

The Secure and Easy Internet Voting

Giampiero E.G. Beroggi
Statistical Office, Canton Zurich

A Swiss e-voting system, operational since December 2004, is based on a service-oriented architecture that lets voters use Internet or mobile phones to cast votes. Two-step encryption and redundant storage systems keep votes authentic and confidential.

Although modern societies rely heavily on information and communication technology for business, work, and leisure time activities, they have thus far seemed hesitant to use ICT for democratic decision-making activities such as voting. Meanwhile, the lost and uncounted votes associated with current paper ballots could very well be contributing to biased political decisions.¹

One reason for the delay in implementing more technologically sophisticated voting methods is the computer science community's almost unanimous wariness of Internet-based elections.² Many governments have simply dismissed e-voting as too risky. Others are not fully aware of e-voting's strong advantages over paper ballots: reliable and secure vote casting, precise vote counting, the option to conduct voting in a centralized and decentralized manner, and the rapid availability of results.

Fortunately, in light of these strong advantages, more countries are beginning to consider e-voting systems,³ but most efforts are still in the conceptual or testing stage. In contrast, three cantons in Switzerland—Zurich, Geneva, and Neuchatel—are already using an e-voting system. The Zurich e-voting system (<https://evoting.zh.ch>), which has been in operation since December 2004, features a modular and service-oriented architecture that lets voters cast their votes through a range of digital media, including computers and mobile telephones (currently) and interactive TV and personal digital assistants (planned).

The system easily integrates into existing software solutions without loss of security and accommodates

either centralized or decentralized operation. Both national and local authorities have embraced the system, particularly its smooth integration with traditional ballot-box voting. Offering both e-voting and paper ballots means that all citizens, regardless of their technology awareness, can vote, and there is no fear of a digital divide among the population. Zurich Minister of the Interior Markus Nottter pronounced the system a “milestone in Swiss democracy [that] opens the ballot to today's information society.”

The “Chronology of the Zurich E-Voting System” sidebar describes key points in developing and implementing the e-voting system. Annual operational costs are \$400,000, which translates to approximately \$0.50 per e-vote. Since the testing phase concluded in April 2006, three communities in Canton Zurich have started using the system. More would like to use it, but the Swiss government has mandated that only 10 percent of the electorate can use e-voting. As soon as the government lifts that restriction, however, all 171 Canton Zurich communities could begin using the system, thanks to the scalability of its service-oriented structure.

HOW THE SYSTEM WORKS

The Zurich e-voting system covers national votes on referenda, votes on citizen initiatives with counter referendum and contingency plans, majority elections, and proportional elections with predefined party lists.

Figure 1 illustrates the e-voting process. Six weeks before e-voting day, communities within Canton Zurich enter in the electronic ballot box the names of citizens

eligible to vote electronically. The electronic ballot box opens two weeks later. To vote, citizens use a special password that Canton Zurich's Statistical Office has mailed to them as part of their voting forms. E-voting then takes place during the next four weeks.

At present, voters can choose between using the Internet and mobile phones to cast their e-votes; other digital alternatives, such as interactive TV and personal digital assistant/Wireless Access Protocol (PDA/WAP) are technologically feasible but not yet active.

Voting process

To vote through the Internet, voters log onto the e-voting website using their identification numbers and follow the site's instructions for vote casting. Figure 2 gives a sample screen from the simulation software. After casting their votes, voters enter a personal identification number (PIN) and compare a security symbol with the one they received in the mail. If the two match, the system accepts the vote.

Two-step encryption protects voter confidentiality. The voter's client computer first encrypts the votes and identification and authentication characteristics, and the e-voting system then checks the incoming votes for their structure and integrity before once again encrypting them. Two redundant subsystems then store the cast votes in a database.

To vote through a mobile phone, voters enter codes to a dedicated phone number using the short message system (SMS). Citizens enter codes for personal identification (g3387y55, for example), the name of the referendum (such as sg1), and the actual yes or no vote (er2 for yes, for example). The SMS message for a user voting yes on referendum sg1 would thus be g3387y55 sg1 er2. The system replies by asking the voter to enter a PIN (separate from the identification access code) and birth date (such as 14031968 for 14 March 1968) in a second SMS message. The citizen receives then a confirmation that the e-vote was entered in the e-voting ballot box.

On voting day, the communities enter the results from the regular ballot box into the vote registration software. As soon as the regular voting ballot box is closed, the e-voting system transfers the e-votes to the computer system that handles the regular votes. An overview of the total results—regular votes and e-votes—is available immediately.

Vote transmission

Because the e-voting system is based on the IT Infrastructure Library, it can accommodate a range of formats—the Extensible Markup Language (XML), the Electronic Markup Language (EML), open database connectivity, the comma-separated value format, and the Simple Object Access Protocol (SOAP)—as well as direct database access. To meet a Swiss government requirement, all formats are convertible to EML for

Chronology of the Zurich E-Voting System

With approximately 1.2 million people, Zurich has the largest population of the 26 Swiss cantons. The Statistical Office of the Canton Zurich (www.statistik.zh.ch), which belongs to the Ministry of Justice and Interior, is responsible for planning and conducting federal and local elections and referenda. As part of its responsibility, the office must provide the technological means for citizens and local authorities to conduct and participate in elections and referenda.

In 2001, the office introduced a fully computerized election and referendum system that connected all 171 communities within the canton, allowing real-time progress monitoring and community assistance on voting days. The e-voting pilot project began in 2003 and successfully completed in spring 2006. The total project cost was \$3.7 million—\$1.9 million for planning and \$1.8 million for implementation.

- **February 1998:** Swiss government defines as part of its ICT strategy the need to test the use of ICT for democratic decision-making processes.
- **August 2000:** Swiss government mandates Federal Chancellery to study the feasibility of e-voting.
- **June 2002:** Swiss Parliament creates legal basis for e-voting pilot study.
- **February 2002:** Federal Chancellery signs contract with Ministry of the Interior of Canton Zurich to participate in the e-voting pilot study.
- **October 2003:** Unisys wins the bid to design the Zurich e-voting system and starts development.
- **December 2004:** First e-voting in Canton Zurich through Internet and mobile phone to elect 70 student board members at the University of Zurich. Voting participation was 93 percent; of the 1,767 people participating in the election, 1,582 used the Internet and 205 used mobile phones. Only one person used the traditional ballot box.
- **October 2005:** First e-voting election in the city of Bulach with 37 percent participating in e-voting.
- **November 2005:** First e-voting for federal and regional offices in three communities. E-voting participation was 37 percent.
- **April 2006:** First e-voting through Internet and mobile phone for proportional election system. E-voting participation was 20 percent.
- **July 2006:** End of pilot project and start of e-voting for any upcoming elections and referenda. Currently, Canton Zurich is waiting for the government to lift its restriction so that all communities can use e-voting.

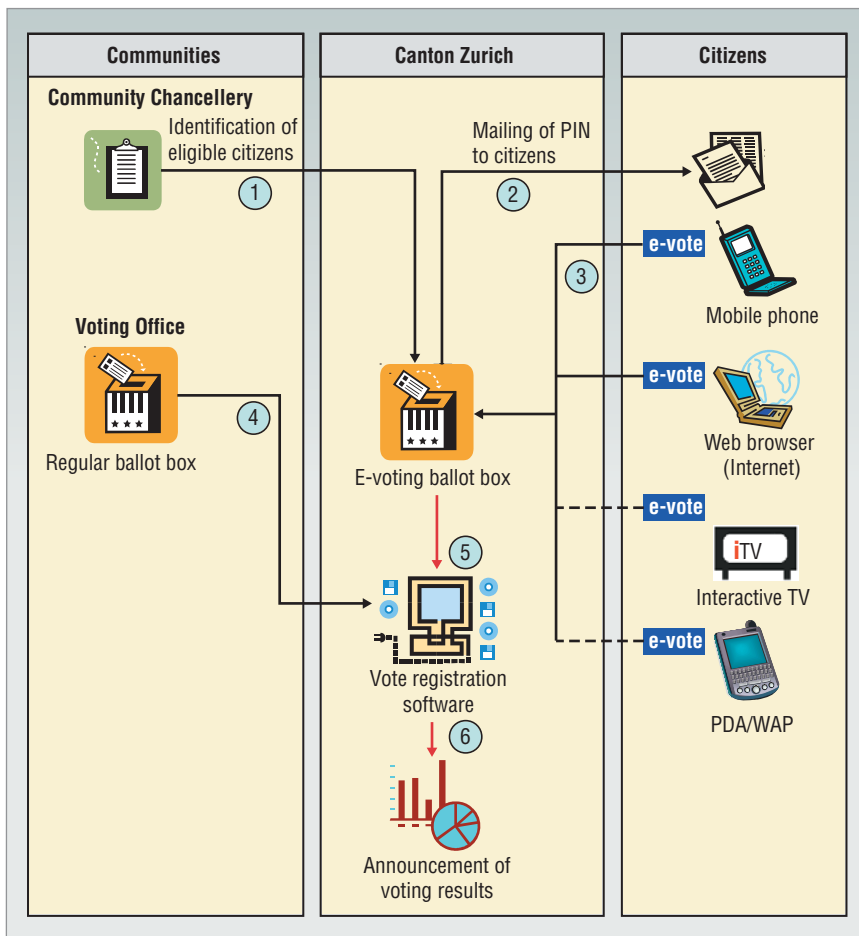


Figure 1. E-voting in Canton Zurich. The e-voting process has six main steps: (1) Communities send a list of those eligible to vote electronically. (2) Voters receive a list of system codes for identifying themselves and the referenda or candidates they are voting for, as well as codes for entering “yes” and “no” responses. (3) Voters cast their vote using their preferred digital medium. At present only Internet and mobile phone options are active, although the system is designed to handle iTV and PDA/WAP as well. The e-voting ballot box closes 24 hours before the regular ballot box. (4) The communities send the paper ballot results to the vote registration software. (5) Finally, Canton Zurich’s Statistical Office counts all votes (electronic and paper) and (6) produces the final vote count.

import. Each community and organization has field mapping and tracing options at all user levels. Swiss standards for e-government dictate how data fields and records are integrated.

To enable voting on a mobile phone, two of the three mobile phone companies in Switzerland use a virtual private network (VPN) communications network to link directly into the e-voting system. The third company uses an IP VPN communications network to link into the Canton Zurich secure network (LeuNet), which in turn links directly to the e-voting system.

SYSTEM DEVELOPMENT

The e-voting system had to ensure voting rights and secrecy, capture votes accurately, and prevent abuses such as multiple votes from the same individual. The

Swiss government was adamant that any alternative to traditional ballot-box voting not compromise the Swiss Federal Law for Political Rights, which protects the fundamental right of citizens to express their free political will without any technological, psychological, or other restriction or bias. The government also wanted an e-voting system that would encourage more citizens to participate in public-policy decision making. Finally, e-voting had to meet the same high security standards as traditional voting approaches.

To meet these requirements, the overarching design goals were to provide more flexibility and security without additional restrictions or controls and to offer a superior service for citizens and communities responsible for elections and referenda. To meet the superior service goal, all current IT systems had to integrate within the e-voting system. The aim was to require only minor changes to the communities’ election and referendum processes.

Another requirement was the ability to operate in the decentralized manner of the Swiss voting structure. Thus, each of the 171 communities within Canton Zurich had to be able to manage its own voting register. The e-voting system also had to account for features of the Swiss elections and referenda rules. For majority elections, this could involve a predefined list of candidates or the entire citizenry. The system had to allow each community to define when the electronic ballot boxes would be open. The election officers would receive the decoding keys with all the passwords to decode the votes on voting day.

Finally, to prevent citizens from abuses such as casting their vote multiple times, the system had to have several safety features, which either the communities could activate individually or the canton could activate centrally.

Testing

The e-voting system had to undergo scientific test monitoring as well as technological testing. The three cantons chosen for these tests, including Canton Zurich, signed contracts with the Federal Chancellery to adhere to four rules during testing:

- No one can intercept, change, or reroute electronically cast votes.
- No third party can obtain knowledge of the cast vote.
- Only registered citizens can vote.
- Every registered person can vote only once.

Testing used an algorithm developed to simulate vote casting, vote counting, and results reporting. The aim of these tests was to reveal gaps that might not be detectable during regular applications. From 2004 to 2006, the e-voting system was tested during real elections and referenda. Swisscom Solutions, Switzerland's leading telecommunications company, conducted the system and internal security audits. The Federal Chancellery also conducted a separate security audit and suggested changes in the architecture, user interface, and password structure. Designers considered these suggestions in improving the e-voting system during the testing phase.

Security

The e-voting system's security requirements are based on the Information Security Management System (BS 7799). Both the Swiss government and the Federal Chancellery assess security annually. External parties perform security audits, one of which involves attempting to hack into the e-voting system (so far, all attempts have failed). The hardware and its physical security environment are in compliance with the US Department of Defense's protection class B2 or lower. The security concept definition complies with both ISO/IEC 17799 and BS 7799.

Data exchange between the communities and the e-voting system is based on the Secure Data Exchange Platform (SeDAP), which is based on the Online Services Computer Interface (OSCI) standard, which in turn is based on SOAP. All entries into the e-voting system—voter identification and authentication as well as voter rights—occur through a secure entry server, which ensures that only registered voters can vote.

Both the citizens' votes through the Internet and the files containing the names of citizens eligible to vote are transmitted using the Secure Sockets Layer (SSL) protocol. The confidentiality of voter access codes and passwords is of utmost importance, so Canton Zurich uses three independent companies to print these. After the system identifies the access codes and the voters cast their votes, the system immediately asks them to vali-

The screenshot shows the e-voting interface for Canton Zurich, titled "Vote of Feb. 2, 2006". On the left, a navigation menu lists "Introduction", "Issues" (Federal Initiatives, Canton, Canton Parliament, Town Commission), "Community" (Initiatives), "Overview/Send", and "Logout". The main content area is titled "Fill in form" and contains three sections: 1a "Decision about the People's Initiative: 'Virtual Government'", 1b "Alternative proposal by the Government", and 1c "Supplementary Question". Each section has a question and two radio buttons for "Yes" and "No". The "Yes" button is marked with a green downward arrow, and the "No" button is marked with a red downward arrow. At the bottom, there are three buttons: "Back", "Forward", and "Cancel".

Figure 2. Sample e-voting screen. A menu indicates which issues are up for e-voting (left). In this case, 1a is the referendum, 1b is the alternative government proposal, and 1c is the supplementary question. Voters click on yes or no three times and then click forward to go to the next screen.

date their vote by entering their birth date and a six-digit numerical identification code. The system accepts their votes only after validation.

Encryption occurs in two steps. The voter's client computer first encrypts the votes and identification and authentication characteristics through an SSL channel (1,024-bit encryption). The e-voting system then checks the incoming votes for their structure and integrity before once again encrypting them (1,024-bit encryption) and passing them to the high-security zone (second firewall). Two redundant systems store the votes on a write-once, read-multiple-times database.

For every election and referenda event, Canton Zurich's Statistical Office uses a virtual community to cast votes and then checks that the e-system properly recorded them. It also analyzes the citizens' votes, making sure that the sum of the validated codes during e-voting equals the sum of received electronic votes. These two plausibility checks must match perfectly—have zero tolerance—for the e-voting to be trustworthy. The separate encryption and storage of cast votes and names of citizens eligible to vote ensures that vote counts are accurate and keeps voting rights from being corrupted.

The literature on e-voting emphasizes the danger of making source code available as a way to build trust in the system,⁴ since attackers with such access could

modify voting and auditing records.⁵ For these reasons, the Zurich e-voting system does not make source code available. Rather, it relies on the ACM Statement on Voting Systems,⁶ which recommends that e-voting systems “embody careful engineering, strong safeguards, and rigorous testing in both design and operation.” The Federal Chancellery supervises the decoding of e-votes, which takes place only after physical balloting closes. As a further precaution, the e-voting hardware itself is in a steel cage with physical access control mechanisms such as fingerprint identification and appropriate safety precautions, such as fire detection and break-in alert.

The ACM statement also recommends that each voter be able to inspect a physical record to verify the accuracy of that vote. Obviously, e-voting does not lend itself to a reproducible recording of each voter’s actions, but the codes provide an audit trail of sorts. This trail is still subject to attack and will never fully replace the physical trail, but a paper trail is equally dangerous in that it provides a visible receipt. Such a receipt could subject voters to bribery from those seeking to sell or buy votes.

Scalability and portability

Because of its service-oriented architecture and modularity, the e-voting system is fully scalable and portable. Cantons can define any number of voting districts, and communities can define their own electorate districts, entering district-specific data and information. Because the e-voting procedure is based on EML, any additional voting device will integrate with the e-voting system. Because voting transfer is independent of the user interface, users can integrate new applications and input devices quite easily. Thus, it is possible to analyze voting results independently of the media used to cast the vote.

ADOPTION RESULTS

Perhaps the main contributor to the e-voting system’s favorable reception is its modularity and service-oriented

architecture. Both national and local authorities have embraced the system because of its extreme flexibility in accommodating both centralized and decentralized operation and the full range of voting concepts, as well as its ability to integrate into existing infrastructure without compromising system security.

Adopting the e-voting system has already heightened voter participation. In response to the high participation in e-voting during the system’s testing phase, the board of the University of Zurich decided to abolish traditional ballot-box voting. Consequently, the 2006 student board elections were, for the first time, based solely on e-voting. The result was higher efficiency and lower cost with no compromise in the approximately 24,000 students expressing their political preferences.

The Swiss ICT Society awarded the Zurich e-voting system the prize for Best Software in 2005, citing “its flexible compliance with complex elections and referenda concepts, its modular structure allowing for extension, and its remarkably high security standard.” In 2007, the system won the 2007 United Nations Public Service Award for “fostering participation in policy-making decisions through innovative mechanisms.” These awards, as well as lessons from the testing phase and first year of general use, are evidence that the e-voting system will successfully handle all Canton Zurich’s 171 communities as well as port to other cantons or to any organization desiring to enjoy e-voting’s compelling advantages. ■

References

1. A.S. Belenky and R.C. Larson, “To Queue or Not to Queue?,” *OR/MS Today*, June 2006, pp. 30-34.
2. D.W. Jones and P.G. Neumann, “Interview: A Conversation with Douglas W. Jones and Peter G. Neumann,” *ACM Queue*, Nov. 2006, pp. 16-23.
3. R. Krimmer, ed., *Proc. 2nd Int’l Workshop Electronic Voting*, Gesellschaft für Informatik, Bonn, Köllen Druck+Verlag GmbH, Bonn, 2006 (in German).
4. J. Kitcat, “Source Availability and e-Voting: An Advocate Recants,” *Comm. ACM*, Oct. 2004, pp. 65-67.
5. B. Simons, “Electronic Voting Systems: The Good, the Bad, and the Stupid,” *ACM Queue*, Oct. 2004, pp. 20-26.
6. J. Grove, “ACM Statement of Voting Systems,” *Comm. ACM*, Oct. 2004, pp. 69-70.

Giampiero E.G. Beroggi is director of the Statistical Office of Canton Zurich. He is also a professor at the Zurich School of Business Administration, where he specializes in decision support systems. Beroggi received a PhD from Rensselaer Polytechnic Institute. He is a senior member of the IEEE and a member of the IEEE Computer Society. Contact him at giampiero@beroggi.net.

Computer Wants You

Computer is always looking for interesting editorial content. In addition to our theme articles, we have other feature sections such as Perspectives, Computing Practices, and Research Features as well as numerous columns to which you can contribute. Check out our author guidelines at

www.computer.org/computer/author.htm

for more information about how to contribute to your magazine.

Innovative Technology for Computer Professionals
Computer