Electronic Voting in the UK: Current Trends in Deployment, Requirements and Technologies

Tim Storer and Ishbel Duncan
University of St Andrews
North Haugh
Fife
St Andrews
KY16 9SX
{tws, ishbel}@dcs.st-and.ac.uk

***Abstract*— Recent controversy regarding reforms to the voting system cast doubt on the likelihood of deploying electronic voting systems in the near future. This paper notes the deficiencies in the approach to requirements for electronic voting in general and outlines some of the recent developments in electronic voting technologies in the UK.**

I. Introduction

The UK Government has set a goal of conducting a General Election utilising electronic voting technology some time after 2006. However, recent controversy regarding other reforms to the voting system cast doubt on the governments ability to achieve this goal. In section II This paper considers the consequences of previous reforms to the voting system in the UK and the results of the early pilots of electronic voting. In section III this paper briefly outlines some flaws in the traditional approach to requirements for electronic voting technologies and outlines some alternative approaches. In section IV the paper considers recent development of the voting schemes and technologies in the UK compared with those deployed in the US. In particular, two systems recently proposed for the UK electoral context are outlined with the intention of illustrating the context dependent nature of electronic voting technologies. Finally section V summarises the trends in UK voting technologies and suggests the likely next steps if the UK is to move towards fully electronic voting.

A. Definitions

There is substantial confusion in the literature regarding the proper terminology for the interaction between voting and technologies. Various terms including voting system, electoral system, voting scheme and voting technology are often used inter–changably. In an attempt to clarify the following discussion, we propose the following definitions:

Voting System The overall term for the collection of processes, algorithms and agents collectively casting votes in order to achieve a decision. A voting system is described by an electoral system; requirements for secrecy of elements of the electoral system; validation of elements of the electoral system and the usability requirements for the voting technology employed.

Election A single execution of a voting system, from identification of participants (e.g. through registration) to identification of the decision made.

Vote The abstract expression of a voter's choice in an election, constrained by the voting system's electoral system.

Franchise The description of an actor's eligibility to participate in an election as a voter. A consequence of this defintion is that a voter is considered to be some actor in the voting system with the authority to cast votes.

Electoral System The method by which a voter's choice is expressed and the algorithm by which the aggregation of all voter's choice are calculated, Single Transferable Vote for example.

Voting Scheme The abstract description of a technology that fulfills the requirements of a voting system.

Voting Technology The artifacts and processes employed to conduct an instance (election) of a voting system. A voting technology implements a voting scheme.

Ballot The implementation of a voter's vote within the voting technology.

Note that these definitions identify a distinction between the particular technology employed to conduct an election and the requirements of the underlying voting system. Further, the definitions do not intend to place any constraints on the requirements for elections, for example, a definition of democracy is deliberately excluded.

II. Voting Technology Pilots

The decision to investigate the use of new technologies for elections was taken following the dramatic decline in turnout after the 1997 General Election. Whilst it is acknowledged that this decline is due to several factors [1], a recurrent theme has been the need to change the voting system in order to improve accessability and convenience. The Government has introduced several reforms to the UK voting system designed to increase the convenience of casting a vote, including the provision of postal voting on demand in 2000 [2]. Consequently, the use of postal voting has increased dramatically. Figure 1 illustrates the increase in use of postal voting between 1992 and 2005, when postal votes represented approximately 15% of all votes cast. Whilst it is unclear whether these

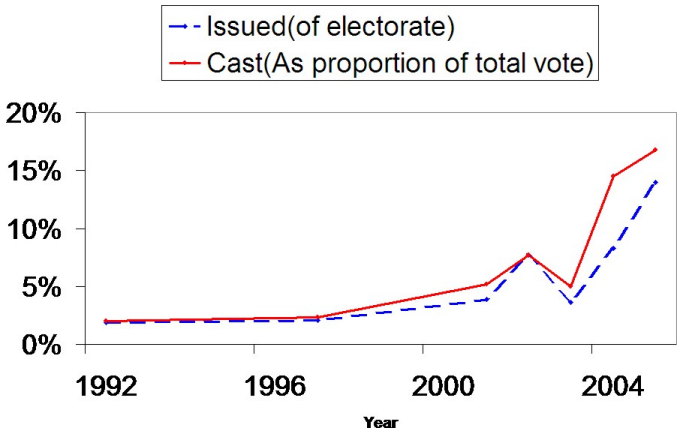

Fig. 1. Trends in Postal Voting over various elections in the UK since 1992

reforms have had much impact on turnout, it is noteworthy that the 2004 European Elections experienced the highest ever turnout in the UK at 42%, compared with a Europe–wide decline [3].

Such changes have not been without controversy, including the conviction of sitting councillors for electoral fraud during the 2004 local elections [4] and similar allegations in Scotland during the recent General Election [5]. Such difficulties have raised questions about the governments committment to future changes to the voting system, given the negative publicity that can ensue. In reality, the postal voting system is vulnerable to the same weak authentication mechansims employed in polling stations, exasperated by the remote nature of the system. Despite these problems, the government has repeated its determination to implement electronic voting in the near future. This is perhaps less surprising given the dramatic increase in applications for postal votes over successive elections.

It is anticipated that there will be further pilots of electronic voting technologies during local authority elections over the next few years towards the General Election expected in 2009–10. These pilots will build on the those conducted in the run–up to the recent General Election, which were conducted in 2000, 2002 and 2003. [1] The trials conducted prior to 2005 were generally deemed to be a success in terms of the technology, although evidence of increased take–up and improvement in turnout are rather more mixed [7]. Whilst the sustained availability of postal voting on demand has provided a period of time in which take–up has improved, the sporadic availability of electronic voting in a given electoral area mitigates against adoption, since a voter is less likely to experiment with a voting system that may not be available in future. The Electoral Commission's proposed new framework model for elections may improve this situtation by providing a basis for implementing electronic voting pilots in a consistent manner [3].

[1]Although region wide all–postal voting was trialed in 2004, there were no trials of electronic voting that year due to opposition from the Electoral Commission [6].

III. Requirements

Various attempts have been made to express the requirements for an electronic voting technology in both the United States and United Kingdom, as well as elsewhere. Early requirements documents addressed specific devices in particular circumstances (typically US), for example electronic counting devices [8] and later requirements for Direct Recording Electronic (DRE) machines [9]. In the UK, a recent study by the commerical arm of GCHQ (the government's electronic communications agency) proposed a security policy for remote electronic voting [10]. An alternative approach has been to develop standards for the implementation of electronic voting technologies based on a common format, the Election Markup Language, for example [11].

It has been noted that such approaches to the requirements are unsatisfactory for several reasons:

- Typically, the requirements are produced for technologies to be deployed in a particular electoral context, which may not be suitable elsewhere [12]. For example, technologies that publish vote values in order to provide some form of verifiability may induce undesirable information leakage in ordinal electoral systems, where voters may used low–ranked candidates to identify their vote publicly without affecting the tally [13].
- The requirements are typically either so high level that reproducable tests based on measurable metrics cannot be employed, or alternatively so low–level that they are only satisfied by a single technological solution [14].
- There is no guarantee (or even some re-assurance) of the completeness of the requirements set. Whilst this is not a problem limited to electronic voting technologies, the use of natural language descriptions of requirements mitigates against the development of a complete set.

Whilst a plethora of requirements documents continue to be produced for electronic voting technologies, a formal basis for their development would be more satisfactory. One approach suggested is to use a technique such as the B–method, where a single high level statement of a particular requirement is developed by successively more detailed stages into a particular voting scheme. Such an approach would require proofs that each stage retains the properties described at a higher level in order to demonstrate a particular scheme fulfills a particular requirement.[2]

An alternative is to develop a modelling approach for describing the components of different electoral systems in a particular manner. Templates might then be developed to state the requirements on the detailed components in terms of secrecy and verifiability for similar elections, which could then be customised for particular contexts [12]. This approach avoids references to particular technological features by stating the requirements for secrecy/verifiability of components on the underlying electoral context.

[2]This suggestion is attributed to Jeremy Bryans of Newcastle

IV. TECHNOLOGIES

The United States has traditionally provided the lead for the development and deployment of new electronic voting technologies. This trend began with the introduction of electronic counting of punch card and optical scan ballot papers and the first of use telephone based voting systems for non–binding referenda [15]. The development of DRE machines in the early 1980s also occurred in the United States as a replacement for the century old Lever machines [9]. Several early theoretical voting schemes and crypto primitives were also developed in the United States, including mix–nets [16] and homomorphic encryption [17].

The interest in modernising voting technologies has resulted in two schemes proposed in the UK. Both schemes permit the election itself to be verifiable rather than providing mechanisms for verifying the correctness of the technology (through machine inspection, parallel testing etc). The two schemes developed in the UK are:

- The **mCESG scheme** was adapted from any existing (flawed proposal) for using mobile phone SMS technology to cast verifiable votes. The system is designed to provide convenience to a voter, together with the ability to confirm that a vote is correctly included in the tally [18]. The system utilises the existing practice of providing voters with a polling card to deliver voting credential information that can be used to cast a vote electronically. To cast a vote, a voter sends a combination of their personal voter number and a personal candidate number printed on the voting credentials, via some delivery medium, SMS for example.

  To confirm that their vote has been received by the election authority, the voter visits the authorities website, where a receipt number for the combination of voter and candidate number (also printed on the voting credentials) is published. This confirms that the vote has been correctly received (but not processed). After the close of the election, the voter can re–visit the site, where the identity of the correct candidate should be published next to the response number. The voter can use the voting credentials to force the election authority to correct the information published on the website. Providing the voter keeps the credential secret, the voter's secrecy can only be violated by collusion between several distinct entities within the Election Authority who initially co-operate to produce and deliver the voting credentials.

  Several adaptions of the mCESG scheme have since been proposed to provide greater protection for voter privacy and to allow the scheme to be used for ordinal electoral systems. A prototype implementation of the scheme is available and is currently undergoing experiments to evaluate usability issues.
- Conversely, the **Prêt á Voter** provides an experience remarkably similar to that of the existing paper ballot/polling station system [19]. On entering a polling station a voter is provided with a paper ballot as normal, except that in place of a serial number, the ballot is marked with a "onion" value. This value represents a layered encryption of randomly generated "germ values", with each layer encrypted under an asymetric algorithm - RSA for example. The lowest level of the onion is a nonce value, equivalent to a serial number. The ordering of candidates on the ballot is randomised, but may be recovered from the germ values A representation of the ballot is provided in Figure 2. To cast a vote, the voter marks the ballot as normal next to their candidate. The left hand side of the ballot is then removed and the right hand side scanned so that the position on the ballot marked and the onion can be published on a publicly available electronic bulletin board. The voter may then leave the polling station with the right hand side of the paper ballot only and later confirm that this receipt was correctly published on the bulletin board.

  During tallying, the onion values stored on the bulletin board are successively decrypted through an RSA–decryption mix. At each stage, the position of the voter's mark is adjusted by a hash of the onion layer germ value, until the original voter's choice on the ballot paper and the stored nonce value are recovered. These are then published to a second bulletin board for further processing, depending on the electoral system in use. The system can be adapted for ordinal electoral systems by adjusting all positions on the ballot paper by the hashed germ during decryption. By passing the votes through a decryption mix, collusion between the k–tellers of the mix is required to associate a onion–position pair with a nonce–position pair.

1. Tea Party	
2. Birthday Party	
3. Dinner Party	
4. Fancy Dress Party	
	x!2%fd

Fig. 2. The paper ballot of the Prêt á Voter scheme. Note the 'onion' value placed on the bottom right of the paper ballot below where the voter marks their choice.

Curiously, neither system addresses the task of voter authentication, assuming this task is undertaken through external technologies and/or procedures. Rather, both systems adhere to the existing requirement of the UK electoral context that voting technologies provide a means for associating a vote with a voter under limited circumstances (an election judge may order a scrutiny of ballot papers and other documentation during an election petititon [20]). For the mCESG scheme, this is provided by collaboration between three domains, the Registration Officer (who stores voter identities), the Returning Officer (who stores candidate identities) and the Vendor responsible for maintaining the vote collection infrastructure. For the Prêt á Voter scheme, it is possible to record the onion value of a ballot paper next to the identity that used it on the marked electoral roll. Should an identity be discovered to have been used fraudulently, the proper onion value can be removed from the bulletin board and the tallying scheme re–run.

Both these schemes have the further advantage that if

more than one vote has been determined to have been cast fraudulently it is possible to mask who they were cast for (on an indivdidual basis) by removing the corresponding response number/onion value of all fraudulent votes at once.

The two schemes reflect a clear difference in design philosophy with the DRE machines employed in elections in the US. Much focus has been on the need to develop standards for testing the correctness of hardware and software of DRE machines prior to deployment on election day, for example [21]. However, the schemes developed for use in the UK (in common with most academic schemes in the US) are designed to provide individual voters to verify their vote, and external observers to verify the entire election. This represents a considerable shift from the existing practice in the UK, where the role of ensuring the correctness of an election result is delegated to the nominated candidates at the count [20]. Whilst the candidates continue to participate in the verification of the election (through encouraging their supporters to check their votes, for example), the primary responsibility for ensuring that votes are properly counted becomes that of the voter.

V. Conclusions

Given the recent controversy regarding changes to the UK's electoral system it seems likely to us that schemes which are most similar to the existing polling station/paper ballot practice will be introduced initially. Systems which implement the Prêt á Voter scheme seems suited to this role, since its primary contribution is to improve the security of the paper ballot system by publicly committing the election authority to the value of a voter's choice, without revealing the value of that choice.

The introduction of a successful electronic voting scheme that *improves* the security of the existing system may go some way to mitigating the concerns regarding electronic voting in general. This may then provide an opportunity at a later date for the deployment of remote electronic voting systems, e.g. those which implement the mCESG scheme. Such systems would be better suited to meeting the governments goal of modernising the voting system and improve the accessability and convenience of the voting process. Such an approach to implementing electronic voting would also follow the Electoral Commission's approach to modernising elections through the deployment of multi–channel voting systems, where the voter is able to choose a channel most suited to their circumstances. Ideally, every voter should be provided with the opportunity to use at least one voting system which is suitable to their particular needs.

References

[1] L. Pratchett, *The Implementation of Electronic Voting in the UK*. LGA Publications, 2002.

[2] "Representation of the People Act," 2000, ch. 2.

[3] "The 2004 European Parliamentary Elections in the United Kingdom," The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, December 2004. [Online]. Available: http://www.electoralcommission.org.uk/files/dms/ECPartElections2004_154%38-11422__E__N__S__W__.pdf

[4] R. Mawrey QC, "Judgement in the matter of a local government election for the Bordesley Green ward of the Birmingham City Council held on the 10th June 2004 and in the matter of a local government election for the Aston ward of the Birmingham City Council held on the 10th June 2004." HM Courts Service, April 2005. [Online]. Available: http://www.hmcourts-service.gov.uk/cms/files/full_judgment_bordesley_gr%een_aston_wards_election_10th_june_2004.pdf

[5] J. Kirkup and F. Urquart, "Scottish seat at centre of postal vote fraud fears," The Scotsman, May 2005.

[6] "Electoral pilots at the June 2004 elections: The location of pilot schemes at the combined European parliamentary and local elections," The Electoral Commission, December 2003. [Online]. Available: http://www.electoralcommission.org.uk/files/dms/Electoralpilots_finalre%port_11383-8941__E__W__.pdf

[7] "Voting for change - an electoral law modernisation program," The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW, 2003. [Online]. Available: http://www.electoralcommission.gov.uk/files/dms/Votingforchange_9829-79%78__E__N__S__W__.pdf

[8] R. G. Saltman, "Effective use of computing technology in vote tallying," National Bureau of Standards, Washington D.C. 20234, Final Project Report NBS SP 500-30, March 1975.

[9] ——, "Accuracy, integrity and security in computerized vote-tallying," National Bureau of Standards, Research Report 500-158, August 1988. [Online]. Available: http://www.itl.nist.gov/lab/specpubs/500-158.htm

[10] "e-voting security study," Communications and Electronic Security Group (CESG). Available at http://www.edemocracy.gov.uk/library/papers/study.pdf, July 2002. [Online]. Available: http://www.edemocracy.gov.uk/library/papers/study.pdf

[11] J. Borras, "Overview of the work on e-voting technical standards," Cabinet Office, UK Government, May 2002.

[12] T. Storer and I. Duncan, "Modelling context for the design of remote electronic voting schemes," in *IADIS International Conference e-Society 2004*, P. Isaías, P. Kommers, and M. Macpherson, Eds., vol. 2. Avila, Spain.: IADIS Press, July 2004, pp. 1001–1004.

[13] M. P. Smith, K. Coughlan, D. Lane, D. O' Hare, and B. Sweeney, "First report on the secrecy, accuracy and testing of the chosen electronic voting system," Commission on Electronic Voting, Kildare House, Kildare Street, Dublin, December 2004. [Online]. Available: http://www.cev.ie/htm/report/first_report.htm

[14] "Assessment of current status of voting system standards and other resources relevant to human factors and privacy," National Institute for Standards and Technology, February 2005.

[15] E. J. Novotny, "Democracy by computer: Design, operation, and implementation of a civic communications system," in *The Systems Approach: Key to Successful Computer Applications, Thirteenth Annual Technical Symposium*. Washington D.C. Chapter ACM and Institute for Computer Science and Technology, National Bureau of Standards, June 1974.

[16] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, February 1981. [Online]. Available: http://world.std.com/~franl/crypto/chaum-acm-1981.html

[17] J. Benaloh, "Verifiable secret ballot elections," Ph.D. dissertation, Yale University, December 1996.

[18] T. Storer and I. Duncan, "Practical remote electronic elections for the uk," in *Privacy, Security and Trust 2004 Proceedings of the Second Annual Conference on Privacy, Security and Trust*, S. Marsh, Ed., National Research Council Canada. Fredericton, New Brunswick, Canada: University of New Brunswick, October 2004, pp. 41–45.

[19] D. Chaum, P. Y. A. Ryan, and S. A. Schneider, "A practical, voter-verifiable election scheme," School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK., Tech. Rep. CS-TR-880, December 2004.

[20] "Representation of the People Act," 1983, ch. 2.

[21] T. R. Wilkey (Chair), "Voting systems performance and test standards," National Association of State Election Directors Voting Systems Board, Standards Document v2.0, December 2001.