Sixth sense
technology

University of Fribourg Information Systems Research Group Seminar work on E-government Case Studies on E-Voting Students: Daniele Cavadini Lorenzo Cimasoni Professor: Dr. Andreas Meier Assistant: Nicolas Werro Autumn Semester 2007 2 Contents 1 Introduction

Introduction Objective and problem deï¬�nition The aim of this Seminar is to give a wide overview on a speciï¬�c E-Government topic, E-Voting, analysing the most interesting case studies and giving as far as possible a wide overview from technical to political perspective. E-Voting has been attracting a lot of interest during the past years trained by the will of many

countries to develop E-Government and EDemocracy systems. The interest of E-Voting is spread at diï¬€erent level of the society, governments, parliaments, electorate, academic and industry are in diï¬€erent way attracted in this argument. In diï¬€erent countries the interest in E-Voting is growing very fast. The number of E-Voting tests that take place is also growing with diï¬€erent approach and motivation for each country. With those test is possible to learn new interesting lesson, share the diï¬€erent project and try to create a really valid E-Voting system. There are some categories that E-Voting tests can be divided, there are private pilot project, countries that tried with diï¬ƒculties to introduce EVoting (H, SLO, US, …), academic works with ï¬�eld test (D, A) and election administrations of countries, regions or municipalities with advanced pilots (CH, UK, EST). Another point to take in consideration is that is possible to subdivide the E-Voting term in 2 diï¬€erent concept: - E-Voting supervised by representatives of governmental with electronic voting machines at the polling stations - E-Voting not physically supervised, like voting from a computer via the internet, by mobile phones (using SMS), via Digital TV, or at public kiosks. This last method can also be called Remote E-Voting, or Internet Voting. The EVE1 research program revealed that Internet voting has been considered by countries which had already modernised their voting system (Figure 1) with measures such as the installation of voting machines in polling stations, the introduction of postal voting or the use of Internet in election or voting campaigns. 1. 2 Proceeding The ï¬�rst case studies treated in this document will be Switzerland, with an introduction on the past and the actual situation for explaining why this country became a very good candidate for E-Voting trials. The Geneva case 1 Evaluating practices and

Validating technologies in E-democracy 2 Figure 1: Example of voting evolution is one of the most important Remote E-Voting project and will be analyzed in diï¬€erent prospective, also comparing it with the other two Swiss cases, Zurich and NeuchË†tel. a Then the United Kingdom that tested a lot of diï¬€erent E-Voting channels during last year's with some interesting results and also diï¬€erent kind of problems. So there is the case of Estonia thet developped a ID card based E-Voting system with the structure of postal voting in Switzerland. And last case treated, United States, was the most diï¬ƒcult one because the lack of valid information and documentation about the test and the problems encountered during pilots or bindings vote. There are also others countries that are involved in E-Voting projects but many of them for the moment are developing their work only in academic ï¬�eld or testing them with non-bindings voting session. The cases analysis reach diï¬€erent activities domains, there are political and juridical discussions, some important technical issues and also society and people changing behaviors. When we get all information from all countries we would like to give a brieï¬‚y conclusion, including our personal opinion about the actual situation. 3 2 2. 1 Case Studies E-Voting in Switzerland Introduction 2. 1. 1 The Swiss e-voting initiative has been introduced in 2002 with the creation of all necessary legal basis and recommendation. In its "Report on the electronic vote, Opportunity, risks and feasibility" on January 2002, the Federal Council in particular asserts the fact that: - E-Voting should be as easy, practical and safe as possible - It should under no circumstances penalize citizens who have no access to electronic communication methods - The electorate should be able to express themselves in one and the same poll on federal, cantonal and municipal issues - The technical infrastructure

should be reliable - The system should make it possible to verify voting capacity - It should help prevent abuse, facilitate the counting of all votes and protect voting secrecy For the pilot trials a list of legal provision has been created, this document is concerned about the security and tell that an E-Voting system has to ensure that: - only entitled voters may take part in the ballot - each voter shall have a single vote and shall vote only once - it is impossible for any third parties systematically to intercept, alter or divert electronic votes or decisively inï¬‚uence the result of the ballot - it is impossible for any third parties to ï¬�nd out the content of the votes cast - all the votes cast are taken into account when the votes are counted - any systematic fraud is impossible In the 2003 with the participation of three cantons (Geneva, NeuchË†tel a and Zurich) with three diï¬€erent pilot project the E-Voting initiative take form with the aim of evaluating the feasibility of remote e-voting. The feasibility is evaluated by diï¬€erent aspects including the potential to increase voter turnout, the security risks and the cost-eï¬€ectiveness. 4 The original idea was to give a wide platform in order to cast votes in referendum and elections and also to give an electronic signature for initiatives, referendum and candidate proposals. For the moment all pilot project are only concerned on voting in referendum and elections. The Switzerland's objective of E-Voting is not to replace the actual ballot or postal voting, but to serve as an additional channel which might increase voter's turnout that become lower and lower since decades (Figure 2), with the exception on singular critical vote (for example entry in the EU). Figure 2: Voter turnout 1919-2007 With the introduction of postal voting in the 90ies the Swiss government tried to reverse the voting behavior giving a new method that make voting more easily accessible. And also very

important the concept of distantpolling has been introduced so that E-Voting will not appear as an absolute revolution. The main categories of people that could be interested on this project are young people that are more interested in the use of Internet but with a below-average participation and also all people that are not able too cast their vote for diﬀerent physical reason, for example physically handicapped individuals or the community of Swiss expatriates. This last community represented by OSA2 demanded the possibility to be able to cast their vote electronically for the 2011 federal election at the lasts. The number of Swiss voters abroad is signiﬁcant, in 2006 there were approximately 650 thousand Swiss residents abroad and 111 thousand of 2 Organisation of the Swiss Abroad 5 them were entitled to take part in Swiss votes and elections. Another aspect to consider is that the Swiss political system is a special one with an extremely large number of polling procedures (vote and elections) on the federal, cantonal and communal level, with four to six voting session every year. And also the voter registration procedures are on a high level because the registration is compulsory and all registries are systematically updated but the problem is that this is done in diﬀerent way for each canton. The Internet coverture in Switzerland give a solid base for all e-government initiatives including e-voting, also the use of Internet among the population grown really fast in the few past years, passing from 28, 8% in 2000 to 67, 8% in 20073 . The Federal Council strategy, with the approval of Parliament, in the medium long term is initially to allow further cantons to implement their own pilot project and also try to enable the E-Voting for the Swiss Abroad from 2008. In order to ensure this every canton has to create a central electronic standardized register that will be the ﬁrst step for implementing E-Voting.

For what is concerning the electronic signing referendum and initiative the perspective for the moment are not so good because the use of digital signatures is not yet so wide used and regulated in Switzerland. The cost of a wide introduction in all cantons of an E-Voting system that will allow all citizens to vote online is estimated with an investment between 400 to 600 million Swiss francs. But there are diﬀerent opinion about the date of an extended electronic vote, for the moment all vote trials that involves a federal vote will be restricted to a maximum of 2% of the canton population in order to prevent any vote manipulation in case of problems, and only those cantons that have shown a really good and secure implementation of e-voting are authorized to proceed for more extended trials. 2. 1. 2 Geneva Pilot Project The canton of Geneva has developed one of the ﬁrst public Internet Voting application in the world. The canton of Geneva introduced in the 1995 the postal voting that today is used by a very large part of citizen (95%), really higher in compair with the Swiss average. The participation with the introduction of postal voting increased by a 20% over 8 years from an average of 30%-35% to an average of 50%-55%. The Geneva project approach was not simply taken by a technical point of view, but they adopted a multidisciplinary approach. They involved the University commissioning a legal and socio-political studies and asked 3 according to Nielsen Net//Rating 6 private companies to develop some parts of the application, test his security, try to penetrate the system and analyze it. The Geneva Government is the owner of its online voting application. In practice an e-voting trials work as follow, all voter receive at home their own voting card (Figure 3) with all material needed to decide how to vote, this part is not diﬀerent as was in the past years. The voting card is subdivided in two

part, the left part is needed to whom decide to cast their vote from Internet and the right part is to ﬁll with birth date and a signature in order to cast the vote at the polling station or by post. Figure 3: Geneva voting card This is done 2 or 3 weeks before the voting session start, then when the time for voting comes the voter has to go with his Internet browser in the apposite web site4 (Figure 4) where ﬁrstly he has to type his 16-digit voting card number as a initial ﬁlter (four number identify the ballot and six identify the voter). Then the voter must ﬁll an online ballot paper similar to the paper one. The system then submit a recap of his choices allowing him to change them in case of mistakes. At the next step the voter attests his identity by giving his PIN code (hidden beneath a metallic ﬁlm), his birth date and his municipality of origin, which are checked in the central register. At the end the voter receive the conﬁrmation of the date and hour of his vote recording. In order to avoid that a voter is able to cast several votes an unique database has been created which records the voting cards numbers and 4 a demo is available at https://www. geneve. ch/ge-vote/demo/votation. html 7 Figure 4: Geneva demo vote website marks all those have already been used to vote for all diﬀerent channel (postal, Internet or polling station). Another precaution taken to avoid that votes can be read before the ballot box opening is that each one is encrypted with two diﬀerent encryption keys5 that are kept in a safe in the police headquarter. In addition the electronic ballot box's content is mixed before being read in order to prevent any date or order matching that can bring to the name of the voter. The entire Internet transaction on the voter side can be resumed in four step: 1. Voter identiﬁcation through his voting card number 2. Vote 3. Conﬁrmation of the voter's choices and voter authentication 4.

Conï¬�rmation of the vote (date and data of recording of the vote) The communication between the citizen's computer and the vote server is protected by the protocol SSL1286 . The vote server use a public key infrastructure that is authenticated with a digital certiï¬�cate. Checking the ï¬�ngerprint of the certiï¬�cate the user can control the authenticity of the server. The e-voting system uses two diï¬€erent type of servers (Figure 5): 5 6 PKI public/private key infrastructure Secure Socket Layer protocol 8 - the internet application server that allow the communication with citizens by means of web pages. This machine use an Apache web server and a Tomcat application server installed in two diï¬€erent partition - the database server that stores all information relative to the electoral roll and the eBallot Box. This server use Oracle version 9 each of those servers are cloned in order to prevent any accidentally lost of data caused by technical or human problems. Figure 5: Physical architecture The vote servers are installed in the basement of Geneva police headquarters. The physical access to the servers is strictly controlled and the access via the network is limited to the entry of a special single optical cable that is the only link with the local network and then the web, several ï¬�rewalls are installed in order to provide protection against intrusion. Also diï¬€erent probes are installed to detect speciï¬�c events in order to protect the system against denial of service or mass attacks. For opening the eBallot box and generate all the results is required the presence of the political parties' controllers. They are required to give the password that enables the registered votes to be doubly decrypted. Then the system generates two diï¬€erent ï¬�les, one ï¬�le containing the image of each ballot paper registered per voting site (submitted in order to generate the overall results) and another ï¬�le taken from the electoral roll

permitting statistical turnout analyses (transmitted to the Cantonal oï¬fce of statistics). The ï¬�le of ballots is processed by a results management system, which also integrates the postal vote count (conducted by optical reader), the counting 9 of ballot box votes (performed manually) and the decisions of the parties' controllers on void or suspect ballot papers. Between January 2003 and April 2005 E-voting has been used in eight oï¬fcial ballots in Geneva. Five of them municipal votes, one cantonal and two federal. These are the voters turnout results of the eight votes: Ballot Ani`res, January 2003 e Cologny, November 2003 Carouge, April 2004 Meyrin, June 2004 Federal/Cantonal, Sept 2004 Vandoeuvres, October 2004 Federal/Cantonal, Nov 2004 Cantonal ballots, April 2005 Reg. voters 1, 162 2, 521 9, 049 9, 180 22, 000 1, 680 41, 200 88, 000 Tot. Turnout 64% 59% 44% 39% 57% 60% 41% 44% E-Voting 44% 29% 26% 22% 22% 32% 22% 20% The average of e-voting is above 20%, all the statistics data collected from those trials are available to any interpretation, for now is not possible to tell if e-voting is going to increase turnout or simply replacing other vote method between who is already an active voter, but the participation to all trials is good and there was no major problem experienced. 2. 1. 3 NeuchË†tel Pilot Project a In NeuchË†tel, a cooperation between the canton and its communes had led a to create a wide platform, or e-government portal, called in French "guichet s´curis´ unique" (Figure 6). e e Using an approach very similar to the one of Internet banking, all the citizens will receive an user ID, a password and a constantly-generated transaction codes to access the public web site which oï¬€er a large variety of egovernment services. E-voting is one of these services, before each vote all citiziens receive at home, with all necessary voting material, an additional speciï¬�c

code that will allow them to cast their vote. All security measures, including for example SSL128, PKI cryptography and certiï¬�cates, are similar to Geneva pilot project. For the ï¬�rst vote trial the possibility to vote online has been given to a small part of people registered at the portal in order to keep the trial to small numbers, both in 2005. The same thing appends for all voting session as showed in the following table. Date 25. 09. 05 27. 11. 05 26. 11. 06 11. 03. 07 17. 06. 07 Extent of trial 1, 732 eligible voters 2, 469 eligible voters 3, 554 eligible voters 3, 757 eligible voters 4, 151 eligible voters Nb. e-votes (share of all votes as %) 1, 178 (68, 0%) 1, 345 (55, 1%) 1, 311 (36, 6%) 1, 538 (40, 9%) 1, 494 (40, 9%) 10 Figure 6: Main page of NeuchË†tel "Guichet S´curis´ Unique" a e e Like for the Geneva case the participation between the citizens enrolled at the portal was good and no major problems has been encountered by the voters casting their vote and by the administration. 2. 1. 4 Zurich Pilot Project The canton of Zurich has about 820, 000 registered voters, and many of them are dispersed in smaller communes, some with less than 200 voters. Each commune uses its own administration system, manages its electoral register, and counts its votes. Because voting is carried out at cantonal and local levels, the plan is to implement E-Voting at local level and have the communes pass on the results to the canton. Zurich has created a cantonwide shared database of voters that will be kept up to date by the communes. Another diï¬€erence between Zurich pilot7 trials and other Swiss trials is the possibility to use mobile phones as vote casting method using SMS. The system has been ï¬�rst tested in the election of the students' parliament at the University of Zurich in December 2004. The ï¬�rst bindings trial involved the commune of B¨lach in November u 2005 in a communal vote with the sequent results:

Turnout 41. 5% (3919 votes) Internet votes 1006 SMS votes 445 Always in November 2005 a second votation has took place and involved three communes, Bertschikon, B¨lach and Schlieren but in this case was a u 7 a demo is available at http://evotingdemo. zh. ch 11 federal vote Eligible voters 16726 e-votes (share of all votes as %) 1154 (22, 1%) SMS votes 243 Then for the ï¬�rst time a communal election took place in April 2006 in B¨lach using the same system as others E-Voting trials. According to Beat u Kocher, mayor of B¨lach, "The vote went smoothly, like Swiss clockwork". u Figure 7: B¨lach E-Voting card example u The last two voting session involed again Bertschikon, B¨lach and Schlieren, u with similar results as showed before, were in November 2006 and June 2007. 2. 2 E-Voting in UK The UK Government in the years from 2000 to 2006 tested various EVoting's systems, precisely in May 2000, May 2002, May 2003, June 2004 and May 2006. 2. 2. 1 Tested methods Diï¬€erent methods were tested including: - Internet 12 - Interactive Voice-Responder - Mobile telephone (SMS) - Kiosk Voting - Digital television Voting - e-counting of paper ballots - smart cards for voter identiï¬�cation purposes - Polling station operated e-register of voters 2. 2. 2 Security / Control The security-strategies and control-methods adopted by the UK are more or less the same than the other countries. Each voter was identiï¬�ed by a unique vote reference number (VNR) consumed when an e-channel had been used, this to exclude multiple voting. During the election day the e-register of all voters was used in polling station to ensure that voters had not previously voted at another polling station or used an e-voting channel. If a voter used the postal vote, than his e-credentials would be disabled. To allows polling station access the e-register were used ISDN connections and laptops, this were done to give the

possibility to the staï¬€ and technicians to rectify problems. In case of a temporary unavailable problem the polling station's staï¬€ had to keep paper records of voters who have voted to insert them later in the system and call the election oï¬fce to verify each voter's eligibility. In case of a permanently down system then they had to convert to traditional voting without the possibility to vote at any polling station. In 2003 the UK Government introduced the smart cards containing the voter's ID to speed up the process of retrieving voter's details. 2. 2. 3 Problems With these pilots the UK Government aim to put robust systems in place for an e-enabled General Election after 2006. During the pilot tests they encountered a lot of general problems. Some of these problems are: - Insuï¬fcient number of back up hardware - Laptops incorrectly conï¬�gured prior to delivery - Few technical support staï¬€ provided - Time and resources needed to set up polling stations underestimated 13 - Not always possible to establish a channel of communication from polling stations and election oï¬fce - ... The trials were far from smooth. Diï¬fculties with electronic counting technology resulted in the electronic count being abandoned in favor of a traditional manual count in some pilot areas. Electronic counting in the other pilot areas was completed although it was slower than expected. The commission blames these problems on "limited testing and insuï¬fcient planning prior to the election". Until now, the UK isn't able to oï¬€er a secure and stable E-voting system. 2. 3 2. 3. 1 E-Voting in Estonia Introduction The subject of e-voting has been actively discussed in Estonia on diï¬€erent levels since the beginning of this century. For the local government council elections of 2005 they decided to introduce the possibility of E-voting their candidates. Estonia uses a diï¬€erent method than the other countries to ensure that a voter

votes only once. This method implies the Identity card. A public key infrastructure enabling secure electronic personal authentication using digital signatures and ID-cards has been created and for the 2005 elections there are more than 800'000 voters' ID-card and digital signatures still ready. The objective is that E-voting must be as similar to regular voting as possible, compliant with election legislation and principles and be at least as secure as regular voting. Estonia tried to do a simple and eï¬cient E-voting system. The security issues provided by the Estonian E-Voting are similar to the other countries: - E-voting must be uniform and secret - Only eligible persons must be allowed to vote - Every voter should be able to cast only one vote - A voter must not be able to prove in favor of whom he/she voted - The collecting of votes must be secure, reliable and accountable To better organize the elections the E-voting have to take place from 6th to 4th day before Election Day, in this way there is still time to organize E-votes. There are 6 simple rule to satisfy for a correct E-voting in Estonia, these rules are accorded to Estonian election legislation and they are: 14 1. On advance polling days, voters may vote electronically on the web page of the National Electoral Committee. A voter shall vote himself or herself 2. A voter shall identify himself or herself using the certiï¬�cate entered on his or her identity card which enables digital identiï¬�cation 3. After identiï¬�cation of the voter, the consolidated list of candidates in the electoral district of the residence of the voter shall be displayed to the voter on the web page 4. The voter shall indicate on the web page the candidate in the electoral district of his or her residence for whom he or she wishes to vote and shall conï¬�rm the vote by signing it digitally using the certiï¬�cate entered on his or her identity card which enables digital signing 5. A notice that the vote has been

taken into account shall be displayed to the voter on the web page 6. Voter may change his or her electronic vote during the advance voting period from 6th to 4th day before Election Day: by voting electronically or by voting in polling station Generally multiple voting is considered as a crime and illegal, but in this case the electronic re-vote isn't considered as "multiple voting", because the system takes into account only one vote (the last given). This method is a good way to avoid illegitimate inï¬, uences, because the voter can cast a new vote (that nullify the previous vote) when the inï¬, uence is gone. Another advantage is that if the electronic system is seriously compromised and the electronic votes are lost, than the voter can cast his vote in the traditional way (because the E-voting closes 4 days before the Election Day, so if there are problems the government is still in time to communicate that a new "traditional" voting-session is required). 2. 3. 2 System deï¬�nition From a technical point of view the e-voting system must be as simple as possible as well as transparent so that a wide range of specialists are able to audit it and if it's the case ï¬�x problems that could occurs. The e-voting system must also be reusable in a way that developing a new system for the next voting is possible and that ameliorating the code it's easy and fast. Estonia takes the security issues very seriously, because in E-voting the weakest part is the voter's PC that can't be controlled, by the way the servers where the votes are stored is under the control of National Election Committee and they can be controlled. The best way to solve these security issues is to grant a strong and versatile security system in the server side. 15 Figure 8: The Envelop Method used by Estonia E-voting Public key cryptography is used here (Figure 8). E-voter (application) encrypts his/her choice (number of candidate) with the system's public key and signs

the result digitally. The votes are collected, sorted, voter's eligibility is veriﬁed and invalid votes are removed (double votes, votes of ineligible voters). Next the outer envelopes (digital signatures) are separated from inner envelopes (encrypted votes). Voter lists are compiled from outer envelopes. Inner envelopes (which are not associated with the identity of the voter any more) are forwarded to the vote-counter who has the private key of the system. The vote-counter (application) outputs the summed results of e-voting. The following requirement ensures that the privacy of e-voters is maintained: at no point should any party of the system be in possession of both the digitally signed e-vote and the private key of the system. In this way the privacy is granted because no one can compare a speciﬁc vote to a voter's name in the database. The voting process takes place as follows: 1. The voter accesses via HTTPS-protocol the "Vote Forwarding Server" (VFS) and identiﬁes him/herself with the ID-card. 2. Some controls are performed (check if voters has already voted, veriﬁes the eligibility of the voter and identiﬁes his or her constituency). 3. The voter application, having the candidate list, asks the user to conﬁrm his/her choice. 4. The voter application transmits its digitally signed envelope to the VFS which veriﬁes the formal correctness of the received material and whether the same person who authenticated him/herself during the start of the session gave the digital signature. 16 5. In case of successful vote the Vote Storage Server (VSS) sends the VFS a conﬁrmation that the vote has been received. A corresponding message is delivered to the voter as well. 6. A "cancelation period" takes place after the E-voting period ends. During this period all voting are confronted and analyzed to remove multiple votes or vote errors. 7. When the cancelation period ends the outer envelopes are

separated from the inner ones. 8. The votes are decrypted by constituencies using the private key. The decrypted vote is checked against the candidate list to determine if it is possible to vote for the candidate in that constituency. 9. The votes to be taken into account are summed by candidates and constituencies, and recorded. Then they are added to the results of the ordinary voting. We can easily see that the Estonia's E-vote system is very well deï¬�ned and the most important particular to keep in consideration is that everyone uses the personal ID-card to authenticate himself. There are some positive aspects like the possibility to change the vote but at the end the system is not completely secure yet and it has to be developed further compared to others countries E-Voting systems. 2. 4 2. 4. 1 E-Voting in USA The SERVE project The Pentagon put an Internet voting system, called SERVE, into place for the 2004 election. The rollout was suspended, however, after a panel of experts issued a scathing report on the security problems inherent in the scheme. Because SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber-attacks, like insider attacks, Denial Of Service attacks, spooï¬�ng of information, automated vote buying. Any one of these attacks could generate catastrophic consequences (large money wasting, impossibility to count the exact number of votes, privacy violation, …). These vulnerabilities couldn't be ï¬�xed by changing the design of SERVE or by correcting some bugs. These vulnerabilities are directly connected to internet's structure and to PC's hardware and software that, today is ubiquitous (this means that an attacker could physically stay outside the polling station's structure and perform some attacks using his notebook or his mobile phone). 17 Because of these

problems and vulnerabilities the development of SERVE had been canceled. The suggestion was to stop researching in these way, waiting until the both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear. 2. 4. 2 Remarks There was a very large debate about the role of all the problem in the EVoting system during the last two presidential elections. A lot of exploits and weakness has been found in all the system and the critics were very intense also because the amount of vote to elect a candidate instead of another was very small. Another aspect to consider is that there was not the possibility to know how polling station code works and accusations against the proprietary source code has been moved. The actual situation is that some states decide to return back using the classical voting method, refusing the new E-Voting because there are too many risks. 3 3. 1 Conclusions Security The advanced work of Geneva project create a good base of comprehension of all possible security problems, the "11 commandments for internet voting" are of special interest as they incorporate an advanced experience with EVoting: 1. Votes cannot be intercepted nor modiï¬�ed 2. Votes cannot be known before the oï¬ƒcial ballot reading 3. Only registered voters will be able to vote 4. Each voter will have one and only one vote 5. Vote secrecy is guaranteed, it never will be possible to link a voter to his/her vote 6. The voting website will resist any denial of service attack 7. The voter will be protected against identity theft 8. The number of cast votes will be equal to the number of received votes 9. It will be possible to prove that a given citizen has voted 10. The system will not accept votes outside the ballot opening period 18 11. The system will be audible Those rules has been taken in account also by the Council of Europe

for underlining the security aspect that will be the base of any E-Voting system. 3. 2 Political choice In compare to all those countries that tried to introduce E-Voting procedures without suï¬cient testing and public debates the "only a step-by-step" approach seams to work better. This approach could leads to the success with voting tests separate or parallel to the oï¬cial vote, then a further step could be to held a valid voting test (pilots) that involve a small part of the population and at the end when the systems has been fully analyzed and approved a bigger number of citizens should be involved. Any change in polling methods provokes a lot of debates with all kind of specialist and with political parties, but the bigger part of critics do not reï¬‚ect the opinion of the majority part of the population that in the past years quite always accept changes in voting system, for example the vote lowered to 18 years old, women's vote rights or postal voting. The introduction of E-Voting at polling station in some countries like in Unites States create a lot of problems when a large series of bugs and errors were founded during important elections, this create a very pessimistic impression about the E-Voting. 3. 3 Internet evolution As Internet and all kind of technological instruments evolves very rapidly, also all diï¬€erent kind of threat changes and evolves too. A solid E-Voting system must be adaptable through the time in order to remain secure and reliable, so the investments has to be constant. Not only the E-Voting system is involved in the Internet evolution but also all diï¬€erent instruments that citizens could use in order to decide how to vote. All kind of information are available in the net passing through political parties web site, web site that collect data from politician, personal blogs, news web site and so on. 3. 4 Considerations The security aspect is the most important one for the E-Voting subject, without an

eï¬fcient and secure system is not possible to create this important part of E-Government initiative. Not only E-Voting subject is concerned on security but all those projects or initiatives that involves the creation, transmission and storage of critical and personal data. There are diï¬€erent opinion about how secure is transmit data trough modern technologies, the most pessimistic says that there are too many 19 problems in computers and network that could not lead to create a valid system. This is true in part, actually there is no system that could guarantee the absolute security but also postal and classic vote have some risk. The important thing is to evaluate those risk and see if are acceptable for the concerning project and how to reduce them to the minimum. A voting system can only work if all the people involved in (citizens, politicians and government) have enough trust in the system and in the technologies that keep that running. 20 References [Bonard 2002] Claude Bonard, The Geneva e-voting project, In: World Civil Society Forum, July 2002, available: http://www. geneve. ch/ chancellerie/E-governement/doc/CB_forummondialsocivile. pdf, accessed 3th of November 2007. [Braun 2006] Nadja Braun, E-Voting - the Swiss experience, CoE: e-voting review meeting, Strasbourg, November 2006, available: http://www. coe. int/t/e/integrated_projects/democracy/ EVoting/pptbraunch. ppt, accessed 4th of November 2007. [Braun 2006] Nadja Braun, Daniel Braendli, Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed, Swiss Federal Chancellery, 2006, available: http://static. twoday. net/evoting/files/ braun_braendli_swiss_e-voting_27_36. pdf, accessed 4th of November 2007. [Buchsbaum 2004] Thomas M. Buchsbaum, E-Voting: International Developments and Lesson Learnt, Deferal Ministry for Foreign Aï¬€airs, Austria, 2004, available: static. twoday.

net/evoting/files/buchsbaum_ p31-42. pdf, accessed 13th of November 2007.

[Estonia 2005] The nation election committee, E-Voting system Overview, Tallinn, 2005, available: http://www. vvk. ee/elektr/docs/ Yldkirjeldus-eng. pdf, accessed 10nd of November 2007. [Etat de gen´ve 2007] Etat de Gen ´ve, Geneva eVoting system best practice, e e In: E-Voting, available: http://www. geneve. ch/evoting/english/ etude_projet_evoting. asp, accessed 2nd of November 2007. [Geneva State 2006] Geneva State Governement, State Council's Report, In: Grand Council on the Geneva electronic voting project, Geneva, May 2006, available: http://www. epractice. eu/files/upload/gpc/ document/574-1185281698. pdf, accessed 4th of November 2007. [Geser 2002] Hans Geser, E-voting projects in Switzerland, Sociology in Switzerland, Zurich, August 2002, available: http://socio. ch/ intcom/t_hgeser12. htm, accessed 10th of November 2007. [Guichet 2004] Rapport du Conseil d'Etat au Grand Conseil, ´ ´ GUICHET SECURISE UNIQUE, In: projet de loi sur le guichet s´curis´ unique (LGSU), NeuchË†tel, August 2004, e e a available: www. ne. ch/neat/documents/Autorites/gc_1414/ODJ_1702/GC_ 2004_10_files/04034_fa. pdf, accessed 12th of November 2007. 21 [McGaley 2003] Margaret McGaley, J. Paul Gibson, Electronic Voting: a safety critical system, Mars 2003, available: http://www. evoting. cs. may. ie/Project/report. pdf, accessed 15th of November 2007. [Swissinfo 2007] Swissinfo, Expatriates push for e-voting, In: News, available: http://www. swissinfo. org/eng/swissinfo. html? siteSect= 43&sid= 7675340, accessed 4th of November 2007. [Tableau 2007] Chancellerie F´d´rale, Tableau synoptique des essais de vote e e ´lectronique ayant eu lieu en Suisse, In: Documents, August 2007, availe able: http://www. bk. admin.

ch/themen/pore/evoting/00776/index. html? lang= fr, accessed 22th of

November 2007. [Xenakis 2004] Alexandros Xenakis, Ann Macintosh, The UK

deployement of the e-electoral register, International Teledemocracy Centre,

Bregenz, July 2004, available: http://www. e-voting. at/scripts/download.

php? F_ID= 103, accessed 13th of November 2007. 22