Procedural Security Analysis of Electronic Voting

Alexandros Xenakis
International Teledemocracy Center
Napier University
10, Colinton Rd., Edinburgh, EH10 5DT
a.xenakis@napier.ac.uk,

Prof. Ann Macintosh
International Teledemocracy Center
Napier University
10, Colinton Rd., Edinburgh, EH10 5DT
a.macintosh@napier.ac.uk

ABSTRACT

Security is among the most important constraints in the implementation of electronic voting because, to date, commercially available technology does not provide a completely secure e-transaction environment. In this paper, we explore the issue of security of e-voting procedures, given the established limitations of technology. We examine security in the context of the increased complexity of multiple-channel voting, provided by a multiplicity of agents involved in the administration of e-elections. As previously suggested, security in e-voting has two aspects, the technical and the procedural one. In the course of interviews and observations conducted during the 2003 UK local government legally binding e-voting pilots we have identified several procedural security gaps and related procedural security measures. After defining the norms of procedural security in e-voting, we adopt an existing framework of e-voting security objectives and use it as an analytical tool to indicate the importance of the procedural aspect of security. In concluding we extend the use of procedural security measures to the need for transparency in electronic voting and the development of trust and public confidence towards the newly introduced voting practices.

1. INTRODUCTION

Electronic voting has a very complex set of security requirements [1]. As such, it is one of the most valuable exploratory areas for the pursuance of a secure e-government transaction environment. In the UK, following the Government's aim to put *"robust systems in place for an e-enabled General Election after 2006"* [2] (p47), 16 e-voting pilots took place in May 2002 [3] and 20 more in May 2003 [4], on a Local Authority level. These were in all cases legally binding elections. The different e-voting technologies piloted involved electronic counting schemes (in some cases combined with traditional paper ballots) touch-screen voting kiosks, internet voting, interactive voice response (IVR) landline telephone voting and SMS text message voting in 2002. Digital television voting and smart card technology for partial voter identification were additionally introduced in 2003. Several local authorities (4 in 2002 and 13 in 2003) offered these technologies as alternative channels of voting, therefore providing a multiple channel e-voting process. In the pilots where two or more channels of voting were offered simultaneously an electronic on-line version of the electoral register was developed and used to provide the necessary voter identification infrastructure.

Presently, technological advances in any of the channels piloted, whether in the UK or elsewhere, have not been able to provide a completely secure e-voting solution. The most recent security analysis of inadequacies of current e-voting technology has been provided by Jefferson [5] based on the US Department of Defence e-voting project (SERVE), which was eventually cancelled. The technological limitations of current e-voting solutions had been previously suggested [1], [6], [7] on a more generic level. For the 2003 UK e-voting pilots, the Electoral Commission found the overall level of security to be of "*a good commercial standard"* adding that "*security can be improved and a significant improvement can be made in many cases in the area of documentation, procedural security and verifiability*" [8] (p114).

The purpose of this paper is to explore the procedural aspect of security in electronic voting and suggest the use of an existing framework of e-voting security objectives for the analysis of procedural security gaps and measures in the field of government provided e-services. Based on the UK documented e-voting experience, in the following sections of this paper we present the two main effects from re-designing the electoral process, define the concept of procedural security in the e-voting context, suggest our analysis approach and provide example cases of its application. Finally we explore the benefits deriving from the adoption of procedural security measures in the design of electronic voting systems.

2. RE-DESIGNING THE ELECTORAL PROCESS

The traditional government organized election, with its polling stations and paper ballots, has little to do with the e-voting process that has been provided in the UK pilots. The use of information and communication technologies in a number of stages of the electoral process has had an inherent effect on the main characteristics of the election event. New technology has provided more than just new gateways for votes to be cast. Effectively the electoral process has been through a "silent" re-engineering phase. Although the use of process re-engineering methods has been academically suggested, and a process stage approach accordingly presented [9],[10] no evidence has been identified to suggest that any kind of organized re-engineering attempt of the traditional electoral process has been undertaken prior to the deployment of the e-voting pilots. Irrespective of the technology used to pilot electronic voting in the different public authorities (PAs) involved, two main changes in the provision of the electoral process have occurred.

The traditional single channel, polling station and ballot paper voting has been substituted or complemented by a number of e-

ICEC'04, Sixth International Conference on Electronic Commerce
Edited by: Marijn Janssen, Henk G. Sol, and René W. Wagenaar
Copyright 2004 ACM 1-58113-930-6/04/10…$5.00

voting channels. The traditional voting process limits one voter to one specific polling station providing him/her with the opportunity to cast a ballot in the same way and time period as every other voter. For each new e-voting gateway offered to the voters, a new channel of voting is automatically created and respectively has to be managed and secured. Provided that traditional polling is still available then all these are additional channels. Given the five new e-voting technologies piloted (SMS, IVR, Internet, Kiosk, DTV) and the fact that postal voting was also an additional channel offered in many cases, the single channel voting was automatically elevated to a seven-channel process. Although there have been no cases where all technologies were piloted together, this remains a possibility for the future. Additionally, channels can be added by variations in the way that new e-voting technologies are introduced, e.g. kiosk voting was offered both in supervised (polling station) and unsupervised locations (public places such as supermarkets) [11], postal votes could be either mailed or hand delivered at collection points [12]. The use of the on-line electronic register at polling stations meant that voters were no longer committed to voting at a specific polling station but could cast a vote at any polling station of their convenience within the pilot wards [13], [14]. This e-enabled element alone multiplied the opportunities (channels) for voting by the number of the e-polling stations. It should also be noted that in most cases all channels were made available simultaneously rather than in different sequential time (voting) periods.

It is therefore evident that the introduction of the e-voting technologies affected more than just the way voters were authenticated and votes were cast and counted. Previously in traditional elections, security risks were limited by the fact that there was only one method of voting, during a relatively short period of time, at a supervised polling location. All or some of these elements of security were lost according to the different combinations of e-voting technology introduced. A voter could cast a ballot in more than one way (channel), and should in turn be excluded from using any other voting channels to comply with the "one voter, one vote" principle [15]. Voting and therefore voter authentication, was not necessarily supervised, nor related to a specific location. Finally the voting periods were extended to more than one day, in some cases up to a week [12], and could be the concurrent for some or all the different voting channels, making this multiple channel process even more difficult to secure.

The second main effect deriving from the re-design of traditional elections to a multiple channel voting process concerns the multiplicity of agents involved in its delivery. The traditional voting process is government provided; any e-element however is provided by commercial suppliers. The electoral process becomes a service, which is outsourced to external IT suppliers so as to be provided to voters. In cases where the multiple e-channel approach was adopted, a number of commercial suppliers had to form consortia in order to be able to provide all the channels that PAs were willing to pilot. To establish the extent of interoperability between e-voting systems the ODPM (Office of the Deputy Prime Minister) occasionally imposed more partners (external to the original consortia) as infrastructure providers. More external partners were occasionally hired to contribute to the promotion of the pilots. All these different agents, from the commercial suppliers' side had to be coordinated and co-operate with the different departments of the PAs. The traditionally involved departments, the election office and the office of the Returning Officer, was complemented by other departments according to the project management needs, such as IT, e-government, press, marketing and administration departments. In effect what used to be a government-owned process, provided by the internal co-operation of a small number of PA departments, became an external commercially provided service demanding the contribution of a number of suppliers, who had not necessarily worked in partnership previously. Moreover, new PA departments were involved, which had no previous involvement or experience of conducting elections. From a security point of view any new agent involved in the delivery of a secure service should be subject to some level of authentication controls according to their involvement in the process and following the requirement for accountability in the design of e-voting systems [1], [15].

The South Somerset 2003 pilot [12] provides a good example of the level of agent complexity that could be encountered. Here a five channel voting process, involving posted or hand-delivered postal ballots, internet, IVR and public kiosk, was provided by a total of eight commercial suppliers: four technology vendors, an infrastructure provider, an ISP provider and two voter engagement specialist partners. Along with commercial suppliers, six different departments of the public authority contributed to the deployment of the pilot.

The re-design of the traditional electoral process through the introduction of e-voting technologies to multiple-channel and multiple-agent provided e-enabled voting, in turn creates more and novel security risks for the new process. These risks need to be identified and managed using all possible controls which do not necessarily need to be of a technical nature but could rather derive from an organised procedural re-design of the voting process to an e-enabled voting process.

3. 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 information and communication technologies. After completing an extensive literature review of the issues involved in the implementation of electronic voting, we have identified the issue of procedural security as one that needs to be further explored. We have therefore theoretically defined the procedural aspect of security in e-voting so as not to confuse it with other aspects of e-voting security such as the technical and physical security measures involved.

To establish our approach, empirical research was undertaken which comprised interviews and observations, conducted both during the run-up to the election and on the actual polling day in one of the 2003 UK pilots. The Local Authority studied was piloting a simultaneous multiple channel e-voting process involving IVR, unsupervised kiosk, SMS and internet voting, combined with an e-register enabled polling station and postal ballots. The pilot was provided by three main technology suppliers, one sub-contracted technology supplier, one infrastructure provider, one ISP and two voter engagement specialist partners. Along with commercial suppliers, four different departments of the public authority contributed to the deployment of the pilot, i.e. twelve agents in total who had to be managed and work co-operatively.

In the course of observation our aim was threefold:

- To identify procedural security risks,
- To identify which measures were adopted (if any) to manage those risks
- To register procedural security risks for which no measure was taken against.

On the day prior to polling station voting, the observer was allowed to follow the PA's e-voting manager in action within the Local Authority premises, during which organisational issues were resolved. On Election Day, observation took place at the operations management centre, which was set up by three of the commercial partners involved to co-ordinate their efforts with those of the different PA departments. After 9pm that day, when voting was over, the observer witnessed the verification process and was provided with the opportunity to acquire hands on experience of the administration of the e-register system used.

The matter of procedural security was also one of the issues discussed in interviews with a number of the agents involved in the delivery of the pilot. Four semi-structured interviews were held with:

- The PA's Returning Officer who has the legal responsibility for the secure conduct of elections in his/her area;
- The PA's e-voting manager who had the managerial responsibility for the overall voting process and production of the final result;
- One of the commercial supplier's management executives who had the task of co-ordinating all technical systems providers for that pilot (six partners out of eight in total);
- One of the commercial suppliers' managers in charge of the deployment of a smart card element that was used for partial identification purposes.

One interview was held some days prior to the election while the other three were held on-site during the election. We have also analysed the detailed evaluation reports of the 2003 UK e-voting pilots provided by the Electoral Commission. These evaluation reports are based on observations, professional quality assurance reports prepared on behalf of the ODPM, and reports of other specialist consultants. This has allowed us to cross-reference and complement the existing body of findings in relation to procedural security risks and measures acquired through our interviews and observations.

4. DEFINING THE CONTEXT AND NORMS OF PROCEDURAL SECURITY

The general review of the 2002 UK pilots' evaluation reports provided limited examples of procedural security risks. Their number can be attributed to the fact that the 2002 pilots were much smaller in scale than the 2003 pilots. There were less cases of multiple-channel voting, less voting technologies introduced and no more than two main commercial suppliers involved in the same pilot, with the majority being provided by one commercial supplier. Nevertheless these initial cases of procedural security have been documented [16] and grouped in the following generic areas:

- The lack of procedures to control the activities of commercial vendors and government officials before and during the election, providing an audit trail of their actions
- Existing measures of procedural security, which are were inadequate to cover all aspects of the electoral process such as the verification of voter provided data, the secure dissemination of voter credentials and the prevention of double voting through multiple voting channels.
- A lack of agent compliance to existing measures of procedural security.

Based on these initial findings Xenakis and Macintosh [16], (p4) consider procedural security in the context of e-voting: "*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"*.

In order to identify the specific areas of application of procedural security, one must primarily establish the overall range of security measures involved. Mercuri and Neumann [17] suggest a generic set of design criteria for verifiable e-voting systems, many of which are relevant to the concept of procedural security as defined above. Gritzalis [1] attributes certain constitutional requirements to specific user requirements but further complements those with a set of non-functional security requirements many of which are closely related to procedural security measures. However, the 2003 UK e-voting pilots were committed to comply with the ODPM statement of requirements for e-voting suppliers [18].This first document specifically defines that risk analysis for all e-voting systems should be undertaken in relation to four generic risk management areas:

1. Physical measures
2. Procedural measures
3. Personnel security measures
4. Technical security measures

Based on the above provided definition we must differentiate procedural security in the e-voting context from traditionally understood physical security measures provided that these measures are not related to the re-design of the electoral process itself. Furthermore we must distinguish procedural security measures from all kinds of technical security measures, whether related to the re-design of the electoral process or not. Finally, while procedural measures are directly applicable, we also consider personnel security measures to be included in the procedural aspect of e-voting security as any re-design of procedural activity involves the re-distribution of roles among the different agents involved in its delivery security.

However security requirements for the 2003 UK e-voting pilots were detailed in a second document [19] which set fifteen distinct security control objectives for the design of e-voting systems which we present in the following section.

5. A FRAMEWORK FOR THE ANALYSIS OF PROCEDURAL SECURITY

According to the ODPM [19] any e-voting system used in the UK must satisfy the following 15 security control objectives (OS). In order to demonstrate the relevance, the importance and the level of applicability of the procedural aspect of security we have used this set of security objectives as a framework for the analysis of our empirical data. We relate the procedural security gaps and the procedural measures identified in the course of our interviews and observations to the security objectives that each gap threatens and accordingly each measure serves. The 15 security objectives are provided hereafter verbatim, in order to introduce a common ground for their understanding, as included in [20] (p7):

1. Effective voter registration (OS1): Voting permission is only granted to those whose *bona fides* have been established.
2. Effective voter authenticity (OS2): E-voting services are only available to those eligible to vote.
3. Effective voter anonymity (OS3): Either during the voting process or at the ballot count the real world identity of the voter cannot be established. With the exception of the ability to warrant under law votes cast.
4. Effective vote confidentiality (OS4): E-voting services must guarantee the confidentiality of the vote until it is counted.
5. Effective system identification and authentication (OS5): Accountable e-voting service processes are only accessible to those individuals and systems that have been authorised to access such processes.
6. Effective system registration (OS6): Access permission to e-voting service processes is only granted to those who *bona fides* have been established.
7. Effective system access control (OS7): Access granted to e-voting service application and assets is the minimum necessary for the identified user to obtain services required.
8. Information integrity (OS8): Ensuring that the voter's intention is received and counted as intended.
9. Service availability (OS9): Continuing access to the e-voting service as and when required must be assured.
10. Information availability (OS10): Continued access to e-voting data assets as and when required must be assured.
11. Service protection (OS11): The e-voting service implementation and associated assets must be protected from external interference and penetration.
12. Operator integrity (OS12): Those operating and administering the e-voting service should be of an unquestionable record of behaviour.
13. Open auditing and accounting (OS13): The e-voting service must keep a proper record of significant transactions. The integrity of audit information must be assured.
14. Third party system authentication (OS14): Third party systems, used by any e-voting service, must demonstrate to the voter they are authorised e-voting agents.
15. Public verifiability (OS15): The e-voting service must be publicly verifiable.

In the following sections we provide examples of our analytical approach in relation to two significant stages of the e-voting process for the integrity of its outcome: voter authentication and voter verification. We indicate the security gaps (WHAT) which can be managed through the use of procedural measures, the measures themselves (HOW) and relate them to the above security objectives (WHY). Presenting this analysis per process stage also indicates WHERE and WHEN these security risks can be met and therefore supports the proactive deployment of procedural measures.

6. VOTER AUTHENTICATION

Procedural measures involving a double mailing approach were set up for disseminating voter credentials. That meant that smart cards containing a voter's ID reached voters by a separate mailing than the polling card, which contained their password. Both voter ID and password were needed during the authentication stage of the e-voting process. These credentials could only be used once and for the purpose of this election only. While the authentication stage serves OS5 in general, the double mailing approach of voting credentials minimizes the possibility of voting credentials being sent to non-eligible (OS2) voters. However the fact that there were many postal transactions increased the possibility of human errors during this process.

For a number of diverse reasons some voters lost either their voter ID or password. There were straightforward procedures in place to cancel the existing voter ID and issue a new one, with a new password. The cancellation of lost credentials and the production of replacement credentials also serve OS2. The procedure could be done at any time from the Election Office but could be undertaken only by someone who had administration rights to the e-register database. This measure is in line with OS5 - the system being administered by an authenticated administrator as well as OS7 – the administrator having access to the e-register database only. During the first day of observation only one person was in charge of executing this specific process. Given that the agent in question was the head of the Election Office we can safely suggest that this was a trusted individual and as such the operator integrity objective OS12 was also satisfied.

Both parts of the replacement voter credentials (voter ID and password) were printed on the same sheet of paper using a standard network printer located in the election office. With regard to procedural security, the new credentials were easily readable as there was no foil over the password, as there would be on a polling card, making them more vulnerable to misuse. This is a case of a security gap in the credential replacement process. Voting credentials should only be known to their prospective user-(voter) in order to satisfy security objectives OS2 and OS5. In order to manage this security gap, the administrator put the voter credentials in an envelope, writing the name of the voter on the envelope. For the dissemination of replacement credentials two measures were adopted. If the credential replacement process took place in the morning then the new credentials would be delivered by PA staff to the voter's home. This first measure served OS1 as in the UK the voter registration process is based on the voters' home postal address. If it was in the afternoon, voters had to come to the election office and provide some form of acceptable identification before being given their new credentials. Legally, this identification was not required but was asked of voters as an extra layer of security thus satisfying OS6. The UK electoral legal framework [21] does not require any identification token from a voter when one asks for a ballot paper at a polling station, other than the oral declaration of one's name and postal address, which are checked against the electoral register so that a second ballot is not given to the same person.

7. VOTER VERIFICATION

In some cases, voters were given a ballot paper at e-polling stations without the polling staff being able to undertake prior checking against the e-register due to technical problems in the deployment of the networked computer system. In these cases the ballot was given in good faith that the voters had not already cast a ballot using one of the other voting channels or at any other polling station. In effect the voter authentication stage was omitted thus creating a security gap relevant to OS2, OS5 and OS6 as already indicated in the previous section.

In the polling stations concerned, in order to maintain service availability (OS9) the election staff either kept a paper note of the voter's name, surname and street address or retained the voter's polling card. This information would enable polling station staff to perform the voter authentication procedure once the network system was restored. From a procedural point of view, retaining the polling card provided a more valid process than keeping notes on a voter's details, as the voter would submit a paper token (polling card) and "exchange" it for a ballot paper. This last measure is in line with OS 5, while both measures satisfy OS13 since they provided an audit trail of administrators' actions.

This whole issue necessitated a new procedural security measure. After the close of polls the verification procedure was undertaken. The objective was to check and mark the register as should have been done during the authentication process prior to granting a ballot. The general rule implemented in the multiple channel voting was that if double voting had happened then the e-ballot would be ignored and the physical (paper) ballot counted. This rule covers the case where someone had voted twice, once in a polling station and once in any of the e-channels, but the case of a voter casting a ballot in two or more polling stations was not covered. The verification process was in line with OS1 as this measure was related to the use of the electoral register. The voter verification process began at 9pm once all voting channels were closed. Eight PCs in the election office were used and a team of people formed to input the data. The platform used was the same as the one installed in all laptops allowing polling officials to check and mark the register from the e-polling stations. The voter information gathered, either as paper-based notes or retained polling cards was used to update the e-register. If the voter was shown as not having voted then he/she would be marked and there was no problem. If the voter was shown as having already voted there were available audit trails providing information as to the channel this voter had used, thus satisfying OS13.

However, verification means keeping account of numbers. So all the paper notes and polling cards should numbered per voter, then the register checked for the number of existing marked voters per channel. When the entry of the notes was over then the new number of marked voters should equal the prior existing number of marked voters plus the entered notes, which should also equal the total number of ballots cast. Unfortunately this procedural measure, which would correspond to OS15 (public verifiability) was not observed.

8. BENEFITS AND FUTURE WORK

The procedural security gaps and measures identified in the previously described e-voting process stages were related to 9 out of the original 15 security control objectives included in the framework we used as an analytical basis. It is therefore obvious that the procedural aspect of security is applicable to many of the security requirements of the e-voting process and can increase the level of security provided by technical means to a considerable extent.

Additionally, procedural security has the potential to serve as a trust building measure in the new e-voting processes. In the interview held with the Returning Officer of the Local Authority where observations took place, he suggested that:

"*People are comfortable with the current system because they have grown up with it. It is not as secure as people think it is but it doesn't matter because it's what they are used to so I think we need to convince people and it's a question of how we do that*"

The election office, where observations took place, provided many opportunities for fraud. For example, those having access to the location could have removed returned smart cards, and in the verification process one could check the names of voters who had not voted at all and therefore even up the number of votes cast with the number of marked voters in the register in an effort to conceal double voting. Yet none of this happened because all the agents present were trusted (OS12). The Caltech-MIT project [22] has long supported the production of a paper proof of the voters' choice as a trust building measure which would allow verification of the vote cast. They have also supported that the most critical moment of voting, is when the voter loses control of ones vote. The explicit deployment of procedural security measures which are open to public scrutiny may start to address this issue. The relationship between increased trust in e-government initiatives and transparency of the processes adopted has been recently suggested [23], [24]. The advantage that procedural security measures present, is that they are understandable by all agents (technical and non-technical). In relation to technical measures they are more visible and therefore increase the overall level of transparency of the process. The greater value of procedural security in e-voting, may therefore prove to be the element of trust building that it fosters rather than the increase in the actual levels of overall security.

Our aim is to develop a comprehensive body of knowledge including a register of encountered procedural risks and measures that have been adopted for their management, relating these findings to the different e-voting process stages and the different e-voting channels or combinations of voting channels. Such a framework could allow proactive use of procedural security measures and better overall security management of electronic voting.

9. REFERENCES

[1] Gritzalis, D., (2002), *Principles and requirements for a secure e-voting system* in Computers & Security, Vol. 21, No 6, pp 539-556, Elsevier Science.

[2] HM Government. (2002) In the Service of Democracy - a consultation paper on a policy for electronic democracy. Published by the Office of the e-Envoy, Cabinet Office, London.

[3] Pratchett, L. (2002) "The implementation of electronic voting in the UK" LGA Publications, the Local Government Association

[4] Electoral Commission. (2003a) Local electoral pilot schemes 2003, Briefing, April 2003

[5] Jefferson, D., Rubin, A., Simons, B., Wagner, D., (2004) A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE), January 2004, Available at www.servesecurityreport.org

[6] Lambrinoudakis, C., Critzalis, D., Tsoumas, V., Karyda, M., Ikonomopoulos, S., (2003). Secure electronic voting: The current landscape, in Secure Electronic Voting, Gritzalis, D., Ed., Kluwer Academic Publishers

[7] Cranor, L.F. (2003), In search of a perfect voting technology: no easy answers, in Secure Electronic Voting, Gritzalis, D., Ed., Kluwer Academic Publishers

[8] Electoral Commission. (2003b). The shape of elections to come: A strategic evaluation of the 2003 electoral pilot schemes, July 2003, Available at www.electoralcommission.gov.uk

[9] Xenakis,A. and Macintosh, A. (2003a); 'Using Business Process Re-engineering (BPR) methods and analysis tools to effectively implement electronic voting'; 3rd European Conference on E-Government ECEG 2003; Dublin, Ireland, July 2003

[10] Xenakis, A. and Macintosh, A. (2003b), 'A Taxonomy of Legal Accountabilities in the UK E-voting Pilots'; DEXA 2003, the 2nd International Conference on Electronic Government - EGOV 2003; Prague, Czech Republic, September, 2003

[11] Electoral Commission. (2003c) Pilot scheme evaluation Basingstoke & Deane Borough Council 1 May 2003

[12] Electoral Commission. (2003d) Pilot scheme evaluation South Somerset District Council 1 May 2003

[13] Electoral Commission. (2003e) Pilot scheme evaluation Sheffield City Council 1 May 2003

[14] Electoral Commission. (2003f) Pilot scheme evaluation St Albans City and District Council 1 May 2003

[15] Mitrou, L., Critzalis, D., Katsikas, S., Quirchmayr, G., (2003) Electronic Voting: Constitutional and Legal requirements, and their technical implications, in Secure Electronic Voting, Gritzalis, D., Ed., Kluwer Academic Publishers

[16] Xenakis, A. and Macintosh, A. (2004); 'Procedural Security in Electronic Voting'; In the Proceedings of the Thirty-Seventh Annual Hawaii International Conference on System Sciences (HICSS-37); Big Island, Hawaii, January 5th-8th, 2004

[17] Mercuri, R., Neumann, P., (2003) Verification of electronic balloting systems, in Secure Electronic Voting, Gritzalis, D., Ed., Kluwer Academic Publishers

[18] ODPM (2002a). Electoral Modernization Pilots, Statement of requirements

[19] ODPM (2002b). E-voting Technical Security Requirements

[20] Electoral Commission (2003g). Technical report on the May 2003 pilots, 26 November 2003.

[21] Watt, B. (2002) Implementing Electronic Voting, A report addressing the legal issues by the implementation of electronic voting, University of Essex

[22] CalTech MIT (2001). Voting: What is, What Could Be, Report of the CalTech MIT Voting Technology Project.

[23] Northrup, T., and Thorson, S. (2003). “The Web of Governance and Democratic Accountability.” Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICCS 2003) Ed. Ralph H. Sprague, Jr.

[24] Welch, E. and Hinnant., C., (2003). “Internet Use, Transparency and Interactivity Effects on Trust in Government.” Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICCS 2003) Ed. Ralph H., Sprague, Jr.