Independent Audits of Remote Electronic Voting: Developing a Common Criteria Protection Profile

Melanie Volkamer[1], Robert Krimmer[2], Rüdiger Grimm[3]

[1]Institute of IT-Security and Security Law (University of Passau)
Innstraße 41, D-94032 Passau, Germany
melanie.volkamer@uni-passau.de, www.isl.uni-passau.de

[2] Competence Center for Electronic Voting and Participation (E-Voting.CC)
Pyrkergasse 33/1/2, A-1190 Vienna, Austria
r.krimmer@e-voting.cc, www.e-voting.cc

[3]University of Koblenz, Research Group IT Risk Management
Universitätsstraße 1, D-56070 Koblenz, Germany
ruediger.grimm@uni-koblenz.de, www.uni-koblenz.de

This article presents the problem of independent evaluation of remote electronic voting systems and provides a solution based on the internationally agreed certification standard Common Criteria. The authors first discuss currently available approaches for the standardization of such systems and then explain the foundation and background of their own approach. The main part describes our core security requirements of remote electronic voting in form of a Common Criteria Protection Profile (including the defined assurance requirements). Finally the discussions and possible areas for improvement of the Protection Profile are presented.

1. Introduction

The fast development and uptake of the Internet in the 1990s led to the transformation of several processes in the field of business (e-Commerce) and public administration (e-Government). So it was mainly a matter of time until the idea of legally binding elections over the Internet emerged. Since the Democrats have tested remote electronic voting in the US Arizona primaries in spring 2000 [Solo04] more and more countries around the world tested and introduced legally binding remote electronic voting. The most prominent examples are the United Kingdom in 2002 and 2003 [Hepp04], the Netherlands [RIES04], Switzerland [BrBr06], and Estonia [MaMa06] providing nation-wide remote electronic voting with its 2007 national parliamentary election. After the practicability has been proven, it is now essential to ensure that remote electronic voting is secure. The main problem with electronic forms of voting is their lack of transparency. You can always trace and track a piece of paper directly and thereby fully understand the electoral process by natural senses when using paper. In contrast, electronic media are per-se not observable without the help of electronic instruments. This leads to an increase in public discomfort and lack of trust in the new forms of voting [OoBe04; Voll05].

In order to ensure the reliability of their systems, election officials use to invite experts to check the e-voting systems[1] for vulnerabilities. In general all experts use their own set of rules or requirements and the evaluation depth varies a lot. This leads to judgements about e-voting systems which are hardly comprehensible by third parties. Moreover, different sets of rules and requirements are not comparable. In order to understand and measure these rules and their implementations, standardized requirements, testing mechanisms, evaluation procedures, and observation techniques are needed. This paper presents a protection profile following the methodology of the Common Criteria (CC) [CC06]. It was written within the context of the German Federal Office for Information Security (BSI), in cooperation with the e-voting expert round of the German scientific association of informatics (GI).

2. Background

Discussions about the security of e-voting systems have often been led in a very emotional way. As long as we do not have a rigorous security model for electronic voting the security of an e-voting system can never be proven but only perceived secure until proven otherwise. This is sufficient with respect to the falsification principle of Karl Popper. But it is not sufficient with respect to the trust of the voters in their system. In order to reach confidence of the voters, developers and election operators have soon started to develop requirement documents which have often emerged to real standards.

Germany was one of the first to have legal regulations concerning the use and testing of mechanical voting machines. The „Regulation of voting machines" was set into place as a law in 1975 and was changed in 1999 [DE99] to allow electronic voting machines as well. In the United States the use of voting machines is decided on a district level which makes national standards on those machines hard to push. Still the IEEE made an effort with the „Project 1583" [SCC05] to develop such a standard in the aftermath of the 2000 Florida experiences. After a controversial debate about the draft standard, it finally was turned down and the working group is still trying to deliberate on the controversial issues. With the establishment of the Election Assistance Commission (EAC) in 2002 a new set of guidelines was developed in cooperation with the National Institute for Science and Technology that has led to the "Voluntary Voting System Guidelines" [VVSG05]. Recent discussions by the technical guidelines committee of the EAC concentrated on the inclusion of mandatory Voter Verifiable Audit Trails and recounts thereof into the next release of the VVSG [TGDC06].

For remote electronic voting one of the first discussions around requirements was the working group set up by US President Clinton in 2000 [IPI01]. The report of this working group defined a number of quality criteria for remote electronic voting. In the succession of the Arizona experiment another project evolved: the election mark-up language standard. This has been developed by companies engaged in electronic voting under the umbrella of the standardization organisation OASIS [EML05]. The German testing authority for physical devices, the *Physikalisch-Technische Bundesanstalt* (PTB), developed a criteria catalogue for networked polling stations in order to support the W.I.E.N. project [PTB04]. It uses a similar methodology like the one used for voting machines. The largest effort to come to a common understanding by a set of criteria for both – remote electronic voting and voting machines – has been conducted by the Council of Europe [CoE04]. With the help of delegates from all 48 member states it has

[1] Note that e-voting comprises the usage of voting machines and remote electronic voting systems.

developed a set of legal, operational and technical standards on electronic voting. It is the most comprehensive and universal international agreed standard to date.
In Germany the scientific association for informatics (GI), decided in 2004 to introduce remote electronic voting as the main channel for the elections of their board of chairpersons. Based on the standards then available [CoE04; PTB04; SCC05], they developed their own catalogue [GI05] in 2005. In parallel to this development the GI established an expert group with the task to use the Common Criteria methodology [CC06] in order to develop a Protection Profile on core requirements for remote electronic voting based on the same standards as used for the catalogue. The idea to apply the CC was already proposed in [CoE04] but not executed. Participants included academics, as well as representatives of relevant bodies like the BSI and the German *Bundesdatenschutzbeauftragter* (data protection office). The BSI subcontracted the PP to the German research centre of artificial intelligence (DFKI), which jointly developed it with the expert group. A report on this work of the group was published in [GKMR06]. The application of the CC has three advantages compared to existing standards: First of all the methodology is word-wide known and accepted. Secondly, the evaluation depth is clearly defined and the third advantages is the possibility to compare different systems based on their evaluation report. Moreover, we do not provide just another list of requirement but we tried to combine all the requirements from other catalogues in our Protection Profile.

3. CC-Introduction

The Common Criteria for Information Technology Security Evaluation (CC) [CC06] are an international standard (ISO 15408) for computer security. They distinguish between customers, developers and evaluators: Customers specify their security requirements, developers define the security attributes of their products and evaluators determine if products meet the claims. Independent of these three groups a certification authority certifies the related statements. The CC contains three parts: “Introduction and Common Model”, “Security Functional Requirements”, and “Security Assurance Requirements”: In addition, a Common Evaluation Methodology (CEM) is provided to exactly guide an evaluator. This makes the whole evaluation process very transparent. Customers specify their security requirements for a category of products – the so called Targets of Evaluation (TOE) – by developing a Protection Profile (PP). These requirements are independent of technical solutions. A PP has to a particular structure and go through a formal evaluation to ensure that it meets various syntactical and documentation rules as well as sanity checks. The evaluation is done by an accredited laboratory. Successfully evaluated PPs are accredited and receive an official certificate. For example, in Germany CC certificates are issued by the IT security authority BSI.
The evaluation insensitivity of the TOE evaluated according to a PP depends on the chosen security assurance requirements (SAR). The CCs predefine seven test depths so called Evaluation Assurance Levels (EALs) whereby level 1 is the lowest and level 7 the highest level. Level 4 is the highest level for typical commercial products and includes the source code evaluation. Level 5 and higher require more and more formal specification methods.

4. Protection Profile “Core Requirements for Remote Electronic Voting”

This chapter summarizes the content of the current version of the Protection Profile.

4.1 PP Introduction

A Protection Profile starts with the introduction part which contains an overview of the TOE. It helps a potential user of the PP to determine whether the PP is of interest or not.
Our PP relates to elections where votes must be cast secretly, but who has cast a vote does not have to be kept secret. It also addresses elections where it is intended that no voter is allowed to cast more than one vote (thus, not including re-voting) while one vote can contain more than one voting option; where the voters must be prevented from proving their vote; and where the calculation of intermediate results during the polling period must be prevented. Amendments to the list of eligible voters during the polling period are not dealt with. The only users involved are the election commission[2], the voter and the intruder. The TOE covers the server-side voting software including the stored data like ballot design and votes and the client-side voting software if available (it is not barred to use the web browser on the client-side).

4.2 Security Problem Definition

The security problem definition describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed, i.e. assumptions about the environment, threats, and organisational security policies.

4.2.1 Threats

T.UnauthorisedVoter: An unauthorised voter or a voter ineligible to vote casts a vote on the client-side TOE. (Motivation: he wants to manipulate the election result; exploited weakness: authentication process; target data: vote)

T.Proof: A voter eligible to vote uses data on his client device that are produced by the client-side TOE during the polling period to prove to a third party that he has voted in a certain way. (Motivation: He wants to prove to a third party how he has voted in order to be able to sell his vote; exploited weakness: files, messages or similar that the TOE produces on the client device. target data: vote)

T.IntegrityMessage: A network attacker intervenes directly in the network in order covertly to delete messages or to amend them selectively while they are in transmission or to generate new messages. (Motivation: He wants to manipulate the election result; exploited point of attack: network; target data: any message)

T.SecretMessage: A network attacker intervenes directly in the network in order to read messages relating to the election while they are in transmission (Motivation: He wants to break the secrecy of the election/extract identification relating to individual voters/manipulate the result of the election/calculate intermediate results; exploited point of attack: communication network; target data: vote/identification data)

T.WrongServer: A network attacker redirects the voter to a hoax (election) server. Hence, the voter does not communicate with the authentic election server. (Motivation: He wants to manipulate the election result/extract identification data/calculate intermediate results; exploited weakness: network; target data: ballot data/identification data/vote)

[2] In addition to the traditional poll workers, any technical staff including system administrators is a member of the election committee. These people needs to be nominated by the traditional poll workers.

T.after-Integrity: A person who has access to the data stored on the TOE after the "polling period including vote count" phase, alters the polling period data in order to influence the result of any recount. (Motivation: The election result is manipulated. exploited weakness: the TOE leaves the data unprotected once the final whistle[3] has been blown; target data: vote)

T.after-ElectionSecrecy: Any person who has access to the data stored on the TOE after the "polling period including vote count" phase can find out how a voter has cast his vote on the basis of the data stored in the TOE. (Motivation: To breach election secrecy; exploited weakness: the TOE leaves the data unprotected once the final whistle has been blown. Target data: vote)

4.2.2 Organisational Security Policies

P.Cancel: The voter must be able to interrupt the voting process on the TOE and to retain his right to vote when doing so.

P.EndElection: The election committee must be warned if they try to end the election before the final whistle time in order to prevent accidental, premature blowing of the final whistle. The election committee is still able to blow the final whistle prematurely.

P.after-BallotBox: After the final whistle, no more votes will be accepted.

P.ElectionSecrecyElectionCommittee: The election committee is not able to use the TOE to breach the secrecy of the election during[4] the polling period.

P.IntegrityElectionCommittee: The election committee is not able to add votes to the ballot box using the TOE. For our purpose the limitation to "using the TOE" is justified because of A.ElectionCommittee. Neither are they able to delete votes in the ballot box or selectively to edit them. In particular, no functions exist that allow the election committee to reset the TOE to its original state after the polling period has begun. Further, the election committee has no possibility to change the list of eligible voters to either allow a voter to cast more than one vote or to change authentication data. Moreover, they are not able to change the ballot data. Once the final whistle has been blown, the election committee can no longer initiate a restart.

P.SecretElectionCommittee: The election committee does not get knowledge of the authentication data. In addition, it must be ensured that the election committee cannot calculate any intermediate results.

P.OverhasteProtection: The TOE can only store votes in the ballot box that the voter has reviewed and confirmed.

P.Correction: No limit may be placed on the number of times that the voter can revise his vote before finally casting it. He must also be able to correct it after reviewing it.

P.Confirmation: The voter receives confirmation from the TOE that his vote was stored successfully. This happens as soon as the vote has been cast and whenever the voter logs in again.

P.Malfunction: The election committee must be able to recognise from the server-side TOE when a malfunction occurs.

P.Log: The listed events must be logged and the election committee must be able to view them:

- Storage of the election data at the start of the election,
- System errors as well as other reductions in the operability of the server-side TOE,
- Interruptions of communication,

[3] The final whistle refers to the termination of the voting process and the availability of the voting application.

[4] Here during the polling period is enough because later on, the problem fits to T.after-ElectionSecrecy

- Start and rerun of the election on the server-side TOE,
- Blowing of the final whistle,
- Start of the vote count,
- Determination of the vote count result.

P.OneVoterOneVote: It must be ensured that each voter can only cast one vote and that no voter unjustly loses his right to vote. This must be ensured especially in the case of aborts caused by the client-side TOE, the IT environment of the TOE or the network as well as malfunctions and restarts at the server-side TOE.

P.AuthElectionCommittee: The authentication function of the TOE must be such that it supports a separation of duty between a minimum of two members of the election committee. The TOE's functions can only be carried out once two members are logged in.

P.StartVoteCount: The election committee can not initiate the vote count until the final whistle is blown. Otherwise the election committee receives an error message.

P.VoteCount: All votes stored in the ballot box are correctly evaluated and are fed into the results.

4.2.3 Assumptions

A.Interface: It is assumed that the election data are properly and correctly installed on the TOE at the beginning of the polling period; that the ballot box is empty; that the election preparation phase has been correctly carried out and that the TOE is correctly initialised.

A.Observation: The voter ensures that nobody is watching him while he votes.

A.ElectionCommittee: The election committee accesses no data other than that on the TOE; i.e., it uses only the functions made available by the TOE.

A.AuthenticationData: The voter knows how to deal with his means of identification and authentication and is consistent in doing so; in particular that he doesn't allow them to fall into the hands of others.

A.ClientDevice: The voter acts responsibly in securing the client device. It is assumed that each voter that installs or uses the client-side TOE does so in such a way that the client device can neither observe nor influence the vote casting process. This includes the assumption that the voter not manipulate his client device.

A.ElectionServer: Protection of the election server against attacks that originate from the insecure network is provided.

A.Availability: The robustness, the quality of service and the availability of the network and of the election server are assumed.

A.ServerRoom: No-one other that the election committee, as appointed by the election organiser, gains entry to the server room or access to the election server for the duration of the polling period and until the vote count.

A.DataStorage: The data storage hardware is functioning correctly.

A.Clock: The correct time is made available by the server's IT environment.

4.3 Conformance Claim

This PP claims conformance with CC Version 3.1 Rel. 1. It is CC Part 2 and Part 3 conformant.

4.4 Security Objectives

The specification of security objectives is divided in those for the TOE and for its environment.

4.4.1 Security Objectives for the TOE (O)

O.UnauthorisedVoter: Only voters eligible to vote who are unmistakeably identified and authenticated by the TOE may cast a vote.

O.Proof: All data that the TOE makes available to the voter can not be used by the voter to prove his vote to third parties.

O.IntegrityMessage: The TOE must verify that the content of the authentication message, identification data, ballot data, vote records and the confirmation cannot covertly be deleted, inserted, replayed or amended during transmission (between the client-side and server-side TOE).

O.ElectionSecrecy: The TOE guarantees election secrecy during transmission; in other words it should not be possible to match the voter to his vote in plain text form. In particular, no conclusions about the number of crosses and/or their position on the vote, or whether it is valid or spoilt, can be drawn from the number or size of the messages.

O.SecretMessage: The TOE guarantees the trustworthiness of the identification data, the content of the authentication message and of the vote during transmission. Finally, this is necessary to deny the network attacker the possibility of calculating intermediate results.

O.WrongServer: The client-side TOE guarantees that it is communicating with the authentic server-side TOE and vice-versa.

O.after-Integrity: The TOE guarantees that the polling period data and the result are stored securely on the TOE once the vote count has taken place. Any changes are recognisable.

O.after-ElectionSecrecy: The data that remain on the election server following completion of the vote count do not allow anyone to see how a certain voter voted – especially encrypted votes, even where supplementary data such as decryption keys are used. A link between vote and voter may not be inferred from the order and/or time of storage of votes in the ballot box.

O.Cancel: The client-side TOE offers the voter a possibility to interrupt the voting process on the TOE and to retain his right to vote when doing such a cancellation.

O.EndElection: The TOE guarantees that the election committee does not accidentally blow the final whistle before the final whistle time. Following an explicit confirmation, the election committee is able to blow the final whistle prematurely.

O.after-BallotBox: The TOE guarantees that no votes are accepted after the final whistle has been blown.

O.SecretElectionCommittee: The TOE guarantees election secrecy on the election server during the polling period including the vote count. The election committee is not able to link voters to their plain text votes.

O.IntegrityElectionCommittee: The TOE guarantees that the election committee cannot insert votes into, or delete or amend votes in, the ballot box. In particular, it guarantees that the election committee cannot reset the TOE to its original state once the election has started. The TOE guarantees that the election committee is not in the position to allow any voter to cast more than one vote and that the election committee can change neither the authentication data in the list of eligible voters nor the ballot data. It is guaranteed that a restart is not possible once the final whistle has been blown.

O.SecretElectionCommittee: The TOE guarantees that the election committee cannot obtain any knowledge of the content of the authentication message. The TOE also guarantees that intermediate results cannot be calculated on the server-side TOE.

O.OverhasteProtection: The TOE will only accept a vote if the voter has explicitly double-checked and confirmed his vote. To this end, the vote is shown to him one more before the vote is finally cast.

O.Correction: The TOE places no limit on the number of corrections a voter can make to his vote before he finally casts it. The voter can correct the vote after it has been displayed for a second time.

O.Confirmation: The TOE allows the voter to check whether his vote has been stored in the ballot box. This means that the voter is presented with an on-screen confirmation once the vote has successfully been stored in the ballot box. Further, if a voter logs in again, the successful storage of his vote will be confirmed on the screen.

O.Malfunction: The election committee can recognise any malfunction on the server-side TOE.

O.Log: The TOE logs the events listed in P.Log and allows the election committee to view them.

O.OneVoterOneVote: The TOE guarantees that that can cast more than one vote and that nobody loses his right to vote without having case a vote. The TOE guarantees the right to vote especially in the case of an abort. This can be caused by a voter on the client-side TOE, the client-side TOE itself or the IT environment of the client-side TOE. The TOE also guarantees that where malfunctions to the server-side TOE occur, as well as to any subsequent restart and the execution of such restart, no data are lost and nobody loses his voting right or is allowed to cast more than one vote. The secrecy of the election is also preserved in these cases.

O.AuthElectionCommittee: The TOE possesses an authentication function that supports separation of duty between a minimum of two members of the election committee. Starting or ending the online election as well as initiating a restart requires two or more members of the election committee to be logged on. The initiating of the vote count is also conditional upon the same requirment being fulfilled. This provides a guarantee analogous to that of a conventional election where two members of the election committee can monitor one another.

O.StartVoteCount: The TOE guarantees that the election committee is only able to initiate the vote count once the final whistle has been blown.

O.VoteCount: The TOE guarantees, that all vote records that are stored in the ballot box after the final whistle has been blown are correctly evaluated (and, where necessary, correctly decrypted) and contribute to the result of the vote count.

4.4.2 Security Objectives for the Operational Environment (OE)

OE.Interface: The TOE voting process takes no account of the preparation phase; instead it relies on correctly prepared data. This includes in particular the election data, the identification data, the prepared ballot box and other data that might be necessary for the execution.

OE.Observation: The voter can cast his vote without being observed. This is the responsibility of the voter. The TOE cannot prevent somebody from looking over the voter’s shoulder while he is casting his vote.

OE.ElectionCommittee: The election committee accesses the data on the server-side TOE only through the the TOE. The election committee would be able to alter or exchange the TOE, which the TOE itself could neither diagnose nor prevent.

OE.AuthData: Only voters are in possession of the identification characteristics and authentication characteristics necessary to participate in the online election as checking for possession of such characteristics is the only way the TOE can ensure that only voters eligible to vote can cast votes.

OE.ClientDevice: The trustworthiness of the client device is the responsibility of the voter because the TOE is not able – nor does it have the authorisation – to scan the entire client device for malicious software nor to remove any malicious software from it.

OE.ElectionServer: The election committee carries out its responsibility to secure the election server in order to exclude the possibility that a network attacker gains access to the server. This can be achieved using up-to-date security technology (including through the use of secure operating systems and isolation of the server-side TOE from other software); hence, it cannot provided by the TOE.

OE.Availability: The TOE cannot influence the availability of the network. This must be sufficiently high to allow the voting process to take place. Likewise, the TOE has no influence on the availability of the election servers on which the TOE is installed. Server failure disables the entire election process, including the vote count and can call the final whistle time into question.

OE.ServerRoom: This objective guarantees that no unauthorised person can gain entry to the election room and access to the election server. This is necessary in order to exclude the possibility of the TOE being altered or exchanged. The TOE can neither diagnose nor prevent such attacks.

OE.Storage: The TOE uses at least the operating system and possibly other software – such as a database for placing votes in the ballot box – and, hence, is reliant on the correct functioning of this IT environment. Beyond that, no potential hazards eminate from the storage unit.

OE.Clock: The server-side TOE can rely on the server's system clock. This is necessary for the creation of reliable log entries and to establish whether the final whistle time has been reached.

OE.WrongServer: The voter verifies that he is communicating with the correct server-side TOE.

4.4.4 Security Objectives Rationale

In [PP07] it is specified which threats are averted and which security policies are ensured by which security objective and which assumptions matches which OE.

4.5 Security Requirements

The security requirements as part of the PP defines the detailed IT security requirements to be satisfied by the TOE or its environment. The requirements are predefined in the CC-catalogue.

4.5.1 Security Functional Requirements

The security functional requirements needed to cover all organisational security policies are: FAU_GEN.1 Security audit data generation; FAU_SAR.1 Security audit review; FDP_DAU.1 Data authentication; FDP_IFC.1 Information flow control policy; FDP_IFF.1 Information flow control functions; FDP_RIP.1 Residual information protection; FDP_UCT.1 Inter-TSF user data confidentiality transfer protection; FDP_UIT.1 Inter-TSF user data integrity transfer protection;

FIA_ATD.1 User attribute definition; FIA_UAU.1/2 User authentication; FIA_UID.1/2 User identification; FIA_USB.1 User-subject binding; FMT_MSA.3 Management of security attributes; FPR_ANO.1 Anonymity; FPR_UNL.1 Unlinkability; FPT_RCV.1/4 Trusted recovery; FPT_TST.1 TSF self test; FTP_TRP.1 Trusted path.

4.5.2 Security Assurance Requirements

The requirements for trustworthiness which the TOE must fulfil contain the components of trustworthiness level EAL 2 augmented from section three of the Common Criteria. The augmented classes are: ALC_CMC.3 Authorisation controls, ALC_CMS.3 Implementation representation CM coverage, ALC_DVS.1 Identification of security measures, ALC_LCD.1 Developer defined life-cycle model.

4.5.3 Security Requirements Rationale

The back-tracing of the security requirements to the security objectives is done in [PP07].

5. Discussions

The development of the PP was driven by regular feedback rounds with experts of different organisations including universities, ministries, administrations, product developers and data protection authorities. Major issues were the level of the EAL, whether to include or exclude observation, the point in time of voter's authentication within the electoral process, and the assumptions for the client's trustworthiness.
A general problem of a protection profile is the assignment of threats: which threats are specified as threats against the system and must be encountered by the Target of Evaluation, and which threats are shifted into "assumptions on the environment"? For example, we have decided not to require any security mechanisms of a remote electronic voting product against attacks on clients. Clients are assumed to be safe and secure. This is particularly manifested by the assumption A.AuthenticationData. This assumption is not globally realistic. However, the violation of this assumption does not affect the whole system, but only single clients. A voting procedure as a whole remains correct and other voters are not affected if this assumptionis not met in singular cases. The responsibility for safe and secure clients can be decentralized among the clients and the voting provider can help the clients with security manuals.
Another problem is the granularity of the protection profile. For example, we have discussed the exact point of user authentication. There are arguments for having the authentication only once, namely when logging into the system. Reasons are usability and anonymity. Other arguments require a fresh authentication immediately before the submission of the vote to the ballot box. This is mainly to support the interception of a session, for example by social engineering. We left this point open and required more roughly that the system must make sure that there is no unauthorized voter. So, the decision about the authentication point is left to the voting provider.
Some of the assumptions made in the assumptions section are questionable and need discussion especially for the application for Governmental Elections. For example, A.Observation has been widely violated in corrupt elections in the past. It does not threaten the value of the whole voting procedure that this assumption is not globally realistic, because it remains correct if this assumption is not met just in singular cases. Moreover, in traditional postal voting, the

assumption A.Observation is as weak as in this protection profile. We decided to keep this assumption on the same level as the postal voting which is even accepted by legally highly protected governmental elections.
A more serious threat to the whole system is a possible violation of the assumption A.ServerRoom, which requires that no unauthorised person has access to the election server. In fact, unauthorised modification of the service procedure may corrupt the voting result. The physical and digital access to any server lies outside the remote electronic voting product itself, which is a server application. Therefore, we shift this requirement to the voting provider as an assumption to the environment. For the duration of the polling period, physical entry to the server room must be controlled. Digital access to the server must be prevented by ordinary access control mechanisms like strong user authentication and intrusion detection and prevention. This is in the PP a duty of the service team. The separation of duty on the voting server side is not yet demanded but necessary to take into account. Therefore in [VoKr07] the application of k-resilience for the evaluation of online-voting systems in addition to the Common Criteria is proposed.

6. Conclusion

This article covers the procedures and discussions of the development of the Protection Profile. It contains the defined threats, the organisational security policies, assumptions, the security objectives for the environment and for the TOE as well as the security functional and assurance requirements. In addition to what a PP usually contains the group added an appendix with a guideline for the election authority how to conduct an election using remote electronic voting systems.
The Protection Profile has been evaluated successfully by the testing authority Security Research & Consulting (SRC) in the first quarter of 2007 but needs the final certification by the BSI which is expected in the second quarter of 2007. Afterwards it serves as a contribution to the international community and can be used for certification of remote electronic voting systems in any country around the world that has adopted the Common Criteria. From our point of view, this contribution is a good starting point but needs to be edited and exchanged after having evaluated the first systems against this PP. There are currently two companies planning to evaluate their systems: Micromata and T-Systems.
Currently, the proposed PP covers a kernel of security requirements which is essential for all applications, but it does not cover the full range of requirements for all applications. The kernel is already sufficient for elections in a private environment. However, for governmental elections it has to be extended based on further experiences to be made.

Acknowledgement: *The authors would like to thank the members of the expert group, namely Kai Rannenberg, Kai Reinhard, Jörg Helbach, Nils Meissner, Marcel Weinand, Tobias Scherner, and Walter Ernestus for the fruitful discussions and feedback during the work on the PP. Further acknowledgements go to the GI and Cornelia Winter for their continuous support.*

8. Reference

[BrBr06] Braun, N., Brändli, D. (2006): Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed, in: Krimmer, R. (ed.), Electronic Voting 2006, (Vol. P-87) Gesellschaft für Informatik, Bonn, pp. 27-35.

[CC06] Common Criteria Project (2006): Common Criteria for Information Technology Security Evaluation, v3.1, http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2 accessed on 2007-04-11.

[CoE04] Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommundation Rec(2004)11 and explanatory memorandum, Council of Europe, Strassbourg, pp. 87.

[DE99] Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland, 1999.

[EML05] OASIS (2005): Election Markup Language v.4, http://xml.coverpages.org/eml.html accessed on 2007-04-11.

[GI05] Gesellschaft für Informatik (2005): Anforderungen an Internetbasierte Vereinswahlen, Informatik Spektrum, Vol. 28, Nr. 5, pp. 432-435.

[GKMR06] Grimm, R., Krimmer, R., Meißner, N., Reinhard, K., Volkamer, M., and Weinand, M. (2006): Security Requirements for Non-Political Internet Voting, in: Krimmer, R. (ed.), Electronic Voting 2006, (Vol. P-87) GI, Bonn, pp. 203-212.

[Hepp04] Heppner, B. (2004): Electronic Voting in the United Kingdom, Thesis WU, Vienna.

[IPI01] 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, pp. 54.

[MaMa06] Madise, Ü., 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, (Vol. P-87) GI, Bonn, pp. 27-35.

[OoBe04] Oostveen, A.-M., Besselar, P. v. d. (2004): Security as Belief. Users' Perceptions on the Security of E-Voting Systems, Proceedings of the ESF TED Workshop on Electronic Voting in Europe, Schloss Hofen/Bregenz, pp. 73-82.

[PP07] Volkamer, M., Vogt, R. (2007): Protection Profile - Core Requirements for Online Voting Systems, Saarbrücken.

[PTB04] Hartmann, V., Meißner, N., and Richter, D. (2004): Online Voting Systems for Non-parliamentary Elections: Catalogue of Requirements, Berlin: Nr. 8.5-2004-1.

[RIES04] Hubbers, E., Jacobs, B., and Pieters, W. (2004): RIES - Internet Voting in Action (Technical report: NIII-R0449), Amsterdam: Radboud University Nijmegen.

[SCC05] IEEE Standards Coordinating Committee 38 (2005): Voting Standards: Project 1583 - Voting Equipment Standard, Project 1622 - Electronic Data Interchange, http://grouper.ieee.org/groups/scc38/index.htm accessed on 2007-04-11.

[Solo04] Solop, F. I. (2004): Digital Democracy Comes of Age: Internet Voting and the 2000 Arizona Democratic Primary Election, in: Kersting, N. and Baldersheim, H. (eds.), Electronic Voting and Democracy (Palgrave, London, pp. 242-254.

[TGDC06] Technical Guidelines Development Committee (2006): Plenary Meeting, December 4-5, 2006, http://vote.nist.gov/meeting20061204.htm accessed on 2007-04-11.

[Voll05] Vollan, K. (2005): Observing Electronic Voting (15): NORDEM.

[VoKr07] Volkamer, M. and Krimmer, R. (2007): Requirements and Evaluation Techniques for Online Voting", In Proceedings of the EGOV Conference 2007, Regensburg.

[VVSG05] Election Assistance Commission (2005): Voluntary Voting System Guidelines v1.0, Washington.