

Free Elections... A change of heart?

By Jason Kitcat, j-dom.org, originally published in LinuxUser magazine

It has emerged that the government has quietly changed its electronic voting policy while seemingly failing to advise the suppliers it expects to provide the e-voting technology. This appears to be the result of the straggling mess of departments who share responsibility for voting policy and implementation are struggling to implement and communicate the government's vision for electronic voting.

Quietly, quietly

The government's u-turn on e-voting policy was not announced in a press conference or even press release but deep with the pages of several obscure documents. I received a summary of the response to the government's e-government consultation via email from the Office of the e-Envoy and was interested to find the following on page 8:

"As a result [of the consultation], some [e-voting] requirements were modified. In particular, a requirement to support 'publicly verifiable code' was introduced, to strengthen the auditability of electoral systems"

pp8 para 17 In the service of democracy – Your Response

At first blush it appeared the government had accepted the arguments of several activists in the Free Software world, however a source within the Office of the e-Envoy soon indicated that this phrase "isn't what you think it is" and hinted that there may have been an erroneous hint towards opening the source of the voting systems. Shame.

To gain further insight I examined numerous documents from the various government departments involved and discovered that changes had quietly been made to the e-voting security requirements at the beginning of November 2002. These changes added several additional requirements which significantly improved the likely security of any systems which met all the stated goals. Most importantly I found the source for the use of the phrase 'publicly verifiable code' in requirement 15 as shown below:

"OS15 Public Verifiability

The e-voting service must be publicly verifiable.

In order to maintain the electorate's belief and willingness to be bound by outcome of an election, an e-voting system should:

1. Verifiably capture the voters' intent
2. Verifiably preserve that intent until tabulation
3. Verifiably tabulate that intent into the election result"

pp12 section 2.4.2 e-voting Technical Security Requirements 1.0

Wonderful news indeed, this additional requirement could significantly improve public trust in an e-voting system. Unfortunately there are several problems with the clause as currently worded: Firstly there is no definition of what public verifiability

entails, could it be a third party (such as the Electoral Commission) examining the systems or any member of the public? Furthermore how could one be sure that the system examined actually is the one in use?

Secondly, and rather interestingly, the clause makes no mention of the parties and their views on the reliability of such methods. In other words this isn't just about the electorate being bound to the outcome but the candidates and their parties. I asked the parties what they thought about e-voting and the government's difficulties managing the process. Various spokespersons responded, most agreeing that e-voting was not going to improve turnout significantly (contrary to government arguments) but could have other benefits.

Conservative MP Eric Pickles, Shadow Secretary of State for Local Government and the Regions commented via email that the Tories were broadly in favour of e-voting "provided proper safeguards are in place against electoral fraud and technological failure. It is important to remember that a computer system crashing has the same impact as a polling station closing early on polling day." But in fact, I would argue, an e-voting system crashing could be worse because it could corrupt the final result, not just delay its delivery.

In a phone interview Lib Dem IT spokesman Richard Allan MP expressed the view that "the linkage to turnout is unhelpful". His view was that "absolute anonymity is not important but control of the access to voting records" would need care. "Most people will not understand the verification [of electronic votes], they will see the process as being tainted" when contrasted with our existing system which is easy for 'Joe Public' to comprehend intuitively. Interestingly he draw a parallel with banks arguing that the government might close polling stations (i.e. branches) in favour of more remote voting methods reducing turnout in the process. "It's a cost benefit question, these 'e-projects' have been developed regardless, but I question the need. [Labour] have tied this up in the e-government agenda, their motives are other than free and fair elections." He argued for the Electoral Commission taking a driving role in electoral reform due to their independent statutory position. Mr Allan is MP for Sheffield Hallam who have already experienced some of the e-voting pilots, and he reported delays resulting in potential voters walking away and important checks being abandoned.

Dr Spence Fitz Gibbon of the Green Party National Executive stated in an email "we believe (from the evidence so far) that e-voting still has a long way to go before demonstrating that data is sufficiently secure [and that] people using it are not going to be disenfranchised through security breaches or technical malfunction." He added that "we still believe that people have the right not to utilise high-technology in their lives and we also recognise that some may not have access to the technology. Subsequently, it is imperative that traditional voting systems continue to be available."

The Labour Party were asked to comment but failed to respond.

Thus the parties are, at best, ambivalent to the technology. While they were unwilling to comment too specifically on the changed requirements all were clearly uneasy with government's record of managing technology. There are certainly clear

arguments to be made for expending the resources currently allocated to e-voting on other more worth projects that would be more likely to re-invigorate the political process. Certainly it was interesting to note during my research the low profile the parties appeared to be giving this issue considering how vital it is to their existence.

Could you explain that?

I have been unable to find any supporting documents to explain these new requirements but we contacted the relevant government departments for clarification. There was initially some confusion over who was actually responsible but it has emerged that Mark Rickard, from the Office of the e-Envoy wrote the phrase 'publicly verifiable code' but he has been strangely unavailable to our requests for comment over the last two weeks. This was the same man who met Dr. Rebecca Mercuri and representatives of FIPR on her recent visit to the UK and signed off on the notes from the meeting, could he also have made the changes as a result of this meeting? One of Dr. Mercuri's key points is that commercially available electronic voting systems lack any form of public verifiability. Mr. Rickard has now been appointed Director of the Hansard Society's e-Democracy programme so perhaps he's too busy to answer. Dr. Mercuri declined to comment.

The original security requirements document emerged from CESC (see Box) but there has been no indication of who made the changes since first publication nor the process behind the formulation of those additional requirements, leaving the new requirements clouded in mystery.

However most bizarrely the electronic voting suppliers bidding for this year's pilots that I contacted either refused to comment or admitted, off the record, that they were completely unaware of these additional requirements and couldn't say how they would comply. Why the government failed to communicate with its suppliers is unclear, nor has it been explained how the bidding process will comply with its own requirements, especially considering the following:

"Providers are expected to comply with, or demonstrate they are actively moving towards these standards. Providers are expected to comply with any changes to the standards in the light of future developments and incorporate developments and improvements into their services."

pp11 Electoral Modernisation Pilots – Statement of Requirement

The only get-out clause I can see is that the government provides a very weak definition of 'moving towards these standards' so that suppliers can actually qualify. However if they do so the good work of the updated security requirements and the Election Markup Language (EML) XML standard (to encourage cross-vendor interoperability) will be neutered.

An alternative interpretation might be that the requirements were changed by one department (Office of the e-Envoy) without consultation with the Office of the Deputy Prime Minister who merrily continued on with the bidding process unaware of the more stringent requirements added with the best of intentions. Or the cynic might

argue that the new requirements were only added after the contractual negotiations had proceeded far enough to make compliance impossible.

Another fine mess

So we are in a position where the government has, on paper, created some improved requirements for its electronic voting technologies. However the reality is that of confusion between departments (see Box) and the likelihood that suppliers won't be made to meet the new requirements. The Office of the Deputy Prime Minister (ODPM) have already missed their timetable for announcing the winning bids for the 2003 pilots. Originally the announcement was planned for 15th January but without explanation the successful council applications (or a portion at least) were announced on the 23rd and we are yet to hear the list of winning suppliers. An ODPM spokesperson only cited "tendering process complications" as the reason for delaying the supplier announcement and my enquiries with suppliers blamed the delays mostly on bureaucracy but also finalising technical compliance to the EML standard and not security issues.

While EML compliance would be a boon one can't help wonder whether the delays are due to a last minute realisation that these additional security requirements have been forgotten. Clearly this is a generous assessment of the government's performance and it may well come down to the fact that despite the good words we will be left with systems that are not verifiable. Once again a text messaging (SMS) voting pilot has been announced even though before the previous text voting pilot a source from the suppliers in question shared their dismay with me that such a system, which they knew to be insecure and unreliable, was going to be forced through. The source claimed that the suppliers had informed the government of the problems with text voting but the belief that it would engage young voters had resulted in the pilot being rammed through. So, despite there having been problems reported in the first pilot and the suppliers' own lack of confidence we see another pilot.

This, taken along with the findings reported in this article, does not inspire great confidence in the electronic voting path the government is taking. Either we face another set of pilots without adequate security requirements being applied or we will see a weak effort to comply with the requirements from the vendors, who with their captive market under extreme time pressure in the run-up to the ballots will be allowed to waltz past the checkpoints designed to safeguard our electoral process. If proper checks and balances are not put in place, such as true public verifiability of the systems, then we risk building an extremely expensive voting system which fails to reliably record our democratic intent. A fair deal for Britain? I think not.

BOX – Who's responsible?

There was some confusion when I talked to various departments but this is the way electoral issues are currently managed. The confusion is partly due to the massive re-organisation after the DTLR was split however there was already confusion when responsibility for elections moved to the DTLR from the Home Office near the beginning of Labour's government.

Office of the Deputy Prime Minister

Responsible for the Electoral Modernisation Pilots, including tendering and funding. Also responsible for local elections.

www.odpm.gov.uk

Office of the e-Envoy

Responsible with all e-government issues and thus ran a consultation which covered e-voting. They also appear to be responsible for formulating the requirements documents and interoperability standards.

www.e-envoy.gov.uk

CESG (GCHQ)

The Communications-Electronics Security Group of GCHQ have been responsible for providing detailed technical security requirements for e-voting and have also developed an alternative security system that the government want to see implemented in the next pilots.

www.cesg.gov.uk

Electoral Commission

A statutory body (i.e. created as a result of legislation) responsible to parliament to ensure elections are run according to the law and are required to report on pilots, party funding during campaigns while working to increase participation in electoral politics.

www.electoralcommission.gov.uk/

The Lord Chancellor's Department

Responsible for setting policy with regards to elections and also implementing legislation, particularly the Political Parties, Elections and Referendums Act (2000).

www.lcd.gov.uk

Links

Election Markup Language

<http://www.oasis-open.org/committees/election/>

Office of the Deputy Prime Minister Elections Page

<http://www.local-regions.odpm.gov.uk/elections/index.htm>

Transcript of meeting between Office of the e-Envoy and Dr.Rebecca Mercuri

<http://www.notablessoftware.com/Papers/UKTranscript.html>

Government E-Democracy Consultation

<http://www.e-democracy.gov.uk/>