identification, proof of voter eligibility, confidentiality of the voters' choice, secure exchange of data with remote voters, sealing of cast votes and accuracy of counting [28]. In one of the official e-voting web sites from the 2003 UK pilots under the general term of security issues the Local Council explained to prospective voters (users) of the piloted e-voting technologies, that the system was secure because it was protected from fraud, mechanical and electrical failure, it authenticated the voter's identity which was in turn protected along with one's vote [35]. However the most comprehensive context of security in e-voting is provided in the e-voting security study prepared by the CESA (Communications-Electronics Security Group) for the UK Government [34]. The CESA standards consider security to be related to a set of principles including voter authenticity, voter anonymity, data confidentiality, data integrity, system accountability (operations are logged and audited), system integrity (not to be able to reconfigure the system during its operation), system disclosability (allowing external scrutiny), system availability (encountering accidental or malicious denial of service attacks), system reliability (developing non-problematic systems), personnel integrity along with operator authentication and control.

4. Security Dependencies

In order to provide a secure environment to conduct electronic voting a series of different factors have to be considered. Firstly the provision of security measures depends on the voting technology used to provide alternative voting channels. Fairweather and Rogerson [24] in their technical options report differentiate between technical solutions for authentication, user interface and conduit (network) for the transportation of data. In the case of kiosk voting in the 2003 Sheffield local government pilot, voter authentication could be achieved either by using a unique combination of pin and password, or by inserting a smart card in a smart card reader that the kiosk provided, instead of the pin [35]. However if voters preferred to cast their vote through the Internet, the authentication measures involved accessing a secure web site and entering the provided pin and password. In the case of SMS voting, in the same pilot, the voter had to create a text message including the pin and password provided along with the preferred candidate's voting code. A similar process to the internet security measures was used for the digital television interface in the 2003 pilots [36].

Security also depends on the approach that each commercial vendor takes in providing e-voting systems to the local government. All e-voting pilot schemes are funded by the central government. There is a formal procurement process inviting commercial vendors to apply, and if successful, become suppliers of e-voting systems to the Government. Successful suppliers are then matched by the central government with the local government authorities, which have also submitted applications to hold an e-voting pilot project in their forthcoming election. Since security is so important, providing the most secure system is a competitive advantage in the e-voting industry. Therefore it is possible to encounter different security measures in the delivery of the same voting channel provided through a different vendor. In the 2002 pilots, internet voting provided in the St Albans local government pilot [4] required the use of pin and password for authentication purposes. Internet voting provided in the Swindon local government pilot [5], by a different commercial supplier, additionally required voters to enter their date of birth.

Furthermore security depends on the location from which voting takes place. Remote or unsupervised voting is by nature more difficult to provide in a secure environment since the voting environment is not controlled by the election administrators, as is the case with polling stations, which in the UK are staffed by government officials. Fairweather and Rogerson [24], in their technical options taxonomy, propose four locations related to electoral procedures, polling place, home, work and public place. Xenakis and Macintosh

[39] have supplemented that with the counting location, as traditionally in the UK the count takes place in a central location and this is currently the same in the e-counting of paper ballots.

Another factor affecting the implementation of security is the delivery of multiple channel simultaneous electronic voting. The CESG security study [34], formally admits that: *"Any election that allows multiple delivery channels cannot keep them perfectly in synchronisation down to the millisecond"* (p.53). The 2002 Sheffield and Liverpool pilots [6],[7] addressed this problem by implementing an electronic version of the electoral register, and a similar solution was introduced for the 2003 Sheffield pilot.

Security measures are also formed on the basis of legal requirements surrounding an election. Based on the Watt [38] and OSCE [31] reports, Xenakis and Macintosh [39] in their taxonomy of legal accountabilities in e-voting in a UK context, presented sixteen legal issues. Half of them are directly related to the security of the electoral procedures, namely the issues of voter identification, voter eligibility, unlawful influence, secrecy, tampering with election material and data, personation, openness to audit and accuracy of results.

Finally security is dependent on usability. The OSCE report refers to: *"balancing of voter accommodation with safeguards against fraud"* (p.27). The Internet Policy Institute in its report dedicated to Internet voting [26] refers to balancing security with other interests, which include interface usability. In the course of a semi-structured interview conducted by the author in relation to the 2003 Sheffield pilot, the Returning Officer emphasized the importance of the usability constraints in the introduction of security measures. He specifically mentioned the choice of introducing a 9 digit password instead of a 16 digit one, as proposed in the CESG security study, on the sole basis that a 16 digit "blind" (not seen while entered) password would not promote the ease of use of the system. Finally, the Electoral Commission [19] in setting standards for e-voting technology specifically asks that: *"Compatible with security considerations, PIN numbers and passwords should be kept to the minimum length possible"* (p.30). The NOP [27] survey on the public opinion on the 2002 pilots regarded the "ease of use" as one of its four evaluation criteria.

To summarize, a secure environment for the delivery of e-voting, is dependent on:

- The type of voting technology used
- The commercial vendor supplied security checks

- The location from where the voting technology is offered
- Whether or not voting is offered through multiple channels at the same time.
- The existing legislation surrounding an election
- The usability of the e-voting system

5. Technologies used and technical security constraints

In the 2002 local government pilots, all 16 local authorities used electronic counting schemes – 7 of which combined with traditional paper ballots only, 6 provided e-voting in the form of touch-screen voting kiosks, 5 provided internet voting, 3 provided phone (touch tone) voting and 2 SMS text message voting [33]. In the local elections held on the 1st May 2003, 20 e-voting pilot projects were approved, having at least one e-voting element. In total 8 Local Authorities piloted e-counting of paper ballots, 8 offered kiosk voting either at polling stations or in public spaces, 14 provided internet voting, 12 piloted phone voting, 4 SMS voting and 3 digital television voting being tested for the first time in the UK [23].

Fairweather and Rogerson [24], refer to four main categories of technological areas posing problems to establishing electronic voting security:

- Denial of service attacks. Hackers could cause these by overloading a system with requests of information, thus preventing voters from casting their ballot.
- Viruses or malicious software could corrupt voting software installed on client (voter) equipment, which could in turn disrupt the casting of votes.
- Hacking of servers could affect the integrity of the vote by breaking into computer systems with the purpose to alter, copy or damage data records and software.
- Limitations to the system's capacity to cope with peak demand during the voting period are purely based on the requirements set in designing e-voting systems and the efficiency of the system provided by the commercial suppliers.

A more detailed approach is taken in the CESG security study. This addresses the same technical problems but focuses on the agents who could provoke them. However, in the context of this paper such technical problems are left to be fully resolved by future technological advances. We consider existing

technical security limitations as the given constraints, which have to be managed by means other than technological research, aiming to decrease the threat they pose to the security of the electoral process to the minimum possible degree.

6. The concept of procedural security in electronic voting

We consider the term procedural security to include all security measures related to the conduct of e-enabled elections, which involve the redesign of an electoral procedural activity, or the introduction of a supplementary process activity or mechanism, aiming at upgrading the security level of the e-voting process, given the technical limitations on security.

The CESG [34] security study refers to: “ *a combination of technical and procedural measures*” (p.25) in relation to four specific security objectives:

- Effective voter registration
- Effective voter anonymity
- Effective vote Confidentiality
- Effective system registration (allowing users to access the system)

The same report also considers as a security objective to establish operator integrity on an administrators' level, as they are in an enhanced position to attack the system, and open auditing by keeping a record of significant transactions.

In line with the above set standards, the statement of requirements for commercial companies tendering to be an e-voting supplier for the 2003 pilot projects [30], called for physical security measures, staff with government level security clearance and political affiliations, while staff and system would be monitored providing access trails and records of actual security breaches.

6.1 Examples of procedural security issues in the 2002 pilots

The 2002 pilots have provided some interesting examples of procedural security issues. In the cases of Westminster and Rugby local government pilots, where the same vendor was contracted [8],[9] the counting process could be accessed only by authorised staff, after scanning a bar coded identity card. Data was stored in a database regulated by two administrators each holding a different 12 character password. The database itself was additionally password protected and a report was run before the start of the count to ensure that there were no pre-loaded votes. However no

precaution was taken against access through a default ID created at the time of the installation of the operating system. In Broxbourne [10] access to the counted votes was allowed to two officials who theoretically could alter the votes with their actions being logged. However this process was never followed; instead all operators of the system used the same user ID not allowing traceability of their actions. Had the proper process been followed, a higher level of security would have been achieved.

In Epping Forrest, South Tyneside and Chorley [11],[12],[13] where the same counting machinery and result collating software were used. The vendor provided software allowed different levels of access to different types of users, however this feature was not used.

In Stratford and Bolton [14],[15] where the same type of touch-screen voting kiosk was used, the data was automatically recorded on a module and archived for six months to provide an audit trail if required. As the module could be physically detached from the kiosk and transferred to the counting centres, secure transportation was also needed. The kiosk used in Chester and Newham [16],[17] had a triple data recording system. Each vote was recorded in the machine's flash memory, and to a data cartridge and at the end of the vote a print out audit was produced. The merged table – containing the results of all cartridges – was locked to prevent any alterations of the produced results. In the case of Newham three administrators had access rights and another three had “super-user” access rights but the system required two of them being present simultaneously for any changes to be made, therefore enhancing the level of security by introducing this specific procedural safeguard.

In Swindon [5] all voters were provided with a 10 digit pin, but a date of birth was also required to allow remote voting, although there were no means available to verify the accuracy of the birth date provided by the voters. This extra element although in line with the ICAVM recommendation [2] that voters should provide their birth date at the time of registration, created usability problems in entering the date through the touch-tone telephone interface.

In St. Albans [4] and Crewe [18] voters were issued separately with a 4-digit PIN and a 16-digit VIN (voter identification number) for remote voting. The double mailing of the two separate access tokens provided one extra layer of security simply by following this process. Passwords to the servers were issued to the vendor's staff although different people had access to their relevant part of the software; this procedure also created one extra layer of procedural security by accordingly adjusting the design of the e-voting system.

In contrast, a different approach was used in Liverpool [6] and Sheffield [7]. All voters were issued with a 6 digit VRN (voter reference number), an 8-digit pin and a 10-digit password. However, all numbers were delivered to the homes of the voters in the same envelope, therefore reducing the security effectiveness of the multiple technical access tokens, through the lack of the procedural safeguard of double mailing.

A further option in the 2002 pilots was the provision of an Acting Returning Officer, to visit on request, a visually impaired person with the voting device to allow them to vote in secret [29], therefore providing an option safeguard against undue influence on physically disenfranchised voters.

6.2 Examples of procedural security issues in the 2003 pilots

At the time of writing this paper the full evaluation analysis by the Electoral Commission of all the 2003 e-voting pilots has not been published, however it does appear that some of the security issues encountered in the 2002 pilots were addressed. Our initial results have been gathered through observation and interviews undertaken during an e-voting pilot at one of the Local Authorities in May 2003. In Sheffield the issue of password was improved. A double mailing of access tokens was used as an extra measure of security. This case involved the distribution of a hardware token, a smart card containing the pin, and a password distributed along with the traditional distribution of the polling card. For touch-tone telephone voting and SMS text message voting the voting code attributed to each candidate was personalised for each voter in order to provide an extra measure of security. However there were issues with regard to usability. The UK law requires candidates for an election to be presented on the ballot paper in consecutive numerical order, with the number on the left side of their names. Personalised voting codes were also a numerical two-digit code, which were put on the right side of a candidate's name. Therefore there was a possibility of the voter using the numerical order digits to select a candidate rather than the personal voting code.

In the case of Rushmoor [37] delivering internet voting, voters were asked to register specifically if they wanted to vote over the internet. A special register of e-voters and a revised version of the register with those entitled to vote the traditional way were in place for the Election Day, therefore potentially excluding double voting. In Sheffield where multiple channel, simultaneous voting was piloted, in cases of double voting, the paper ballot cast would be counted. Cases

of double electronic voting were excluded as long as the e-version of the registered performed as expected. In examining staff training material there appeared to be some instances where the software interface could have allowed the e-voting system to be accessed, if two authorised administrators entered their passwords. The two-person rule is also included in the CESG [34] e-voting security study in relation to operators' integrity. The same system also allowed administrators to change their passwords once they had accessed their system for the first time. During the election day, this feature led to at least one case of a presiding officer of a polling centre, losing access to the on-line electoral register as they had forgotten the password entered when prompted to change the original password given.

6.3 Overview of procedural security issues

In this section we have considered both the 2002 and 2003 local government e-voting pilots from the perspective of procedural security. From this we have highlighted specific examples, which cause concern. These include:

- Lack of procedures to check vendor-installed systems for security breaches.
- Government personnel not following the procedural security guidelines
- Inadequate checking of voter provided data
- Security is compromised because of usability issues such as the case of the voter authentication process
- Lack of procedures to secure voter passwords and pin data.
- Lack of procedures to exclude double voting through multiple voting channels.
- A multiplicity of processes which provide authorised administrator rights to voting systems and voting data without always providing traceability of administrators' actions.

How to overcome such procedural security problems creates many challenges. Some possible mechanisms to overcome these challenges are further discussed in the following sections.

7. Procedural security and allocation of procedural responsibility

In practice, the redesign of the electoral process in a UK context is happening in many experimental forms, depending on the choice of piloted technology and

commercial vendor. There are three principle challenges deriving from the redesign of the electoral process as it is actually happening in the UK since the first major e-voting pilots in May 2002.

The first concerns the deployment of simultaneous multiple channel electronic voting. The challenge is to ensure that is an adequate level of procedural security in place to guarantee one vote, and only one vote, is cast per eligible voter, given that there is the possibility for that voter to choose from a variety of e-voting options. For example, in the case of the UK 2003 pilots one local government authority offered four voting options – SMS, IVR, Internet and traditional-paper. To address this, the Electoral Commission wishes to explore the electronic management of voter registration [20]. They propose procedural reform [21] such that multiple channel real-time e-voting combined with traditional ballots should only happen under the provision of a national electronic register.

The second challenge is to establish procedural security measures to ensure adequate staff training and voter education on the interaction with the new technology (both hardware and software) is provided and undertaken appropriately in order to reduce usability issues. This is further complicated in hybrid electoral processes where only specific stages of the process are electronic. An example of a hybrid stage is the electronic register of voters as piloted in the Sheffield 2003. In this case, the voters were able to vote electronically (through internet, SMS, touch-tone telephony or public kiosk) during a specified period leading up to the actual election day and on election day, or they could choose to visit any polling station of their convenience on election day where they would be authenticated by a government agent. In order to establish the voter's right to cast a ballot, the government agent was equipped with an internet connected laptop through which they could check the central electronic register and establish the eligibility of the voter. Optionally these voters could use a smart card which had been provided to them prior to the election. This meant that instead of the voter stating their identity and the government agent searching the register, the smart card passed over a plug-in reader would automatically did the eligibility check, without the need to key in the voter name or address. After the authentication of the voter had been established they would proceed to cast a paper ballot in the traditional way. This e-enabled, but not totally electronic, electoral process involves the interaction of people, either voters or local council staff, with different pieces of software (e-version of the electoral register, connectivity software, web browser software) and hardware (laptop, smart card, smart card reader) in order to e-enable the electoral process; that produces a

hybrid version of the traditional electoral procedures. There are many human-error interaction risks in any hybrid process model of this kind that could interrupt the normal flow of the process.

The third challenge concerns the co-ordination of all the different agents involved in the delivery of e-voting services. In their technical option report, Fairweather and Rogerson [24], suggest a set of agents involved in the deployment of electronic elections, namely:

- Central Government
- Local Government
- Those seeking election
- Minority groups
- Citizens as voters
- Suppliers of technological elements
- Systems developers.

The traditional electoral administrators, the local election office, are supplemented by the at least one commercial vendor or a group of subcontracting vendors and a set of overseeing central authorities. We therefore have more processes, which are more complex, delivered through the combined efforts of more people who are not necessarily used to working together. The challenge is to establish procedural security to ensure the agents' roles and responsibilities are explicitly represented, understood and adhered to.

The concept of procedural security is related to all three of the above challenges since there is a human aspect to be managed in all three of them. The parallel delivery of traditional voting with e-voting in the first case, the combination of both traditional voting and e-voting in the second and the co-ordination of administrators in the third.

We therefore suggest that we must primarily allocate responsibilities of tasks among the different agents involved in delivering electronic voting. The Caltech-MIT [1] refers to the same objective as "*separation of duty*" (p.44), which exists in traditional voting and tends to be lost in the form of e-voting.

Responsibilities are typically allocated between e-voting administrators, whether commercial or government agents, at a high level, on the basis of a document defining the contractual obligations of partners in delivering e-voting. However, in the course of our research we have established that poor understanding of agent responsibilities is a contributing obstacle to the transparency of the electoral process. Given the growing dependency of government bodies on commercial vendors to deliver e-voting solutions, the two-person rule suggested by the CESC, which suggests that one administrator would be commercial staff and the second government staff, could alleviate

this problem and provide better internal process transparency.

The Caltech-MIT has long acknowledged the beneficial aspect of observers to the openness of the electoral process. This has recently been complemented by the Electoral Commission calling for a change in UK law to allow more observers in more stages of the electoral process [22]. However, this introduction of observers also needs to be defined by procedures safeguarding the integrity of the e-voting process. In the course of observation, we have concluded that under the concept of trust, an observer enters the norms of a "secure e-voting zone", and as such is presented with certain possibilities for malpractice. A malicious observer would therefore be in a position to commit fraud, therefore the same set of integrity rules applying to commercial and government staff should also apply to such observers.

8. Conclusions

The issue of security in electronic voting has two aspects: the technical security and the procedural security aspect. It can be argued that the technical aspect is of greater importance since electronic voting is a technical solution, however it does face certain barriers, which can only be overcome by further technological advances in the general field of e-transaction technologies and user authentication. Even though there are limitations with the technical security, we can enhance the present level of security by focusing on the procedural aspect of it.

In our research we have established:

- The lack of sufficient and detailed procedures to control specific activities of commercial vendors prior to the election and during the election;
- The lack of sufficient and detailed procedures to control specific activities of government officials prior to the election and during the election;
- Measures of procedural security that are in place but are inadequate to cover all aspects of the electoral process
- Measures of procedural security that are in place but there is a lack of agent compliance to them.

We have also identified three procedural security mechanisms:

- The design of procedural security measures to supplement the technology used for multiple

channel simultaneous voting, such as a national electronic version of the electoral register, so as to ensure one vote, and only one vote, per eligible voter.

- The design of procedural security measures to ensure adequate staff training and voter education on the interaction with the new technology, where this is more acute in hybrid electoral processes.
- The need to define more explicitly the roles and responsibilities of the multiple agents involved in the deployment of electronic voting.

Our research has established the need for procedural security measures while at the same time demonstrated that the existing procedural safeguards are insufficient. Procedural security is directly applicable to procedures where the human factor is involved. However, since we are in a phase of re-defining the electoral procedures, we must primarily re-define the procedural responsibilities of the agents involved. This analysis will in turn provide opportunities for process improvement. Transparent responsibility allocation among the agents involved in the electoral procedures will further establish the value of the procedural aspect of security, as it will indicate possible areas of application, further to those presented in this paper.

9. References

- [1]CalTech MIT (2001). Voting: What is, What Could Be, Report of the CalTech MIT Voting Technology Project.
- [2]Coleman, S. & Independent Commission on, Alternative Voting Methods (2002). Elections on the 21st Century: from paper ballot to e-voting. Electoral Reform Society.
- [3]Modernising Elections A Strategic Evaluation Of the 2002 Electoral Pilot Schemes.
- [4]Pilot scheme evaluation St Albans City and District Council, 2 May 2002.
- [5]Pilot scheme evaluation Swindon Borough Council, 2 May 2002.
- [6]Pilot scheme evaluation Liverpool City Council, 2 May 2002.
- [7]Pilot scheme evaluation Sheffield City Council, 2 May 2002.
- [8]Pilot scheme evaluation Westminster City Council, 2 May 2002.
- [9]Pilot scheme evaluation Rugby Borough Council, 2 May 2002.
- [10]Pilot scheme evaluation Broxbourne Borough Council, 2 May 2002.
- [11]Pilot scheme evaluation Epping Forrest District Council, 2 May 2002.
- [12]Pilot scheme evaluation South Tyneside Metropolitan Borough Council, 2 May 2002.
- [13]Pilot scheme evaluation Chorley Borough Council, 2 May 2002.
- [14]Pilot scheme evaluation Stratford on Avon District Council, 2 May 2002.
- [15]Pilot scheme evaluation Bolton Metropolitan Borough, 2 May 2002.
- [16]Pilot scheme evaluation Chester City Council, 2 May 2002.
- [17]Pilot scheme evaluation London Borough of Newham, 2 May 2002.
- [18]Pilot scheme evaluation Crewe and Nantwich Borough Council, 2 May 2002.
- [19]The Electoral Commission, Ballot paper design, Report and recommendations. June 2003
- [20]The Electoral Commission, The electoral registration process, Report and recommendations. June 2003
- [21]The Electoral Commission, Voting for change, An Electoral law modernisation programme, June 2003.
- [22]The Electoral Commission, Observers at elections in the UK. Report and recommendations, April 2003
- [23]The Electoral Commission Local electoral pilot schemes 2003, Briefing, April 2003.
- [24]Fairweather, B. & Rogerson, S. (2002.) Technical Options Report, De Montfort University, Leicester.
- [25]HMSO (2002). In the service of democracy, a consultation paper on a policy for electronic democracy.
- [26]IPI (2001). Report on the national Workshop on Internet Voting: Issues and research agenda. Internet Policy Institute.
- [27]NOP World (2002). Public Opinion In The Pilots 2002, A report summarising the aggregate findings from surveys carried out by NOP Research in May 2002 In 13 electoral pilots scheme areas.
- [28]OASIS (2002). Election and Voter Services Technical Committee, Election Mark-up Language (EML): e-Voting Process and Data Requirements.
- [29]ODPM (2002). Office of the Deputy Prime Minister, Government Response to the Electoral Commission Report: Modernising Elections – A Strategic Evaluation of the 2002 Electoral Pilot Schemes.
- [30]ODPM (2002b). Electoral Modernisation Pilots, Statement of requirements
- [31]OSCE (2001). Office for Democratic Institutions and Human Rights, Guidelines for reviewing a legal framework for elections, Warsaw.
- [33]Pratchett, L. (2002). The implementation of electronic voting in the UK. LGA Publications, the Local Government Association.
- [34]The Crown (2002). E-voting security study.
- [35]URL (www.votesheffield.com) consulted April 2003
- [36]URL (www.kerrier.gov.uk) consulted April 2003
- [37]URL (www.rushmoor.gov.uk) consulted April 2003
- [38]Watt, B. (2002). Implementing Electronic Voting, A report addressing the legal issues by the implementation of electronic voting, University of Essex.
- [39]Xenakis, A. & Macintosh, A. (2003). A Taxonomy of Legal Accountabilities in the UK e-voting pilots. In proceedings of DEXA, E-GOV 2003, Springer.