An Exploratory Study of Voter attitudes towards a Pollsterless Remote Voting System

Tim Storer[*], Linda Little[†] and Ishbel Duncan[*]

June 14, 2006

Abstract

This paper describes an exploratory study of a prototype implementation of a pollsterless remote voting scheme, mCESG. The aim of the study was to investigate voter attitudes towards the system in general, with particular interest in the pollsterless vote verifiability provided. Although the focus of the study was one particular prototype system, the results provide some guidance to the design and implementation of future voting systems, particularly with regard to voter interest in vote verification.

1 Introduction and Motivation

A substantial amount of work has been undertaken into user-perceptions of remote electronic voting (REV) systems. A study for the UK Office of the e-Envoy investigated user perceptions towards electronic voting systems in general, noting that introducing new technologies into democratic structures met with only modest enthusiasm, the use of electronic voting was seen as more relevant than electronic participation systems [3]. In addition the study found anecdotal evidence to suggest that voters were more interested in e-voting once the various channels had been discussed. Other studies have investigated voting systems using 'think aloud' techniques to identify problems with usability and to understand what the voter thinks a voting machine is doing [1, 15].

Oostveen investigated voter's understanding of the security properties of voting systems [9]. The study noted that voters are willing to accept statements from voting client *pollsters* that their vote has been successfully collected without requiring demonstrable evidence to support the statement [9, 10]. The term pollster refers to the need for the voter to employ a complex artifact to undertake a cryptographic voting protocol on their behalf. Rivest has noted that for conventional cryptographic voting schemes, the pollster *is* the voter, from a protocol perspective [8]. The voter is required to present their choices to the pollster and trust that it will then behave correctly with respect to them. Conversely, Hubbers and Pieters have noted anecdotal evidence to suggest that voters appreciate simple verification mechanisms, but that confidence in a voting system is reduced if the verification activity incorrectly leads the voter to conclude that the voting system is trying to cheat [5, 11].

Malkhi has proposed the development of *pollsterless* voting schemes [7], in which the voter directly performs the voting protocol without requiring support from a pollster capable of performing cryptographic operations. Electronic devices are still used, but only to perform communication activities. Pollsterless schemes have several advantages, including:

- If the pollsterless scheme is *voter verifiable*, then the voter does not need to trust the software artifacts correct operation in order to verify that their has been correctly counted.
- Voting can be conducted on much simpler devices which lack computational power normally required for cryptographic voting schemes.

[*] School of Computer Science, University of St Andrews

[†] PACT Laboratory, University of Northumbria

The mCESG scheme is derived from a pollsterless remote voting scheme proposed by CESG in a Security Study for the Office of the e-Envoy [2]. Although the original CESG scheme incorporated several desirable features (including convenience and mobility) several flaws were also noted, in particular a lack of voter verifiability. The mCESG scheme corrected this flaw, providing voters with the ability to confirm that their vote had been successfully counted [12]. Several adaptations to the mCESG scheme have also been presented [14], introducing variations that accommodate ordinal vote casting and receipt freeness. However, the study presented here is concerned with the basic mCESG scheme, particularly from the voter's perspective.

The exploratory study of the mCESG scheme presented here provides an investigation of voter's reactions to and acceptance of a pollsterless remote voting scheme which permit highly mobile voting (voting can take place on any connected device and in any public location) and also permits voters to confirm that their vote has correctly contributed to a tally of votes. Whilst the desirability of receipt-free verifiability has been asserted as a desirable property for cryptographic voting schemes, that desirability has not been tested, and it is noteworthy that the existing UK remote voting system, postal voting, permits a voter to construct a receipt for their vote (by photocopying the paper ballot, or transferring the paper ballot to an attacker) and the system is used satisfactorily and regularly for UK public elections. The study presented here investigated whether the voter is able to understand why the information presented to them constitutes evidence that their vote has been counted and also whether the provision of evidence is considered valuable by voters.

The remainder of this paper is organised as follows. Section 2 describes the features of the mCESG scheme relevant to the study. Section 3 describes the design of the user acceptance study, which employs focus groups directed by video taped activity scenarios. Section 4 describes the results of the study, whilst Section 5 reviews the work described and identifies future work to be undertaken in this area.

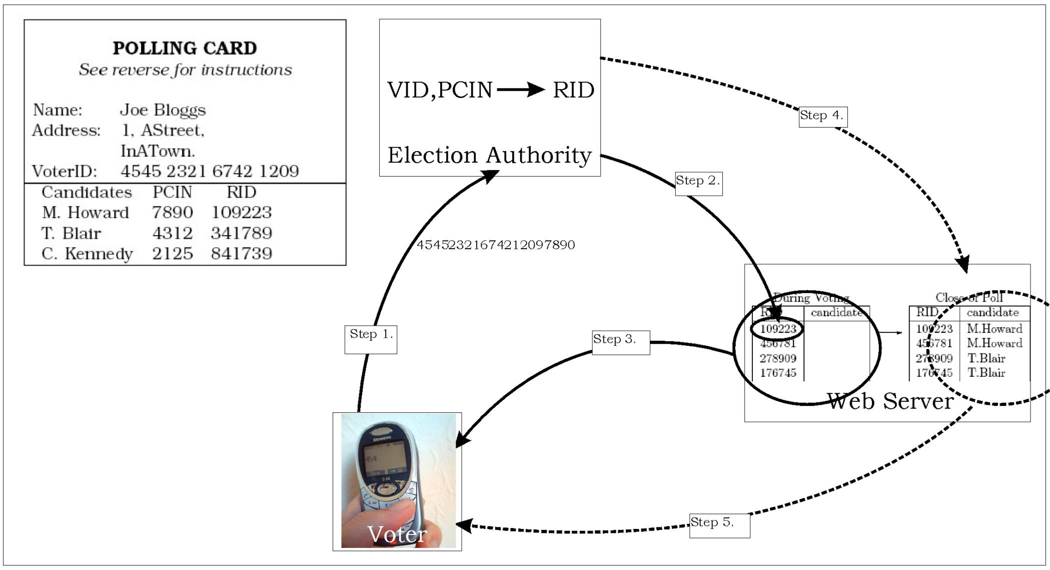
2 The mCESG Scheme

The scheme is illustrated in Figure 1. Voters are provided with a set of voting credentials consisting of a Voter Identification number (*vid*) and a set of Personal Candidate Identification Number (*pcin*) and *Receipt* Identification numbers (*rid*), one each for each candidate. To cast a vote, a voter prepares a message consisting of their own *vid* number and the *pcin* number of their chosen candidate. This message is then sent via an available channel (such as an SMS message) to the Election System for processing.

Given a valid *vid:pcin* combination, an *rid* value is published on a publicly accessible bulletin board. The voter may then determine that the correct *rid* has been published for the vote they have cast. The Election System sends a message to the voter indicating that their vote has been successfully processed, although the voter should consider this message to be informative only and not proof of receipt.

If the Election System publishes the wrong *rid* value for the voter's choice, the voter must contact the Election System via some other channel in order to have the incorrect *rid* value removed and cast a second vote. The voter may take this action at any point until the end of voting. Conversely, the Election System may publish no *rid* value at all for a cast vote. In the circumstances where no relevant *rid* value is published after some latency period, the voter should re-attempt to cast their vote. If repeated attempts at vote casting do not result in a (correct or otherwise) *rid* value being published, the voter should assume that their vote is not reaching the Election System and should revert to the strategy described for a wrong *rid* value being published. Note that since voting is assumed to occur over insecure channels (as per the pollsterless property) the scheme's design deliberately accepts the potential for votes to be intercepted, say in a Denial of Service attack, but not to be interpreted or modified by an eaves-dropping attacker.

Assuming the correct *rid* value is published, the Election System is now committed to the *rid* choice of the voter publicly in a manner which the Election System cannot later de-commit from. However, at this stage, the Election System is not committed to processing the voter's



POLLING CARD

See reverse for instructions

Name: Joe Bloggs
Address: 1, AStreet,
InATown.
VoterID: 4545 2321 6742 1209

Candidates	PCIN	RID
M. Howard	7890	109223
T. Blair	4312	341789
C. Kennedy	2125	841739

During Voting

RID	candidate
109223	
456781	
278909	
176745	

Close of Poll

RID	candidate
109223	M.Howard
456781	M.Howard
278909	T.Blair
176745	T.Blair

Figure 1: The vote casting and checking process of the mCESG remote electronic voting scheme. Voters are provided with a set of voting credentials consisting of a Voter Identification (*vid*) number and a set of Personal Candidate Identification Number (*pcin*) and Receipt Identification numbers (*rid*), one each for each candidate. To cast a vote, a voter prepares a message consisting of their own *vid* number and the *pcin* number of their chosen candidate. This message is then sent via an available channel (for example, an SMS message) to an Election Authority for processing (Step 1). Given a valid *vid*:*pcin* combination, an *rid* value is published on a publicly accessible bulletin board (Step 2). The voter may then determine that the correct *rid* has been published for the vote they have cast (Step 3). Once the close of poll has been reached, the Election Authority (through collaboration between the Vendor and Acting Registration Officer domains) publishes the association between *rid* and candidates for each vote (Step 4). At this stage, a voter can confirm that their vote has been handled properly (i.e. that the correct candidate is associated with their *rid*) but not that the *rid* itself is correct (Step 5).

choice accurately. To effect this second commitment, once the close of poll has been reached, the Election System publishes the association between *rid* and candidates for each vote. This does not reveal the association between votes and voters, since the voting credentials are assumed to be a secret possessed only by the voter. At this stage, a voter can confirm that their vote has been processed accurately (i.e. that the correct candidate is associated with their *rid*) but not that the *rid* itself is correct, since this would violate the undeniability property.

The mCESG scheme thus achieves voter verifiability by publicly committing the Election System to a voter's choice that the voter can confirm with respect to their voting credentials. The credentials thus constitute a *receipt* with which a voter may request the Election System change the candidate name associated with a *rid* value on the bulletin board. The scheme preserves the secrecy of vote to voter association under the assumption that a voter does not reveal their credentials to a third party. Further details of the scheme and the architecture for the supporting voting system can be found in [12, 13].

3 Study Design

The study was undertaken within a broader investigation by the PACT Laboratory of psychological aspects of online privacy and trust[1]. The study employed videotaped scenarios in order to direct focus group discussion to elicit responses from which results are extracted. A later stage of planned work will be to construct questionnaires for completion by a larger group of participant. The questionnaire will be designed with respect to the results obtained from the study described

[1] The study is funded by the ESRC

here and with reference to the Technology Acceptance Model [4].

Initially, a videotaped scenario which captured the vote casting and checking activities described in the previous section was developed as a storyboard consisting of three scenes. A registration phase, unrelated to the prototype mCESG system itself, is included to provide the focus groups with a complete scenario. The registration phase illustrates the voter filling her personal details (name, address etc) into a web form. The second, vote casting scene, covers the voter receiving and compiling voting credentials as described in the previous section and the casting of a vote using SMS messaging on a mobile phone as the communication channel in a public location. The voter also uses a computer located in an office to complete the first vote checking phase during this scene. The final scene of the scenario illustrates the online vote tallying and checking procedure. Appendix A illustrates the storyboard that was developed for the mCESG scenario.

Once the storyboard had been finalised, a script for the scenario was generated, describing the voter's behaviour and actions during the three scenes. The script was then passed to a media production company, which reduced the volume in order to complete the three scenes within a shorter period of time. The revised, summarised script was then approved before being filmed by the production company employing professional actors.

The procedure for initiation and conduct of the focus groups is as follows. 304 participants from the Newcastle upon Tyne region were divided into 38 focus groups (ranging in size from 4 to 12 people). Participants were categorised in terms of:

- Age
- Gender
- Disability
- Level of educational achievement
- Technical stance (technically knowledgeable and also attitude towards technology use).

Participants were allocated to focus groups as a result of this categorisation in order to encourage discussion. Prior to attending the focus group, participants were provided with information as to the project's objectives.

Each focus group session lasted ninety minutes and covered four different scenarios - e-voting, shopping, health and finance[2]. The scenarios were shown to the focus group first, followed by a discussion on each of the topics, directed by a moderator who was a member of the PACT laboratory. Each focus group was tape recorded and the ensuing conversations later transcribed. The transcripts then underwent qualitative analysis and open coded, identifying several categories of opinion. The procedure is identical to that for other topics covered by the wider PACT-AMI project, described by Little [6].

4 Results

Table 1 summarises focus group responses to the videotaped scenario which they viewed. The focus groups were aggregated into three classifications by the PACT psychologists - non-technical experience, technical experience and a separate disabled group. The non-technical and technical groups were further sub-divided according to level of education (low and high) reached. The categories listed for responses are grouped in terms of social trust/security and privacy issues.

4.1 Social Issues

Exclusion Refers to the potential for some societal groups to be unable to use the voting system.

Social Interaction The desirability of communal properties of polling station voting systems.

[2] Details of the three other scenarios, which are outwith the scope of this paper, can be found in [6]

Topic	Technical		Non-Technical		Disabled Participants
	Low	High	Low	High	
Social Issues					
Exclusion	-	-	-	-	-
Social Interaction	-	-	-	-	-
Social/Moral Values		-	-	-	
Convenience	+	+	+	+	
Encourage young voters	+		+	+	
Mobility	+	+	+	+	+
Motivation		-	-	-	
Trust					
Security	-	-	-	-	-
Verification	-	-/+	+	-/+	
Privacy Concerns					
Informational	-	-	-	-	-
Physical	-	-	-	-	-
Tracking/Anonymity	-	-	-	-	-

Table 1: Results of the mCESG user acceptance study. The table categories positive and negative reactions to videotaped scenario of the mCESG scheme from focus groups. Focus groups are categorised according to technical experience and level of educational achievement, as well as including separate information on a group of disabled participants. Reactions are grouped by social, trust and privacy issues. A '+' indicates the focus group gave a positive response on a category. A '-' indicates that the group gave a negative response on a category. '+/-' indicates that both positive and negative issues were discussed by the group. No symbol indicates that a topic was not raised by a group.

Social/Moral consequences. Whether the mCESG system would trivialise voting or reduce sense of responsibility for the democratic process.

Convenience Whether the scheme permits voters 'with busy lives' to participate in voting.

Encourage young voters Whether the participants thought the viewed system would improve participation amongst younger voters.

Mobility The advantage of not having to attend a polling station to vote, which is related to convenience.

Motivation Whether the voting system viewed by participants would reduce the likelihood of participation, which is related to the question of social/moral consequences.

4.2 Trust

Security That the system does not appear secure, and therefore reduces trust.

Verification Whether the ability to verify a vote as having been counted was appreciated and trusted.

4.3 Privacy Concerns

Informational Refers to whether participants were comfortable with personal information and voting intention being processed electronically.

Physical Whether voting in public locations was a concern in terms of privacy, which is related to the desirability of mobility and convenience.

Tracking/Anonymity Refers to concerns as to whether a voter's choices could be tracked via an electronic voting system.

The results illustrate a mixture of reactions to the scenario, from positive, to mixed and negative, with some groups not raising some of the issues at all. As discussed in the design of the study, the conversation between participants was not heavily constrained by the discussion moderator. As such, the recurrence of themes across groups is in itself, interesting, since this suggests the system raises similar issues from all participants. The videotaped scenario elicited positive responses primarily for the usability aspects of the voting scheme, notably the mobility and convenience, although all focus groups noted concern about whether some groups would be excluded from voting by the system. This perhaps reflects the fact that the scenario did not suggest that multiple voting channels were envisaged, of which mobile phone voting was just one. Participants also raised concerns about the 'behind the scenes' processing of personal information and the security of the infrastructure. The occurrence of these topics is interesting, since the scenario did not discuss directly how voter information was handled to ensure privacy and security, but instead focused on usability and verifiability aspects. The concerns raised by the participants suggest that the implementation of voting schemes will need to be accompanied by explanation as to the reasons voters should accept voting as secure.

In addition to the responses categorised as positive and negative, several other topics were raised with respect to the voting system which can be considered to be assertions as to the desirable properties for a voting system, rather than a specific comment on the system proposed

Transparency The inner workings of the voting system should be demonstrable, it shouldn't be possible to mask inner workings. This was a desire raised by the high-education/ technical focus group.

(De-)Centralisation The control of the voting system should be de-centralised to prevent abuse. The raising of this issue suggests an intuitive public understanding of dependability issues and the importance of distributing trust.

Control and choice An issue raised by several focus groups was the importance of users *retaining control of the right to choose who to vote for.* The discussion of this issue amongst focus groups is interesting from the perspective of pollster/pollsterless voting schemes. Verifiable voting schemes permit a voter to determine (if the voter understands the verification mechanism) directly that their choice has been reflected by a voting system. Conversely, cryptographic voting schemes require the voter to give their choice to a pollster which votes on their behalf, and thus the voter does not directly retain control of their choice. The discussion of this issue in the context of a pollsterless voting scheme, therefore suggests potential for future research on the topic of vote verifiability and voter trust.

5 Conclusions

The work presented here investigated the extent to which users accepted and understood the mechanisms of a pollsterless voter verifiable remote voting scheme. In particular, the study provides some guidance as to the likely demands from voters for a successful remote voting system in the UK context.

References

[1] Benjamin B. Bederson, Bongshin Lee, Robert M. Sherman, Paul S. Herrnson, and Richard G. Niemi. Electronic voting system usability issues. In Gilbert Cockton and Panu Korhonen, editors, *Proceedings of the 2003 Conference on Human Factors in Computing Systems, CHI 2003*, volume 5 of *chi letters*, pages 145–152, Ft. Lauderdale, Florida, USA, April 2003. ACM.

[2] e-voting security study. Communications and Electronic Security Group (CESG), July 2002.

[3] e-democracy report of research findings. COI Communications/Office of the e-Envoy, December 2002.

[4] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8):982–1003, August 1989.

[5] Englebert Hubbers, Bart Jacobs, and Wolter Pieters. RIES: Internet voting in action. In Randal Bilof, editor, *Proceedings of the 29th Annual International Computer Software and Applications Conference, COMPSAC'05*, pages 417–424, Edinburgh, Scotland, July 2005. IEEE Computer Society.

[6] Linda Little, Stephen Marsh, and Pam Briggs. Trust and privacy permissions for an ambient world. To Appear Trust in E-Services: Technologies, Practices and Challenges, January 2006.

[7] Dahlia Malkhi, Ofer Margo, and Elan Pavlov. E-voting without 'cryptography'. In Matt Blaze, editor, *Financial Cryptography, 6th International Conference, FC 2002, Revised Papers*, volume 2357 of *Lecture Notes in Computer Science*, pages 1–15, Southampton, Bermuda, 2003. International Financial Cryptography Association, Springer.

[8] Margaret McGaley. Report on DIMACS workshop on electronic voting theory and practice, May 26 - 27, 2004, December 2004.

[9] Anne-Marie Oostveen and Peter van den Besselaar. Ask no questions and be told no lies security of computer based voting systems; user's trust and perceptions. In Urs E. Gattiker, editor, *EICAR 2004 Annual Conference CD-ROM*, Grand-Duché de Luxembourg, May 2004. European Institute for Computer Anti-Virus Research.

[10] Anne-Marie Oostveen and Peter van den Besselaar. Security as belief user's perceptions on the security of e-voting systems. In 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*, volume 47 of *Lecture Notes in Informatics*, pages 73–82, Schloß Hofen / Bregenz, Lake of Constance, Austria, July 2004. Gesellschaft fr Informatik.

[11] Wolter Pieters. What proof do we prefer? Variants of verifiability in voting. In Peter Ryan, Stuart Anderson, Tim Storer, Jeremy Bryans, and Ishbel Duncan, editors, *Workshop on e-Voting and e-Government in the UK*, pages 33–39, Edinburgh, UK, February 2006. National e-Science Centre, University of St Andrews.

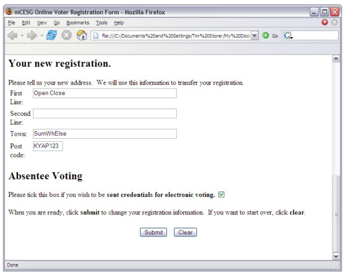
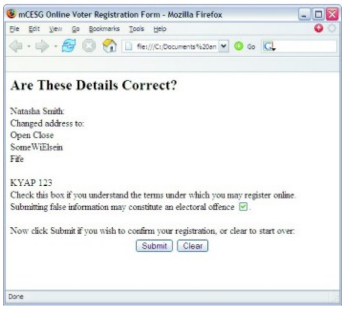
[12] Tim Storer and Ishbel Duncan. Polsterless remote electronic voting. *Journal of E–Government*, 1(1):75–103, October 2004.

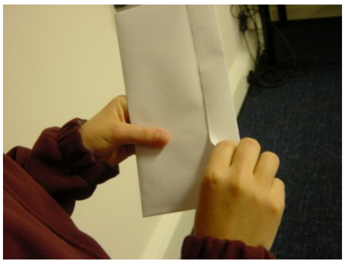
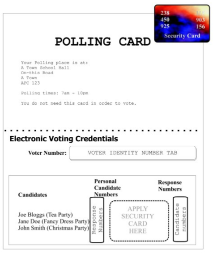
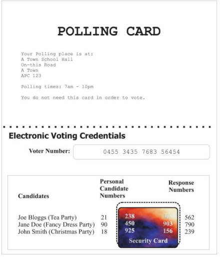
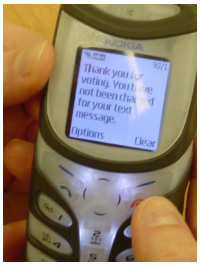
[13] Tim Storer and Ishbel Duncan. Practical remote electronic elections for the UK. In Stephen Marsh, editor, *Privacy, Security and Trust 2004 Proceedings of the Second Annual Conference on Privacy, Security and Trust*, pages 41–45, Fredericton, New Brunswick, Canada, October 2004. National Research Council Canada, University of New Brunswick.

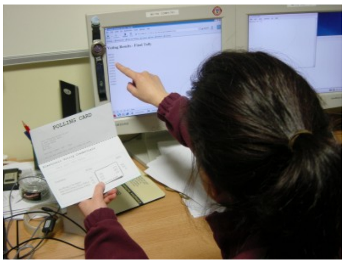
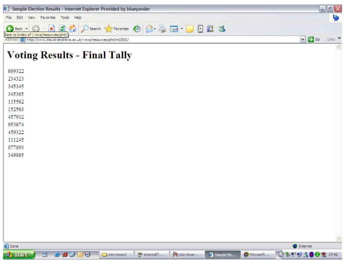
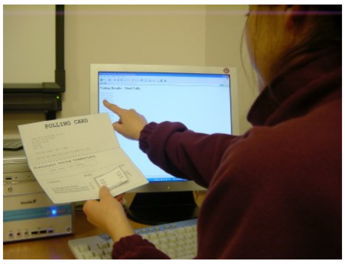
[14] Tim Storer and Ishbel Duncan. Two variations of the mCESG pollsterless e-voting scheme. In Randal Bilof, editor, *COMPSAC 05 The 29th Annual International Computer Software & Applications Conference*, pages 425–430, Edinburgh, Scotland, July 2005. IEEE Computer Society.

[15] Maarten W. van Someren, Yvonne F. Barnard, and Jacobijn A.C. Sandberg. *The Think Aloud Method A practical guide to modelling cognitive processes.* Knowledge Based Systems Series. Academic Press, London, 1994.

A Videotaped Scenario Storyboard

	 mCESG Online Voter Registration Form - Mozilla Firefox File Edit View Go Bookmarks Tools Help file:///C:/Documents%20and%20Settings/Tim%20Storer/My%20Doc Go Done **Your new registration.** Please tell us your new address. We will use this information to transfer your registration. First Line: Open Close Second Line: Town: SumWhElse Post code: KYAP123 **Absentee Voting** Please tick this box if you wish to be **sent credentials for electronic voting.** ☑ When you are ready, click **submit** to change your registration information. If you want to start over, click **clear**. Submit Clear	 mCESG Online Voter Registration Form - Mozilla Firefox File Edit View Go Bookmarks Tools Help file:///C:/Documents%20an Go Done **Are These Details Correct?** Natasha Smith: Changed address to: Open Close SomeWiElsein Fife KYAP 123 Check this box if you understand the terms under which you may register online. Submitting false information may constitute an electoral offence ☑. Now click Submit if you wish to confirm your registration, or clear to start over. Submit Clear

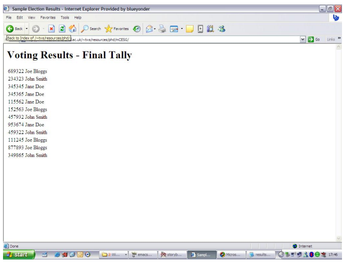
1.Having moved house, Natasha decides to register to vote at her new local authority online, rather than by post.	2.Natasha fills in a form online, using the registration document sent to her house. She decides to request electronic voting credentials because she may be busy on polling day.	3.Natasha checks the box to indicate that she has understood her legal obligations before clicking submit.
	 POLLING CARD Your Polling place is at: A Town School Hall On-this Road A Town APC 123 Polling times: 7am - 10pm You do not need this card in order to vote. Electronic Voting Credentials Voter Number: VOTER IDENTITY NUMBER TAB Candidates — Personal Candidate Numbers — Response Numbers Joe Bloggs (Tea Party) Jane Doe (Fancy Dress Party) John Smith (Christmas Party) Response Numbers APPLY SECURITY CARD HERE Candidate numbers 238 115 450 903 925 156 Security Card	 POLLING CARD Your Polling place is at: A Town School Hall On-this Road A Town APC 123 Polling times: 7am - 10pm You do not need this card in order to vote. Electronic Voting Credentials Voter Number: 0455 3435 7683 56454 Candidates — Personal Candidate Numbers — Response Numbers Joe Bloggs (Tea Party) 21 238 115 562 Jane Doe (Fancy Dress Party) 90 450 903 790 John Smith (Christmas Party) 18 925 156 239 Security Card
4.Two separate voting credential documents arrive in the post. This helps prevent the credentials being intercepted by a fraudster.	5.The voting credentials are sent as two separate documents polling card and a security card (top right).	6.Natasha removes the protective tabs on the polling card and sticks the security card where indicated, to reveal the complete Voter Number and Candidate Numbers.
		
7.On her way to work, Natasha opens her polling card to cast a vote, using her mobile phone. She types her Voter Number and the Candidate Number of her choice into an SMS message.	8.In a few mintues, a confirmation message arrives at Natasha's mobile.	9.Natasha sits down at her desk at work. She works in an open plan office, where one colleague sits near enough to see her screen.

	 Sample Election Results - Internet Explorer Provided by blueyonder Back to Index of /~tws/resources/phd/ Address http://www.dcs.st-andrews.ac.uk/~tws/resources/phd/mCESG/ Voting Results - Final Tally 689322 234323 345345 345365 115562 152563 457932 953674 459322 111245 877893 349865 Done	

10.Natasha checks that the Response Number next to her chosen candidate on her voting credential has been published on the election's webpage along with those for all votes cast.

11.Natasha uses the search function of her web–browser to find the number.

12.After the close of poll, Natasha can confirm that the correct candidate was published next to her Response Number on the election's webpage.


Sample Election Results - Internet Explorer Provided by blueyonder
File Edit View Favorites Tools Help
Back
Search
Favorites
Back to Index of /~tws/resources/phd/
.ac.uk/~tws/resources/phd/mCESG/
Go
Links
Done
Internet
start
2 Wi...
emacs...
storyb...
Sampl...
Micros...
results...
17:46

Voting Results - Final Tally

689322 Joe Bloggs
234323 John Smith
345345 Jane Doe
345365 Jane Doe
115562 Jane Doe
152563 Joe Bloggs
457932 John Smith
953674 Jane Doe
459322 John Smith
111245 Joe Bloggs
877893 Joe Bloggs
349865 John Smith

13.Natasha uses the browser search function to find her number again. Assuming everybody else checks their vote, the results of the election will be accurate.