Online Voting Project – New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles

Klaus Diehl, Sonja Weddeling

T-Systems Enterprise Services GmbH
Onlinevoting
Pfnorstr. 1
64293, Darmstadt, Germany
{klaus.diehl | sonja.weddeling}@t-system.com

Abstract: For several years, T-Systems Enterprise Services GmbH has been researching the creation of a highly secure voting system that meets the latest cryptological standards. With exclusive responsibility for the W.I.E.N (Wählen in elektronischen Netzwerken, Voting in electronic networks) research project supported by the government since 2005, T-Systems are studying the implementation of online voting in non-parliamentary elections. The voting system previously designed in this project was subjected to a thorough review by a renowned cryptologist from a German university in the summer of 2005. Some encryption processes were then modified, resulting in a highly secure voting protocol with the provisional working title of t-voting, which is simpler and quicker to implement. By adding important new steps within the core architecture, the strenuously disputed claims to the publicness of voting and its transparency are demonstrated. A public notice displayed on the bulletin board gives voters an overview of votes cast. Considering that online voting is seen as an alternative to postal voting, this actually increases the element of being "public". The principle of universality is augmented in online voting as the access options are simplified, which means that more voters can participate in the election.

1 Introduction

Since 2001, T-Systems has been researching the creation of a highly secure voting system that is virtually fraud- and interference-proof from cryptological perspectives with the assistance of the PTB (*Physikalisch Technische Bundesanstalt* - national metrology institute providing scientific and technical services) and other prominent institutes. T-Systems has been exclusively responsible for the W.I.E.N (*Wählen in elektronischen Netzwerken*, Voting in electronic networks) research project supported by the Federal Ministry of Economics and Labour since the start of 2005. This project involved the implementation of online voting at networked polling stations in non-parliamentary elections and its examination from a legal, technical and organizational viewpoint. During this project, past experiences in the field of electronic voting were

documented. In fall of last year, the voting system developed in the W.I.E.N. project using renowned cryptologists underwent a security review. The scientists came to the conclusion that the workflow of the core architecture was too laborious in various places and also contained security flaws. After a report was produced, the voting system was extended to include important cryptological add-on modules and the client-server architecture optimized. The result is a modified voting system core that incorporates state-of-the-art technical security and has been co-developed by the PTB. The environment of the voting system, which affects voting preparation, implementation and post-processing, has remained unchanged, as has the credo of an information-based division of powers and the use of blind signatures. The voting system being developed by W.I.E.N. was completed at the start of 2006, thereby concluding the project.

The newly developed and implemented voting system should now undergo a certification process based on the common criteria as per the ISO/IEC 15048 standard in cooperation with an accredited testing centre and the BSI (*Bundesamt für Sicherheit in der Informationstechnik,* Federal Office for Information Security). It is initially planned to create the protection profile, which is subdivided into three individual protection profiles relating to voting preparation, implementation and post-processing. The legislative instances for non-parliamentary elections in particular, e.g. work council elections, staff council elections and social security elections should be integrated early on. Once these protection profiles are created, they should be certified by the BSI to form the basis for their registration. When this process has been concluded successfully, an evaluation of the system in view of the previously established requirements is planned. Lastly, the voting system should be certified on the basis of the common criteria and also be subject to a comprehensive check by the PTB simultaneously to create a basis for legal legitimization.

In addition, the voting system developed in W.I.E.N., which is limited to the voting of networked polling stations, was and is being extended to include a remote voting system. The security requirements of such a system should first be examined and defined, and based on the results obtained software engineering should be the next step. The online voting project will perform business management studies of remote voting and the creation of its legal basis in parallel.

2 Adherence to Voting Legislation Principles

2.1 Voting legislation principles for publicly regulated elections with emphasis on the publicness of the election

For the analysis of the legal principles of elections, the voting legislation principles of Art. 38 of the Constitution of Federal Republic of Germany, federal, state and municipal voting laws and regulations for non-political elections (staff council, social security and works council elections) must be applied. The first principle is that of **universality**, in which the electronic voting must be equated to postal voting. A general election is one in which all citizens can participate regardless of their status or gender, and no voters are

excluded from voting unwarrantedly. Through improved access options such as e.g. the remote voting procedure which take account of the increased mobility and individualization of voters, the principle of universality is increased. The next principle is that of **directness**, which means that all entitled voters – without the interposition of electors - must cast their vote in the polling station themselves. There must be no further contact between voters and electoral candidates after voting. This voting principle generally poses no problems for Internet voting. Another principle is **freedom** of election, which means no pressure of any kind can be exerted on the voters, such as bans, sanctions or discrimination, to force them to participate in the election or to cast their vote for a specific party. Freedom of election is protected by the principle of confidentiality. The principle of freedom also includes permitting the possibility of casting an intentionally invalid vote. Next is the principle of **equality**, which means that all voters have the same number of votes with the same count and success value. The last principle refers to the **secrecy** of election. All voters must be able to cast their vote such that no-one can determine how they are voting or have voted. Voters must therefore be unobserved while casting their vote. In addition to the voting legislation principles expressly mentioned in Art. 38 I of the Constitution, there are unwritten constitutional voting principles, for political elections at any rate: publicness of election, simultaneity, comprehensibility and freedom of charge. The **publicness** of the voting process including the monitoring of the voting result is one of the most important tools for adhering to the principle of liberty. Publicness permits transparency and monitoring in elections and is necessary for all voting stages. This begins with voting preparations: polling dates and locations are publicized, the parties present their candidates publicly, electoral registers are displayed publicly and polling stations are made publicly accessible. Voting itself is a public act, but the casting of votes is secret. Finally, the determination of the election result and its publicization are also public. Votes are counted by the members of the electoral committee at a public meeting. The process of obtaining the voting result of both votes cast in person and the postal vote must be traceable for all citizens. Publicness must therefore also apply to the determination of the result.[1] Public monitoring is performed by the electoral committee, but also by any member of the public who attends. Remote Internet voting from a computer at home removes the location of voting from public view and should therefore primarily be used only as an addition to voting at the polling station.

The principle of **comprehensibility** of an election means that the act of voting must generally be simple and traceable for voters. If voting machines are used, the electoral committee must be provided with as much training material and technical expertise to allow it to guarantee and monitor the correctness of the voting process, which is its duty. Voters must also examine the casting of votes using voting machines.

[1] [KA04], p. 29.

Another point is the **simultaneity** of voting, which is still strenuously disputed in postal voting. There is a distinct advantage to Internet voting here, as in comparison to postal voting, which is generally a pre-vote, this permits the simultaneity of votes cast in person and remote voting.[2] Lastly, **freedom of charge** of election is an element of the democratic principle – voters must not incur a cost through exercising their democratic right to vote.

2.2 The new voting system and voting legislation principles

Public monitoring of digital voting both in person and remotely is problematic. From constitutional perspectives, the replacement of visual and comprehension monitoring by electoral boards and other members of the public (as witnesses etc.) is not possible.[3]

The voting system developed previously in the W.I.E.N. research project conformed to the principles of the Federal Electoral Law, which was implemented through the information-based division of powers and the use of reliable voter identification via a qualified digital signature.[4] By adding the bulletin board in the modified voting protocol, the strenuously disputed claims to publicness of election and its transparency can now be demonstrated. A public notice displayed using the bulletin board gives voters an overview of votes cast and can track voting live on the Internet if the electoral organizer wishes. Considering that online voting is seen as an alternative to postal voting, this actually increases the element of publicness. The principle of universality is increased in online voting as the access options are simplified, which means that more voters, including e.g. those impeded due to professional or health reasons, can participate in the election.

The public must be able to monitor the correct implementation of the election at all times. For this reason, they have read access to all content on the bulletin board. Only the voter status is not visible here if voting policy precludes this, which is to be assumed. The bulletin board is a passive data memory. This means that it cannot record or establish any proprietary communications. In this context, the bulletin board is viewed more as an instance as it does not participate in the newly introduced T-Voting voting procedure like the other roles. The role of the bulletin board is to make all necessary information available for implementing the voting process, taking this entitlement and access concept into account. As with a bulletin board, the data can be either read or written here depending on the rights of participants. Due to the restrictive nature of this concept, it is not possible to subsequently modify data that has already been written.

The role of the public refers to e.g. the following groups of people in works council elections:

- Entitled voters
- Unions represented in the company, or the relevant union representatives
- Employers

---

[2] [KA04], p. 34.
[3] [KA04], p. 30
[4] [BB00], p. 4.

During the voting preparation phase, the public has the option of contesting the electoral register. The 'notice' of the electronic electoral register and the process for contesting the register are already regulated in the applicable electoral regulations of the Works Constitution Act. During the voting stage, the public have no access to the data on the bulletin board. The participation of the public in the vote counting process, which is subdivided in turn into the mixing of votes and the subsequent counting of votes, is possible. The vote result can be published via the bulletin board for the user group of the public role after the votes have been counted.[5]

Public participation in the physical counting of votes is not possible due to restrictions of the medium as the votes are tallied by a computer program. However, to perform the entire process of electronic vote counting with the involvement of the public, once the electronic ballot box is closed vote counting is introduced with the process of vote mixing and the subsequent counting of votes by projecting attendance and determining the result at the polling station.

3 Technical Modification of the Voting System

3.1 Previous Voting Protocol

The voting protocol devised previously in W.I.E.N. was based on the voting protocol developed in 1993 by Fujioka, Okamoto and Ohta entitled "A practical secret voting scheme for large scale elections"[6]. This voting system primarily entails the physical and administrative separation of the electoral register and electronic ballot box. Specifically, the W.I.E.N. voting system consisted of four server services which are each linked with a database for storing persistent data. The relevant data memories, which are relational databases in their basic structure, were:

Distributor The distributor is used as a server service for transmitting the electronic constituency data. Using this, voters can connect to the authorized electronic electoral register (Validator) and the assigned electronic ballot box (Psephor) via the voting clients

Mandator In an election with voter ID/voter passport as a form of identification, the Mandator is responsible for outputting the keys of the voter

Validator The Validator provides the electronic electoral register for a specific election. Voters can also use the server service to log into the electronic voting system. The electoral office server releases the voting documents (ballot slips). It also confirms the blind vote.

[5] [PO06], p. 12 ff.
[6] [FU93], p. 244-251.

Psephor The data model of the Psephor contains the electronic ballot box. It manages the encrypted electronic votes and releases the ballot record in counting mode.

Voting client The voting client is used to determine the identity of voters, display the ballot slip, control communications, conceal and reveal information, and cast votes.

The voting protocol propagates the use of a blind signature procedure and other cryptographic procedures that protect cast votes from manipulation and unauthorized viewing. This voting protocol is still based on an encryption using public and private codes. Online voters are uniquely identified using a qualified digital signature.

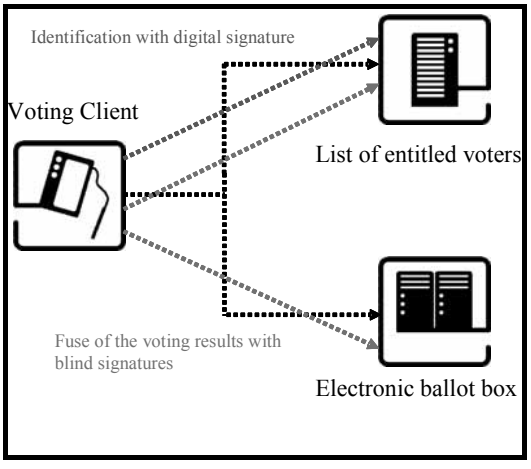

Figure 1: Principle of information-based division of powers

3.2 Newly implemented voting protocol

The voting system previously designed in this project was subjected to a thorough review by a renowned cryptologist from a German university in the summer of 2005. Some encryption processes were then modified, resulting in a highly secure voting protocol with the provisional working title of t-voting, which is simpler and easier to implement. However, the main principles of the previously developed architecture and the technologies used have remained the same.

The voter list server that issues voters with vote confirmation certificates using a blind signature[7] was also retained. Parts of the newly implemented cryptological techniques were examined back in spring 2005 using several voting tests and a legally valid test vote. In spring 2006, this voting system is also to be used for several works council elections and an Executive Staff Representation Committee election in the Deutsche Telekom group. Significant new developments include the addition of further participants. As a result, there is an interposed mix net, which separates the encrypted votes cast from the identity of the voter and stores these in random order. In addition, a bulletin board was integrated that acts as a bulletin board and shows the votes cast for everyone to see. Everyone can read messages published, but only authorized parties can store messages there. It is still not possible for anyone to delete or overwrite messages once they are written. Another element is the connection of a Tallier, which is responsible for counting the encrypted votes as a separate instance. All new developments were connected to the existing voting environment, including the administration modes.

[7] cf. [CH84]

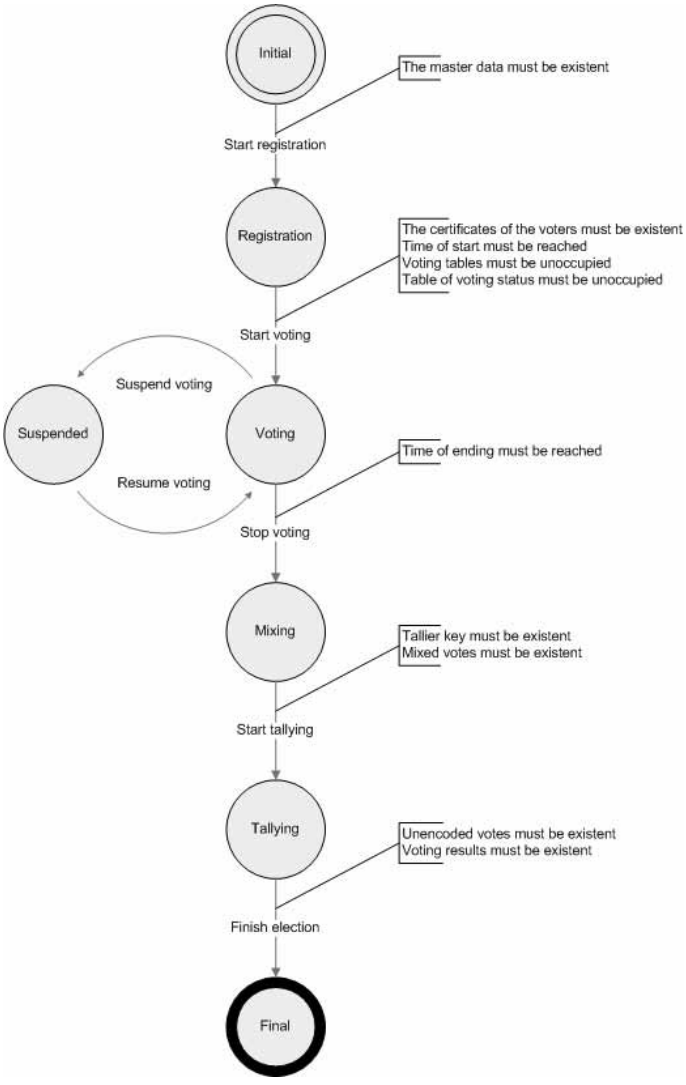

Figure 2: T-Voting phase model

The security requirements for electronic voting systems are not standardized, but science is agreed on a certain number of requirements:

Accuracy:

- A valid vote cannot be changed
- All valid votes are counted
- Invalid votes are not counted

Democracy:

- Only entitled voters can vote
- Each voter casts only one vote

Confidentiality:

- Anonymity: It is not possible to link a vote to a voter
- Untraceability: No voter can prove that he/she cast a specific vote
- A voter cannot be forced to cast a specific vote
- All votes remain secret up to the end of the election

Verifiability:

- Universal: Everyone can verify that all valid votes were counted
- Individual: All voters can verify that their valid vote was counted

The protocol uses blind signatures as per David Chaum. This mechanism prevents the signatory from being able to read the message to be signed. Another anonymization technique is the mix net as per David Chaum. Essentially, a mix net receives a number of messages, encrypts them and forwards the new messages in random order. The network thereby breaks the link between the incoming and outgoing messages. To ensure confidentiality and authentication, public key systems are used, e.g. RSA from Ron Rivest et al.

The system requires the following assumptions:

A trustworthy Public Key Infrastructure (PKI) is available and is used. All public keys are validated. A certification office issues relevant PKI certificates. This implies that all encryptions are performed using the correct public keys. All parties participate in the PKI. The cryptography used is strong and virtually unbreakable.

For communication, a protocol such as e.g. TCP/IP is used that secures the arrival of messages. We also assume that communication is protected by a protocol such as e.g. PKI-based TLS, which guarantees the reciprocal authentication of parties and the confidentiality of communications.

The registration stage is completed correctly.

There is trustworthy access control of the voting booth. This ensures that only entitled voters enter the booth, and that there is only one person in the booth at a time. The booth is constructed so that it is impossible to observe the voting process. This includes side-channel attacks (e.g. via power usage analysis).

The voting booth, mix net and bulletin board are considered trustworthy.

The voter, Validator and Tallier are not trustworthy. A valid vote is one that is in the correct form, is signed by the Validator, is encrypted in the correct order using the public key of the counter and the mix net, and is published on the bulletin board.

4 Conclusions

Through changes to the voting system developed previously in the Online Voting Project, most legal reservations against electronic voting were rebutted. The voting protocol became simpler and faster to implement, but most significantly now offers better integration of the general public through the use of a bulletin board. Previously existing technical security flaws were also eliminated. This brings us one step closer to our objective of making electronic voting feasible at networked polling stations in the short term and using any terminals without any technical, legal or organization problems in the medium to long term. We are assuming that online elections in non-parliamentary elections in Germany are now within the realms of possibility.

References

[BB00] Stephan Breidenbach and Alexander Blankenagel. Rechtliche Probleme von Internetwahlen. Berlin 2000.

[BU05] R. Araujo, A. Wiesmaier and Johannes Buchmann. The T-Vote Protocol. Darmstadt 2005.

[CH84] David Chaum. Blind signature system. In David Chaum, editor, Advances in cryptology: Proceedings of Crypto ’83, pages 153–156, New York, USA, 1984.

[FU93] Atsushi Fujioka, Tatsuaki Okamoto and Kazui Ohta. A practical secret voting scheme for large scale elections. In: Jennifer Seberry and Yuliang Zheng (Publisher) Advances in Cryptology - AUSCRYPT '92, Edition 718 der Lecture Notes in Computer Science, Page 244—251. Springer Verlag. Berlin 1993.

[KA04] Ulrich Karpen. Gutachtliche Stellungnahme zu elektronischen Wahlen. Hamburg 2004.

[PO06] Projekt Onlinewahlen, T-Systems Enterprise Services. Berechtigungs- and Zugriffskonzept Bulletin Board - Szenario: Betriebsratswahl. Darmstadt 2006.

[RI04] Volker Hartmann, Nils Meißner and Dieter Richter. Online-Wahlsysteme für nicht-parlamentarische Wahlen: Anforderungskatalog. Physikalisch Technische Bundesanstalt. Berlin 2004.