Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed

Dr. Nadja Braun, Daniel Brändli[1]

Swiss Federal Chancellery
Political Rights Section
Bundeshaus West
3003 Bern, Switzerland
{nadja.braun | daniel.braendli}@bk.admin.ch

Abstract: In Switzerland the Federal Chancellery in cooperation with three cantons has carried out since 2003 a number of pilot trials with the aim of evaluating the feasibility of remote e-voting. Based on a legal basis respecting the council of europe's recommendations five pilot trials have been authorized at national referendums in 2004 and 2005. The pilot trials were evaluated for a number of different aspects, including the potential of e-voting to increase voter turnout, the security risks and its cost-effectiveness. The evaluation has shown that e-voting is feasible in Switzerland. The decision on how to proceed now rests with the Federal Council and the Parliament.

1 Introduction

At the request of the Federal Council and the Parliament and in cooperation with the cantons of Geneva, Neuenburg and Zürich, the Federal Chancellery has carried out a number of pilot trials over the last five years with the aim of evaluating the feasibility of e-voting in Switzerland[2].

In Switzerland, the terms "e-voting" or "vote électronique" are understood to refer primarily to so-called "remote e-voting"[3] – the casting of ones vote via the Internet, by SMS or by other electronic data transmission media. In direct-democratic Switzerland, e-voting is meant to include not only the casting of votes in elections and referendums, but ultimately also the giving of 'electronic signatures' for initiatives, referendums and proposals for candidates for membership of the National Council.

[1] The opinions expressed in this paper do not represent any official statement.
[2] The first milestone within this pilot phase was established by the report [B02] of 09.01.2002.
[3] The same procedure i.e. the casting of a vote elsewhere than in a polling station, is also referred to as "remote internet voting" or "remote voting by electronic means (RVEM)".

The pilot studies of recent years were restricted to voting in elections and referendums, as electronic signature might possibly require an officially recognized digital signature to enable positive identification of the signatory. To date, however, suitably approved digital signatures have not been sufficiently widely used in Switzerland[4].

The following two chapters give, firstly, an outline of the pilot studies and, secondly, a presentation of the major results of the evaluation[5].

2 Pilot Trials

2.1 Preconditions for pilot trials in Switzerland

The legal basis for the legally binding use of e-voting was created on 21st June 2002 within the context of a partial revision of the federal law of 17th December 1976 on political rights (BPR, SR 161.1)[6]. This legislation allows the Federal Council, in consultation with interested cantons and municipalities, to authorize pilot trials which are limited as to place, time and subject matter. A special requirement is that strict control of eligibility to vote, the secrecy of voting and the recording of all votes must be guaranteed. The trials must not be open to misuse. The rules of implementation (Art. 271-27q of the ordinance of 24th May 1978 on political rights, VPR, SR 161.11) set out the preconditions which must be fulfilled before the Federal Council can approve pilot trials of e-voting[7]. The rules of implementation likewise place special emphasis on ensuring security, protecting the secrecy of the vote, checking voter eligibility and preventing the casting of multiple votes.

In implementing the pilot projects, attention was also paid to the *recommendations of the Council of Europe*, in addition to the Swiss legal provisions [C04]. The core message of the CoE recommendation is that e-voting must respect all the principles of democratic voting, and must be as reliable and secure as non-electronic voting. In the recommendation, special emphasis is placed on there being a high level of security, on the characterization of e-voting as an additional form of voting and on the neutrality of the technology. These keynotes are fully endorsed in Switzerland.

---

[4] As of 1st January 2005 (Federal Law on electronic signature, ZertES, SR 943.03), the legal basis for binding transactions is in place.

[5] Publication of the evaluation in the form of a report of the Federal Council for the attention of the Parliament is planned for summer 2006.

[6] Art. 5 § 3, Clause 2, Art. 8*a,* Art. 12 § 3, Art. 38 § 5 and Art. 49 § 3 BPR plus Art. 1 § 1, Clause 2 Federal Law of 19.12.1975 on the political rights of Swiss living abroad (BPRAS, SR *161.5*).

[7] Cf. also the Federal Council directives to the cantons in the circular of 20.09.2002 regarding the application of these rules of implementation (Federal Gazette *2002* 6603-6609).

The *authorization of pilot projects* relating to national ballots is the responsibility of the Federal Council. In order to lessen risks, the Federal Council can limit the scope of the pilot project in respect of place, time and subject-matter. The conditions detailed in the Swiss ordinance on political rights must be observed cumulatively, unless the directive explicitly states otherwise. Any planned use of e-voting at the national level must be authorized in advance by the Federal Council. The cantons had to include detailed technical documentation in their requests for such authorization. Before the first trial, the three pilot systems were checked by professional outside companies engaged by the Federal Chancellery, to ensure that the systems were secure and hacker-proof.

An extremely important precondition for e-voting is the *standardization of the registers of voters*, which are normally kept by the communes. In developing their systems, the pilot cantons were able to refer in part to cantonal regulations, and in part to an agreed standard developed by the eCH association [E04, cf. also B05]. Individual cantonal or communal identifiers were used for personal identification in each case. Due to the lack of unambiguous numerical identification, no cross-cantonal exchange of data between the different voter registers was possible.

In order to preserve the secrecy of the vote, all personal data (name, address, date of birth etc.) were anonymized after the individual voting permits had been generated. The unique voting permit number could then be used to check (against the voting register) whether an individual had already voted, thus ruling out the possibility of multiple voting.

2.2 Pilot trials at national referendums in 2004 and 2005

In 2004 and 2005, a total of five e-voting pilot trials were carried out in the cantons of Geneva, Neuenburg and Zürich on the occasion of national referendums (cf. Table 1). Without exception, all five trials proceeded successfully and without mishap. Prior to the first official use, each of the three electronic voting systems was subjected to an extensive test run overseen by independent experts.

Date	Canton/Communes	Extent of trial	Number of electronic votes (share of all votes as %)
26.09.2004	Geneva: Anières, Carouge, Cologny, Meyrin	22.137 eligible voters	2.723 (21,8%)
28.11.2004	Geneva: Anières, Carouge, Cologny, Collonge-Bellerive, Meyrin, Onex, Vandoeuvres, Versoix	41.431 eligible voters	3.755 (22,4%)
25.09.2005	Neuenburg	1.732 eligible voters*	1.178 (68,0%)
27.11.2005	Zürich: Bertschikon, Bülach, Schlieren	16.726 eligible voters	1.154 (22,1%) (of which 243 by text message)
27.11.2005	Neuenburg	2.469 eligible voters*	1.345 (55,1%)

Table 1: Pilot trials carried out at national referendums

3 Evaluation of the Pilot Trials

The pilot trials were evaluated for a number of different aspects, including the potential of e-voting to increase voter turnout (3.1), the security risks (3.2) and its cost-effectiveness (3.3). These three aspects of the evaluation are summarized below.

3.1 Benefits to and effects on direct democracy

An important argument which is repeatedly raised in favor of e-voting is its potential to increase voter turnout. It is argued that certain groups – young people, on account of their increased use of the Internet; older people, because of their limited mobility; Swiss citizens living abroad, because of lengthy international mail delivery times; blind or partially-sighted persons – would make more frequent use of their voting rights if e-voting were in place.

* Users of the official "Guichet unique" electronic office

In 2004, the Federal Chancellery commissioned the research institute gfs.bern to undertake an empirical study on the potential effect of e-voting on voters across Switzerland [G05][8]. Two-thirds of the eligible voters currently have access to the Internet. The percentage is even higher for younger voters and those who are better educated. The survey revealed that 54% of those asked could imagine using e-voting. The most common reason given for readiness to use e-voting was its user-friendliness. Fears about data security were expressed most strongly by people who will probably not use e-voting.

"Assuming that you were already able to vote electronically, is it highly likely, very likely, fairly unlikely or highly unlikely that you would cast your vote electronically?"

© gfs.bern, Electronic Vote, 2003/2004 (N=4.018)

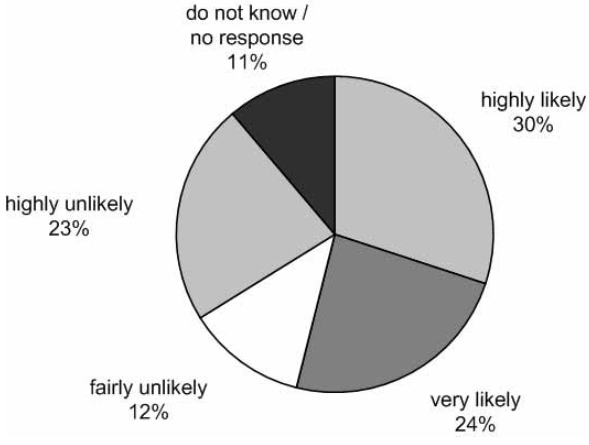

Figure 1: The potential effect of e-voting on Swiss voters

The use of e-voting was not only dependent on a person having available access to the Internet, but also on whether those asked make regular use of this medium for their professional and/or private affairs. Well-educated young males living in urban areas showed the greatest level of interest in e-voting. But the potential is greater than 50% even in the 40-65 age-group of voters and for people from the middle classes.

[8] The studies are based on a supplement to four VOX analyses (ex-post analyses of national referendums) from 2003 and 2004. A total of 4,018 Swiss citizens entitled to vote in national elections and referendums were asked for their opinion .

According to the study, e-voting is particularly attractive to people who stated that they did not vote in referendums either “at all” or “only sometimes”. This finding could be an indication either for a replacement by other forms of voting or for a potential increase in turnout. The potential is greater, the higher the level of interest in political issues and in active participation in political debate. Nonetheless, the study comes to the conclusion that e-voting would have no effect on the balance of power between the different political camps.

The Federal Council had as early as 2002 expressed some skepticism towards the estimates of certain experts of a possible increase in voter turnout [B02, p. 654f.]. Even after the completion of the pilot trials and their academic evaluation, it would be right to preserve such skepticism. The study cited here resulted in an unexpectedly high assessment of the potential of e-voting. As with the indications of a potential increase in voter turnout in all three pilot cantons, these findings would have to be corroborated by multiple trials in all three cantons.

3.2 Risks and security measures

Academics and scientists have grappled intensively with the risks of electronic voting, as e-voting has to meet the very highest security requirements [cf. e.g. A04; J04; M02; O02; R02; S04]. The emphasis has been on the dangers of technical manipulation, as well as on the general threat to a democracy posed by technical risks. Most fears concern ways of ensuring the secrecy of the vote [Br05; Mu02]. A major risk concerns the susceptibility to so-called ‘spoofing’. Voters could give their access data and their vote to a bogus Internet site without realizing it. Using the hacked information, unauthorized persons could subsequently submit their own political preferences to the official referendum server. A similar form of attack might consist in hacking unnoticed into the data flow between the official referendum server and the voter and changing the information so as to affect the vote (man-in-the-middle attack). Within company networks (Intranets), system administrators could try to spy on employees as they vote or seek to influence the vote in some way. It might be possible, finally, to use the buffer store of a voting machine to find out how an individual had voted.

Secure e-voting is feasible: the pilot trials have demonstrated this. But ongoing security depends on being able to maintain control of continually changing threats and risks. The necessary security measures cannot be developed and put in place once and for all. Just as the potential sources of danger (hackers, viruses, Trojan Horses etc.) are continually changing, so must the security measures be continually adapted and improved.

Many suitable security measures were tested as part of the pilot trials. It was important to rule out any risks of systematic misuse. As with conventional forms of voting (ballot-box or postal votes), the possibility that with e-voting, too, individual votes may be falsified, blocked or altered, or that a person’s voting behavior might be observed or deduced, can probably never be completely excluded. Everything must, however, be done to prevent the occurrence of any systematic irregularities or abuses [Br05].

The security measures taken during the pilot trials in the cantons of Geneva, Neuenburg and Zürich succeeded in foiling all registered attacks. Independent experts emphasized the efficiency of the security measures undertaken and credited each of the three cantonal systems with an excellent security architecture.

Postal voting is often used as a comparison to assess the risks of e-voting. Parliament demanded of e-voting a similar level of security to that of postal voting. The required benchmark was exceeded in the pilot trials. The following table[9] summarizes the requirements and the measures undertaken deriving from the legal and security considerations and compares them with analogous requirements and measures in respect of postal voting.

E-voting requirements	**Analogy(-ies) with postal voting**	**Measures taken during the pilot trials**
Positive identification: A person taking part in a referendum or an election must be positively identified as the person he/she claims to be.	Eligible voters give a handwritten signature on the voting permit or on the reply envelope. Voting slips are also filled out by hand.	• Individual and secret access code • Validation by indicating date of birth and/or place of birth • Use of digital signatures imaginable (in the future) • Other security queries such as the self-documenting AHV number would, however, be questionable (protection of secrecy of vote)
Authenticity of the e-voting system Voters must know for certain that their vote will be placed in the designated ballot-box and that it will be included in the count.	Postal votes are delivered by the postal service, handed in in person at the local authority office or posted in the community postbox.	• The SSL can be checked by the voter using his/her fingerprint • The authenticity of the server can be checked by means of a response code and/or pictorial symbols.
Single vote: A voter may cast only one vote.	The voting permit is issued only once and according to name. In postal voting, the original voting permit must be sent back in the return envelope. Repeat voting is thus impossible.	• Immediate cancellation of authorization to vote in the voter database, as soon as a vote (electronic or postal) has been registered • Clear signs on the voting envelope (e.g. an unbroken seal over the secret access code) show whether a citizen could have already voted electronically.
Preservation of voting secrecy/data protection: The voting intention of the voter must remain secret.	The completed voting slips reach the municipal offices in a separate sealed envelope. After verifying the signatures, the voting permit and the voting slip must be separated.	• Separate storage of personal data and voter-specific details on separate systems • Constant shuffling of the electronic ballot-box by means of a random generator. This makes it impossible, for example, to deduce the name of a person based on the sequence of votes cast.
Provisions against risks from 'Acts of God': Interference with voting from storms,	Analogous risks also exist for municipal offices/town halls, the special communal postbox, polling stations, postal sorting offices and	• Use of several redundant servers • Housing of servers in high-security buildings (entry control, fire protection, back-up power supply)

[9] The information in the table refers only to the solutions tested so far in Switzerland in the context of the pilot trials and does not claim to be exhaustive. Cf. also [V04, p. 57f.]

E-voting requirements	Analogy(-ies) with postal voting	Measures taken during the pilot trials
power failures, earthquakes etc.	postal delivery services.	
Reproducibility and provability: It must be possible to recount votes when the tally of votes is very close or in the event of an appeal.	Paper votes can always be recounted. Different people can be asked to undertake the recount. If they wish, citizens can be present at the recount (transparency).	• Preparation of conventional and electronic records, which are countersigned by the relevant authorities when the votes are counted • Preparation of a separate data storage medium (CD-ROM containing the data from the electronic ballot-box and all Log files) • The interests of voters are secured by special inspectors selected by the political parties
Trust: The entire procedure must be trustworthy and able to be checked.	Postal voting enjoys a wide measure of trust among the general public.	• Involvement of inspectors in all sensitive processes • Independent checking of the source codes, Open Source method • Disclosure of proprietary applications
Defence against external attack: a) Enduser devices (personal computers, mobile phones): possible interception and altering of the votes e.g. by the use of "Trojan horses".	Voting material is stolen from the eligible voter by removal from the letter-box after delivery. Systematic misuse cannot be excluded if many voters do not vote and do not tear up their voting papers before disposing of them.	• Multiple protection through Firewalls • Code-voting procedure (Zürich SMS, online transmission of the vote as a numerical code) • Use of state-of-the-art virus protection software
b) "Transport" of the vote from the user to the server: possible interception and alteration of the votes (man-in-the-middle attack).	Voting envelopes could fall into the wrong hands or be destroyed if they are removed from the communal postbox or if a postal sack is stolen or lost in transit.	• Encryption of the vote (SSL) • Details of vote transmitted graphically and not as text • All online packets are tested for their integrity using horizontal checksums
c) Platform (core element of an e-voting system): e.g. "Denial-of-service attacks"	Arson attack on the communal postbox. Or the delivery of the votes is impeded or prevented by a breakdown of the postal service. The risk is small, but increases with increasing centralization of postal services.	• Use of several redundant servers • Collaboration with various providers (DNS hacking)

Table 2: E-voting and postal voting: comparison of requirements and security measures

3.3 Cost-effectiveness of e-voting

Despite the need referred to above for e-voting to satisfy the highest security requirements, it must also be so simple to use that it can be used by every eligible voter. The challenge therefore lies in providing the greatest possible degree of security at an affordable price. At the same time, user-friendliness must not be excessively restricted. Postal voting can provide comparisons in this area too.

In its 2002 report, the Federal Council estimated the cost of a nationwide introduction of e-voting, including running costs over a 10-year period, at 400-620 million Swiss francs [B02, p. 685f.]. This summary estimate was reviewed using the data from the pilot trials. The Federal Chancellery tallied the total costs of the pilot projects at the end of 2005. There were also specific cantonal costs which were not borne by the Federal Chancellery (e.g. the cost of extra jobs and staff).

The financial cost for the development and operation of an e-voting system for both elections and referendums can amount to 15 million Swiss francs. The sum includes operating and maintenance costs for ten years, estimated staff and service costs and the amortization of the development costs. Such a system is scaled for a very large canton or for shared operation by several smaller cantons. If we assume that 1 million voters can use the system, the cost per electronic vote would be less than half a Swiss franc.

Assuming that several cantons operate an e-voting system together, and that those processes which are common to all forms of referendum (such as, for example, the printing of the voting permits, the creation of the voting register, the checking of voting rights etc.) feed into a cantonal or supra-cantonal election and referendum system, the implementation of e-voting would be more cost-effective than postal voting.

4 Conclusions

The pilot trials carried out at communal, cantonal and national levels have shown that e-voting is feasible in Switzerland. The pilot systems and the know-how gained by the pilot cantons is available to other interested cantons for the most part free of charge. The pilot cantons and some other cantons are interested in the progressive extension of the pilot trials to encompass the whole canton, and can also imagine extending the system to cover elections as well, if need be. This would require them to follow strategic guidelines laid out by the Federation, as well as federal assistance in the necessary adaptation of the existing legal provisions.

E-voting is a complex system involving many people at several different levels. A step-by-step approach makes it possible to gather experience and apply it to the improvement of electronic voting. Switzerland has approached the subject from the start at a cautious pace. Once the pilot phase was concluded, it was therefore possible to undertake a thorough evaluation of the various developments in the cantons and to point to a possible way forward. It is now for the political sphere to make the decisions as to how to approach the progressive implementation of an e-voting system. A cautious approach is also necessary in order to minimize risks. E-voting has only a chance of being introduced if all those involved – voters, politicians and authorities – have a lasting acceptance of and trust in the new procedures.

The decision on how to proceed now rests with the Federal Council and the Parliament.

References

[A04] Alvarez, R. Michael/Hall, Thad E.: Point, click and vote, Washington 2004.

[B02] Bericht über den Vote électronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte vom 9. Januar 2002 (report of 09.01.2002 on the Opportunities, Risks and Feasibility of the Electronic Exercise of Political Rights), Bundesblatt 2002, S. 645-700 (BBl 2002 645). Available at: www.admin.ch/ch/d/ff/2002/645.pdf.

[B05] Bundesamt für Statistik: Die Harmonisierung amtlicher Personenregister, kantonale und kommunale Einwohnerregister, Amtlicher Katalog der Merkmale (The standardization of official registers of persons, cantonal and communal registers of residents, Official Catalog of Criteria), Neuchâtel 2005. Available at: http://www.bfs.admin.ch/bfs/portal/de/index/infothek/erhebungen__quellen/statistik_und_register/registerharmonisierung/publikationen.Document.65357.html.

[Br05] Braun, Nadja: Stimmgeheimnis (Secrey of the vote), Diss. Bern 2005.

[C04] Council of Europe: Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies. Available at: http://www.coe.int/t/e/integrated_projects/democracy.

[E04] eCH-Standard "0027:Meldeprozesse" (Reporting processes), as of 29.10.2004. Available at: http://www.unisg.ch/org/idt/echweb.nsf/0/D38E4752D42D358AC1256F3C002F6B0A?OpenDocument&lang=de.

[G05] Research institute gfs.bern: "Das Potenzial der elektronischen Stimmabgabe" (The potential of e-voting), study commissioned by the Federal Chancellery, Bern 2005.

[J04] Jefferson, David/Rubin, Aviel D./Simons, Barbara/Wagner, David: Analyzing Internet Voting Security, Communications of the ACM, 47, Nr. 10, 2004, S. 59-64.

[M02] Mitchison, Neil: Protection against "internal" attacks on e-voting systems, in: Muralt Müller, Hanna/Auer, Andreas/Koller, Thomas (eds.): E-Voting. Tagung 2002 für Informatik und Recht, Bern 2003, S. 255-266 German and French only).

[Mu02] Muralt Müller, Hanna und Koller Thomas (eds.), E-Voting, Tagung 2002 für Informatikrecht, Bern 2002.

[O02] Oppliger, Rolf: E-Voting sicherheitstechnisch betrachtet, digma, 4, 2002, S. 184-188.

[R02] Rubin, Aviel D.: Security Considerations for Remote Electronic Voting, Communications of the ACM, 45, 12, 2002, S. 39-44.

[S04] Schryen, Guido: How Security Problems Can Compromise Remote Internet Voting Systems, in: Prosser, Alexander/Krimmer, Robert (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society, Bonn 2004, S. 121-131.

[V04] Der Vote électronique in der Pilotphase, Zwischenbericht der Bundeskanzlei vom 18. August 2004 (E-Voting in the Pilot Phase, interim report of the Federal Chancellery of 18.08.2004). Available at: http://www.admin.ch/ch/d/egov/ve/dokumente/Zwischenbericht.pdf).