Towards the impact of the operational environment on the security of e-voting

Axel Schmidt, Melanie Volkamer, Lucie Langer, Johannes Buchmann

Technische Universität Darmstadt
Hochschulstr. 10
64289 Darmstadt
CASED
Mornewegstr. 32
64293 Darmstadt
{axel, langer, buchmann}@cdc.informatik.tu-darmstadt.de
volkamer@cased.de

Abstract: Our paper deals with the security of operational environments for e-voting and its importance for the security of electronic elections. So far the security of e-voting was focused on secure e-voting protocols. We show that the security of electronic elections requires a secure operational environment as well. We provide a comprehensive catalogue of organizational and technical requirements which have to be satisfied by the operational environment in order to operate secure remote electronic elections. Our findings provide a basis for the design and evaluation of a secure operational environment for e-voting. Security requirements for e-voting have been defined in several catalogues. We analyzed the important catalogues from the Council of Europe and the German Informatics Society as well as two Common Criteria Protection Profiles on e-voting to derive the organizational and technical requirements they include for the operational environment. We propose a procedure based on IT-Grundschutz/ISO27001 in order to use our findings for the evaluation of the operational environment thereby improving trustworthiness and security of electronic elections.

1 Introduction

Electronic voting promises to greatly improve the general experience of voting and democratic participation. However the security of electronic elections is of prime importance. Our paper deals with the question which organizational and technical requirements an institution must satisfy in order to provide a secure operational environment to carry out secure electronic elections. Our findings provide a basis for design and evaluation of such a secure operational environment to provide secure electronic elections. Hence our results are of great value for all institutions which want to perform secure electronic elections.

So far research concentrated on the security of electronic voting systems, in particular cryptographic protocols and the corresponding voting software. In [LSB08] we showed that such protocols alone cannot achieve the security of electronic elections. The operational environment, in which the electronic voting system is operated, has to satisfy many technical and organizational requirements as well in order to enable secure electronic voting. In our previous work we analyzed state-of-the-art online voting protocols for their requirements towards the operational environment. In this paper we extend our work by including the most relevant sources for e-voting security requirements which we analyzed in depth for their requirements towards the operational environment.

Recently, the German Federal Office for Information Security (BSI) published two Common Criteria Protection Profiles on "Basic set of security requirements for Online Voting Products" and "Digital Voting Pen System" intended for the evaluation of electronic voting systems ([BSI08]; [BSI07]; [CC]). We scrutinized these Protection Profiles to identify the requirements they need the operational environment to satisfy, in which the voting systems are deployed. Moreover, we analyzed the "Legal, Operational and Technical Standards for E-voting" from the Council of Europe for their requirements for the operational environment [Co04]. At last we included the catalogue of requirements for online elections in non-governmental organizations of the German Informatics Society [GI05] to derive their requirements for the operational environment.

The result is a very comprehensive catalogue of organizational and technical requirements for the operational environment of electronic elections. Examples are technical prerequisites like secure hardware, secure communication channels, secured rooms for server computers and emergency precautions as well as organizational matters like secure registration of voters, monitoring of the voting system and trustworthy personnel.

Finally we propose how our findings could be used as a basis for evaluation and certification of the operational environment to verify its suitability to securely operate electronic elections thereby improving the security and trustworthiness of electronic elections. For the evaluation we recommend a procedure following IT-Grundschutz/ISO27001 methodology [BSI]. Therefore we studied the IT-Grundschutz-Catalogues of the BSI [BSI05]. These catalogues provide a comprehensive set of requirements, threats and safeguards for securing IT systems and their environment with regard to organizational, personnel, infrastructural and technical matters. We analyzed the applicability for the evaluation of operational environments for e-voting. We also show how the concept of the Voting Service Provider can facilitate the effort of providing a secure operational environment thereby making secure electronic elections feasible.

1.1 Related Work

To our knowledge, the security of operational environments for e-voting and its impact on the security of electronic elections has not been considered in depth so far. The most relevant catalogues on e-voting security are introduced and analyzed in Section 2.

1.2 Our contribution

In [LSB08] we showed that in order to achieve secure electronic elections the operational environment must satisfy many organizational and technical requirements. The study was limited to requirements which we derived from e-voting protocols. In this paper we extend our earlier work. We analyze the most important sources for e-voting security to derive the so far most comprehensive catalogue of requirements for the operational environment of electronic elections. Our catalogue can be used as a basis for the design and evaluation of such operational environments to verify their suitability to operate secure electronic elections, thereby improving the security and trustworthiness of electronic elections. We show how our catalogue can be integrated in the evaluation concept for Voting Service Providers.

Our paper is organized as follows. In Section 2 we introduce the sources for our analysis. In Section 3 we present the requirements for the operational environment derived from the analysis. In Section 4 we give recommendations how to evaluate a secure operational environment based on our findings. Section 5 concludes our paper.

2 Analyzed sources

In [LSB08] we showed that the use of secure e-voting protocols is not sufficient to implement secure electronic elections. The protocols need many organizational and technical requirements to be fulfilled by the operational environment in which the voting system is operated.

Based on ([BSI08]: 1.2.5) we define the operational environment to include the hardware, the operating system, additional application software, the network infrastructure, the involved personnel (including the election host) and the building and rooms where the voting system is located. Because our findings are intended to be a basis for evaluation procedures we focus on the server side environment. In online voting scenarios the client side environment is under control of the voter and therefore cannot be generally evaluated. Here the voter must be assisted on securing his client side environment. We consider this issue in the category “Assistance and training”, Section 3.

In [LSB08] we categorized the requirements we found in the analyzed protocols. But in addition to the specific requirements from the protocols there are many more requirements given in the e-voting literature. While some of them are directly related to the e-voting scenario, others describe general requirements for secure environments in which security critical IT systems are deployed. To provide a comprehensive foundation for the evaluation of operational environments for e-voting it is necessary to include all these requirements. In this paper we therefore analyze the most relevant sources on e-voting security for their requirements towards the operational environment in electronic election scenarios.

The German Federal Office for Information Security (BSI) recently published two Common Criteria Protection Profiles on electronic voting ([BSI08]; [BSI07]). In the Common Criteria context, Protection Profiles describe assumptions, objectives, requirements and threats for a specific family of IT products [CC]. Such a Protection Profile can be used by the manufacturer as guidance to construct a secure IT product. Moreover, products can be evaluated according to Common Criteria with regard to their compliance with the requirements of the Protection Profile. In 2008, the BSI released the Common Criteria Protection Profile "Basic set of security requirements for Online Voting Products". This Protection Profile aims to provide security requirements for online voting products like for example the software system used for online elections. This Protection Profile is intended to be used as a foundation for the evaluation of online voting systems in Germany. Although the Protection profile concentrates on the security of the software system, it still includes assumptions on the security of the operational environment. We integrate these assumptions as requirements in our catalogue.

In 2007 the BSI published another Protection Profile on the "Digital Voting Pen System". This system is intended for the use in electronic elections based on polling stations. Again in addition to the description of security requirements for the digital voting pen system, the Protection Profile provides security requirements for the operational environment in which the digital voting pen system is deployed. We analyze and include these requirements in our catalogue.

The German Informatics Society (GI) published a catalogue on requirements for Internet based elections in associations [GI05]. The GI carries out the election of its chairmanship electronically since 2004 [GI]. The GI catalogue considers requirements for the voting system development and the execution of the election, requirements for the voting servers as well as requirements for the voting software system including security and usability aspects. Although requirements for the operational environment are not explicitly stated we could derive such requirements as consequence to the requirements for the software system.

In 2004, the Council of Europe published a recommendation on "Legal, Operational and Technical standards for E-voting" [Co04]. This recommendation includes many security requirements and has been internationally considered and accepted. Again the authors did not focus on the issue of a secure operational environment. Still we could derive such requirements from the catalogue.

To sum up, we analyzed the most approved and relevant sources to derive a catalogue of security requirements for the operational environment of electronic elections. By including the security requirements derived from the electronic voting protocols we analyzed in [LSB08], we finally present a comprehensive catalogue of security requirements for the operational environment of electronic elections.

At first our catalogue can be used by election hosts (i.e. the party which wants to carry out an electronic election) to see which requirements have to be considered to provide a secure operational environment for secure electronic elections. But most important, the catalogue provides a basis for evaluation of the operational environment for electronic elections and thus can improve trustworthiness and security of electronic voting.

3 Requirements for secure operational environments

In the following we will integrate the security requirements we derived from the sources mentioned in Section 2 into categories based on the families we defined in [LSB08]. We extended the number of families to include all new requirements we found. We also include the results of our previous work, namely the requirements for the operational environment coming from the protocols. We point out that due to space limitation we cannot provide detailed descriptions of the requirements in our catalogue. For the protocol related requirements, details can be found in [LSB08].

Furthermore, we point out that besides a secure operational environment, secure electronic elections of course require a secure voting protocol. As our paper concentrates on the security of the operational environment we assume a secure voting protocol in the following.

We will refer to the respective sources using literature references.

Trusted components

To achieve the security objectives of e-voting (see [LSB08]), many e-voting protocols assume certain components of the voting system to be trustworthy. The protocols cannot enforce the secure operation of the components. Thus this must be taken care of by the operational environment in which the voting system is implemented. For example, such components are a trustworthy administrator who checks the eligibility of voters [Oh99], a trustworthy registration authority which is assumed not to collude with an adversary [JCJ05] or a trustworthy time stamp server which allows voters to prove that they have cast their vote in time before the election terminated [Ba01]. Moreover to guarantee security of the electronic election several protocols require that certain components must not be able to collude maliciously because otherwise the secure function of the protocol is threatened (see also ([GI05]: Y-3)). For example, [Oh99] can achieve secure function only as long as the number of colluding participants does not exceed a determined threshold. Hence the operational environment must satisfy these requirements for the voting system components to ensure the secure function of the protocols. More details on these protocol related security requirements for the operational environment can be found in [LSB08].

Trusted communication

The operational environment of an electronic voting system must provide secure communication channels between the vote-casting device and the election server. The communication channels must be protected against modifications and disclosure. The operational environment therefore provides the cryptographic operations and protocols for the operation of a communication channel which ensures integrity and confidentiality of the communication data ([BSI08]: 151,193; [GI05]: G-4).

The protocols [Oh99], [JCJ05], and [CCM07] use anonymous channels to prevent senders from being identified and hence ensure anonymity. Several protocols even require an untappable channel to provide perfect secrecy in an information-theoretical sense. [JCJ05] uses an untappable channel during registration to prevent simulation and forced-abstention attacks. Again we point out that such secure communication channels cannot be enforced by the voting protocol itself. They have to be operated by the operational environment.

Trusted storage and erasure

During an electronic election plenty of highly security critical data have to be stored, for example cryptographic keys, blinding factors, ballot data, the electoral roll or monitoring and audit records. Partially data has to be stored in the long term, partially it has to be erased securely after the election is finished. Long term storage of election data often is requested by corresponding legal regulation to allow reproduction of election results. Secure erasure of certain data often is required to prevent being used as receipt for the vote cast.

The operational environment must provide storage media which is functioning correctly. Integrity and availability of all stored data like vote records in the ballot box, user data and voting result must be ensured as long as required. Errors during the storing of votes must be reported to the voting system's security functions. Capacity of storage media must be sufficient ([BSI08]: 146,187, [Co04]: III.97,99; [BSI07]: 4.2). Furthermore, the operational environment is assumed to store audit records from the server-sided voting system in a way that they are protected against unauthorized manipulations, deletion or adding ([BSI08]: 148, 189). Ballot data buffered on the voting device outside the control of the voting system have to be erased securely after the voting process ([BSI08]: 152, 194). For online elections, this eventually is the responsibility of the voter. Still the voters must be instructed how to erase buffered data. The operational environment must provide techniques to secure the integrity of data ([BSI08]: 191), loss of data must be prevented ([Co04]: III.77). Sensible data like decryption keys must be protected from disclosure. This can be realized by secure storage or secure erasure after the election ([BSI08]: 150, 192). The archiving techniques and the duration of it must be specified by the election host. The election host, i.e. the operational environment, must take care of the cleansing (uninstallation and deletion of data) of the server-sided voting system ([BSI08]: 446; [GI05]: X-9).

The protocols [Ba01], [JCJ05], [LK02], [Oh99] need the private keys of the voters to be stored securely to guarantee privacy. The blinding factors used for blind signatures in [Ba01], [LK02] and [Oh99] have to be stored safely because disclosure would threaten anonymity of the voters. [JCJ05] and [CCM07] need secure erasure mechanisms to delete registration data and the private credential shares.

Trusted application of cryptography

The majority of e-voting protocols extensively use public key cryptography to implement their security objectives. For example, they use encryption, electronic signatures and blind signatures to ensure at least confidentiality, integrity, authenticity as well as certificates for registration purposes [LSB08]. Consequently cryptographic encryption and signature keys, certificates and public keys need to be generated and distributed securely. In a Public Key Infrastructure (PKI), a Certification Authority provides secure generation and distribution of keys and certificates. These actions cannot be provided by the e-voting protocol. Thus the operational environment must take care of appropriate measures. These could be either providing a PKI or assigning a third party to do so.

The operational environment must provide the cryptographic mechanisms to establish secure communication between the vote-casting device and the election server, ensuring integrity and confidentiality. Moreover, the operational environment is assumed to provide the means for generation, distribution, access and destruction of cryptographic keys ([BSI08]: 193; [GI05]: X-6).

The protocols also require PKI techniques. [Ki01] uses a PKI for key distribution and registration of the voters. [CCM07] and [LK02] use certificates for registration purposes. [Ba01] uses a public key of the election authority certified by an independent Certification Authority. [JCJ05] proposes to generate the tallier's key pair by a trusted third party.

Trusted time

Several processes during an electronic election require exact time data. All components of the voting system must use the same time to prevent errors. For example, if components do not use exact time data, ballots could be rejected on mistake because the election server already closed the voting phase but following the client's time the voting phase is still open. This can lead to many problems including legal consequences like for example voters complaining about not being able to cast their ballot during voting phase. Moreover, exact time is required to match monitoring and audit events with the actual voting processes to generate reliable records. The voting protocols cannot provide correct time. This has to be done by the operational environment.

The operational environment of the server makes correct time and time stamps available conforming to the actual time. The required exactness is defined by the election host ([BSI08]: 147,188,419; [Co04]: III.84; [BSI07]: 4.2).

Trusted organization

The security of electronic elections, especially online elections, also depends on a secure organization of the election. There are many organizational tasks which must be performed securely. Of course the organization cannot be provided by the voting protocols. The election host and its operational environment are responsible for the secure organization. Due to the number of organizational requirements, we restrict to some examples.

The election host must take care of correct election preparation. The electoral board must identify the voters correctly ([BSI07]: 4.2). The voting system must be set up correctly. Correct operation must be checked ([Co04]: I.31,III.73). The candidate list and time tables for all election phases including ending time of the voting phase must be set and published. If the election also allows traditional voting in parallel, the election host must ensure that voters cannot cast several votes via different voting channels. Registration and checking of the electoral roll must be possible for all voters ([BSI08]: 138,179,417,418,429; [GI05]: X-8; [Co04]: II.37,43).

The election host and its operational environment must take care of trusted delivery of relevant voting materials as well as authentication means (like for example smart cards, certificates or passwords) required to cast a vote. Items must be delivered in time and only to eligible voters ensuring integrity, authenticity and confidentiality ([BSI08]: 141,182,427 and [GI05]: X-7).

After the voting phase the voters shall be prevented from logging on to the voting system. Acceptance of votes should be extended shortly to enable voters who logged into the system lately to finish casting their vote. The election host specifies the appearance of the ballot on the vote-casting device ([BSI08]: 419,441).

Several protocols themselves require trusted delivery of voting equipment like smartcards in [Ki01] and [Ba01] or the randomizers for vote-casting in [LK02].

Trusted logging and monitoring

To facilitate reproduction of the election process and later investigation in case of problems, it is recommended to record all relevant processes and events during the election. This includes logging of all voting system processes as well as monitoring of the hardware, the secured rooms and the personnel. In the similar scenario of Certification Authorities in Germany, such measures are even required by legal regulation ([SigG01]: §10).

The voting system shall be auditable. All data and actions related to the election processes, attacks, and malfunctions shall be recorded. The election host defines how to monitor network and election server and identify malfunctions ([BSI08]: 421,439; [GI05]: Y-4; [Co04]: II.57,59,III.103).

Trusted installation and configuration

To ensure secure function, the electronic voting system must be installed and configured correctly. The integrity of the system must be protected, database consistency must be assured. The minimum requirements for all related hardware and software must be satisfied. The voting system must not enter any undefined state and must be able to recover from interruption.

Election data (ballot data, electoral register with authentication data, ending time of the election) must be transferred to the election server correctly, the ballot box must be empty. The server-sided voting system must be configured and initialized correctly including authentication data of the electoral board and its personnel ([BSI08]: 138,179; [BSI07]: 4.2).

Availability

All eligible voters must be able to cast their vote at any time during the voting phase. Therefore availability of the voting system must be guaranteed. Connection bandwidth and maximum number of simultaneous connections have to be in line with the expected size of the election [LSB08].

The operational environment must guarantee the robustness, quality of service and availability of the network and of the election server. The election host ensures that the availability can be recovered in case of malfunctions. Backup systems shall be implemented ([BSI08]: 144,185,437,438; [Co04]: I.30,III.71).

Protection of the voting system

The integrity of the voting system must be protected to ensure its secure function. This includes software and hardware. Especially the safety of the hardware can only be protected by the operational environment. To protect the voting system software, standard measures like anti-virus software, intrusion detection systems and firewalls must be implemented to prevent attacks from the network or malware [LSB08]. All sensible components of the voting system must be protected from unauthorized access. In case of emergency the election host must provide appropriate measures to protect the security of the election. Here emergencies regarding the voting system as well as the environment must be considered.

The audit system and audit data shall be protected against attacks like unauthorized modification. The election host is responsible to protect the election server from network attacks. The server must withstand outside influences like power or temperature fluctuation or humidity. Only authorized personnel are allowed to enter the server room or access the server. Secure operating systems and a security concept for protection of the server and the environment must be provided.

Emergency plans in case of inconsistent storage of votes or malfunctions of network or election server are required ([BSI08]: 143,145,184-186,420,439,444; [GI05]: Y-1,Y-2; [Co04]: I.32,III.70,109; [BSI07]: 4.2).

Trusted personnel

The election host's personnel are required to be trustworthy. They access the voting system only in the expected way, they do not install malware or modify user or system data. They do not forward their authentication data to others. They follow the election host's instructions. They observe the voting system and report detected malfunctions ([BSI08]: 140,181,185; [BSI07]: 4.2).

Assistance and training

To ensure correct handling of the voting system by all voters the election host must provide assistance on its usage. Moreover the election host must train and instruct all personnel involved in the election how to perform their tasks correctly.

The election host must advise the voter how to use the voting system, how to cast his vote unobserved, how to deal with his authentication data and how to secure his vote-casting device (e.g. in online election scenarios where home computers are used as voting-device). The vote-casting device is assumed to be able to properly display the ballot, to verify authentic communication with the server, to transfer the ballot to the server and to delete the vote afterwards. Here the election host can also assist. The personnel are sufficiently trained to understand the secure operation of the voting system and to use it appropriately. The election host must instruct them to use the voting system only in the intended way, not to install malware, not to modify the voting system or election data and not to forward their authentication data. Moreover, they are instructed how to observe the network and the election server and how to detect malfunctions ([BSI08]: 139-142,149,180,181,183,185,190; [GI05]: X-4; [Co04]: II.38,46,III.92,93).

4 Evaluation of operational environments

Our catalogue of requirements is intended to be used as a basis for security evaluation of operational environments for e-voting. An evaluated and certified operational environment improves trustworthiness and security of electronic elections for both voters and election hosts. Therefore evaluation is strongly advisable. So far there is no special evaluation concept for operational environments for e-voting. The next step is to determine an evaluation methodology. Common Criteria focuses on the evaluation of software systems. For our purpose, we therefore recommend to use the IT-Grundschutz methodology [BSI05]. The IT-Grundschutz-Catalogues provide a comprehensive set of modules describing all security relevant aspects of complex IT systems like hardware, software, network infrastructure and personnel and relate them to threats and safeguards. The IT-Grundschutz-Catalogues are intended for securing and evaluating complex IT systems. Moreover, IT-Grundschutz provides an internationally approved evaluation methodology based on the IT-Grundschutz-Catalogues/ISO27001 [BSI]. Items which are not included, like for example very specific requirements or measures for e-voting, can be added as new modules. Such specific e-voting extension is intended to be future work. To sum up, IT-Grundschutz is particularly suitable for the evaluation of operational environments.

An analysis shows that the majority of requirements from our catalogue are already covered in the IT-Grundschutz-Catalogues. For example, there are modules describing threats and safeguards for data protection, cryptographic concepts, archiving, emergency planning, personnel, training, and organization in module catalogue B1 [BSI05]. Section B2 considers the security of buildings and server rooms, while B3 focuses on server systems. Network security like heterogeneous networks and remote access issues can be found in B4. Moreover, the IT-Grundschutz-Catalogues provide a comprehensive set of safeguards. For example, for archiving they recommend backup systems or appropriate storage media, for personnel they provide training plans and for server rooms they propose special entry controls. These safeguards can be implemented to provide the necessary functionality of the operational environment.

Some specific requirements of our catalogue are not covered in the IT-Grundschutz-Catalogues. For example, the very specific requirement of an untappable communication channel is not considered. Such new requirements can be added in new extension modules for IT-Grundschutz and thereby be included in the evaluation.

In [LSB08] we introduced the concept of the Voting Service Provider (VSP), a qualified trusted third party which technically carries out an electronic election as a service on behalf of the election host. In this scenario the VSP provides the secure operational environment. Therefore the evaluation would have to be done only once for many elections as the VSP can operate many elections for different election hosts. Hence the election host does not need to provide and evaluate the operational environment and thus safes money and effort. For VSPs we proposed an even more sophisticated approach for evaluation. The VSP's voting software system shall be evaluated according to Common Criteria, based on the Protection Profile for online voting systems [BSI08]. In a project on remote electronic voting in Germany, a circle of experts in e-voting and technical law is developing a legal regulation for remote e-voting and VSPs. This legal framework follows the basic ideas of the German Signature Law [SigG01] and the corresponding German Signature Ordinance [SigV01], the legal regulation for electronic signatures and Certification Authorities in Germany. The new legal regulation includes the demand for evaluation of the voting system as well as the operational environment of the VSP similar to the security concept given in the Signature Ordinance. Here our catalogue of requirements can be used as basis for the evaluation of the operational environment of the VSP according to the legal regulation. Since we included the Protection Profile [BSI08] in our analyzed sources, its requirements for the voting system as well as for the operational environment are regarded in our recommended evaluation concept for VSPs. Thus our catalogue is a good choice for evaluating the operational environment of VSPs.

We conclude that a Common Criteria evaluation of the voting software combined with an IT-Grundschutz/ISO27001 evaluation of the operational environment based on the requirements from our catalogue, embedded in the legal regulation for e-voting and VSPs, is the most comprehensive evaluation approach for electronic elections so far. The result will be secure, trustworthy and legally binding electronic elections.

5 Conclusion

The result of our paper is a comprehensive catalogue of organizational and technical requirements that have to be fulfilled by the operational environment in order to enable secure electronic elections. We derived these requirements from a comprehensive analysis of relevant literature on security in e-voting. We point out that a further analysis might reveal even more detailed requirements. Possible methodologies could be a threat analysis based on attack trees [Sc99], or KORA, a method to translate abstract legal stipulations into concrete technical design concepts [HPR92]. We consider this as future work. Our paper extends our previous work where we derived requirements for the operational environment from e-voting protocols [LSB08].

Our findings can be used as a basis for evaluation of operational environments to analyze their suitability for operating secure electronic elections. We recommend an evaluation methodology based on IT-Grundschutz. We point out that secure electronic elections require both a secure voting protocol and a secure operational environment in which the voting system is operated. Consequently we recommend the evaluation of both parts. We show how the concept of the Voting Service Provider can facilitate this approach. The combined approach of a secure e-voting protocol embedded in a secure operational environment is an important step to enable secure electronic elections.

References

[Ba01] Baudron, O.; Fouque, P.A.; Pointcheval, D.; Stern, J.; Poupard, G.: Practical Multi-Candidate Election System. *PODC*, S. 274–283, 2001.

[BSI] BSI (German Federal Office for Information Security): IT–Grundschutz Zertifizierungsschema. http://www.bsi.de/gshb/zert/ISO27001/schema.htm.

[BSI05] BSI (German Federal Office for Information Security): IT–Grundschutz Catalogues, http://www.bsi.de/english/gshb/download/it-grundschutz-kataloge_2005_pdf_en.zip, 2005.

[BSI08] BSI (German Federal Office for Information Security): Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products. http://www.bsi.bund.de/cc/pplist/pplist.htm#PP0037, 2008.

[BSI07] BSI (German Federal Office for Information Security): Schutzprofil Digitales Wahlstift-System. http://www.bsi.de/cc/pplist/pplist.htm#PP0031, 2007.

[CCM07] Clarkson, M. R.; Chong, S.; Myers, A. C.: Civitas: A Secure Remote Voting System. Technical Report TR2007-2081, Cornell University, 2007.

[CC] The Common Criteria Portal (CC): http://www.commoncriteriaportal.org/.

[Co04] Council of Europe (CoE): Legal, Operational and Technical Standards for E-voting. Recommendation Rec(2004)11, http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_recommendation/Rec(2004)11_Eng_Evoting_and_Expl_Memo.pdf, 2004.

[SigV01] German Ordinance on Electronic Signatures (Signaturverordnung, SigV). http://bundesrecht.juris.de/sigv_2001/index.html, english translation: http://www.bundesnetzagentur.de/media/archive/3613.pdf, 2001.

[SigG01] German Signatures Law (Signaturgesetz, SigG). http://bundesrecht.juris.de/sigg_2001/index.html, english translation: http://www.bundesnetzagentur.de/media/archive/3612.pdf, 2001.

[GI05] GI (German Informatics Society): GI-Anforderungen an Internetbasierte Vereinswahlen. http://www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf, 2005.

[GI] GI (German Informatics Society): Wahlen und Ordnungen, http://www.gi-ev.de/wir-ueber-uns/leitung/wahlen-und-ordnungen/.

[HPR92] Hammer, V.; Pordesch, U.; Roßnagel, A.: KORA - eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme, Arbeitspapier 100, provet, Darmstadt, 1992.

[JCJ05] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-Resistant Electronic Elections. In WPES '05, In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, S. 61–70, ACM, 2005.

[Ki01] Kim, K.; Kim, J.; Lee, B.; Ahn, G.: 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, SSGRR2001, L'Aquila, Italy, 2001.

[LSB08] Langer, L.; Schmidt, A.; Buchmann, J.: Secure and Practical Online Elections via Voting Service Provider. In: Proceedings of ICEG 2008, S. 255-262, Academic Publishing, UK, 2008.

[LK02] Lee, B.; Kim, K.: Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer. In: Proceedings of ICISC 2002, Vol. 2587 of LNCS, S. 389–406, Springer, 2003.

[Oh99] Ohkubo, M., Miura, F., Abe, M., Fujioka, A. and Okamoto, T.: An Improvement on a Practical Secret Voting Scheme. In: ISW '99: Proceedings of the Second International Workshop on Information Security, Vol. 1729 of LNCS, S. 225–234, Springer, 1999.

[Sc99] Schneier, B.: Attack Trees. Dr. Dobb's Journal, 1999.