Secure Online Elections in Practice

Lucie Langer, Axel Schmidt, and Johannes Buchmann

Technische Universität Darmstadt
Department of Computer Science
Cryptography and Computeralgebra
Hochschulstraße 10, 64289 Darmstadt, Germany
{langer, axel, buchmann}@cdc.informatik.tu-darmstadt.de

Abstract. Current remote e-voting schemes aim at a number of security objectives. However, this is not enough for providing secure online elections in practice. Beyond a secure e-voting protocol, there are many organizational and technical security requirements that have to be satisfied by the operational environment in which the scheme is implemented. We have investigated four state-of-the-art e-voting protocols in order to identify the organizational and technical requirements which these protocols need to be met in order to work correctly. Satisfying these requirements is a costly task which reduces the potential advantages of e-voting considerably. We introduce the concept of a Voting Service Provider (VSP) which carries out electronic elections as a trusted third party and is responsible for satisfying the organizational and technical requirements. We show which measures the VSP takes to meet these requirements. To establish trust in the VSP we propose a Common Criteria evaluation and a legal framework. Following this approach, we show that the VSP enables secure, cost-effective, and thus feasible online elections.

Keywords: E-Voting, E-Government, Voting Service Provider, Certification Authority

1 Introduction

Remote e-voting is becoming more and more important in our mobile era. In 2007, Estonia was the first country to implement remote e-voting in parliamentary elections (cf. [11], [25]). Another example of a successful e-voting application is the election of the chairmanship of the German Informatics Society (*Gesellschaft für Informatik*, GI) which has been carried out electronically since 2004 using the POLYAS remote voting system [23]. In 2006, 4005 out of 4070 GI members cast their vote electronically over the internet (cf. [15]).

There are many more potential applications of e-voting, for example elections of a works council in a company. However, for e-voting to be widely used, it must be possible to implement secure e-voting systems with reasonable effort. A thorough analysis of the protocols [3], [20], [22], and [24] shows that in order for those protocols to run securely, the operational environment needs to meet a number of organizational and technical requirements, such as the existence of a public key infrastructure, private communication channels, or trusted system components. Modifying this environment in such a way that these requirements are met may be a very complex and costly task. This reduces the potential advantage of using an e-voting system considerably.

In this paper we solve this problem by introducing a Voting Service Provider (VSP). The VSP is a trusted third party which organizes an electronic election on behalf of the institution which holds the election. We show that the VSP can be made responsible for satisfying the majority of the organizational and technical security requirements that are not covered by the underlying protocols but have to be met in order for an e-voting system to work securely. The VSP releases its clients from setting up the operational environment accordingly, thereby making e-voting much more cost-effective. The VSP can be a separate unit within the organization where the election takes place. But to strengthen the effect of the VSP, we propose to make it an institution on its own that carries out electronic elections on behalf of other organizations and institutions.

The definition of a VSP is inspired by an analogous entity within a public key infrastructure: The Certification Authority (CA), a trusted third party that issues digital certificates. It is not sufficient for a CA to implement the necessary cryptographic protocols properly. A CA also needs to meet many organizational and technical requirements. The way each CA addresses and implements these requirements is usually described in the Certification Practice Statement (CPS) [8] of the CA. Examples for such requirements can be found in the European Directive for Electronic Signatures [13, Annex II], or in the regulations [33] for legal CAs in Germany. These also show that CAs permitted to issue qualified certificates operate under stringent organizational and legal conditions. Furthermore, they are usually observed by some independent authority. Similarly, we propose to establish a legal framework and an independent supervisory body for VSPs as well.

1.1 Related Work

Organizational and technical requirements for e-voting have been specified in several catalogues, of which we mention the leading ones from Europe and Germany: The Council of Europe has come up with a comprehensive set of standards on e-voting [10], including remote e-voting as well as voting machines. The catalogue is divided into three parts: Legal standards, operational standards referring to the organization and conduction of the election, and technical requirements addressing issues like accessibility, operation, and audit of the voting system. In Germany, the GI has developed a catalogue of requirements for online elections in non-governmental organizations [14]. Furthermore, since 2006, a Common Criteria Protection Profile for remote electronic elections has been developed under leadership of the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) [5]. Currently it is under certification, which is planned to be completed in a couple of months. First experiences can be found in [26].

Regarding the idea of a trusted VSP, to the best of our knowledge, there are no implementations so far which fully comply with our concept. Most e-voting systems either offer mere software solutions like Scytl [31] or they are out of our scope since they use paper ballots (e.g. [29]) or polling stations (e.g. [12]). The CyberVote project [1], a research programme funded by the European Commission, developed an internet voting software prototype. The software includes server and client components and allows voting using PCs, handheld devices or mobile phones. The project also considered legal aspects of e-voting software. The voting system POLYAS [23] matches our concept best in terms of carrying out electronic elections on behalf of the institution which hosts the election. POLYAS offers online elections for organizations and associations and has been used for the election of the GI chairmanship since 2004 [15]. The POLYAS voting software is to be evaluated against the Protection Profile [5]. We will show that our concept to establish trust in the VSP is more comprehensive.

1.2 Our contribution

Although the idea of outsourcing certain functions to a third party exists since the 1980s, it has not been fully applied to e-voting yet. Furthermore, while the requirements for e-voting have been laid down in several catalogues, a concept for satisfying these requirements while maintaining the usability of e-voting has not been provided. We give a solution to this problem by linking the security requirements to the concept of a service provider: We derive the motivation for establishing service providers for remote electronic elections from the organizational and technical requirements of current e-voting schemes. We show that the VSP can be made responsible for satisfying most of these requirements, thereby reducing effort and cost for the election host and making e-voting feasible in large scale. Focusing security demands on the VSP simplifies verification of e-voting security issues, but also increases the importance of trust in the VSP. We argue that it is in fact a trusted third party by providing sufficient measures to establish trust in the VSP.

We do not discuss which particular techniques the analyzed protocols use to achieve the security objectives of e-voting, e.g. anonymity or democracy. We also do not investigate the security of cryptographic algorithms employed in these protocols. We rather assume that the protocols and the cryprographic primitives used by them work securely as specified. Furthermore, we do not deal with security of the client platform which is a major issue on its own and out of the scope of this work.

The paper is organized as follows. In Section 2 we analyze four important e-voting protocols [3], [20], [22], [24] and identify major organizational and technical security requirements that need to be met in order for those protocols to work securely. In Section 3 we introduce the VSP. We show how the security requirements identified in Section 2 can be satisfied by the VSP. Section 4 gives an evaluation of our results, providing measures to establish trust in the VSP. In Section 5 we conclude the paper.

2 Organizational and technical security for e-voting

In order to enable secure electronic elections it is not sufficient to implement a secure e-voting protocol. To achieve the *security objectives* of e-voting (see below), all e-voting protocols need certain *security requirements* to be met, i.e. organizational and technical conditions that have to be satisfied by the environment in which the voting system is implemented. In this section we analyze the four e-voting protocols [3], [20], [22], [24] and identify the security requirements that those protocols need to be satisfied in order to work securely.

First we review the security objectives for e-voting following [27]. One of the most important security objectives for e-voting schemes is *privacy*: It must be impossible to associate a vote with the voter who cast it (*anonymity*), all ballots must remain secret until voting is completed (*fairness*), a voter must not be able to prove in which way she voted (*receipt-freeness*) and cannot be forced to abstain from voting or to vote in a particular way (*uncoercibility*). Another security objective is *accuracy*: Votes cannot be altered, duplicated or eliminated, all valid votes are counted correctly, and invalid votes are not counted. Of equal importance is *democracy*: Only eligible voters are permitted to cast their vote and only one vote per voter is accounted. In contrast to paper-based voting systems, most e-voting schemes are verifiable. *Individual verifiability* means that every voter can verify that her vote was accounted correctly. *Universal verifiability* is achieved if anyone is able to verify the correctness of the voting process and its results.

The e-voting protocols [3], [20], [22], and [24] achieve most of those security objectives. But to do so, they need several organizational and technical security requirements to be satisfied. We now describe these requirements, categorized in families. We also mention the related security objectives.

Trusted components (Tr_Comp). All four voting protocols that we have analyzed rely on trusted components. The security of the protocols is based on the fact that these components work securely as specified. The secure operation of the components is not enforced by the voting protocols. It is assumed to be guaranteed by the environment in which the voting protocol is implemented. [24] requires a *trustworthy administrator* who authorizes eligible voters. [22] assumes that an administrator does not collude with an adversary to issue an illegally modified randomizer device to a voter. [20] assumes that the *registration authority* is trustworthy and does not collude with an adversary. [3] requires a *trustworthy time stamp server* which allows voters to prove that they have cast their vote in time before the election terminated.

Of particular importance is the requirement that trusted components *do not collude maliciously* with each other. In case of a threshold scheme, the number of colluding parties must not exceed a certain bound. Civitas, an implementation of [20], assumes that not all of the distributed registration tellers collude in order to forge or disclose a valid private credential (cf. [9]). [24] achieves anonymity, fairness, democracy, and universal verifiability as long as the number of colluding participants does not exceed a determined threshold.

Trusted communication (Tr_Comm). The voting protocols we have analyzed require trusted communication between the participants and the components of the voting system. [24], [20], and [9] use *anonymous channels* which prevent senders from being identified and hence ensure anonymity. [9] uses an anonymous channel for vote casting to support uncoercibility.

[20] even requires an *untappable channel* to provide perfect secrecy in an information-theoretical sense. This channel is used during registration to prevent simulation and forced-abstention attacks. [9] requires an untappable channel between the voter and at least one trusted registration teller. This untappable channel allows the voter to construct a fake credential to achieve uncoercibility. In fact, an untappable channel is considered to be the weakest known assumption for receipt-freeness according to [17].

Trusted storage and erasure (Tr_SE). The voting protocols under analysis need to store and erase sensitive data. Examples for sensitive data are the *private keys* of the mix net and tallier units used in [20] and [24] as well as in their implementations [9] and [21]. The private keys of the voters must be stored securely in order to guarantee privacy. [3], [24], and [21] use blind signatures to anonymize votes. The *blinding factor* must be stored safely because disclosure could compromise anonymity.

The long-term verifiability of elections requires trusted *long-term storage* of the corresponding data (see [16]). Trusted erasure mechanisms are, for example, necessary in [20] to delete registration data. Also, the *private credential share* used in [9] must be erased by each teller after it has been delivered to the voter. Once the voter has computed the private credential from the shares, these must also be erased.

Trusted application of cryptography (Tr_AC). The analyzed e-voting protocols and all other e-voting schemes that we are aware of use cryptographic mechanisms, in particular public key cryptography. Public key cryptography is applied to distribute symmetric keys and to establish the authenticity of the entities of the e-voting system.

The application of public key cryptography requires a *public key infrastructure* (PKI). In this PKI, keys are generated and distributed securely. A Certification Authority (CA) issues certificates that prove the authenticity of public keys, i.e. bind a public key to the identity of its owner. The PKI technology plays a significant role for enabling large-scale online voting. The infrastructure itself solves certain problems that appear in electronic elections, such as user registration and identification.

In the analyzed voting schemes public key cryptography supports anonymity and democracy. [21] employs a PKI for key distribution and registration of the voters. In [22] and [9] voters use their public key certificate for authentication when registering for the election. [3] requires that the public key of the election authority is certified by an independent CA. [20] proposes to generate the tallier's key pair by a trusted third party. This can be realized within a PKI.

Miscellaneous (Tr_Misc). Several of the analyzed voting protocols require *trusted delivery* of voting equipment to the voter. [3] and [21] make use of smartcards. In [22], tamper-resistant randomizers are employed for vote casting. Those objects must be delivered reliably before the election starts. Additional voting documents such as a polling card must be distributed securely as well.

To achieve uncoercibility, voting protocols often assume that an adversary cannot observe the voter during the very moment of voting (cf. [22], [20]). In remote electronic elections this is the responsibility of the voter and may require extra measures.

General requirements. Besides e-voting-specific organizational and technical security requirements which we have taken from the analyzed protocols, there are general requirements that apply to all security critical electronic systems. Just as the specific requirements, the general requirements must be satisfied in order to achieve the security objectives. In the following we review several general security requirements and relate to the security objectives they support.

In any e-voting system including those that implement the protocols under analysis, all components need to be set up as required. This includes proper installation and configuration of the software and the usage of appropriate hardware which meets the minimum hardware requirements of the system. After installation, the *integrity* of the e-voting system has to be protected.

To ensure democracy, *availability* of the voting system must be ensured. Casting votes must be possible for any user at any time during the election. Connection bandwidth and maximum number of simultaneous connections have to be in line with the expected size of the election.

To ensure accuracy and democracy, the voting system must not enter any undefined state during the election. The voting process must be able to recover from an interruption during vote casting (cf. [19]). *Database consistency* has to be guaranteed.

Election servers must be protected against viruses, trojan horses, and network attacks such as denial of service (cf. [19], [6], [28]). All installed software (like operating systems or browsers) has to meet the minimum requirements for the voting system to function properly.

For the sake of democracy, proper *assistance* to the users of the e-voting system has to be provided.

3 The Voting Service Provider

In Section 2 we have shown that secure e-voting can only be achieved if a secure e-voting protocol is implemented in an environment that meets many organizational and technical security requirements. Satisfying those requirements is a very complex and expensive task. This reduces the potential advantage of e-voting considerably. In this section we solve this problem by introducing a *Voting Service Provider* (VSP). The VSP is defined as follows:

Definition. *The* VSP *is a trusted third party carrying out electronic elections on behalf of the* election host, *which is the institution that holds the election.*

We show that the VSP is responsible for satisfying the majority of the organizational and technical security requirements we have identified. This makes it much easier to meet the complex security requirements in a verifiable way. Allocating security critical tasks to the VSP on the other hand demands a high level of trustworthiness of the VSP. We address this issue in Section 4. As an external institution, one VSP carries out many elections for several different election hosts. Thereby the election hosts share the cost for implementing the measures to meet the security requirements. This reduces the expenses for each individual election host.

Now we show how the VSP satisfies the requirements identified in Section 2, referring to the measures recommended in the Safeguard Catalogues of the German Federal Office for Information Security [4].

Trusted components (Tr_Comp). All trusted components such as the trustworthy administrator, the registration authority or the time stamp server are operated by the VSP. For example, the time stamp server is monitored and partitioned off. If the adminstrator or the registration authority is human, the VSP employs measures like legally binding contracts, non-disclosure agreements, or dual-control to support their trustworthiness (cf. [4, M 3.10], see also General requirements). The VSP guarantees that the trusted components do not collude maliciously. Their communication capabilities to other components are restricted to the indispensable minimum. The VSP prevents malicious collusion by logical or even physical separation where necessary (cf. [14], [4, M 2.73]). Logical separation is realized by adequate design and implementation of the voting software. For physical separation, the VSP uses separate hardware or provides separate rooms for each component. These rooms may be secured by physical access control (see Tr_SE).

Trusted communication (Tr_Comm). The VSP provides for trusted communication between the participants of the electronic election. Anonymous channels can be implemented using a mix net as proposed in [24]. This mix net is securely operated by the VSP.

The VSP can establish an untappable channel using postal service as suggested in [20]. To realize an untappable channel between system components, the VSP may separate the involved components physically and disconnect them from any network (cf. [4, M 5.61]). Authorized personnel of the VSP then exchanges data by transferring read-only storage media like recorded DVDs.

Trusted storage and erasure (Tr_SE). The VSP takes physical precautions to guarantee the secure storage of private keys of server components such as mix net or tallier. Safety areas or separate rooms may be used for these components, physical access control restricts access to authorized personnel of the VSP (cf. [4, M 1.29, 2.6]). Possible access control mechanisms are for example locks and keys, card access or biometric identification systems (cf. [4, M 2.17]). Also, the VSP can monitor these rooms by a video surveillance system (cf. [4, M 1.53]). The VSP realizes secure storage of private keys or blinding factors on the part of the voter by secure software design or by distributing tamper-resistant hardware such as smartcards.

The VSP ensures reliability of storage media by using backup or redundancy systems, e.g. mirror harddrives. That way, loss of ballot data can be prevented. To guarantee long-term security, the VSP archives all relevant election data on reliable storage media in a physically secured room.

The VSP realizes secure erasure of data, such as the private credential shares used in [9], by means of software. There are approved methods for secure erasure by overwriting data with random bits, so called "file shredding" (cf. [4, M 2.167]).

Trusted application of cryptography (Tr_AC). If no trusted PKI is already used by the election host, the VSP is responsible for providing an adequate PKI. The VSP either uses PKI services of a third party or establishes its own PKI. In the latter case the VSP provides all necessary hardware and software and is responsible for secure operation and maintenance of the PKI. Key generation is performed in a secure environment using suitable key generators. The VSP distributes the keys on suitable data media (e.g. smartcards) or via communication channels which ensure their confidentiality (e.g. encrypted with a key encryption key), integrity (e.g. MAC-secured) and authenticity (e.g. with a digital signature) (see [4, M 2.46]). The VSP uses a PKI based on X.509 certificates specified in [2] and [18]. X.509 certificates are used for realizing qualified certificates [30]. For example, qualified certificates according to the German Signature Act [32] are implemented using X.509.[1]

Several countries have issued or plan to issue electronic citizen cards, i.e. smartcards which support e-government. The underlying PKI can be used for legally binding electronic elections on the national level. Requirements like secure key generation or secure digital signatures are provided by such an infrastructure. In this case, the VSP does not deal with these issues. This fact simplifies the VSP's deployment, which in turn supports deployment of remote e-voting. Therefore, promotion of citizen cards is a long-term goal.

Miscellaneous (Tr_Misc). The VSP is responsible or even legally liable for the secure delivery of any voting equipment required. Depending on the underlying e-voting protocol, the VSP delivers smartcards (cf. [3]) or tamper-resistant devices like the randomizers used in [22]. Moreover, the VSP may be charged to distribute legally required voting documents like polling cards. The VSP delivers electronic items like the credentials used in [20] via a confidential and authenticated channel such as a TLS connection or via secured e-mail using S/MIME.

[1] Note that qualified certificates have a different meaning in the various specifications, regulations, countries, etc.

The VSP informs the voter about her duty to care for not being observed while voting. If the election takes place in a company and voters cast their vote from their workstations, the workplace is supposed to be configured in a way which does not allow the computer screen to be observed by third parties while voting (cf. [4, M 1.29, M 3.9]). The VSP advises the election host on achieving these measures.

General requirements. The VSP is responsible for installing and configuring the voting system correctly. The VSP enforces integrity of the voting software by using digitally signed system code (cf. [4, M 4.177]). Furthermore, the VSP provides safe rooms combined with appropriate access control to support software integrity. Only authorized personnel of the VSP has access to the voting system and the areas where the election server is located (cf. [4, M 1.58, 2.6–2.8]).

To ensure availability of the election system, the VSP employs appropriate hardware. The VSP chooses memory, CPU and storage capacity of the server computers adequately to guarantee the necessary data processing performance. Connection bandwidth and maximum number of simultaneous connections have to be in line with the expected size of the election. To ensure database consistency, the VSP enforces rollback policies by using appropriate software design (cf. [4, M 2.130]). The VSP runs standard security software like anti-virus and firewall programs on all computers under its responsibility and makes use of intrusion detection systems (cf. [4, M 4.3]). Also, the VSP ensures that the minimum requirements of the voting system are met by all software components on the VSP's hardware, for example operating systems, browsers or Java runtime environment. To prevent system unavailability caused by a power outage or system failure due to flood or fire, the VSP enforces special safety regulations regarding the rooms or the whole building where the server components are located (cf. [4, M 1.1–1.29, 1.58]).

The VSP provides the skilled personnel which is necessary to set up and maintain the voting system. Trustworthiness of the personnel is achieved by legally binding contracts such as non-disclosure agreements (cf. [4, M 3.2, 3.33, 3.50]). The VSP enforces policies regarding prevention of operating errors and misuse by the personnel. For example, accessing the vote server, e.g. in order to start the election application, should be regulated by dual-control (cf. [14]).

The VSP is the point of contact in all questions regarding the election process. The VSP offers assistance to the voters regarding questions on how to register and cast their vote correctly by providing online assistance and offering a helpline.

Table 1 summarizes our results. It contains the organizational and technical security requirements and how the VSP satisfies them. The table is restricted to the requirements which we have identified in the protocols [3], [20], [22], and [24]. Thus, long-term storage as well as the general requirements we have described are not included.

Requirement	**Family**	**Protocol**	**Measures**
trustworthy administrator, trustworthy registration authority	Tr_Comp	[24], [22], [20]	legally binding contracts, non-disclosure agreements, dual-control
trustworthy time stamp server	Tr_Comp	[3]	secure operation, monitoring, partitioning-off
prevention of malicious collusion	Tr_Comp	[24]	logical or physical separation, restricted communication capabilities
anonymous channel	Tr_Comm	[24], [20]	secure mix net
untappable channel	Tr_Comm	[20]	physical separation, data exchange via read-only media, postal service
secure storage of private keys (server-side)	Tr_SE	[24], [20]	safety areas, physical access control, surveillance, reliable storage media
secure storage of blinding factor (client-side)	Tr_SE	[24], [3]	secure software design, tamper-resistant hardware
erasure of private credential share	Tr_SE	[20]	secure software design, file shredding
PKI	Tr_AC	[24], [3], [22], [20]	X.509 certificates, smartcards (e.g. electronic citizen cards), secure communication channels, secure hardware
delivery of voting equipment	Tr_Misc	[3], [22], [20]	electronic items are delivered via confidential and authenticated channel (TLS) or secured e-mail (S/MIME), hardware equipment requires logistics solution

Table 1. Security requirements and how the VSP satisfies them

4 Analysis of the concept

In our concept, the majority of the security critical tasks is centralized in one institution, namely the VSP. Thus it has to be trustworthy. The VSP provides those security critical tasks as a service, a concept which is similar to Certification Authorities (CAs). To establish trustworthiness for the VSP we therefore employ the approved procedures used for CAs in Germany: A product evaluation, e.g. following Common Criteria [7], as well as legal regulation including a special law and supervision by an independent control authority. We explain this in more detail:

To ensure proper function, the e-voting software used by the VSP is evaluated and certified according to Common Criteria. In Germany, the Protection Profile for online elections (see Section 1.1) is intended to be used for that purpose. Regarding the hardware, the VSP uses certified components in all security relevant areas. The organizational structure, the workflows and thus the VSP as a whole is evaluated according to adequate methods. Here we follow the approach used for German CAs: According to the German Signature Act [32], each CA must provide a security concept (*Sicherheitskonzept*) which records how organizational requirements are met. Among others these include workflow management, reliability of employed personnel, and emergency precautions [33, §2]. The control authority then evaluates this security concept and verifies that the CA complies with the specified measures.

A special law regulates the legal requirements for electronic elections and VSPs. CAs in Germany are bound to the German Signature Act [32]. Currently, an analogical law for VSPs is in preparation. The law covers security aspects (like the usage of certified software and hardware) as well as requirements for the organization and operation of the VSP. This includes the existence of an independent authority which is responsible for controlling and supervising the VSP. For example, the control authority ensures legal conformity of the VSP. Auditing is scheduled on a regular basis. In conclusion we observe that, compared to the POLYAS voting system [23], our concept to establish trust in the VSP is more comprehensive since POLYAS restricts itself to software evaluation.

As the majority of security critical tasks is allocated to the VSP, the idea of a single point of failure is induced. However, the advantages of the centralized concept outweigh this. Due to the centralized structure it is easier to install and configure a secure e-voting system satisfying all security requirements. An institution like the VSP can easily be supervised, controlled as well as evaluated and certified according to legal requirements as proposed above. We assume that individual election hosts cannot involve themselves into a Common Criteria evaluation as this is a costly, time and resources consuming process. However, if a VSP is employed, this evaluation must be done only once for many elections of various election hosts. The advantages of a service provider have proven themselves in the analogical concept of a CA which served as a role model.

5 Conclusion

By analyzing state-of the-art e-voting protocols we have shown that secure electronic elections can only be achieved if a secure e-voting protocol is implemented in an environment that satisfies many organizational and technical security requirements. We have introduced the concept of a Voting Service Provider as a trusted third party and we have shown that the VSP can be made responsible for satisfying the majority of the security requirements. Deploying a VSP makes it much easier to verify that e-voting security requirements are met.

Since one VSP can be used by many election hosts, e-voting through VSPs is more cost-efficient. Employing a VSP allows the election host to benefit from the advantages of e-voting while at the same time keeping its own effort low. Using a VSP therefore makes e-voting much more feasible.

References

1. The CyberVote Project. http://www.eucybervote.org/, last checked 19.02.2008.
2. ITU-T Recommendation X.509 (2000). Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. ISO/IEC 9594-8:2001.
3. Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Guillaume Poupard. Practical Multi-Candidate Election System. In *PODC*, pages 274–283, 2001.
4. Bundesamt für Sicherheit in der Informationstechnik. *IT–Grundschutz–Kataloge*, 2006. http://www.bsi.de/gshb/deutsch/m/m01.htm, last checked 13.02.2008.
5. Bundesamt für Sicherheit in der Informationstechnik. Schutzprofil Basissatz von Sicherheitsanforderungen an Onlinewahlprodukte. Draft, 2007.
6. Mike Burmester and Emmanouil Magkos. Towards Secure and Practical E-Elections in the New Era. In Dimitris Gritzalis, editor, *Secure Electronic Voting*, volume 7 of *Advances in Information Security*, pages 63–76. Kluwer Academic Publishers, 2003.
7. The official website of the Common Criteria Project. http://www.commoncriteriaportal.org/, last checked 13.02.2008.
8. S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. *RFC*, 3647, November 2003.
9. Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: A Secure Remote Voting System. Technical Report TR2007-2081, Cornell University, May 2007.
10. Council of Europe. Legal, Operational and Technical Standards for E-voting. Recommendation Rec(2004)11, September 2004. http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/, last checked 13.02.2008.
11. Council of Europe and Estonian National Electoral Committee. Internet Voting in the March 2007 Parliamentary Elections in Estonia. Report for the Council of Europe, July 2007. http://www.vvk.ee/english/CoE%20and%20NEC_Report%20E-Voting%202007.pdf, last checked 13.02.2008.

12. Ananya Das, Yuan Niu, and Till Stegers. Security Analysis of the eVACS Open-Source Voting System, 2005.
13. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML, last checked 13.02.2008.
14. Gesellschaft für Informatik. GI-Anforderungen an Internetbasierte Vereinswahlen (”GI requirements for Internet based elections in non-governmental organizations”), August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf, last checked 13.02.2008.
15. Gesellschaft für Informatik — Wahlen und Ordnungen. http://www.gi-ev.de/wir-ueber-uns/leitung/wahlen-und-ordnungen/, last checked 13.02.2008.
16. Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, and Marcel Weinand. Security Requirements for Non-political Internet Voting. In Robert Krimmer, editor, *Electronic Voting 2006. Proceedings of the 2nd International Workshop on Electronic Voting 2006,(2-4 Aug 2006), Bregenz*, number 86 in Lecture Notes on Informatics, pages 203–212. Gesellschaft für Informatik, 2006.
17. Martin Hirt and Kazue Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 539–556. Springer-Verlag, 2000.
18. R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. *RFC*, 3280, April 2002.
19. Rui Joaquim, Andre Zuquete, and Paulo Ferreira. REVS — A Robust Electronic Voting System. In *Proceedings of IADIS International Conference e-Society 2003*, pages 95–103, 2003.
20. Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *WPES*, pages 61–70. ACM, 2005.
21. Kwangjo Kim, Jinho Kim, Byoungcheon Lee, and Gookwhan Ahn. Experimental Design of Worldwide Internet Voting System using PKI. In *Proceedings of SSGRR International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet*, August 2001.
22. Byoungcheon Lee and Kwangjo Kim. Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer. In Pil Joong Lee and Chae Hoon Lim, editors, *Information Security and Cryptology – ICISC 2002, 5th International Conference Seoul, Korea, November 28-29, 2002, Revised Papers*, volume 2587 of *Lecture Notes in Computer Science*, pages 389–406. Springer, 2003. http://www.springerlink.com/content/91cf7ct3b9mmu9qa/fulltext.pdf, last checked 21.02.2008.
23. Micromata. Polyas Online Voting Solutions. Online-Wahlen für Verbände und Vereine, 2005. http://www.micromata.de/produkte/documents/polyas_broschuere_72dpi.pdf, last checked 13.02.2008.
24. Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. An Improvement on a Practical Secret Voting Scheme. In Masahiro Mambo and Yuliang Zheng, editors, *ISW*, volume 1729 of *Lecture Notes in Computer Science*, pages 225–234. Springer, 1999.

25. Organization for Security and Co-operation in Europe (OSCE), Office for Democratic Institutions and Human Rights (ODIHR). *Final Report on the 4 March 2007 Parliamentary Elections in Estonia*, June 2007. http://www.vvk.ee/english/OSCE%20report_EST_2007.pdf, last checked 19.02.2008.
26. Kai Reinhard and Wolfgang Jung. Compliance of POLYAS with the BSI Protection Profile – Basic Requirements for Remote Electronic Voting Systems. In Ammar Alkassar and Melanie Volkamer, editors, *VOTE-ID*, volume 4896 of *Lecture Notes in Computer Science*, pages 62–75. Springer, 2007.
27. Andreu Riera. An Introduction to Electronic Voting Schemes. Technical Report PIRDI 9-98, University of Barcelona, October 1998. http://pirdi.uab.es/document/pirdi9.ps, last checked 13.02.2008.
28. Aviel Rubin. Security Considerations for Remote Electronic Voting over the Internet, 2001. http://eprintweb.org/S/authors/cs/ru/Rubin/6, last checked 13.02.2008.
29. Peter Y. A. Ryan. Pret a voter with a human-readable, paper audit trail. Technical Report 1038, Newcastle University, School of Computing Science, July 2007.
30. R. Santesson, W. Polk, P. Barzin, and M. Nystrom. Internet X.509 Public Key Infrastructure Qualified Certificates Profile. *RFC*, 3039, January 2001.
31. Pnyx.core: The Key to Enabling Reliable Electronic Elections. A Description of Scytl's Cryptographic e-Voting Security Software. White paper, Scytl Secure Electronic Voting, Barcelona, Spain, December 2005. http://www.scytl.com/docs/pub/science/PNYXCOREWhitePaper.pdf, last checked 13.02.2008.
32. German Electronic Signature Act (Gesetzliche Rahmenbedingungen für elektronische Signaturen, SigG). http://bundesrecht.juris.de/sigg_2001/index.html, last checked 13.02.2008.
33. German Electronic Signature Ordinance (Verordnung zur elektronischen Signatur, SigV). http://bundesrecht.juris.de/sigv_2001/index.html, last checked 13.02.2008.