Robert Krimmer

Internet Voting in Austria: History, Development, and Building Blocks for the Future

Thesis

DOKTORAT DER SOZIAL- UND WIRTSCHAFTSWISSENSCHAFTEN

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

1. Beurteilerin/1. Beurteiler: **ao.Univ.Prof. Mag.Dr. Andreas Mild**

2. Beurteilerin/2. Beurteiler: **o.Univ.-Prof. Dr. Alfred Taudes**

Eingereicht am: _____

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Titel der Dissertation:

Internet Voting in Austria:
History, Development, and Building Blocks for the Future

Dissertation zur Erlangung des akademischen Grades

einer Doktorin/eines Doktors

der Sozial- und Wirtschaftswissenschaften an der Wirtschaftsuniversität Wien

eingereicht bei

1. Beurteilerin/1. Beurteiler: **ao. Prof. Dr. Andreas Mild**

2. Beurteilerin/2. Beurteiler: **o.Univ.Prof. Dr. Alfred Taudes**

von **Dr. Robert Krimmer**

Fachgebiet: **Wirtschaftsinformatik**

Wien, im **September 2017**

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Ich versichere:

1. dass ich die Dissertation selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

2. dass ich diese Dissertation bisher weder im In- noch im Ausland (einer Beurteilerin/ einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

3. dass dieses Exemplar mit der beurteilten Arbeit übereinstimmt.

Datum _____ Unterschrift _____

Internet Voting in Austria:
History, Development and Building Blocks for the Future

A dissertation submitted to the

WU Vienna University of Economics and Business

Department of Information Systems and Operations

Institute for Production Management

to obtain the degree of
Doctor of Social and Economic Sciences

by

Robert Krimmer

2017

Abstract

This dissertation aims to investigate the origins of Internet voting, analyze several deployments of Internet voting technology in Austria and identify – based on these accumulated experiences – building blocks that can be useful in decision-making on and planning of future uses of Internet voting technology within Austria and throughout the world.

In line with the goals of this thesis, it will address the following research questions:

- How did Internet voting originate?
- What experiences were noted in the process of implementing Internet voting in Austria?
- What building blocks can be identified for developing future Internet voting both inside and outside Austria?

Internet voting is part of a transformational movement that applies information and communication technologies to daily business activities. It is only logical that elections are also considered for applying electronic (remote) communication technologies. While early efforts were driven by the belief that elections could make easy use of the Internet, it was shown that while the principles have to be interpreted and consequently applied in a different way, the same principles can still be derived for Internet voting, like integrity, secrecy, transparency, accountability and public confidence. The need to have forms of decision making in electronic networks has been identified in its beginnings and has received continuous attention throughout its development. At the height of the excitement about the possibilities of the Internet, countries raced to become the first to run a legally binding election using electronic voting systems. While several candidates emerged (e.g., Costa Rica, Bosnia Herzegovina, Germany, United States), Estonia was victorious in 2005. To date, Estonia is the only country that has introduced this form of voting without any preconditions or other limitations.

In Austria, the intentions to use information and communication technologies (ICT) in elections concentrated on parliamentary affairs. Spurred by the efforts around student elections in Germany, Austria sought to conduct Internet voting in 2000. In the years thereafter, considerable progress was made at WU Vienna University of Economics and Business (WU), and this progress spearheaded the debate in the early 2000s. At the beginning in the years 2001-2003, technical solutions were sought to verify voter eligibility and maintain voter privacy. Later, more sophisticated algorithms were developed, and functionalities like quotas in election commissions were added.

The Federation of Students' elections in 2009 were a remarkable event that demonstrated highly contentious political debate around the topic. This debate continued after the elections, which were held in May 2009 and suffered from the intense debate and protests and consequential organizational shortcomings. The experiences also showed that accurate legal regulations are needed to show interaction with the constitutional legal texts and to ensure accountability to a remote electronic voting channel through legal means. International standards were a first step, but regulations based on actual experience were needed to show how remote electronic voting channels could be realized and how to avoid problems identified in pilot implementations. This practical knowledge also shows that sophisticated algorithms are not always the key to success. Rather, several key implementations make use of very basic technical means to realize the tasks given by law. One should not forget about the voters. They not only need to use such systems, but they also need to understand the processes in order to build trust.

The constitutional court ruling lifted the election and ruled that the respective ordinance was not in line with the requirements of the law. Hereby, the court established higher requirements resulting barriers for offering Internet voting channels in future elections. While the election administration system, which was a pre-requisite for the Internet voting system, was discontinued in the election thereafter, it returned in recent elections where postal voting was offered.

On the basis of the aforementioned experiences, twelve building blocks were compiled discovered. These include design decisions, such as the following: the form of electronic voting, adaptations of the legal base, the technical means for identification and secrecy, observation, control functions for the electoral commission, evaluation processes, transparency functions, ballot sheet designs, controlling the organizational context as well as providing options for planning and implementation. This framework therefore facilitates and eases the generation of feasibility studies and other analyses and decision making ahead of using Internet voting in an election. With little adaption it can also be used for the use of other voting technologies.

This work utilizes theoretical work and knowledge from adaptations of legal texts. These texts cover a wide range of topics, including methods for implementing identification and anonymity functions in remote electronic voting as well as testing and certifying systems that require transparent procedures. The findings also show that implementing remote an electronic voting system is a complex topic. It requires trust in the election administration; otherwise, suspicion will arise when more technology is introduced and implemented in an election process. Remote electronic voting is one of the most challenging information technology (IT) projects. Most Internet approaches do not allow for voter anonymity. Also, elections have a fixed date; therefore, they must take place whether or not the system is ready.

Contents

List of Figures

List of Tables

1 Scope and Aim

This dissertation investigates the origins of Internet voting, analyzes Internet voting technology deployments in Austria and identifies basic building blocks from these accumulated experiences to inform future Internet voting systems within Austria and throughout the world.

Similar to the rest of the world, the emergence of the Internet in the 1990s led people to believe that an Internet-based election may allow voting at any place and any time. This idea reached the general political debate when the Federation of Students' elections *Hochschülerinnen- und Hochschülerschaftswahlen* in May 2009 offered the possibility to cast a binding vote in an election regulated by federal law for the first time. While this premiere was assessed by the general public as a failure, it nevertheless delivered very important lessons for the future.

Surprisingly, the origins of electronic voting (E-Voting) in Austria can be traced back to the beginning of parliamentarism during the Habsburg Monarchy. The first person to propose using electricity for conducting votes in the Habsburg Parliament was the inventor and Austrian telecommunication pioneer Carl Albert Mayrhofer in 1863.[1] He put forth a petition on 17 September to the *Abgeordnetenhaus* (Mayrhofer, 1863). Voting at that time required the members of parliament (MPs) to either stand up or remain seated in order to show their approval or disapproval. His arguments included that, with the use of electricity, the voting process could be conducted in less time and in a more efficient and secure manner. In addition, he argued that it would allow for a secret vote. Nevertheless, the MPs did not take his proposal seriously and simply referred the petition to the parliamentary committee for changing the rules of procedure. Several years later, between 1878 and 1883, Mayrhofer undertook another attempt to improve the voting process, which was motivated by the ongoing construction for the new Parliament located

[1] He was the first private operator of a telegraphic service as well as a network for pneumatic tube mail within Vienna (Herzog and Pensold, 2010).

at the *Ringstraße*. He had further refined his proposal and replaced the use of electricity with pneumatics, which was criticized by others (Zetsche, 1881). He had invented this mechanism for the purpose of synchronizing clocks within the city limits of Vienna and Paris (Sánchez Miñana, 2010). In 1878, he had exhibited a prototype of his machine in the parliament of Lower Austria, written a petition to the *Herrenhaus* and published a pamphlet discussing various arguments in favor of the new voting mechanism (Mayrhofer, 1880). His endeavors even nurtured the development of a competing solution by Josef Schaller and Wilhelm Hauck. Nevertheless, neither petition resulted in the installation of voting technology in the Austrian parliament (Haus der Abgeordneten des österreichischen Reichsrathes, 1880).

As far as my research has determined, this was the first documented attempt to introduce an electronic means for a public voting process. In Austria, unlike in the United States, Germany, the Netherlands and France, inventors were not successful in advancing mechanical or electronic technologies for casting votes until the new millennium. In this regard, the developments in Austria related to Internet voting between 2000 and 2010 can be considered a novelty.

In order to accomplish the goals of this thesis, the following research questions were formulated:

- How did Internet voting originate?
- What experiences occurred when implementing Internet voting in Austria?
- What building blocks can be identified from these experiences, and how can they be used to inform future Internet voting systems within Austria and throughout the world?

The dissertation is based on practical and theoretical work regarding Internet voting in Austria. This includes actual implementation research as well as presentations and discussions of this work at several conferences and research venues. It also includes personal conversations with decision makers within Austria and throughout the world.

Parts of this thesis have been previously published as research articles as detailed below. These articles were either used in full or in parts, and they have also been expanded upon for this thesis. The articles focus on analyzing as well as developing an Internet voting solution for the Austrian context. They draw upon international experience as well.

- Chapter 2 focuses on the historic development of Internet voting as well as early efforts and legal constraints. This chapter is based on the following publications:

  - Gibson, J. Paul, **Krimmer, Robert**, Teague, Vanessa, Pomares, Julia (2016): A Review of E-Voting: the past, present and future, Springer Annals of Telecommunications, (71) 7, p. 279-286;

  - **Krimmer, Robert**, Triessnig, Stefan, Volkamer, Melanie (2007): The Development of Remote E-Voting around the World: A Review of Roads and Directions. In: Alkassar, Ammar, Volkamer, Melanie (Eds.): *E-Voting and Identity – VOTE-ID'07*, LNCS Vol. 4896, Springer, Berlin, 1-15; and

  - **Krimmer, Robert** (2016): Constitutional Constraints for the Use of Information and Communication Technologies in Elections, Electoral Expert Review, Special Issue, 28-35

- Chapter 3 focuses on experiences with Internet voting in Austria and is based upon the following publications:

  - **Krimmer, Robert**, Lehner, Christoph, Stangl, Siegfried, Varga, Bernhard, Stein, Robert, Wenda, Gregor, Kozlik, Johannes (2009): E-Voting im Rahmen der Wahlen zur Österreichischen Hochschülerinnen- und Hochschülerschaft 2009. In: Hauser, Werner, Kostal, Mario (Eds.): *Jahrbuch Hochschulrecht*, Neuer Wissenschaftlicher Verlag, Wien, 539-551;

- **Krimmer, Robert**, Ehringfeld, Andreas, Traxl, Markus. (2010): The Use of E-Voting in the Federation of Students Elections 2009. In: Krimmer, Robert, Grimm, Rüdiger (Eds.): *Proceedings of EVOTE2010*, LNI Vol. 167, GI, Bonn, 33-44; and

- **Krimmer, Robert**, Ehringfeld, Andreas, Traxl, Markus (2010): Evaluierungsbericht – E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009, Bundesministerium für Wissenschaft und Forschung, Wien.

- Chapter 4 focuses on the building blocks of Internet voting systems and is based upon the following publications:

  - **Krimmer, Robert** (2014): Identifying Building Blocks of Internet Voting: Preliminary Findings, Proceedings of Informatik 2014, GI LNI Vol. 232, p. 1381-1389; and

  - **Krimmer, Robert** (2016): Verifiability: a New Concept Challenging or Contributing to Existing Election Paradigms? 13th EMB Conference. Council of Europe.

The thesis consists of three parts, as shown above. The first part gives an overview of the early experiences and legal constraints of Internet voting in chapter 2, the second presents the collected experiences in Austria in regard to Internet voting in chapter 3 and the third part analyzes this and uncovers the building blocks for Internet voting in chapter 4.

2 History of Internet Voting

In this chapter, we will analyze the historic origins of Internet voting, the first Internet voting efforts and the frame that constitutions and legal frameworks provide.

2.1 Roots

Using information and communication technologies for elections has always been a common theme for elections. We can differentiate two main forms that are used within elections—those being conducted in controlled (voting in polling stations) and uncontrolled environments (remote voting). Postal voting is the earliest example of remote voting— early ideas can be traced back as far as the Roman Empire (Staveley, 1972)—that depends on an underlying communication network to properly function. More reliable records date back to the seventeenth century where postal voting was allowed for merchants in Switzerland (Braun, 2006). Postal voting is still used in many elections around the world, and it is the standard against which remote electronic voting is most often compared (Krimmer and Volkamer, 2005). The next major communications infrastructure that facilitated remote voting was the telephone network, which has provided an alternative voting procedure for a specific subset of the electorate—usually those with disabilities—in a small but significant number of democratic elections. The telephone network is also used to support convenience voting (Gronke et al., 2008), including voting by FAX. In contrast to the primitive technology used in postal voting, some American astronauts have been able to vote from space since 1997; the first American to do so was David Wolf, who was living on Russia's Mir Space Station and was granted special disposition to remotely vote by his home state of Texas.[2]

Since then, there has been much research regarding remote voting using the Internet. As the Internet evolves, we expect that remote voting systems will also evolve. As we progress towards cloud services and virtual networks (Fernandes et al., 2011), then the

[2] http://www.nasa.gov/mission pages/station/expeditions/expedition18/vote.html

future of remote voting may be simply another trustworthy e-government service (Carter and Bélanger, 2005) that is run on the cloud (Zissis and Lekkas, 2011). Configuring and running elections on a virtual machine is certainly appealing, but we must address the problems associated with Internet voting in general before we can examine the additional complexities introduced by virtualization.

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

The foundations of Internet voting are found in the democratization movement and the general availability of mass electronic media (e.g., television) after the second world war. At the same time, at this time, the Internet was simply a network of distributed computers, communicating using packets of information (Davies et al., 1967). During this time, the idea of enhancing democracy through the use of electronic means was supported by several bright minds (Dahl, 1956, Zittel, 2001) in order for 'democracy to finally come true' (Fuller, 1963).

The idea of enabling remote voting through electronic means needed some time before it could be implemented. Similar to the developments associated with paper voting, first implementations of remote electronic voting focused on recording votes without necessarily guaranteeing secrecy. In a first attempt, Murray Turrof came forward with an implementation of a group-based decision-making process in a closed networked environment in the 1970s (Turoff and Hiltz, 1977). He started his work while the Internet mainly served as an exchange for data between researchers. He used a decision-making process based on the Delphi method (for an introduction, see Häder [2009]), which is usually structured in two phases: first, the experts gather ideas; then, they vote on their personal preference for these proposals. While limited to experts and closed networks, it still constituted one of the first implementations of an electronic voting process that included voting from remote locations.

While it was possible in the closed networks to use some more complex decision-making rules, more simple forms of decision making were possible with the general public. Here, the mass media – and with it the general availability of the (color) television that soon became a ubiquity – played an important factor. For many, including Etzioni (1972), Becker (1981) and Vowe and Wersig (1983), the emergence of cable TV brought with it the possibility of bi-directional communication and allowed electronic town hall meetings to be held. However, due to the high costs for bi-directional switches and hubs, the cable networks only allowed for uni-directional broadcasting of TV programs[3]. Due to this deficit in infrastructure, these hopes did not materialize. A different mass communication technology brought more success for participatory and voting means: the telephone and 'televoting'[4]. Televoting was used in the U.S., for example, in Hawaii for public deliberative polling (Slaton, 1990). In Austria, Alton-Scheidl (1997) implemented a similar effort with his so-called 'Grätzltelefon', a public messaging board, where one could call a telephone line and leave messages for public deliberation. However, it was only implemented for one pilot case in Austria and did not find further adoption. One of the identified issues was that it was very hard to communicate the technical parts of the projects to the general public.

Following the model of the British Post Office's view data service (Bright, 1979), in the early 1980s, many European telecoms introduced publicly available telecommunication networks that were accessible through special terminals. *Minitel*, the French implementation of view data, was the most successful, with several million of installed terminals. In Germany and Austria, the system was called *Bildschirmtext* or short *BTX*, and its success was limited. Common to all of these first public data networks were

[3] This only changed with the need for broadband Internet access through the means of cable TV networks that led to a considerable amount of investment in this infrastructure in the 1990s.

[4] For a discussion of security concerns with regards to voting by phone, see Saltman (1990).

many different applications, such as each country's phone book in electronic format.[5] In some cases, these systems offered simple voting applications. In Germany, where the newly formed Green party agitated against the systems' introduction, a treaty of all German *Länder* required that any public polls using *BTX* had to ensure the anonymity of the participants (Kuhn, 1984).

Given the technical possibilities of the *BTX* system, it must have been clear that anonymity can only be guaranteed organizationally, and hence, for political voting, more sophisticated technical solutions would be needed.

The first online polls were rather easy to realize technically, because secrecy was not required, or it was sufficient to rely on the organizational guarantees of vote secrecy. The first efforts that would minimize the requirements to the organizational context were developed in the context of asynchronous cryptography. Most proposals during this time were associated with secure multi-party communications (Schoenmakers, 1999), for which elections turned out to be an interesting application field. For an overview of early proposals and protocols, see Horster and Michels (1995).

[5] In Austria, WU was one of the largest content providers, and they offered their students the possibility to register for university courses online (Göpfrich, 1985).

After the first theoretical discussions, some researchers were followed with implementations such as the Sensus system by Cranor and Cytron (1997) or the Cybervote system (EU, 2000), which was one of eight projects within the EU 5th Research Framework program featuring research related to E-Voting[6]. Since then, subsequent EU framework programs have provided no further funding related to E-Voting to date.

At the time, several new economy start-up companies focused on realizing Internet voting, such as *Election.com*, *Safevote.net* or *Votehere.net*.

With this increasing interest, a 'political race' began in the mid-1990s to be the first country to allow Internet voting in general elections. At the time, it seemed to be only a matter of time rather than a question of technical feasibility—particularly after Bill Clinton ordered further investigation of the issues at the end of 1999. The resulting report was published at the beginning of 2001 (Mote et al., 2001), but the events in the November U.S. presidential elections (Bush vs. Gore) focused American attention on the integrity and auditability of election results. Most Internet voting trials have taken place outside the U.S. The following chapter provides an analysis framework for these early efforts.

2.2 Early Internet Voting Efforts

The development of an electronic democracy with a transnational character (Held, 1999) needs the further development of e-enabled instruments of democracy (Heindl et al., 2003), including e-initiatives, e-referenda and E-Voting instruments. Amongst them, remote E-Voting has received the largest attention, and it reached the national level in

[6] These included, in addition to CYBERVOTE http://cordis.europa.eu/project/rcn/52634_en.html, the following projects: EVE, http://cordis.europa.eu/project/rcn/57874_en.html; AGORA 2000, http://cordis.europa.eu/project/rcn/52651_en.html; DEMOS, http://cordis.europa.eu/project/rcn/52637_en.html; E-POLL, http://cordis.europa.eu/project/rcn/57444_en.html; EURO-CITI, http://cordis.europa.eu/project/rcn/52635_en.html; WEBOCRACY http://cordis.europa.eu/project/rcn/52649_en.html; and EDEN, http://cordis.europa.eu/project/rcn/57135_en.html.

Estonia first. On March 3, 2007, the Estonian national election offered the world's first legally binding remote e-voting possibility (Estonian National Electoral Committee, 2007). With that event, remote E-Voting finally gained international attention even though experts warned three years earlier in the SERVE report that the internet was not yet ready to support elections (Jefferson et al., 2004). Today, most other nations are still in the phase of experimentation. To date, most trials do not follow classical experimental setups (Alvarez and Hall, 2004) and are embedded in their national context (Svensson and Leenes, 2003), which makes comparison and learning from others difficult.

This analysis was the first attempt to conduct a state-of-the-art analysis (Fettke, 2006) of 104 remote E-Voting uses of Internet voting between 1995 and 2007. We analyzed research articles, working papers and press releases of 104 e-elections conducted around the world. While we aimed to obtain a representative sample, it is clear that the current cases cannot serve this purpose. Rather, they give an indication of how remote E-Voting has developed so far. In the following, we will first provide theoretical background regarding remote E-Voting; then, we will present the results of our review. Finally, we will discuss the findings and provide conclusions.

2.2.1 Theoretical Background

In this chapter, we will define remote electronic voting and explain our research methodology.

2.2.1.1 The terminus technicus remote electronic voting and its variants

Definition. The Council of Europe recommendations define electronic voting as "the use of electronic means in at least the casting of the vote" (Council of Europe, 2004). We first must consider elections in a broad sense (for our purposes, this includes e-referendums) and then concentrate on the implications of ICT usage therein.

The Electoral Process. The United Nations facilitated the agreement on the International Covenant on Civil and Political Rights (United Nations, 1966). Article 25 defines eight principles for elections that depict the entire electoral process: (i) periodic elections, (ii) genuine elections, (iii) stand for election, (iv) universal suffrage, (v) voting in elections on the basis of the right to vote, (vi) equal suffrage, (vii) secret vote and (viii) free expression of the will of the voters. Suksi (2005) groups these principles into a cycle consisting of three periods:

1. Pre-Election Period: The period from calling an election until the actual start of the polling.
2. Election Period: The actual Election Day when the voting takes place.
3. Post-Election Period: The period during which the results are announced and a new election is called.

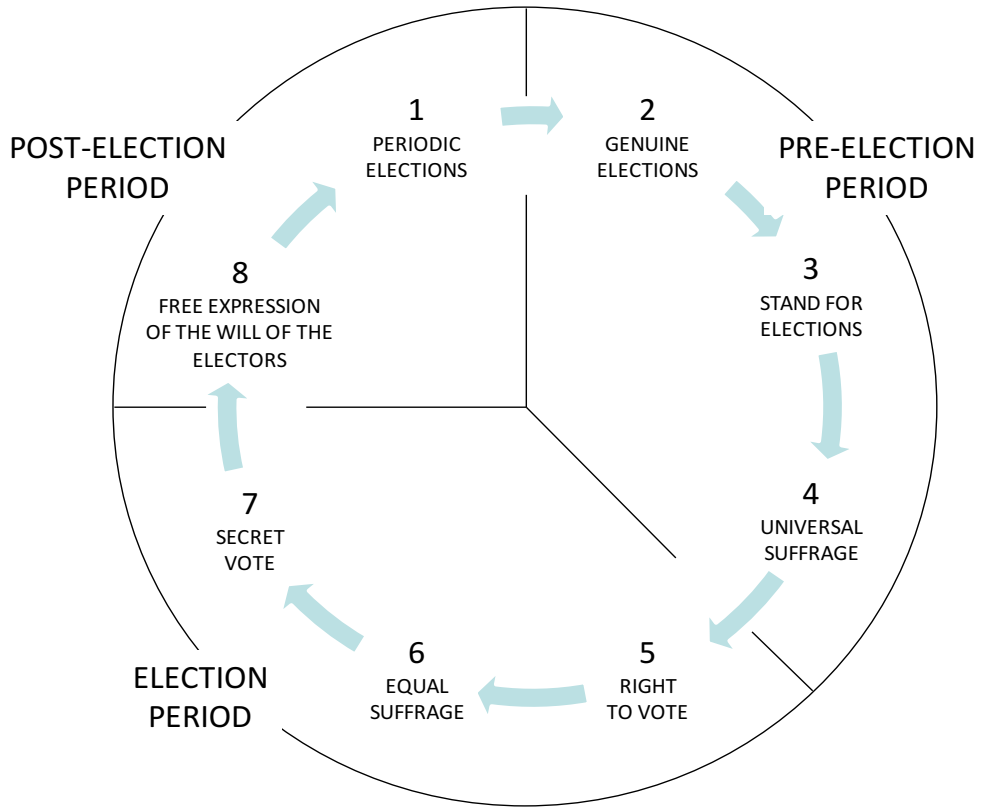

Figure 1: The Electoral cycle (Krimmer, following (Suksi, 2005))

Local/Remote. The electoral process usually takes place at the polling station and is supervised. This can be referred to as voting at presence. There is also the possibility of remote voting. The criterion to differentiate those two is if an election commission supervises the act of voting or not (Krimmer, 2002). At current elections, the voter comes to the polling station, and the election commission checks the identity and eligibility and ensures the voter's anonymity when casting the ballot. When the election has finished the election, the commission counts the votes. With remote elections, the identity and the right to vote is checked beforehand or remotely, and the voter has to make sure that his anonymity is not compromised. This raises questions of voter coercion and vote buying (Krimmer and Volkamer, 2005).

Forms. Voting systems can be assigned to six basic groups with regards to their form or place. The medium hand requires the presence of voters and is limited to a certain number of people; it does not allow for voting in an uncontrolled environment. In modern institutionalized elections, this medium is very seldom used. Most modern-day elections use paper as a medium of choice. Polling station voting using paper ballots is characterized by the controlled environment and the usage of paper as a medium. Postal voting also uses paper but provides no controlled environment. If the ballot is cast electronically, one can differentiate between voting machines that are placed in the controlled environment of a voting station and remote electronic voting that also uses an electronic channel as a medium but provides no controlled environment. Table 1 gives an overview of different types of media (Volkamer and Krimmer, 2006):

Environment / **Medium**	**Controlled**	**Uncontrolled**
Hand	In-Person	-
Paper	Polling Place	Postal Voting
Electronic	Voting Machine	Remote Electronic Voting

Table 1: Forms of electronic voting

Multi-Channel. It is possible that one election uses more than one form of voting. From the operational viewpoint, it is important to note whether or not more than one channel is allowed and if paper and electronic channels must be combined. When counting the votes, the system must ensure that multiple voting through different channels is not possible. One has to make sure that the individual results of the channels are combined in such a way that the end result is correct. For the time being, democracy theory and constitutional law (requirement of universality) require additional paper channels if everyone does not have access to the Internet (or the skill to use the Internet); thus, remote E-Voting can only be an optional channel in legally binding elections for the time being.

Levels. Remote E-Voting can take place at elections of diverse levels of attention. We differentiate five different levels determined by political importance, legal commitment and parallel testing. The political importance is defined by Lijphart (1998) as such that the first and the second level elections are politically binding, which means they are regulated by law and the results of the elections have consequences. The most rigid legal framework is found with first-level elections (e.g., presidential, parliamentarian). On the second level, less important political elections can be found. Typical elections for that level may be local elections. Elections of lesser importance, because of their lesser political impact like federations of students or union elections as well as elections in corporations can be considered as the third level. These tend to have fewer rules on how the election must be conducted. Still, some kind of outcome is dependent on the result of the election. They must all fulfill certain rules so the outcome of the election can be binding and some kind of action can be derived. This leads to another classification of elections. A test can be defined as an election that has the sole purpose to test the system. Such tests are often conducted in an early stage of system development, and their sole purpose is to test the system. A logical next step is to simulate an election and test the system parallel to a binding one. The aim of such a test is to test the system under realistic conditions, and the results of which are not legally binding. These five categories build the five levels of elections, as shown in Table 2.

Levels		Leg. Binding	Org. Binding	Non-Binding
1st Level:	national	☑		
2nd Level:	regional, local	☑		
3rd Level:	org., assoc., companies	(☑)	☑	
4th Level:	shadow, parallel			☑
5th Level:	technical test			☑

Table 2: Levels of elections

Identification and Anonymity. The basic problem of electronic voting requires solving the unequivocal identification of a voter and, at same time, being able to guarantee anonymity with a secret ballot casting (Kofler et al., 2003).

Identification. For identifying a voter, three basic criteria can be used to differentiate the technologies: (i) knowledge, (ii) possession and (iii) properties. A fourth possibility is a combination of any of the three technologies. The following identification technologies are used in remote E-Voting:

1. Username and Password: The voter must remember a secret.
2. Transaction Number (TAN): The voter possesses something that identifies him/herself.
3. Biometrics: The voter him/herself with his/her individual biometric properties identifies him/herself. A biometric feature reader is needed.
4. Smart Cards: The voter knows a secret and also has possession of a card that identifies him/her. Otherwise, a property pattern of the voter is stored on a smart card that can be checked against the voter's property when casting a ballot – either way, a smart card reader is needed.

Anonymity. It is critical for a voting system to guarantee anonymity. There have been many articles written to categorize and cluster protocols that guarantee anonymity (Schlifni, 2000, Mitrou et al., 2003, Horster and Michels, 1995, Smith and Clark, 2005). While the criteria used in these papers are very sophisticated, in practice a simpler and more distinctive criterion is time (Puiggali and Morales-Rocha, 2007)—that is, at which point in the electoral cycle is secrecy (anonymity) established?

1. In the pre-election period: Anonymity is established in the pre-election period by the organizing institution. The most common implementation of such a system uses transaction numbers (TAN). These numbers are generated centrally and a scratch-field is applied. Then, in a second step, the voter's address is applied and sent to the voter who can use the number anonymously for exactly one vote.

2. During the electoral period: With this method, anonymity is established during the vote-casting procedure. It can either be done by separating the servers in an identification and ballot box server or by blind signatures; the most common implementation of Chaum's blind signature (Chaum, 1981) is used in the Fujioka et al. algorithm (Fujioka et al., 1993). The process can be explained as follows: the voter fills out the ballot sheet then puts it in a carbon-copy envelope. The voter then signs another envelope with his/her personal signature and inserts the carbon-copy envelope and sends the package to his/her register. They check the voting eligibility based on the voter's signature, then they sign the carbon copy envelope and return it to the voter. The voter opens the cc-envelope and has a signed ballot sheet (due to the carbon copy) and the voter's register has never seen the ballot sheet. Finally, the voter returns the ballot sheet to the ballot box and has thereby cast a valid vote anonymously.

3. In the post-electoral period: In this case, anonymity is established after the end of the election day; the votes can still be identified, but the count can only be conducted together, meaning the content of a single vote is never released. The most common implementations use homomorphic encryption like the Schoenmakers algorithm (Schoenmakers, 1999) or hardware security modules like the Estonian system (Estonian Election Committee, 2004).

Provider. To conduct an electronic election is a complex undertaking and is usually operated by a consortium. We identified the provider that was critical or characteristic for the entire system. Of special interest was in which country the provider operated and how much experience the company had.

Size. One important criterion for assessing E-Voting use is the number of votes that are cast. Looking at the sample, we grouped the elections into three size groups. The first group (A) contains all elections with more than 30,000 votes. The middle group (B) contains elections with a number of e-votes between 3,000 and 30,000. The last group (C) consists of small elections with a number of e-votes smaller than 3,000.

Criterion	**Category**				
Level	National	Regional	Association	Shadow	Test
Channels	Electronic		Paper and Electronic		
Identification	Username/PW	TAN	Signature	Biometric	
Anonymity	Pre-election period		Election period	Post-election period	
# Votes	A		B	C	
	# >30,000		30,000 > # > 3,000	# < 3,000	

Table 3: Criteria to categorize remote E-Voting

2.2.1.2 Methodology

A review can be organized in many ways. The approach we selected follows the handbook of review synthesis (Cooper and Hedges, 1994), which proposes five phases: (i) problem description, (ii) literature research, (iii) literature analysis, (iv) analysis and (v) presentation.

(i) The goal was to conduct a review of the progress of remote electronic voting. (ii) We used research articles, system documentation, whitepapers, technical reports, and even press releases as information to conduct our review. As remote electronic voting is a very new topic for the general public, often more than one source had to be consulted to gain a complete picture of the topic. Not surprisingly, research articles usually provided more insight on the project setup and system description yet lacked actual election-related data. Therefore, press releases were used to supplement this information. To find appropriated sources, we used a network of experts around the world that we invited to provide data or point to relevant documents. We provided them an online questionnaire on a public website to identify relevant elections. Because of the multitude of sources, the data was consolidated. This consolidation made it difficult to find common ground, so we needed to add an extensive array of integration work. (iii) The criteria that were developed in the previous chapter were used to characterize the elections. (iv) The collected data were then entered into a database for analysis. Finally, we (v) presented and discussed the analyses in the following chapters.

2.2.2 Results

In total, we identified 139 elections in 16 countries between 1 January 1996 and April 30, 2007 where remote E-Voting occurred. For the analysis, we needed a minimum amount of information regarding every election. We had to eliminate 35 elections in total. Three elections were excluded from analysis because of missing data about voters and turnout. The most common reason for exclusion was for not having system documentation available, which applied to thirty elections. Without documents, we could not assess which forms of identification or anonymity were used. Finally, two elections could not

be included because we lacked information on the voter data and on the system that was used. In total, we had 104 fully documented elections that we could include in the following analysis. These elections were held in 13 different countries on three continents; two elections were held trans-nationally. The first election was held in 1996 in Finland, and the last was held in 2007 in Estonia. The following table shows the distribution of all elections over time and by country. From the analysis, excluded elections are put in brackets.

	Countries																
Year	**AG**	**AT**	**AU**	**CA**	**CH**	**DE**	**EE**	**ES**	**FI**	**FR**	**NL**	**PT**	**SE**	**UK**	**US**	**WW**	**Total**
1996									1								1
1998						1											1
1999						1 (1)			1								2 (1)
2000		1				2 (3)									1 (1)	1	5 (4)
2001					(3)	4 (1)							1				5 (4)
2002					(2)	2 (1)		(1)		3				5			10 (4)
2003		1			2	3		1 (2)		2				14			23 (2)
2004		2			7	4 (2)		2 (3)			2					1	18 (5)
2005	(1)				10	3 (3)	2	2 (3)				1					18 (7)
2006		1	(1)	1	4	9		(4)		1	1						17 (5)
2007			(1)		1	1	1			1							4 (1)
????								(2)									(2)
incl.		**5**		**1**	**24**	**30**	**3**	**5**	**2**	**7**	**3**	**1**	**1**	**19**	**1**	**2**	**104**
(excl.)	**(1)**		**(2)**		**(5)**	**(11)**		**(15)**							**(1)**		**(35)**

Table 4: Number of elections per year and country included (excluded) in review

The countries with the most elections were Germany (30), Switzerland (24) and the United Kingdom (19). Surprisingly, the United States has just 2 publicly documented elections.

Example. As an example, we will walk you through the process of classifying elections with the example of the 2007 parliamentary elections in Estonia. The election was on the national level and was legally binding. This places the election into *level 1* of the 5 levels. It was also a *multi-channel election* that offered both paper and remote E-Voting

channels. Voters could cast their vote electronically over the Internet before Election Day or at local polling stations on or before Election Day on paper. The voters could use the remote E-Voting system with their national ID card, *a smart card* which bears a digital signature. The vote is first encrypted using the public key of the ballot box, and it is then signed by the voter with her private key. To count the votes, Estonia uses a hardware security module for hidden result calculation, which means anonymity is established in the *post-electoral period*. The *provider* of the system was Cybernetica AS, which is of *Estonian* origin. Approximately 940,000 people were eligible, registered voters, and 30,275 cast their votes electronically. This places the election into the *group A* of large elections.

The other elections were categorized in the same way. The result of the systematization is depicted in Table 5 and is described below.

Criterion	**Category**				
Level	National (4; 3.8%)	**Regional (38;36.5%)**	Association (30; 28.9%)	Shadow (27; 26%)	Test (5; 4.8%)
Channels	Electronic (39; 37.5%)		**Paper and Electronic (65; 62.5%)**		
Identification	Username/PW (4; 3.9%)	**TAN (84; 81.5%)**	Signature (15; 14.6%)	Biometric (0; 0%)	
Anonymity	**Pre-election period (53; 50.9%)**	Election period (29; 28.2%)	Post-election period (21; 20.4%)		
# Votes	A, # >30,000 (9; 8.7%)	B, 30,000 > # > 3,000 (30; 28.9%)	**C, # < 3,000 (65; 62.4%)**		

Table 5: Overview of the results

Level. With 38 cases, the 2nd level group is the biggest. The 3rd level is the second largest group with 30 elections. Of all of the binding elections, the group of national elections is the smallest (one in Estonia, one in Switzerland and two in the Netherlands). 27 elections had shadow elections, and only five elections had a sole test purpose. Interestingly, the legally binding elections account for over 40% of the cases.

Multi-channel. In one third of the cases, the remote voting channel was the only method to cast votes. For the majority (65 cases) of the elections, E-Voting was just an additional channel to the traditional paper method.

Identification. With 84 elections, the most favored way of identifying voters was the TAN system. 15 elections used signature cards, and only 4 elections used a relatively insecure username and password system. Biometric systems were not used at all.

Anonymity. In two-thirds of the investigated remote E-Voting elections, the anonymity was established before Election Day using organizational pre-registration. The second most common way was to establish it during the electoral period, which was used in 28.2% of the cases. The use of establishing anonymity after the election was used in 20.4% of the cases.

One election did not fit the categorization in the field of identification and anonymity because the identification was done based on IP-address, and anonymity could therefore only be guaranteed organizationally.

Size. The elections with remote E-Voting have a large span width between the largest (130,000) and smallest (54) number of voters. Most elections were rather small, as 65 elections had fewer than 3,000 votes cast. 28.9% of the elections had between 3,000 and 30,000 voters. In the largest group with over 30,000 votes, only 9 elections could be found.

Provider. In total, 25 different providers organized the analyzed elections. Four of them account for 54.8% of all of the conducted elections, while the other 45.2% were distributed amongst 21 providers. Most providers (76%) only had experience in their home country; the six who had operated elections outside their home country had done so in a maximum of three foreign destinations. Only one provider had operated solely abroad, which is due to the fact that it is located in the U.S. but also has a strong base in European countries.

2.2.3 Discussion

Starting with the reported findings in the previous chapter, we will now discuss the results more closely. The "idea" of collecting all elections was very ambitious. 1st level and most 2nd level documentation is publicly available. Most of the time, election information is not in one place, but with enough work, the information can be gathered. For elections on the third level, public information is oftentimes difficult to obtain. We know that there are a lot of elections in the U.S. in the private sector, but we simply could not obtain public documentation for them.

Everybody wants to sell a success story. This is especially noticeable when looking at turnout data. The most inconvenient low numbers simply are left out. The problem of selective information is not just a problem with result numbers but with information about elections in general. A language and regional bias is noticeable and also inherent in the method of experts referring to experts and resources. Nearly all papers and documentation only deal with single cases. There are very few comparative sources. Some initiatives can be found, but nothing is comprehensive.

Generally, it is hard to maintain data quality. The problems result from combining multiple sources that use different wording, are incomplete and may even be contradicting. A broader constant process would be needed. The U.S. and Asia can surely contribute to the process. Experts are asked to leave their box and overcome their bias. A start would be the 30 elections that had to be excluded because of missing technical system documentation.

Elections. The number of elections that use remote E-Voting has risen during the time span of our review. Interestingly, most of the cases took place in the new millennium with a heap in 2003 and have maintained at that level since then. Further, the number of countries using E-Voting is rising as well. Still, the average cycle for political elections is 4-5 years, which also limits the number of possible legally binding E-Voting uses. We also noticed a strong bias of remote E-Voting in Europe, where 100 of the 104 cases are located. This is of course due to the fact that Europe has a large number of countries and also inherently has the largest number of elections to conduct. Furthermore, the biggest potential of remote E-Voting (i.e., to conduct trans-national elections) has not yet been widely implemented. Only two elections in that area have been noticed so far. This may be because these elections could only happen on a 3rd level as the potential candidate for this (i.e., the European Union) has no mandate for elections yet and cannot make legislation for this as of now.

Level. We were surprised that 40% of the conducted elections were legally binding (1st and 2nd level). A large stake can be attributed to the pilot series at the local level in 2002 and 2003 in the United Kingdom. On the national level, the number is much smaller and has happened only in three countries (Estonia, Netherlands and Switzerland). In most countries that use remote E-Voting channels, laws or even the constitution have to be changed, which makes remote E-Voting very unlikely to occur spontaneously. E-Voting requires a strategic intention of the government. On the third level, with not legally binding elections, we expected to see more cases; instead, they make up only 29% of the total number. This could relate to a lack of interest in publishing the experiences associated with remote E-Voting. Reasons could be due to a low public interest or because it has already been conducted more than once. In the field of non-binding elections, i.e., the area of testing a system, it is clear that most cases took place in parallel with a real election, and only few are pure functionality tests or fictional elections. The reason for this is the problem of motivating the voters – why should they participate?

Identification. Much attention should be placed on identification (ID). The numbers showed very clearly that the ID of choice for electronic voting is a TAN. A TAN system is easy to handle because voters recognize it from lottery tickets. In addition, it is also cost effective since no reader is needed. Furthermore, the TAN is a good way for the election organizers to conduct project marketing. The most secure way (i.e., signature cards) has the obvious problem associate with usability, and it is too costly.

Anonymity. Similar to the case of identification, we found that most election organizers (71.3%) choose algorithms that establish anonymity in their premises – either before or after Election Day. This has to do with the fact that in these algorithms, the least number of calculations is necessary on the side of the voter, which means that the voting procedure requires less additional software (e.g., Java programs, applets) and can run in an ordinary browser. Establishment during the electoral period was used in 28.2% of the cases.

Multi-channel. If we check the use of multiple channels in combination with the five levels, a clear pattern emerges. 99% of all legally binding elections at the national and regional levels have at least one paper channel parallel to the electronic channel. In the 3rd level, 58% use only electronic channels, and 42% also use paper and electronic channels at the same time. The 4th level excludes, per definition, paper-based channels, and the 5th level only uses electronic channels.

Size. When looking at numbers for votes cast, one can clearly see that electronic elections are still an emerging field. Systems are gradually tested starting with smaller numbers. But, in absolute figures, all of these elections are not comparable to traditional elections. The biggest legally binding election to date (i.e., the Arizona State Democratic Preference Primary in March 2000) had around 40 thousand votes cast.

Provider. Only four providers organized the majority of elections. These are also the providers that organized elections in different countries. The rest is distributed among 21 providers, which in most cases only operate in their home country. This is most probably explained by the lack of trust in foreign companies and the fear of outside countries controlling such a core element of democracy.

2.2.4 Summary

Since this field has been around for 12 years, a review of the collected experience was greatly needed. A review of the conducted e-elections on a structured basis was a challenge due to the fragmented characteristic of the available information. Our sample of 104 cases covers 12 years, 3 continents and 14 countries. In general, data quality is the biggest obstacle to overcome.

Our research shows that although there have been four legally binding, top-level, remote E-Voting elections, the field is still not yet mature. The best indicator is the relatively small size of the cases. 62% of the elections have less than 3,000 voters, and only 8.7% have more than 30,000. These numbers are far from any traditional election.

The obvious target area foreseen by the visionaries – that is, citizens living abroad and transnational elections – was the focus of only seven elections.

Conducting e-elections needs a technical provider that is usually is an IT-company. Interestingly, they operate only in their home country. There seems to be resistance in engaging companies from abroad.

For implementation, selecting the right identification and anonymity schema is crucial for success. Here, most cases selected a combination of TAN and pre-electoral establishments of anonymity. The information of a theoretically secure signature and the establishment of anonymity during voting falls back in adoption most probably because of needed infrastructure. However, the Estonian example shows that legally binding remote E-Voting with signature smart cards is possible.

Handling multiple channels involving paper and electronic vote casting does not seem to be a problem. On the contrary, 99% of all legally binding elections offered remote E-Voting in addition to paper-based vote casting.

Future research should focus on understanding and learning from what has been done so far. In this way, any academic involved in remote E-Voting should follow basic academic styles. This means that experiments should follow basic experimental designs, but documentation should also be comprehensive, analytic and comparable. Based on existing approaches (Buchsbaum, 2005, Krimmer and Triessnig, 2007), academics should develop guidelines for how to properly document E-Voting uses, similar to election observation reports (Eriksson, 2002, OSCE Office for Democratic Institutions and Human Rights (ODIHR), 2005).

To make this research more valuable, it should be accessible by third parties in a public database. This would help readers learn from the results and also gain further insights in projects not included in this review.

It would also be interesting to deepen the analysis of the available material, especially in the field of technology following a longitudinal approach. Here, development could deliver interesting insights into the adoption of identification and anonymity technologies.

Overall, remote electronic voting has not reached the maturity needed to be applied in large-scale elections of major importance. More research is needed related to the effects, outcomes and security of remote E-Voting. Documenting the experience, as has been done here, is a first step to building a research strategy.

2.3 Legal Constraints

An analysis addressing whether the use of information technologies for electoral processes would be legally possible is typically found when analyzing the beginning of any electronics voting proposal. Often, law and regulations have been cited as an excuse for not pursuing the implementation of a technology, despite the possibility to change such laws/regulations if a majority of the policy makers so decided.

We use the definition put forward in the OSCE/ODIHR Handbook (2013) for how to observe New Voting Technologies, which it defines as "the use of information and communications technologies (ICT) applied to the casting and counting of votes", including ballot scanners, electronic voting machines and Internet voting, whereby we understand its application to parliamentary elections, thus involving regular citizens.

Such an introduction of new technologies requires careful discussion of electoral reform, which is usually initiated by the drafting of a feasibility study. Such feasibility studies will encompass technical, political, social and legal elements and will need to examine all of the possibilities of such a system as well as proposing which technical features should be brought forward.

These general considerations are important, since they determine to what extent existing legal basis of an election would need to be modified. However, technical choices are influenced by the legal framework, thus creating a difficulty in deciding which decisions to make first – those regarding the technical means or changes to the legal basis.

The technical possibilities of electronic elections are beyond the scope of this study. This study instead focuses on the constraints and guidance that the legal basis can provide. This is typically the starting point of any national debate on electronic voting where two main questions arise: Is the proposal in line with our legal basis? If so, is it also in line with international standards?

There are some general reports and studies that address these issues, such as a study commissioned by the Venice Commission of the Council of Europe in 2004, which found general compatibility of remote voting with international commitments, including postal voting and Internet voting (Grabenwarter, 2004b). In the same year, the Committee of Ministers of the Council of Europe passed a recommendation for how electronic voting systems should be designed (Council of Europe, 2004). At the third meeting of reviewing the recommendation, it was amended by two documents to reflect recent developments in transparency and certification (Council of Europe, 2011b, Council of Europe, 2011a). Consecutively, the fourth and fifth review meeting recommended updating the recommendation, which has been passed by the Committee of Ministers of the Council of Europe in June 2017. For a more indepth background on the genesis, see Wenda and Krimmer, 2016.

At a national level, most publications that address legislation regarding remote electronic voting concentrate the discussion on whether it is in line with the constitutional requirements of the respective country.

Elections are essentially the expression of the socio-political culture of a country and, therefore, naturally depend on the context in which they are held. However, a certain set of common set of standards have evolved over time. These are best described in international documents, such as the United Nations' International Covenant of Civil and Political Rights (ICCPR), the European Convention of Human Rights (ECHR), the OSCE Copenhagen and Maastricht Documents and other regional electoral standards.

The ICCPR describes in its article 25 that elections should give …"Every citizen [...] the right and the opportunity [...] (a) To take part in the conduct of public affairs, directly or through freely chosen representatives; (b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors; (c) To have access, on general terms of equality, to public service in his country".

Based on Art. 25 of the ICCPR, Markku Suksi developed an 8-stage cycle depicting the electoral process (2005). Today, ICT can be used in any step of an electoral cycle, which is increasingly being done. Examples include the use of sophisticated election management systems for election administration, electronic voter registers, electronic mark-off systems/poll books, biometric voter identification, electronic voting machines, ballot scanners and, most often, electronic result transmission and vote tabulation systems.

The use of ICT challenges not only the election process *per se* but also the election legislation. Thus, most national discourse around this issue begins by examining relevant parts of the constitution. The legal basis should describe the principles and electoral process in a way that is technologically neutral. However, since constitutions have been written and modified with paper-based processes in mind, it is important to question whether or not new standards are required for electronic election processes.

While this question has never been answered definitively, the absence of new international standards or principles suggests that new voting technologies will be held to the same standards as paper-based elections.

In this regard, data protection laws (e.g., the CoE convention on data protection comes to mind (Council of Europe, 1981)), which originally dealt with the transition from paper-based to electronic processes, are the best available guide for how to approach the modernization of an electoral process. Unfortunately, this is often neglected. A vote can be considered sensitive personal data, as it contains one's personal political opinion. Therefore, two important principles should be considered:

Proportionality. The documentation should include the principle of proportionality when handling personal data, and it should serve as a guiding indicator. In other words, the use of ICT in elections should add value to the groups affected and should only then be pursued.

Accountability. Documentation should provide necessary accountability to the voter, since an electoral code is often one of the first sources of information that a voter consults. It should provide any affected individual/group with the ability to see how his/her/their personal data (i.e., vote) is being processed.

First, let us come back to constraints put forward by the electoral principles, which are often summarized with universal, equal, free, secret and personal elections:

Universality. All eligible voters – without undue restrictions – should be able to cast their vote. This requires the establishment of a voter register, either through active or passive registration. In most countries, this already takes place using electronic means. The principal problem here is to ensure that all voters are able to participate in the election via the electronic channel, avoiding establishing unsurmountable barriers to voter participation (e.g., in cases of ICT illiteracy or literacy in general). For this reason, the CoE recommends that electronic means should only be used as an alternative option rather than replacing paper voting completely. This led to some debate in the case of Kazakhstan's experimentation with electronic voting machines during the early 2000s:

should voters be given the choice between electronic voting machines in polling stations and voting on paper? When given the choice, most voters opted to vote using the paper method, and this ultimately led to the abandonment of the system in 2011 (OSCE/ODIHR, 2011).

Equality. Each vote should carry equal weight. In the context of electronic voting, equality requires that all voters have an equal chance of their vote counting. This is of particular importance in cases of multi-channel elections (e.g., paper-based voting in polling stations, postal voting and Internet voting[7]). For example, electronic voters might have a higher chance to secure a valid vote, because the system will not allow them to cast an unintentional spoilt ballot, which cannot be prevented in paper-based systems. Also, the ballots should look similar, giving each candidate equal possibilities to be elected. This can be bothersome, as the equidistance between candidates on a ballot (often referred to as an "Australian ballot") cannot be guaranteed on a technical device. Also, it cannot be guaranteed that all candidates will be displayed at the same time.

Secret election. The requirement for secrecy ensures that a voter does not have to fear coercion or intimidation and can therefore vote freely. The voting booth under supervision of the polling station committee is normally a reliable protection from such undue influences; however, in remote voting, the voter has to guarantee this him/herself. To address this, Estonia introduced the possibility for a voter to cancel his/her Internet vote by subsequently voting at a polling station on paper as well as allowing Internet voters to recast their vote an infinite number of times (one voter in the 2011 Riigikogu elections cast their vote 500 times), where only the last cast vote would be counted. Secret elections also require that no link can be established between the voter and their vote.[8] In particular, the system should ensure that no voter can be associated with his/her vote using

---

[7] For a more in-depth discussion of postal voting vs. Internet voting, see Krimmer and Volkamer, 2005.

[8] For an overview of the technical means associated with ensuring vote secrecy, see earlier in this chapter.

the sequence in which the votes were cast, the time when the vote was cast, any disclosure of information such as IP-addresses or other identifying information such as digital signatures, etc. This is not technically trivial in remote electronic voting systems; the electronic voting system used for the 2005 Venezuelan parliamentary election included a programming error that allowed detection of the sequence of how a vote was cast (EU Election Observation Mission to Venezuela, 2006). In elections where voter verifiable paper audit trails (VVPAT) are kept, these must represent the individual vote of a single voter rather than storing all votes together on one roll of paper and thereby revealing the sequence of how the votes were cast. This could consequently endanger the secrecy of the vote.

Integrity of the Election / Personal Elections. To ensure the integrity of an election, only eligible voters should be able to participate. For this, polling stations require voters to show identification documents, and electronic mark-off systems help to ensure that no voter can vote more than once—this is particularly important for elections involving multiple channels.

In addition to the traditional election principles, there are three additional principles that are important for the credibility of an election: transparency, accountability and public confidence, all of which are political commitments of the Copenhagen and Maastricht documents of the OSCE.

Transparency. Janez Lenarcic, former OSCE/ODIHR director, once said that one can touch, see and feel paper – but not bits and bytes (Lenarčič, 2010). This essentially outlines the challenge that E-Voting poses for elections. By introducing advanced technology, one removes the essential possibility for the average person to understand the electoral process from casting the vote to entering the overall election results. This requirement of knowledge is disadvantageous in general, but it is particularly bothersome with elections, where nobody should be excluded. The German constitutional court argued in its judgement from (2009) that any election technology needs to be verifiable

without any prior specific knowledge, and they thereby introduced a new principle of publicity. This basically requires voting technology to provide a means of voter-verifiability, whether on paper (e.g., ballot scanners) or E-Voting machines (with VVPAT). For Internet voting, this probably mandates the introduction of individual verifiability, which uses cryptographic means to verify that the vote was essentially recorded as cast and cast as intended.

Accountability. This principle complements the requirement for election integrity, because it fosters the overall trust in an election. If every step of the election's preparation and completion is properly documented, one is always in a position to precisely determine what has happened. While electronic systems can help with accountability, such systems cannot document everything, so some aspects must be left to the human observer and the election commission (e.g., the setup of such systems and interactions beyond the command level). For this purpose, some election authorities are engaging with professional IT auditors that are in the position to document every interaction with the system and conformity with a pre-defined set of commands/operating manual. Nevertheless, for courts, this expert rule is not always sufficient, as in the case of the Austrian elections, where the constitutional court demanded full accountability of the process, which can also be assessed without the help of experts. Again, a system that allows both individual verifiability and universal verifiability (that all votes that have been recorded are also counted and tabulated) is required.

Public confidence. Public confidence is particularly difficult to achieve in an election because it is not based on facts or measurable items but on understanding and perception of individuals that form the collective trust in a given election system. The German constitutional court (2009) differentiates between blind trust and established trust. Blind trust refers to the unverified trust in a technology because one cannot understand it, whereas verified or established trust refer to cases in which the election stakeholder has challenged the system, verified its proper functionality and built their confidence in the system over time.

To date, most E-Voting studies discuss approaches for developing more sophisticated algorithms to solve the problems of unequivocally identifying voters, secretly casting votes and counting them honestly and accurately. Few authors have addressed how the technology influences the legal basis or provided actual guidance on how to use such a system (Krimmer, 2012). However, following recent high-profile courts decisions on this issue, collaborations between technical and legal sciences are emerging, leading to more sustainable electronic election projects.

While there is no definite solution to the problem of whether technology depends on law or law depends on technology, it is clear that single-disciplinary approaches are insufficient and that integrated, collaborative efforts are required to deliver legislation for electronic elections as well as the procurement of such systems.

Security is the ultimate concern when discussing the use of electronic election. Due to their complexity, important principles are sometimes questioned. However, it should be made clear that any electronic system must always meet the exact same standards applied to traditional paper-based systems. While some of the principles need interpretation and/or translation into digital realities, this does not necessarily mean that they should be altered.

2.4 Summary

In this chapter, we have demonstrated the origins of Internet voting, provided an analysis of some of the first remote electronic voting systems and analyzed the frame that constitutions and international standards have provided for the conduct of Internet voting.

3 Internet Voting in Austria

Austria debated the use of electronic means for voting in its parliament several times in the second half of the 19th century. Unlike the neighboring countries of Germany, which used it for some years in the 1970s (see documentation of its last use in 1973 in Schindler [1999]), or Switzerland, where it was permanently installed for the *Nationalrat* (federal council) in 1994 (Das Schweizer Parlament, 2014), the topic never reappeared in serious discussions in Austria. Furthermore, despite that mechanical and electronic voting machines have been used in Germany (for information regarding mechanical voting machines, see Amt für Statistik und Wahlen der Stadt Dortmund [1961], and for information regarding electronic voting machines, see Bundeswahlgeräteverordnung [1999]) and have been considered for elections in Switzerland (Schweizer Bundesrat, 1975), no use or discussion of such devices have been considered in Austria to date.

However, the case of Internet voting is different. Here, Austria has developed considerable interest and experience over time.

3.1 The Beginnings

During the 1990s, the Internet developed quite rapidly. Generally, it was considered that the time was ripe for the Federal Chancellery of Austria to develop its own information-society strategy with the help of a large group of experts. The report was finalized at the end of 1996, but Internet voting was not considered feasible for the near future due to concerns about voting secrecy and the danger of manipulation (Knoll and Grossendorfer, 1996).

The first attempt in regard to the organization of an Internet election came from private actors in 1999. One of the primary Internet providers in Austria, offering Internet through its cable television network in the city of Vienna and other municipalities in Austria, had a very active user base. Users were not very satisfied with the quality of the Internet service and decided to establish a group that would represent their own interests. The first working group that set up the election decided to hold it between October 19 and

November 28, 1999 using a basic web page. The customers' official e-mail addresses and passwords were used to verify eligibility. Furthermore, the participation of a self-set minimum of 1,500 customers was required. For further details, see the regulations in Plattform Anwender.Interessen.Gemeinschaft. (1999b). With 557 participating customers, this quota was not reached, and the election was thereby considered invalid (Plattform Anwender.Interessen.Gemeinschaft., 1999a).

A month later, in December 1999, a second attempt was initiated. It was decided to hold the election in the following year between May 1 and 31, 2000 (Arbeitsgemeinschaft Uservertreter Wahl, 2000). In the second attempt, identification was based on the IP address of the voter, meaning that the Internet voting platform accepted only votes from within the provider's network. Similar to the first attempt, secrecy of the vote was provided by organizational means since – according to their own statement – the organizers of the election had no possibility of identifying the owners of the IP addresses. In order to offer proof of the election's integrity, the server was handed over to an independent auditor/observer for verification (Arbeitsgemeinschaft Uservertreter Wahl, 2000, Krejcik, 2003a, Krejcik, 2003b).

Apart from these limited practical experiences, the only other work noticeable around Internet voting were several elaborations of voting protocols for Internet voting, such as those from Hassler and Posch (1995), Horster (1995) and Schlifni (2000) as well as the participation of the city of Vienna in the EU-funded electronic democracy research project known as EDEN (Bertorello, 2001).[9]

[9] The EU funded a number of research projects dealing with Internet voting, such as Cybervote or E-Poll, with the aim of cost reduction and fast and clear results presentation within the fifth framework program (Galetsas, 2001). It did not do so under the sixth or seventh framework program.

Changing the Federation of Students' Law. This was expected to change when the legally binding election of the German University of Osnabrück's student parliament on February 2-3, 2000, conducted by the *Wählen im Internet* (Voting in the Internet) project, gained a great deal of media attention not only in Germany but also in Austria (Forschungsgruppe Internetwahlen, 2000). In particular, the *Österreichische Hochschülerschaft* (ÖH, Austrian Federation of Students) as well as the *Österreichische Hochschülerschaft an der Wirtschaftsuniversität Wien* (ÖH WU, Federation of Students at WU Vienna University of Economics and Business) were very interested in this project, since their election had suffered from a particularly low voter turnout for several decades (Krimmer, 2002).

Furthermore, WU had gained a reputation as the most-advanced university in Austria in terms of university administration. The rector of the WU, Hans-Robert Hansen, had pushed for replacement of the paper-based student ID with a multifunction plastic smartcard. As early as the 1980s, during his first term as WU rector, he had advocated for the introduction of such a card, but the project was halted early on because of data protection concerns. In 1995, the WU PowerCard enabled some 250 students to use the PC labs 24 hours a day, 7 days a week, in a pilot project, much to the satisfaction of all involved (WU Zentrum für Informatikdienste, 1997). Based on its success, the administration's modernization project WU-IS/2000[10] included equipping all 20,000 WU students with such plastic cards, but the project also had the intention to include digital signature functionality (WU Zentrum für Informatikdienste, 1998). Together with Austria being the first country to implement the European Digital Signatures directive 1999/93/EG with the enactment of the Austrian *Signaturgesetz* (Digital Signature Law), which went into effect on January 1, 2000 (Menzel, 2000), it seemed only a matter of a few months before students could receive their new student IDs in the fall of 2000.

Motivated by the Osnabrück example, the ÖH and the ÖH WU formed an internal working group to pursue the intention of introducing Internet voting for the upcoming

[10] The project consortium that implemented the WU-IS/2000 project consisted of Siemens Austria, init GmbH, and Datakom GmbH. Siemens was responsible for the hardware and project management, init for the software and Datakom for the provision of the fully qualified digital signatures.

elections. It was clear that this would result in a need to change the legal framework for the bi-annual elections, which are governed by the *Hochschülerschaftsgesetz 1998* (Law on the Federation of Students). There proved to be a window of opportunity as the government at the same time planned to establish student federations also at the *Pädagogische Akademien* (pedagogical academies), which would require a change in the law. When the draft law was sent out for comments, the chairman of the Federation of Students, Martin Faißt, sent a letter to the Austrian Federal Minister of Education, Science and Culture, Elisabeth Gehrer, on May 15, 2000 (Faißt, 2000). In this letter, he requested that the minister introduce a form of remote voting, whether via post or electronically, for the elections to the Austrian Federation of Students, the legal representation of students in Austria, regulated by its own federal law.

Gehrer's ministry, the *Bundesministerium für Bildung, Wissenschaft und Kultur* (Federal Ministry for Education, Science and Culture, BMBWK), in response formed a new working group together with the ÖH and ÖH WU to discuss possible ways of introducing remote voting. For the ministry, it was clear that the introduction of remote voting could take place only in a "modern form," meaning using electronic means. In a first effort, a study trip was undertaken from September 18-20, 2000 to learn from the experiences of the University of Osnabrück as well as the returning officer of the state of Brandenburg in Germany.

Only weeks before this visit, the WU had originally planned to replace the paper-based student IDs with new smartcard-based plastic ID cards (Wirtschaftsuniversität Wien, 1999). However, the provider of the digital signatures, Datakom Austria GmbH, was behind schedule, because they had difficulty accrediting their services by the oversight body, *Rundfunk & Telekom Regulierungs GmbH* (RTR).[11] Nevertheless, they were still

[11] At that time, Datakom was a daughter company of the Austrian Post and the Austrian pioneer in terms of digital signatures. After the enactment of the Austrian Digital Signature Law on January 1, 2000, Datakom wanted to become the first accredited

expecting to receive the accreditation before the end of the year, since it was a high priority for them because the equipment of the then 20,000 WU students with digital signatures would have been Datakom's first large-scale deployment. So, the working group traveled to Osnabrück with the assumption that all WU students would have new student IDs with digital signatures by the time the Federation of Students elections would take place.

The talks with Dieter Otten, head of the research group *Internetwahlen* from the University of Osnabrück, went well, so the working group prepared a contract of cooperation between the ministry, ÖH, ÖH WU and the University of Osnabrück. The working group sought to use the Internet voting solution developed by the University of Osnabrück at the WU because of the availability of infrastructure and the perceived high comfort level of the students for using IT. The students would use their new digital student IDs to cast their votes at specially prepared voting terminals in the polling station at WU during the May 2001 Federation of Students' election.

---

trust center to offer fully qualified digital signatures to the public. It was able to offer simple digital signatures with lesser legal quality almost immediately on January 27, 2000 (Tischler, 2000). But, it was more complicated for them to fulfill all the technical, organizational and security requirements for fully qualified digital signatures that were requested by the *Bestätigungsstelle* (certification body), the *Zentrum für sichere Informationstechnologie - Austria* (A-SIT, Center for Secure Information Technology – Austria). Its approval needed to be accredited by RTR.

In spite of the fact that protesting against the introduction of tuition fees for studying at Austrian universities took most of the student representatives' attention, the working group had prepared the changes to the *Hochschülerschaftsgesetz* (HSG, Federation of Students' law), so the *Ministerrat* (ministerial council) of the government decided that Internet voting would be introduced on November 29, 2000 (BMBWK, 2000). The changes included the amendment of Sections 34, 39 and 48 of the HSG.[12]

The amendment followed the principle of technological neutrality, although essential core elements are mandated by it. Section 34 Para. 4 HSG provides that the technology used to verify the identity of the voter must comply with the requirements of electronic signatures in accordance with the Signature Law and must comply with the provisions of the Data Protection Act 2000. In particular, this meant that the Data Protection Commission is required to approve the system, because sensitive data will be processed by the election system in accordance with § 18 Para. 2 DSG 2000, i.e., the political opinion of the voter. The electronic election system must provide a technical setup for the Election Commission so that it can carry out its tasks in accordance with § 34 Para. 5 (4) HSG.

As part of the election process, a provision was made in § 34 Para. 5 (5) HSG to provide a confirmation of consent step – in other words, a question asking if the voter wishes to cast the vote in the format indicated. Furthermore, computers set up on the premises of the university offering the possibility of electronic voting were to be equipped with visual protection. This does not apply for electronic voting over the Internet on home personal computers according to the explanations in the 2001 parliamentary discussion. This is also conclusive in the sense that, in the case of a conventional election, persons

[12] The introduction of electronic distance voting in the area of interest groups has been made possible by the Constitutional Court decision of 1996 - VfGH, VfSlg 14440, according to which election law can be interpreted more broadly in the case of interest group elections as compared to national elections. In the case of the latter, the 1985 - VfGH, VfSlg 10412. See also (Menzel, 2001).

casting their vote by mail are themselves responsible for exercising the right to elect freely, secretly and personally without supervision by the Election Commission. After the Election Commission made computers available for electronic voting in the Austrian Federation of Students' Union elections, the establishment of visual protection facilitates this type of voting. Furthermore, certification according to § 34 Para. 6 is required for the E-Voting system, which must be carried out by the Confirmation Authority according to the Signature Law. This Confirmation Authority may also be consulted to conduct a review in the event of irregularities pursuant to § 39 Para. 7 HSG before any declaration of invalidity is issued by the Election Commission. In Article 48 HSG, the responsible Federal Minister shall be empowered to introduce E-Voting through a regulation.

On December 21, the ministry also sent out a draft version of the *Hochschülerschaftswahlordnung* (HSWO), the ordinance regulating further details of the voting process (Stangl, 2000), including some for the conduct of Internet voting, which includes the following:

- The election commission should make sure before the beginning of the election – if necessary with the help of technical experts –that the hard disks are empty;

- The election commission should ensure that enough voters should participate in the election so that there are enough votes to safeguard the anonymity of the voters;

- Information about voters and anonymized votes should be stored on separate hard disks;

- Any data produced by the electronic election should be transferred to read-only media (CD-ROMs), and any data should be deleted.

The working group was assured several times that new student IDs would be rolled out in February 2001. However, shortly after the beginning of the new year, before the co-operative agreement could be signed or the ordinance passed, it became clear that the time frame anticipated by the WU and its service providers could not be achieved, and its introduction would be further delayed until summer.[13] Hence, on January 17, 2001, the working group announced the postponement of the effort (Österreichische Hochschülerschaft, 2001).

Nevertheless, the changes to the Federation of Students' law were passed in parliament on February 1, 2001 (Brinek et al., 2001). However, the ordinance for the conduct of the Federation of Students' elections did not include the previously proposed changes with regards to Internet voting (Bundesministerium für Bildung Wissenschaft und Kultur, 2001). Hence, the student elections in May 2001 did take place in all Austrian universities using paper ballots.[14]

---

[13] The rollout of the smartcards finally took place without equipping them with digital signatures. On December 17, 2001, Datakom received the necessary accreditation (Telekom-Control-Kommission, 2001) and started public offering of digital signatures on February 4, 2002. Shortly thereafter, it announced that the issued student ID cards had to be replaced during the summer 2002, as the original chip was suitable for fully qualified signatures (Tischler, 2002). Then, on September 27, 2002, Datakom sold its digital signature products to its only competitor A-Trust GmbH. On October 1, 2002, Datakom was reintegrated within its mother company, Telekom AG, and ceased to exist. In 2005, WU started to offer services using digital signatures (WU Zentrum für Informatikdienste, 2005).

[14] For a description and lessons learned from running the Federation of Students' elections at the University of Vienna and the potential of Internet voting, see Menzel and Stöger (2003).

Later that year, the parliament also passed similar amendments to the *Wirtschaftskammergesetz* (law for the chamber of commerce) in order to allow electronic voting for their elections as well (Kopf and Haigermoser, 2001).[15]

After the elections, as one of its last efforts, the ÖH WU published a questionnaire in its biweekly magazine *WUaktuell*. The survey aimed to determine the interest of its members in Internet voting (ÖH WU, 2001a). Approximately 84 percent of the WU students were actually in favor of its introduction (ÖH WU, 2001b). This gave encouragements to all persons involved that Internet voting would really be more a matter of time.

[15] Next to the Federation of Students, the Austrian Chamber of Commerce was a second driver – at least for some time – for the use of ICT in elections. Its elections take place every five years, and in 2000, for the first time, a networked voter register was used to identify the voters as well as an optical scanner to count the votes in its elections in Vienna (Nettig, 2000). In 2005, five polling stations were equipped with self-developed electronic voting machines (de Carlo, 2007, Hantsch, 2006). These machines did not fulfill the criteria (no digital signature, no evaluation by A-SIT) set forth in the chambers law. However, nobody appealed against its use, so the results remained legally binding. Nevertheless, the machines were not used in the 2010 elections. For a general overview of IT use in preparation of elections in Austria, see Botz (2008).

3.2 The Research Group E-Voting.AT

The public discussion of Internet voting for the Federation of Students' elections revived the academic discussion in Austria as well. WU researchers Alexander Prosser and Robert Müller-Török presented a paper at the ICEIS conference in July 2001 in Setubal, Portugal, where they proposed the first version of their algorithm, which separated the voting process into two phases: identification and vote casting. Furthermore, the algorithm was designed for multifunctional smartcards to ideally fulfill three functions: (i) to identify the voter, (ii) to store the anonymous voting token and (iii) to provide for a secure processing environment (Prosser and Müller-Török, 2001).[16]

In July 2001, WU Professor Alfred Taudes learned of the efforts of the ÖH WU and proposed to join efforts with Alexander Prosser and Robert Krimmer. Shortly thereafter, Robert Kofler, who had programmed the department's webpage as part of his master's thesis under the supervision of Alexander Prosser (Kofler, 2003), also joined the team. In September 2001, the research group E-Voting.AT was founded and began to develop a working prototype. As one of the first steps, the research group negotiated a cooperative agreement with the ÖH WU, which was signed on November 10, 2001 (Panny et al., 2001).

Furthermore, the research group established a consultative body, where members from the BMBWK, the City of Vienna, A-SIT, ÖH WU and the *Bundesrat* (Federal Council, upper house of the Austrian Parliament) took part. Between 2001 and 2003, the body met four times. The aim of the advisory body was to raise awareness for Internet voting with relevant stakeholders in Austria. Early on, it became clear that developing an Internet voting project would require substantial legal knowledge, and a second, less formalized cooperative arrangement was established with Professor Michael Holoubek from the WU Institute for Public Law as well as assistant professor Patricia Heindl.

[16] Refined versions of the algorithm were later published in the journal *Wirtschaftsinformatik* (Prosser and Müller-Török, 2002) and in the proceedings of the Hawaiian International Conference on System Sciences (Kofler et al., 2003).

Next, the research group looked for an industry partner that could help with the implementation of the project. The trust center Datakom was first chosen, despite their problems with offering fully qualified digital signatures.

After initial positive sounding meetings in fall of 2001, a project proposal was prepared by E-Voting.AT together with Holoubek & Heindl on behalf of Datakom in order to develop a pilot implementation of the E-Voting.AT algorithm intended for use in the 2003 WU Federation of Students' elections.

On November 19, 2001, a project proposal was submitted to the research agency FFF with the aim to develop a prototype and to use it in the 2003 Federation of Students' elections at the WU (Datakom Austria GmbH, 2001).

After the submission of the proposal, the work continued. One of the challenges during the beginning of the project was to assess the feasibility of whether the multifunctional smartcards available at the time in Austria would be able to fulfill the required functions as designed (Prosser and Müller-Török, 2002). The research project put a strong focus on the calculation and storage of the voting token, including how to best protect the token's secrecy. In order for the smart card to calculate and store a voting token, it would require the card to not disclose any information that could lead to the identification of the voter (Kofler et al., 2004).

However, talks with Siemens and A-SIT identified the following problematic issues with using the smartcard, which was to be deployed to WU students:

- The smartcard's unique ID and the certificate of the owner of the smartcard could not be read freely;
- Neither the owner of the chip nor other applications on his/her behalf were able to write onto the smartcard;
- The smartcard contained only a signature key pair and was missing a key pair for encryption;
- The standard operating systems for multifunctional smartcards did not provide the necessary operators in order to be a secure processing environment (Kofler et al., 2004).

On January 18, 2002, Alexander Prosser informed the group's partner, Datakom, about these issues and had them withdraw the submitted project proposal before the scientific committee could decide whether or not to fund the project (Prosser, 2002). Despite some continued talks with Datakom, including discussing how to equip the WU students' cards with the missing second key pair, the funding application was not taken up again, and the partnership ended.

Without consistent funding, the research group decided to continue its efforts. The first research results were published at the International Legal Informatics Symposium in Salzburg in February 2002 (Prosser et al., 2002a). There, a working contact was established with Nadja Braun, who was then working for the E-Voting project of the Swiss Federal Chancellery.

Next, the development of the prototype was intensified, as it was the group's intention to maintain cooperation with the ÖH WU. In the summer of 2002, Martin Karl-Unger joined the research group in order to strengthen the development efforts of the client. The focus of the work was now to find a partner for modifying an existing or developing a new multifunctional smartcard from scratch.

Despite the fact that no partner was found right away, an e-government infrastructure project by the Austrian government facilitated the further development. The project was able to make use of a newly developed interface based on the HTTPS protocol to interact with Austrian smart cards. This interface had been presented earlier in the year by the *Bundesministerium für öffentliche Leistung und Sport* (BMÖLS, Federal Ministry for Public Service and Sport) as part of a new service in addition to the digital signature, the *Bürgerkarte* (citizen card or national ID). The need for it arose because digital signatures only allow for authentication of a person but not for its identification (unless the digital signature is known beforehand). The purpose was to link a digital signature to the respective data record of the citizen in the *Zentrales Melderegister* (ZMR, central population register). In addition, the concept also contained a so-called security layer that would provide access to the smart card using standard HTTPS commands (Leitold et al., 2002). The concept and its specification had been released to the public on August 30, 2002.

The initial prototype implemented the first step of the algorithm, which consisted of verifying the voters' identity using the security layer and generating the anonymous voting token. It was presented to the public together with its source code in December 2002 (Prosser et al., 2002b). The source code was obfuscated, which made it hard for third parties to understand.

3.2.1 First Shadow Election with Internet Voting and the E-Voting.AT Action Plan

Based on the prototype, talks with the ÖH WU were taken up again. It was also clear that legally binding elections could not be held because the appropriate digital signature infrastructure would not be available. Hence, the plan was to conduct a shadow election,[17] where the identification using digital signatures would be replaced by using the students'

[17] A shadow election is a mock election that took place at the same time as the real, legally-binding election. A voter participating in a shadow election must participate twice to both test the e-voting system and to cast a legally binding vote (on paper).

usernames and passwords, which they use for accessing their e-mail accounts. Further, the eligible students were limited to participants in the elective courses of the WU Institute for Information Processing and Information Management; this comprised 980 students.

For identification, the E-Voting.AT project sought support from the *Zentrum für Informatikdienste der Wirtschaftsuniversität Wien* (ZID, WU center for IT services), to which E-Voting.AT gave the student ID numbers of the eligible participants. ZID then created a hash number on the basis of the student ID (without corresponding names), which served as internal IDs for the test. This ensured that the identification and authentication of the test participants were completely in the hands of the ZID. Hence, E-Voting.AT had no information about the names of the students that participated in the shadow election.

The shadow election required the students to conduct two steps: (i) to obtain a voting token issued any time between May 1 and 19, and then (ii) to use this voting token between May 20, 2003, 9:00 and May 22, 2003, 15:00 to cast their vote. In order to ensure that the encrypted votes were not opened before the end of the election, representatives from the three largest parties in the *Universitätsvertretung* (UV, Federation of Students' university parliament) held the three shares of the decryption key.

When looking at the usage numbers, 412 students had a voting token issued, but only 355 students actually cast a vote (86%) (Prosser et al., 2003). As the client of the Internet voting software required the use of Java, several users had issues installing the software because they did not realize that the test election would require the installation of the Java runtime environment (JRE). In a survey conducted amongst the participants of the test, a large majority (81.2 %) turned out to be in favor of voting online. The most important factor was to be able to vote without having to go to the polling station, i.e., it was a matter of convenience. The participants also felt that E-Voting was a very secure and anonymous process. The survey also found that the participants were generally interested in politics, which lends support to the belief that Internet voting will activate the already activated (Dickinger et al., 2003).

In the aftermath of the shadow election, the project team conducted several activities to increase the outreach of the project:

- the advisory board held another meeting;
- an outreach campaign was started in order to set the public agenda to foster Internet voting efforts; and
- a meeting with stakeholders was held in order to disseminate the project results and find potential new partners.

The E-Voting.AT advisory board met for a fourth time on June 24, 2003 to discuss the results of the shadow election. One of the major outcomes of this meeting was the decision to organize an international conference to reach out to other groups working on electronic voting issues within Europe. Jürgen Weiss, the chairman of the federal council at that time, recommended the conference be held in Schloss Hofen in Lochau near Bregenz, the center for continuing education of the region of Vorarlberg.[18]

The outreach campaign was started in cooperation with the research colleagues from the WU constitutional law department, Michael Holoubek and Patricia Heindl. The project team wrote a letter to the president of the *Verfassungskonvent* (constitutional convent), a body installed by the Austrian government to discuss possible changes to the constitution (Holoubek et al., 2003). The intent of the letter was to make the convent discuss the possibility of introducing Internet voting.

[18] This was the start for the EVOTE conference series, which took place between 2004 and 2014 every second year. In 2016, the conference was merged with the Vote-ID conference to become E-Vote-ID and since takes place every year.

During the summer of 2003, the *Österreichische Computer Gesellschaft* (OCG, Austrian Computer Society) *Arbeitskreis für E-Democracy/E-Voting* (working group on e-democracy/E-Voting)[19] held a strategic discussion on the possible introduction of E-Voting, in particular, to give further input to the constitutional convent. An action plan was prepared, which included the following steps in sequential order:

1. Identification of Target Groups

   This included elections to pressure groups within the country as well as federal elections for citizens living abroad.

2. Development of the Infrastructure

   The necessary infrastructure (e.g., a central voter register) as well as distribution and daily use of appropriate smart cards with digital signatures.

3. Gaining Experience

   The introduction should follow a step-by-step approach with a slowly growing user group before implementing the project at full scale.

4. Legal Adaptations

   According to the previously identified target groups, the necessary adaptations of the legal base including the constitution should be discussed.

[19] This working group was established in late 2002 to build a network of people in research and practice who were interested in the topic of e-democracy and e-voting issues around these topics. In eight meetings in 2002 and 2003 some twenty presentations by experts on the topic were held and a proceedings band with the results of the presentations was published (Prosser and Krimmer, 2003b). While the working group still exists today, it is significantly less active than in the initial phase. It currently focuses on organizing e-democracy and e-participation conferences including a public wiki (www.ocg.at/ak/edemocracy/wiki2).

This action plan was presented at a press conference on July 29, 2003 (Prosser and Krimmer, 2003a). Later that day, the president of the constitutional convent notified the project team that he had forwarded the letter sent by the project in May to the members of the convent (Fiedler, 2004). Consecutively, the bureau of the convent discussed the topic of E-Voting together with postal voting. While there was a general agreement that postal voting should be introduced, such an agreement could not be found for E-Voting (Fiedler et al., 2005).

As the third activity for project outreach, meetings with several electoral stakeholders were held. The project had already met regularly with the *Stadt Wien* (Administration of the City of Vienna), the *Bundesministerium des Inneren* (BMI, Ministry of the Interior) and the *Bundesrechenzentrum* (BRZ, Federal Computing Center) a daughter company of the *Finanzministerium* (BMF, Ministry of Finances) to gain additional input and make them aware of the project. But, with the successful conduct of the shadow election, the interest in the project grew. Further meetings were held with the following groups: *Wirtschaftskammer Österreich* (WKÖ, Austrian Chamber of Commerce), several big IT companies including IBM and Oracle, and the *Bundesministerium für auswärtige Angelegenheiten* (BMaA, Federal Ministry of Foreign Affairs). The interest of the BMaA came, in particular, from the department for Austrians living abroad, which was led by Thomas Buchsbaum. He had contacted the research group at the beginning of 2003, because he was looking for input on remote electronic voting for his participation in the working group for establishing a standard on electronic voting within the Council of Europe.[20] Furthermore, citizens living abroad were identified as a group that could

[20] Upon suggestion from the British delegation, the Council of Europe had established a working group in order to create a European standard for electronic voting in 2002. This group eventually managed to conclude its work in summer of 2004 and the committee of ministers adopted the "Recommendation (2004)11 on Electronic Voting" on 30 September of that year. (For background of the project, see Remmert, 2004)

potentially benefit from using Internet voting.[21] Also, in the discussions during a presentation in the BMaA in June 2003, it became clear that the role of the election commissions was underestimated so far—in particular, their ability to start, interrupt or close an election, which set the agenda for the further work of the research group.

3.2.2 Federal Presidency Election and Inter-Ministerial Working Group on Electronic Voting

During the public outreach campaign, the Austrian branch of IBM expressed particular interest in collaborating with the project. While IBM itself had no experience with Internet voting as such, they had commissioned studies on electronic democracy (for example, Davies [2000]) and were interested in several e-government projects. In August 2003, a mutual understanding was reached that IBM Austria would explore entering a strategic partnership with the E-Voting.AT initiative, including forming a research project where IBM would invest considerably. As a second partner, the BRZ was considered. Together, E-Voting.AT, IBM and BRZ began to work on a project proposal to be submitted to the *Forschungsförderungsgesellschaft* (Austrian research council, FFG), which had a funding scheme for public private partnerships for applied research.

Before the research proposal could be submitted, several rounds of negotiations took place. In order to test the newly formed partnership, a new shadow election was planned, and the upcoming *Bundespräsidentschaftswahl* (Federal Presidency Election) at the end of April 2004 was chosen as the ideal candidate. However, BRZ canceled its participation in the shadow election shortly before. A-Trust, the successor of Datakom as trust center for providing digital signatures, was able to quickly replace BRZ's role as the sponsor of the event.

[21] In February 2004, e-voting for citizens living abroad was made the topic of discussion during the e-democracy sessions at the IRIS conference in Salzburg Austria. For more information, see Braun, Buchsbaum, Krimmer, and Prosser (2004).

This time, all WU students – which included approximately 20,000 people – were entitled to participate in the shadow election in order to cast votes for the new Austrian president via the internet. The two major parties nominated two strong candidates: Heinz Fischer from the SPÖ and Benita Ferrero-Waldner from the ÖVP. Soon, Internet voting also became an issue in the election—both candidates held different opinions, although they pretty much followed the party lines. While Fischer was against the introduction of Internet voting,[22] Ferrero-Waldner, not surprisingly as minister of foreign affairs, supported the topic, in particular, because of the benefits for Austrians living abroad.

The set-up of the project was very similar to the 2003 shadow election, except that this time all 20,000 WU students were entitled to participate. The WU ZID again provided support for the student logins. Voting tokens were issued between March 22 and April 22 around the clock, and students were able to vote online any time between April 23 09:00 and April 25 17:00. A total of 1,786 voting tokens were issued (some 9% turn out), and of these, 961 were used to cast a vote (reducing the turn out to some 5%), so nearly 47 % of the voting token holders did not participate in the second step of the process. This may have been due to problems with Java, as some 120 support incidents had to be solved, mainly concerning the installation of JRE.[23] The role of the electoral commission was strengthened this time; however, the recent research results that allowed for majority decisions of the election commission were not implemented in time. The members of the commission consisted of Gabriele Kotsis, president of the Austrian Computer Society, Horst Breitenstein, WU vice rector, and Michael Holoubek, professor for constitutional law.

---

[22] Heinz Fischer mentioned during a public debate at the WU on March 16, 2004 (ÖH WU, 2004) that his son, Philipp Fischer, had written a diploma thesis on the topic at the Danube University Krems in the late 1990s. According to Fischer, his son concluded that this form of voting should not be pursued. Philipp's thesis was one of the first Austrian academic theses on this topic. University employees confirmed its existence; however, it was not possible for the university library personnel to retrieve a copy from their archives.

[23] In a subsequent research project, an auto-install process was developed by Daniel Walch that could reduce the number of support incidents (2006).

The counting ceremony on April 25 became a major event attended by some 100 visitors during which the encrypted electronic votes were loaded, the key shares entered by the electoral commission, the decrypted votes counted, and the results presented. In a survey conducted after the shadow election, it came as no surprise that E-Voting ranked high amongst WU students as a future application for multifunctional cards (Arami et al., 2004).

After the successful election test and EVOTE conference, the consortium of IBM, BRZ and E-Voting.AT continued negotiations and talks for submitting a joint research proposal. These discussions developed very slowly. When it became known that decision makers within the WU would not support the submission of the research proposal, the interest of the project partners IBM and BRZ faded. The attempt to achieve sustainable financing for E-Voting research at WU failed once more.

Despite this failure to institutionalize E-Voting research at the WU, the two test elections put pressure on political decision makers to discuss whether or not voting via the Internet was a possible future option for Austrian elections.

In an interview on the evening of April 25, 2004, after the count of the Internet votes, the head of the election department in the BMI, Robert Stein, announced that the Federal Minister of the Interior, Ernst Strasser, had commissioned a feasibility study for the introduction of Internet voting in the form of an inter-ministerial working group (Stein, 2004).

The group immediately began work in May 2004. Three sub-working-groups each focused on different aspects: international aspects, chaired by Thomas Buchsbaum from the BMaA; technical aspects, chaired led by Herbert Leitold from A-SIT;[24] and legal affairs, chaired by Robert Stein. Over a period of half a year, some 50 experts, including Robert Krimmer and Alexander Prosser, met several times to discuss the issues and develop a final report addressed to the minister of the Interior. The work was concluded on December 15, 2004. The conclusions of the report were as follows:

- The introduction of electronic voting for elections to federal, regional, or municipal parliaments requires a change of the constitution.

- Electronic voting must fulfill the principles for elections in the same way as paper-based elections.

- The Council of Europe's "Recommendation (2004)11 on Electronic Voting" does not in any way conflict with existing Austrian legislation.

- Electronic voting must give the election commissions the same opportunities for control as paper-based elections do; in particular, results of electronic voting should only be accessible by a joint effort of a majority of election commission members.

- The citizen card shall be the form of identification for any electronic voting efforts.

- Costs of electronic voting cannot be assessed; however, they must be split evenly between municipal, regional and federal institutions.

[24] Within the framework of this technical working group, Thomas Rössler – on behalf of A-SIT – presented an overview of the state of the art in electronic voting, which served as a basis for the discussions (Rössler, 2004a).

- A central voter register is a pre-requisite for electronic voting and would potentially result in synergy effects, i.e., lower costs in the long run.

- Technical challenges mainly stem from the requirement of keeping votes secret while also avoiding the cast of multiple votes in different voting channels.

- Due to the high number of polling stations, it is not an aim to equip them with electronic voting machines.

- The introduction of Internet voting at the federal level requires a series of tests at lower levels, including regional and municipal. Furthermore, tests that include only a subset of voters should not be pursued due to the possible unequal treatment of voters within the electorate. Instead, gaining experience with electronic voting in the elections of pressure groups (e.g., Federation of Students or the Chamber of Commerce) should be considered.

- The introduction of electronic voting requires proper preparation over a period of several years. Potential accelerating factors could include the existence of a central voter register and a high degree of diffusion of the citizen card amongst the Austrian population.

- Electronic voting should be used only as an additional means of casting a vote and should not result in any reduction in the opportunity to cast a vote on paper (Bundesministerium für Inneres, 2004).

While most of these recommendations were in line with international practice, the requirement that electronic votes can only be conducted for the whole of a given electorate is specific to the Austrian context. Other countries have chosen to handle deployment differently, such as Switzerland's incremental approach to deployment.

After this report was published, it seemed as if a long-standing discussion had ended. It was clear that E-Voting could be done technically, and it was legally possible to conduct elections within the Federation of Students or the Chamber of Commerce. However, E-Voting in national elections would require changes to the constitution, which would require the agreement of ÖVP and SPÖ.

As no sustainable funding could be acquired, the E-Voting.AT research group disintegrated within the second half of 2004, as Martin-Karl Unger, Robert Kofler, and finally Robert Krimmer decided to focus on other work.

3.3 The Competence Center for Electronic Voting (E-Voting.CC)

When the long-planned first EVOTE conference took place at Castle Hofen in Lochau/Bregenz, Austria, in July 2004, the dissolution of E-Voting.AT research group had already started; Robert Kofler did not participate. At the conference, several interesting perspectives on electronic voting were presented, including new E-Voting algorithms (Riera and Cervelló, 2004), empirical analysis of early user assessments of E-Voting (Oostveen and van den Besselaar, 2004), security assets (Prosser et al., 2004b) as well as the soon-to-be finalized Council of Europe "Recommendation (2004)11 on Electronic Voting" (Remmert, 2004). During the course of the conference, it became clear that the landscape of electronic voting was quite scattered at that time, and there were similar experiences in different projects and contexts. The proceedings (Prosser and Krimmer, 2004b) were soon out of print due to high demand. This gave the organizers reason to believe that an increased, structured exchange of ideas, research and experiences would generally improve the quality of conduct of E-Voting. In early 2005, Robert Krimmer and Stefan Triessnig joined forces to develop an E-Voting competence community that was based around a database to contain a structured collection of all Internet voting experiences that could be found in literature, classical media and the Internet.

When it was time to organize the second EVOTE meeting for 2006, the Council of Europe was particularly fond of the idea of making the conference an academic forum for reviewing its E-Voting recommendation. It seemed to be the right time to start a competence center instead of a community, and so E-Voting.CC was founded on 24 July 2006. Besides organizing the EVOTE conference series, E-Voting.CC focused on conducting studies and providing consulting on the topic of E-Voting and e-democracy.[25]

After the 2006 conference, the work with Triessnig continued, and data on some 110 uses of Internet voting around the world were collected.[26]

The *Gesellschaft für Informatik* (GI, German association for informatics) was one of the first associations in Germany that organized their internal elections mainly via the Internet (but maintained the ability for voters to apply to vote by mail). The GI had established an *Arbeitskreis* (consultative body) on E-Voting with several members from German academia, such as Rüdiger Grimm, Melanie Volkamer and Robert Krimmer on behalf of E-Voting.CC. The aim was to review and improve the overall security of GI's Internet voting procedures through proposing an evaluation and certification process. The group decided to draft a protection profile in accordance with the Common Criteria standard (2012); the profile was completed as one of the first for electronic voting worldwide (Grimm et al., 2006).[27]

---

[25] One major activity in this area was the contribution to the CoE recommendation on electronic democracy, for which the center drafted annex 1 (Krimmer et al., 2009).

[26] This data is accessible publicly at http://db.e-voting.cc (Krimmer and Triessnig, 2007). The database itself was originally implemented by Daniel Botz and later improved by Martin Androsch (2011).

[27] Other known profiles include the French PP-CIVIS (Direction centrale de la sécurité des systèmes d'information, 2006), the proposed US IEEE standard 1583 (IEEE Standards Coordinating Committee 38, 2005) and the Chinese proposal (Lee et al., 2010).

In a separate effort, Volkamer and Krimmer collaborated to develop criteria for the critical issue of ensuring the everlasting secrecy of a vote (Volkamer et al., 2006). With paper-based elections, it seems obvious that if a vote cannot be attributed to a voter at the time of an election, it will stay unattributable in the future. With electronic elections, however, where the secrecy of a vote often relies solely on the need for enormous amounts of computing capabilities to break its protection, time has become an issue. In this effort, Volkamer and Krimmer identified weaknesses in post-election Internet voting schemes, where the vote and the voter's identity are jointly communicated in one package and only separated during counting.

Further studies by E-Voting.CC included work on election observation (Krimmer and Volkamer, 2006a), E-Voting readiness (Krimmer and Schuster, 2008) and verifiability (Weddeling et al., 2008).

3.4 E-Voting2006.AT

Two years after the second election test of the original E-Voting.at team, Alexander Prosser undertook a third test with a new team and a new cooperation partner, the Wiener Zeitung (Viennese Newspaper). This newspaper is the official journal of the Republic of Austria, and it has a special status due to its ownership by the Federal Chancellery. With this project, the newspaper ventured into new areas in order to broaden its business concept. The idea of the project was to run another election test, but this time, the test would be aimed at the prime target group for Internet voting: Austrian citizens living abroad. This project also implemented the original algorithm (Prosser and Müller-Török, 2002) and incorporated lessons learned from the first two tests, such as exploring the possibility of recovering voting tokens in order to lower the number of voters lost between the first and the second phase of the test. In this test, Austrians living abroad had to register themselves for the test, and 293 actually did. However, only 148 actually participated in the second phase and cast a vote. During the election test, several researchers, including some from A-SIT and the GI consultative body on E-Voting, detected weaknesses in the implementation that would have allowed full access to the project database (Grimm, 2006). This problem was confirmed by the project team and further discussed in their report (Prosser and Steininger, 2006).

3.5 TU Graz

The *Technische Universität Graz* (TU Graz, Technical University of Graz) and its *Institut für angewandte Informationsverarbeitung und Kommunikation* (IAIK, institute for applied information processing and communications) with its head, Reinhard Posch, always had a special role when it comes to E-Voting in Austria. In 1995, a first protocol was written at the institute about conducting elections in local area networks by Vesna Hassler and Reinhard Posch (1995), and in the years thereafter, he was actively involved in making Austria the first country within the European union to pass a law to allow for electronic signatures. He even coauthored the first commentary on the *Signaturverordnung*, the ordinance of the Austrian signature law (Brenn and Posch, 2000). Together with the signature law, the association A-SIT was also given the role as the certification agency for digital signatures (Bundeskanzleramt, 2000). Since its foundation in 1999, Reinhard Posch has been its technical managing director. Also, in the summer of 2000, Reinhard Posch was appointed Chief Information Technology Officer of the Austrian Government. During the negotiations for the passing of HSG in parliament, and section 6 of paragraph 34 was included, which tasked A-SIT to evaluate the conformity of the given E-Voting system with the law without specifying the requirements any further. In 2002, when the work in the Council of Europe started to develop a recommendation on E-Voting, Herbert Leitold, took a leading role in drafting technical parts of the recommendation, including a strong reference to Common Criteria.

Within Austria, he led the BMI technical sub-working-group for technical aspects of E-Voting in 2004.[28] His colleague, Thomas Rössler, prepared a state-of-the-art document on the technical aspects (Rössler, 2004a), as his PhD thesis project "eVita" dealt also with the Internet (Rössler, 2004b). In 2005, they jointly developed an E-Voting protocol (Leitold et al., 2005). In this proposal, they used the Austrian citizen card for identification purposes as well as a hardware security module to decrypt the votes. The protocol establishes the anonymity during the counting of the votes; this approach is very similar to the one chosen in Estonia (see Madise and Martens [2006]).

[28] For more information on this working group see previous section thereon.

At the end of 2005, Martin Mayer, whose diploma thesis Thomas Rössler supervised, approached the Federation of Students of the TU Graz to develop a prototype to be used in the 2007 Federation of Students' elections.[29] In the beginning, the student body was positively inclined towards supporting this effort and debated actively in two meetings of the Federation of Students' university representation body in December 15, 2005 and January 18, 2006. After the debate, the body decided to pursue this project under certain conditions, including full access to the source code of the E-Voting components. One student representative, Hartwig Brandl, expressed in that meeting his discomfort with this decision and pointed out that the representative body for the study program Informatics had passed a resolution against the introduction of Internet voting (Hochschülerschaft an der Technischen Universität Graz, 2005, Hochschülerschaft an der Technischen Universität Graz, 2006). Despite the overall positive decision by the student representatives at TU Graz to pursue this project, it did not take off.

In the fall of 2006, a meeting of all chairpersons of the 21 Federation of Students' organizations in Austria was held by BRZ to determine whether they were interested in organizing an Internet voting pilot. The discussion ended without a concrete decision. Discussions, however, continued in the background. Hartwig Brandl, who was also a member of the national Federation of Students' parliament, had been actively discussing the problems of E-Voting. In the end, various bodies passed three resolutions: the meeting of the student representatives in informatics from Germany, Austria and Switzerland, which met in Graz on 10 December, passed the first resolution (Konferenz der Informatikfachschaften, 2006). It was followed by the student representative body from the faculty of informatics of TU Graz on December 12 (Fakultätsvertretung Informatik an der HTU Graz, 2006). Finally, the national Federation of Students' parliament passed a resolution on December 15 against the use of Internet voting (ÖH Bundesvertretung, 2006; see also Brandl et al. [2007]).

[29] He finalized his master thesis two years later (Mayer, 2008).

3.6 E-Voting in the Austrian Federation of Students Elections 2009

Building upon the work in the inter-ministerial working group, the agreement of the new government at the end of 2006 agreed to introduce postal voting. The coalition agreement also included an agreement to investigate the feasibility of E-Voting.

On May 11, 2007, the Federal Minister for Science and Research *Dr. Johannes Hahn* took the occasion of a speech at the University of Linz to announce the plan to implement E-Voting in the 2009 Austrian Federation of Students' elections. (Hahn, 2007)

3.6.1 The Project

The first step in this project was a feasibility study conducted in the summer of 2007 (Krimmer, 2007). The main task was to integrate E-Voting without compromising the existing paper-based voting in the polling station. To do so, an additional voting channel via the Internet was to be offered from Monday 8:00 through Friday 18:00 during the week before the paper-based election days. During these days, all students of Austrian universities should have the possibility to participate in an Internet election without pre-registration. For identification purposes, the Austrian citizen card (a smart card bearing a digital signature) in accordance with section 2 nr 10 of the 2004 Austrian E-Government law was to be used. After the end of the Internet-based vote casting, the votes were to be stored in an encrypted way until the general counting of votes at the end of the last voting day. Students who had voted through the Internet would be marked "voted" in the voter register, thereby guaranteeing the one-man-one-vote principle. The next step was then to adapt the legal framework.

3.6.2 Updating the Federation of Students' Act (HSWO)

As the HSG already allowed the use of electronic voting, only the HSWO had to be changed to give directions on how to implement electronic voting. The Federal Minister was authorized by virtue of § 48 HSG to introduce electronic voting with a regulation. The corresponding amendment to the Austrian Federation of Students' Act was issued on October 2, 2008 in BGBl II 351/2008. The amendments included the following:

- The definition of specific E-Voting terms;

- The integration or modification of deadlines, which depend on election day;

- Adaptations, additions and amendments resulting from the introduction of the electronic voting system and the election administration system.

3.6.2.1 Definition of terms

The terms necessary for E-Voting were specified by the definitions of the new § 1 HSWO. With reference to § 34 Para. 4 HSG, it was determined that E-Voting is an electronic procedure of distance voting using the Internet. This requires two systems:

- The electronic voting system used to conduct E-Voting. According to § 64 Para. 1, the Internet portal consists of the central access point for all eligible voters to vote and obtain information on E-Voting as well as the election server software and the E-Voting client.

- The election administration system function is to assist the Election Commission in the performance of its tasks during the election.

Both systems are maintained by the Federal Minister in accordance with § 61 HSWO and are made available to the election commissions.

3.6.2.2 The Electronic Voting System

The additions required for the use of the electronic voting system were mainly regulated in the newly inserted section 8 HSWO. This included regulations on the type of identity verification, requirements for the electronic voting system, operation of and access to the electronic voting system, counting and declaration of invalidity of votes cast by means of E-Voting. Moreover, § 61 HSWO stipulates that the electronic voting system must comply with § 34 and § 39 HSG.

3.6.2.2.1 Technical Requirements for the Voting System

The technical requirements for the voting system (i.e., client, election server software, Internet portal) are regulated by § 64 HSWO. The regulatory authority specified that the system being used must be state of the art (e.g., it must include blind signatures, homomorphic encryption, mixers[30]), and the points below must be ensured:

- Anonymity of the election process, (§ 64 Para. 2);

- The client must be able to run on standard operating systems and Internet browsers (§ 64 Para. 5);

- The election process must be offered uniformly in German as well as in other languages if necessary and possible (as required by § 64 Para. 5) and

- The Internet portal must be designed in an accessible way (§ 64, Para. 6).

3.6.2.2.2 Certification of the election system

The election system shall be certified by the Confirmation Authority 60 days before the first day of the election. In particular, the recommendation of the Committee of Ministers of the Council of Europe to the Member States should be reviewed and existing, applicable protection profiles[31] should be drawn up in accordance with Common Criteria (§ 64 Abs 3 HSWO). Moreover, for the purpose of verification by experts, the members and observers at the Election Commissions are also given access to the source code of the client and the election server software and the verification report of the Confirmation Authority (§ 64 Para. 7 HSWO).

---

[30] For an overview of the technologies used, see Volkamer and Krimmer (2006).

[31] The deadlines specified in §§ 20 Para. 3, 22 Para. 1, 26 Para. 6, 28 Para. 3 and 29 Para. 1 to 3, § 51 Para. 1 and 2 were accordingly moved earlier by one week.

3.6.2.2.3 Operation and access

After the election server software has been examined within the scope of acceptance of the voting system, § 65 HSWO stipulates that it must be operated in a highly secure data center with the greatest possible transparency while maintaining secrecy of the ballot and protected against physical and virtually unauthorized access. Access to these premises may only be possible to persons previously accredited by the chairperson(s) of the Election Commission. The criteria for accreditation are to be decided at a meeting of the Austrian Federation of Students' Election Commission.

In § 66 HSWO, the Austrian legislation specified special electronic voting system security requirements for the time period where E-Voting starts until the votes are counted. The votes cast by E-Voting shall be kept secure until the vote count is carried out within the framework of the electronic voting system. The decryption of the secured votes shall only be possible with the entering of two keys, which are sealed by the Election Commission and remain sealed until the end of the election.

3.6.2.2.4 Archiving

Under the continuous protection of secrecy of the ballot, the client and the election server must be archived three weeks after the last election day and will be handed over to the chairperson of the Austrian Federation of Students' Election Commission. The latter must keep the archive for at least five years, in the event of an objection, at least until the end of last-resort proceedings (§ 69 HSWO).

3.6.2.2.5 Starting, interrupting, resuming and terminating

With the introduction of electronic voting (E-Voting), the task field of the Election Committee had to be expanded and adapted to the requirements of E-Voting. According to the HSWO amendment, the Election Commissions are now responsible for starting, interrupting, resuming and terminating the E-Voting process at the respective universities (§ 14 Para. 1 (17) HSWO).

3.6.2.3 Electronic Voting Process

3.6.2.3.1 Deadlines and access to the voter lists

The realization of E-Voting as an advanced vote requires some changes in election procedure. Thus, according to § 62 HSWO, electronic voting takes place from 8:00 a.m. on the eighth day to 6:00 p.m. on the fourth day before the first election day. In case of interruptions, this period may be extended to 12:00 a.m. Since § 35, Para. 8 of the Federation of Students' Act stipulates the time between the deadline and the first election day as seven weeks, the time period for the inspection of the voter lists was reduced to one week (§ 20 Para. 1 HSWO), and the other deadlines needed to be adjusted as well.[32] To compensate for this, a new option was created in section 3 for individuals to be able to review their voting eligibility via the Internet portal using their citizen card. The paper-based election register had to be used to check the voting eligibility of other voters.

3.6.2.3.2 Voting

The citizen card serves as a proof of identity for participation in the election by means of E-Voting, according to E-GovG (§ 63 HSWO).

Changes were made to §§ 37, 38 and 39 HSWO with regard to exercising of the right to vote, the determination of voter identity and the avoidance of double votes. § 37 Para. 1 HSWO added E-Voting as an alternative voting method; § 38 in conjunction with § 63 HSWO specified that a citizen card can be used as proof of identity. In § 38 Abs 3 in conjunction with § 39 Abs 1 HSWO, the Austrian legislature regulated that voters who cast e-votes get tagged on the voter list as having e-voted and thus can no longer participate in the conventional paper ballot process in order to exclude a double vote by means of E-Voting and conventional paper ballot process. This can only be done by scheduling E-Voting a week before the conventional paper ballot process.

[32] See Grimm et al. (2006) and FN 27.

A number of additional adaptations were necessary to handle E-Voting ballots the same as paper ballots. Thus, a consent confirmation provision was made for all e-votes. This stipulates that before the vote can be cast legally, the selected voting option has to be reconfirmed with a validity note (§ 39 Para. 5 HSWO in conjunction with § 34 Para 5 (5) HSG). This regulation is intended to be the equivalent of another look over the ballot before casting it into ballot box. In addition, it was stipulated that the election options must be represented as much as possible on the electronic ballot the same way as on they are on the traditional paper ballot, and, by means of appropriate technical measures, all election options must be brought to the attention of the voter before casting the final vote. Invalid votes[33] shall also be allowed (§ 43 Para. 1 HSWO). The validity of the started election activities by means of E-Voting must be ensured in the same way as the conventional paper ballot by the chairman or at the end of the period. 20 minutes were granted in §39 Para. 6 HSWO for this purpose.

If the student's PC does not work for electronic voting, the student may also cast his/her vote on a computer provided by the Principal with visual protection and the technical components for the use of the citizen card pursuant to § 33 Para. 1 HSWO at the university.

3.6.2.3.3 Rules for declaration of invalidity and interruption

In order to safeguard the secrecy of the ballot, the legislature stipulated that a certain number of votes must be given per Election Commission, since there would otherwise be a risk that conclusions could be drawn about the electoral behavior of individual persons due to the low number of votes. If fewer than three votes are cast for an institution to be elected, they must be deleted and declared invalid. The E-Voting tags on the list of eligible voters must be deleted, the affected voters must be immediately informed about this and they must be invited to recast their vote in writing (if possible also by telephone and email or fax) (§§ 66 and 67).

[33] Invalid votes are possible by selecting more options than allowed.

In circumstances that prevent voting, the Election Commission must interrupt the election. Such a circumstance is, in particular, the non-availability of the electronic voting system due to technical problems or attacks on the election system that hinder the proper conduct of the election process. In case of imminent danger, such an interruption or postponement may also be carried out by the chairperson of the Austrian Federation of Students Election Commission. It is also their responsibility to resume the E-Voting process once the danger has passed (§ 48 Para. 1 HSWO).

The respective Election Commission decides on the validity of the votes cast before the interruption, after consultation with the Confirmation Authority pursuant to the Signature Law (§ 39 Para. 7 HSG).

3.6.2.3.4 Vote count

The legislation stipulates special security requirements for the electronic voting system for the time from voting by means of E-Voting until the votes get counted. The votes cast by E-Voting shall be kept secure until the vote count is carried out within the framework of the electronic voting system. The decryption of the secured votes shall only be possible with the entering of two keys, which are sealed by the Election Commission and remain sealed until the end of the election (§ 66).

The safeguarding of the secrecy of the ballot is regulated, in particular, by the fact that the individual vote is encrypted with the public key of the Election Commission.[34] This prevents the vote from being counted before the end of the paper ballot. For this purpose, the Election Commission for the Austrian Federation of Students had to be assigned the task of handling the generation, administration and addition of two electronic keys for the encrypting of the vote while preserving anonymity (§ 15 (7) HSWO). The chairperson

[34] An asymmetrical encryption method is used for this purpose. The public key is made available to the Election Commission; the private part is only used for decoding at the beginning of the vote count.

must generate the two electronic keys—one must remain with him/her, and the second one must be left to the entire commission (§ 35, Para. 5 HSWO). The entering of the electronic key in the electronic voting system must be carried out by the chairperson and another member designated by the Election Commission. Thereafter, the keys shall be kept sealed until the beginning of the count (§ 35 Para. 6 HSWO), and the presidents of the Austrian Federation of Students Election Commissions shall be informed about the entering of the key ((§ 35 Para. 7 HSWO).

This procedure takes place at the premises of the datacenter after conclusion of the last election activity (§ 66 HSWO) on the last election day after 5 p.m.

3.6.2.4 Election Administration System

The election administration system was developed to support the Election Commissions necessitated a number of changes to the HSWO.

3.6.2.4.1 How is the data for the creation of voter lists collected?

The data regarding the voters are based on the databases of the universities and are regulated in § 7 UniStEV 2004 and operated by BRZ *ex lege*. This is an information system according to § 50 DSG 2000, which is operated by the BRZ based on § 7 UniStEV 2004 and is reported to be DSG 2000-conform. In order for the chairpersons of the Election Commissions to be able to create voter lists, they are authorized to access this database in accordance with § 7a UniStEV 2004 (in conjunction with § 6 Para. 1 (2) HSG). This authorization is further regulated by § 8 Para. 2 BiDokG, where administrative procedures for data security are set out.

3.6.2.4.2 Creation of voter lists

In § 18 Para. 1 and 3 HSWO, the respective chairperson of the Austrian Federation of Students Election Commission is entrusted with the task of drafting a preliminary voter list; then, the final voter must be drafted by comparing with the reporting date during the winter semester. The duplicate creation is necessary because of the complex organizational effort required to create area-specific person identifiers. This register must be generated in paper form up to five weeks before the first election day, and it can be updated and printed out after electronic voting at the latest one day before the first election day pursuant to § 18 Para. 7 HSWO.

3.6.2.4.3 Sector-specific person identifiers

Sector-specific person identifiers (bPK) are required according to the E-Government Act (E-GovG) so that citizen cards can be used without prior registration for electronic voting. Pursuant to § 10 Para. 2 E-GovG, area-specific person identifiers can only be created without a citizen card by the Civil Registry Office. To this end, the chairman of the Election Commission submits a request to the Civil Registry Office for initial provision of an entire data application with area-specific person identifiers according to § 16 Para. 2 StZRegV. Since area-specific personal identifiers can only be generated by the Data Protection Authority as the Civil Registry Office according to § 7 Para. 1 E-GovG, the processing of the personal data in accordance with DSG 2000 is ensured.

3.6.2.4.4 The Chairperson of the Election Commission and Clients in the Sense of the Data Protection Act 2000

In § 18 HSWO, the chairperson of the Election Commission is assigned the task of creating the voter lists. For this purpose, he/she can use a service provider pursuant to § 10 Data Protection Act 2000 and conclude an appropriate agreement. It must be taken into account that sensitive data is being processed, i.e., the political opinions of individuals, and therefore a preliminary verification of the data application is required pursuant to § 18 Para. 2 DSG 2000.

3.6.2.4.5 Documentation of the Election

The Election Commission is supported in documenting the election in that the predefined documents have been translated into corresponding electronic forms with fill-in assistance. In the unlikely event of a failure of the election administration system, it will be ensured that the paper-based templates of documents 1 to 13 can be used,[35] since only the respective paper-based document is legally binding.

This particularly facilitates documentation of the election process, since according to § 33 HSWO, the president of the university shall provide computers with which a non-binding and additional electronic voter lists and voting record must be kept using the election administration system pursuant to § 40 Para. 2 HSWO.

The results of the election are also transmitted with the election administration system according to § 46 Para. 9 HSWO.

3.6.2.5 Summary of Principles for Electronic Elections

With the approval of electronic voting within the framework of §§ 34, 39 and 48 HSG, the legislators have created the legal basis for E-Voting for the first time in Austria.

With the amendment of the Federation of Students Elections Act published in October 2008, the Federal Minister for Science and Research issued the applicable law to be implemented by the Federation of Students elections in the second quarter of 2009.

Overall, the first-time implementation of E-Voting in Austria represents a particular challenge in which many legal aspects had and still have to be taken into account. The provisions of HSWO 2005 presented in more detail here thus represent a milestone in the path towards an electronic democracy.

---

[35] See §§ 34 Para. 2, 46 Para. 9, 47 Para. 1, and 57 Para. 1 HSWO

3.6.3 E-Voting from the Voter's Point of View

The following chapter explains E-Voting from a voter's point of view. In addition to the web portal, checks on voting entitlement, management of the election and the test code verification is described.

3.6.3.1 The Web Portal

For the elections to the Austrian Federation of Students in 2009, a web portal was provided for the first time on the part of the Federal Ministry of Science and Research (BMWF) at www.oeh-wahl.gv.at. On technical safety grounds, it consisted of two websites—one with the contents (web front end) and one with the voting technology (application). The website's aim was to provide students and interested parties with information on the Austrian Federation of Students elections with its contents as well as to provide them with all the official documents available for download.

Figure 2: Design of the web portal

The second voting technology website can be described as an electronic "voting booth". The actual electronic election took place on it. The URL for this website was not communicated on technical safety grounds but was merely linked to the banner on the www.oeh-wahl.gv.at website. The electronic voting booth could be directly accessed through corresponding clicks.

Students who vote or wish to inform themselves about the elections, members of the Election Commissions, Federation of Students representatives, journalists, Federal Ministries, advocates of E-Voting and interested parties (nationally and overseas) and opponents of E-Voting-were identified as target groups.

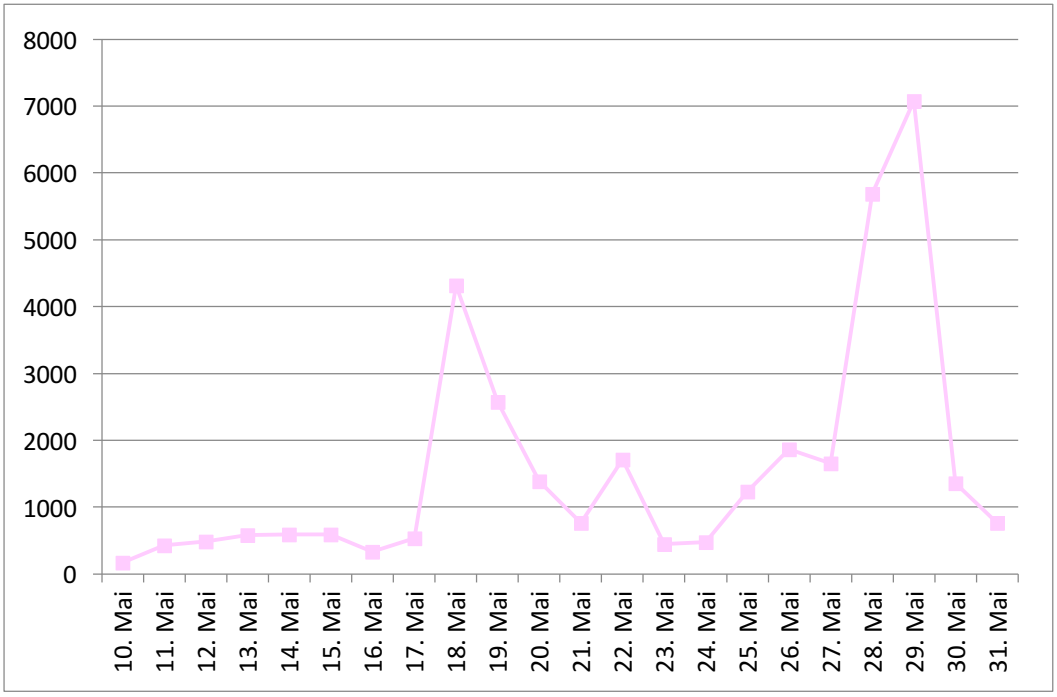

Figure 3: Access statistics for unambiguous visitors to oeh-wahl.gv.at

Established Internet portal. Visitor statistics show that on the first day of voting for the electronic elections, over 4,000 unique visitors accessed the website of www.oeh-wahl.gv.at. The number of daily visitors then dropped at an increasing rate until, on the last day of online voting, once again almost 2,000 visitors accessed the website. At the end of the paper-based election, the number increased significantly to 7,000 visitors per day. This allows us to conclude that the website not only established itself successfully as an E-Voting platform, but it also became a central website for information on election results and additional information relating to elections to the ÖH.

The content of the website was continuously delivered, improved and extended throughout the course of the project by the project team of the Federal Ministry for Science Research and Economy. Information on concrete use by the election client was in turn handled by the Federal Ministry. In any case, the structure of the website fulfills and exceeds the legal requirements for barrier-free access.

A version of the Internet portal was placed on the Internet by a group running in the election.

Figure 4: Persiflage of the oeh-wahl.gv.at website (image altered)

Trusting the Internet portal. The choice of an ".gv.at" address represents an important security feature. In addition to certification by a trustworthy service provider, it would have been possible to use what are known as Extended Validation Certificates, with which additional identification characteristics are anchored in the website's certificate. In principle, we should ensure that a certain address becomes established among the student body so that other websites with similar content are not called up by accident (for example, through a Google search) when trying to vote in the election. For example, a

canvassing group published a fictitious election website at a similar web address (see illustration above), where visitors were also offered election-based services, and an election was simulated. We must add that precisely these actions contradict the statement of principles recommended by the Council of Europe and presented to the groups campaigning in the elections to the Austrian Federation of Students.

3.6.3.1.1 The Self-Diagnosis Tool

A self-diagnosis tool was presented to the students, making it easier for the end user to determine whether they had installed the software required for E-Voting.

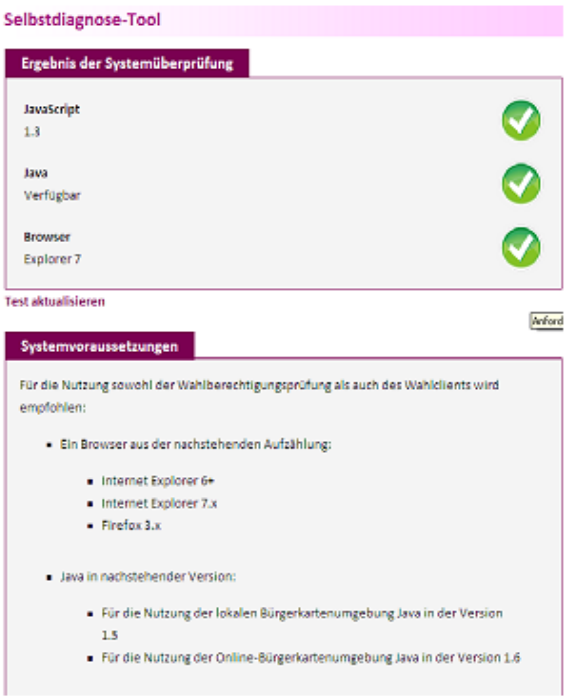

Figure 5: Self-diagnosis Tool

Furthermore, students could call up all the documents provided by the respective electoral commission as well as the ordinance on the voting dates. Altogether, around 400 documents were available. Sub-dividing them according to universities and subject majors ensured simple and rapid access to documents sought. The results were published in the results region after the elections and were structured according to university.

Helping students to help themselves. The self-diagnosis tool was very well received and was used by students. It proved to be an important tool for fault analysis as part of the support process during the election. In terms of improving the self-diagnosis tool, experiences in the 2009 elections for the Austrian Federation of Students revealed the following:

- It is necessary to check the Java version, and it is very helpful to check the Java distribution;

- The interface between Java applets and the citizen card environment should be tested.

3.6.3.2 The E-Voting Process from Voter's Point of View

We can supplement our discussion of an electronic election from the voter's point of view by listing the procedures in the election App. In the present project, the following steps occur:

1. First, the website http://www.oeh-wahl.gv.at is visited, and then the field "To field for submitting vote electronically" is selected in the top right.

2. Next, the student selected the university at which they wished to exercise their right to vote. In cases where the potential voter wished to vote at more than one university, the election process described below would have to be repeated for each university.

3. After selecting the university, the voter received precise instructions for how they could register their citizen card securely:

- Firstly, the card-reader device must be connected to the computer, and then the citizen card must be inserted into the reader device.

- Now, the voter has the opportunity to either use the online citizen card environment or the previously installed local citizen card environment.
- Following this, the voter is prompted to input their four-digit PIN Code[36] in order to identify themselves.

- Next, the voter had to confirm their identity with an electronic signature, triggered by inputting the six-digit PIN Code.

4. All ballot cards were displayed in sequence once the voter's right to vote had been successfully checked.
   - First, the ballot card for the university representative board is displayed. The voter could select one of the groups standing for election.

   - Next, the ballot paper for the university studies representative board is displayed, for which the corresponding voter was entitled to vote. The voter is able to select three to five candidates here. The exact number that could be chosen is shown in the top half of the screen above.

5. Invalid votes could be triggered by selecting no candidates or too many candidates.

[36] The length of the PIN Code that must be input will differ according to the signature card used. Details in this document refer to e-card on the basis of the high distribution where the PIN Code to approve the personal identifier has four digits and the PIN Code to trigger the qualified signature has six digits.

6. Once all the ballot papers have been completed, the ballot sheets are displayed once again in an overview with all options chosen. This protects against submitting votes too quickly (Protection against Haste).

7. Finally, the vote is submitted with a declaration made in place of an oath that the electronic vote was filled out personally, unobserved and uninfluenced, through inputting a six digit PIN Code.

8. Following the successful storage of the vote(s), the voting system displayed a check code and the associated confirmation code. Once this is noted by the voter, the user is then able to check on the website after the end of the election whether their own vote has also been counted.

The e-voting process is supplemented by cryptographic steps, which are represented here for submitting and counting postal votes in a postal election.

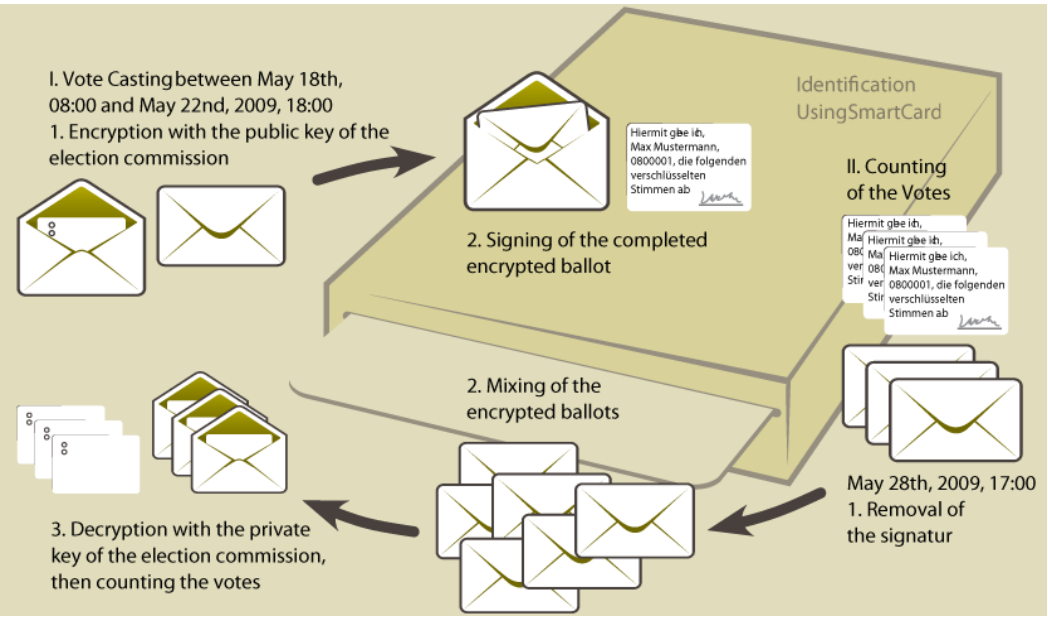

Figure 6: Overview of the e-voting process

3.6.3.3 The E-Voting Process as an Election Application

The following portrays reproduce the process of the voting event.

3.6.3.3.1 Selecting the University

In an initial step, the student selects the university at which they wish to cast their vote.

Figure 7: Selecting the University

3.6.3.3.2 Selecting the Citizen Card Environment

Next, the student must select the citizen card environment they wish to use. Voters have the choice here between the local citizen card environment and an online citizen card environment. The local citizen card environment requires successful installation of a version of the citizen card software, whilst the online citizen card environment is a Java applet, which can be downloaded from the respective website prior to each use.

These screens further offer a representation of subsequent authentication. Here, we portray the difference between the two PIN Codes required for this in text and also using graphics.

The online citizen card environment is used as a further consequence. The local citizen card environment has an analogous format.

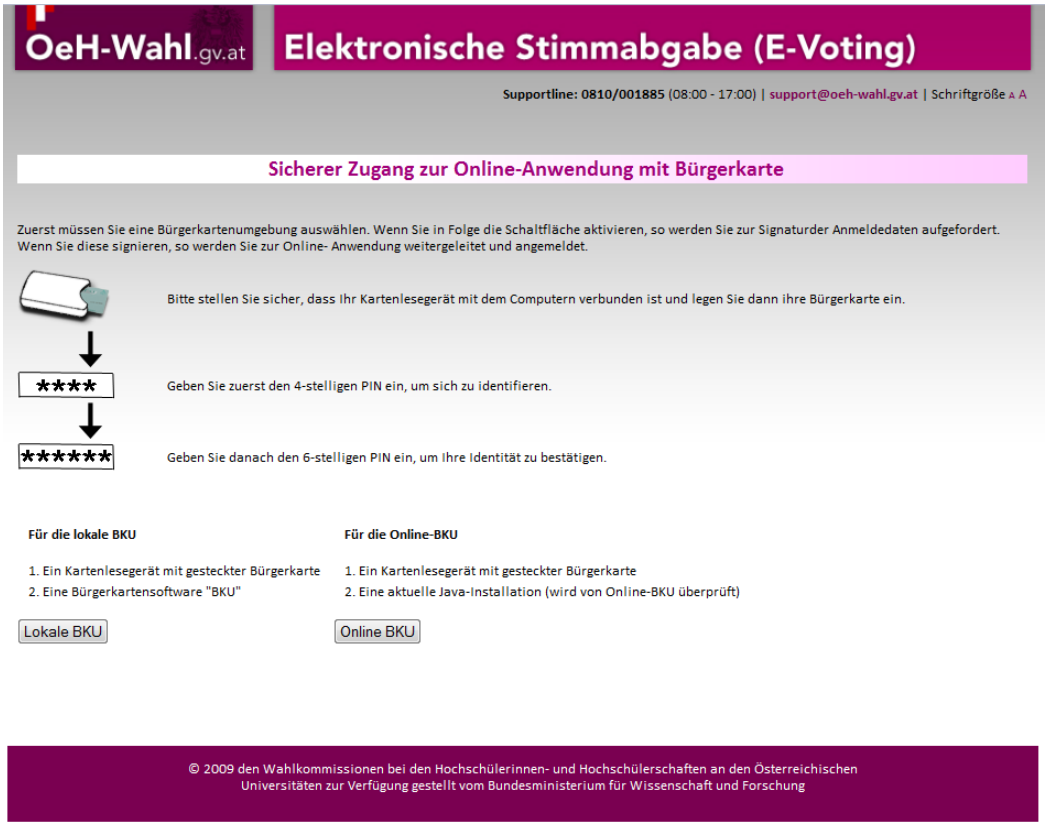

Figure 8: Selecting the Citizen Card Environment

The online citizen card environment is signed digitally on safety grounds. The digital signature can be checked by the voter.

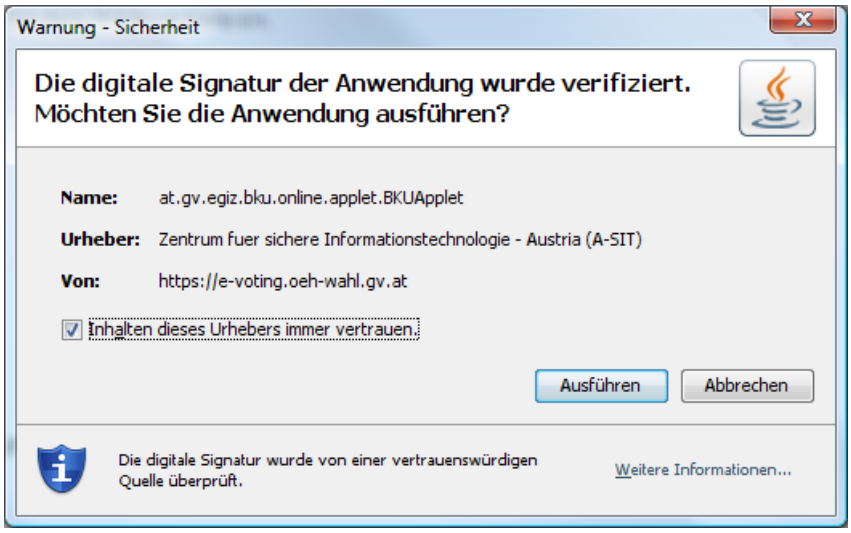

Figure 9: Signature in the Online Citizen Card Environment

3.6.3.3.3 Inserting the Citizen Card

As soon as the online citizen card environment has started up, an iFrame opens with appropriate instructions to insert the citizen card into the card-reading device (if it has not already been inserted into the card-reader) to input the four-digit PIN Code and after this the six-digit PIN Code.

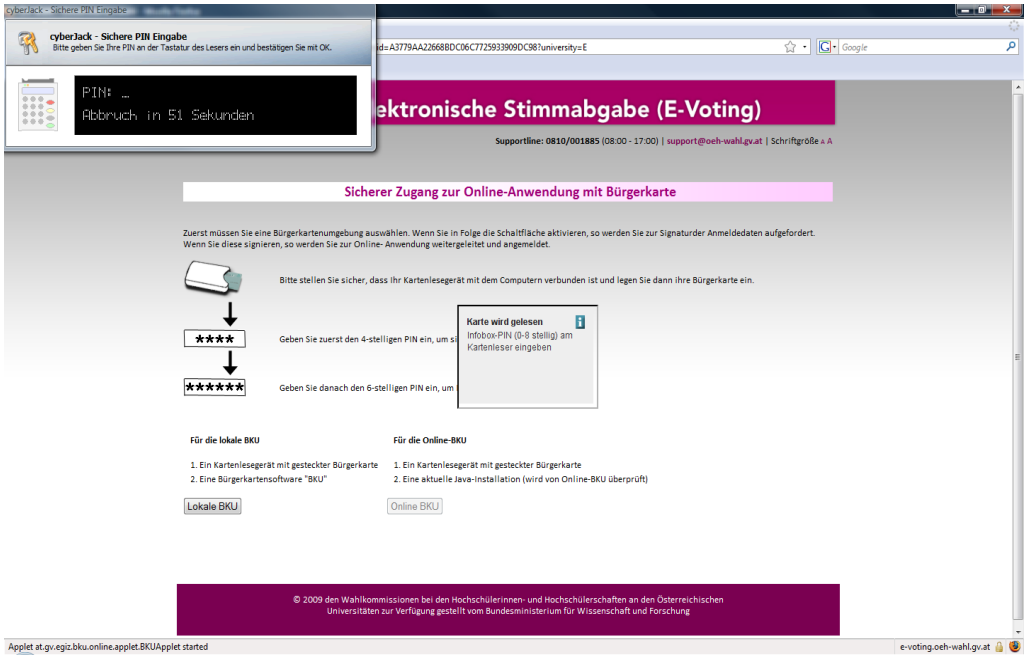

Figure 10: Registration

3.6.3.3.4 Displaying the Ballot Paper for the University Representative Board

The E-Voting client opens following successful authentication, which was likewise realized as a signed Java applet on safety grounds. Analogous to paper-based voting, the voter first receives the ballot sheet for the election to the University Studies Representative Board at the chosen university.

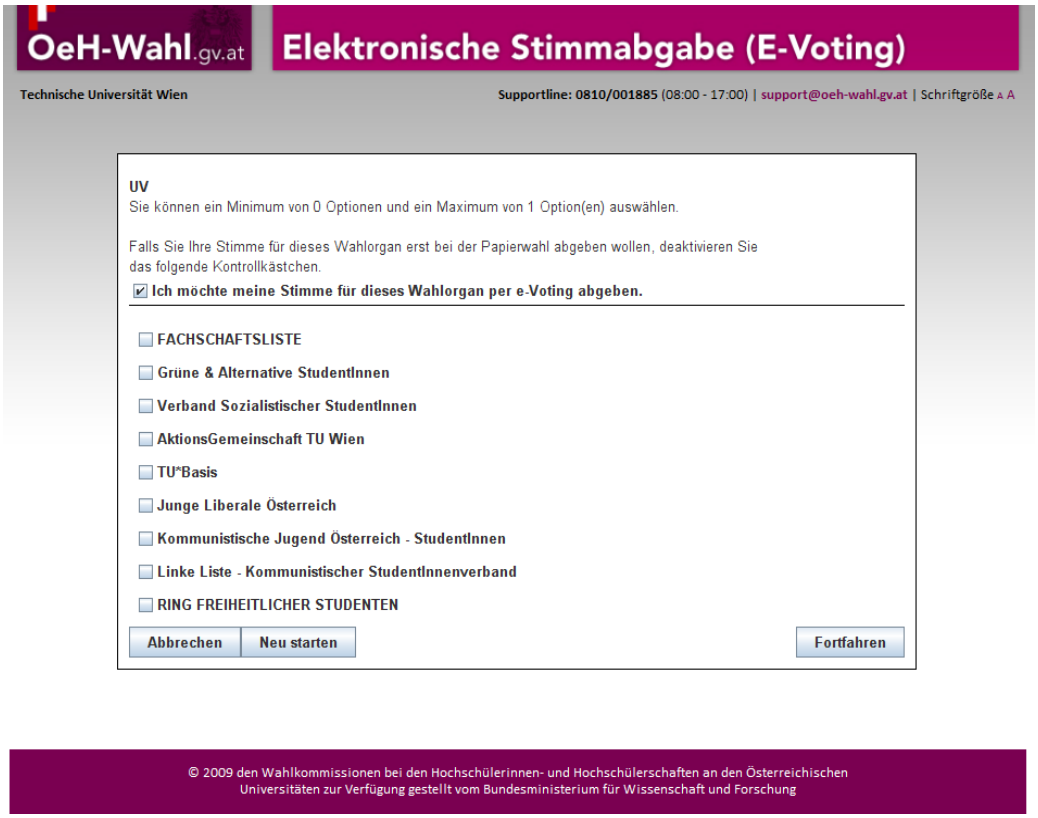

Figure 11: Ballot Sheet for the University Students' Representative Board

3.6.3.3.5 Displaying Ballot Papers for Student Subject Representative Board

By pressing "Continue", the voter now receives the next ballot sheet. After the ballot sheet for elections to the University Representative Board, all the ballot sheets for the election to the University Students' Representative Board follow. A student may take part in none, one or a number of the elections to University Students' Representative Board at a university corresponding to their voting rights. The voter can decide for each ballot whether the ballot paper should be submitted electronically or in the traditional paper form. A mixture of routes is possible, so that, for example, votes for the University

Representative Board and the Study Representative Board may be submitted by E-Voting, while the remaining University Representative Board votes may be submitted via the paper-based election.

The box labeled “I should like to submit my vote for this elected body by E-Voting” is activated by default. If it is deactivated by the student, then the ballot sheet is grayed out, and no voting option can be selected. This also includes when using a screen reader. This means that it is not possible to submit a vote electronically for the elected body given on the ballot sheet, but a paper-based route is instead required.

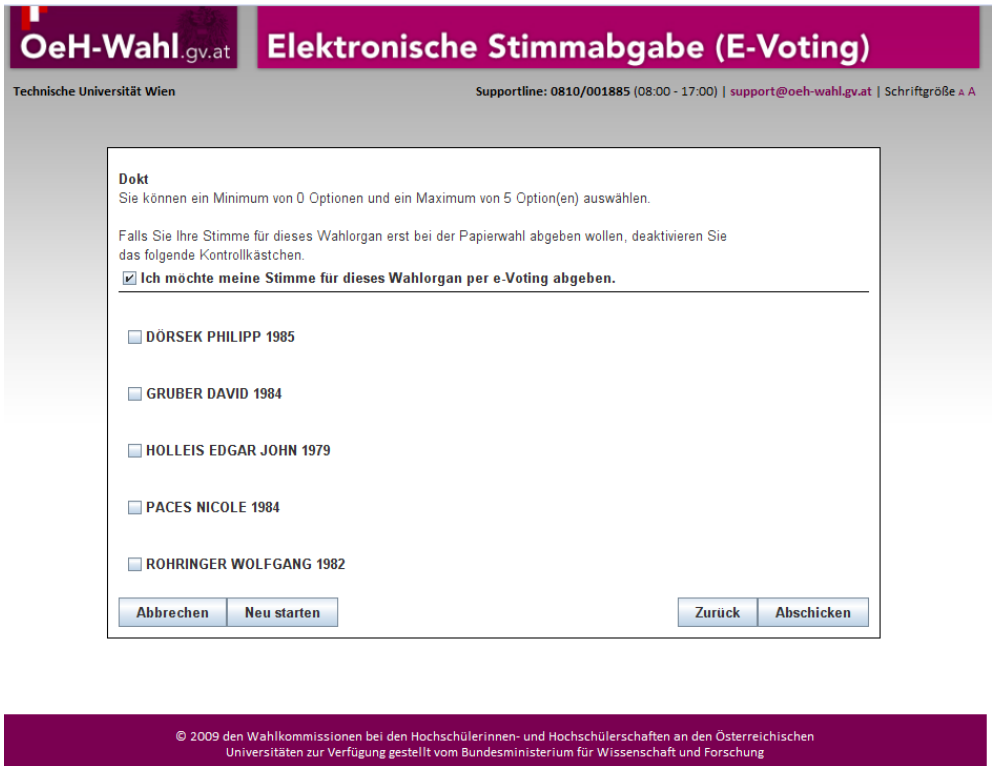

Figure 12: Ballot Sheet for a University Studies Representative Board

3.6.3.3.6 Protection Against Haste

Once the last ballot sheet has been filled out, the so-called excess haste protection appears. All of the voting options selected are displayed here once again, and the voter must confirm them once more. If a ballot sheet should prove invalid or if all of the voting options have not been exhausted, then the student is informed of this in the images portrayed — for example, in the election to the University Studies Representative Board, the choice of three to five options is possible, which are often not all used. In this case, these are merely instructions, and submitting invalid ballot sheets is still possible in spite of these instructions.

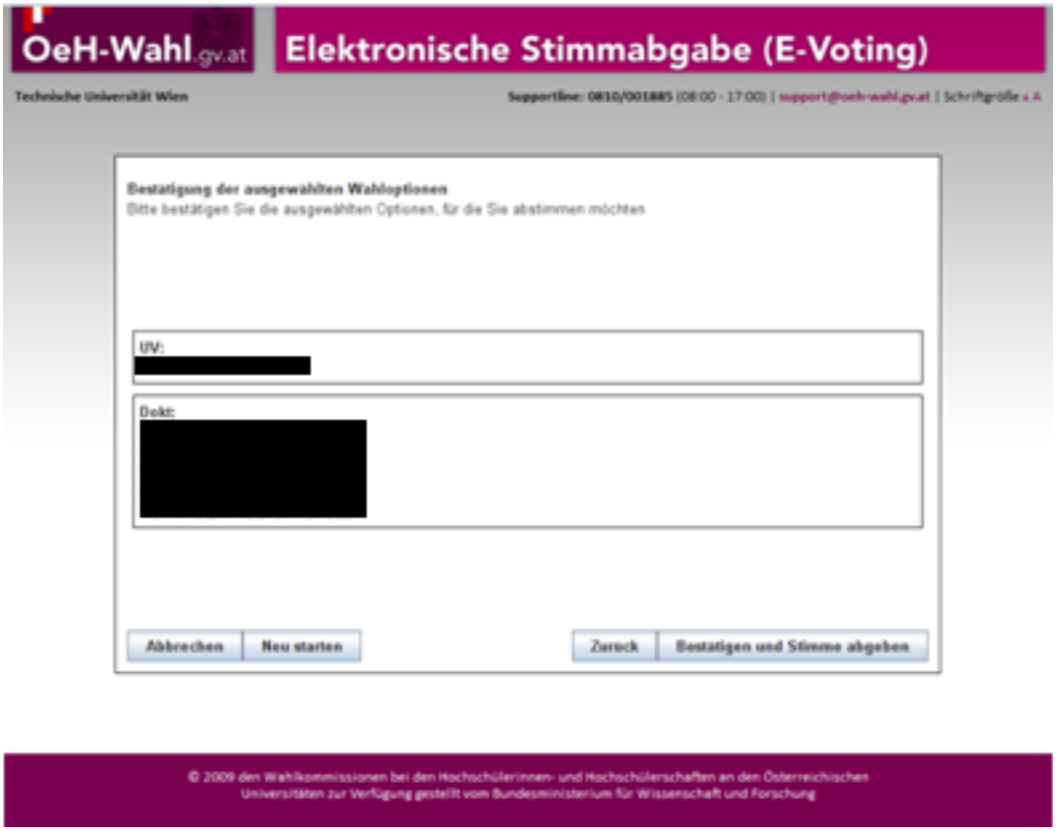

Figure 13: Protection Against Excessive Haste

3.6.3.3.7 Declaration in Place of an Oath and Confirmation

Immediately before submitting the vote, the student is prompted once again to input the six-digit PIN Code. The voter signs a declaration in place of an oath in a similar way to paper-based elections that the vote was submitted unobserved in secret and without any undue influence. The encrypted ballot sheet is signed by the voter electronically.

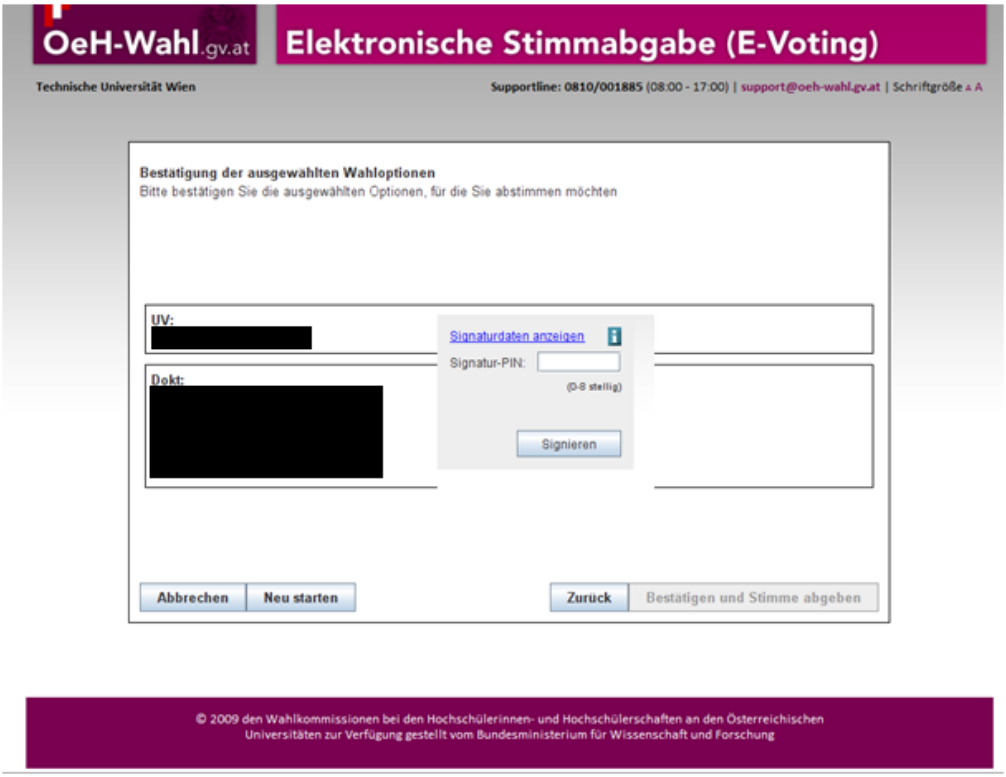

Figure 14: Confirmation of Casting the Vote

3.6.3.3.8 Depicting the Check Code and Confirmation Code

Once the vote has been submitted, the student reaches a page that confirms the vote has been successfully cast. In addition, the check code and confirmation code are portrayed including an explanation. The confirmation page provides the opportunity to print it off, as some web-browsers merely print off the web-page with their internal browser print option; it does not not, however, print the content of the applet. Using the button “Return to University selection”, we return once more to the page that lists all of the universities. To cast a vote at another university, the voter must first authenticate themselves once more.

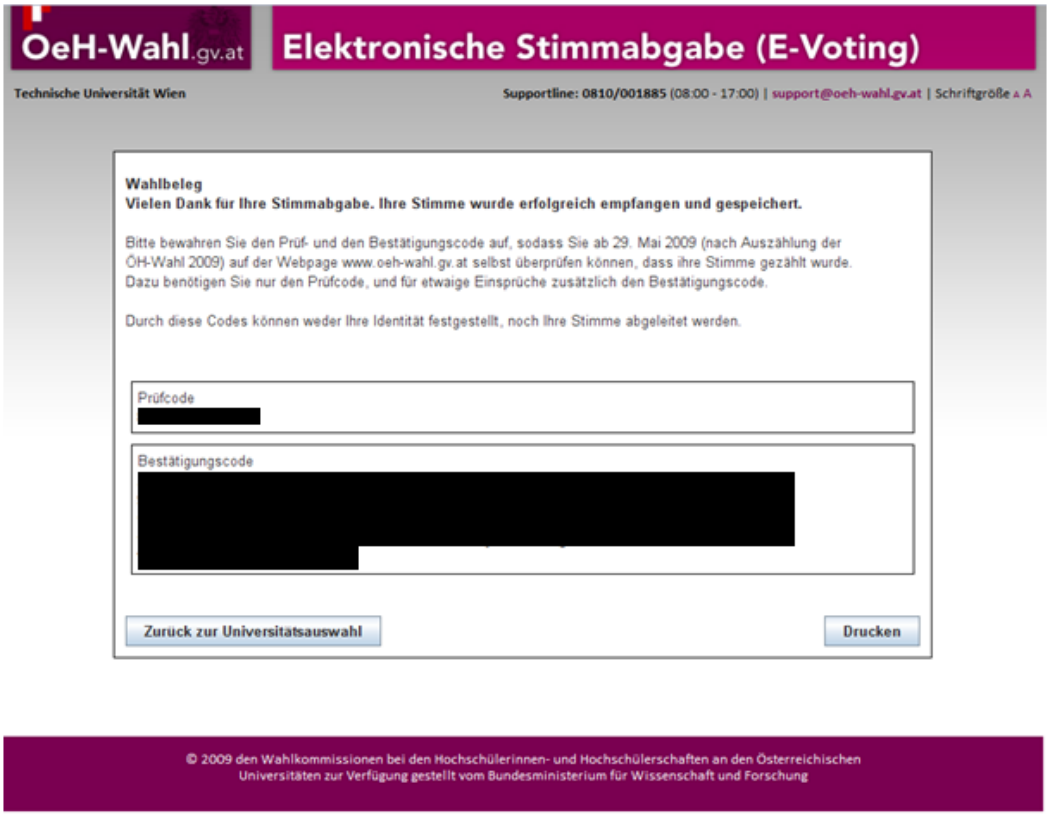

Figure 15: Confirmation Page with Check Code

Example of a check code:

```
8bef3c8e07b8fe76
```

Example of a confirmation code:

```
KYPquQl2IuFkABwFKIYia0v95NQKqJCOanWXAVIdj7nYTh0HuD57srqp+wfNEgPSLw
H3cxExyItV1zI5D6oLRjdfJqzJiBusZNSITEtEyDpeT1D7FEpcm4tlRm
FPLteKTCj1TSmw9crO7fvbJhC+u1uIZJTZfbaz9C69l2B0nvKI7IaIyH7F+nHn
G2hFAnHSznJ5sLmCJTlMND+rb9YgtJasXkScIghTf4pZz0D9QWRjrSnTfL1+UbAKqL
GbWNwKljFwrdw/0c8gCac5fMhn5z2iSuUw4DbFJvEEeokrr1nwrc9
snaY96z8/kadZ1KxUVSSbz7nDZF9iQWwDuQ6XCA==
```

3.6.3.3.9 Attempt to Submit a New Vote

If a student has exercised their right to vote at a university and has registered again, then a corresponding instruction is issued.

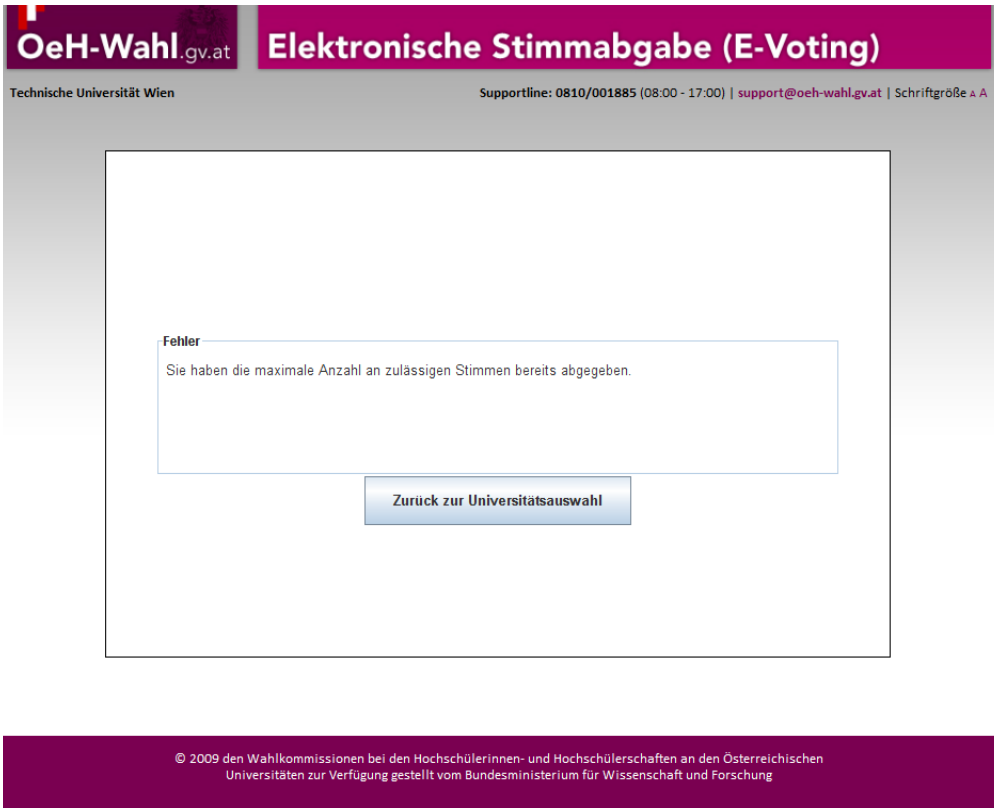

Figure 16: Notice of renewed registration after successfully submitting a vote

3.6.3.3.10 Opportunities for Improving the Election Process

Submitting a new vote by overwriting the previous vote submitted would be technically possible without endangering the secret election process; however, this is not provided for in HSWO 2005. Theoretically, changing votes with subsequent votes (i.e., over-writing votes) would also be possible during paper-based voting.[37]

[37] These processes were introduced in Estonia as a measure against vote-buying and voter coercion.

Since the choice of the citizen card environment has proven in part to be not user-friendly, interactive selection is possible using the Ministry of Finance's E-Government solution.

Figure 17: Authentication on FinanzOnline by means of an integrated online citizen card environment

Selecting the citizen card environment. The intention was to let students select the citizen card environment. This is not uploaded until the citizen card environment to be used has been selected. Selecting the citizen card environment was viewed by students as not necessary and complicated. Integrating citizen-card-based authentication in a similar format to that used by Finanz-Online[38] would be worth considering.

Here, the online citizen card environment is launched straightaway, and the user – in order to use the local citizen card environment – must click on his or her own button. This normally saves the user an additional selection step.

[38] Finanz Online offer authentication by means of the citizen card, see https://finanzonline.bmf.gv.at. Improvements to the images portrayed are possible using the online citizen card environment. The iFrame was judged by students as being too small or not sufficiently clearly noticeable, although it appears in the center of the browser window. The size of the representation of the iFrame for the online citizen card environment could be dynamic, appropriate for the computer screen resolution and the size of the browser window, or it could blank out the remaining content of the browser window or could "gray it out".

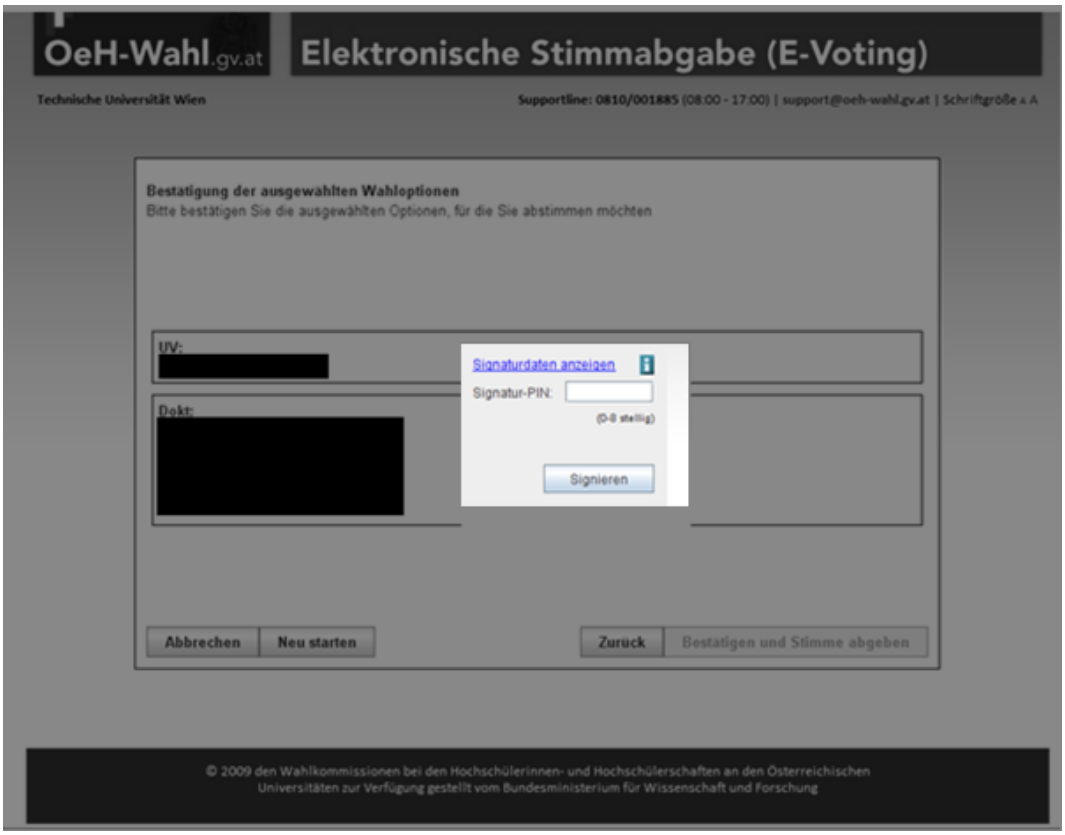

Figure 18: Sketch – Highlighting the Citizen Card Interaction

In this illustration, we portray how the citizen card interaction could, for example, be emphasized or highlighted by darkening the remaining area of the screen.

Improved citizen card integration and interaction. The difference between inputting the six-digit PIN code (for the digital signature) and inputting the four-digit PIN code (to authorize the identity link) should be clear and understandable throughout the entire election process and in all components required for it (e.g., in the online citizen card environment and the local citizen card environment). An advantage for the online citizen card environment arises here, since this can be designed in a manner to better integrate it into the overall process in terms of a user interface.

The error messages from both MOCCA and MOA should be more easily configurable for users. For example, in the case of non-modified implementation of MOA, “identity link not found” means that the four-digit PIN code was entered incorrectly.

For security reasons, a time-out was implemented when using the online citizen card environment for signing the statutory declaration and the encrypted ballot sheet.

The time-out was configured at thirty seconds. Should the time-out be exceeded, the student is logged out, and a page opens with an additional indication that the vote was not cast and that it is therefore possible to try again. This restriction of a time-out did not pose a problem for the test group in the run-up to the election, but it led to several phone calls during electronic voting.

Both over-writing votes by casting more than one electronic vote as well as over-writing a vote submitted electronically by casting a paper vote represents an interesting possibility regarding additional security against vote-buying. Furthermore, it would combine the advantages of both election procedures. Adapting the Austrian Federation of Students electoral rules would be necessary in order to render this principle possible.

The voter did not have full orientation throughout the entire voting process This could be improved using graphic elements.

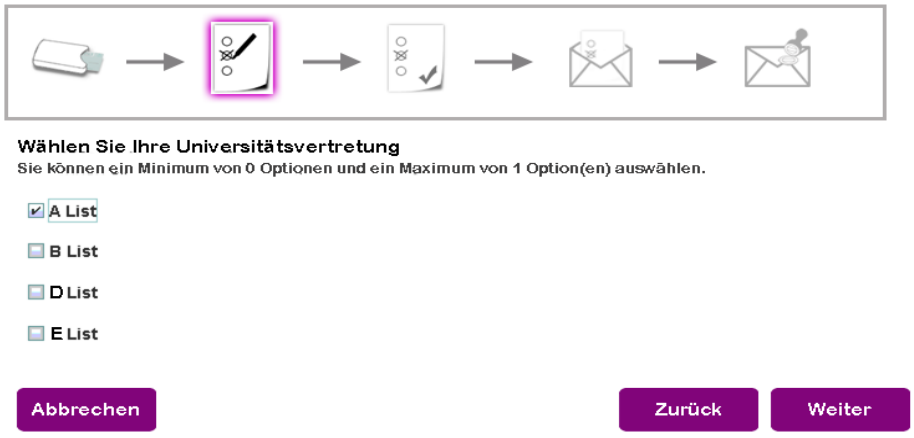

Figure 19: Sketch – Voting process guided by Graphics

Graphic representation of the election process. The election process was found to be simple and understandable. Graphic representations of the process present throughout the entire election process would ensure additional transparency. Particular attention should be paid to ensuring universal accessibility.

3.6.3.3.11 Usability of the Voting Software

The Usability Test, which was designed as an on-site survey including a questionnaire, was carried out using a stabilized initial version of the voting software. This version did not yet contain any of the usability improvements the project team had already reported to the software manufacturer. The improvement possibilities noted by the students were taken into consideration in the next version of the voting software.

The usability of the voting software was improved as well as possible from the project team feedback corresponding to the requirements of election rules for elections to the HSWO 2005. To this end, primarily the pilot application as well as screenshots delivered by the software manufacturer were used.

Improving ease of use. For more comprehensive usability tests, corresponding cycle times should be taken into account in overall project planning for any coming elections. The election client and integration of the election client into the Internet portal must be analyzed by a test team, whereby it should be possible to carry out tests in an in-house test laboratory. It is recommended that the election software manufacturer provides the project team with up-to-date ready to use versions, so that feedback can be derived as efficiently as possible through concept and design tests and can be directly entered and integrated into the development process. Creating the definition file for output texts should be explicitly taken into account in the project plan. The texts must be quality-checked several times for comprehensibility and accuracy by a test group.

3.6.3.3.12 Universal Accessibility

Universal accessibility of both voting software as well as web portals was one of the mandatory criteria requiring to be fulfilled by the software producer and the operator. The companies Scytl as well as BRZ possess great experience regarding the requirements for universal accessibility from other projects[39].

On safety grounds, the election client based the system on a Java applet solution. Screen readers were required to have Java Support or the possibility of addressing SUN Java Access Bridge[40] in order to be able to process the election client's representations.

---

[39] Universal accessibility is a mandatory requirement of all E-Voting projects. The company Scytl has already co-operated closely with many blind people and organizations for the visually impaired in different projects. Amongst these we must highlight ONCE (http://www.once.es/new/home/) and Vision Australia (http://www.visionaustralia.org.au/). The voting solution was successfully validated on WAI AA Standard. The company BRZ has built up competence both throughout our country and overseas in the field of universal accessibility of web services. We must highlight here the realization and operation of the help.gv.at portal (https://www.help.gv.at), which was distinguished with BIENE Award (http://www.biene-award.de/award/). The official assistant received the golden BIENE (‚*Accessible Internet Provides New Insights*') in the category "Complex Procurement and Transaction service provisions".

[40] The Java Access Bridge makes addressing and interaction with the Java Accessibility API possible. The Java Access Bridge is freely available at http://java.sun.com/javase/technologies/accessibility/accessbridge/index.jsp. We referred to the necessity of carrying out an additional installation in the help region of the Internet portal, in so far as the Java Access Bridge is not already included in the screen reader's installation packet anyway.

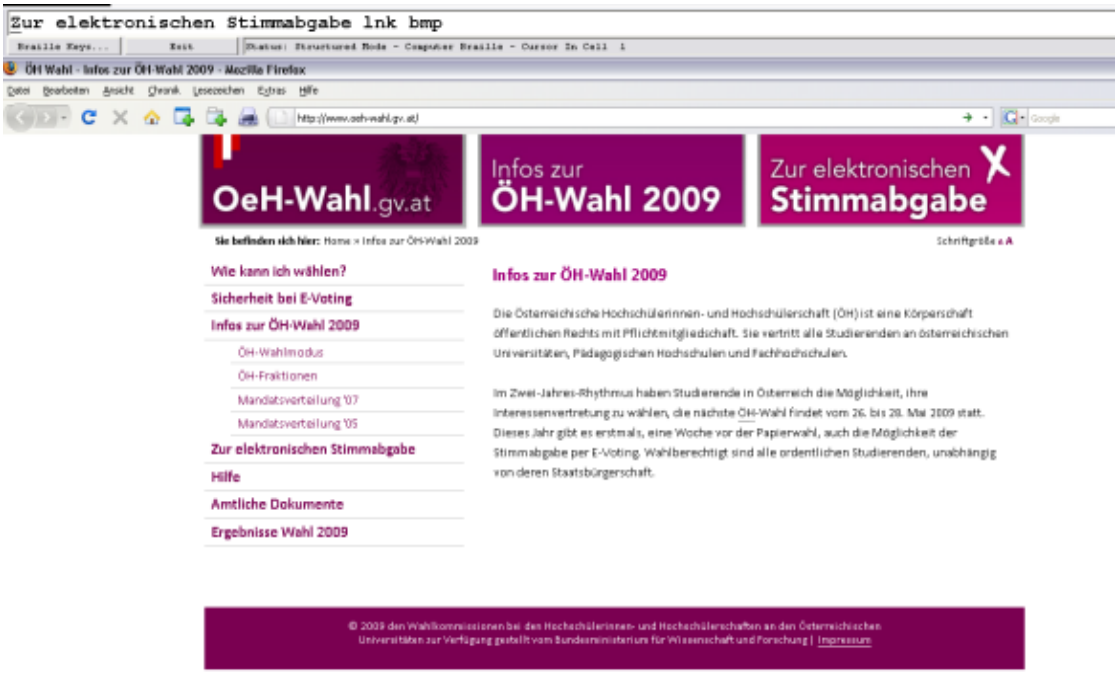

Figure 20: Observing the portal page using Screen Reader

The voting software was tested for universal accessibility at the earliest point possible in the project. During the course of iterative modifications within the Release Cycles and internal test applets, additional improvements were obtained both through testing with the appropriate accessibility tools as well as through collaborating with blind people. In this case, it is worth a particular mention that focusing of Java applets presents a problem. Some screen readers that were tested treat a Java applet similarly to an independent window; however, we cannot switch back to this window with the usual keyboard commands if we should lose focus.

The focus is of course set automatically on the applet; however, in order to solve the problem of changing focus, an "invisible" button/link[41] for people with good vision was built into the website, in which the Java applet was integrated. Through exiting as well as switching back into the Java applet again, this no longer presented a problem.[42]

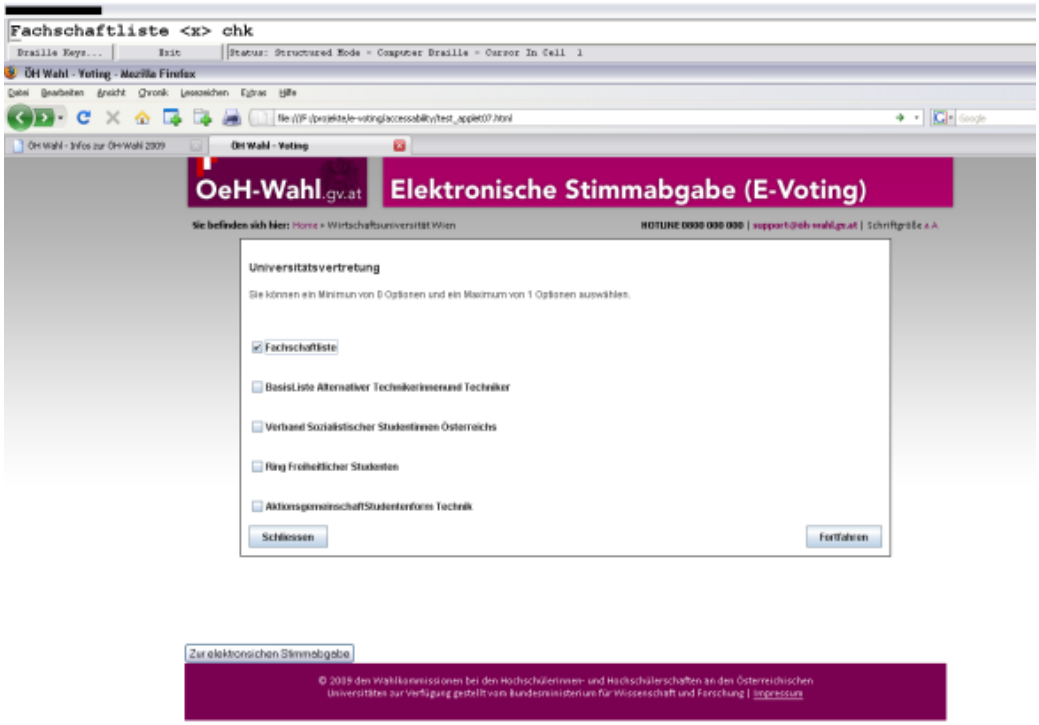

Figure 21: Test of Voting Processes using Screen reader

[41] The button "To submit electronic vote" was set invisibly via Stylesheet, so that this could no longer be detected visually on the website. Screen reader, however, reproduced the button as a reference.

[42] An example of verification tools for accessibility, which was used for testing the voting client based on Java, is the Java Accessibility Helper. In this case, we are dealing with a graphic tool, which verifies all UI components for their accessibility by means of the keyboard, that names, status values, etc., are correct through so-called Assistive Technologies (for example Screen reader, Screen Magnifier) can be selected and processed. The result of the test is an Accessibility Report, in which defects are classified („must be fixed", „not serious" etc.) an are listed. See http://java.sun.com/developer/earlyAccess/jaccesshelper/docs/index.html

Particular attention was given to simple navigation. To do this, the voting process was designed in a very linear manner. Following selection of the university, authentication takes place, then the individual ballot sheets are filled out, followed by confirmation and submission of the ballot sheet with the declaration in lieu of an oath. Finally, the student is directed back to select the university again.

Both the portal pages as well as the voting client, self-diagnosis tool, pilot application and the verification of the right to vote followed a standardized layout and have uniform navigation elements and page structures. All functions are accessible both via the mouse and using keyboard commands, whereby all the usual browsers[43] were supported.

In the overall layout design, the needs of color-blind and people who perceive colors incorrectly were taken into consideration.

[43] Internet Explorer, Firefox and Safari were actively tested and were supported; less well-known browsers such as Opera or Google Chrome were not constituent parts of the actual testing and approval cycles; however, we do not know of any problems associated with using them.

Figure 22: Testing the Web Portals for the Color-Blind

The entire portal has the opportunity to enlarge the size of the text, which was made easily visible in the top right-hand corner of every page. At the same time, the size of the election client's text within the Java applet was scaled (up or down) via the same element.

Universal accessibility. The universal accessibility of the portal system and election services as well as the project's efforts to ensure universal accessibility were praised by the monitoring committee for implementing the UN Convention on the Rights of Persons with Disabilities in accordance with § 13 of the federal law on treatment of people with disabilities (Bundesbehindertengesetz)[44].

[44] We will refer to this as Monitoring Commission from now on.

It was proposed that training videos be accompanied by interpretation by a sign language interpreter. Furthermore, the needs of non-verbal students should be met.

The provision of information in the Internet portal regarding use and support of explicit screen readers proved difficult. The risk of advertising or favoring commercial and competing products had to be taken into account here; therefore, the information provided was limited to general aspects. Nevertheless, possible provision of information for various named screen readers is desirable.

In order to improve the issue of screen reader support by Java, the responsibility for which lies primarily with the screen reader manufacturers, timely provision of a demo application to test accessibility is suggested. This demo application should be tested directly by screen reader manufacturers. Both the appeal to screen reader manufacturers to carry out tests and processing of feedback should take place as part of a cooperation between the project team and various associations and organizations that support people with disabilities. The results should at least be published in the information portal. In particular, this includes naming all screen reader products, versions and runtime environments that do not correctly correspond to the Java accessibility API. This will allow qualitative improvements to screen reader products in the medium term.

3.6.3.4 Checking the Right to Vote

Corresponding to § 20 para. 4 HSWO 2005, any member of the Austrian Federation of Students can verify their right to vote for the respective university Federation of Students' body on the Internet four to five weeks prior to the last day of voting date using the citizen card in accordance with § 2 Z 10 E-GovG.

3.6.3.4.1 Selecting the University

First, the student selects the university.

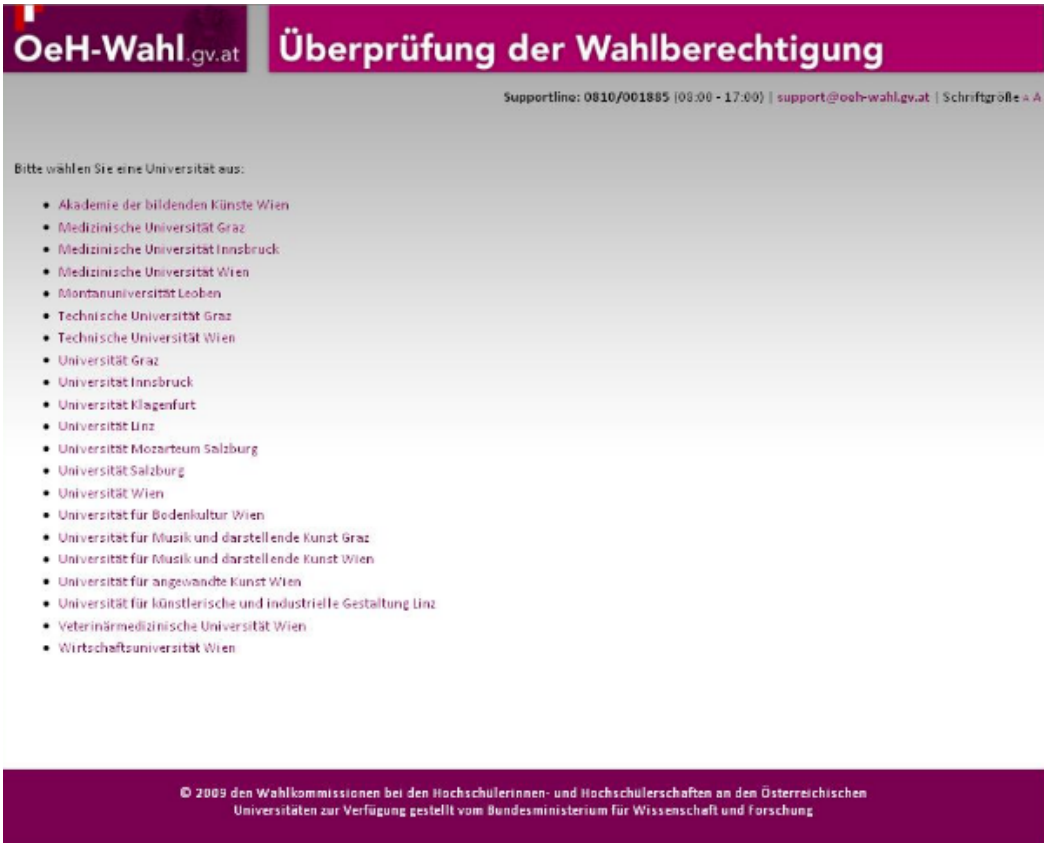

Figure 23: Checking the Right to Vote – Selecting the University

3.6.3.4.2 Authentication

Finally, authentication is carried out by means of the citizen card using the MOA Module.

Figure 24: Checking the Right to Vote – Authentication using the Citizen Card

The personal identifier is read off by inputting the four-digit PIN Code.

Figure 25: Checking the Right to Vote – Registration 1/2

The registration is signed by inputting the six-digit PIN Code. The user is authenticated in this way.

Figure 26: Checking the Right to Vote – Registration 2/2

3.6.3.4.3 Displaying Rights to Vote

The voting entitlement rights are displayed after successful authentication.

Figure 27: Checking Voting Entitlement – Representation of Rights to Vote

3.6.3.4.4 Realization

The verification of rights to vote does not require a Java applet. The rights to vote are listed on an HTML-based paged. The website refers to the fact that people should contact the respective electoral commission if voting entitlements are not correct. To this end, all of the contact details were listed on one of the pages.

The check of voting entitlements can be used by every person who has a citizen card. If no right to vote can be found, the user is informed of this.

Online citizen card environment for checking voting rights. For project-related reasons, the online citizen card environment (MOCCA) was not yet available at the time of verifying students' right to vote. Integrating the online citizen card environment would lead to higher acceptance and use.

3.6.3.5 Individual Verifiability

A simple version of individual verifiability in the form of a check code was realized within the information portal. A simple website for inputting a form served this purpose, which compared the input against a database.

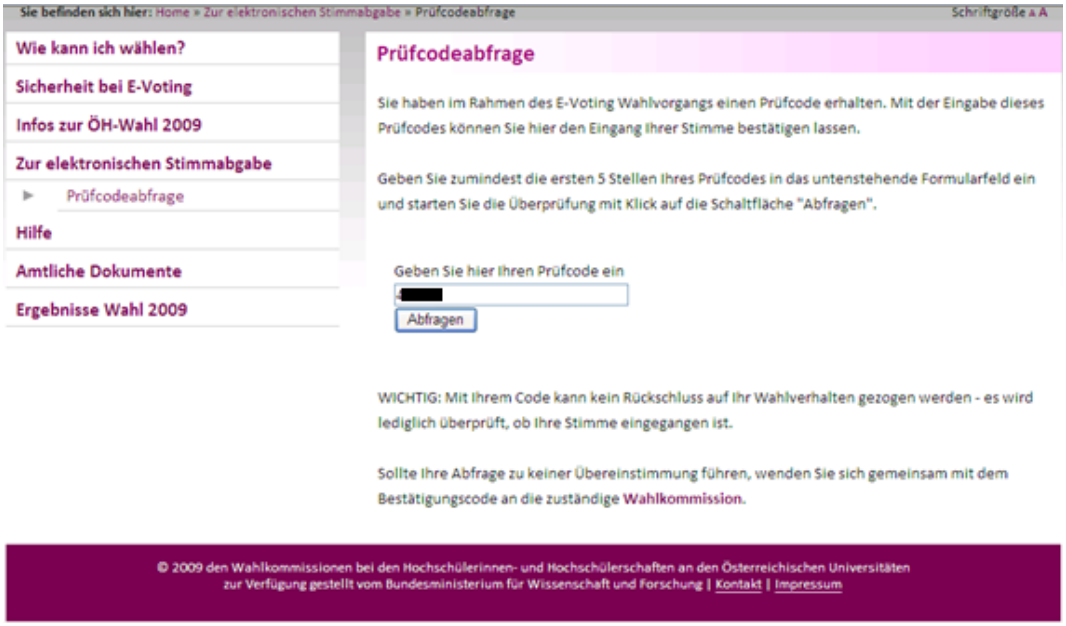

Figure 28: Check Code Verification – Request

At least the first five symbols of the check code had to be input into the system, and following this, all possible matches were listed.

Figure 29: Check Code Verification – Output

Availability of individual verifiability. It is not known how many students used the security code verification function. The communication as to when this function was available needed improvement. It was clear that security code verification could not be placed online until the public announcement and the objection period that commenced with that public announcement.

Furthermore, positioning the function within the Internet portal was less than ideal. The primary reason for this was to locate the function in the area “Submit electronic vote”. A more active application is desirable. This defect can be easily remedied the next time the function is used by publishing a separate, clearly visible area for security code verification within the web portal for the entire duration. This will then represent a constant integral component of the web portal; the function will, however, only be activated during the period for objections.

3.6.4 E-Voting from the Server Side

This chapter describes significant aspects of the voting system. There is an overview of the process actions, method of functioning and also of the security principles. At this time, we limit ourselves to the significant areas, so this is not an exhaustive and comprehensive list and description of all of the security mechanisms used. First, the technical process is described in principle in the following sequence: the voting server, monitoring, voting the voting administration system as well as the personal computers in the universities.

3.6.4.1 Functional Description

In the foreground of voting, the so-called Mixing Laptop is set up. This takes place in an audited process. The voting is configured on this notebook, a cryptographic key is created and at the end of voting, the electronic ballot boxes are opened and counted.

The notebook must satisfy the highest security requirements. To this end, the notebook may never be connected to any network or computer/ device. This is likewise the case during the installation process. The installation must take place in the presence of an installation consultant and in the presence of an installation monitoring body.

The integrity of the system and monitoring of the installation process is guaranteed by the people in attendance and, furthermore, through physical security measures. The mixing notebook is kept physically secure at all times.

The implementation of the installation is designed transparently. The integrity of all installation media is checked by the people in attendance for the installations. Each step of the installation is implemented step-by-step according to the installation description and is protocolled.

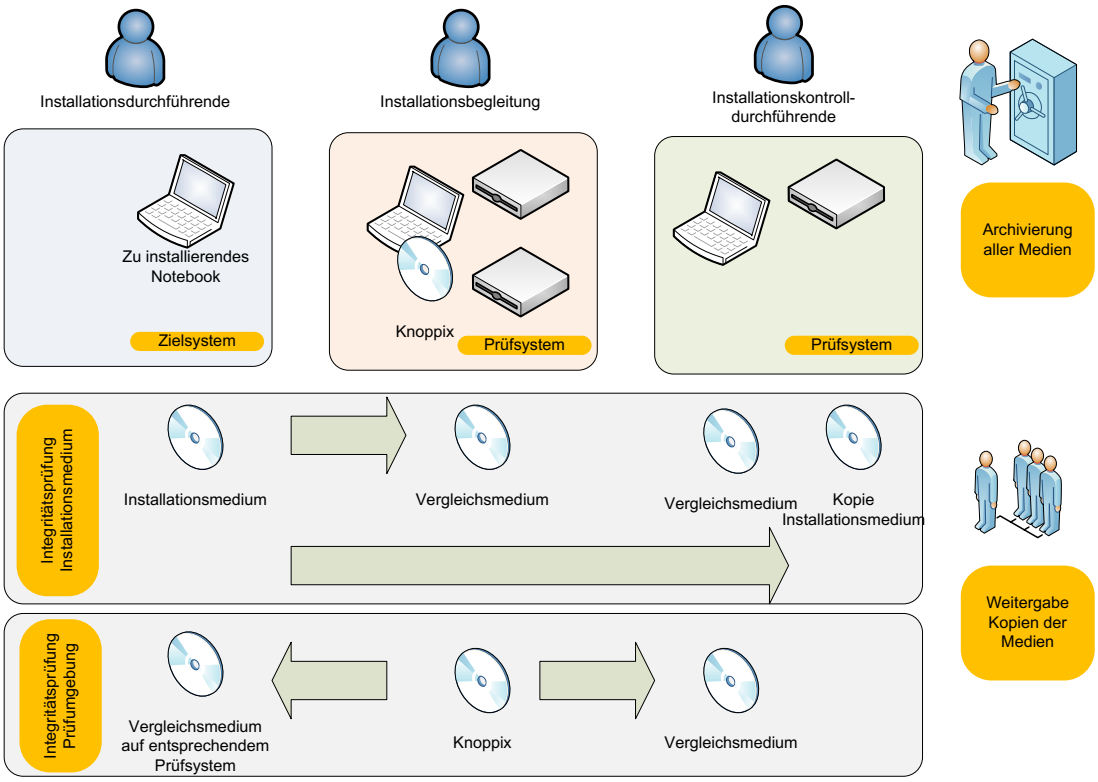

Figure 30: Installation process Mixing Notebook

The mixing laptop (target system) must be set up with end-to-end auditing. In order to do so, all installation media are compared using binary comparison and/or check sums with reference media prior to being inserted into the target system. Exclusively trustworthy sources must be used as data sources – both for the installation medium as well as for the reference media. This includes hardware and software companies (e.g., Microsoft, Oracle). The following factors are decisive here: distribution, age and service life of the software, region of use of the software and field of activity of the company providing the software.

In order to ensure that no manipulations can arise through the examination itself, the installation media must be unalterable, referring exclusively to CDs/DVDs with a closed setting.

Furthermore, the check system itself must be open to examination, and it must be transparent. In order to achieve this, a system provided on a Knoppix is used. Following installation, the Knoppix CD is mutually checked and archived by all of the participants to verify its authenticity.

With the exception of the Pnyx software packet and the Oracle configuration scripts (which deposit the corresponding tables and users for the Scytl software), all of the installation media can be copied and passed on to observers. This step is merely subject to technical licensing limitations (e.g., freely passing on Windows XP Installation CDs).

In a process similarly audited by the Election Commission[45] corresponding to § 15 para. 7 of HSWO 2005[46], a cryptographic key pair was generated on the mixing laptop. In this instance, public and a private keys are used for voting. The private key is divided up digitally and is handed over to members of the electoral commission on password-protected smartcards. The passwords are determined by members of the voting commission and are input. When doing so, the classic security principles of ownership and knowledge are used. The private key can only be reconstructed through consolidating the electoral commission's smartcards.

[45] Exactly two representatives of the Electoral Commission. The private key is divided up onto four smartcards, each of the people receive two cards each; three smartcards are required to re-create the private key (threshold value 3).

[46] § 15 HSWO 2005. The Electoral Commission is liable in particular for the production, administration and addition of two electronic keys for the electronic voting system.

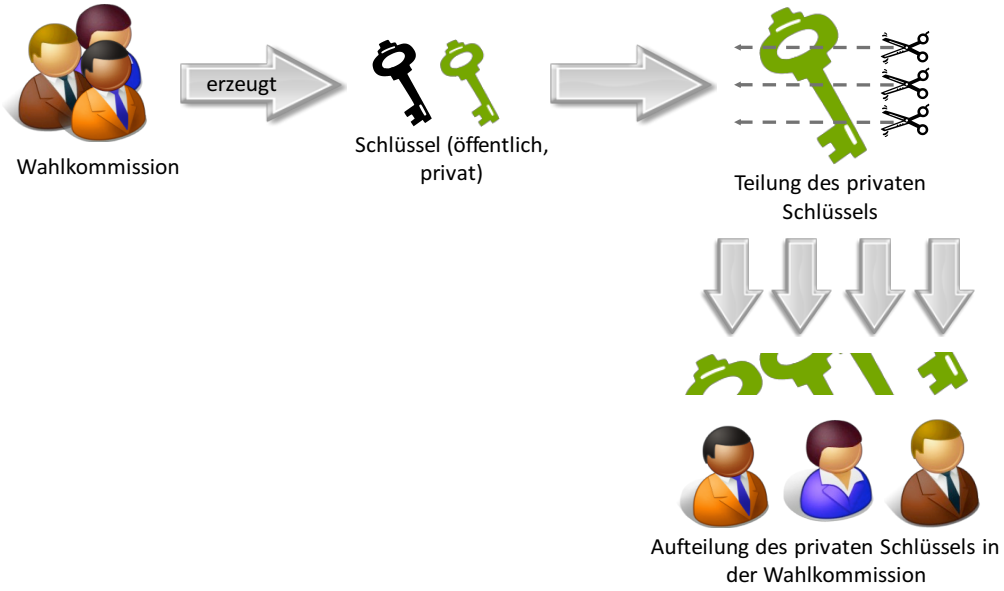

Figure 31: Progression of Key generation

Finally, the mixing notebook is stored securely until electronic voting has ended. The physical security of the mixing notebooks is a part of monitoring the election. It is stored in a high-security region of the computer data center and is sealed. The seals are only broken and re-sealed in audited process steps in the presence of the Electoral Commission at the end of electronic voting, for counting the votes cast and for final destruction of the data.

In order to take part in the electronic voting procedure, the student must fulfill the following requirements. He or she must have an active citizen card and a card-reader device. The computer or the notebook used must have one of the customary browsers[47] installed, and it must support the use of Java[48]. The student can check whether these requirements are fulfilled before voting using an appropriate self-diagnosis tool. The self-diagnosis consists of a webpage, which requests the system components required and checks their version and functioning.

[47] Internet Explorer 6+, Internet Explorer 7.x, Firefox 3.x.

[48] Java Version 1.5 for using the local citizen card environment; Java Version 1.6 for using the online citizen card environment.

Since it is possible to vote at a total of 21 different universities overall, the student must first select the corresponding university.

In accordance with the election rules § 63 HSWO 2005[49], the citizen card is used for voter identification and authentication. This is the case both for the voting transaction as well as for verifying the right to vote in accordance with § 20 para. 4 of HSWO 2005 [50].

Once the voter has their personal identifier approved by inputting the four-digit PIN Code (identification), he or she is prompted to sign a standard text. With this step, the voter can prove his/her identity (authentication).

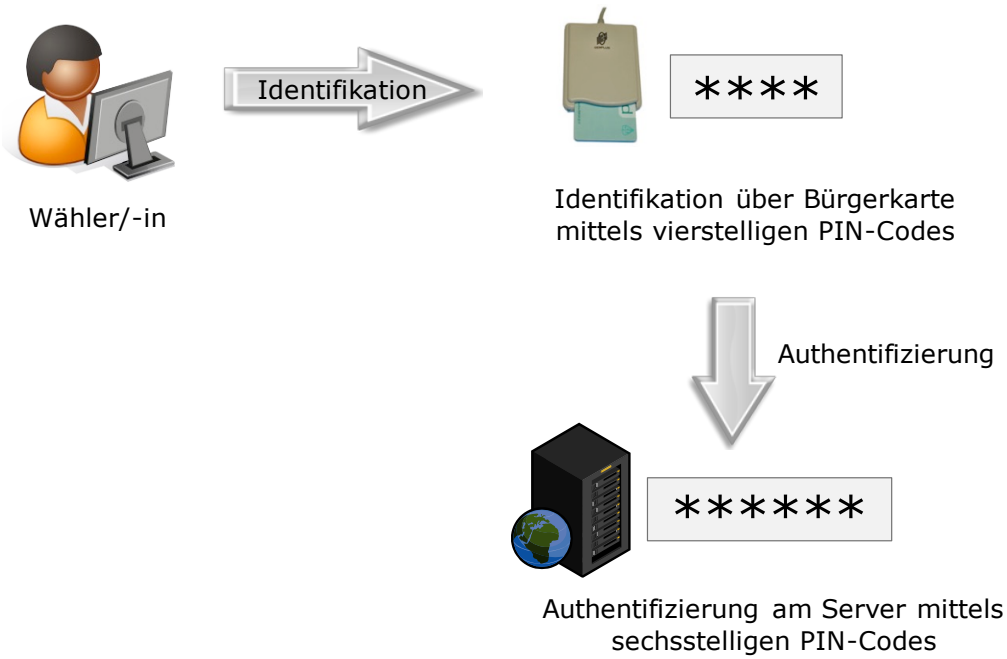

Figure 32: Identification and Authentication of the Voter

[49] § 63 HSWO 2005: The citizen card is used to provide the identity of the student in accordance with § 2 Z 10 E-GovG.

[50] § 20 para. 4 HSWO 2005: During this period, every member of the ÖH may check their entitlement and right to vote for the respective elected bodies by using the citizen registration card in accordance with § 2 Z 10 E-GovG on the Internet.

Finally, the ballot sheets are presented. With each ballot sheet, the voter can decide whether he/she wishes to submit this electronically or at the polling station. By filling out all the ballot sheets, if the voter wishes to submit electronically, the student is presented with all of the selected voting options once again. In addition, in each case, for every ballot sheet, a note is made of whether there were more voting options available or whether too many options were chosen. In a similar way to paper-based voting, submitting a vote with an invalid ballot sheet is not prevented.

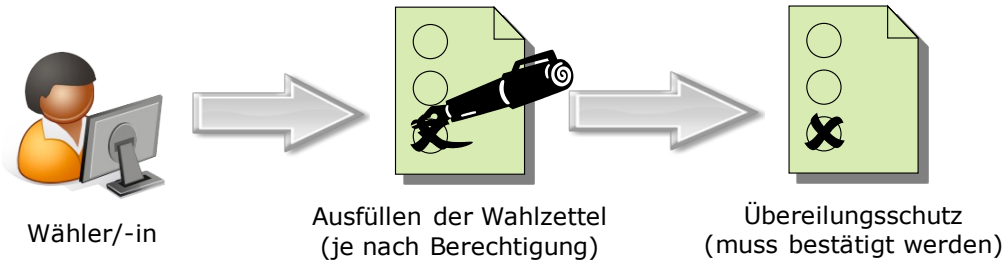

Figure 33: Protection against Excess Haste

With the confirmation of all voting options chosen, each ballot sheet is encoded with the public key. Finally, the student is prompted to input the six-digit PIN Code, whereby the ballot sheets[51] are signed. The signature guarantees that each manipulation of the ballot sheet is acknowledged.

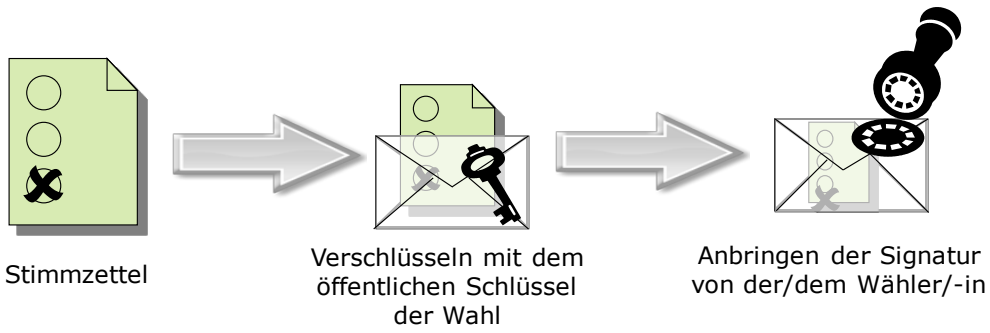

Figure 34: Encrypting and applying the signature

[51] Precisely, not only the encrypted ballot sheet is signed, but parts of the transfer protocol are signed. This includes the check sums amongst other things of the encrypted ballot sheets.

The encrypted ballot sheets including their signatures are deposited and linked up cryptographically in the corresponding digital ballot boxes. By means of the encrypted ballot sheets, voting rights that have been exercised – similar to sealed a sealed envelope that has the name of the voter on it – is registered in the voter's name.

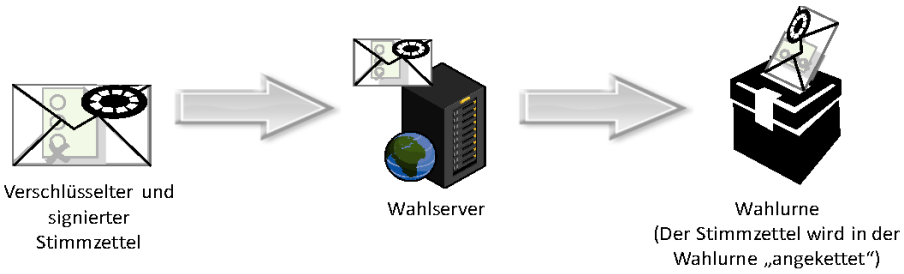

Figure 35: Transferring the Vote to the Election Server

The check code serves as an additional security function. In this case, we are dealing with a randomly generated combination of numbers and letters, which is generated on the student's computer and is added to the electronic voting envelope. Here, it is important that the check code is known only to the student. Neither assignment to the student nor assignment to the voting options is possible using the check code. In this way, we can exclude vote-buying. Furthermore, at the end of the voting transaction, the student is issued a control code. This is required together with the check code for any appeals that may occur following the count.

On completion of electronic voting, the voting rights exercised are selected and marked off in the electoral roll, so that there is no possibility of people submitting votes more than once.

When counting the votes, the digital ballot boxes are transferred to the mixing laptop. Secure data transfer is protected both through technical measures as well as through cryptographic processes.

The entire integration chain is checked on the mixing laptop. This includes, amongst other things, that all signatures are valid, that no closed electronic envelope lies in the wrong ballot box or that no unknown person or persons have submitted votes more than once. This process step consciously mistrusts the integrity of all other systems used in the election. The check for integrity is carried out prior to the paper-based vote. Should any errors occur following the verification, the Electoral Commission can also declare the electronic voting as invalid and can inform voters of this in plenty of time to take part in the paper-based election and to cast their votes once again[52].

During the course of counting, which according to § 46 para. 8 HSWO 2005[53] may not take place until after the end of the voting transactions, the signatures are firstly removed, then the electronic envelopes are mixed and are decoded through adding the Electoral Commission's key.

Figure 36: Anonymization of ballot sheets

[52] § 48 para 4 HSWO 2005: if E-Voting is declared invalid in accordance with§ 39 para 7 HSG 1998, then voters who submitted their votes by means of E-Voting are permitted to cast their votes once again at the polling station.

[53] § 46 para 8 HSWO 2005: Counting votes submitted by means of E-Voting is started by adding the electronic key in accordance with § 35 para. 6 HSWO 2005 by the Electoral Commission for the Austrian Federation of Students. This must take place on the final day of voting following the final voting transaction.

At the same time with the opening of the voting envelope, the check codes are also recorded. Following official approval, the results of the election are published on the Internet.

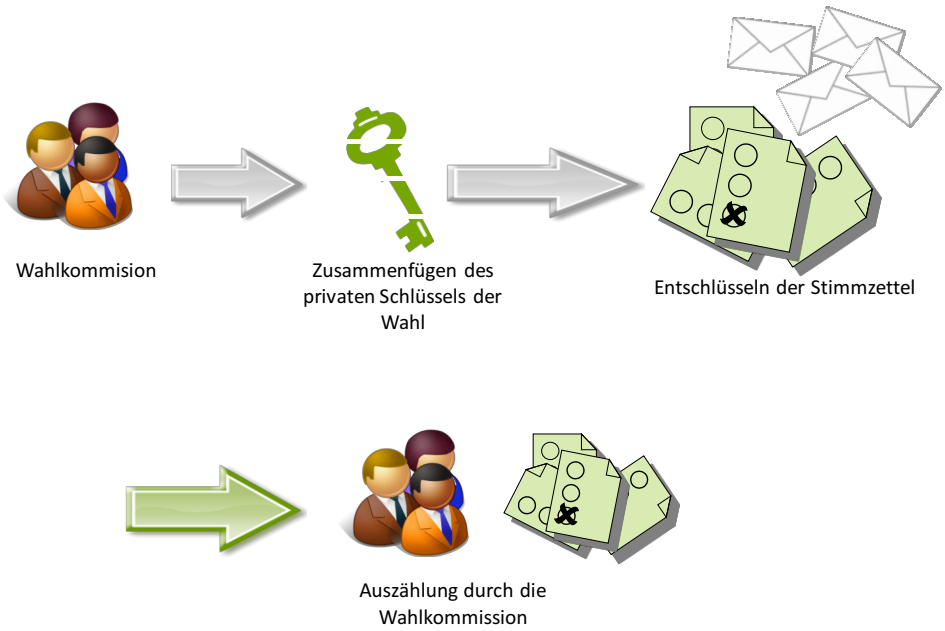

Figure 37: Reconstructing the Electoral Commission's key

The voter can verify by means of an online request whether their ballot sheet reached the count and was counted by the Electoral Commission. Should the check code not appear on it, then the student is responsible for notifying their Electoral Commission. The student can prove cryptographically together with the control code that the vote really did need to be counted.

IT Experts / Audit. During implementation of the project, it was decided that all audited processes should be monitored by a legally authorized IT expert and the Confirmation Agency in accordance with § 34 para. 6 of the law governing the Federation of Students (HSG) 1998. This contributed considerably towards increasing transparency. Monitoring by the Confirmation Agency in accordance with § 34 para. 6 HSG 1998 was part of the

condition for implementation[54]. The installation process for the mixing notebook satisfied the high requirements in terms of control, traceability and transparency. Throughout the project, the integrity of the hardware used was verified through tests. The hardware was not part of the certification in accordance with § 64 para. 3 HSWO 2005.

3.6.4.2 E-Voting Server Infrastructure

The infrastructure was redundantly distributed in two locations: the Computing Center at BRZ, and the Parallel Computing Center at BRZ. The locations are approximately 5 kilometers away from one another.

Both locations satisfy the requirements of the most modern and secure computer centers with regards to physical security, power supply, fire protection, access control systems, recording systems (real-time video monitoring, recording accesses) and much more.

The E-Voting system was regarded as a highly critical system, and for this reason, it was subject to the highest security mechanisms of the technical computer company BRZ.

All infrastructure components of the voting system were divided at the location in protective storage cabinets. Access to the protective storage cabinet in a secure area of a server room was only granted to authorized personnel. Any access was monitored and recorded by the safety control group.

[54] Certificate published by A-SIT see http://www.a-sit.at/pdfs/bescheinigungen_hsg/bescheinigung_hsg_final_sig.pdf

In addition, both of the protective storage cabinets for installing the mixing server were secured up until the secure deletion of all data following voting using metal seals and steel wire fasteners. The metal seals used are marked with unique numbers.

Figure 38: Sealed protective Cabinet

The security of the systems was tested using penetration tests. Special attention lay in securing against distributed Denial of Service (dDoS) attacks. For this reason, throughout the entire period of the project, a close collaboration was maintained with CERT.at[55] and ACOnet[56] for detecting and reacting to dDoS attacks across all networks.

---

[55] CERT.at is the Austrian national CERT (Computer Emergency Response Team). As such, CERT.at is the contact partner for IT security on a national level. It interconnects other CERTs and CSIRTs (Computer Security Incident Response Teams) from fields of critical infrastructure, ICT (Information and Communication Technology) and gives out warnings, alerts and tips to SME (small and mid-sized enterprises). With attacks on computers on a national scale, CERT.at co-ordinates and informs the network operators in each case and the local security teams responsible. See http://cert.at/

[56] ACOnet is the Austrian scientific network for public-purpose installations for research, education and culture, which provides its participants with access to other scientific networks and the Internet. ACOnet is operated by the Central Information Technology Service of the University of Vienna in cooperation with other universities throughout the whole of Austria. See http://www.aco.net

3.6.4.3 Integration of MOA Modules

The integration of MOA-ID and MOA-SP to the greatest extent gave us no technical problems. Improved documentation for this module[57] reduced the workload. In principle, in spite of this, the preference was for the E-Government strategy to make integrating the citizen cards into another service as offered easier through providing standardized modules.

The MOA-ID and MOA-SP modules were installed by the operator BRZ, special configuration details from the point of view of the application were specified by the software supplier Scytl.

Implementation of MOA-ID and MOA-SP. The MOA modules were installed in an especially secure manner. The basis of the E-government strategy consists, among other things, of provision of the MOA modules and their source codes. The knowledge and experience gained from the E-Voting project regarding installation, configuration and operating the MOA modules represent a valuable contribution to further development and improvement.

3.6.4.4 Monitoring

The screen for monitoring voting is connected directly to the database. There is a representation of the current number of voters per university who have already taken part on this screen. The video signal in this case is transferred into a separate observation room.

[57] Documentation from MOA-ID and MOA-SP/SS can be found at http://egovlabs.gv.at/docman/index.php?group_id=6.

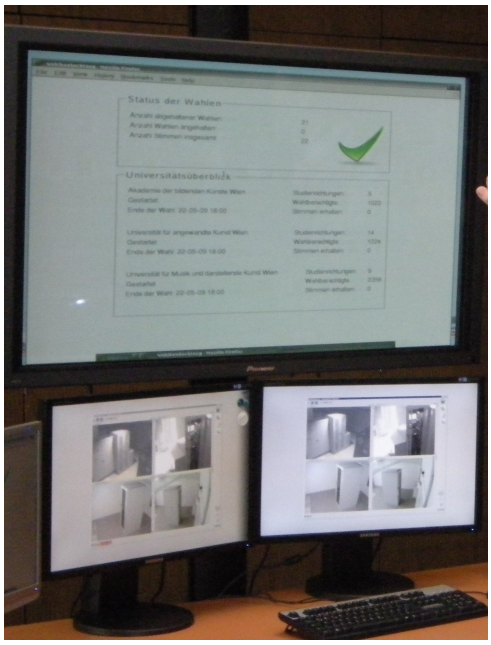

Figure 39: Screen in the observation room with the current number of voters

In the observation room, we could gain insight both into the current status of the voting (number of voters per university, status of the election, i.e., started/suspended/re-started/completed) as well as check the physical security and non-violation of the voting system and the mixing laptop (real-time video monitoring of both locations including motion indicator and alarm system). The regulations on accessing the monitoring room were determined by the definition of an Election Monitor defined in HSG 1998 and was guaranteed by corresponding security guard personnel from the company BRZ.

Monitoring the Election. Permitting more people to monitor the election would increase transparency. A corresponding legal basis would need to be created for this purpose. Technically speaking, election monitoring over the Internet would be possible. To this end, it is important to note the frequency of data updates.

3.6.4.5 The Election Administration System

The Election Administration System[58] is defined in § 1 para. 6 HSWO 2005 as a hardware and software system for supporting the Electoral Commission in realizing their tasks during the election that is to be carried out.

The elections to the Austrian Federation of Students take place at 21 universities. In this process, a series of tasks are cared out by the Chairs of the Electoral Commissions and their Vice-Chairs at the respective university, which up until now were determined by individual solutions and auxiliary equipment. For example, in each case they had an individual electronic system at the Vienna University of Economics and Business or at the University of Graz, which supported the efforts of the Electoral Commission electronically. Both the technical realization as well as the extent of support was different for each system tried until now. Electoral Commissions from other universities had no such type of system available, and their tasks were characterized by self-generating Excel macros, Excel tables and Word files, which normally could be drawn up quickly.

It was decided in the course of the project for the Austrian Federation of Students Elections in 2009 to develop a central electoral administration system and to make it available to all 21 Electoral Commissions and the Federal Election Commission. The aim was to develop a standardized system, which supports the activities of the Federal Election Commission and of the 21 Chairs of the Electoral Commissions and their Vice-Chairs. Some of the activities and functionalities are listed here:

---

[58] The election administration system may not be confused with the almost identically named admin system of the E-Voting System. The admin system of the E-Voting system is that component which runs as a service on the mixing laptop and which in the course of an audited process with the Federal Election Commission creates the cryptographic key for voting as well as carrying out configuration of the electronic votes being cast.

- Drawing-up the electoral rolls, which are printed out and hung in a public place for reference;

- Configuration of voting, whereby the corresponding paper ballot papers are generated and reproduced on site. The number of the 374 different ballot papers required is determined by the voting administration system;

- Generating letters of notification to those elected;

- Generating different forms filled out corresponding to HSWO 2005.

During paper-based voting, the voting administration system is also used by the Electoral Sub-Committees at the respective universities to draw up a standardized reconciliation list corresponding to § 40 para. 2 HSWO 2005[59].

Figure 40: Using the voting administration system during paper-based Voting

Operated by a member of the Electoral Sub-Committee, this acts as an additional opportunity to monitor the paper-based reconciliation list, which is managed by another member of the Electoral Sub-Committee.

[59] § 40 Abs. 2 HSWO 2005: At the same time, a non-binding reconciliation list must be managed in the voting administration system by a member of the Electoral Commission.

At universities at which polling stations are set up in such a way that students can cast their votes at more than one polling station, there is a requirement for the respective Electoral Sub-Committee at a polling station to know about the voting rights that have been exercised at other polling stations in order to prevent multiple votes being cast. Up until now, this was marked by a stamp printed by the Electoral Sub-Committee in the Student's ID document on casting a vote. Through the voting administration system, it is now possible for Electoral Sub-Committees to now query those entitled to vote centrally online[60]. Therefore, we only need to fall back to the previous system (e.g., using a stamp) in the case of a system failure or in the case of not being able to access the voting administration system.

The basis for the E-Voting system consists of the electronic electoral roll recorded in the voting administration system as well as the defined elections. The results of the paper-based voting input by the Electoral Sub-Committee are counted by the voting administration system together with the outcomes for electronic votes cast. The overall results are exported from the voting administration system and are published in text and graphically in the web portal.

In order to prevent failures or outages associated with the voting administration system, it was operated redundantly at two locations. The voting administration system is technically separate from the E-Voting system. It runs on its own servers, and they have no access to the E-Voting system. Any data transfer from the E-Voting system to the voting administration system and the other way around takes place by CD/DVD. The authenticity of the media was assured cryptographically and through audited organizational processes.

[60] An appropriate computer must be available it the Electoral Sub-Commission in the polling station for this. This is regulated in § 33 para. 1. HSWO 2005.

Access to the voting administration system was protected by using certificates as well as a user name and password.

Further development of the election administration. As part of the introduction of a central system for election administration to support the activities of the electoral commissions, a process of continuous improvement and further development should be commenced.

The need for further development arises because it was not possible to implement all the desired functions due to time constraints and because the focus was on the stability and realization of functional requirements rather than optimum usability. Consideration must also be given to all experiences that were gained after practical implementation. Additional changes to the election administration system may arise through modifying the legal basis.

In any case, centralized operation and further development of a uniform election administration system for all 21 universities leads to targeted standardization and improvements in quality. This centralization represents an efficient solution vis-à-vis the individual solutions that existed until now and that have been implemented, leading to more transparency for all involved.

3.6.4.6 Personal Computers at Universities for Electronic voting

§ 33 para. 1 HSWO 2005 specifies that the Dean must provide students adequate numbers of personal computers with Internet access and the technical components for using citizen cards in accordance with § 4 E-GovG and privacy shields in accordance with § 34 para. 5 Z 6 HSG 1998 throughout the period in accordance with § 62 HSWO 2005, and they must make them publicly accessible for casting votes by means of E-Voting.

In consultation between the Federal Ministry and the Central Information Technology Services of the universities corresponding to legal guidelines, setting up PCs in each university city was considered adequate. Personal computers, on which it was possible for students to cast their vote electronically were set up on site; they were installed and operated in all university towns in sufficient numbers by the respective ZID.

The principal consideration of deciding whether personal computers should be set up centrally or otherwise and installed by local ZID was made in favor of the local solutions on grounds of complexity of a standardized solution and the short project duration period. The local ZIDs were supported by the Federal Ministry through specifications and recommendations; however, the realization was almost completely the responsibility of the competency of the ZID. Operation was likewise predominantly smooth during the voting phase, even when there were numerous cases of vandalism (*intentional destruction*) and acts of sabotage to PCs.

Setting up PCs at the universities. The integration of IT centers into the overall project should take place at an earlier point in time in future elections. The provision of a sample application and implementation of a test election are decisive factors. In addition, a suitable communication platform must be established between the IT centers and the project team, particularly with regard to reporting incidents during the voting phase. The decision as to whether locally or centrally installed PCs should be used must be evaluated under new perspectives. The decision as to whether locally or centrally installed PCs should be used must be evaluated under new perspectives.

The PCs at the universities were viewed very positively by the disability officers in universities; however, continual improvement of universal accessibility in terms of the access to and operation of the PCs in universities was also highlighted.

3.6.5 Pre-Voting Phase

The realization of the project commenced in November 2008 with the specification phase. Following this, the project was presented to the media in a specialist conference. Parallel to this, the university publicity departments prepared for the project with the "Unitour". The usability test in March 2009 was the last test prior to the legal start of voting on the key date. The verification of voter entitlement (*of the right to vote*) at the end of April was the first opportunity for students to try out the citizen registration card in the context of this project.

3.6.5.1 Enquete

On December 3, 2008, a conference took place in Vienna, Austria, initiated by the BMWF on the subject of "Political Opportunities to Participate using New Media" with the participation of national and overseas experts in the fields of "Participating over the Internet", E-Democracy as well as E-Voting. The aim of the conference was to explain a number of facets of political participation using the Internet in general as well technical and legal aspects and also in particular E-Voting to the interested audience of experts. Ultimately, the conference served to deliver both to advocates as well as critics of E-Voting a platform in order to exchange arguments in what were sometimes very intense and controversial discussions.

3.6.5.2 University Tour

The tour of the universities was initiated between August and October 2008 by the BMWF. The aim here was to visit as many universities as possible in the seven university towns (Vienna, Graz, Linz, Salzburg, Innsbruck, Klagenfurt and Leoben) and to enter into discussions with the stakeholders (usually the Vice-Deans, University Chancellors, employees of the CITs and also members of the local electoral Commissions) as well as with the local student unions.

Preparation for visits and their implementation was completed by staff of the BMWF or of the Federal Electoral Commission as well as by externals of the BMWF Team. The aim, with respect to the elections to the Austrian Federation of Students, was to already make reference to the additional E-Voting channel in May 2009 and to make the university employees and the local Student unions aware of the subject. By the end of November 2008, such visits had been completed at almost all universities.

3.6.5.3 E-Government Initiative studi.gv.at

3.6.5.3.1 Background

In cooperation with the Austrian Federal Chancellery, the Austrian Ministry of Finance, the Principal Association for Social Security Funding Agencies as well as the BMWF, the campaign studi.gv.at was initiated in September 2008 in order to start an E-Government Strategy for the field of students. This project was set up in parallel with the E-Voting project, since mutual synergies arose and both projects profited from one another to an equal measure. The general degree of recognition of the citizen card as well as of the opportunities to use it – in particular, for students – was the focus of attention for this project.

3.6.5.3.2 Realization

Numerous measures were commenced in order to achieve as large a number of activations as possible:

- A dedicated website www.studi.gv.at was set up. The students were able to inform themselves on the citizen card and the applications relevant for students. During the summer semester, increasing opportunities to use the citizen card for E-Voting was also at the center of attention;

- Card-readers were distributed to students free of charge. The card-readers were distributed directly to the universities free of charge in the context of the initiative to those students, who allowed their citizen card to be activated;

- Advertising took place for studi.gv.at at universities throughout Austria using billboards and flyers;

- Free of charge citizen card activation services were provided at universities: Tutors were specially trained and authorized for this, with their number increasing throughout the course of the project from 22 to 30. The coaches had specially designed laptops, mobile data cards, information folders, polo shirts, laptop cases and covers, badges and roll-ups. Furthermore, detailed documentation regarding the citizen card as well as its uses and its meaningfulness were put together;

- In addition, student volunteers were trained as "Registration Officers", which were able to activate further citizen cards according to the snowball principle.

3.6.5.3.3 Outcome

From the start of the studi.gv.at initiative up to and including the election phase for the Austrian Federation of Students, we were able to record more than 14,000 citizen card activations by students. The following table presents activations by month, divided up in sequence for the phases mentioned above. In addition, the overall activations are shown as well as the distribution by percentages of activations for each respective phase.

Month	New Activations	Number per Phase	Percentage per Phase
October 08	Introductory and Set-up Phase	2,458	17.23%
November 08			
December 08			
January 09	Pre-voting Phase	5,660	39.67%
February 09			
March 09			
April 09			
May 09	Voting phase	4,529	31.74%
June 09	Election Follow-up Phase	1,621	11.36%
July 09			

Table 6: Number of Activations

The table above shows the activations per month, which is divided in sequence into the phases named above. In addition, the overall activations are shown as well as the distribution by percentages of activations for each respective phase.

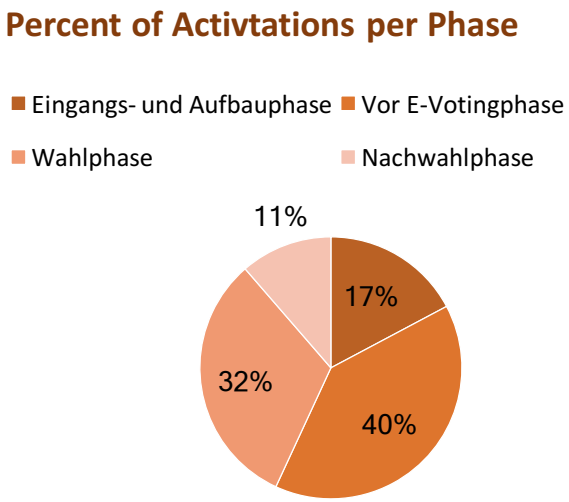

Figure 41: Percentage Distribution of the Activations per Phase

The graphic illustration shows that in the pre-voting phase and the voting phase, the most activations were triggered by percentage.

Sustainability of citizen card registrations. Particularly during the entry phase and development phase of the authorization process, a number of unexpected server breakdowns occurred, rendering authorization impossible during these periods. Through direct communication with responsible persons at the central register and A-Trust, further similar problems were largely avoided throughout the course of the project.

Students were pleased that card readers were distributed free of charge as part of the studi.gv.at campaign. However, there were complaints that there was no personal contact via a telephone hotline for rapid responses to queries.

A lot of information was gathered regarding the students' acceptance of the citizen card and its functions through the studi.gv.at campaign. In addition, a very good overview of the opinions in the individual study facilities and universities was compiled, particularly regarding E-Voting.

The information on the studi.gv.at website regarding application options offered by the citizen card should be integrated into existing information services (help.gv.at or bmwf.gv.at).

In the longer term, the physical presence during authorization, the lengthy duration and inputting two different PIN codes pose problems in terms of usability for the use of the citizen card.

Regular use of corresponding applications seems to be the key to sustainable use by students.

3.6.5.4 Certification

Corresponding to § 64 para. 3 HSWO 2005[61] as well as § 34 para. 6 HSG 1998[62], the technical components used and the components used directly for casting a vote and for verifying identity must be certified according to the latest level of technology in accordance with § 19 Signature Act by a Confirmation Office. Certification must be completed up to 60 days before the first day of voting, whereby recommendations from the Council of Europe on legal, operational and technical standards for E-Voting are monitored.

---

[61] § 64 para. 3 HSWO 2005: The client and the election server software must be certified by 60 days before the first day of voting by a Certification Agency in accordance with § 34 para. 6 HSG 1998. As part of the certification, fulfilling the security requirements by electronic voting system with the involvement of recommendations from the meeting of Ministers of the Council of Europe on Member Countries in accordance with Article 15 para. b Statute of the Council of Europe, BGBl. 121/1956 in the currently valid edition, no. Rec(2004)11 dated September 30th 2004 on the legal, operational and technical standards of E-Voting ("Legal, Operational and Technical Standards for E-Voting") must be tested. Furthermore, in the examination, the existing useable protection profiles should be considered.

[62] § 34 para. 6 HSG 1998: The technical components used by the Electoral Commission and the components, which are used directly for casting votes and for verifying identities, must be tested sufficiently according to the latest status of technology and must be tested continuously. The fulfillment of security requirements must be certified by a Certification Agency in accordance with § 19 SigG [Signature Act]. This Certification Agency also pronounces recommendations for the other technical components, which are used when casting the vote.

3.6.5.4.1 Object for Testing

Testing took place from December 1, 2008 until March 25, 2009 on the basis of transferred documents and the source code. Using the documentation from the manufacturer, we examined whether the security architecture for the software could fulfill the security requirements of HSG 1998 and HSWO 2005. Using the source code provided by the manufacturer, we were able to understand whether the security functions presented in the documentation phase were also correctly implemented.

The actual technical installation was not the subject of the test nor operation of the certified components nor the infrastructure required for this. The designs intended for this were evaluated by expert reports, and based on this, the corresponding conditions for use were defined, which must be followed throughout the life cycle of the components and data elements used.

3.6.5.4.2 Certification and Conditions for Use

On March 27, 2009, A-SIT completed the certification process and published the results online[63]. The following five conditions for use were defined in the course of certification with consideration of the object being examined:

Condition for Use 1: Key Lengths

Client and election server software must be configured so that the key lengths for the cryptographic algorithms used are selected in such a way that these correspond to the latest level of technology and achieve the level of security required for qualified electronic signatures.

Condition for Use 2: Client

For secure use of the client, we must set as a prerequisite that the computer chosen by the voter in each case is free from software that could influence the correct functioning of the client or that we can observe it. For this reason, corresponding security

[63] See http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_hsg/index.php

information must be provided via the web portal, which must be displayed to the voter prior to casting the vote. In particular, a representation must also be made of how they can check the genuineness of the clients and how they can prevent residual information being stored on the client's computer.

Condition for Use 3: Election server software

The prerequisite must be set for secure operation of the election server software that these are compiled and installed on trustworthy systems. The concepts presented in the course of certification for the compilation and installations must be strictly kept to for this reason, and the steps carried out must be protocolled. For systems used in the generation of security-relevant keys, secure processes must be used, which reliably and continuously prevent a detection of residual information for the keys being generated.

Condition for Use 4: Electronic Ballot Box and Electoral Commission Key

The electronic ballot box and the Electoral Commission's partial components of the private key must be deleted or destroyed in a secure manner following counting of the votes, and this must be proven in an independent audit. The systems and data involved must be monitored throughout the entire life-cycle, including all components and data elements and protocolled and operated in such a way that manipulation or data transfer to an external recipient can also be excluded by the organization of the system.

Should deletion not be possible on legal grounds, then the organization must ensure that the owner of the partial components of the Electoral Commission's private key has no access to the electronic ballot box and that opening the electronic ballot box (for any possible new implementation of the mixing process) can only be carried out under the same secure conditions as during the course of the election. Where the electronic ballot box has been stored, we must further ensure that if the lengths of the keys used for encryption no longer achieve the required level of security required for qualified electronic signatures, an addition encryption of the electronic ballot boxes must be provided. The infrastructure and the encryption process in this case must be subject to technical and organizational monitoring during the life-cycle of the components and data elements. The key used in this case must be generated under the

same secure conditions as during the course of the election, it must be divided into partial components and it must be handed over to the Chair of the Electoral Commission as well as to further members of the Electoral Commission.

If one of the owners of a partial component should no longer exercise their function in the sense of HSG 1998 or HSWO 2005 during the life-span of the partial components of the private Electoral Commission's key, then care must be taken to ensure secure transfer of the partial components to a member of the Electoral Commission, who does not hold any further partial components for safekeeping.

Condition for Use 5: Election Key CA

The security and operational concept of the certification agency ("Election-CA"), which will issue the certificates for the election software, must demonstrably correspond to the safety requirements of the electronic election in the spirit of HSG 1998.

Figure 42: Conditions for Use

3.6.5.4.3 Fulfilling the Conditions for Use

Appropriate consideration must be given in the project to fulfill the conditions of use. The length of the key for cryptographic algorithms was configured to 2048 bits (1); the corresponding information, instructions and information were published via the web portal (2); the processes for compiling and installation of the election software was carried out, verified and audited according to the concepts presented (3); the details on data destruction were followed and were implemented and audited in a verified process (4) and likewise the security details for constructing the Election CA for the voting key were followed (5).

3.6.5.4.4 Online Citizen Card Environment

On the basis of the integration of the online citizen card environment (MOCCA), changes were made to the certified election software during the later phases of the project. The changes included supporting the XML Signature Requests in order to make the use of the online citizen card environment possible. In this way, casting votes was made possible, requiring no further software installation to the client computer for the citizen card function, whereby the risk of any conspicuous targeted manipulation of the client as part of the installation was significantly reduced.

A-SIT confirmed on May 15, 2009 that the changes completed had no influence on the confirmed fulfillment of the security requirements of § 34 HSG 1998 as well as of § 64 HSWO 2005 on certification A-SIT-1.078. Supplement no. 1 associated with the certification was published on the A-SIT website[64].

3.6.5.4.5 Experience for Future Certification

Successful certification is based to the greatest extent of the experience of the company Scytl with different certification processes from previous projects. The corresponding documents were provided in good time, and queries on additional, detailed information were answered quickly.

Certification task. The effort involved in the certification process is considerably reduced when using the same election software, since the source code has already been checked. In case of any changes or adaptations (e.g., in the user interface), these should simply be analyzed further (taking the overall context into account) by the independent certification center.

---

[64] http://www.a-sit.at/pdfs/bescheinigungen_hsg/ASIT_bescheinigung_hsg_erg1_090515_sig.pdf

A prerequisite for this is that the source code already used is available to the independent certification center in order to allow differences between the old and new source code to be identified clearly and securely, which is the case with A-SIT.

3.6.5.5 Usability Test

A usability test was carried out on March 18, 2009 at the WU Vienna University of Economics and Business and at Montanuniversität Leoben. The aim was to verify the ease of use of the voting system for students. A preliminary version of the voting system was used, into which all of the internal project improvements desired regarding the voting transaction has been implemented. Feedback from students was supposed to be collected in order to verify the development process sought and, where necessary, to adjust it through additional or changed functionalities.

Preparing for the test, an election was configured in which the best skiing country (similar to an election to the University Representative Board) and the best skier (similar to an election to a University Studies Representative Board) stood for election. On the day of the test, which was set to run from morning until afternoon, the required infrastructure was built up at both universities. All students were able to take part, to enter discussions with members of the projects and to take part in continuous improvement of the voting process. The feedback collected to the greatest extent corresponded to the targeted intention of the project and was converted for use in the genuine election. The votes were counted at the end of the usability test. This step served the function of the first test run for the technical and organizational processes for recording votes in the genuine election.

Contrary to diverse reports[65], there were absolutely no systemic crashes of the E-Voting system. The system functioned without any problems both during the usability tests as well as during the genuine election following it.

3.6.5.6 Check of Right to Vote

The check of the right to vote was provided from 23 to 30 April 2009. It provided the first opportunity to use the citizen card. At this opportunity the individual voter could check their own entitlement and right to vote following identification by means of their citizen card. The check of entitlement and right to vote was used by approximately 370 different people[66]. At this time it was already shown that a number of people had forgot the PIN codes for their citizen card, or had entered it incorrectly. There was a hotline available throughout the entire duration of the check of entitlement of the right to vote.

On the basis of complaints received against the lists of voters during the right-to-vote verification, missing datasets could be subsequently uploaded from the university data sharing, and so data synchronization between the universities and the data sharing could be improved.

Use of the voting rights check. The electronic voting rights verification, taking into account the customary low use of the same opportunity in paper form, can be considered a great success. The high number of incorrectly entered PIN codes was a large problem for the acceptance of the process. The coordination between universities and the data network should be further improved for cut-off date queries in the future.

---

[65] See, amongst others, Hauser (2009).

[66] This is stated precisely from 370 different citizen cards. One individual person may have several.

3.6.5.7 Inspection for Members of the Electoral Commissions

The aim of inspection access for members of the Electoral Commission is the fulfillment of the statutory legally prescribed requirements. At the same time, a high level of acceptance for the development of the election and the inspection should be generated. The modality of the inspection is governed in § 64 para. 7 HSWO 2005. According to this paragraph, the Federal Minister must grant Members of the Electoral Commission insight into the client source code and into the election software. Furthermore, the right to inspect the test reports in accordance with§ 64 par. 3 HSWO 2005 must be granted.

The inspection took place on May 8, 2009 in the premises of the Federal datacenter company, BRZ. The participants had to register in advance. In accordance with the legal fundamentals, only members of the Electoral Commission and their observers were permitted to attend.

The inspection of the test report for certification and of the source code was designed for up to 250 people, and 28 were present. The progression was discussed with the participants at the start of the event. The progression was divided into a number of so-called sessions, which introduced the overall system and operation in the form of expert lectures. From the first session, at the same time as this, inspection of the source code was possible on two notebooks in a separate room. The notebooks were operated by employees of the software provider Scytl, who displayed the desired part of the source code on request or the corresponding functionality and were available to reply to any queries.

The test report was made available on a further, additional notebook. If there were any bottlenecks in capacity, further notebooks would have been available.

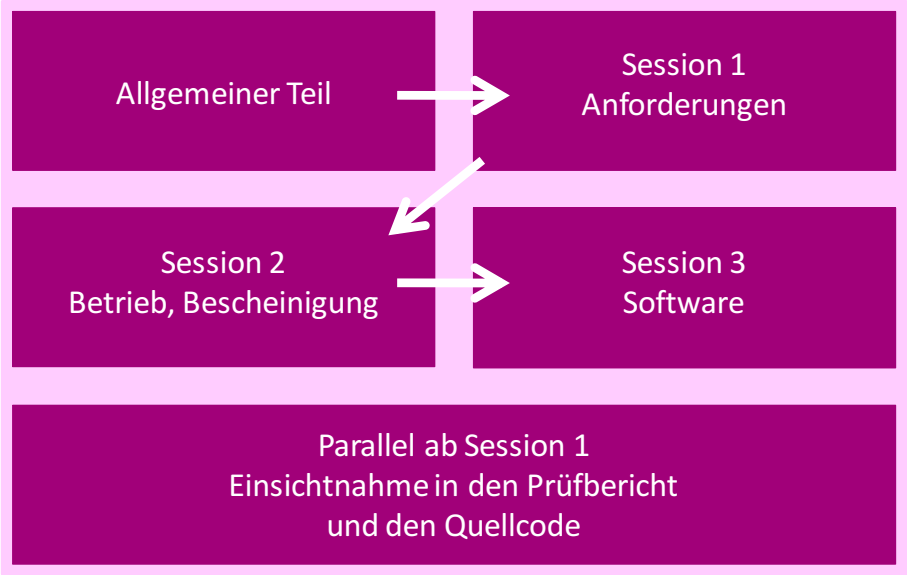

Figure 43: Presentation during Inspection for Members of the Electoral Commission

Prior to the first session, the participants were reminded of their obligation to official secrecy, which they are subject to as a result of their role as a member of an Electoral Commission or as an Electoral Observer since taking up their office. On the grounds of protection of intellectual property, neither laptops, cell phones (with photographic cameras) nor similar devices were allowed to be taken in. These details were received from the software provider and were taken into consideration during inspection.

P R E A M B L E

The aim of this declaration for Inspection according to § 64 para. 7 HSWO 2005 in the sensitive area of elections is to weigh up between the greatest transparency possible on the one hand and between justified interests of the company implementing the security contract on the other hand. With E-Voting for the Austrian Federation of Students we are dealing with an innovation, being carried out in Austria for the first time. The process of inspection of the source code was accordingly designed according to legal guidelines. The experiences gained serve both those carrying out the inspections, to gain detailed insight into the technical processes as well as to the implementing party, to gain new development potential for designing comparable

processes. In this sense, the BMWF on the one hand requests understanding for the declarations required from participants, on the other hand they request support and assistance in continuing to develop the process. The evaluation form issued for this also serves this purpose.

D E C L A R A T I O N

The undersigned increasingly takes cognizance that in their function as a member of an Electoral Commission / Electoral Observer, they are an official in the legal sense of the word and with this are subject to regulations for official secrecy for the aforementioned function and in this way must fundamentally keep all facts they learn of from the aforementioned role secret.

The undersigned further takes cognizance that violating official secrecy according to §310 StGB can be punishable with imprisonment of up to 3 years.

Figure 44: Preamble and Declaration on Official Secrecy

The entire source code for the election software was displayed, including any comments listed in the code. The source code was identical with that which was compiled in an audited process on May 11, 2009 (and was also tested at this time by a Certification Agency and Auditor through 1:1 comparison and was archived in a comprehensible manner) and was used for the elections (likewise verified by the Certification Agency and Auditor through a combination of a number of check sum methods as well as additionally through a binary comparison and comprehensively archived). It was subject to the certification process of the Certification Agency (testing of the source code for several months). Alongside the source code, the entire test report from the Certification Agency was available for inspection by those persons present. At no time were there any bottlenecks during the inspection.

Accompanying talks by the Project Team contributed to an objective discussion. Queries were addressed in great detail.

Viewing the evaluation report and source code. The source code is inspected by an independent certification center in accordance with the legal regulations; this is the opportunity for electoral commissions to inspect the source code and primarily to view this report. The task of inspecting the source code is the responsibility of the certification center, in accordance with the regulations, whereby the result of the inspection is presented to the Electoral Commissions. From this point of view, both time-based as well as organizational framework conditions would be sufficient. The difference between review by an evaluation body and an inspection must be portrayed better. When the Electoral Commissions are inspecting the check report for certification and the election software and the client's source code, a representative of the independent certification center should be present to explain the evaluation method and to answer questions regarding certification directly. Furthermore, the certification center can confirm the authenticity of the source code in advance prior to the inspection. The performance when viewing the report and source code, the presence of experts and the software developers themselves were well received. A completed event offered a broad overview of the overall system, whereby detailed questions could be addressed at any time. In the long term, we can consider using as many open-source-based components as possible to increase acceptance.

3.6.5.8 Project Advisory Board

The Project Advisory Board was set up by Federal Minister Johannes Hahn in January 2009 and has met a total of three times under the direction of departmental chief Friedrich Faulhammer[6733]. It was the aim of this Project Advisory Board to inform people in the region of this project about the project on an up-to-date basis and to accept critical suggestions for the further progression of the project.

---

[67] The three meetings took place on January 22, April 30 and June 16, 2009 in the offices of the BMWF.

The Project Advisory Board is comprised of representatives from the following institutions: the Austrian Federation of Students, the Federal Election Commission for the Austrian Federation of Students 2009, the University Conferences, the office of the Federal Chancellery, the Federal Ministry for Home Affairs, the Federal Ministry for European, Integration and Foreign Affairs, the Federal Ministry of Finance as well as of the Federal Ministry for Science and Research, the Principal Association for Social Security Funding Agencies, the data Protection Commission as well as scientists (political scientists, representatives of technology and constitutional law)[68].

In constructive meetings, the partial project outcomes were presented and were discussed, and recommendations were also accepted for the further course of the project.

The last meeting took place after the election in June 2009, and the participants' experiences were presented there.

Project Advisory Board. Setting up a project advisory board is advisable for future elections using E-Voting because it allows critical feedback to be obtained on individual project stages from representatives of various institutions (e.g., stakeholders, federal ministries, science).

[68] The members of the Project Advisory Board included the following: Samir Al-Mobayyed, Thomas Buchsbaum, Peter Filzmaier, Michael Holoubek, Karl Korinek, Waltraut Kotschy, Gabriele Kotsis, Manfred Matzka, Christian Rupp, Peter Parycek, Klaus Poier, Reinhard Posch, Volker Schögerhofer, Günther Simonitsch, Robert Stein, Gregor Wenda, Arthur Winter, Harald Wögerbauer, Heribert Wulz.

3.6.5.9 Council of Europe Recommendation: List of Ethical Principles

The Council of Europe has already driven through some significant developments in the field of electronic voting. It issued its legal, technical and organizational recommendations for E-Voting[6935] in 2004, which represent the first standardization document for an international organization of the subject.

Since that time, the Council of Europe has also used these developments in its member countries in the field of use for Information Technology and communication technology during the voting process. Based on experiences in Estonia[70], where E-Voting was in very high demand, the Council of Europe recommended a List of Ethical Principles similar to those used in Estonia. This document was translated into German and was relayed on to the Electoral Commissions at the respective universities.

List of Ethical Principles for E-Voting

Principles for the correct and proper implementation of E-Voting

Through the Estonian advances in the use of information technology in different areas of life and the readiness of citizens, to use these new communication media, in the context of anchoring E-Voting in law, an opportunity was seen to support the legal voting principle of free choice through selecting this additional channel for casting votes.

It is important to establish that E-Voting does not mean the role of traditional methods of casting votes. It is also part of the general responsibility that E-Voting takes place legitimately and successfully. This task was written down in the following principles for the correct and proper implementation of E-Voting:

1. The election process of E-Voting – and in particular the condition that the guarantee of privacy of casting a vote is a detail derived from legal election

[69] (Council of Europe, 2004)

[70] (Trechsel, 2007)

principles – should be explained to the voters neutrally and impartially; the voters should have risks cleared up which are associated with surrendering the citizen card and the PIN Code to other people.

2. No joint E-Voting activities (amongst others election parties, E-Voting Service Desks) should be organized on E-Voting days. Such events are viewed as violations of the legal principle of voting in free elections.
3. Voters may not be compelled to cast their votes by E-Voting, in which case computers are made available, at which the voter should cast their vote, in order to influence him or with the clear intention, of collecting their votes.
4. Advertisements on the Internet containing a link to the dedicated E-Voting webpage should be prevented in order to reduce the risk of accessing an incorrect webpage (phishing). This hyperlink could be used to record personal voter details.
5. No election advertising or campaigns should take place in the sphere of public PCs, which are equipped with card-reading devices.
6. Where the possibility exists, a neutral and honest person should be included in the role of an election monitor and both the election commissions as well as the public should be informed of the results.
7. During the election campaign and following the election, if the legitimate progression of the E-Voting was checked, E-Voting and the legitimacy of the entire voting process should not be scrutinized on political grounds.

Figure 45: List of Ethical Principles

Agreeing to a statement of ethical principles for E-Voting. For future elections, a body of experts with representatives from all groups involved in the Austrian Federation of Students and interested in standing for elections should develop its own agreement – developed specifically for elections for the Austrian Federation of Students – regarding ethical principles for E-Voting. This process should be set in motion in the semester before the semester of the election.

3.6.5.10 Training

Along with the introduction of E-Voting, the use of the voting administration system was the second large new development for the Austrian Federation of Students Elections in 2009. This system presented a fundamental paradigm change for the Electoral Commission; however, almost all technical voting administration processes were supported by the system.

In order to design the use of the system to be as smooth as possible for the Electoral Commission, training for the Chairs and their deputies were organized at the same time as the final development steps. The following appointments were held:

- 2/4/6 March 2009: Training sessions in Vienna, Salzburg and Graz;
- 17 March 2009: PC Training at BRZ in Vienna;
- 15/17 April 2009: PC training in Vienna, Salzburg and Graz;
- 20/25 May 2009: PC training - Sub-election Commissions in Vienna, Salzburg and Graz.

The training was carried out by means of training documents and by means of specially prepared training scenarios. The training sessions were made more difficult by the continuous and dynamic development of the voting administration system, which was necessary on the basis of the short project duration.

Training electoral commissions. The training and the final operation of the election administration system were both faced with special challenges during the ongoing further development in terms of teaching end-users non-final elements and operational steps. In the future, the software and training documents should be available in advance. While the training of electoral commissions in two days at three locations approximately two weeks before the cut-off date can easily be organized, training sub-electoral commissions is only possible by spending a half-day, shortly before paper-based voting takes place, as the members of the sub-electoral commission are only appointed immediately prior to the

election. A problematic issue here is that the members of the sub-electoral commissions change very regularly throughout the election period. In order to combat this, several measures are recommended for the next election, such as a training program for tutors who could carry out fixed training on site at short notice. Furthermore, it would be possible to provide more online help and training videos.

3.6.5.11 Parliamentary Inquiries

During the project duration of the Austrian National Union of Student Elections in 2009, a number of parliamentary questions were asked and answered by the Federal Minister of Science, Research (and Economy). Table 7 summarizes these. Both the questions and the replies can be downloaded from the website of the Austrian Parliament.

Query#	Query asked by	Date of Query	Response#	Date of Response
0873/J[71]	Dr. Martin Graf et.al.	12 Feb 2009	882/AB [72]	04.07.2009
1149/J[73]	Musiol, et.al.	05 Mar 2009	1171/AB[74]	05.04.2009
1167/J[75]	Grünewald, et.al.	09 Mar 2009	1262/AB[76]	05.08.2009
2000/J[77]	Musiol, et.al.	07 May 2009	1968/AB[78]	07.06.2009
2550/J[79]	Musiol, et.al.	24 June 2009	2562/AB[80]	08.24.2009

Table 7: Overview of Parliamentary Questions

[71] http://www.parlament.gv.at/PG/DE/XXIV/J/J_00873/pmh.shtml
[72] http://www.parlament.gv.at/PG/DE/XXIV/AB/AB_00882/pmh.shtml
[73] http://www.parlament.gv.at/PG/DE/XXIV/J/J_01149/pmh.shtml
[74] http://www.parlament.gv.at/PG/DE/XXIV/AB/AB_01171/pmh.shtml
[75] http://www.parlament.gv.at/PG/DE/XXIV/J/J_01167/pmh.shtml
[76] http://www.parlament.gv.at/PG/DE/XXIV/AB/AB_01262/pmh.shtml
[77] http://www.parlament.gv.at/PG/DE/XXIV/J/J_02000/pmh.shtml
[78] http://www.parlament.gv.at/PG/DE/XXIV/AB/AB_01968/pmh.shtml
[79] http://www.parlament.gv.at/PG/DE/XXIV/J/J_02550/pmh.shtml
[80] http://www.parlament.gv.at/PG/DE/XXIV/AB/AB_02562/pmh.shtml

3.6.5.12 Data Protection Authority

In the Data Protection Act of 2000, as a second official commission alongside the Austrian Data Protection Authority, the Data Protection Council was also set up. In the Data Protection Council, unlike with the Data Protection Authority, we are concerned with an authority providing consultation and advice. The Data Protection Authority remained skeptical concerning the (at that time planned) change to the Federation of Students election regulation and recorded that before E-Voting could be introduced, an extensive discussion on constitutional law was first required.[81]

The Austrian Data Protection Authority carried out a preliminary check during the course of the project for the data applications E-Voting and the election administration, in which all the relevant legal data protection aspects were checked. Following a successful legal examination by the Data Protection Authority, a data registration number was issued both for the election administration as well as for the voting system.

Data protection and E-Voting. Fulfilling the requirements of data protection laws presented a special challenge during the project. From a purely organizational point of view, for example, a total of 231 forms had to be filled out and approved by the Data Protection Authority.

[81] http://www.ots.at/presseaussendung/OTS_20080714_OTS0138

3.6.5.13 Forming a sector-specific Personal Reference Number (‘*bPK*’) in collaboration with the Population Register and the Data Protection Authority

Forming sector-specific personal reference numbers for the Austrian Federation of Students Elections was carried out in six steps.

Step 1: After only partial advance checks were arranged from the organizations responsible up until the Austrian Federation of Students Elections 2009, which conformed to the Datenschutzgesetz 2000 (*Data Protection Act 200*), further provisions were made as part of this project. For this purpose, notification of two data applications was given by the Chairs of the respective Electoral Commissions at the universities: E-Voting and the election administration system. Following successful approval by the Austrian Data Protection Authority, the systems could start operating from the start of April, and the electoral roll lists could be drawn up.

Step 2: The basis for the lists of the voters’ data is found in data that is shared by the universities, which is governed in § 7 UniStEV 2004 and is managed by the BRZ. In this case, we are dealing with an information technology sharing system in accordance with § 50 DSG 2000. In order that the Chairs of the Electoral Commissions could draw up the lists of voters, the Chairs of Electoral Commissions first had to call up the information according to § 7a UniStEV 2004. This authorization to call up is further governed by § 8 para. 2 Educational Documents Act, where administrative processes are also standardized for data security. Once this first step has been completed, the data for the list of voters in accordance with § 18 HSWO 2005 are physically in the possession of the Chairs of the Election Commissions.

Step 3: The Chairs of the Election Commissions now commissioned the BRZ to draw up the electoral rolls, and in this case, they are a legal data protection service provider. A service provider agreement in conformance with DSG 2000 was concluded between each Chair and the BRZ for this purpose.

Step 4: The Chair of the university in each case applied to the sourcePIN registration authorities, contained within the offices of the Data Protection Authority, to be issued with the initial sector-specific personal identifiers by the sourcePIN authorities.

Step 5: Following the approval by the sourcePIN registration officials, the service provider for the Chair could transfer the data to the Central Register of Residents at the Department of the Interior, which then computed the Personal Reference Number *(bPK)* or identified non-matching events.

Step 6: Some 10% of the sourcePIN data could not be issued with a sector-specific Personal Reference Number *(bPK)* by the Central Register of Residents *(ZMR)* on the grounds of different styles of writing, special symbols, input errors and similar data quality problems. The BRZ worked through these cases manually, and in this way, in a second run, 100% of the bPK allocations could be achieved.

Future use and storage of sector-specific personal identifiers. The sector-specific personal identifiers created for the 2009 elections for the Austrian Federation of Students should also be capable of being used for future elections and applications in the Austrian universities sector. Storage in universities' data network would be logical for this. To this end, changes in the legal basis are required. This could increase the spread of citizen card uses in universities.

3.6.5.14 "Distributed Denial of Service" Attack

A separate section is dedicated to a so-called distributed Denial of Service attacks (dDoS). dDoS is a targeted attack on a service coordinated by many attackers, with the aim of generally overloading the system, so that it is no longer available to any possible users. A typical example would be for 100 people to agree with each other and to constantly ring up the emergency response number for assistance, whereby (almost) no genuine emergency telephone calls could be processed there any longer. The access becomes significantly more dangerous by being automated – for example, by using a computer that dials the emergency response number around the clock at very short intervals without any human involvement.

At the election to the Austrian Federation of Students, there was an organized attack on the system. In the time before the elections[82], an open appeal took place through ARGE DATEN to subject the E-Voting (and later the application) to an "availability test", through which one should or could also permit a program[50] likewise published by ARGE DATEN to run continuously throughout the entire duration of electronic voting. The appeal to use this including instructions for use was carried out amongst other things by e-mail dispatch and targeted positioning on the website. It should be noted that the voting system was not published until the start of electronic voting, for which purpose at this time neither the voting system nor the web address deposited were known.

Evaluation by CERT.at[83]

In the time before E-Voting commenced for the Austrian Federation of Students elections in 2009 a "test tool" written in JavaScript on the website of ARGE DATEN ('BAD DATA') was published for the availability of the E-Voting systems. CERT.at has taken a closer look at this and came to the following realizations:

[82] The 'availability test' tool used Javascript and was published on a website from ARGE DATEN

[83] CERT.at provided this expert opinion to the BMWF.

The Tool

The tool was implemented inside a normal website using JavaScript. An input screen first prompted a page for testing for inputting URLs (once by HTML, and once as a picture), secondly suitable URLs for the E-Voting system were prescribed and third a waiting time between tests and 'loading coefficient' (number of downloads running in parallel) had to be entered. The default had been re-set here for 500 msec and five, i.e., ten times per second the page (and the image) should be called up.

After the script commenced, the corresponding number of (invisible) iFRAMES were inserted into the document, and these were regularly loaded again by means of a timer with the page to be tested. Parallel to this, the image given is also called up in the same frequency.

A code in the main part of the page tries to compute an availability statistic from the log of downloads and displays this.

The ARGE DATEN server is only involved in downloading the tool embedded in the HTML, and the actual test is completed entirely in the user's browser.

Evaluation of Potential for Danger

At first glance, the tool is harmless: it does not attempt any of the classical attacks, such as SYN Flood, SQL Injection, XSS or even especially extensive queries. The problem arises simply from the scaling, that is, if a) the parameters are changed and/or b) many people use the tool in parallel.

Even a short test showed that with corresponding parameterization (some 10 copies every 5 msec), a PC can fully use up the bandwidth of an ADSL or cable connection and can access more than 10 Mbit/s of data from specified web servers. If only one hundred Internet users with a good Internet connection followed the appeal from ARGE DATEN, the distributed use of this tool would have caused a bandwidth requirement in the region of gigabits for the operators of the E-Voting server.

The attacks in Estonia in May 2007 were based on similar principles: Instructions and simple scripts were published in web forums, on even inexperienced users can

take part in ‘distributed Denial of Service’ attacks. The contribution of each individual person involved was insignificant, but the total of these gave rise to an attack that severely affected the country.

CERT.at transmitted these doubts to ARGE DATEN on May 14, 2009.

Measuring Availability or an Attack tool?

It is legitimate to examine the availability of E-Voting systems and to want to measure how well E-Voting functions. The points listed below should be followed:

- Each active measurement influences the system to be measured, and in this way, it falsifies the result. (See, for example, Heisenberg uncertainties in physics.)
  Example: If we wanted to test the prompt achievability of the European emergency response number 112, then it would not make any sense to make several thousand test telephone calls per second, as this is a multiple of the normal load and in this way the genuine achievability is falsified.
- What load must the E-Voting system be designed for? Completely unrealistic numbers were named by ARGE DATEN for this.
  As with normal elections in polling stations, we must not assume that all voters wish to vote at the same time. In particular for the Austrian Federation of Students’ election, which lasts for a number of days, it would be absurd and unnecessarily expensive to design the voting booths and the E-Voting server in such a way that all voters (or even those entitled to vote) could vote at the same time. A brief rough estimate (1% of E-Voting of typically 250,000 voters, distributed throughout five days for 18 hours/day) on average shows around one voting transaction every two minutes. We cannot expect this will run so evenly; however, even with a correction factor of 100, the result still lies at less than one voting transaction per second. A test that carries out several queries per second thus dominates the legitimate load of the server very easily.
- Every safeguard of the server makes the measurement worthless. The classical defense mechanisms against ‘distributed Denial of Service’ attacks are based on

the fact that the server ignores troublesome queries or that these are already blocked before they reach the server.

Publishing a ‘test tool’ with the proposal to use this over as extensive an area as possible is therefore not expedient if we were really trying to determine the correct availability information.

Frequent use of the laptops would force the operator of the E-Voting system to perform one of the following:

- to completely unnecessarily overdesign the server and the connection in order to be able to reply to all queries, which would cause unnecessary costs; or
- to allocate the tests as dDoS attacks and to block these.

Defense Mechanisms

The task of securing a webserver against such attacks is one of the problem situations that operators of popular or controversial websites must solve regularly. The techniques for doing so are well-known, and there are appropriate books, software and also appliances available for purchase on the market.

We are always concerned with differentiating legitimate users from problematic attacks and filtering out the lattermost as efficiently as possible. In the simplest case (which still would have proved sufficient here), we simply recognize whether the same client calls up the same URL at short intervals time and again repeatedly. Blocking clients is also problematic if in parallel to the disturbing action, access is also attempted from a legitimate user from the address. This could occur if, for example, one voter starts the “Test Tool” prior to attempting to vote or if many users access the election system from the same IP address by means of Network Address Translation (NAT).

However, an analogy to normal paper-based voting is valid: If a polling station is besieged by demonstrators, legitimate voters must reckon with obstacles and delays.

Summary

- The tool was not suitable for making meaningful measurements of availability.
- An extensive use of the tool would have a similar appearance to a "Denial-of-Service" attack.
- Publication of the tool must at least be classified as clumsy.
- Defending against such an attack would have been possible without any problem provided that corresponding provisions had been made.
- Interference with legitimate voters by users of the "test tool" cannot be completely excluded.
- In general, we must emphasize that with the spread of broadband Internet connections, it becomes easier and easier to cause a high server load with simple tools.

Figure 46: Evaluation of the dDOS attacks by CERT.at

Although the attack could very easily be stopped by appropriate applications upstream of the voting system, of the web portal as well as through a special JavaScript[84] and the availability and functionality of the electronic voting system was not endangered at any time, we must note here that such a type of planned attack on an election is unique and is also not known of in other countries. In any case, it is doubtful in a democratic political system that a legitimate election could be obstructed and prevented in Austria by these methods for the first time.

[84] The attack was based on pages called within invisible iFRAMES. The attack tool was ended immediately by means of a Javascript query of whether the page is called up in such an iFRAMES and where necessary the entire pages must be re-loaded outside the iFRAMES. This Javascript was specified at the start of the project by experts monitoring the project for the integration of the election software and was an integral constituent part of the certified election software solution. The Javascript was likewise integrated in the web portal when electronic voting started, whereby all the tools running up until that time for 'availability checks' were automatically ended.

Furthermore, it is dubious that a tool will be made available precisely for ARGE DATEN and will be accessed for use, with which one can also attack all other networks and data without any problems, except for the actual individual addresses of ARGE DATEN, (as for argedaten.at, .com or .net …), which were not accepted.[85]

Risk of a dDoS attack. The risk of dDoS attacks is not specific to E-Voting. Handling of dDoS attacks was part of the security concept of the E-Voting system and led to corresponding organizational and technical security precautions being taken and being planned for in the project. A key security measure is that § 48 para. 4 HWSO 2005[86] and HSG § 39 para. 7[87] state that if E-Voting is declared invalid due to impaired security or functionality during the election, voters who submitted their vote through E-Voting must be permitted to submit their vote again at the polling station.

---

[85] The addresses cited were configured in the tool for "Check for Availability" as non-legitimate addresses in the source code, whereby this list has been changed a number of times or was added to. After the tool was deactivated, this check was also removed including the addresses.

[86] § 48 para. 4 HWSO 2005: If the E-Voting has been declared invalid according to § 39 para. 7 HSG 1998, then the voters who cast the vote by means of E-Voting are approved for submitting a new vote in the polling station.

[87] § 39 para. 7 HSG 1998: The Chair of the Electoral Commission must discontinue voting when the security or the functionality of the electronic components deposited with the Electoral Commissions is compromised during voting. In such cases, the Electoral Commission must decide on the validity of the electronic votes cast prior to termination with the involvement of a Confirmation Office in accordance with § 19 of the Signature Act.

3.6.6 Voting Phase

3.6.6.1 E-Voting

Punctually, on May 18, 2009 from 08:00, casting electronic votes was possible. This was released by the voting system. One minute later, the first legally valid vote had already been cast.

On Monday morning, it was discovered that the abbreviations were missing on the ballot papers for all 21 University representative elections. Furthermore, it had been determined that one party had been described merely a 'Young Student Initiative' (*Junge Studenteninitiative*) instead of as the 'Junge Europäische Studenten Initiative' (*Junge Europäische Studenteninitiative*) on the ballot sheet for the University representative elections at the University of Vienna. The reason for the mistake with the abbreviation lies in a communication problem during the data export from the voting administration system to the election system.[88] The lack of a part of the name of a party arose from a co-ordination problem.[89]

It is important to emphasize here that these were not mistakes from or by E-Voting, but they represent mistakes during the preparation of the elections, which arose for both the paper-based voting as well as for E-Voting; this point is often represented incorrectly. In this case, reference has in particular been made to the mistakes discovered in the electoral rolls of the University of Salzburg during paper-based voting.

Casting electronic votes technically successfully ended on May 22, 2009 at 18:00.

---

[88] The electronic voting system merely portrays the data exported from the election administration system.

[89] The 'Young European Student Initiative' (*Junge Europäische Studenteninitiative*) was still incorrectly entered in the voting administration system at the time of data export.

Implementation of E-Voting. During preparations for paper-based and electronic elections in the future, a technical and organizational authorization process should be introduced in agreement with the relevant chairperson of the electoral commission at the corresponding university.

3.6.6.2 Support

Alongside the help setting on the homepage of the project, telephone support from BRZ was also available on a number that could be reached for a local rate. During the first test run, telephone and e-mail support was offered as part of the check on voting entitlement (*right to vote*).

First- and second-level helpdesks with telephone-based and e-mail support were provided for the duration of the checks of voting entitlement and of electronic voting, and were staffed from Monday to Friday from 08:00 h until 17:00 h every day.

Help and Assistance. Support by telephone and by e-mail was not in great demand. This allows us to conclude that the help and assistance for the electronic election was very well documented on the website and that the actual problems experienced clearly arose before this, for example, during installation of the card reader or through forgetting citizen card PIN codes. Mobile signatures could be a great help here, as the main problems (inputting PIN code / card readers) would no longer occur.

3.6.6.3 International Election Monitors

On May 18-19, 2009, the Federal Ministry for Europe, Integration and Foreign Affairs, held an international workshop on the subject 'E-Voting from overseas' in English language. At the invitation of the Federal Minister Science, Research and Economy, those attending the workshop could observe the elections to the Austrian Federation of Students.

Observers realized there that monitoring E-Voting must follow new approaches, in particular, end-to-end monitoring of the entire process chain must be possible, since pure observation of the processes on the day of voting only permits minimal conclusions to be made.

Monitoring Electronic Elections. It seems logical to make the essential E-Voting processes (i.e., generating the keys, sealing, voting system, counting votes) accessible to election monitors during future elections, following comprehensive instruction.

In order to illustrate the status of the elections more transparently, and in particular the complexity of the Austrian Federation of Students elections, the level of detail of mapping on the election monitoring screen should not only be on a university by university basis, but it should also show the number of voters on a study course basis. The misleading presentation of numbers of votes obtained should be improved. The difference between a submitted vote and the voter's profile should be depicted more clearly.

3.6.6.4 Paper-based Voting

Paper-based voting was carried out from May 26-28, 2009. For the first time, support from electronic voting administration system was available to the Sub-Electoral Commissions at all 21 universities. An online electoral list was used based on the electoral roll for the polling station. Precisely in the electronically supported record of the allocation between students and polling station, there were faults prior to commencement, which were swiftly discovered at the start of the first day of voting and were also resolved. For those polling stations, based on allocations according to the starting letter of surnames (as opposed to those based on student matriculation numbers or which had no additional division), students whose surnames started with a special symbol were not taken into consideration. For example, the following were defined:

- Those students with surnames starting from A to M were assigned to polling station 1;

- Those students with surnames starting from N to Z were assigned to polling station 2. For example, there was no definition which polling station “Mr. Franz Ísak” or Ms. “Marta Ásdís” were to be allocated. This could be swiftly resolved through an additional filter.

During elections at the University of Salzburg, during paper-based voting, it was discovered that the electoral roll was incorrect. The cause for this can be derived from an operational error of the voting administration systems.

Improvements to the election administration system for support at the polling station. A process for evaluation and continual technical and organizational improvement of the election administration was launched in the form of workshops to support the activities of the chairs of Electoral Commissions and members of the sub-electoral commissions. Missing features, improvements – above all in usability – as well as faults were recorded and should be transformed for the next elections to the Austrian Federation of Students. An online platform is recommended in order to achieve the best transparency possible for the chairs of electoral commissions at the universities and agree on the requirements. Requested changes as well as jointly worked out realizations are listed in the form of open project management.

3.6.7 Post-voting Phase

The post-voting phase commenced with counting of paper-based and electronic votes on May 28, 2009 and ended with the destruction of the data.

3.6.7.1 Counting the Votes

Counting the paper-based votes had already started at the universities once the last of their own polling stations was closed. Counting electronic votes was carried out in public in the presence of the Electoral Commission in the offices of the Austrian Federation of Students of A-SIT as well as of the operational team of the BRZ from 17:00 on the last day of voting. After completing comprehensive security and documentation processes, the electronic results were available 1.5 hours later in the voting administration system. For individual Electoral Commissions at smaller universities, this waiting time was too long, and they postponed the announcement of the final result until the next day. A further delay arose from results of the electronic vote not being accessible at the respective universities until the results of the paper-based votes for the Electoral Commissions had been input. In particular, this presented a problem because the media wanted to have the results immediately. The time is however prescribed by § 46 para. 8 in combination with § 32 para. 2 HSWO 2005.

Availability of results. In order to reduce pressure from the media, it makes sense to legally permit counting the electronic vote as early as during the course of the afternoon in the electoral rules. A news blackout on the results would then need to be imposed for those universities whose polling stations have not yet closed. Results of the electronic vote could – after examining the law basis – also be made available on an individual basis, since this was very much in demand from the media.

3.6.7.2 Destroying Voting System Data

The data to be destroyed is recorded in the Austrian Federation of Students Election Ordinance 2005 in the following paragraphs:

- § 69 HSWO 2005: E-Voting data and software must be archived three weeks after the last day of voting and handed over to the Chair of the Electoral Commission for the Austrian Federation of Students. This person must store the data in a suitable form for five years in accordance with § 53 para. 4 in the case of an appeal in accordance with §§ 58 or 59 at least up until the end of the final appeal process. In particular, voting secrecy must be guaranteed.

- § 53 para. 4 HSWO 2005: The Electoral Commission of the Austrian Federation of Students and Electoral Commissions at the universities must store election files in an ordered and clear form for a period of five years and ballot sheets or ballot papers for a period of two years. The act of voting for the Electoral Commission at the Austrian Federation of Students includes acts of voting concerning the voting community and the list associations standing for election.

From, this it was ascertained that with an electronic voting system, the electronic ballot sheets, source code and the voting software code compiled for must be stored. The electronic ballot sheets are those data that are the outcome of the counting process. In this case, the electronic ballot sheets must be handled similarly to ballot papers in paper-based voting[59], during which time the secrecy of the ballot must not endangered through ownership. The electronic ballot sheet contains no form of reference to voters.

All other electronic voting system data must be destroyed within three weeks of the last day of voting as a consequence of the legal obligation to deletion under data protection. In particular, this includes the electronic ballot boxes.

Although one could consider a virtual destruction as sufficient by repeatedly overwriting the data with random values, a conscious decision was made on grounds of security and transparency for a physical and thermal destruction of all media. Therefore, all of the hard discs from the election servers and laptops (in particular, from the mixing laptops) were physically destroyed in an audited process by the company Reisswolf and were subsequently melted down. All media were uniquely marked during the setup and were transported in a sealed safety container and were for their identity and their completeness during the course of destruction.

Figure 47: Physical Destruction of Data

Two of the four smartcards with the interrupted private voting key were likewise destroyed with auditing following the data destruction[90]. The two other smartcards were destroyed by other member of the Federal Electoral Commission.

[90] Care must be taken that three of the four smartcards are required to de-code the electronic ballot boxes as well as the passwords with which the smart cards have been secured (locking the card following three incorrect attempts to input the code). Both the knowledge as well as the property has been distributed to members of the Federal Electoral Commission. The Federal Electoral Commission in turn has no unmonitored physical access to the electronic ballot box as opposed to with the paper-based election, in which the Electoral (Sub-)Commission in the respective university opens the ballot box when counting the votes with the exclusion of the public and the media and counts them.

Destruction of data. Destruction of data should take place in public similarly to counting the electronic votes. To this end, the corresponding spatial and organizational framework conditions should be created. This includes, for example, accessibility of the physical data destruction facility, appropriate moderation and presentation to a large number of people, transferring a large number of people from one location to another and much more. Video transmission could be considered.

3.6.7.3 Arbitration Process and Monitoring Commission

In the period from March 3 to May 4, 2009, there was a conciliation process between one of the blind students concerned and the BMWF. This had shown that a group of blind people could possibly be excluded. These circumstances were discussed in a constructive atmosphere, and agreements were reached. Unfortunately, on legal grounds, information for the use of certain Screen readers could not be published in the intended manner on the web portal www.oeh-wahl.gv.at. One possibility to improve these circumstances was accepted as part of the evaluation consultation.

The number of students with disabilities who used the opportunity to cast their vote electronically is not known. However, this resulted in a telephone call to a blind student during the election, who evaluated successfully casting their vote very favorably.

On July 21, 2009, a meeting took place at the Federal Ministry of Labor, Social Affairs and Consumer Protection of the independent Monitoring Commission, in which the E-Voting Project and the legal fundamentals at that time with regard to universal accessibility for casting votes conventionally at Austrian Federation of Students votes was discussed.

On one hand, the E-Voting Project and the efforts connected to this were praised without exception; on the other hand, errors with the legal fundamentals of paper-based voting at that time were identified. Therefore, in the Monitoring Commission's opinion, § 37 para. 4 HSWO 2005 must be adjusted to the Equality Act. In particular, the introduction of voting templates was proposed, since they have also been in use for the elections to the Austrian Parliament since 1992.

On August 18, 2009, arbitration negotiations took place in Klagenfurt between a blind student and BMWF, the content of which was likewise the introduction of voting templates. The complainant was satisfied with the outcome of the negotiations on grounds of the approval by representatives of the Federal Ministry to recommend to the Federal Minister the realization of the best possible legitimate use of voting templates before the coming elections in consultation with Chairs of the Electoral Commissions, disability speakers at the universities and also in direct collaboration with disability associations.

Integrating people with disabilities. People with disabilities were always a target group of the project, as electronic forms of voting precisely accommodate this group of people. As this advantage of E-Voting was not actively communicated, fears increased that these voters could be excluded by this new technology. In the end, it became clear that much can be learned from E-Voting, particularly in the non-electronic field. However, for the future, it will be necessary to integrate this group even more closely into the communication channels from the start of the project.

Introducing ballot papers suitable for those with disabilities for paper-based voting is also an important suggestion to come from this project. Corresponding preliminary work has already been carried out, and such ballots can be implemented in a legally compliant manner during the next elections to the Austrian Federation of Students.

3.6.8 Presentation of the Evaluation Report

In the beginning of 2010, a *Rochade* took place within the executive branch when the seat of the Minister of Science and Research became vacant. Johannes Hahn had become the successor of Benita Ferrero Waldner as the Austrian member of the European Commission and was followed by Beatrix Karl. The evaluation report was released on April 2, 2010, and she announced in an interview with the newspaper *Der Standard* not to continue the use of E-Voting in the upcoming federation of Student elections in 2011 (2010). While it was expected that this would end the discussions around E-Voting, this was not the case. Instead, it provided new impetus to the debate.

The discussions around E-Voting, in particular the doubts about the legality of its implementation, led to some 20 appeals against the election results of the 2009 Federation of Students' elections as well as the legal basis as established in the Federation of Students' law, and in its corresponding ordinance for the conduct of the elections. The Austrian Constitutional Court bundled several of the appeals and rejected most of them for formal reasons. In December 2011, however, after a public hearing, the court came forward with several decisions with regards to E-Voting, out of which most were rejected. The constitutional court came to the conclusion that the regulations with regards to E-Voting in the Federation of Students's law was in line with the constitution; however, the ordinance, which provided the essential organizational framework, was considered to be not in line with the law because it lacked legal determination. The main problem was due to the lack of possibility for the electoral commission to fully take account for the conduct of the electronic part of the election without the help of a third party, including that advance elections (like in the case of the E-Voting for the student elections) need to be regulated in the law. This decision was also discussed controversially in literature (see amongst others, Poier [2013], Oswald [2016], Balthasar and Prosser [2012], Goby and Weichsel [2012]). Nevertheless, Parycek et al. (2017) propose a synthesis of requirements for E-Voting based on decisions of the constitutional court. One of the proposed points, verifiability, is also discussed in a subsequent chapter.

3.6.9 Summary

The year-long discussions and preparations for a first attempt to use Internet voting for a legally binding election had its culmination in the effort around the Federation of Students' elections. At the time, it was one of the most ambitious E-Government projects of the year in 2009. The objective here was to supplement the paper-based voting process used up until now with an electronic voting channel and therefore to create new possibilities for casting votes.

It has been demonstrated that in the legal context, statutory legal specifications were supplemented by numerous implementation regulations in the Federation of Students' ordinance.

A very high level of security was also provided in the area of technical infrastructure through the citizen card. In particular, the highest level of data protection could also be guaranteed with the use of sector-specific Personal Reference Numbers.

In the area of socio-political discussion, it was shown that many contents of dialogues for introducing remote voting had to be carried out for the first time. This was surprising because the year before votes could be cast by postal vote in elections to the Austrian Parliament. The intense preoccupation of parties campaigning for the election in principle had no positive influence on the intrinsic perception of the institution of the Austrian National Federation of Students.

With the realization of components of Internet voting, significance was placed on state-of-the-art technology, and therefore comprehensive measures for universal accessibility were put in place as well as a sample application for familiarization purposes with the voting process. Importance was placed on the highest level of security when realizing the voting process itself – both in identification using citizen cards as well as in operating failsafe computer data centers at two separate locations. The continuous casting

of votes was overseen using the vote monitoring function, and operation was also monitored with cameras. For the first time, the introduction of a voting administration system supported the work of the Electoral Commission throughout the course of the entire election process.

The implementation of the project can be illustrated in three phases. In the pre-voting phase, numerous activities were implemented in order to facilitate this use. An open discussion was held in December 2008 in the context of a specialist conference and an accompanying tour including conversations with stakeholders at all university locations. The software used was certified by A-SIT to increase transparency, and a review of this evaluation report and the source code was facilitated for members of the Electoral Commission. Before the elections, numerous training sessions were held in order to familiarize the Electoral Commission with handing the system. One challenge was to issue the Electoral Commission with sector-specific personal identifiers for the first time, which was combined with the initial regulation of data protection for the voting system.

The project studi.gv.at was planned at the same time as a measure to increase penetration of citizen cards at universities. Comprehensive information in the form of flyers and posters were circulated amongst students, and public consultation meetings were held. At the beginning, however, the number of authorized students only developed slowly, which above all could be derived from the lack of applications available. Authorization only became more appealing as E-Voting drew closer and closer.

The pre-voting phase was characterized by intensive discourse as well. Along with numerous podium discussions, information campaigns using flyers and even movie spots placed by the Austrian National Federation of Students, there were also numerous parliamentary questions to be answered from the BMWF. Likewise, a swift technical defense against dDoS attacks proved effective; however, it led to many discussions.

The voting phase itself consisted of electronic voting and paper voting. The former was possible in the context of casting votes brought forward to the earlier dates of May 18-22, 2009 and which ran without any technical problems. 2,161 students, or almost one percent, used the opportunity to cast their vote(s) electronically. The biggest problem was that students forgot their PIN Code associated with their citizen card. Incorrect ballot papers (with abbreviations missing or the wrong name of a faction campaigning in the elections), problems caused through incorrect inputting and lack of communication can be prevented in future by introducing improved administrative processes. The voting administration system proved itself in the development of paper voting, even though the level of training provided for the Electoral Sub-Committees could be improved.

In the post-voting phase, counting votes and destruction of data was completed; this was necessary in accordance with the Data Protection Act. Consideration should be given here to time-based components when publishing the results of future elections, as this is of very great interest to the media. The discussions regarding E-Voting did not loosen either once the results were published, but they were kept alive through a large number of appeals and complaints to the Constitutional Court.

Despite all efforts, the areas of transparency and accountability did not receive enough attention due to a lack of public confidence in the election technology and the election itself. This subsequently led to the discontinuation of the pilot and also a number of appeals against the election results leading to the Constitutional Court lifting of the election result, which showed that, most importantly, the implementation of the law's principles into an ordinance needs to include technical detail (Goby and Weichsel, 2012).

3.7 Overview of the Experience with Internet Voting in Austria

To this date, the efforts to conduct Internet voting for the Austrian Federation of Students' elections in 2009 has been the only effort aiming for a legally-binding result, as was described in the previous chapter. Clearly, the experiences with implementing such new election technologies have shown that what once seemed a technical problem became much more. At the beginning, the technical solutions for the main problem of verifying the eligibility of voters and maintaining secrecy was at the center of attention. Later, more sophisticated algorithms were developed, and functionalities like quota in election commissions were added. However, the experiences showed that accurate legal regulations are needed, which not only show the interaction with the constitutional legal texts but also on how to give accountability to a remote electronic voting channel through legal means. International standards were a first step, but regulations based on actual experience are necessary to show how remote electronic voting channels can be realized and where it is needed in order to avoid problems identified in pilot implementations. Furthermore, this practical knowledge also shows that sophisticated algorithms are not always the key to success. Rather, several key implementations make use of very basic technical means to realize the tasks given by law.

One should not forget about the voters. They not only need to use such systems but also need to understand the processes in order to build their trust.

It can be ascertained that early efforts testing Internet voting in Austria were uncoordinated and lacked a more general strategy. Early on, it was clear that the Federation of Students' election would play an important role.

As such, the Austrian premiere of a first implementation of a remote electronic voting channel in a legally binding election showed successfully how a participation via the Internet is possible in a political decision-making process. The pilot projects offered experiences from which to learn. This especially includes the adaptation of paper election

processes to the requirements of processing electronic votes as well as the intensive public discussion. The public discourse had to be led and was very important to the topic of E-Voting as well as to the discussion of remote voting channels in Austria in general. It also shows that an electoral context with a history of heated debates about electoral reforms did not turn out to be the best place for introducing new voting technologies. It has framed the debate about electronic voting in Austria (Wenda, 2016) and provided important technical, organizational, political and legal lessons (Prosser and Krimmer, 2004a). Table 8 provides an overview of the E-Voting implementations in Austria.

Name	Voting Period	Identification	Anonymity	Eligible Voters	Registered Voters	Participating Voters	Turnout
First Telekabel/UPC Usergroup Election	19.10.1999 – 28.11.1999	Username & Password	Separation during voting / Organisational	Ca. 15000	N/A	557	11
Second Telekabel/UPC Usergroup Election	2.5.2000 – 31.5.2000	IP Address	Pre-electoral, organisational	Ca. 15000	N/A	4740	30
First Internet election	20.5.2003 – 22.5.2003	Username / Password	Separation during Voting (two-phase)	Some 1300	978	355	36
Second – Federal Election of President	23.4.2004 – 25.4.2004	Username / Password	Separation during Voting (two-phase)	20000		961	-
Test Election for Austrians living abroad	12.10.2006 – 14.10.2006	Username / Password	Separation during voting (two-phase)	Some 500,000	-	148	
Federation of Students' elections 2009	18. – 22.05.2009	Smart Card	Post-electoral Mixing	230528	N/A	2161	0,94

Table 8: Internet Voting Implementations in Austria

4 Identification of Building Blocks

When introducing information and communication technology to any given electoral process, very similar decisions need to be made. Based on the analysis of the experiences in the previous chapters, we explored and identified decision modules or building blocks that could be used when developing an electronic electoral process. We identified twelve important areas when designing, building and finally deploying a remote electronic voting channel via the Internet:

1. Deciding on the form of electronic voting used;
2. Adapting the legal basis;
3. Selecting the technical means to solve the main paradox of unequivocally identifying the eligible voter;
4. Ensuring the secrecy of the vote;
5. Observing, assessing and verifying all steps of the electoral process;
6. Giving the election commission control over the process; and
7. Evaluating that the software works as required;
8. Enabling overall transparency for the process;
9. Designing a fair ballot sheet;
10. Protecting private data;
11. Providing for the organizational context;
12. Conducting a feasibility study to determine all of these steps ahead of a first implementation.

Figure 48 gives an overview of these topics, and in the following, these building blocks are described in more detail.

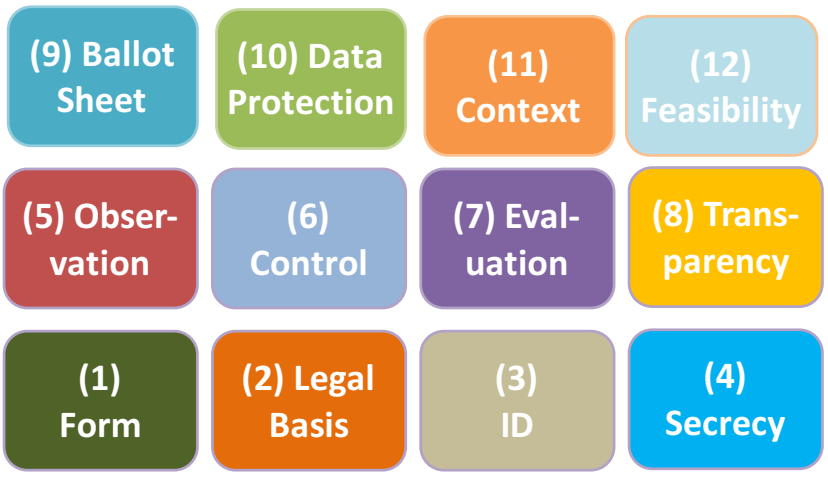

Figure 48: Building Blocks of Internet Voting

In this chapter, we present these twelve building blocks that seem important for the conduct of Internet voting in more detail.

4.1 Forms of Voting Technology

The question about which means are actually used to count, transmit or cast votes is crucial for the determination of the process and the entire election.

(1) Stand-alone voting machines. Elections can be supported by electronic means through stand-alone voting machines that store the casted votes locally and count and transmit the results at the end of the election. However, these machines can be designed in very different ways. They can consist of a computer limited by software to that particular use. The machines can also utilize push-button machinery or touchscreens. There are also voice-activated machines for visually-impaired voters, but naming all possible designs is not the objective of this study. Another option with stand-alone voting machines are stand-alone machines that have no connection to other machines, which would require the election results to be summed up by election officials.

(2) Internet elections are possible in many ways and have several subgroups and different names, such as remote E-Voting or mobile voting. The important aspect of this voting method is that the vote must be able to be casted from any laptop, tablet or mobile phone, and the eligibility to vote must also be verified via an online channel. Internet voting is the electronic equivalent of postal voting. Next to these four clear election forms, there are two additional election processes that cannot be accounted to one group alone.

(3) Ballot scanning is one of such mixed forms, as the system still uses paper ballots that are scanned and accounted for electronically. The scanning process is usually conducted in one of two forms. First, a central counting center is erected, where the ballots are transported and counted. Second, a scanner is installed above every ballot box; when a voter introduces the vote, the scanner scans the ballot directly and transmits the result to a central counting position.

Scanning is usually a suitable technology to accustom voters and election officials to an electronic back-end system, since important parts of the election process are now conducted electronically, but voters do not have to get used to changes within their election habits.

The last possibility is a mixed form between remote and presence voting. **(4) Locally operated Internet voting systems** voting uses electronic election machinery, but the machinery is, in this case, not placed in ballot stations but in libraries, schools or other public buildings. The environment is not controlled in this situation.

The following table from (OSCE/ODIHR, 2013) summarizes these forms in the following overview. This table exemplifies the different possibilities within an election design.

Place of voting / Medium	Used in a Controlled Environment	Used in an Uncontrolled Environment	Used in Mixed Environments
Voting with paper ballots	Voting with paper ballots in polling stations	Postal voting	Mobile ballot box voting
Voting with electronic means	(1) Electronic voting systems; (4) Locally operated Internet voting	(2) Internet voting	Hybrid electronic voting solutions: Systems using Internet voting technology
Paper ballots and electronic counting	(3) Ballot scanner		Centrally-counted postal votes using ballot scanners

Table 9: Overview of Different Possible Uses of Voting Technologies

4.2 Legal Basis

When designing the legal basis for electronic voting, among the first questions is whether or not it is in line with international commitments. Hence, most publications on national legislation regarding remote electronic voting concentrated on whether it is in line with the constitutional requirements of the respective country (Ziska, 2004, Karpen, 2005). Also, the Venice Commission of the Council of Europe commissioned a study (Grabenwarter, 2004a, Grabenwarter, 2004b) that found general compatibility.

On the international level, the Council of Europe also passed the only legal document – though not legally binding – with a recommendation on how electronic voting systems should be designed (Council of Europe, 2004). At the third meeting to review the recommendation, it was amended by two documents to reflect recent developments in

transparency and certification (Council of Europe, 2011a, Council of Europe, 2011b). In 2017, an updated version of the recommendation was released. The recommendations have been updated and condensed, and the overall number of recommendations have been reduced. Furthermore, the guidelines were matched to relevant recommendations, and thereby the scope of the document was expanded. Also, guidelines can be more easily amended and changed compared to the actual recommendation.

4.3 Identification

The identification of voters is an essential part of the whole voting process, and it is closely linked to the available online identity management infrastructure in the country where the election is being conducted. Early on, this was identified as one of the core components of developing voting technology solutions (Krimmer, 2002). Several forms of identification exist.

The first form of identification is to use a **(1) token**, which can be designed in different ways. The token usually provides a one-time code to the voter. Reusable token solutions are also easily possible if the distribution and disposal process ensure absolute anonymity. One-time solutions are usually based on a random number. These codes usually have between five and 15 alphanumeric figures, which are usually produced in secure printing center and then protected by a scratch field. This prevents the number from being seen by all third parties. The scratch field as well as the printer need to comply with several security requirements for the protection of the number. In addition, after the field has been scratched, security must be ensured, which means that a transition of the number should be made impossible. A transition is only not possible if the code is provided to the voter immediately before the vote is cast.

The identity of the voter is safe if the token is disposed or destroyed immediately after the successful casting of the vote. The token solution does not automatically provide secrecy. Any of the solutions provided in this chapter can be matched with any form of anonymization.

Transaction numbers have various advantages. As a rather simple system, they require relatively small administrative capacities and are easy to handle for the voter.

The second and simplest way of identification is via the combination of a **(2) user name and password**. Every voter gets an individual user name and password, but the weakness of this simplistic approach is that secrets could be shared and, therefore, become known to unauthorized third parties.

A third and more permanent version is to use a signature or **(3) identity cards**. These chip cards require a card reader to enable the identification of individual voters. Identity cards can and should be equipped with digital signature functionality. This method is among the most secure ways of personal identification and is more reliable than any other currently available system. The most prominent issues of the procedure are the need for a strong, reliable software system and problems with the handling of cards. The use of passwords, card readers, different software front-end interfaces and digital signatures can be challenging for the inexperienced user.

Some countries have equipped their citizens with such cards (Maaten, 2004), and in Austria, the smart cards are linked to the existing population registers (Leitold et al., 2002). For others, such solutions were (i) too costly, (ii) delayed due to data protection concerns (Reichl et al., 2005) or (iii) delayed for a long time due to lack of national certification providers (Schweizer Bundesrat, 2007). In such cases, one-time passwords (transaction authorization numbers – TANs) were used, which resulted in high costs for printing and distribution of voting cards for each election (Braun, 2004). However, the

increased level of security came at the price of usability. While TANs are easily used by voters, smart cards can require high level of transaction costs to issue them as well as prove a high barrier to participation, which is hard to overcome.

For the successful conduction of any election, it is essential to only allow voting by persons who fulfill the eligibility criteria. It is also of paramount importance that the participating person is really the person who he or she claims to be.

4.4 Vote Secrecy and Anonymity

Ensuring the freedom of the voter to cast a ballot of his/her choice requires that it remain impossible to link a voter and his/her vote – both at the time of casting the vote as well as in the future. Many algorithms have been proposed in the past 30 years, all of which hide either the vote or the voter by cryptographic and/or organizational means. For an overview of different available algorithms, see Paulsen (2011) and Sampigethaya and Poovendran (2006).

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

The importance of the anonymization process is based on the difficulty of protecting electronic data in the long term. Depending on the identification method, the different phases of the election process may also be of importance. In the case of transaction numbers, for example, the rest of the paper should also be anonymous. If personalized, which might be helpful for a smooth organization, the personalization should only be printed or written on the paper after the protective layer of the scratch field protects the code below. This aspect is particularly linked to the randomized token system described below, as it can be designed in a very similar manner.

The first approach is to hand out randomized **(1) tokens** that the voters use to interact with the machines. The tokens should be handed out immediately before the election to prevent a third party from seeing the particular number and, thus, identifying the vote within the computer system. The tokens should also be collected again directly after the ballot is cast due to the same reasons.

Another approach would consist of a hardware-based solution. In the case of **(2) stand-alone voting machines,** this procedure is possible. The voter either does not enter credentials at all, or the source code could provide a separation within the data storage mechanism. In this manner, it is not possible to identify an individual vote without having the code and having access to both data storages. The approach of not entering credentials at all is a very simple solution, but it requires that an external solution is the organization of the election process itself. A voter must not be able to vote multiple times while at the station.

The currently most promising software-based solution is the **(3) cryptographic** solution. Many different forms of cryptographic solutions are possible using hardware modules, one of which is also used in the Estonian Internet elections—that is, the double-envelop method. The concept is simple but particularly promising because it imitates the postal voting process. One envelope with the identification contains another envelope that is anonymous. This anonymous envelope contains the vote and is then stored in a database with only this information. More information on how to treat the data in the long term can be found in the data protection decision module. Other proposals include using blind signatures, such as proposed in Kofler et al. (2003).

The most successful form of supporting free vote casting is allowing the voter to cast a vote more than once while ensuring that only the last vote counts (Volkamer and Grimm, 2006). However, this requires changing legal regulations, which, for example, in the Austrian case described in the previous chapter, was not possible.

4.5 Observation and Verifiability

In the municipal elections on May 7, 1989, the former German Democratic Republic (GDR) organized for the last time. The electoral system in use did not follow full democratic principles, but it was rather an administrative process where the goal of a polling stations election administration was to have the highest possible voter turnout and the highest approval rating for the unified party list. Actually, the voters also had no real choice: they could only take the ballot paper and put it into the ballot box, but there was only one way to make a real choice by invalidating all candidates on the ballot paper. As an example, civil society wanted to show that they were not satisfied with the ruling party by invalidating as many ballot papers as possible. Also, the voters were allowed to stay in the polling station to conduct a domestic election observation activity. Therefore, they stayed and counted the number of invalidated votes. The election authorities, however, did not report the correct number of invalidated votes (they reported rather ameliorated numbers), and the voters in turn demonstrated a month later in what was known as the election fraud demonstrations. These demonstrations proved how corrupt the system was.

This experience was a leading motive when the German Constitutional Court had to assess the appeal of a citizen against the 2005 *Bundestag* elections finally in March of 2009. Its ruling was a bit surprising but was of revolutionary nature: it ruled that voting machines – without the possibility for voters to count the votes without prior knowledge ("laymen") – were to be considered unconstitutional (and thereby demanded that voter-verifiable paper audit trails would have to be introduced) and that ended the story of E-Voting in Germany (Federal Constitutional Court, 2009).

Verifiability. Elections are generally considered to be one of the essential elements of modern-day democracy in order to establish "the rule by the people." The procedures by which elections are held have evolved considerably over time and differ depending largely on the context in which they take place and the available technology. Over time, many different methods have been used, including casting votes by shouting, a show of hands, swords, stones, wax tablets, etc. Today, the predominant form of casting votes worldwide in order to participate in elections is to fill out a paper ballot (see also Krimmer

[2012]). Internationally accepted norms depicting the voting process such as the Int. Covenant on Civil and Political Rights (United Nations, 1966) or the Copenhagen Document (OSCE, 1990) are used to establish what constitutes a democratic election. While these do not mention a preference for a particular form of casting a vote, it is clear that they have been developed and written with the paper-based voting process in mind.

The evolution of more-sophisticated voting technology than the paper ballot originated in the mid-19th century. This period saw the discussion of mechanical vote-casting devices, which was followed by proposals for electrified voting machines for parliaments. The U.S. can be considered the forerunner in adopting various forms of mechanical and electr(on)ic vote-casting and counting devices, including pull-lever machines, punch-card systems, direct-recording E-Voting machines or ballot scanners (Jones, 2003). Their adoption flourished due to the decentralized nature of the U.S. election administration and their decision-making processes (Harris, 1934).

All of these voting technologies have one inherent problem in common: The process from casting votes to counting votes is pretty much unobservable, due to the need to keep the voters' choices secret as well as the problem that one cannot touch bits and bytes (Lenarčič, 2010). Despite some critical voices (Saltman, 1975, 1988), these technologies were nevertheless considered safe for a long time.

The U.S. presidential elections of 2000, particularly in the state of Florida, changed this picture considerably. In the close presidential race between George W. Bush and Al Gore, the high failure rate of punch-card systems combined with the lack of a robust legal framework led to problems in trying to determine the "original voter intent" and a delayed determination of the election's outcome. Not only did this lead to a decline in the public's confidence in voting technology but also in the validity of calling the U.S. the "greatest democracy on Earth." Contrary to expectations, the U.S. invested even more heavily in voting technology, believing that the source of the problem was the choice of the wrong voting technology instead of a complete overhaul of the way the election administration, legal framework and voting technology interact. (Saltman, 2006)

This debacle, however, provided impetus to cryptographic researchers who since the early 1980s had been trying to realize fully E-Voting processes (Chaum, 1981, 1982). With computer systems, the sharing of power is difficult to implement. Early on, proposals included functionalities to allow for the public to check whether the election administration reported the results honestly and did not manipulate the elections. In paper-based elections, this can be verified by recounting the ballots. In e-elections, recounting the ballots does not necessarily result in greater confidence in the results as long as the system being utilized for the count does not use a programming system that is different from the original tool. Hence, there was a need for a different method to verify the election administrators and their honest reporting of election results. Subsequently, the concept of verification by individual voters and the general public was born (Benaloh, 1987, Schoenmakers, 1999, 1998).

As one of the first examples, the OSCE/ODIHR took up this development and defined "verifiability on an individual basis [… where] voters are provided with possibilities to verify that their vote was cast as intended, stored as cast, and (ideally) counted as recorded." On a universal (public) level, a voting technology with verifiability "provide[s] means for an independent third party to establish that the result of an election was reported honestly and without manipulation through either manual or mathematical checks" (OSCE/ODIHR, 2013).

With the transformation of transactions in the private and public sector through the general availability of the Internet in the 1990s, it seemed only a matter of time until elections would also be held via the Internet. A real race had begun to see which country would be the first to offer Internet voting (I-voting) to all of its voters (Kubicek et al., 2002). Despite promising initial efforts in the U.S. (Gibson, 2001) and Germany (Otten, 2001), it was Estonia that succeeded with a rather simple system in 2005 (Drechsler and Madise, 2004, Madise and Martens, 2006). However, only a small number of countries followed suit to offer I-voting for first-order elections, including the Netherlands, France, Switzerland and Norway (Krimmer and Kripp, 2009). Furthermore, most of the algorithms used were rather simplistic in their design and did not offer any possibility for voters to verify their votes (Krimmer et al., 2007).

The 2009 verdict of the German Constitutional Court changed the public view on E-Voting machines when the court decided that it must be possible for voters to ascertain for themselves without "prior knowledge" that election results had been reported honestly and that their votes had been entered in the results (Federal and Constitutional Court, 2009). This led the project managers of the Norwegian I-voting project to look for solutions to this problem, and during their procurement process, a verifiable I-voting protocol was proposed by researchers from Estonia (Ansper et al., 2009). The Norwegian elections in 2011 can be considered the first use of verifiability in Europe (OSCE/ODIHR, 2012).

In the same year as the first use of verifiability, an Estonian student managed to program a Trojan horse that would cast a different vote than the one intended by the voter in the 2011 Riigikogu elections. He consequently filed a complaint, which was eventually turned down by the Estonian Constitutional Court (Vinkel, 2012). This incident led to an electoral reform process where it was decided to introduce individual verifiability for upcoming elections where I-voting is offered (Vinkel, 2012). It was first used in the October 20, 2013 municipal elections in Estonia. Furthermore, Switzerland also announced the introduction of verifiability as a requirement for elections with full I-voting (Schweizer Bundesrat, 2013).

As such, some questions can be put forward with regards to verifiability. Thinking along the lines of the above regarding verifiability, some questions come into mind that can guide our future investigations on the topic:

1. What are the aims provided in the academic (mainly technical) literature for introducing the concept of 'verifiability' to existing election processes, including I-voting, and what purported use do the decision makers in practice plan to gain from introducing this concept?

2. How does verifiability actually work in practice, and what would a generic process model for individual and universal verifiability look like?

3. Does verifiability as a concept also have applicability for paper-based elections, i.e., without Internet voting?

On the basis of the existing academic literature, one can put forth the following working hypotheses:

1. Verifiability is a new concept that enables voters on an individual level to verify whether their votes were cast as they intended, recorded as cast and counted as recorded as well as on a universal level that no manipulations occurred, and the results were reported honestly.

2. Verifiability adds a new paradigm to the world of elections. It has the potential to add a considerable level of control for the general public over the conduct of elections.

3. Verifiability has been invented and defined by cryptographic researchers and hence needs to be translated into the reality of elections—for example, a legal framework must be defined for its use, it must be usable and understandable by voters so that it actually makes a difference, etc.

4. In line with the general trend to provide more accountability to the public, future elections must offer voters the potential to control the election administration. Therefore, in the future, verifiability will play an important part not only for election administration of I-voting but also of paper-based elections.

Forms of Verifiability. There are two general forms of verifiability possible: individual and universal verifiability. Both of these topics are critical for the trust that the electronic system can trigger within the voting community. A third form can be identified when combining both approaches.

(1) Individual verifiability is easier to achieve, because it means that the voter is able to control what was counted as intended. The problem with this process is that the vote must be cast-as-intended, transmitted-as-cast and counted-as-transmitted in order to enable a control for the individual. The process is made further problematic by the fact that the voter should be able to control the result without being able to prove the vote to anyone else in order to prevent vote buying and other forms of influencing the clients. One established form of dealing with these challenges is the "paper-audit-trail," which is a process of printing the results in anonymized form. The paper trail is then thrown in a ballot box to enable a control of the full result and to prevent voter fraud. If the printout shows that the vote was wrongly cast, the voter must have the ability to recast the vote. It is of vital importance that if a paper-audit trail is used, then the legislation states clearly if the ballot box with the paper trail or if the electronic results are seen as the primary results. The legislation should, thus, clearly state which of the two methods is used for the election count and which is used for the re-count in case of a challenge against the results of the election.

Another form of achieving individual verifiability is to hand out code sheets. The code sheet consists of two rows of codes. If the voter would like to verify the vote, he or she can introduce the appropriate code of the first code line. If the vote was counted correctly, the screen will show the matching code out of the second code line. If this is not the case, the voter needs to be able to recast the vote.

(2) Universal verifiability, on the other hand, is a much more complex issue. It is a cryptographic process with the target of providing mathematical proof that all votes were counted correctly without having a database that states who voted for what. Universal verifiability means that a person with sufficient technical knowledge can confirm that the election results match the votes cast and that the election was conducted accurately. Universal verifiability also enables a true recount, which individual verifiability does not provide.

(3) Full end-to-end verifiability means that both individual and universal verifiability are properly functioning. Although end-to-end systems are still rather rare, they are the objective of every election system, since only this step can show that there were no alterations and manipulations to the election results.

4.6 Control by the Electoral Committee

Traditional voting processes are organized by an election committee. Oftentimes, election administrators have a legal background and only limited technical experience. They often consult with technically experienced personnel or companies to conduct the electronic voting processes. Still, election committees should remain in full control of the conduct of the election. This becomes challenging when there is a need to allow the election commission to start, stop or interrupt the process. Most algorithmic solutions propose no technical means for this and therefore require organizational measures through regulation, such as detailed contractual relations with the vendor helping to implement this control element. As such, practice and theory agree on this. Some academic proposals even implement cases when the members of the electoral commission do not agree (Prosser et al., 2004a).

4.7 Evaluation and Certification

In addition to the necessity of overall trust- and transparency-enhancing measures, the correct functioning of the electronic voting software is in doubt if it is not verified before its actual use. Before evaluations can be performed, one has to translate legal requirements into functional and organizational requirements. Here, the technical part of the Council of Europe recommendation has made a fundamental contribution to the development of generally accepted technical requirements. Before such international technical standards can be used for certification, it was necessary to develop national approach in the case of Austria (A-SIT, 2009). Re-use of these techniques by others is limited, since they are either designed for specific existing systems, tied to national (electoral) legislation or too generic (Volkamer, 2009). Further guidance can also be found in Barrat et al. (2015).

4.8 Transparency

Paper-based voting processes are easy to understand and to follow. The use of electronic means presents the inherent problem that electronic bits and bytes cannot be seen. This results in a process that requires access to documentation of the actual proceeding of the operation of the electronic voting system as well as advanced mathematical and technical knowledge to understand the overall logic behind it. While early efforts introduced confirmation numbers that would allow voters to verify that their confirmation number is included in a public bulletin board, recent research proposes the use of end-to-end verifiability approaches (Ryan et al., 2009), which would allow the voter to verify whether his/her vote was cast as intended, recorded as cast as well as counted as recorded. The proposals use (mathematical) proofs to allow these checks. Practical experience with end-to-end verifiable systems is limited (only available in Norway and Estonia), and trust and transparency in the conduct of the electronic election remain pre-requisites. They may be enhanced through efforts like this, in particular, when considering universal approaches that could support observation efforts (Krimmer and Volkamer, 2006b, OSCE/ODIHR, 2013).

4.9 The Ballot Sheet

When considering electronic voting systems, two issues with ballots arise. First, the display of ballots can be cumbersome; second, the options available to the voter need to be discussed. The options in this chapter should always be observed under the condition that the electronic system profits from being as closely designed to the paper election as possible.

First, we will discuss the **ballot display**. Given a possibly large number of candidates, it might not be possible to display all candidates on one screen page. Solutions to this could be a **(1) scrollable list** of the candidates in the order established within the lists. Another method would be to display the ballot sheet as a **(2) reduced/compressed image** in size that allows the voter to increase the size in whatever part he/she wants. Another alternative for the design is a **(3) random order** process in which every candidate has an equal chance to be at the top of the list and every voter receives a different list. With this procedure, it is guaranteed that all candidates have the same chance of being elected.

Second, the **ballot options** should be discussed. Given that not all voting processes necessarily have to use electronic means, both voting channels (paper-based and electronic) need to be treated equal. Hence, all options available on paper ballots need to be provided in electronic ballots as well. Therefore, the electronic ballot sheets also need to have possibility with regards to **(1) abstention** and **(2) invalidity**, since the results and democratic rights of the voters would be influenced if these possibilities were not provided. An issue of interpretation is whether or not the election administration wishes to inform voters about potential **(3) over and under voting** before the vote is cast. A warning prevents unwanted invalidity while enabling voters to vote in any form they prefer.

4.10 Data Protection

The decision-module anonymization previously mentioned that data protection is a continuous issue that is essential to maintain trust in the entire system. Nevertheless, most experts recommend a physical destruction of the data when they are not needed anymore and the legal storage time has been reached. Determining this time in terms of fixed legal rules is important in order to prevent an unnecessary security breach.

For all methods, it is crucial to also think about the anonymity of the data after the election. Therefore, even though a randomized token was used during the election, the stored data should be additionally secured and encrypted to prevent a possible decoding. This accounts for the scenario where cryptographic technologies are used to protect the anonymity of the data as the calculation capacities constantly improve, which makes older encrypted data easier to solve for newer systems.

The protection of electronic data should be based on a legal framework with regards to data protection. Regulations should clearly state for how long and where the data should be stored. After that period, the data should be **(1) overwritten** or, as an even more secure yet drastic method, **(2) physically destroyed**. In the case of physical destruction, everything stored in memory that is associated with the election should be destroyed, which might not be feasible for numerous election designs, as it would include all computers and tablets involved.

The storage of data must be controlled at any given point in time. The same accounts for the storage of the rest of the electronic voting equipment before, during and after an election. The access to the machines and data needs to be controlled at any given point to prevent manipulation and fraud.

4.11 Organizational Context

For the introduction of electronic means, a number of organizational issues need to be considered, including sourcing, management, software review and public acceptance testing.

In-/Outsourcing. The setup and the use of electronic voting systems is a task that requires specialized skills on the network and the application level. Naturally, **(1) outsourcing** of either function may be considered as a real option, but it is also possible to develop the systems **(2) in-house**. Outsourcing requires considerable amount of training of the electoral commissions in order to retain control of the electoral process. Also, outsourcing requires time-consuming procurement but allows for using state-of-the art technology. For in-house development of an application, a considerable amount of know-how would need to be built up, which might be difficult to retain.

Source code publication. Whether or not the source code should be published is an important issue. **(1) Open source technology** can ensure trust with a new election system, since it allows independent verification of the contents and functions of the software but may require help/input by academics. **(2) Closed-source software** is the standard way for commercial solutions.[91]

Election management is also crucial for a smooth development. The management needs to decide of how to educate the election support staff and the commission members so that they can effectively run and observe the voting process. The legal aspects of what election commission members are allowed to access and what they do is also to be determined or interpreted by the electoral management. Control is also a crucial aspect, and the 'four-eyes' principle should be respected at all times during the entire electoral process. The principle states that at all times and during every process there must be at

[91] For further information, see Clouser et al. (2014).

least two people observing or handling the particular step in the election procedure without the need for help by third parties.

Public acceptance testing. For any changes in the election process, it is of fundamental importance that the voters recognize and support the changes. Trust in the new system can only be ensured if the electors agree to the development; if not, they must provide a way to test the system. Therefore, it is crucial that the role and formation of election bodies during the elections is discussed thoroughly.

External evaluation of the software. In order to establish trust with the given electronic system, it is useful to consider external evaluation of the system. It is therefore important to determine the requirements against which the system shall be evaluated against.[92]

Schedule. Election organization is not determined in a single day. There are three phases within any election process: The preparation, the election and the determination of the results. These three steps can be understood as a cycle where the first stage begins when the last stage ends. The introduction of technical support in all of these three stages is accompanied by risks and possibilities. Electronic counting – including the use of scanners or similar machines – covers the last phase of the electronic cycle, and electronic voting covers both the second and third phase of the elections. Both of these technologies lead to a loss in controllability for the average voter. Trust in the system and the administration must hence be ensured before the election process begins. Clear legislation that paves a way for clear procedures for all cases is an important aspect for these developments. Elections are ultimately cyclical, and administrations learn through every election, and changes must be adapted and accounted for in the preparation process for the next election. Usually, newly discussed changes to the election process are not made for the next election but for the following election.

[92] For further guidance, see Barrat et al. (2015).

The schedule is dominated at the preparation level. Training of the staff, feasibility studies and the evaluation of the systems takes up most of the time. The electronic system will benefit from **(1) holding a pilot in an election in the upcoming election** and an evaluation of that pilot with the effective introduction of E-Voting for the subsequent election.

An introduction at **(2) the next upcoming election** would be risky and lacks proper study and experience gathering.

4.12 Feasibility Study

The first central step in the procurement process is to extend and revise the feasibility study to be undertaken by the Secretariat. This extended study shall investigate the following issues.

Time. The time frame to the next election is short. Requirement Engineering, Procurement, Training and Deployment take time. We recommend that the Secretariat carefully considers all issues regarding time and lets this determination feed into the decision making process about which technology to procure.

Requirements. Based on the requirements we have outlined above in Section 5, the specific requirements for the voting solution to be used for the election shall be determined. Vote Integrity, Vote Secrecy and Verifiability are those that are indispensable. Any compromises among these three should be taken into account and documented with utmost care.

Operational Capacity. Running an election using electronic voting equipment will require qualified personal to configure, setup, and monitor the electronic voting technologies. Also, those who will act as election commission members will have to be trained to interact with the system. The allocation of resources is necessary well in advance. Plans must be made.

Budgets. Budgets must be made available for procurement, quality control, running the election and optionally for the secure storage of the technology, such as iPads or other hardware artifacts.

Building Blocks. All of the issues described in these building blocks should ideally be discussed and determined when conducting a feasibility study. It is clear that a study cannot cover all possibilities, but the effort needs to be genuine and as detailed as possible.

4.13 Summary

The identification and definition of building blocks greatly helps to discuss and design an electronic voting process before an actual election takes place. While these building blocks were based on Internet voting, they can easily be adapted to other voting technologies and applied in most contexts where such technology shall be introduced to an existing paper-based voting process. Discussing electoral reform is inherently difficult due to the political interests of the decision makers involved, and electronic voting makes it even more complicated. Having a clear agenda based on these building blocks should be helpful and should provide for a more educated and transparent discussion.

5 Conclusions

This thesis describes the development of remote electronic voting and has derived building blocks that can be used when designing future implementations. Clearly, what once seemed as merely a technical problem became a much more complex issue.

The work presented herein focused on the following questions:

1. How did Internet voting originate?

2. What were the significant moments associated with Internet voting in Austria?

3. What building blocks can be identified for developing future Internet voting systems within Austria and throughout the world?

First, Internet voting is part of a transformational movement regarding the widespread application of information and communication technologies. It is only logical that elections also apply electronic (remote) communication technologies. While early efforts were driven by the belief that elections could make easy use of the Internet, it was shown that while the principles must be interpreted and consequently applied in a different way, a number of principles (e.g., integrity, secrecy, transparency, accountability, public confidence) remain important. The need to have forms of decision making in electronic networks has been identified in its beginnings and received continuous attention throughout its further development. At the height of the excitement about the possibilities of the Internet, several countries tried to become the first to implement electronic voting systems, including Costa Rica, Bosnia Herzegovina, Germany and the United States, and Estonia succeeded in 2005. To date, Estonia is the only country that has introduced this form of voting without any preconditions or other limitations.

Second, in Austria the intentions to use ICT in elections used to be concentrated on parliamentary affairs. Then, the efforts around student elections in Germany sparked the wish to conduct Internet voting in Austria in 2000. In the years thereafter, considerable progress was made at WU Vienna University of Economics and Business, and therefore, the university can be considered the driver of the debate in the early 2000s. At the beginning, the technical solutions for the main problem of verifying the eligibility of voters and maintaining privacy was at the center of attention. Later, more sophisticated algorithms were developed, and functionalities like quota in election commissions were added.

The Federation of Student elections in 2009 was a remarkable event that provided a great deal of experience for how heated and divided the political debate around the topic could become. This debate continued after the elections were held in May 2009, which suffered from the intense debate and consequential organizational shortcomings. Furthermore, the experiences showed that accurate legal regulations are needed, which not only show the interaction with the constitutional legal texts but also demonstrate how to give accountability to a remote electronic voting channel through legal means. International standards were a first step, but regulations based on actual experience in pilot implementations were especially important as well. This practical knowledge also shows that sophisticated algorithms are not always the key to success. Rather, several key implementations make use of very basic technical means to realize the tasks given by law. One should not forget about the voters. They not only need to use such systems, but they also need to understand the processes in order to build their trust with the systems. The Constitutional Court ruling that lifted the results of the election and ruled that the respective ordinance was not in line with the requirements of the law put high requirements and thereby barriers for offering Internet voting channels in future elections. While the election administration system, which was a pre-requisite for the Internet voting system, was discontinued in the election thereafter, it returned in recent elections where postal voting had to be offered.

On the basis of these experiences, it was possible to derive a set of twelve building blocks related to electronic voting systems. These building blocks include simple design decisions, such as the form of electronic voting, adaptations of the legal base, the technical means for identification and secrecy, observation, control functions for the electoral commission, evaluation processes, transparency functions, ballot sheet designs, controlling the organizational context, and the provision of options for planning and the implementation. This framework therefore facilitates and eases the generation of feasibility studies and other analyses and decision making ahead of using Internet voting in an election. With little adaption it can also be used for the use of other voting technologies.

This work utilizes theoretical work and knowledge gained in the areas of adaptations of legal texts. Through a literature review, this work provides information for how to implement identification and anonymity functions in remote electronic voting as well as for how to test and certify systems and identify areas that require transparent procedures. The findings also show that the implementation of remote electronic voting is a complex topic. It requires trust in the election administration; otherwise, suspicion will arise with the introduction of more technology in an election process. Remote electronic voting is one of the most challenging IT projects. Not only does the requirement for secrecy of a vote rule out many approaches towards IT security in the Internet, but elections themselves are inherently special projects: they must take place on a fixed date and time regardless of whether the system is functional.

6 Acknowledgements

Writing a PhD thesis requires passion[93], but it also requires an encouraging environment. I would like to thank several people without whom this work might never have been accomplished.

First, I thank Andreas Mild who provided for a safe harbor, and Alfred Taudes who was essential from the beginning of this thesis to this very end. Further thanks go to Peter Filzmaier for his support.

Second, I want to thank all of the colleagues at the Department for Production Management, who I have worked with over the years, including Alexander Prosser, Robert Kofler and Martin-Karl Unger for discussing, deliberating, creating and considering the many ideas we had during the time of the E-Voting.AT project.

Third, I would like to thank all of my colleagues in academia dealing with the topic of e-voting, e-participation and e-democracy, in particular, Melanie Volkamer, Nadja Braun Binder, Wolfgang Drechsler, Gregor Wenda, Robert Stein, Maria Wimmer, Norbert Kersting, Andreas Ehringfeld, Markus Traxl, and Priit Vinkel. Also, I want to thank the team behind the e-voting conferences in Schloss Hofen over all those years, including Gisela Traxler, Katharina Kozlik, Dirk-Hinnerk Fischer, Manuela Troy and Marcella Künzler. Also I would like to thank former minister Jürgen Weiß for facilitating the connection with the Schloss. In addition, I want to thank all of the participants from all over the world who helped me to gain a better understanding of the issues at hand.

I am also deeply thankful for the support by Thomas Buchsbaum in various capacities throughout all the years.

[93] A better term would be its corresponding word in German – *Leidenschaft* ("creating pain").

Furthermore, I want to thank my friends in Vienna, Warsaw, Tallinn and all around the world who shared my excitement, musing and suffering and who were there when there seemed to be no end to this ever-winding road. In particular, I would like to thank Werner Weingraber and Alexander Szlezak for having the gratitude and patience to listen and share a beer when I was in need.

Lastly, my gratitude goes to my wife Maren and daughter Pauline as well as my parents Otto and Verena and my brothers Peter and Paul, including their families, for motivating, understanding and never losing their faith in me.

This thesis belongs to you all.

7 Bibliography

All links were verified on September 1, 2017.

2010. Karl, B.: "E-Voting wird 2011 nicht mehr eingesetzt". *Der Standard*, 2010-04-02.

A-SIT 2009. Bescheinigung nach § 34 Abs. 6 HSG 1998. A-SIT-1.078. Wien: A-SIT.

Alton-Scheidl, R., Schmutzer, R., Sint, P. P. and Tscherteu, G. 1997. *Voting, Rating, Annotation. Web4Groups and other projects: approaches and first experiences,* Vienna, OCG.

Alvarez, R. M. and Hall, T. 2004. *Point, Click, & Vote,* Washington, D.C., Brookings Institution Press.

Amt für Statistik und Wahlen der Stadt Dortmund. 1961. Stadtvertreterwahl am 19. März 1961. *Dortmunder Statistik*.

Androsch, M. 2011. *Development of an E-voting Database - Enhancement in Contribution, Usability, User Management, Security, Performance, and Statistics*. Master Thesis, WU Vienna University of Economics and Business.

Ansper, A., Heiberg, S., Lipmaa, H., Øverland, T. A. and Van Laenen, F. 2009. Security and Trust for the Norwegian E-Voting Pilot Project E-valg 2011. *Identity and Privacy in the Internet Age*. Berlin: Springer.

Arami, M., Koller, M. and Krimmer, R. 2004. User Acceptance of Multifunctional Smart Cards. *ECIS 2004 Proceedings*.

Arbeitsgemeinschaft Uservertreter Wahl. 2000. *ARGE UV Wahl - Wahlinformationen*. Available: http://web.archive.org/web/20000510104840/http://uv-wahl.chello.or.at/.

Balthasar, A. and Prosser, A. 2012. E-Voting in der „sonstigen Selbstverwaltung" – Anmerkungen zum Beschluss des VfGH vom 30. Juni 2011, B 1149, und zum Erkenntnis des VfGH vom 13. Dezember 2011, V 85–96. *Journal für Rechtspolitik,* 20**,** 47-85.

Barrat, J., Bolo, E., Bravo, A., Krimmer, R., Neumann, S., Parent, A. A., Schürmann, C., Volkamer, M. and Wolf, P. 2015. *Certification of ICTs in Elections,* Stockholm, International IDEA Group Publishing.

Becker, T. 1981. Teledemocracy: Bringing power back to the people. *The futurist,* 15**,** 6-9.

Benaloh, J. 1987. *Verifiable secret-ballot elections*. PhD thesis, Yale University.

Bertorello, L. 2001. *The Electronic Democracy European Network (EDEN)*. Available: https://web.archive.org/web/20020328001110/http://www.edentool.org/.

BMBWK. 2000. Novellen zum UOG und zum Hochschülerschaftsgesetz im Ministerrat. *OTS*, 2000-11-29.

Botz, M. D. 2008. *Unterstützung von Wahlen in Österreich durch Informations- und Kommunikationstechnologie mit besonderer Berücksichtigung von E-Voting*. Vienna University of Economics and Business Administration.

Brandl, H., Schindler, L. and Czaby, V. 2007. Bedenken der ÖH Bundesvertretung zu E-Voting bei Hochschülerinnen- und Hochschülerschaftswahlen. Österreichische Hochschülerinnen- und Hochschülerschaft.

Braun, N. 2004. E-Voting: Switzerland's Projects and their Legal Framework – in a European Context. *In:* Prosser, A. and Krimmer, R. (eds.) *Electronic Voting in Europe: Technology, Law, Politics and Society*. GI.

Braun, N. 2006. *Stimmgeheimnis. Eine rechtsvergleichende und rechtshistorische Untersuchung unter Einbezug des geltenden Rechts,* Bern, Stämpfli Verlag.

Braun, N., Buchsbaum, T. M., Krimmer, R. and Prosser, A. 2004. *E-Democracy und E-Voting für Auslandsbürger,* Wien, Working Papers on Information Processing and Information Management.

Brenn, C. and Posch, R. 2000. *Signaturverordnung,* Wien, Manz.

Bright, R. D. 1979. Prestel The World's First Public Viewdata Service. *IEEE Transactions on Consumer Electronics,* CE-25**,** 251-255.

Brinek, G., Graf, M. and Niederwieser, E. 2001. Abänderungsantrag zum Bericht des Ausschusses für Wissenschaft und Forschung über die Regierungsvorlage 394 d.B. zum Bundesgesetz, mit dem das Hochschülerschaftsgesetz 1998 geändert wird (414 d.B.).

Buchsbaum, T. 2005. *Questions and challenges of e-voting, and attempts to find answers and solutions* BMEIA.

Bundeskanzleramt 2000. Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins "Zentrum für sichere Informationstechnologie - Austria (A-SIT)" als Bestätigungsstelle.

BMBWK 2001. Hochschülerschaftswahlordnung 2001 (HSWO 2001). Vienna.

Bundesministerium Für Inneres 2004. Abschlussbericht zur Arbeitsgruppe "E-Voting". Vienna.

Bundeswahlgeräteverordnung 1999. Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland vom 3. September 1975 (BGBl. I S. 2459), die zuletzt durch Artikel 1 der Verordnung vom 20. April 1999 (BGBl. I S. 749) geändert worden ist.

Carter, L. and Bélanger, F. 2005. The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information systems journal,* 15**,** 5-25.

Chaum, D. 1981. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM,* 24**,** 84-88.

Chaum, D. Blind Signatures for Untraceable Payments. Advances in Cryptology: Proceedings of CRYPTO '82, 1982 Santa Barbara, California, USA. 199-203.

Clouser, M., Krimmer, R., Nore, H., Schürmann, C. and Wolf, P. 2014. *The Use of Open Source Technology in Election Administration*, International IDEA.

Common Criteria Project. 2012. *Common Criteria for Information Technology Security Evaluation, v3.1 Release 4*. Available: http://www.commoncriteriaportal.org/cc/.

Cooper, H. and Hedges, L. V. 1994. *The Handbook of Research Synthesis,* New York, Russel Sage Found.

Council Of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*. Available: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

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

Council Of Europe. 2011a. *Guidelines of the Committee of Ministers of the CoE on Certification of E-voting Systems (2011)*. Available: https://web.archive.org/web/20131108005558/http://www.coe.int:80/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf.

Council Of Europe. 2011b. *Guidelines of the Committee of Ministers of the CoE on Transparency of E-enabled Elections (2011)*. Available: https://web.archive.org/web/20131108005738/http://www.coe.int:80/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf .

Cranor, L. F. and Cytron, R. K. Sensus: A security-conscious electronic polling system for the Internet. HICSS, 1997. IEEE, 561-570.

Dahl, R. A. 1956. *A Preface to Democratic Theory,* Chicago, University of Chicago Pres.

Das Schweizer Parlament. 2014. *Parlamentswörterbuch - Stimmabgabe im Nationalrat*.

Datakom Austria Gmbh 2001. Prototyp für die weltweit erste rechtsverbindliche Online-Wahl.

Davies, D. W., Bartlett, K. A., Scantlebury, R. A. and Wilkinson, P. T. A digital communication network for computers giving rapid response at remote terminals. Proceedings of the first ACM symposium on Operating System Principles, 1967. ACM, 2.1-2.17.

Davies, L. 2000. Digital Democracy. *IBM Government Journal*.

De Carlo, A. 2007. Wirtschaftskammer Wahlen 2005. *Electronic Democracy 2007 (EDEM07)*. Vienna: OCG.

Dickinger, A., Prosser, A. and Krimmer, R. 2003. Studierende und Elektronische Wahlen: Eine Analyse. *In:* Prosser, A. And Krimmer, R. (eds.) *E-Democracy: Technology, Law and Politics*. Vienna: OCG Verlag.

Direction Centrale De La Sécurité Des Systèmes D'information 2006. Profil de Protection Machine à voter (PP-CIVIS).

Drechsler, W. and Madise, Ü. 2004. Electronic Voting in Estonia. *In:* Kersting, N. and Baldersheim, H. (eds.) *Electronic Voting and Democracy: A Comparative Analysis*. London: Palgrave.

Eriksson, A. 2002. *Handbook for European Union Election Observation Missions,* Stockholm, Sida.

Estonian Election Committee. 2004. *General Description of the E-Voting System*. Tallinn. Available: http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf.

Estonian National Electoral Committee. 2007. *Parliamentary Elections*. Available: http://www.vvk.ee/r07/paeveng.stm.

Etzioni, A. 1972. Minerva: An Electronic Town Hall. *Policy Sciences,* 3**,** 457-474.

EU. 2000. *The EU Cybervote Project* .

EU Election Observation Mission To Venezuela. 2006. *Final Report of the December 4th 2005 Election in Venezuela*. Caracas. Available: **Fehler! Linkverweis ungültig.**.

Faisst, M. 2000. *Stellungnahme 9/SN-45/ME vom 15. Mai von der Österreichische Hochschülerschaft zu dem Ministerialentwurf betreffend Bundesgesetz, mit dem das Hochschülerschaftsgesetz 1998 geändert wird*.

Fakultätsvertretung Informatik an der HTU Graz. 2006. *Resolution zum Thema E-Voting*.

Federal Constitutional Court. 2009. *Judgment of the Second Senate of 3 March 2009 on Voting Computers*. https://web.archive.org/web/20130514042655/http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html.

Fernandes, N. C., Moreira, M. D., Moraes, I. M., Ferraz, L. H. G., Couto, R. S., Carvalho, H. E., Campista, M. E. M., Costa, L. H. M. and Duarte, O. C. M. 2011. Virtual networks: Isolation, performance, and trends. *Annals of telecommunications-annales des télécommunications,* 66**,** 339-355.

Fettke, P. 2006. State-of-the-Art des State-of-the-Art. Eine Untersuchung der Forschungsmethode "Review" innerhalb der Wirtschaftsinformatik. *Wirtschaftsinformatik,* 48**,** 257-266.

Fiedler, F. 2004-07-29 2004. *RE: E-Voting im Verfassungskonvent*. Type to Holoubek, M., Prosser, A., Heindl, P. and Krimmer, R.

Fiedler, F., Böhmdorfer, D., Fischer, H., Glawischnig, E., Kahr, C., Khol, A., Kostelka, P., Orthner, A. and Scheibner, H. 2005. Bericht des Österreich-Konvents. Vienna.

Forschungsgruppe Internetwahlen 2000. Zweiter Zwischenbericht zum Projekt 'Strategische Initiative: Wahlen im Internet' nach Abschluss der Wahlen zum Studierendenparlament der UOS am 2. Februar 2000. Osnabrück: Universität Osnabrück.

Fujioka, A., Okamoto, T. and Ohta, K. 1993. A Practical Secret Voting Scheme for Large Scale Elections. *Advances in Cryptology - AUSCRYPT92*. Berlin: Springer.

Fuller, R. B. 1963. No More Secondhand God (late Night, April 9, 1940). *No More Secondhand God - and other writings*. 4 ed. Carbondale: Southern Illinois University Press.

GaletsaS, A. 2001. Presentation: EU Research Projects on e-Democracy. Brussels: European Commission.

Gibson, R. K. 2001. Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary. *Political Science Quarterly,* 116**,** 561–583.

Goby, B. and Weichsel, H. 2012. Das E-Voting-Erkenntnis des VfGH: gesetzwidrige Ausgestaltung der ÖH-Wahlordnung. *Zeitschrift für Hochschulrecht, Hochschulmanagement und Hochschulpolitik: zfhr,* 11**,** 118-125.

Göpfrich, H. R. 1985. Konzept für die BTX-Unterstützte Organisation und Administration der Lehre an Universitätsinstituten. *In:* HANSEN, H.-R. (ed.) *GI/OCG/ÖGI-Jahrestagung 1985. Wirtschaftsuniversität Wien Übersichtsbeiträge und Fachgespräche zu den Themenschwerpunkten Softwaretechnologie/Standardsoftware/Büroautomation/Bildschirmtext*. Springer.

Grabenwarter, C. 2004a. Briefwahl und E-Voting: Rechtsvergleichende Aspekte und europarechtliche Rahmenbedingungen. *Journal für Rechtspolitik,* 12**,** 70-77.

Grabenwarter, C. 2004b. *Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe*. Available: https://web.archive.org/web/20130110194312/http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.pdf.

Grimm, R. 2006. *RE: Implementierungsschwächen im Wahltest WU Wien und Wiener Zeitung*. E-Mail from 2006-10-20.

Grimm, R., Krimmer, R., Meissne, N., Reinhard, K., Volkamer, M., Weinand, M. and Helbach, J. 2006. Security requirements for non-political internet voting. *Electronic Voting 2006*. GI LNI.

Gronke, P., Galanes-Rosenbaum, E., Miller, P. A. and Toffey, D. 2008. Convenience Voting. *Annual Review of Political Science***,** 437-455.

Häder, M. 2009. *Delphi-Befragungen: Ein Arbeitsbuch*, Springer.

Hahn, J. 2007. E-Voting bei den nächsten ÖH-Wahlen möglich. Available: http://www.ots.at/presseaussendung/OTS_20071029_OTS0130/

Hantsch, N. 2006. Gut gewählt: WKO wickelt Kammerwahlen auf Basis .NET ab.

Harris, J. P. 1934. *Election Administration in the United States,* Washington, Brookings Institution Press.

Hassler, V. 1995. *Aspects of Group Communications Security*. Dissertation, Technische Universität Graz.

Hassler, V. and Posch, R. 1995. *A LAN voting protocol,* Graz, dbv-Verlag.

Haus der Abgeordneten des Österreichischen Reichsrathes. 1880. *Stenographisches Protokoll der 41. Sitzung der IX. Session vom 29. Januar*. Kaiserlich-königliche Hof- und Staatsdruckerei.

Hauser, M. 2009. *Systemabsturz bei E-Voting Testwahl. Presseaussendung der Hochschülerschaft an der TU Graz*. Available: http://www.ots.at/presseaussendung/OTS_20090319_OTS0110.

Heindl, P., Prosser, A. and Krimmer, R. 2003. Constitutional and technical requirements for democracy over the Internet: E-democracy. *In:* Traunmüller, R. (ed.) *Electronic Government*. Berlin: Springer-Verlag Berlin.

Held, D. 1999. The Transformation of Political Community: Rethinking Democracy in the Context of Globalization. *In:* Shapiro, I. and Hacker-Cordón, C. (eds.) *Democracy's Edges*. Cambridge + New York: Cambridge University Press.

Herzog, M. and Pensold, W. 2010. Die Anfänge des modernen Kommunikations- und Medienwesens. *In:* Rumpler, H. and Urbanitsch, P. (eds.) *Die Habsburgermonarchie 1848-1918: Soziale Strukturen*. Vienna: Verlag der österreichischen Akademie der Wissenschaften.

Hochschülerschaft an der Technischen Universität Graz 2005. Protokoll der zweiten ordentlichen Universitätsvertretungssitzung.

Hochschülerschaft an der Technischen Universität Graz 2006. Protokoll der 1. außerordentlichen Sitzung der Universitätsvertretung der Hochschülerinnen- und Hochschülerschaft an der Technischen Universität Graz im Wintersemester 2005/06 am 18.1.2006.

Holoubek, M., Prosser, A., Heindl, P. and Krimmer, R. 2003-06-26 2003. *RE: Behandlung der Einführung von E-Voting im Verfassungskonvent*. Letter to Fiedler, F.

Horster, P. and Michels, M. 1995. Der Vertrauensaspekt in elektronischen Wahlen. *In:* Horster, P. (ed.) *Trust Center*. Braunschweig: Vieweg.

IEEE Standards Coordinating Committee 38. 2005. *Voting Standards: Project 1583 - Voting Equipment Standard, Project 1622 - Electronic Data Interchange* https://web.archive.org/web/20070214034026/http://grouper.ieee.org:80/groups/scc38/index.htm.

Jefferson, D., Rubin, A. D., Simons, B. and Wagner, D. 2004. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).

Jones, D. W. 2003. *A Brief Illustrated History of Voting*. Available: https://www.cs.uiowa.edu/~jones/voting/pictures/

Karpen, U. 2005. *Elektronische Wahlen?,* Baden-Baden, Nomos Verlag.

Knoll, N. and Grossendorfer, E. 1996. Informationsgesellschaft. Bericht der Arbeitsgruppe der österreichischen Bundesregierung. Wien: Bundeskanzleramt.

Kofler, R. 2003. *Erstellung eines CMS unter Integration unterschiedlicher Informationssysteme mit OpenSource Tools: [am Beispiel der Webpage der Abteilung für Produktionsmanagement]*. Diplomarbeit, WU Vienna University of Economics and Business.

Kofler, R., Krimmer, R. and Prosser, A. 2003. Electronic voting: algorithmic and implementation issues. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (CD-ROM)*. IEEE.

Kofler, R., Krimmer, R., Prosser, A. and Unger, M. K. The role of digital signature cards in electronic voting. HICSS37, 2004. IEEE, 7 pp.

Konferenz Der Informatikfachschaften. 2006. *E-Voting Resolution der 34,5ten Konferenz der Informatikfachschaften vom 6. - 10. Dezember 2006*.

Kopf, K. and Haigermoser, H. 2001. Antrag betreffend ein Bundesgesetz, mit dem das Wirtschaftskammergesetz 1998 geändert wird. Nationalrat.

Krejcik, M. 2003a. *RE: E-mail from 11 June 2003*.

Krejcik, M. 2003b. *RE: E-mail from 23 June 2003*.

Krimmer, R. 2002. *e-Voting.at - Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen*. Diploma Thesis, Vienna University of Economics and Business Administration.

Krimmer, R. 2007. Durchführung der Hochschülerinnen-und Hochschülerschaftswahlen mittels elektronischer Abstimmungsverfahren: Machbarkeitsstudie. Vienna.

Krimmer, R. 2012. *The Evolution of E-voting: Why Voting Technology is Used and How it Affects Democracy*. Ph.D. Dissertation, Tallinn University of Technology.

Krimmer, R. and Kripp, M. 2009. Map of E-Voting Activities World-Wide. *Modern Democracy*, 8-9.

Krimmer, R., Kripp, M. and Mendez, F. 2009. *Indicative Guide No.1 to Recommendation Rec(2009) 1 of the Committee of Ministers to member states on e-democracy - Generic tools and policies for an electronic democracy*. Strasbourg: Council of Europe. Available: http://www.coe.int/t/dgap/democracy/Source/EDemocracy/CAHDE_IV/CAHDE indicative guide no 1 Eonly_23Feb09.pdf.

Krimmer, R. and Schuster, R. 2008. The E-Voting Readiness Index. *Electronic Voting 2008*. Bonn: GI LNI.

Krimmer, R. and Triessnig, S. 2007. *Database of E-Voting Uses Worldwide*. Available: https://web.archive.org/web/20140824073354/http://db.e-voting.cc:80/.

Krimmer, R., Triessnig, S. and Volkamer, M. 2007. The Development of Remote E-Voting Around the World: A Review of Roads and Directions. Vote-ID 2007, Springer.

Krimmer, R. and Volkamer, M. 2005. Bits or paper? Comparing remote electronic voting to postal voting. *EGOV (Workshops and Posters)*.

Krimmer, R. and Volkamer, M. 2006a. Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting. *Working Paper Series on Electronic Voting and Participation*. Vienna.

Krimmer, R. and Volkamer, M. 2006b. Observing Threats to Voters' Anonymity: Election Observation of Electronic Voting. *In:* Grönlund, Å., Scholl, H. J., Andersen, K. V. and Wimmer, M., eds. Electronic Government: Communication Proceedings, Krakow. Trauner Verlag, 43-50.

Kubicek, H., Karger, P. and Wind, M. 2002. Stilles Wettrennen. *Kommune21***,** 12-13.

Kuhn, F. 1984. Bildschirmtext: Einstieg in das Zeitalter der Neuen Informationstechnologien. *In:* Kuhn, F. and Schmitt, W. (eds.) *Einsam, überwacht und arbeitslos. Technokraten verdaten unser Leben*. Stuttgart: Die Grünen.

Lee, K., Lee, Y., Won, D. and Kim, S. 2010. Protection profile for secure E-voting systems. *Information Security, Practice and Experience*. Springer.

Leitold, H., Hollosi, A. and Posch, R. Security Architecture of the Austrian Citizen Card Concept. 2002. IEEE, 391-400.

Leitold, H., Posch, R. and Rössler, T. 2005. E-Voting: A Scalable Approach using XML and Hardware Security Modules. *2005 IEEE International Conference on e-Technology, e-Commerce and e-Service*. IEEE.

Lenarčič, J. 2010. *Address by Ambassador Janez Lenarčič, Director of the OSCE Office for Democratic Institutions and Human Rights (ODIHR), at the OSCE Chairmanship Expert Seminar on the 'Present State and Prospects of Application of Electronic Voting in the OSCE Participating States', in Vienna, Austria on 16 September 2010*. Vienna. Available: http://www.osce.org/odihr/71361.

Lijphart, A. 1998. The Problem of Low and Unequal Voter Turnout - and What We Can Do About It. *Institute for Advanced Studies: Political Science Serices*. Vienna: Institut für Höhere Studien (IHS).

Lindblad, J. and Suksi, M. 2005. *On the Evolution of International Election Norms: Global and European Perspectives,* Turku, Institute for Human Rights.

Maaten, E. 2004. Towards Remote E-Voting: Estonian Case. *In:* Prosser, A. and Krimmer, R. (eds.) *Electronic Voting in Europe Technology, Law, Politics and Society*. Bregenz: GI.

Madise, Ü. and Martens, T. 2006. E-Voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. *In:* Krimmer, R. (ed.) *Electronic Voting 2006*. Bonn: Gesellschaft für Informatik.

Mayer, M. 2008. *Electronic voting using the concept of the Austrian Citzen Card*. TU Graz.

Mayrhofer, C. A. 1863. *Petition betreffend der Annahme des von Carl Albert Mayrhofer erfundenen electro-magnetischen Abstimmungsapparates vom 17. September*.

Mayrhofer, C. A. 1880. Der Pneumatische Abstimmungs-Apparat für Parlamentarische Corporationen in seiner facultativen Verwendung bei den Sitzungen der beiden Hohen Häuser des Österreichischen Reichsrathes. Vienna.

Menzel, T. 2000. *Elektronische Signaturen,* Vienna, Verlag Österreich.

Menzel, T. 2001. E-Voting an österreichischen Hochschulen. *In:* Schweighofer, E., Menzel, T. and Kreuzbauer, G. (eds.) *Auf dem Weg zur ePerson*. Vienna: Verlag Österreich.

Menzel, T. and Stöger, K. 2003. Potential von E-Voting für zukünftige ÖH-Wahlen. *In:* Prosser, A. and Krimmer, R. (eds.) *E-Democracy: Technology, Law and Politics*. Vienna: OCG Verlag.

Mitrou, L., Gritzalis, D. A., Katsikas, S. and Quirchmayr, G. 2003. Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications. *In:* GRITZALIS, D. A. (ed.) *Secure Electronic Voting*. Boston + Dordrecht: Kluwer Academic Publishers.

Mote, C. D., Bloch, E., Cranor, L. F., Fountain, J. E., Herrnson, P., Jefferson, D., Mann, T., Miller, R., Powell, A. C. and Solop, F. 2001. Report of the National Workshop on Internet Voting: Issues and Research Agenda. Washington: Internet Policy Institute.

Nettig, W. 2000. Jourfixe von WK-Wien-Präsident Komm.-Rat Walter Nettig. Wien.

ÖH BUNDESVERTRETUNG. 2006. *Resolution E-Voting*.

ÖH WU 2001a. eVoting - Auf in die Zukunft!? *WUaktuell Issue 13, 11*.

ÖH WU 2001b. Klick ist chick! *WUaktuell Issue 11, 16*.

ÖH WU. 2004. *WU-Flash #169: Podiumsgespräche Bundespräsidentenwahl*. Issue from September 9, Vienna.

Oostveen, A.-M. and Van Den Besselaar, P. Security as Belief. User's Perceptions on the Security of E-Voting Systems. *In:* Prosser, A. and Krimmer, R., eds. ESF TED Workshop on Electronic Voting in Europe, 2004 Schloss Hofen/Bregenz. 73-82.

OSCE. 1990. *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE*. Available: http://www.osce.org/odihr/elections/14304.

OSCE Office For Democratic Institutions And Human Rights (ODIHR) 2005. *Election Observation Handbook*, OSCE.

OSCE/ODIHR. 2011. *Election Observation Mission to Kazakhstan*. Available: http://www.osce.org/odihr/elections/78714.

OSCE/ODIHR 2012. Election Expert Team Report on the 12 September 2011 Local Government Elections in Norway. Warsaw.

OSCE/ODIHR 2013. *Handbook for the Observation of New Voting Technologies,* Warsaw, OSCE/ODIHR.

Österreichische Hochschülerschaft. 2001. WU-Signaturkarte noch immer nicht zertifiziert: Evoting-Projekt daher für heuer gestorben. *OTS*, 2001-01-17.

Oswald, M. 2016. E- Voting in Austria: Legal Determination Matters *In:* DRIZA Maurer, A. and Barrat, J. (eds.) *E-Voting Case Law: A Comparative Analysis*. Routledge.

Otten, D. 2001. Wählen wie im Schlaraffenland? Erfahrungen der Forschungsgruppe Internetwahlen mit dem Internet als Wahlmedium. *In:* Holznagel, B., Grünwald, A. and Hanssma, A. (eds.) *Elektronische Demokratie: Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis*. Munich: Verlag C.H. Beck.

Panny, W., Prosser, A., Weingraber, W. and Klöckler, G. 2001. Vereinbarung zwischen der Hochschülerschaft an der Wirtschaftsuniversität Wien und dem Institut für Informationsverarbeitung und -wirtschaft der Wirtschaftsuniversität Wien über eine Partnerschaft zur Entwicklung eines System zur elektronischen Stimmabgabe (E-Voting-System).

Parycek, P., Sachs, M., Vikar, S. and Krimmer, R. Voting in E-participation: A Set of Requirements to Support Accountability and Trust by Electoral Committees. In: Krimmer, R. and Volkamer, M. (eds.). E-Vote-ID 2017, 2017. Springer.

Paulsen, C. 2011. *Sicherheit von Internetwahlen,* Hamburg, BoD, Books on Demand.

Plattform Anwender.Interessen.Gemeinschaft. 1999a. *Wahlergebnis*. Available: http://web.archive.org/web/20000425063758/http://plattform.telekabel.at/default.htm.

Plattform Anwender.Interessen.Gemeinschaft. 1999b. *Wahlmodus*. Available: http://web.archive.org/web/19991012194601/http://plattform.telekabel.at/diskussion.html.

Poier, K. 2013. E-Voting – mehr als nur ein einmaliger Flop? Die Entscheidungen des VfGH zur ÖH-Wahl 2009 und ihre Folgen für E-Voting in Österreich. *Jahrbuch Öffentliches Recht 2013*.

Prosser, A. 2002. *RE: E-voting*. E-mail to Tischler, H. from January, 18.

Prosser, A., Kofler, R. and Krimmer, R. 2002a. e-Voting.at: Vom e-Government zur e-Demokratie. *In:* Schweighofer, E., Menzel, T. and Kreuzbauer, G. (eds.) *IT in Recht und Staat*. Wien: Verlag Österreich.

Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. 2002b. e-Voting.at. Entwicklung eines Internet-basierten Wahlsystems für öffentliche Wahlen. *In:* Institute For Information Systems And Operations (ed.) *Working Papers on Information Systems, Information Business and Operations*. Vienna: WU Vienna University of Economics and Business.

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

Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. 2004a. *Implementation of Quorum-Based Decisions in an Election Committee,* Berlin, Heidelberg, Spinger.

Prosser, A., Kofler, R., Krimmer, R. and Unger, M. K. Security Assets in E-Voting. *In:* Prosser, A. and Krimmer, R., eds. Electronic Voting in Europe, 2004b Lochau/Bregenz. 171-180.

Prosser, A. and Krimmer, R. 2003a. Aktionsplan e-Voting.at: Aktionsplan für die Abhaltung von Wahlen über das Internet in Österreich. Vienna.

Prosser, A. and Krimmer, R. 2003b. *E-Democracy: Technologie, Recht und Politik,* Vienna, OCG.

Prosser, A. and Krimmer, R. 2004a. The Dimensions of Electronic Voting: Technology, Law, Politics and Society. *In:* Prosser, A. and Krimmer, R. (eds.) *Electronic Voting in Europe: Technology, Law, Politics and Society. Proceedings*. Bonn: Gesellschaft für Informatik.

Prosser, A. and Krimmer, R. 2004b. *Electronic Voting in Europe: Technology, Law, Politics and Society*, Gesellschaft für Informatik.

Prosser, A. and Müller-Török, R. Electronic Voting via the Internet. International Conference on Enterprise Information Systems ICEIS2001, 2001 Setùbal. 1061-1066.

Prosser, A. and Müller-Török, R. 2002. E-Democracy. Eine neue Qualität im demokratischen Entscheidungsprozess. *Wirtschaftsinformatik,* 44**,** 545-556.

Prosser, A. and Steininger, R. 2006. e-voting2006.at. An Electronic Voting Test Among Austrians Abroad. *Working Papers on Information Systems, Information Business and Operations, 02/2006*. WU Vienna University of Economics and Business.

Puiggali, J. and Morales-Rocha, V. 2007. Remote Voting Schemes: A Comparative Analysis. *In:* Alkassar, A. and Volkamer, M. (eds.) *E-Voting and Identity*. Springer Berlin / Heidelberg.

Reichl, H., Rossnage, A. and Müller, G. 2005. *Digitaler Personalausweis: Eine Machbarkeitsstudie*, Duv.

Remmert, M. Towards European Standards on Electronic Voting. *In:* Prosser, A. and Krimmer, R., eds. ESF TED Workshop on Electronic Voting in Europe, 2004 Schloss Hofen/Bregenz. 13-16.

Riera, A. and Cervelló, G. Experimentation On Secure Internet Voting In Spain. *In:* Prosser, A. and Krimmer, R., Eds. ESF TED Workshop on Electronic Voting in Europe, 2004 Schloss Hofen/Bregenz. 91-100.

Rössler, T. G. 2004a. E-Voting: A Survey and Introduction. Graz: Secure Information Technology Center - Austria (A-SIT).

Rössler, T. G. 2004b. *eVita - The e-Voting Project*. Available: https://web.archive.org/web/20040918194132/http://www.iaik.tugraz.at/aboutus/people/roessler/evita/index.php.

Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S. and Xia, Z. 2009. Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security,* 4.

Saltman, R. G. 1975. Effective Use of Computing Technology in Vote-Tallying. Washington D.C.: National Bureau of Standards.

Saltman, R. G. 1988. Accuracy, Integrity, and Security in Computerized Vote-Tallying. Washington D.C.: National Bureau of Standards.

Saltman, R. G. 1990. Vote-by-Phone - Promises and Pitfalls. Washington, D.C.: National Institute of Standards and Technology (NIST).

Saltman, R. G. 2006. *The History and Politics of Voting Technology. In the Quest of Integrity and Public Confidence,* New York, Palgrave Macmillan.

Sampigethaya, K. and Poovendran, R. 2006. A framework and taxonomy for comparison of electronic voting schemes. *Computers & Security,* 25**,** 137-153.

Sánchez Miñana, J. 2010. The International Adventures in Wireless Telegraphy of Franco-Austrian Engineer Victor Popp and their Epilogue in Spain. *In:* INKSTER, I. (ed.) *History of Technology*.

Schindler, P. 1999. *Datenhandbuch zur Geschichte des Deutschen Bundestages: 1949-1999; Eine Veröffentlichung der Wissenschaftlichen Dienste des Deutschen Bundestages,* Baden-Baden, Nomos.

Schlifni, M. 2000. *Electronic Voting Systems and Electronic Democracy: Participatory E-politics for a New Wave of Democracy*. Dissertation, Technische Universität Wien.

Schoenmakers, B. 1998. *18 May 1998: Report on the Dutch Internet election experiment*. Available: http://groups.yahoo.com/group/e-lection/message/18.

Schoenmakers, B. 1999. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. *Advances in Cryptology - Crypto99*. Springer-Verlag.

Schweizer Bundesrat 1975. Botschaft des Bundesrates an die Bundesversammlung zu einem Bundesgesetz über die politischen Rechte (9. April 1975). *Bundesblatt*. 127 ed. Bern.

Schweizer Bundesrat. 2007. *Anfrage 07.1031 zu 'Digitale Signatur'*. Available: http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20071031.

Schweizer Bundesrat 2013. Bericht des Bundesrates zu Vote électronique. Auswertung der Einführung von Vote électronique (2006–2012) und Grundlagen zur Weiterentwicklung. *Bundesblatt 2013*. Bern.

Slaton, C. D. L. 1990. *Televote: Expanding citizen participation in the quantum age*. PhD, University of Hawaii at Manoa.

Smith, A. D. and Clark, J. S. 2005. Revolutionising the voting process through online strategies. *Online Information Review,* 29**,** 513-530.

Stainer-Hämmerle, K. 2009. *Die Briefwahl im deutschen Sprachraum. Ein systematischer Ländervergleich unter Berücksichtigung der Wahlrechtsgrundsätze in Deutschland, Österreich, Liechtenstein und der Schweiz,* Saarbrücken, Saarbrücker Verlag für Rechtswissenschaften.

Stangl, S. 2000. Entwurf der Verordnung über die Wahl der Organe der Vertretung der Studierenden (Hochschülerschaftswahlordnung 2000 - HSWO 2000). Vienna: BMBWK.

Staveley, E. S. 1972. *Greek and Roman Voting and Elections,* Thames and Hudson, Cornell University Press.

Stein, R. 2004. Mag. Robert Stein im Interview im Rahmen der Auszählung der Schattenwahl parallel zur Bundespräsidentenwahl 2004. *In:* EBNER, T. (ed.) *MonitorTV*.

Suksi, M. 2005. Participation through Elections and Referendums. *In:* Lindblad, J. and Suksi, M. (eds.) *On the Evolution of International Election Norms: Global and European Perspectives*. Turku: Institute for Human Rights, Abo Akademi University.

Svensson, J. and Leenes, R. 2003. E-voting in Europe: Divergent democratic practice. *Information Polity,* 8**,** 3-15.

Telekom-Control-Kommission. 2001. *Bescheid A 7/2001-114*. Available: https://www.signatur.rtr.at/repository/tkk-accreditation-datakom-20011217-de.pdf.

Tischler, H. 2000. *Digitale Signatur "a-sign" von der Telekom Control genehmigt Datakom Austria erster offizieller Zertifizierungsanbieter in Österreich*. Available: http://www.ots.at/presseaussendung/OTS_20000127_OTS0047/digitale-signatur-a-sign-von-der-telekom-control-genehmigt-datakom-austria-erster-offizieller-zertifizierungsanbieter-in-oesterreich.

Tischler, H. 2002. Stand und Entwicklung des Einsatzes von Chipkarten in Österreich und an der WU. Available: http://wi.wu-wien.ac.at/studium/Abschnitt_2/LVA_ss02/IT_FK_SS02_Folien/WU-wien_020430_tischler.pdf.

Trechsel, A. 2007. Internet Voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe.

Turoff, M. and Hiltz, S. R. 1977. Development and Field Testing of an Electronic Information Exchange System: Final Report on the EIES Development Project. New Jersey Institute of Technology.

United Nations. 1966. *International Covenant on Civil and Political Rights*.

Vinkel, P. 2012. Presentation to the OSCE Human Dimension Committee on 27 March 2012 by the Estonian Delegation on Follow-up to the Recommendations contained in the 2011 OSCE/ODIHR Election Assessment Mission Report. Vienna.

Volkamer, M. 2009. *Evaluation of electronic voting: requirements and evaluation procedures to support responsible election authorities,* Berlin, Springer LNBIP.

Volkamer, M. and Grimm, R. 2006. Multiple Casts in Online Voting: Analyzing Chances. *In:* Krimmer, R. (ed.) *Electronic Voting 2006*. Bregenz: GI.

Volkamer, M. and Krimmer, R. 2006. Die Online-Wahl auf dem Weg zum Durchbruch. *Informatik Spektrum,* 29**,** 98-113.

Volkamer, M., Krimmer, R. and Soc, I. C. 2006. *Secrecy forever? Analysis of anonymity in Internet-based voting protocols*.

Vowe, G. and Wersig, G. 1983. Kabeldemokratie - Der Weg zur Informationskultur. *Aus Politik und Zeitgeschichte,* 45**,** 15-22.

Walch, D. 2006. *Deployment von Applets: Entwicklung eines Modells für eine benutzerfreundliche und breite Verteilung von Java Applets*. WU Vienna University of Economics and Business.

Weddeling, S., Volkamer, M., Paulsen, C., Mlynczak, K., Meletiadou, A., Meissner, N., Krimmer, R. and Helbach, J. 2008. Verifiability in Electronic Voting - An Interdisciplinary View. *Reduktion der Komplexität durch Recht und IT, IRIS '08*.

Wenda, G. and Krimmer, R. 2016. Towards an Update: The Council of Europe's Ad-hoc Committee of Experts on E-Voting (CAHVE) and its impact on International Organisations. IPSA Conference, Poznan.

Wenda, G. 2016. E-Voting in Austria: A National Case Study. Electoral Expert Special Edition 2016, 139-149. Available: http://www.roaep.ro/prezentare/wp-content/uploads/2016/08/Expert_Electoral_Ed_%20Speciala%202016.pdf

Wirtschaftsuniversität Wien. 1999. *WU Wien bekommt modernstes Universitätsverwaltungssystem Europas*. Available: http://www.ots.at/presseaussendung/OTS_19990907_OTS0241/wu-wien-bekommt-modernstes-universitaetsverwaltungssystem-europas-bild.

WU Zentrum Für Informatikdienste 1997. PowerCard. Erfahrungsbericht über die Einführung eines neuen Studienausweises auf Basis einer Multifunktions-Chipkarte. Ein Projekt des Zentrums für Informatikdienste der WU-Wien.

WU Zentrum Für Informatikdienste 1998. Sollspezifikation Projekt 2gether der Wirtschaftsuniversität Wien.

WU Zentrum Für Informatikdienste. 2005. *ZID-Newsletter vom 07.04.2005, Ausgabe 10*. Available: http://www.wu.ac.at/it/downloads/newsletter10_2005-04-07.pdf.

Zetsche, K. E. 1881. *Handbuch der elektrischen Telegraphie: Die elektrischen Telegraphen für besondere Zwecke,* Berlin, Springer.

Ziska, B. 2004. *Verfassungsrechtliche Rahmenbedingungen für E-Voting*. Available: http://www.rechtsprobleme.at/doks/ziska-e-voting.pdf.

Zissis, D. and Lekkas, D. 2011. Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly,* 28**,** 239-251.

Zittel, T. 2001. Electronic Democracy and Electronic Parliaments. *In:* Filzmaier, P. (ed.) *Internet und Demokratie: The State of Online Politics*. Innsbruck ; Wien: Studien-Verlag.