The Ministry of Economics and the Interior
Slotsholmen 10-12
1216 Copenhagen K

DemTech, The IT-University of Copenhagen
Rued Langgaards vej 7. DK-2300 KBH S
Direct phone. 7218 5282
carsten@itu.dk
Copenhagen, December 14, 2012

This is the English translation of DemTech's official response to the public hearing on the proposal to change the Danish election laws on elections for the Danish Parliament, of Danish members to the European Parliament, and for municipalities and regions (in order to experiment with digital voting and tallying).

The purpose of the research project "DemTech", situated at the IT University of Copenhagen, is to investigate whether it is possible to modernize the electoral process by means of digital technology without compromising the voters' trust in the democratic procedure. DemTech therefore welcomes the prospect for Denmark to gain experiences with digitalization of voting and tallying.

In an international perspective, the current Danish election process works very well, and Danish voters trust the process of voting and tallying. The main question is thus how to maintain trust in light of the changes to Democracy, which digitalizing voting and tallying will affect. In this perspective—and in light of negative experiences with e-voting in other countries—we believe that trials must be approached with the greatest care and with a persistent focus on the democratic aspect.

In the following, we will suggest a roadmap how to make the changes more transparent in the areas that the bill would affect if implemented, how to strengthen democratic control, and how to raise awareness about the effects of digitalization.

Trust in the voting process

As mentioned in the bill, IT is already used in elections. Since the 1990s, it has been Danish policy to use computers to optimize a range of work processes, such as filling out the electoral roll and to support other tasks, such as managing election officials. Hitherto, in contrast, there has been resistance toward digitalizing the act of casting and tallying ballots. In exactly these processes it is challenging to preserve basic democratic principles, not the least of which are the secrecy of the vote and public control. This is why it is paramount to address explicitly the changes to democracy, which a digitalization of voting and tallying imply, to ensure true public control and the secrecy of the vote. This consideration has not become any less important in light of experiences with e-voting in other European countries.

In 2009, the German Supreme Court declared the election law from 2005, which allowed digital ballot casting and tallying, unconstitutional, because it failed to enable citizens to exert public control. The use of digital technology relied on knowledge about IT, which cannot be expected to be mastered by all citizens. (Bundesverfassungsgericht Urteil BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1 - 163)).[1]

In 2008, Holland abandoned the use of digital voting and tallying in response to public critique. The Dutch parliament decided to return to paper and pencil, recognizing that it was not possible to protect the secrecy of the vote because, among other reasons, managing the election had been delegated to private companies to such an extent that public control had been undermined.

Both cases exemplify that the implementation of digital ballot casting and tallying potentially prevents public control of elections. This raises the concern whether the law proposal can be implemented without challenging §31 of the election law, which emphasizes that all voters are obliged to accept the role of election manager or election official.

The involvement of private companies in the electoral process raises new concerns with regards to control mechanisms. The law proposal only suggests involving audit expertise in the evaluation of elections. It is, however, highly problematic if the result of the vote will come to rely on relatively few elections officials and technicians employed by private vendors. We believe that the law proposal should specify how openness and precise requirements to the technology (both product and processes) would be ensured so that the public has realistic means to ascertain what happens and to retain trust.

Furthermore, we believe that the law proposal should contain a range of technical requirements, and that it ought to state more precisely how and to what extent voting and tallying processes should be digitalized. It is relevant, but not sufficient, to mention the European Council's recommendations and to state that these will be addressed as the Ministry of the Interior settles on the frames for digital elections (4.8). These recommendations are very general and insufficient. The law must include requirements to technology complying with precise standards for quality of design, development, evaluation, and for how vendors must be able to prove to their customers, the auditing authorities, governments, and evaluators that their product complies with the requirements. This is, among other reasons, because digitalization

[1] http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html

raises the new question of what constitutes a valid vote. If the law specifies, that one vote is one physical piece of paper, this requires the voting machines to produce a paper version, which makes it possible to assess whether every vote has been counted. Therefore, we suggest that a vote is explicitly defined in the law as a physical paper ballot which can be verified by voters, and that digital versions are defined as secondary representations of the vote.

Technological requirements and processes

The implementation of a digital ballot casting and tallying system will face a series of technically complex challenges. Several other countries which have followed the path towards digital election technologies using public tenders without formulating detailed quality and security standards have ended up losing large financial investments, violating basic aspects of the election process (e.g., the secrecy and freedom of the vote), and trust in the election process has suffered. The bill does not specify in thorough detail what will be required of the technological solution. This is understandable, because, at this point it is undesirable to commit oneself to any particular technological solution. However, the great risk is that stating only very general requirements does not guarantee sufficient quality in practice.

Therefore we recommend that a digital ballot casting and tallying system must live up to the requirements that can be extracted from a series of significant national and international analysis in the area (VerifiedVoting[2], ACCURATE[3], Jones' work[4], the U.S. EAC[5]-especially the work of NIST[6], the California Voter Foundation, the Caltech-MIT Voting Technology Project[7], the Diebold report[8], the SERVE report[9], the SAIC report[10], the RABA report[11], etc.[12]) These requirements should also apply to existing digital elements in the election process, including the digital electoral roll, and Denmark's Statistics' tallying system.

We suggest the following requirements:

1. The programs must handle electronic votes correctly, and the system must protect votes with the same degree of care and caution with which humans

[2] http://verifiedvoting.org/
[3] http://accurate-voting.org/
[4] http://www.cs.uiowa.edu/~jones/voting/
[5] http://www.eac.gov/
[6] http://www.nist.gov/itl/vote/tgdc.cfm
[7] http://vote.caltech.edu/
[8] http://avirubin.com/vote.pdf
[9] http://servesecurityreport.org/DoDMay2007.pdf
[10] http://www.elections.state.md.us/pdf/risk_assessment_report.pdf
[11] http://people.csail.mit.edu/rivest/voting/reports/2004-01-20%20RABA%20evaluation%20of%20Diebold%20AccuVote.pdf
[12] See, in particular, Rubin's Brave New Ballot; Herrnson et al.'s Voting Technology, and Jones and Simons's Broken Ballots.

today handle paper ballots.

2. The program code works on behalf of the voters. Therefore one must be able to produce proof (i.e., certificates) which convinces the electorate that the correctness of the count is as good as a manual count of paper ballots.
3. The program code, associated intellectual property rights, and any custom hardware must be public property during the entire process, including the development phase.
4. APIs, data files, system logs, and other user interfaces and artefacts must be developed according to ‘best practices’.
5. The implementation of a digital system for voting must be done in accordance with a principle of minimalism. I.e., the system should only be capable of collecting, printing and/or tallying votes—no more, no less.
6. Electronic systems for voting should be recognized and certified as safety-critical systems in accordance with international standards.
7. An independent certification body should be accorded the task of ensuring that the standards are followed.

Complementing these requirements, we recommend that the program code must comply to the highest existing standards on security and correctness, which applies to safety-critical systems such as nuclear power plants, financial systems, and transportation systems (An exemplary set of mandatory international standards for spaceflight and aeronautics is “DO-178 Software Considerations in Airborne Systems and Equipment Certification”).

We recommend adding such requirements to the bill itself. Other countries have failed to do so and, consequently, these requirements have been ignored. Concerning security and correctness we recommend that voting systems be developed in compliance with ”Common Criteria Evaluation Assurance Level 7 (ISO/IEC 15408)”. Concerning security we recommend the requirement to comply with the best international practices in information security, e.g., the ISO/IEC 27000-series of standards.

In the effort to ensure compatibility and avoid that access to vendor-controlled parts of systems gets blocked, we recommend to comply to international standards for ”interoperability and open data formats”, e.g., IEEE working group P1622[13] or similar. Moreover, current and future international standards in data-formats for electronic voting-elements (e.g., paper ballots, electoral rolls, lists of candidates) should be recognized. This would, for example, make it possible to use several mutually independent tallying systems, which may enhance trust in a particular tally or in a re-count.

[13] http://grouper.ieee.org/groups/1622/

In order to ensure that the voting system complies with local and international requirements, we recommend to confirm to ”traceability of requirements conformance” (per ISO/IEC 24765), and thereby a specific way to comply with the requirement found in recommendations from The European Councils Ministerial Committee (EC Rec(2004)11)[14], ensuring that the current system actually complies with the requirements to which it is subjected.

Concerning the validity of the vote (i.e., the ability to provide a guaranty that the elections result is correct) the following is recommendable. First, we recommend using ”Rivest and Wack’s principle of software independence”[15]. Second, we recommend that any voting system which eliminates or deflates the importance of the paper ballot and the manual count of it must be assessable by election officials and voters. Finally, we recommend ‘best practices’ in relation to risk-limiting post-election audits[16], which are used in California and Ohio as a standard for digital tallying.

Even though it does not guarantee an error-free system, we also recommend the law warrants that the hardware and software of the system is Open Source. Open Source contributes to transparency. We recommend using a publicly accessible Open Source-license such as GPL, MIT, BSD, Apache, Eclipse, etc.

Furthermore we suggest that the entire development process is kept transparent by making election technologies and artefacts publicly accessible (not only after an election, which is currently the most open procedure followed internationally), but that all artefacts are subjected to public control from the very beginning, for instance by making them available via a service like GitHub[17].

Doing so would mean that Denmark could benefit from its existing and internationally recognized tradition for citizen involvement. For instance, IT-experts would be able to participate in checking, maintaining, developing, and conducting electronic elections. We expect that this openness would also strengthen trust in the transformed electoral process.

As regards handling and archiving elections materials, we recommend that the bill specifies more precisely how these materials will be safeguarded and for how long they will be filed. No matter whether we are dealing with physical objects, such as the logbooks used today, or digital logs and encrypted votes, these have to be protected from manipulation. We recommend following ‘best practice’ standards in

[14] https://wcd.coe.int/ViewDoc.jsp?id=778189
[15] http://en.wikipedia.org/wiki/Software_independence
[16] http://static.usenix.org/event/evtwote09/tech/slides/hall.pdf
[17] http://github.com

“digital forensics” e.g.. ISO/IEC 27037:2012 or similar[18]. For example, it is a very complex and important task to describe how to destroy the digital votes so that they cannot be traced back to individual voters in order to protect the secrecy of the vote.

Experience in other countries has shown that it is problematic to rely on off--the-shelf and closed source software and hardware because this often results in systems that are built which are not secure or do not work correctly. In any case, we recommend following a minimalists principle. Any technology which assists in filling out or printing a valid ballot should only be able to fulfil this task, e.g., it should not be able to run standard programs, for instance word-processors, email programs, or similar (because these systems are not open, they pose a potential threat). In general, the relevant ISO/IEC and IEEE standards should be followed, especially the ones directly relevant for safety-critical systems and electronic elections (e.g., ISO 9000:2005, ISO 9001, ISO/IEC 29110, ISO 12207:2008, ISO/IEC 24765, IEEE 830-98, IEEE 1220-2005 and ISO/IEC 12207).

It should be mentioned that several IT-development and consultancy organizations only comply with ISO 9000 & ISO 9001, which exclusively certifies the quality of paperwork, and not the quality of the processes and technology. Minimal but rigid requirements should be applied to the depth and quality of security evaluations. There are similar problems ignoring critical standards of practice, as other countries have seen, without demands for a minimal and rigid security revision. Reading the current draft bill, we find that there is a risk that such an evaluation will not be applied (as is the case today), or only a lightweight version will be enforced, which will not be able to reveal any real security issues, either to the authorities or the public.

Evaluation

It is constructive that the bill makes it possible to set up requirements for planning, conducting, and evaluating trials with digital voting and tallying in order to assess whether the municipalities possess the necessary technical, personnel, and economic capacities to use such digital systems.

Technical requirements are mentioned, and in the above, we suggest that they are specified and included in the bill itself, and so are demands on the municipalities to provide information to citizens, to educate personnel, election managers as well as officials, and to take care of organizational aspects. Furthermore it demands that the municipalities participate in evaluations.

But the idea of evaluation in the bill is limited to questions of user-friendliness and efficiency improvements. This is reflected, for instance, in the important discussion

[18] http://www.iso27001security.com/html/27037.html

of whether it should be mandatory in the trials for voters to cast their vote digitally or not. The argument for making digital voting voluntary is justified by acknowledging that voters may lack IT skills. Yet, insofar as the purpose of the trial is to assess the citizens' trust in digital elections, one must argue that participation needs to be voluntary. This will allow citizens to state their opinion on digital voting as citizens, and not just as IT users. The idea that the citizens' ability to master digital voting is a measure of their trust in the system is not true. The question of citizens' individual experiences with system success or failure must not be mistaken for the question of trust in elections and democracy.

We suggest that all of the aforementioned evaluation is made mandatory and has to address questions of security, as well as functional, organizational, social, and not least, democratic aspects. If one has to envisage how the trust of the voters will be affected in the long run, it is absolutely necessary to include cultural and material conditions, as well as the practical execution of elections, and not just centre on individual experiences.
Furthermore, we suggest that independent and non-commercial bodies should conduct the evaluations.

Economic consequences

Considering the broad range of technical and organizational changes that the law proposal points out, we wonder why, in the section that assesses the economic consequences, it is stated that the main share of the costs will be one-time expenses for buying software and equipment, and that expenses for maintenance, the continued development of the system, education, and other activities will be minimal. This statement contradicts research results, which points to the inverse. Start-up expenses normally amount to a small part of the overall costs, against which expenses for maintenance and further development completely overshadows.

Furthermore, for example, the Norwegian report "Electronic Voting – Challenges and Opportunities" from 2006 points out how trials must be expected to require more resources than ordinary elections, not only because new expenses appear, but also because it will take more time to train the personnel and to assist voters. There might be a need for more ballot booths, because voters will take longer casting their vote, etc.

Summary

We from DemTech welcome the opportunity to gain experience with digitalization of the electoral process. Yet, we suggest that more time should be spent preparing trials and evaluations. As public control is challenged and it becomes more difficult to ensure the secrecy of the vote, trials and evaluations should address questions about how to maintain trust. Our suggestion as to how these questions can be handled is to specify in the bill itself a range of technological requirements. The aim is to ensure control of the process and create greater transparency as well as a good understanding of the consequences of digitalization.

Furthermore, we have pointed out that evaluations must address broader cultural, and material conditions besides questions of user friendliness and the voters' abilities to use a certain technology. Finally, we had hoped for the opportunity to conduct non-binding trials, allowing one to think 'out of the box' and gain experience without taking the risks that the current bill entails.

Yours truly,

C. Schürmann

Carsten Schürmann, Primary Investigator, the research project DemTech, Associate Professor, PhD.