E-Voting Election Test to the Austrian Federal Presidency Election 2004

Alexander Prosser, Robert Kofler,
Robert Krimmer, Martin Karl Unger

Arbeitspapiere zum Tätigkeitsfeld
Informationsverarbeitung und Informationswirtschaft
Working Papers on
Information Processing and Information Management

Nr./No. 02/2004

Herausgeber / Editor:
Institut für Informationsverarbeitung und Informationswirtschaft
Wirtschaftsuniversität Wien · Augasse 2-6 · 1090 Wien
Institute of Information Processing and Information Management
Vienna University of Economics and Business Administration
Augasse 2-6 · 1090 Vienna

pm production management

e-Mail: **e-Voting@wu-wien.ac.at**
WWW: **http://www.e-Voting.at**

Supported by:

IBM

A-TRUST

Content

Preface **3**

1 E-Voting: A Definition **5**

2 The E-Voting.at Algorithm **7**

3 Election Test to the Federal Presidency Election 2004 ..... **11**

4 Requirements to the National ID card **13**

5 OCG Working Group E-Democracy **15**

6 The Role of Digital Signature Cards in Electronic Voting **19**

7 History of E-Voting.at **29**

Preface

Electronic submission of votes via the Internet (e-voting) has become a real technological possibility. In contrast to administrative e-Government applications e-voting touches the very core of our democratic systems and hence has to be treated with the appropriate care. Legal restrictions and high quality parameters apply to this area. In the design of e-Commerce or e-Government applications it has been customary to use the electronic media to change the underlying business process, however, in e-voting the processes to be implemented are given and it is the e-voting system that has to adjust to the legal framework, which is mainly given by the General Voting Principles.

Design and implementation of e-voting represent a particular responsibility in regards to these Principles. Due to the sensitivity of the application, e-voting can only be used after extensive tests and feedback from practical application. The election test described in this Working Paper describes such a test conducted in parallel to the Federal Presidential Election in 2004.

We owe thanks to our partners, who enabled us to conduct the election test:

Our sponsors and industry partners IBM Austria and A-Trust, in particular Dr. Ludwig Brüstle, Christian Peter and Mag. Cornelius Granig (IBM) as well as Josef Ferstl and Thomas Jilek (A-Trust).

The Student Union at the University of Economics and Business Administration and their chairmen, Michael Suppan and Günter Klein.

The members of the test election committee (see Section 2 for their role in the electronic election process), Prof. Gabriele Kotsis, Prof. Michael Holoubek and Dr. Horst Breitenstein.

We owe special thanks to the University IT department, for their friendly and unfaltering support in hosting the election test, Dr. Georg Miksch, Peter Mika, Alfred Nagl and Gerhard Gonter.

We dedicate this working paper to all our partners, who supported us in conducting this trial.

The Authors, May 2004

1 E-Voting: A Definition

Before one can start a discussion on electronic election procedures, one should clarify certain forms and phases of paper or e-elections.

PAPER-BASED ELECTIONS

In traditional paper-based voting, one can distinguish between voting in polling stations (in the presence of an election committee) or absentee voting using mail ballots. Figure 1 summarises the different steps in the voting process for these forms.

Process steps	Polling station	Absentee voting
Voter identification	Identification at election committee in the polling station.	Identified application for mail ballot sheet by the voter prior to election, which is sent to the known address of the applicant.
Vote casting	Polling booth during opening hours of polling station.	Mail ballot is filled in at an arbitrary location and at any time prior to a certain deadline.
Vote counting	Manual count by election committee, transfer of local results to centralised counting SW.	Manual count of ballot sheets upon reception of mail vote by the election committee till deadline.

Fig 1: Traditional election processes

IT-SUPPORTED ELECTIONS

The same fundamental distinction can also be made for voting systems using IT support.

Various types of electronic (or mechanical) devices may be used to automate the voting process in the polling station; absentee voting can be implemented by various means with the Internet being only one of them. Figure 2 provides a summary:

Process steps	Polling station	Absentee voting
Voter identification	Identification at election committee in the polling station.	Either by receiving the token (=TAN) to cast one vote by mail (= absentee voting) or electronic application.
Vote casting	Polling booth during opening hours of polling station using IT-supported (or mechanical) device.	Vote is transferred to electronic ballot box using various media: SMS, phones, proprietary networks or via the Internet.
Vote counting	Automated counting.	Automated counting.

Fig 2: IT-supported election processes

Given the above systematisation we understand e-voting as absentee voting using the Internet. It comprises of one identified and two anonymous steps:

(i) application for electronic voting token (identified), (ii) vote casting and (iii) vote storage and counting (both permanently anonymous). The criteria usually applied to e-voting systems in the literature were summarised in an Internet Policy Report [IPI01] on e-voting as (i) correctness in counting votes, (ii) dishonest voters cannot disturb the election, (iii) permanent anonymity, (iv) voters can only vote once, (v) only authorised voters may vote, (vi) independence (no undue influence is exercised on the voter), (vii) verifiability, (viii) receipt-freeness (voters cannot prove how they voted).

2 The E-Voting.at Protocol: Guaranteeing Secure and Legally-binding Elections via the Internet

Internet elections (e-voting) have become a real possibility, but the General Voting Principles have to be guaranteed in either way. Funded by the Anniversary Fund of the City of Vienna the first system to vote via the Internet has been developed that technically guarantees these constitutional voting principles.

When developing an e-voting-system one has to solve the following problems:

- Unambiguous identification of the voter,
- Absolute anonymity when casting the vote
- The administration must not be able to (a) corrupt the anonymity or (b) to manipulate any vote.

The actual prototype is based on a protocol developed by Prof. Alexander Prosser, Institute for Information Processing and Information Economics at WU Vienna that has been published internationally. It is thereby available for public discussion and examination. For absolute protection of the anonymity the protocol divides the election in two stages:

- Registration phase, where the voter identifies him/herself and applies for an electronic voting token and
- The vote casting phase, where the electronic voting token is used to cast a vote anonymously.

REGISTRATION

The protocol is designed for use with the Austrian National ID card [Pos03]. The prototype uses the real infrastructure of the National ID card and the central register (ZMR) and offers a standardized interface for trust center services for authentication; as for this test smart cards were not available in a large enough number, the standard student login was used for the authentication.

All students of WU could participate in the test election. For data protection reasons the unique student identification numbers were not used for the registration database, instead derived hashed numbers were provided by the University IT department ZID and saved in the registration database. Requests for issuing electronic voting tokens were checked against that database (for a more detailed technical description see [PKK03]).

Userview	*Technical process*
➢ Opening the Web page www.e-voting.ac.at to apply for a voting token.	➢ This login page was hosted due to data protection issues by the University IT department.
➢ Entering the student login	➢ The student login was checked against the data by the University IT department and then hashed and digitally signed.
➢ Redirection of the student to a Web page for issuing of the electronic voting token	➢ A signed Java applet that guides the user through the following steps is loaded from the registration server.
➢ User enters password for encryption of	➢ As the electronic voting token is not

the electronic voting token and confirms it.	saved on a smart card but on any storage media, one had to encrypt it with a user-selected password.
➢ This step is fully automatic; no user input is required.	➢ The electronic voting token is sent to the registration server and is signed blindly [Cha81, 87]; i.e. it is signed authentically, the signer does not see what is signed; **thereby the electronic voting token cannot be traced back to the applicant.**
➢ This step is fully automatic; no user input is required.	➢ Validation token is sent to the trust center for the blind signature ➢ Signed validation token is returned. ➢ The issue of the voting token is marked in the voter register
➢ The student selects a location for saving the encrypted electronic voting token.	➢ The electronic voting token is saved at the selected location.
➢ The user gets a final message.	➢ The Java applet is unloaded.

Fig. 3: Registration process

Remarks:

- After issuing the electronic voting token the eligible voter is removed from the conventional voter register. Double voting is prevented.
- If the electronic voting token or the validation token is lost in transfer, a reissue is possible, i.e. the blindly signed voting token will again be sent to the applicant – using cryptographic procedures it is secured that no one besides the applicant can decrypt the voting token.
- As it was only a test election, an additional step requiring the user's confirmation - that it was not a real election - was built in. The same confirmation was also required during the vote casting itself.

VOTE CASTING

When the eligible voter casts the vote on Election Day, then the authentication is done using the electronic voting / validation token. This step is completely anonymous.

The election committee known from conventional voting is emulated, it serves as measure to prevent manipulation by the administration of the election servers. Its members are nominated by the candidating parties. Each member creates an asynchronous key pair, and the ballot sheet is encoded with each separate public key of the comissioners. The private key is kept secret.

Userview	*Technical process*
➢ Opening the Web page for casting the vote.	➢ The signed Java applet that guides the user through the following steps is loaded from the ballot box server.
➢ Entering the password	
➢ Selecting and loading of the electronic voting token using a separate file dialogue.	The ballot box server-checks ➢ If the voting token has already been used, ➢ the authenticity of the signatures on the voting and validation token. ➢ If authorised, the voter receives the ballot sheet.
➢ Ballot sheet filled in and sent to the ballot box. ➢ As protection from precipitation the user is required to confirm the selection.	➢ Ballot sheet is encoded with the public keys of the commissioners and sent with the voting/validation tokens to the ballot box server. ➢ The authenticity of the voting/validation token is again checked. ➢ In positive cases the coded vote is saved.

Fig 4: Vote casting process

COUNTING

The votes are submitted encoded; they can only be read after the members of the election committee have entered their private keys in the system. After the end of the election the encoded results will be published in the Internet. The committee members can then provide their private keys for the results to be decoded and counted.

All key pairs of the election committee members are also published so that everybody can reconstruct the final result.

Further cryptographic protocol parts prevent the administration from inserting votes or from deleting encoded votes before the end of the election.

REFERENCES

[Cha81] Chaum, D.: Untraceable electronic mail return addresses and digital pseudonyms. In: Communications of the ACM, Vol. 24(2), 1981, S. 84-88.

[Cha87] Chaum, D.: Blinding for Unanticipated Signatures. In: Chaum, David; Price, Wyn (Eds.): Advances in Cryptology, EUROCRYPT '87, Springer-Verlag, Berlin, 1987, S. 227 –233

[KKPU04] Kofler, R., Krimmer, R., Prosser, A., Unger, M.: The Role of Digital Signature Cards in Electronic Voting. Proceedings of 37th Hawaiian International Conference on System Sciences, Hawaii, 2004.

[PKK03] Prosser, A., Kofler, R., Krimmer, R.: Implementing an Internet-based Voting System for Public Elections - Project Experience. Proceedings of ICEIS 2003, Setubal, 2003.

[Pos03] Posch, R.: Das Konzept der Bürgerkarte. Chief Information Office, Wien, 2003.

3 The E-Voting Election Test to the Federal Presidency Election 2004

The prototype presented in the previous chapter was first used in an election test in parallel to the student union elections at WU Vienna in May of 2003. This report is on the second use in another election test during the federal presidency election in April of 2004.

As at this test election the National ID card was not available in large enough numbers, the project team had to replace the two National ID card roles, by

- Using the identification facilities by the WU computer center.
- The electronic voting token was saved on a non-specific medium.

All 22.000 students of WU Vienna were eligible to participate in the test election. The application for the voting/validation token could be signed from March 22nd till April 22nd 2004, the vote casting itself took place from Friday, April 23rd till Sunday, April 25th 5 pm. On 25th of April at 5 pm the ballot box was opened and decoded by the election committee (consisting of Prof. Gabriele Kotsis, President of the Austrian Computer Society; Prof. Michael Holoubek, Institute for Constitutional and Administrative Law; Dr. Horst Breitenstein, WU Vice Dean) and votes were decoded and entered the tally.

EVALUATION OF THE TEST ELECTION

All components of the system – registration, vote casting and the opening/counting of the ballot box worked perfectly well. For the support of the user a helpdesk was available where 129 requests for help via phone or e-mail were registered. 50 % of the requests concentrated on help regarding the installation of Java itself or a forgotten password of the electronic voting token. Obviously the time between the Registration and the actual vote casting should be shortened. It was also shown that persons that can use a web browser can also use an e-voting system.

Using National ID cards will facilitate the use of the e-voting system even further, as all read and store operations will be done automatically by the card readers – the respective file dialogues which are necessary in the current prototype will be eliminated.

1786 students applied and saved an electronic voting token, out of which 961 then casted their vote. These votes were distributed as follows:

➢ Valid voting tokens	1.786
➢ Votes cast	961
➢ Invalid votes	42
➢ Abstention	56
➢ Valid votes	863
➢ Dr. Benita Ferrero-Waldner	408 (47,28%)
➢ Dr. Heinz Fischer	455 (52,72%)

Fig. 5: Results of the test election

The distrubiton of the test election votes corresponded to the results of the real election with 0,3 percentage points. In conjunction with the results of the first test election in May 2003 where also no significant difference to the actual results could be manifested, the hypothesis

- H0: e-voting results in the same results in the digital voting process as in the paper based voting process.

could not be falsified.

4 Requirements to an E-Voting-enabled National ID card

In 1999 Austria was the first country to pass the European signature directive with the signature law. The e-government law 2004 is based on the Registration Law (Meldegesetz) 1995 and the signature law and introduces the National ID card „Bürgerkarte“ (citizen card). Using such a card for e-voting is requiring specific modifications that have to be implemented.

The field for which the e-voting system has been developed is a smart card that features the digital signature and a national ID card functionality. The national ID card is the ideal medium for e-voting. The card has to fulfill two tasks for e-voting: firstly it has to allow to sign the application for an e-voting token and secondly to store the e-voting token on the card. To be able to store the e-voting token on the medium, certain requirements have to be met in order to guarantee that no misuse of data is possible:

- The e-voting token has to be protected from illegitimate read-access, i.e. by storing in a PIN-secured area. This is possible today.

- On election day one must guarantee that the ballot box application only can read the e-voting token and not any other information that could reveal the identify of the voter. This is currently not realised as the digital certificate and the personal identification file (part of the national ID card concept) can be accessed without any restriction.

- Another function lies in the integration of essential parts of the e-voting protocol into the operating system of the smart card. The PC of the user is potential insecure environment, viruses and Trojan horses are an every day threat [Schr04]. To circumvent these problems, it is only logical to move all critical protocol parts in a secure medium like a smart card (i.e. like the unblinding process of the e-voting token for details see chapter 2). This also means that the operating system of the smart card has to allow for this or has to be modified in accordance to the in [KKPU04] and in chapter 2 described algorithm. The mathematical operation needed would be:

- The smart card gets the certificate of the relevant constituency, where the voter is eligible to vote. This certificate holds the public key `(e, n)` of the constituency. The card takes a random number `t` and a to `n` different number `r` and calculates `x` as
  `x = (t * (r^e %n)) %n`
  and sends this number `x` to the registration server. This server calculates the number `y` as `y = x^d %n` and returns the number `y` to the applet. The applet resolves the number `r1` so that: `(r * r1) %n = 1`

  The rules of the residue class arithmetic allows for the following transformations:
  `y = x^d %n` and due to
  `x = (t * (r^e %n)) %n`
  `y = (t * r^e)^d %n`
  `y = (t^d * ((r^e)^d %n)) %n`
  `y = (t^d * r) %n`
  `(y * r1) %n`
  `= (t^d * ((r * r1) %n)) %n`
  and `(y * r1) %n = t^d %n`

  Then the smart card has to multiply the number `y` with `r1` and reduce the resulting number with modulo `n`, so to get the number of the term `(t^d %n)` `t^d %n = (y * r1) %n`
  The now indirect calculated number of the term `(t^d %n)` is called `td` and forms together with the number `t` a part of the electronic voting token.

RESUME

The national ID card concept provides the best premises for the use with e-voting as many attack scenarios like viruses and Trojan horses can be averted. To do so amendments have to be implemented in the national ID card concept that are not part of the standard operating systems.

REFERENCES

[KKPU04] Kofler, R., Krimmer, R., Prosser, A., Unger, M.: The Role of Digital Signature Cards in Electronic Voting. Proceedings of 37th Hawaiian International Conference on System Sciences, Hawaii, 2004.

[Schr04] Schryen, G.: Security Aspects of Electronic Voting. Proceedings of 37th Hawaiian International Conference on System Sciences, Hawaii, 2004.

5 Working Group E-Democracy of the Austrian Computer Society

Electronic transactions over the Internet, particularly using the World Wide Web have become an integral part of economic life. Recently also the public sector has started to use the new medium for its administrative processes (e-government). Still it stays to question how the Internet could be used to support democratic decision processes (e-democracy).

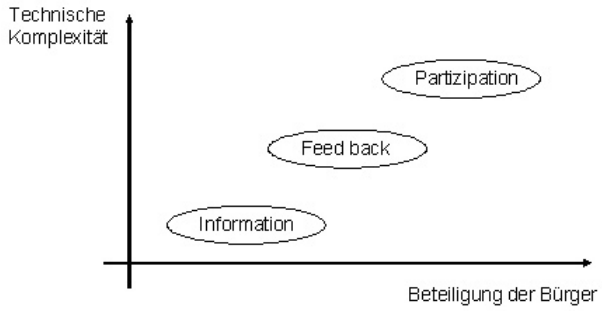
As the discussion in Austria is still very low compared to Scandinavia or the Switzerland, the Austrian Computer Society has decided to install an own working group that deals with this topic: e-democracy.

To do so, there are of course technical questions to be solved but the technology can not be seen on its own: legal and political questions are also central questions.

On one side they influence the design respectively the ability to implement such a technical system. Furthermore an information system is more than an electrification of an existing process. The information system changes the process, as it is/was the case in the private sector. The interdependencies between the technical/organizational design of a system and the legal/political surrounding are an integral part of the working group.

WHAT IS E-DEMOCRACY?

Figure 6 tries to categorise e-Democracy systems by measuring the level of participation of the citizens and the technical complexity of the respective systems.



Fig, 6: e-Democracy Systems

Systems for the sole purpose to inform the citizen respectively to provide feedback of the citizen to the politician are relatively easy to implement. For example virtual political congresses or discussions can be realised with existing technologies. Still they are not to be underestimated to support an informed decision by the citizen.

On the other side only few experiences are available with forms of electronic decision making, may it e-petitions or anonymous voting (e-voting). Especially with the latter the discussion of design and impact is also influenced by technical questions.

Especially in this area the research is in the beginning and therefore the task for the working group is to include researchers of different disciplines and companies to offer a discussion plattform for this new topic.

ACTIVITIES

The constitution of the working group took place on November 26th in 2002. After a first discussion of the topics the second meeting started with three presentations.

2nd meeting on January 28th 2003 at 3pm,
on the topic „*Technical questions of e-Democracy/e-Voting*“ with presentations of:

- Mag. Christoph Reissner, A-Trust:
  „*Die Digitale Signatur in Österreich*”
- Martin Krippner, Bearingpoint Infonova:
  „*Technische Herausforderungen von e-Voting*“
- Ao. Prof. Dr. Alexander Prosser, Institut Informationsverarbeitung (WU Wien):
  „*e-Voting.at: Einhaltung der verfassungsrechtlichen Wahlrechtsgrundsätze bei öffentlichen Wahlen im Internet*“

3rd meeting on April 4th 2003 at 3 pm,
on the topic „*Legal questions of e-Democracy/e-Voting*“ with presentations of:

- Nadja Braun, lic. iur., Schweizer Bundeskanzlei:
  „*e-Democracy in der Schweiz*“
- Dr. Patricia Heindl, Institut für Verfassungsrecht (WU Wien):
  „*Verfassungsrechtliche Implikationen der e-Democracy/e-Voting*“
- Dr. Thomas Menzel, BMBWK:
  „*Die Regelung von e-Voting im Hochschülerschafts- und Wirtschaftskammergesetz*“

4th meeting on May 26th 2003 at 3pm,
on the topic „*Socio-Political questions of e-Democracy/e-Voting I*“ with presentations of

- Mag. Peter Parycek, MAS, Donau-Universität Krems:
  „*Elektronische Demokratie auf Gemeindeebene*“
- Mag. Laurent Straskraba:
  „*Zugang des Bürgers zu öffentlichen Informationen im Rahmen von e-Government Initiativen*“
- Mag. Harald Pecival:
  „*Der überforderte Wähler - Welche Anforderungen stellen elektronische Abstimmungen an die Benutzer?*“
- Mag. Robert Kofler:
  „*Erfahrungsbericht zur Ersten Internet-Wahl Österreichs im Rahmen der ÖH Wahlen 2003 an der WU Wien*“

5th meeting on June 27th 2003 at 3pm,
on the topic „*Socio-Political questions of e-Democracy/e-Voting II*“ with presentations of

- ao. Prof. Dr. Peter Filzmaier, Universität Innsbruck, Mag. Maria Beyrl, BDF-net:
  „Wahlbörsen zu den Nationalratswahlen 2002“
- Mag. Roman Winkler, MSc (LSE), Institut Technologiefolgeabschätzung (ÖAW):
  „*Potenzial und Hemmnisse elektronischer Deliberationsprozesse für repräsentative Demokratien*“
- Dr. Robert Rittler, LLM, Verlag Medien & Recht:
  „*Politikwissenschaftliche Aspekte von Internetwahlen*“

6th meeting on October 10th 2003 at 3pm,
on the topic „*Political Education and the Internet*“ with presentations of

- Christoph Dowe, Geschäftsführer PolDi.Net :
  „*Politik-Digital.de - Ein Erfahrungsbericht*“
- Mag. Wolfgang Russ, Informationszentrum Politische Bildung:
  „*Erwachsenenbildung im Internet*“

7th meeting on January 23rd 2004 at 3pm,
on the topic „*Technical solutions for the e-Democracy*“

- Dipl.-Ing. Sonja Hof:
  „*Technische und organisatorische Sicherheit in der Praxis*“
- Peter Reichstädter, IKT Stabstelle der Bundesregierung:
  „*e-Government Gesetz und seine Anwendungen*“
- Martin Karl Unger:
  „*e-Voting auf der Seite des Wählers: Eine Anforderungsanalyse*“

8th meeting on April 2nd 2004 at 3pm
on the topic „International developments and standardisation of e-voting“

- Dr. Thomas Buchsbaum (Bundesministerium für auswärtige Angelegenheiten):
  „*e-Voting: Europäische und Internationale Entwicklungen*“
- DI Herbert Leitold (IAIK, TU Graz & A-SIT):
  „*e-Voting: Technische Lösungen und Standards*“

PUBLICATION

In November of 2003 a proceedings band on the topic „*e-Democracy: Technology, Law and Politics*“, that was published by the Austrian Computer Society:

- Alexander Prosser, Robert Krimmer (Hrsg.): „*e-Democracy: Technologie, Recht und Politik*", Band 174 der Schriftenreihe der Österreichischen Computergesellschaft, Wien 2003.

ELECTRONIC VOTING IN EUROPE

In cooperation with the European Science Foundation the working group is organizing a workshop on e-voting in Europe from 7th till 9th of july 2004. More information available at http://www.e-voting.at/ted:

Keynotes

„*Making Electronic Democracy work in Europe*“,
Michael Remmert (European Council)

„*Electronic Democracy in Austria*“
Christian Rupp (Executive Secretary for E-Government, Austrian Federal Chancellery)

„*Electronic Voting in Europe*“
Alexander Prosser, Robert Krimmer (WU Vienna, Austria)

Presentations

„*Secure Internet Voting in Spain*“
Andreu Riera, Gerard Cervelló
(Scytl Online World Security, Spain)

„*Vade-mecum for the e-Voting advocate*“
Bernard van Acker (IBM, Belgium)

„*The UK deployment of the e-electoral register*“
Alexandros Xenakis, Ann Macintosh
(Napier University, Scotland)

„*Technical Requirements of Online Voting Systems*“
V. Hartmann, N. Meißner, D. Richter
(Physikalisch-Technische Bundesanstalt, Germany)

„*E-Voting: Switzerland's projects and their legal framework – in a European context*“
Nadja Braun (Federal Chancellery, Switzerland)

„*Ask No Questions and Be Told No Lies*“
Anne-Marie Oostveen, Peter van den Besselaar
(Royal Academy of Arts and Sciences, The Netherlands)

„*How Security Problems Can Compromise Remote Internet Voting Systems*“
Guido Schryen (RWTH Aachen, Germany)

„*Transparency and e-Voting: Democratic vs. Commercial Interests*“
Margaret McGaley (NUI Maynooth, Ireland)

„*E-Voting and Biometric Systems?*“
Sonja Hof (University of Linz, Austria)

„*From Legal Standards to an E-Voting System*“
Melanie Volkamer (DFKI Saarbrücken, Germany)

„*Electronic Voting: Cryptographic or Organisational Security?*“

Alexander Prosser, Robert Kofler, Martin-Karl Unger
(WU Vienna, Austria)

„*E-Voting and the Architecture of Virtual Space*“
A. Maidou, H.M. Polatoglou (Aristotele University of Thessaloniki, Greece)

„*E-Voting: International Developments and Lessons Learnt*“
Thomas Buchsbaum (Ministry for Foreign Affairs, Austria)

„*E-Voting in Austria: Legal requirements and first legislatory steps*“
Patricia Heindl (WU Vienna, Austria)

6 The Role of Digital Signature Cards in Electronic Voting

Published at 37th Haiwaiian International Conference of System Sciences, Hawaii, 2004.

By Kofler, Robert; Krimmer, Robert; Prosser, Alexander; Unger, Martin Karl.

Abstract

As electronic voting enters the stage of real-world implementations, digital signature cards emerge as a basic infrastructure element for e-voting. The paper focuses on three main functions of such cards: (i) Authentication and (as National ID Card also) identification, (ii) as a storage media and (iii) as a secure processing environment. These properties enable protocols for secure e-voting, which guarantees the General Voting Principles.

However, the diffusion of digital signature cards is still relatively low and in many cases, electronic vote casting has to be implemented without such cards. The paper reports on a test election conducted in Austria in May 2003 using a protocol designed for digital signature cards, which was adapted to a case, where such cards are not (yet) available. The necessary adaptations clearly show the importance of digital signature cards for secure e-voting.

1. ELECTION PROTOCOLS

1.1 General Voting Principles

The General Voting Principles as specified, for instance in the Austrian Federal Constitution are [38]:

- General voting specified that nobody is to be excluded from the election; his is achieved by maintaining paper-based voting systems.

- The principle of immediate voting demands that the votes have to reach the central voting-teller directly and non-altered. The principle of equal voting demands that each individual can cast her/his vote only once and that all votes have the same weight. Of course, e-voting is a different media and cannot exactly emulate a paper-based ballot (e.g., the electronic media can guide users through complex and error-prone voting procedures thereby effectively excluding an unintentionally invalid vote; hence, a group that votes electronically has a higher potential to cast valid votes than a paper-based group; does this discriminate one against the other?). It still remains to be decided, how “equal” the two voting media have to be.

- Much more problems are in the principles of secret, personal and free voting. e-Voting poses similar problems like postal voting. In both the votes are not given within a secure polling booth, but the voters themselves must look for the secret and free voting act. Therefore postal voting is allowed only in some countries and also there only in exceptional cases.

The criteria specific to e-voting were suggested in an Internet Policy Report [18] on e-voting as (i) correctness in counting votes, (ii) dishonest voters cannot disturb the election, (iii) permanent anonymity, (iv) voters can only vote once, (v) only authorised voters may vote, (vi) independence (no undue influence is exercised on the voter), (vii) verifiability, (viii) receipt-freeness (voters cannot prove how they voted).

1.2 E-Voting Protocols: Different Approaches

There are several cryptographic approaches in the literature to implement secure e-voting:

Anonymous channel. These approaches date back to Chaum’s proposal of a MIX net [7], where the original message is encrypted with the public keys from several servers and then passed from one server to the next, each decrypting with its private key and passing the message on to the next server in large batches with a different order (mixing). The problems with this approach – which Chaum intended for a completely different application – are that at least one of the mix servers has to be honest; if, consequently, the number of servers is increased, the protocol becomes slower and more vulnerable and to prevent mixers to introduce fake votes.

Extensions of the original schema can be found in Park et al. [28] and in Sako and Kilian [33], however, both

schemes were broken ([27], [17]). Later approaches by Abe [1] and Jakobsson [19, 20] apart from algorithmic improvements add much to the stability and performance of the protocol and the computational effort in the client is reduced considerably (one collective key instead of several consecutive keys); however, it still has to be analysed and tested in prototype implementations, whether the basic difficulties in MIX nets have been completely addressed.

All-or-nothing disclosure of secrets (ANDOS). ANDOS protocols provide a sender-anonymous channel. They emulate the anonymous purchase of a bitstring [3]. This could be used in one-stage or two-stage protocols. Nurmi et al. [24] and Salomaa [34] suggested issuing voting tokens using ANDOS, which can then be used anonymously to cast a vote. There are improvements of the protocol in terms of efficiency and complexity by Niemi [22] and Hassler and Posch [15], but one of the main disadvantages of ANDOS protocols still is their limited scalability, also voters can prove how they vote, which enables vote buying.

Homomorphism. The vote is cast as a binary yes/no vote, encoded following a homomorphic scheme, and submitted to a number of ballot box servers. Due to the homomorphism the summary count of yes/no votes is possible without having to know the individual votes. [10] This advantageous property is also the main problem of the approach: Only binary votes can be cast.

Blind signature. The best known along these lines is certainly Fujioka, Okamoto and Ohta [14], which has also been implemented several times . This protocol, in spite of its popularity, has some fundamental problems concerning voter anonymity and in that fake votes for non-voters can be introduced by the administration. The problem of introducing fake votes was addressed by [4] by introducing voter pseudonyms sent through anonymous channels to all candidate servers, which are then used to authenticate the vote itself.

This adds considerable complexity to the protocol and the paper does not propose the details of the necessary anonymous channel; this would have to be subject to further research. In a later extension proposed by Okamoto [26] the problem is addressed by having several blind signature servers, anonymity relies on the usage of a MIX net with the limitations already mentioned above.

Schneier proposed an interesting extension to the blind signature voting schemes [36]. The protocol combines registration and voting in one stage and voters generate several empty ballot sheets and submit them to a registration server. The server may request the keys to open some of these ballot sheets; one is returned signed blindly. The protocol ensures that no faulty votes are blindly signed, however, the protocol does not offer any mechanism to protect anonymity other than the [14] protocol. The same applies to [5]. Both make use of MIX channels.

The blind signature approach seems to be the most promising, for it has the potential to preserve voter anonymity and to check election fraud; also, it scales well. Prosser and Müller-Török developed a blind-signature based protocol, which clearly shows to what extent the realisation of secure e-voting depends on digital signature card infrastructure.

1.3 A Two-stage Voting Protocol

Voting systems do not only have to provide secure (above all, anonymous) Internet voting on the application (=cryptographic) layer, but the system has to be considered in its entirety. Here, any type of fraud on the operating system level has to be considered as well. That is why the protocol strictly separates registration and voting stage:

Registration:

1. The registrator has one blind signature key pair (e,d) per constituency (c); each trust centre participating in the election has its (E,D).

2. The voter sends his voter ID to the registrator, which after checking the voter's eligibility answers with (c) and the appropriate (e). The voter also polls her trust centre for (E).

3. The voter creates random tokens (t) and (T) according to RSA and preparing them for a blind RSA signature (b(t), b(T), c, b(t)) and a standard text applying for a signed e-voting token is sent to the registrator, which after checking the credentials again blindly signs and returns d(b(t)). The voter removes the blinding layer and obtains d(t).

4. The voter obtains D(T) in a similar way from the trust centre.

Storage:

The voter stores t, d(t), D(T), c and her voter ID on a secure media.

Voting:

1. Some (all) candidates form RSA key pairs (k, k') and publish their respective k'. The k' are ordered (e.g., corresponding to the order on the ballot sheet).

2. On election day, the voter sends her ID and t, d(t), T, D(T), c to the ballot box server, which knows all relevant e and E.

3. If the ballot box can authenticate the tokens for the constituency indicated and if they have not already been used, it returns an empty ballot sheet BS and the relevant k'.

4. The voter codes the filled-in BS with k' and untamperably links the tokens to this k'(BS). The ballot box once again checks the tokens and stores the ballot.

After the election finished, the candidates reveal their secret k and the ballot sheets are opened.

2. THE ROLE OF DIGITAL SIGNATURE CARDS

2.1 Authentication and Identification

Digital signature cards serve as a means of authentication based on the European signature directive [11]. Anybody can access the directory server of the respective trust centre to retrieve a person's public signature key and modulus to verify the signature of a document received.

This is to be distinguished from identification, where the person's identity is to be proven. This is the purpose of a National ID Card. Austria has already issued such a card [25] based on the Central Registry (Zentrales Melderegister, ZMR). For every person residing in Austria, address information is stored in the ZMR. Also citizens from other EU countries are stored, who may vote on the municipal level. In addition, also Austrian citizen's living abroad are stored in the ZMR, if their addresses are known (e.g., when they applied for a mail ballot from abroad).

Basically, the National ID Card can be any digital signature card, which combines the digital identity of the holder (her trust centre certificate) and the real identity (the ZMR entry). This link is implemented by combining the public key (including the modulus) of the digital certificate and the ZMR number, where the combination is digitally signed by the ZMR. This is referred to as Personal Identification (PI). Hence, the card can be used as a means of identification where also the constituency can be derived from the ZMR entry. There is no need for voters to specifically register for elections.

The system described above utilises both the authentication and the identification function: In the first step, the PI is sent to the registration server to determine the voter's identity and to derive the relevant constituency. The application for an election token is signed by the cardholder (for more details, see Section 2.3 on secure processing).

2.2 Storage Media

Such separation of registration and voting, however, raises the issue of where to store the election token between registration and election day, when the token is used to request a ballot sheet and to eventually cast a vote. General storage media, such as diskettes, hard disk drives, USB keys etc. are readily available, however, they are not linked to a person, they offer no or limited protection of the data stored, and most are error-prone and may result in loss of data. Also, they enable free replication of an election token. The above protocol does prevent multiple usage of election tokens, however, it is certainly not desirable to have multiple copies of an election token, which may even be produced by a legitimate process, such as a data backup.

Hence, the logical storage media seems to be the digital signature card or the National ID Card, resp. As a suitable storage media it has to fulfil certain privacy criteria:

- The election token has to be stored PIN-protected. This can be achieved: The current card issued by the main supplier a-trust [2], for example, offers at least 2 “info-boxes” which are 2K storage areas in the file system of the card which can be PIN protected. Industry-standard card readers can write and read these areas, once they have been created on card initialisation. Since after the election the token and all other data associated with the election protocol can be deleted from the card, the info-boxes can then be used for other purposes.

- There must be no information stored on the card unprotected, which enables an application to identify the cardholder. This is a decisive qualification, as the current version of the National ID Card stores the Personal Identification and the digital certificate without any protection. This would enable a fraudulent voting application to read personal information when accessing the token.

Due to the last restriction, the current National ID Card in Austria cannot be used for these purposes. Here, it becomes obvious that the card had originally been designed for a totally different paradigm, that there is no legitimate anonymous use of the card. However, since the card has to be renewed after three years to increase key length, the above anonymity requirements can be incorporated in the next generation.

2.3 Secure Processing

One of the main concerns in electronic voting is the possibility of fraudulent manipulations of the voter’s PC or voting terminal. In some respects, this seems to be the primary concern in e-voting and the major impediment for implementing e-voting [18].

Digital signature cards, however, have the same problem in their basic function, that is digital signatures: A document could be displayed to the prospective signor and when it comes to the digital signature process a fraudulent programme resident on the signor’s terminal could modify the document that is actually signed. This would undermine the entire system to the same extend as would the possibility to forge digital signature keys.

However, this problem was solved by Secure Viewers, which provide a secure tunnel between a viewing application which displays the document to be signed and the signature card. The signor can be assured that the document displayed and the byte string sent, compared to the digital signature card are identical. Therefore, the argument that e-voting is impossible because the PC is an insecure terminal per se cannot be maintained.

The algorithm proposed in Section 1.3 utilises the Secure Viewer delivered with the Austrian National ID card for signing the application for an election token and for displaying critical data stored on the card before it is released. Thereby the decisive elements of the protocol run in the operating system of the National ID Card.

This imposes additional requirements on the command set implemented in the operating system of the card.

3. SUBSTITUTING THE FUNCTIONS OF A DIGITAL SIGNATURE CARD

Although postal (absentee) voting is not enabled in Austria for National Elections, e-voting has been enabled for elections to the student union parliament based on §34 of the Student Union Law (HSG 2001).

For the acceptance of e-voting a study has been conducted right after the last Student Union Elections in June 2001, where two issues were under concern: (i) whether or not the students want to elect their representatives over the Internet and if (ii) e-Voting will replace traditional voting in the near future. In the study of the 1033 participating students 83,6 % prefer e-voting over booth voting and 71 % are of the opinion that e-voting will replace traditional forms of voting. [21]

For the results of the Internet election, e-voting.at defined two hypotheses: (H1) e-voting raises the voter turn out and (H2) e-voting results in the same results in the digital voting process as in the paper based voting process.

Since digital smart cards were not available in sufficient quantities, the implementation of the algorithm described in Section 1.2 was adapted for a test election without using the infrastructure of digital signature cards.

This replacement clearly shows where the value added of signature and National ID Cards is and it reveals the difficulties to realise secure e-voting without them. (Figure 1 provides an overview).

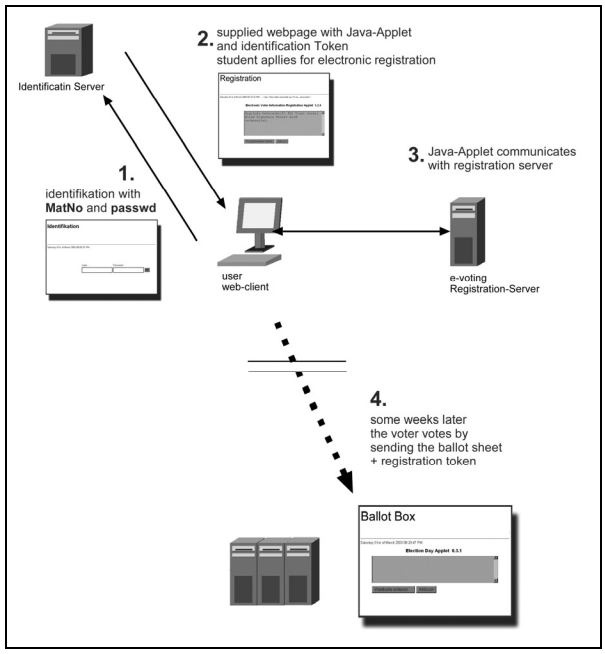


Figure 1: System used for the test elections

3.1 Authentication and Identification

Step 1. In contrast to the original algorithm the student does not use her student ID card with the digital signature but identifies herself with a standard login procedure. This is done at a webpage of an inhouse identification system by entering the student identification number and their password.

Step 2. This system identifies the students and sends them a different via SSLv3 secured webpage which contains

(1) The unique identification token and
(2) The Registration Applet

This unique identification token is used to pass on the identification information from the service provider (in this case the university's IT department) which removes the necessity for the organization conducting the election to pass on individual data to service pro-

vider of the voting process. To do so this unique identification token consists out of several components:

(e,d) ..... RSA keypair of identification unit
MatNo..... Student's identification number
S..... secret number, only known to the identification unit
tokentime ... is a Unix timestamp

The unique token is generated by adding the secret number S to the unique student information number MatNo and hashing this information using SHA1, then adding a timestamp and finally signing the data with the private key of the identification unit. This includes the following properties: (i) this identification token can only be created by the identification unit, as it is signed with its private and secret RSA-key (d) so nobody else can calculate it, (ii) the combination of SHA1-encryption and (MatNo+S) guarantees a unique primary key in the registration database which cannot be decrypted and finally (iii) the timestamp is used to prevent resend-attacks by somebody who cracks the SSLv3/TLS-Protocol – therefore the identification unit and the registration unit must synchronize their system time. The timeout is calculated between the token time and the system time of the registration server. Useful values are between 15 and 30 seconds.
This unique token is then passed on to the registration unit.

Step 3. The registration server decrypts the token with the public-RSA key (e) of the identification unit and calculates the validity of the token time. If the token time is valid the registration server compares the "SHA1(MatNo+S)-part" of the token with its registration database and when TRUE it returns the constituency specific public key, so that the Applet can process its numbers for the blind signature and the token can be stored on a medium of choice of the student. The usage of the token is as described in Section 1.3.

3.2 Secure Storage

The test election system uses an arbitrary storage media where PIN protection of files is not available. Hence a different approach was chosen.

The voter chooses a password which is used as a secret key to encrypt and to decrypt the electronic voting permit. The electronic voting permit is encrypted with a user-supplied password before it is written into a file on the storage medium.

After the file which contains the electronic voting permit is read from the storage medium, the user is prompted to enter the password. The password is used to decrypt the electronic voting permit.

The file which contains the electronic voting permit can be accessed without knowledge of the password, but without entering the correct password it will not be possible to use that file for casting a vote.

3.3 Secure Processing

This point clearly shows how essential the use of smart cards for e-voting is. Literally nothing could be supplied to replace the security offered by the combination of a protocol run in the protected environment of the digital signature card and the Secure Viewer on the other.

That is why we hold that full compliance with the General Voting Principles can only be assured by the use of digital smart cards.

4. SUMMARY

The paper outlined a digital signature card-based protocol for remote Internet voting and its requirements in terms of security. The central hypothesis is that secure voting following the General Voting Principles can only be implemented using digital signature cards as a secure processing and storage environment.

The voter turnout for the test election has been 36%; the real paper-based student union election could attract 26%, hence the turn-out in the electronic election was 40% higher than in the conventional, paper-based system.

A “workaround” solution that can be applied in the absence of digital signature cards was proposed. Such a system can substitute a National ID Card to some extent in terms of identification and authentication and secure storage, but it also shows the limitations of a non-smart card-based approach.

References

[1] Abe M.: Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Centers. In: Advances in Cryptology - EUROCRYPT '98, Springer-Verlag, Berlin, 1998, pp. 437-447

[2] a-trust: Certificate Policy für qualifizierte a.sign Premium Zertifikate für sichere Signaturen, Version 1.0, Vienna, 2003

[3] Brassard, G., Crepeau, C., Robert, J.-M.: All-or-Nothing Disclosure of Secrets. In: Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86, Berlin, Springer Verlag, 1987, pp. 234-238

[4] Baraani-Dastjerdi A., Pieprzyk J., Safavi-Naini R.: A Practical Electronic Voting Protocol Using Threshold Schemes. In: Center f. Computer Security Research, Department of Computer Science, University of Wollongong, Australia, 1994

[5] Borrell J., Riera A.: Practical Approach to Anonymity in Large Scale Electronic Voting Schemes. In: Universitat Autónoma de Barcelona, Departament d´ Informática, Catalonia, Spanien, 1999

[6] Chancellerie d´Etat de Genève: Cahier des charges e-voting. In: http://www.geneve.ch/chancellerie/e-government/cahier_charges.html accessed on 2003-03-05

[7] Chaum, D.: Untraceable electronic mail return addresses and digital pseudonyms in: Communications of the ACM, Vol. 24(2), 1981, p. 84-88

[8] Chaum, David :Blinding for Unanticipated Signatures. In: Chaum, David; Price, Wyn (Ed.):Advances in Cryptology, EUROCRYPT ’87.Springer-Verlag,Berlin 1987, S.227 –233

[9] Cranor, L. F., Cytron, R. K.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: Proceedings of the Hawai International Conference on System Sciences (HICSS-97). Hawai 1997. http://lorrie.cranor.org/pubs/hicss/hicss.html accessed on 2001-02-04

[10] Cramer R., Gennaro R., Schoenmakers B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology-EUROCRYPT'97, Lecture Notes in Computer Science 1233, Springer-Verlag, Berlin, 1997, pp. 103-118

[11] European Union: Directive 1999/93/EC, http://www.qlinks.net/comdocs/elsig/ accessed on 2002-12-04

[12] Feghhi, J.; Feghhi, J.; Williams, P.: Digital Certificates – Applied Internet Security. Addison-Wesley, Reading 1999

[13] Gemeinde Fellbach.: Jugendgemeinderat Fellbach. http://www.fellbach.de/wahlen accessed on 2001-11-20.

[14] Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology – AUSCRYPT92. Springer-Verlag, Berlin 1993, pp.244 –251

[15] Hassler, V. Posch, R.: A LAN voting protocol. In: IFIP/SEC 95, Capetown, 1995, pp.154-167

[16] Horster P., Michels M., Petersen H.: Blind Multisignatures and their relevance for Electronic Voting. In: IEEE-Press, 11th Annual Computer Security Applications Conference, 1995, pp. 149-156

[17] Horster P., Michels M.: Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme. In: Asiacrypt´96, LNCS 163, Springer-Verlag, Berlin, 1996, pp. 125-132

[18] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC), 2001. http://www.internetpolicy.org/research/e_voting_report.pdf, accessed on 2001-11-20

[19] Jakobsson M.: A Practical Mix. In: Advances in Cryptology - EUROCRYPT '98, Springer-Verlag, Berlin, 1998, pp. 448-461

[20] Jakobsson M.: Flash Mixing. In: Information Sciences Research Center, Bell Labs, New Jersey, http://www.bell-labs.com/user/markusj (2002-11-19)

[21] Krimmer, R.: e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen, Thesis, WU Vienna, Vienna, 2002

[22] Niemi V.: Cryptographic protocols and voting. In: Results and Trends in Theoretical Computer Science, Springer LNCS, Springer-Verlag, Berlin, 1994, pp. 307-316

[23] Niemi V., Renvall A.: How to Prevent the Buying of Votes. In: Advances in Cryptology-Asiacrypt´94, Springer-Verlag, Berlin, 1995, pp. 164-170

[24] Nurmi, H., Salomaa, A.; Santean, L.: Secret ballot elections in computer networks. In: Computers and Security 36 (1991) 10, pp. 553 –560

[25] OCG: Austrian Computer Society Membership Card, Vienna, http://members.ocg.at/ accessed on 2002-12-05

[26] Okamoto T.: An Electronic Voting Scheme: IFIP´96, Advanced IT Tools, Chapman and Hall, London, 1996, pp. 21-30

[27] Pfitzmann B., Pfitzmann A.: How to Break the Direct RSA-Implementation of Mixes. In: Eurocrypt 89, Springer-Verlag, Berlin, 1989, pp. 373-381

[28] Park, C., Itoh, K., Kurosawa, K.: All/Nothing Election Scheme and Anonymous Channel. In: Lecture Notes in Computer Science 765, Advances in Cryptology Eurocrypt 93, Berlin, Springer Verlag, 1994, 248-259

[29] Prosser, A., Müller-Török, R.:Electronic Voting via The Internet. In: 3rd International Conference on Enterprise Information Systems ICEIS-2001, Setubal 2001, pp. 1061–1066

[30] Prosser, A., Müller-Török, R.: Ein Algorithmus zur sicheren elektronischen Stimmabgabe über das Internet. Proceedings of the International Conference on Operations Research OR 2002, Klagenfurt, 2002

[31] Prosser, A., Müller-Török, R.: E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. In: Wirtschaftsinformatik 44(2002) 6, pp. 545-556

[32] Rivest, R.: Cryptography and Information Security Group Research Project: E-Voting. In: http://theory.lcs.mit.edu/~cis /voting/voting.html accessed on 2001-11-19

[33] Sako, K., Kilian, J.: Receipt-Free, Mix-Type Voting Scheme. In: Lecture Notes in Computer Science 921, Advances in Cryptology Eurocrypt 95, Berlin, Springer Verlag 1995, pp. 393-403

[34] Salomaa, A.: Verifying and Recasting Secret Ballots in Computer Networks. In: Maurer, H.A. (ed.): New Results and New Trends in Computer Science, Springer-Verlag, Berlin 1991, pp.283 –289

[35] Soundcode VoteHere Inc.; Compaq Computer Corp.; Cisco Systems Inc.; Entrust Inc.: VoteHere Gold.Soundcode Inc.,Bellevue, 2001 http://www.soundcode.com/ voteheregold.html accessed on 2001-07-20

[36] Schneier B.: Applied Cryptography, Addison-Wesley, Boston, 1996

[37] Tilborg van, H.C.A.: Fundamentals of Cryptology. Kluwers Academic Publishers, Boston 2000

[38] Walter, R; Meyer, H.: Grundriß des österreichischen Bundesverfassungsrechts. 9th ed., Manz Verlag, Vienna 2000

7 History of E-Voting.at

2000 Preliminary work involving algorithmic and cryptographic research. At a very early stage, members of the current project team were involved in the wording of an addendum of the Austrian Chamber of Commerce and the Austrian Student Union Law enabling e-voting for their elections.

2001 Laws on e-voting for Chamber of Commerce and Student Union Elections were passed by the Austrian Parliament. The project was initiated in mid-2001 with four members at the department of Information Science at the University of Economics and Business Administration, Vienna (WU), who until today form the project team. The first sponsor was the City of Vienna, whose grant was used to develop the original prototype, which implements a two-stage voting procedure: (i) identification and authorisation of the voter, who obtains a voting token that can be used to (ii) anonymously cast a vote on election day. A research co-operation was founded with the Institute of Constitutional and Administrative Law at WU. A project advisory committee was established headed by the President of the Austrian Federal Council.

2002 A first version of the e-voting prototype was released for public download including publicly available system documentation; the test election in 2003 was prepared with usability tests in the focus group. The working group "e-democracy" in the Austrian Computer Society was founded by the project team, www.e-voting.at was founded as a discussion forum for e-democracy in Austria. A first international co-operation was established with the Swiss Federal Chancellery.

2003 Version 2 of this prototype was released incorporating limited support of an election committee for supervision of the election process, identification and authentication using National ID/signature smart cards. It was used in a field trial in May 2003 at a test election parallel to the student union election at WU (registration for voting tokens 1st – 19th Mai, voting 20th – 22nd May). 978 students were eligible, 410 obtained an election token and 355 cast a vote using the system. The paper-based election showed a voter turnout of 26% as compared to 36% in the e-voting trial. Co-operations were established with the Austrian Foreign Ministry and the Institute for Interdisciplinary Research at Klagenfurt. International research co-operations were established with the Teledemocracy Centre at Napier University (Scotland), the German Federal Ministry of the Interior and the Information School at the University of Washington.

2004 Version 3 of the e-voting prototype was released, which incorporates full support for the election committee supervising the election process, multi-language support and enhanced robustness in view of hardware and connectivity failures. A test election parallel to the election for the Austrian Federal President was conducted with 20,000 eligible participants (registration 22nd March – 22nd April, voting 23rd – 25th April).