Identifying Building Blocks of Internet Voting: Preliminary Findings

Robert Krimmer[1]

Tallinn University of Technology
Ragnar Nurkse School of Innovation and Governance
Akadeemia tee 3
12618 Tallinn, Estonia
robert.krimmer@ttu.ee

Abstract: In this paper we present preliminary findings of a case study analysing the implementation experience with Internet voting in Austrian academic tests and one election. The project identified a first set of six building blocks which seem important for the conduct of Internet voting, which include legal basis, identification, secrecy, transparency, control, and evaluation.

1 Introduction

Recognizing each other as equal is the central precondition for a society to develop democratic institutions [Dahl1998]. Over time, societies have developed various forms of decision making, which are often also ways that culture is expressed. In one way or another, all democracies use elections to make legitimate decisions. As Kofi Annan [KA2000] once put it: 'Democracy must be more than free elections, [but] it is also true […] that it cannot be less.' As such elections are one expression of the culture and identity of a society; however, they are also processes in continuous evolution that differ from society to society.

An election is a formal process by which members of a society make a choice on a topical question or candidate for a public office. Since the end of the Second World War, many efforts have been undertaken to establish a common understanding of what constitutes a democratic election. The United Nations' first set out standards [UN1966] for the main qualitative factors that an election has to satisfy: holding genuine periodic elections, extending the right to all citizens to stand and to cast a (secret) vote, and allowing free expression of the will of the vote. But these standards say little about procedures, leaving unanswered the questions of how and with which methods elections are to be conducted.

[1] Research for this article was supported in part by Estonian Research Council's institutional grant IUT19-13.

Initially, elections were held in controlled environments using a variety of technologies including vocal communication, show of hands, stones, wax tablets, or fragments of clay. Today paper ballots are most commonly used. With the increasing need to accommodate citizens' mobility, paper ballots are also used to allow for voting in uncontrolled environments, i.e. to allow the voter to make choice either inside or outside of a dedicated polling station, using the postal service to receive and return the ballot.

As soon as electricity became available, the question arose, whether it could be used to allow for electrified and later electronic voting. One of the earliest efforts to develop electronic vote casting machines date back to 1849 when Martin de Brettes developed an early model. Werner von Siemens and Thomas Edison followed with similar proposals All of them were designed for the use by parliamentarians. Despite public interest, none of these inventions were ever actually used [Krim2012].

It took over 100 years for the use of electronic voting machines in polling stations to spread happening in the 1970s in the U.S. [Toka2005] and the Netherlands [Leye2010], and in the late 1990s in Germany [BWGV]. At about the same time, research started to make the visionaries' dreams come closer to reality. It was David Chaum [Chau1982], on the basis of the advances in cryptography by Diffie & Hellman [DH1976] with the use of asymmetric keys as well as ist implementation by Rivest, Shamir & Adleman [RSA1978], who made casting secret votes via the Internet possible for the first time.

It took a little longer for this experiment to reach real elections. When the Internet became available to the public in the 1990s, a transformative process gained momentum. It started by enabling online purchasing (e-commerce), continued by processing government transactions (e-government) and finally also reached democratic procedures, bringing with it remote electronic voting that promised to transform democracy.

Unlike the storm that shocked the traditional business world, developments in election process take much longer, mostly because introducing remote electronic voting involves many more questions than the basic ones of who is able to offer a product cheapest and fastest.

Nevertheless a number of experiments with remote electronic voting via the Internet. The first legally binding elections via the Internet took place in the United States with the Arizona primaries (for an analysis of this trial in 2000 see Solop in [Solo2004]) and in the student parliament elections in Osnabrück/Germany [Stege2000] in early 2000. In Switzerland discussions started in 1998; since 2004 the Swiss have been gaining experience in a step-by-step approach, starting with three pilot cantons Geneva, Neuchâtel, and Zurich [Brau2004], and expanding in recent years to thirteen [Burn2011]. The small Baltic republic of Estonia was the first country in the world to introduce remote electronic voting for all elections in 2005. Since then it has held six nation-wide elections with an electronic remote channel [VVK2014]. Australia experimented in 2007 with remote electronic voting, also investigating how vision-impaired persons can benefit from such a voting channel [AEC2007]. In 2011 and 2013, Norway piloted a remote electronic voting channel in local government elections that allows the possibility for the voter to verify if the vote was cast as intended [MLGR2011, 2013].

Overall, the number of users of electronic voting has increased over the past few years. But the trend has not been uniform, and has spurred intensive discussions amongst election administrators, researchers, vendors, media, observers, and last but not least voters. While the decision whether or not to introduce remote electronic voting remains a question to be answered by responsible decision makers, the implementation of Internet voting presents challenges of its own.

In this paper we present preliminary findings of a project which tries to identify the building blocks of Internet voting. The project deals with the case of Austria, where after several experiments, including two academic tests in 2003 [PKKU2003] and 2004 [PKKU2004], a highly contested Internet voting project was implemented in 2009 [KET2010]. These three elections where examined in detail for the identification of building blocks which seemed important for the conduct of Internet voting.

2 Methodology

The aim of the study is to identify building blocks of Internet voting. Such an approach, to conduct an in-depth study of a contemporary phenomenon using multiple sources of evidence in its real-life context, is the typical application of case-study methodology [Yin2003]. This is an area where traditionally there has been little prior research in the IS field [BGM1987]. For this case study the following sources of information were used for its compilation: (i) project reports of the academic tests and the election, (ii) academic papers, (iii) legal documents, (v) media reports on the issue, (vi) as well as further documents that help understand the case study context and content.

The case study analysis was organized in three phases: (i) define and design; (ii) prepare, collect, and analyze; and (iii) analyze and conclude, following Yin [2003]. For the analysis of the data, a reference framework was used [Krim2012] to identify emerging patterns throughout the implementations [Klug2000].

3 Identifying Building Blocks

The preliminary findings of the project hint that a first six areas have to be paid attention to when designing, building and finally deploying a remote electronic voting channel via the Internet:

1. The adaptation of the legal basis;
2. The selection of technical means to solve the main paradox of unequivocally identifying the eligible voter; and at the same time
3. Ensuring the secrecy of the vote;
4. Evaluating that the software works as required;
5. Giving the election commission control over the process; and
6. Enabling overall transparency for the process.

Figure 1 gives an overview of these topics and in the following these building blocks are described in more detail.

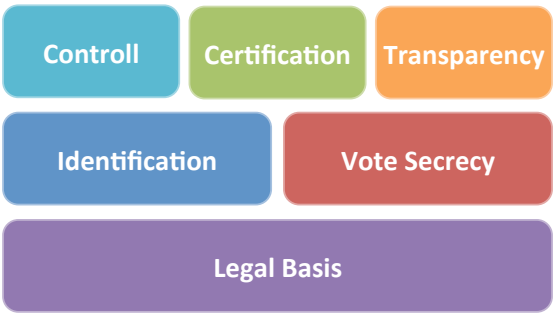

Figure 1: Building Blocks of Internet Voting

3.1 Legal Basis

When designing the legal basis for electronic voting, the first question is whether or not it is in line with international commitments. Here the Venice Commission of the Council of Europe commissioned a study [Grab2004a, Grab2004b] which found general compatibility. In addition, the Council of Europe also passed a recommendation on how electronic voting systems should be designed [CoE2004]. At the third meeting of reviewing the recommendation, it was amended by two documents to reflect recent developments in transparency and certification [CoE2011a, CoE2011b]. Most publications on national legislation regarding remote electronic voting concentrated on whether it is in line with the constitutional requirements of the respective country [Zisk2004; Karp2005]. In the end, project experience showed that most importantly the implementation of the law's principles into an ordinance needs to include technical detail [GoWe2012].

3.2 Identification

The identification of voters is an essential part of the whole voting process, and closely linked to the available online identity management infrastructure in the country where the election is being conducted. Some countries have begun to equip their citizens with smart cards [Maat2004] and in the case of Austria the smart cards are linked to the existing population registers [LHP2002]. For others such solutions were (i) too costly, (ii) delayed due to data protection concerns [RRM2005], or (iii) delayed for a long time due to lack of national certification providers [CH2007]. While in such cases one-time passwords (transaction authorization numbers – TAN) were used, which resulted in high costs for printing and distribution of voting cards for each election [Brau2004]. However the increased level of security came at the price of usability. While TAN are easily used by voters, smart cards can require high level of transaction costs to issue them as well as prove a high barrier to participation which is hard to overcome.

3.3 Vote Secrecy

Ensuring the freedom of the voter to cast a ballot of his/her choice requires that it remain impossible to link a voter and his/her vote, both at the time of casting the vote as well as in the future. Many algorithms have been proposed in the past 30 years, all of which hide either the vote or the voter by cryptographic and/or organizational means. For an overview of different available algorithms see [SP2006; Paul2011].

Most of this research however does not include experience in real-world elections. This can be assumed to be the reason why most algorithms used in practice are of less sophisticated nature than those considered state-of-the-art in research.

The most successful form of supporting free cast of a vote is allowing the voter to cast a vote more than once, while ensuring that only the last vote counts [VG2006]. However, this requires changing legal regulations which in the Austrian case was not possible.

3.4 Control by the Electoral Committee

Traditional voting processes are organized by an election committee. Often election administrators have a legal background and only limited technical experience. They often consult with technically experienced personnel or companies to conduct the electronic voting processes. Still, election committees should remain in full control of the conduct of the election. This becomes in particular challenging when there is need to allow the election commission to start, stop or interrupt the process. Most algorithmic solutions propose no technical means for this and therefore require organizational measures through regulation, such as detailled contractual relations with the vendor helping to implement this control element.

3.5 Certification

In addition to the necessity of overall trust- and transparency-enhancing measures, the correct functioning of the electronic voting software is in doubt if it is not checked before its actual use. Before evaluations can be performed, one has to translate legal requirements into functional and organizational requirements [LSBV2010]. Here, the technical part of the Council of Europe recommendation [CoE2004, CoE2011a/b] has made a fundamental contribution to the development of generally accepted technical requirements. Ahead of such international technical standards that can be used for certification, it was necessary to develop national approach in the case of Austria [ASIT2009]. Re-use of these techniques by others is limited, as they are either designed for specific existing systems, tied to national (electoral) legislation, or too generic [Volk2009].

3.6 Transparency

Paper-based voting processes are easy to understand and to follow. The use of electronic means presents the inherent problem that electronic bits and bytes cannot be seen. This in effect results in a process that requires access to documentation of the actual proceeding of the operation of the electronic voting system, as well as advanced mathematical and technical knowledge to understand the overall logic behind it. While early efforts introduced confirmation numbers that would allow voters to verify that their confirmation number is included in a public bulletin board, recent research proposes the use of end-to-end verifiability approaches [Ryan2009], which would allow the voter to check whether his/her vote was cast as intended, recorded as cast, as well as counted as recorded. The proposals use (mathematical) proofs to allow these checks. Practical experience with end-to-end verifiable systems is limited (only available in Norway and Estonia) and trust and transparency in the conduct of the electronic election remain pre-requisites, but can possibly be enhanced through efforts like this, in particular when considering universal approaches which could support observation efforts [KrVo2006; NVT2013].

4 Summary

The preliminary analysis of this project shows insights in the development process that the field of remote electronic voting has taken. Clearly the experiences with implementing such new election technologies have shown that what once seemed a technical problem became much more. At the beginning the technical solutions for the main problem of verifying the eligibility of voters and keeping their vote secret was at the center of attention. Later more sophisticated algorithms were developed and functionalities like trying to give more control to election commissions were added. However, the experiences showed, that accurate legal regulations are needed, which not only show the interaction with the constitutional legal texts but also on how to give accountability to a remote electronic voting channel through legal means. International standards were a first step, but much more necessary are regulations based on actual experience which show how remote electronic voting channels can be realized and where it is needed in order to avoid problems identified in pilot implementations. Further this practical knowledge also shows that sophisticated algorithms are not always the key to success. Much rather, several key implementations make use of very basic technical means to realize the tasks given by law. One should not forget about the voters. They not only need to use such systems but also need to understand the processes in order to build up trust. It requires trust in the election administration; otherwise suspicion will arise with more technology in an election process.

Last but not least it also shows that remote electronic voting is one of the most challenging IT projects. Not only does the requirement for secrecy of a vote rule out many approaches towards IT-security in the Internet, but also elections themselves are special projects: they have a fixed date when they have to take place – if the system is ready or not.

References

[AEC2007] Australian Election Commission: *Federal Electronic Voting Trials*. Canberra 2007. Available from http://www.aec.gov.au/Voting/electronic-voting.htm, retrieved 03-11-2013.

[ASIT2009] A-SIT: *Bescheinigungen nach § 34 Abs. 6 HSG 1998*. Available from http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_hsg/index.php, retrieved 16-04-2014.

[Brau2004] Braun, Nadja: E-Voting: Switzerland's Projects and their Legal Framework. Paper read at ESF TED Workshop on Electronic Voting in Europe, GI LNI, Bonn 2004.

[BGM1987] Benbasat, I., Goldstein, D. K., & Mead, M.: The Case Research Strategy in Studies of Information Systems. *MIS Quarterly, 11*(3), 369-386, 1987.

[Burn2011] Burnand, Frédéric. 2011. *E-Voting 2011 auf Sparflamme*. Swissinfo 2011, retrieved on 11-08-2013.

[BWGV1975] *Bundeswahlgeräteverordnung of 3 September 1975 (BGBl. I p. 2459), last changed on 20 April 1999 (BGBl. I p. 749)*. Available from http://www.gesetze-im-internet.de/bundesrecht/bwahlgv/gesamt.pdf, retrieved 11-02-2014.

[CH2007] Schweizer Bundesrat: *Anfrage 07.1031 zu 'Digitale Signatur',* 2007. Available from http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20071031 retrieved on 03-05-2014.

[Chau1982] Chaum, David. Blind Signatures for Untraceable Payments. Paper read at Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara 1982.

[CoE2004] Council of Europe: *Legal, operational and technical standards for e-voting. Recommundation Rec(2004)11 and explanatory memorandum*. Council of Europe, Strassbourg 2004.

[CoE2011a] Council of Europe: *Guidelines of the Committee of Ministers of the CoE on Certification of E-voting Systems (2011)*. Council of Europe, Strassbourg 2011. Available from http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Evoting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf, retrieved on 20-02-2012.

[CoE2011b] Council of Europe: *Guidelines of the Committee of Ministers of the CoE on Transparency of E-enabled Elections (2011)*. Council of Europe, Strassbourg 2011. Available from http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf, retrieved on 20-02-2012.

[Dahl1998] Dahl, Robert A.: *On Democracy*. New Haven, London: Yale University 1998.

[DH1976] Diffie, Whitfield, Hellman, Martin E.: New Directions in Cryptography. *IEEE Transactions on Information Theory* 1976, 22 (6): 644–654.

[Grab2004a] Grabenwarter, Christoph: Briefwahl und E-Voting. *Journal für Rechtspolitik* 12 (2): 70-77, 2004.

[Grab2004b] Grabenwarter, Christoph: *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, 2004*. Available from http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.pdf, retrieved on 12-12-2008.

[GoWe2012] Goby, Barbara, Weichsel, Herbert: Das E-Voting-Erkenntnis des VfGH: gesetzwidrige Ausgestaltung der ÖH-Wahlordnung. Zeitschrift für Hochschulrecht, Hochschulmanagement und Hochschulpolitik (Zfhr) 2012(11)3: 118-125.

[KA2000] Annan, Kofi: *UN Secretary General Kofi Annan's Closing Remarks to the Ministerial on June 27th 2000*. Available from http://www.demcoalition.org/pdf/un_secertary_gen_kofi_annan.pdf, retrieved 02-02-2014.

[Karp2005] Karpen, Ulrich: Elektronische Wahlen? Nomos Verlag, Baden-Baden 2005.

[KET2010] Krimmer, Robert, Ehringfeld, Andreas, & Traxl, Markus : Evaluierungsbericht: E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009. Bundesministerium für Wissenschaft und Forschung (BMWF), Vienna 2010.

[Klug2000] Kluge, Susanne: Empirically Grounded Construction of Types and Typologies in Qualitative Social Research. *Forum Qualitative Sozialforschung,* 1(1), Art. 14, 2000.

[Krim2012] Krimmer, Robert: The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy. Dissertation, Tallinn University of Technology, Tallinn 2012, Available from http://digi.lib.ttu.ee/i/?798, retrieved 02-06-2014.

[KrVo2006] Krimmer, Robert, Volkamer, Melanie: Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Electronic Government EGOV, Trauner Verlag, 43-52, Linz 2006.

[NVT2013] OSCE/ODIHR: Handbook for the Observation of New Voting Technologies, Warsaw, 2013.

[Leye2010] Leyenaar, Monique: *Electronic Voting: A Case Study from the Netherlands. Presentation at CiO Seminar on 'Present State, and Future Prospects of the Application of Electronic Voting in the OSCE Participating States' in Vienna on 16 and 17 September 2010*. Available from http://www.osce.org/cio/71355, retrieved on 02-04-2014.

[LHP2002] Leitold, Herbert, Hollosi, Arno & Posch, Reinhard: Security architecture of the Austrian citizen card concept, Vienna 2002.

[LSBV2010] Langer, Lucie, Schmidt, Axel, Buchmann, Johannes, Volkamer, Melanie: A taxonomy refining the security requirements for electronic voting: analyzing helios as a proof of concept. ARES, IEEE 2010.

[Maat2004] Maaten, Epp: Towards Remote E-Voting: Estonian Case. In: TED Workshop on Electronic Voting in Europe, GI LNI, Bonn 2004.

[MLGR2011] Ministry of Local Government and Regional Development: *The e-vote project,* Oslo 2011. Available from http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658, retrieved on 11-03-2012.

[MLGR2013] Ministry of Local Government and Regional Development: *The e-vote 2013 project*, Oslo 2013. Available from http://www.regjeringen.no/nb/dep/kmd/kampanjer/valg/nytt-om-valg/2014/Rapport-fra-Cartersenteret-om-forsok-med-internettstemmegivning.html?id=756400, retrieved on 05-05-2014.

[Paul2011] Paulsen, Christian: *Sicherheit von Internetwahlen*. Hamburg: BoD, Books on Demand, 2011.

[PKKU2003] Prosser, A., Kofler, R., Krimmer, R., & Unger, M. K.: Die erste Internet-Wahl Österreichs: Ein Erfahrungsbericht von e-Voting.at. The first Internet-Election in Austria: The Findings by e-Voting.at, Institute of Information Processing and Information Management, Vienna 2003.

[PKKU2004] Prosser, A., Kofler, R., Krimmer, R., & Unger, M. K.: E-Voting Election Test to the Austrian Federal Presidency Election 2004. Institute of Information Processing and Information Management, Vienna 2004.

[RRM2005] Reichl, H., A. Roßnagel, and G. Müller. 2005. *Digitaler Personalausweis: Eine Machbarkeitsstudie*: Duv.

[RSA1978] Rivest, Ronald L., Adi Shamir, and Leonard M. Adleman.. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* 21 (2):120-126, 1978.

[Ryan2009] Ryan, Peter Y.A., David Bismark, James Heather, Steven Schneider, and Zhe Xia: Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security* 4 (4), 2009.

[Solo2004] Solop, Frederic I.: Electronic Voting in the United States: At the Leading Edge or Lagging Behind? In *Electronic Voting and Democracy: A Comparative Analysis*, edited by N. Kersting and H. Baldersheim. London: Palgrave, 2004.

[SP2006] Sampigethaya, Krishna, and Radha Poovendra. A framework and taxonomy for comparison of electronic voting schemes. *Computers & Security* 25 (2):137-153, 2006.

[Stege2000] Stegers, Fiete: Virtuelle Wahl: Ab 0:00 Uhr kann geklickt werden. *SPIEGEL Online,* 2000.

[Toka2005] Tokaji, Dan P.: The Paperless Chase: Electronic Voting and Democratic Values. *Fordham Law Review* 57, 2005.

[UN1966] United Nations: *International Covenant on Civil and Political Rights* 1966. Available from http://www2.ohchr.org/english/law/ccpr.htm, retrieved on 20-04-2013.

[VG2006] Volkamer, M., & Grimm, R.: Multiple Casts in Online Voting: Analyzing Chances. In R. Krimmer (Ed.), *Electronic Voting 2006* (Vol. 86, pp. 97-106). Bregenz: GI, 2006.

[Volk2009] Volkamer, Melanie: *Evaluation of electronic voting: requirements and evaluation procedures to support responsible election authorities*. Vol. 30. Berlin: Springer LNBIP, 2009.

[VVK2014] Vabariigi Valimiskomisjon: *Internet Voting - Voting Methods in Estonia - Estonian National Electoral Committee* 2014. Available from http://www.vvk.ee/voting-methods-in-estonia/engindex, visited 06-05-2014.

[Yin2003] Yin, R. K.: *Case Study Research. Design and Methods* (3 ed.). Thousand Oaks, London, New Delhi, Sage Publications, 2003.

[Zisk2004] Ziska, Bernd: *Verfassungsrechtliche Rahmenbedingungen für E-Voting* 2004. Available from http://www.rechtsprobleme.at/doks/ziska-e-voting.pdf, retrieved 03-02-2014.