Verifiability and Other Technical Requirements for Online Voting Systems

Niels Meißner, Volker Hartmann, Dieter Richter

Department of Metrological Information Technology
Physikalisch-Technische Bundesanstalt (PTB), Braunschweig and Berlin
Abbestraße 2 – 12
10587 Berlin, GERMANY
{Nils.Meissner | Volker.Hartmann | Dieter.Richter}@ptb.de

Abstract: When developing a catalogue of technical requirements for online voting systems to be used in legally ruled, non-parliamentary elections, major interdisciplinary problems arise which currently cannot be solved. Technical requirements are not yet definable due to lacking legal preconditions, and legal definitions are not yet definable due to lacking technical experience. Problems of this type are the role of a technically necessary intermediate storage of votes, the so-called last call problem and the general problem of ensuring verifiability. The problem of verifiability is discussed from the technical point of view to bring forward a possible solution[1].

1 Introduction

There are numerous application areas in which technical systems are subject to legal verification. The general aim is the protection of users, consumers or customers, respectively, who are usually not able to assess all possible risks. Electronic voting is one of those areas, and even a very sensitive one. Other areas are e.g. measuring systems used in commercial transactions and private households, and gaming systems.

Technical requirements play a key role in the management of regulated areas. Although in their shape of a technical nature, they are the most important interface between regulators and technicians, between developers and testers, between manufacturers and customers.

Looking at the situation in the area of electronic voting systems and, in particular, of online voting systems, it can be stated that there are several approaches to define requirements for online voting systems [JO00; UK02; NV02; CH03; US01; CE04]. In general, their state can be characterised as relatively general or not complete.

---

[1] The work is funded by the German Federal Ministry of Economics and Labour under the registration mark 01 MD 248.

This was the reason for taking the initiative to elaborate technical requirements for online voting systems. This initiative is embedded in a project of PTB funded by the German government, which aims at the development of concepts for testing and certifying online voting systems to be used in legally regulated, but non-parliamentary elections (e.g. elections of shop committees, staff councils, shareholder elections).

This paper aims in its main part, section 4, at the problem of verifiability as one of the major problems of online voting systems. Before, in section 2, the catalogue of requirements is briefly explained. The catalogue has been developed at PTB and discussed in two national working groups. One of these groups is dealing with technical aspects of testing and certification, the other one with legal aspects. In section 3, major interdisciplinary problems are described which were fixed in discussions in the two working groups.

2 The catalogue of requirements

The catalogue of requirements [HM04] gives criteria which are to be met by online voting systems. Its purpose is to set a technical standard which can serve as an orientation for both, developers and examiners of online voting systems. Well-defined requirements are, in particular, a precondition for the examination and certification of systems, which have to be performed carefully in order to build confidence in the systems.

Even though the state of the art is progressing both from the technical point of view and as regards the acceptance of online voting systems by society, the catalogue is intended to provide some guidance on the requirements presently acceptable.

The second reason for developing the catalogue is to contribute to the ongoing discussions on online voting systems. The document represents expertise and opinions from different backgrounds in Germany. It may be considered as a reference for further activities.

The scope of application is given by legally ruled non-parliamentary elections. The requirements are also applicable to any other non-parliamentary type of election not regulated by law, whereas one or another requirement might be weakened. As to the application in parliamentary elections, the authors are convinced that most of the requirements are also valid. Particular analysis, however, is necessary to decide on potential extensions of the requirements.

For the definition of the requirements, it has been assumed that elections take place exclusively at supervised and networked polling stations. Applications allowing voting from at home or any other private place are explicitly not included in the definition.

3 Selected Legal Questions

Basically, any set of technical requirements represents a certain interpretation of the general legal requirements given. An interpretation shall follow as close as possible the initial legal intention. However, if the general legal requirements are not yet defined or only very roughly defined – as it is the case with some aspects of online voting systems – then problems arise with the definition and harmonisation of technical requirements. Three major problems of this type are described in the following subsections.

3.1 The role of an intermediate storage

Online voting systems have a feature that is unknown in conventional voting systems: It is the physical state of an (encrypted) vote after having finally completed its electronic casting at the voting terminal and before putting it into the electronic ballot box. This state may last only a fraction of a second but can also, in case of a communication interruption, last for several minutes or even hours. In the latter case, the vote must be stored and held ready for communication in an intermediate storage. An intermediate storage could also be regarded as a conceptual element of the voting system used, for instance for the management of a certain vote transfer protocol.

The main question that arises concerns the legal definition of an intermediate storage. One may ask what the intermediate storage is from the legal point of view? Is it an episode of the vote transfer process, is it already part of an extended ballot box or is it still part of the vote casting? The answer to these questions has an impact not only on the technical requirements for an intermediate storage but also on the answers to related questions as e.g. with respect to the registration of vote casting in the list of voters, feedback from a successful input into a ballot box to the voter.

3.2 The last call problem

A special problem of voting systems with distributed components is the harmonisation of the beginning and the end of the vote casting. Aside from the clear definition of deadlines to be given for the vote casting, the closing procedure must be defined. In particular, it must be ensured that no vote that has been cast regularly within the defined deadlines will be excluded from vote counting. This means that the ballot box must not be closed for the reception of further votes until it has been ensured that no further regular vote is “in the air.”

The technical solution relates to the solution of an intermediate storage described in the previous subsection. The legal problem is to what extent the solution of the last call problem must be prescribed. This question is very sensitive because complaints directed against the incompleteness of votes considered due to a technical failure of the system are very likely. The general aim from the legal point of view is to ensure and prove the completeness and correctness of an election result. The proof shall pass a verification. In so far, the last call problem is a special aspect of a more general problem of verifiability described in the next subsection.

3.3 Verifiability

Verifiability is an essential feature of an election demanded by electoral jurists. It is linked with such aspects as confidence in the election, transparency and preparation for a possible contestation of the election. There are different types of verification. The difference may be characterised by the groups of persons who are authorised to access the information gathered for verification (audit information). The variation reaches from everybody interested (public verifiability) to voters, election officials only and independent auditors to court only. A verification by court is usually caused by complaints that the results of an election were not correct or that the election has not been executed according to the rules.

In general, the technical problem can be described as the definition of the necessary technical measures that are required to pass a verification. So far, however, there is neither a definition nor any practical experience as to what kind of technical proof and evidence is sufficient for a verification. This explains the difficulty technicians and legal experts are currently facing.

4 Selected problem: Ensuring verifiability

4.1 Basic considerations

Basically, the verifiability is, on the one hand, a matter of designing a technical audit and, on the other hand, a question of correctness proofs. An audit needs to be specified with respect to, e.g., the information content to be observed and logged, data structures, security measures, etc. Correctness proofs are closely related to the anonymisation methods used. A basic principle that must be regarded and must never be violated is the sanctity of the anonymity.

As regards the audit, approaches are known from auditing sensitive systems. In particular, the security of audit logs is well treated in literature [BE97; CP03; GA87]. However, so far no specific approach for electronic voting systems is known. It seems to be clear that an auditing must address two aspects: the path that a vote takes through the network-based online voting system and the technical states of the components of the electronic system during the whole voting process. In particular, all abnormal technical states must be logged in order to be able later to judge whether the conformity of rules was kept.

An approach currently discussed in the USA is the so-called paper audit trail. The content of the vote is printed before the vote casting is finally completed. Then the correctness can be verified by the voter. If everything is correct, the print-out is put into an additional ballot box and the electronic vote is stored. In case of a contestation of the election, the paper ballots can be counted separately and used for the verification. This principle results in an additional complexity and source of errors such as, for example, jamming of printer paper, empty printer cartridge, etc. In addition, in case of a contestation, the lengthy, fault-prone hand counting remains.

This approach will not be further discussed here. Rather, initial ideas are outlined how the audit can be organised with the blind signature type encryption and with the homomorphic encryption type.

4.2 Principle applicable for systems using blind signature encryption type

Some systems [IV02; KK02] use blinded signatures [CH83] to secure the anonymity of the votes (Figure 1). [IV02] works as follows: After having identified and authenticated the voter, he/she gets signed electoral documents from the election server. The signature is necessary to ensure the protection of data integrity. After having filled in the ballot, the voter blinds the vote, i.e. he/she multiplies the data by a random number and sends the thus blinded vote back to the election server. The server signs the blind vote without being able to see the voting decision and sends it back to the voter. The voter removes the blinding, i.e. he/she divides the blind signature by the blinding factor to get a signature of his vote. He/she then encrypts the vote and the signature with the public key of the tallier and sends the data to the ballot box. Either the transmission takes place anonymously or the vote is made anonymous by the ballot box server stripping away voter ID information. After having closed the vote casting, the anonymous votes and signatures are sent to the tallier which decrypts them separately. Only votes with a valid signature of the election server are counted.

In the algorithm in [KK02], two tokens and not the vote are blindly signed in the registration phase. These signed anonymous tokens allow the voter to receive the ballot and vote anonymously later in the voting phase.

Unlike the systems that use homomorphic encryption (see 4.3), these systems have no inherent verification mechanism. Therefore an additional mechanism has to be embedded to ensure verifiability.

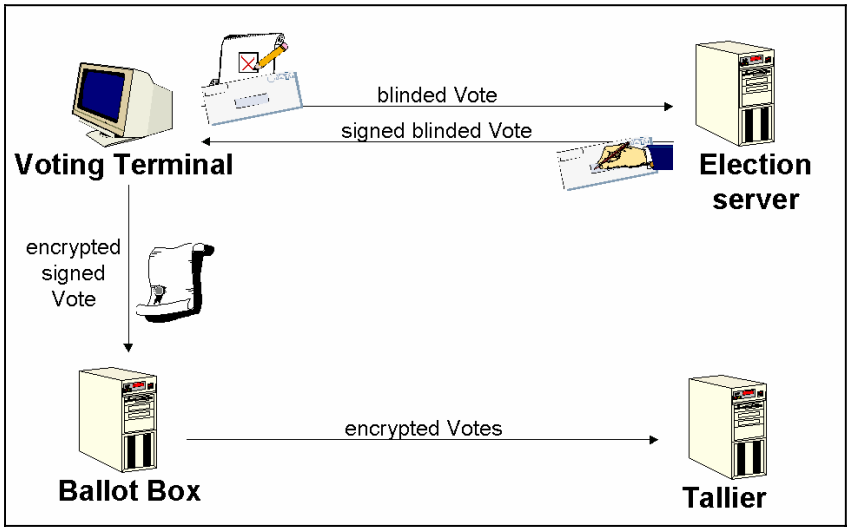

Figure 1: Schematic view of an Online Voting System using blind signatures

For the support of the verification, additional information and effort are necessary. A possible approach is illustrated in Figure 2. This figure shows how the proper execution of the election can be documented. The basic idea is to design an audit data set, which is logged with all single steps during the "lifetime" of a vote. A part of this audit data set is a token, which serves for the identification of the individual vote cast.

This token is generated at the time when the voter has been accepted as eligible for voting. Simultaneously, it is encrypted with the public key of the auditor and inserted into the audit data set. This structure is signed and sent to the voter together with the electoral documents (ballot, etc.). From this moment, the audit data set accompanies the encrypted vote. At each relevant point passed by the vote data, the audit data set is enriched with the necessary audit information and signed again by the appropriate entity. When reaching the ballot box, the audit data set is separated from the vote data and stored separately. To guarantee verifiability, the audit data sets are sent to the audit box during or after the election and the tokens are decrypted. With this information, each individual vote casting can be reconstructed by using the token and the signed audit information.

The anonymity of the vote is not endangered because of the strict separation of the audit data from the content of the vote through encryption. The information content of the audit data to be gathered depends on the subject of possible verifications and may be adapted to the particular needs. The correct counting of the votes, however, cannot be verified by the approach developed here.

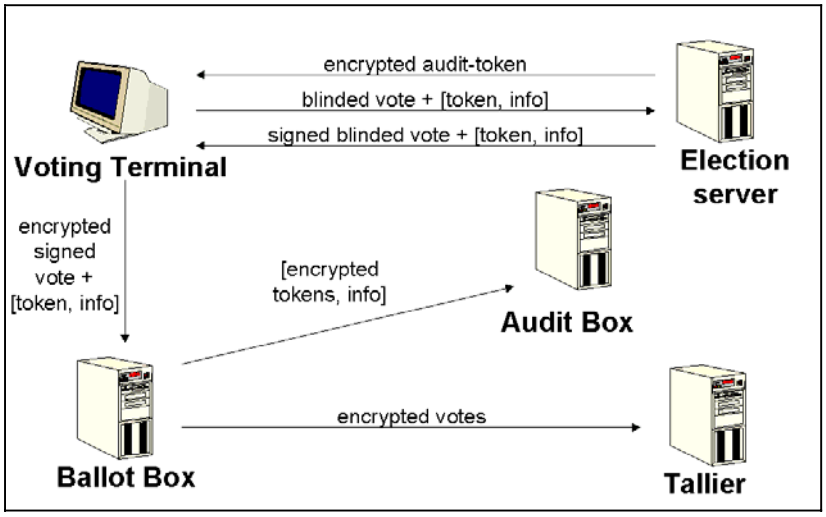

Figure 2: Schematic view of the audit data set approach

4.3 Principle applicable for systems using a homomorphic encryption type

Voting systems using homomorphic encryption [CY99; VH02; CG97], Figure 3), work with a communication model called bulletin board. It is a public broadcast channel with memory. All information sent to the bulletin board is readable by everyone. Every authorised user can add messages to his own area, but no one can delete any data from the board.

The central element of the homomorphic encryption is the feasibility to sum up data without encrypting them, i.e. without knowing the exact content of the data. This is a feature that is typical of the principle of homomorphism. More precisely speaking, the homomorphic encryption ensures the mathematical law that the product of encrypted data is the encryption of the sum of the data:

$$Enc(v_1) *...* Enc(v_n) = Enc(v_1 +...+ v_n).$$

The method works as follows: Before the election, the talliers generate distributed asymmetric keys (e.g., [PE91; GJ99], threshold cryptography). These keys are a single public encryption key and for each tallier a secret decryption key. To decrypt a message encrypted with the public key, more than at least half of the secret keys have to be used. Therefore more than half of the talliers would have to be corrupted in order to break the anonymity or manipulate the election result.

Only authenticated voters are allowed to write on the bulletin board. The voters send their votes encrypted with the public part of the distributed key to the bulletin board, together with a zero knowledge proof of correctness. After the voting phase, the talliers take all the encrypted votes from the bulletin board and form their homomorphic sum. Afterwards this sum is decrypted using the distributed parts of the key and sent to the bulletin board with proofs of correctness of the summation and the decryption. By skilful

application of zero knowledge proofs, and because everybody (even external observers) can read the information on the bulletin board, everyone can verify the correctness of the results. This includes the correct summation and the completeness of votes included.

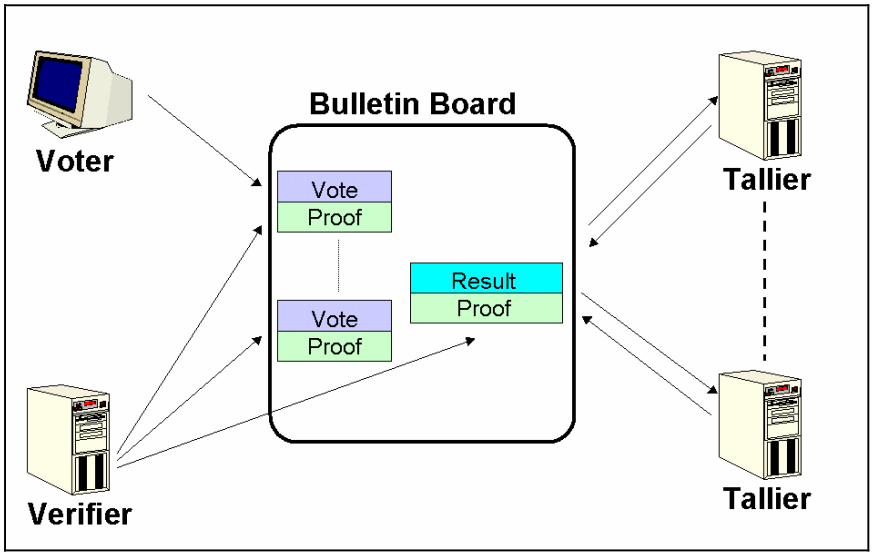

Figure 3: Schematic view of an online voting system using homomorphic encryption

Online voting systems with homomorphic encryption secure, in particular, the casting of correctly formed votes as well as a correct counting. This is verifiable during the election, and, in addition, remains verifiable after the election. However, this encryption type cannot monitor the proper execution of the election. In order to trace the execution, an additional audit logging is necessary. Since the information on the bulletin board can be used for verification, less information is probably needed for the audit logging compared with systems that use blind signatures.

5 Conclusions

Technical requirements of online voting systems have been developed and discussed in a community with different expertise and experience. There are still several unsolved interdisciplinary legal and technical problems left. Sufficient technical experience does not yet exist to decide profoundly on the respective legal aspects. Vice versa, there is no clear legally defined background as an initial point to solve the technical problems. This looks like a deadlock situation. From the technical point of view, this situation can be overcome step by step by assuming certain legal conditions required, then specifying the technical issue to be dealt with and implementing corresponding components or methods. From the experience gathered, feedback can be given to evaluate and adapt the initial legal assumptions. This is the way that has been chosen with the discussion of verifiability in section 4. A new technical approach to ensure the verifiability of voting systems that use blind signatures was presented.

References

[BE97] M. Bellare, B. S. Yee: Forward Integrity For Secure Audit Logs, 1997, http://www.loganalysis.org/sections/research/fi.pdf

[CE04] Council of Europe: Draft - Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, http://www.coe.int/t/e/integrated_projects/ democracy/02_Activities/02_e-voting/

[CG97] R. Cramer, R. Gennaro, B. Schoenmakers: A secure and Optimally Efficient Multi-Authority Election Scheme, Advances in Cryptology – EUROCRYPT'97, Vol. 1233 Lecture Notes in Computer Science, Springer Verlag, 1997, pp. 103-118

[CH83] D. Chaum: Blind signatures for untraceable payments., Advances in Cryptology – Crypto'82, Plenum Press, 1983, pp. 199-203

[CH03] Verordnung über die politischen Rechte vom 24. Mai 1978 (as of 28 January 2003), 161.11, http://www.admin.ch/ch/d/sr/161_11/

[CP03] C. N. Chong, Z. Peng, P. H. Hartel: Secure Audit Logging with Tamper-resistant Hardware, SEC 2003, 73-84, http://www.ub.utwente.nl/webdocs/ctit/1/00000099.pdf

[CY99] CyberVote, an innovative cyber voting system for Internet terminals and mobile phones, IST-1999-20338, www.eucybervote.org/reports.html

[GA87] P. R. Gallagher: A Guide to Understanding Audit in Trusted Systems, NATIONAL COMPUTER SECURITY CENTER, NCSC-TG-001, VERSION-2, Library No. S-228,470, 1987, www.radium.ncsc.mil/tpep/library/ rainbow/NCSC-TG-001-2.pdf

[GJ99] Gennaro, Jarecki, Krawczyk, Rabin: Secure Distributed Key Generation for Discrete-Log Based Cryptosystems, Advances in Cryptology – EUROCRYPT'99, Vol. 1592 Lecture Notes in Computer Science, Springer Verlag, 1999, pp. 295-310

[HM04] V. Hartmann, N. Meißner, D. Richter: Online Voting Systems for Non-parliamentary Elections - Catalogue of Requirements, PTB, 2004, work in progress

[IV02] Erste verbindliche Online-Wahl im LDS – Abschlussbericht über Online-Personalratswahl im Landesbetrieb für Datenverarbeitung und Statistik (LDS) Brandenburg im Mai 2002, www.i-vote.de

[JO00] B. Jones: California Internet Voting Task Force, A Report on the Feasibility of Internet Voting, January, 2000, www.ss.ca.gov/executive/ivote/

[KK02] R. Kofler, R. Krimmer, A: Prosser: Electronic Voting: Algorithmic and Implementation Issues, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), 2002

[NV02] Network Voting System Standards (Public draft 2 – 12.04.2002), VoteHere, Inc. www.fec.gov/pages/vss/comments/NetworkVotingSystemStandards.pdf

[PE91] T. Pedersen: A threshold cryptosystem without a trusted party., Advances in Cryptology – EUROCRYPT'91, Vol. 547 Lecture Notes in Computer Science, Springer Verlag, 1991, pp. 522-526

[UK02] e-Voting Technical Security Requirements, Issue 1.0, 08 November 2002, X/10049/4600/6/21, Crown Copyright, http://www.odpm.gov.uk/stellent/groups/ odpm_localgov/documents/page/odpm_locgov_605209.pdf

[US01] Voting System Standards, 2001, www.fec.gov/pages/vss/vss.html

[VH02] www.votehere.net (Demo, www.votehere.net/products_rv.htm#demo)