Vote Casting in any preferred Constituency: A new Voting Channel

[1]Jurlind Budurushi, [2]Maria Henning, and [1]Melanie Volkamer

[1] CASED / TU Darmstadt, Germany
[2] provet, Universität Kassel, Germany
{jurlind.budurushi,melanie.volkamer}@cased.de,
{maria.henning}@uni-kassel.de
[1]http://www.secuso.cased.de
[2]http://www.uni-kassel.de/fb07/institute/iwr/

Abstract. In our society a rising number of people change their residence regularly. Insofar, mobility seems to be necessary even on Election Day, which is the reason why an increasing number of eligible voters use the opportunity of postal voting. Thereby, the abidance by the election principles, especially the freedom and secrecy of elections, is automatically transferred into the private sector. This would not be necessary if eligible voters had the possibility to cast their vote in any preferred constituency within the electoral area. Therefore, we investigate in this work if and how vote casting in any constituency can be constitutionally compliant, while maintaining the current electoral system. We also consider the integration of the new German electronic ID card for voter identification and authentication.

1 Introduction

The use of various services over the Internet is part of many peoples' everyday life. Through this, it is no longer required that the individual is present at a particular time or place to conduct its business. The need for this kind of mobility exists independent of special events, thus also on Election Day. For this reason, some countries provide postal voting in order to enable as many people as possible to participate in the election. Postal voting was established in Germany in 1956 with the third Federal Electoral Act [7]. Through this, voters who were not able to visit a polling station because of health reasons or any other issues were enabled to cast their vote at home. While in 1957 only 4,9 % used this option, for the elections to the 17$^{\text{th}}$ German Bundestag in 2009, about 21,4 % took the opportunity of postal voting (ref. to Table 1 in [2]). The increase of postal voters may be justified due to both: the rising mobility of the citizens, and the relaxation of application requirements for postal voting. But the shift of a democratic legitimized election to the private sector raises the question whether

postal voting in its present form is still constitutionally compliant and in particular if it complies with the public nature of elections [25]. However, postal voting is an indispensable opportunity for voters, who cannot be present in the polling station of their constituency because of health reasons or for those that cannot be in the election area on Election Day. In contrast, voters who are able to visit a constituency within the electoral area should be offered the additional opportunity to cast their vote in any preferred constituency. Through this new voting channel, voters would be as mobile and flexible as when using the opportunity of postal voting, but they would cast their vote in an environment that is controlled by the electoral committee. In addition the compliance with the election principles would be guaranteed.

In the following, we consider vote casting in any preferred constituency in the context of the elections for the German Bundestag on Election Day. Thereby, we investigate different possibilities of this new voting channel. Furthermore, we identify the advantages and disadvantages and compare all possibilities against each other from a legal and technical perspective. We do not aspire to change or suggest changes concerning the German electoral system, which means the composition of the German Bundestag and vote casting by selecting a candidate and the list of a party. While maintaining the current electoral system but voting from any constituency, two issues should be considered carefully: one is how to authenticate voters that vote in foreign constituencies and provide them with the respective ballot, and the other one is how to return the ballot to the local constituency in order to tally the votes.

This work considers legal implications of allowing voters to cast their vote from any constituency in Germany and respective technical solutions in order to realise this ambition. The findings of this work might also apply in countries that have similar legal requirements to Germany, especially member countries of the European Union (EU). However, legal requirements might be slightly different even within the EU. Therefore, a similar analysis, which could consider or could be based on this work, must be conducted for each country, individually.

2 General possibility of Vote Casting in any preferred Constituency

According to § 1.2 in conjunction with § 2.2 Federal Electoral Act the territory of Germany is divided into 299 electoral districts. Every electoral district is subdivided into constituencies. Thus, constituencies are the lowest spatial division of the electoral area from an organisational point of view (ref. to § 2, m.n. 5 in [29]). They are important in the context of casting the votes because they define the place where to do so. According to § 14.2 Federal Electoral Act, voters can cast their vote only in that constituency, in whose electoral register they are recorded in. According to § 14.3 a) Federal Electoral Act, the casting of votes in any preferred constituency within the electoral district requires the ownership of

a ballot record which is only given in case of applying for it within a prescribed period.[3]

The casting of votes in any preferred constituency of the electoral area is not compatible with the current regulations of electoral law. However, this is owned to the election process and not to the constitutional regulations. For instance, Article 38.1 sentence 1 of the Basic Law does not require that eligible voters cast their votes only in the constituency they are registered in. In case the checking of the eligibility to vote is guaranteed and it can be ensured that every eligible voter casts his or her vote only once and personally (see section 3), voters shall be able to cast their vote in any preferred constituency, not only in the one they are registered in. As the election system shall be maintained, it must be ensured that the cast vote is tallied in the constituency the respective voter is related to (see section 4).

3 Checking of Eligibility

The following remarks apply in case voters cast their vote in the constituency they are assigned to or in any preferred constituency.

3.1 Ballot Record

Voting by people from foreign constituencies could be made dependent on the submission of a ballot record. Insofar, it could be referred to the current regulations, whereas the grant of a ballot record is possible only on request, § 17.2 Federal Electoral Act, and voting by submission of a ballot record requires the presentation of an official identity document, § 59 Federal Electoral Code. Thus, in contrast to § 14.3 a) of the Federal Electoral Act, the possession of a ballot record would qualify for vote casting in any preferred constituency within the electoral area (and not only within the electoral district). This approach has the advantage that no new infrastructure is required in order to check the eligibility of voters in a foreign constituency. In that regard, the existing electoral registers can be used for checking the eligibility of voters in a foreign constituency, similar to postal voting. Those voters who have applied for a ballot record could cast their vote in any preferred constituency. Those who have not applied for a ballot record could cast their vote only in the constituency they are registered in.

However, this approach also has a number of disadvantages (which exist in the current implementation as well, but would affect a larger number of voters in our approach): The voter loses her right to vote in case she loses the ballot record. Furthermore, a coercer could conduct a forced-abstention attack by requiring the voter to hand out the ballot record. Both threats also exist in the current election system. Voters, who have received a ballot record and lost it subsequently, cannot refer to the issuance of it. The replacement of a lost ballot record is generally

[3] A ballot record entitles the voter to do postal voting or to cast her vote in any constituency within the electoral district. For further information please see section 3.1.

not considered in order to prevent a double vote (ref. to § 17, m.n. 15 in [29]). According to § 28.10 sentence 2 of the Federal Electoral Code, a new ballot record can be issued only with a credible assurance of a lack of access until 12 o'clock the day prior to the election. A further disadvantage of this approach is that only voters who have applied for a paper record within the prescribed period are able to cast their vote in an optional constituency. This could be solved by sending paper records to all eligible voters. However, this would strengthen all the disadvantages outlined above.

3.2 Centralised / Decentralised Electoral Register

If voting in any preferred constituency was provided the electoral committee could - according to the current regulations - only check the eligibility of voters registered in the respective electoral register. Thus, for checking the eligibility to vote of voters from foreign constituencies, the electoral committee would have to check the electoral register of the constituency the voter is registered in - easier to implement - a centralised electoral register[4], if this is legally permitted and feasible.

A centralised electoral register could easily be produced in the presence of a centralised Federal Register of Residents. However, a centralised Federal Register of Residents is neither provided in the current Framework Registration Act [8] nor in the Registration System Act for further development of the registration system, which passed the Germany Bundestag on 6/28/2012 but stands in a conciliation committee at the moment [11]. A draft which was written by a consultant and published on 12/6/2007 [24] focused the application of a centralised Federal Register of Residents. However, this concept was rejected by various data privacy experts. The criticism was not against such a register in general, but explicitly against the number and type of data, which were listed and considered in § 3 of the draft to be stored in the register. This includes an unjustifiable intervention in the law of informational self-determination, which results from Article 2.1 in conjunction with Article 1.1 Basic Law. Therefore, the establishment of a centralised electoral register cannot be fundamentally rejected. According to the principle of dedicated use in the Data Protection Law, voters' personal data may be used only for the specified purpose, namely to check the eligibility to vote. Beyond that, the centralised electoral register may store only that data which is required to check the eligibility to vote: first- and surname, birthday and current residential address.[5]

[4] The information on the centralised electoral register (server) can be replicated among several servers in order to avoid a single point of failure.

[5] The electoral registers get compiled on the basis of the population registers stored in the registry offices. Insofar, the surname, the first name, the date of birth and the residential address of eligible voters are transferred from one register to another one.

3.3 Voter Identification and Authentication, and Access to the Electoral Register

Classical Voter Identification and Authentication (I/A) Verification of the eligibility to vote requires a prior identification and authentication of the citizen. Currently eligible voters are notified in writing about their registration in the electoral register. This election notification also serves as a proof of identity (ref. to § 14, m.n. 9 in [29]). According to § 56.3 of the Federal Electoral Code, voters shall submit the election notification on demand of the electoral committee. In case they do not submit the election notification, they must identify themselves. The submission of the election notification and the identification document is not necessary in any case, but at the behest of the electoral committee. It is not required in case of personal acquaintance between the voter and the electoral committee. However, the Federal Electoral Code does not permit the inference, whether a particular identity document shall be submitted. In that regard, each official document needs to be sufficient in order to provide a proof of identity. Therefore, the document should include a photo, as otherwise the verification of the identity is not guaranteed.

Electronic Electoral Register (EER) The right to vote can be checked against the voters personal data, which are stored on the de-/centralised electoral register. The transmission of personal data from the registration office to public authorities is already intended in § 18 Framework Registration Act and § 34 Registration System Act in case the personal data is necessary to fulfill their jurisdiction or necessary by the jurisdiction of the receiver to fulfill its corresponding tasks. In addition, according to § 14.1 sentence 2 Federal Electoral Code, the electoral register can be maintained through an automatic process as well.

The transmission of voters' personal data, namely first- and surname and current residential address, is necessary in order to check if the citizen is eligible to vote and whether he or she already cast a vote. The personal data could be transferred over a secured communication channel, for instance over telephone or Internet, which is already intended according to § 39.3 Registration System Act. The use of a telephone is impractical and therefore not further considered in this work. The access to the electoral register over the Internet would be secured by the application of standard cryptographic protocols for secure communication, like SSL/TLS [31]. The main disadvantages of an electronic electoral register, which is accessible over the Internet, are DoS/DDoS attacks. However, there are a number of techniques in order to mitigate such attacks, e.g. as presented in [30] and [21].

Regarding the transmission of personal data it is questionable, whether the electoral committee, as the receiver of the mentioned data, can be classified as a public authority in the context of the outlined regulations. On one hand, the municipal authorities carry out the statutory work assigned by the Federal Electoral Act on behalf of the federal government (ref. to No. 43 in [29]). On the other hand the electoral committee acts as an election body for the municipal

authority. Insofar the personal data of voters could be transferred to the electoral committee directly. Thus, the access of the electoral committee to electoral registers of other constituencies is not generally forbidden.

EER and Classical Voter I/A By checking the eligibility to vote over the Internet and maintaining the classical identification and authentication of voters, the electoral committee would have to enter the necessary data of the voter manually. The personal data of the voter could be taken by the presented document, captured electronically and sent as a request to check the eligibility to vote for the respective voter.

With this form of checking the eligibility to vote, a corresponding Public Key Infrastructure (PKI) [19] needs to be provided in order to ensure secure transmission of the personal data. This introduces additional costs. Another disadvantage of this approach is that the personal data transferred is confidential and secure only until the provided cryptographic encryption scheme is secure. Thus, an attacker who intercepts the encrypted personal data, which is transferred over the network, is able to determine who has participated in the election and who has not. Furthermore, this could violate the secrecy of the vote, depending on whether the ballot is electronically transferred and how it is transferred.

EER and (German) Electronic Identity Card for Voter I/A Electronic identity cards (e-ID cards) have been already used in electronic voting for legally binding elections. Hereby, the most prominent examples are Estonia [12] and Austria [1]. Furthermore, the use of e-ID cards in electronic voting has been proposed in many scientific works, for instance [3], [4], [9], [20] and [26], and has been also analysed in [6]. In particular, the authors in [3] and [4] propose the use of the German electronic identity card "Der neue Personalausweis" (German e-ID card) in electronic voting.

Thus, the eligibility to vote could also be checked with the German e-ID card. The German e-ID card enables, due to its data fields, shown in Figure 1, and particularly due to its eID-Functionality, the so-called Restricted-ID, a unique service-related online authentication [16].

Furthermore, the German e-ID card supports age verification, a query of the place of residence and a pseudonymisation (Restricted-ID). These functionalities could be used for checking the eligibility to vote as they provide the necessary data, which can be compared to the corresponding personal data stored in the electoral register. Figure 2 shows an abstract infrastructure and the interaction between the involved components.

By using the Restricted-ID functionality, neither the PC of the electoral committee[6] nor the electoral register would know for which voter the eligibility to vote is being checked. The electoral register can respond to the request, if a Restricted-ID (voter) is eligible to vote or not, without knowing the particular

[6] In Germany the authorisation of voters and the tallying of votes is carried out at the constituency where votes have been cast.

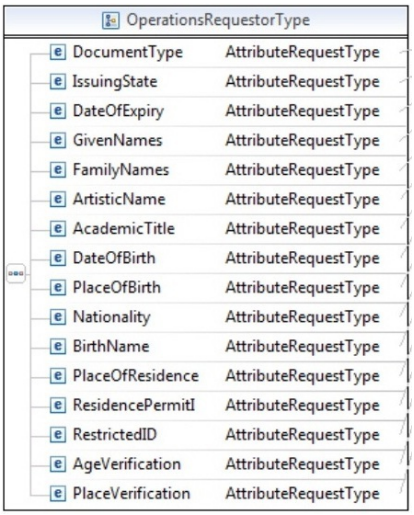

Fig. 1. Data fields of the German e-ID card (Source: [17], Figure. 13).

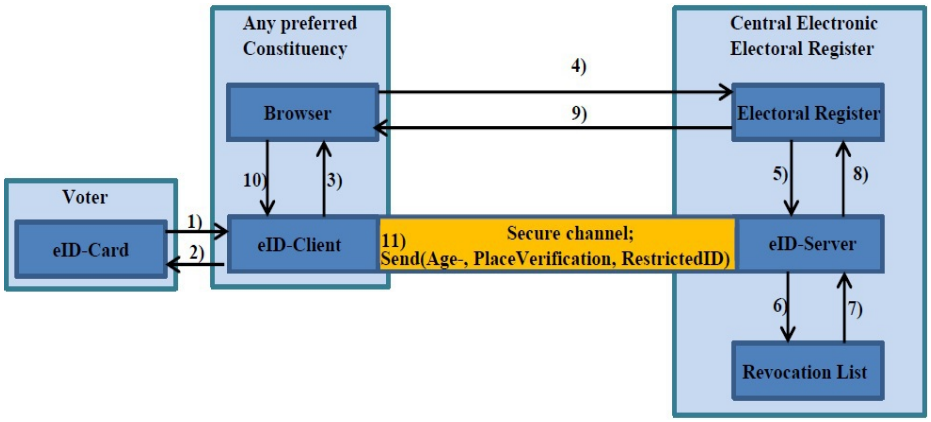

Fig. 2. Abstract Infrastructure and Interaction between involved Components.

voter behind the Restricted-ID. However, the identity of the voter could be revealed in case the cryptographic algorithms, which are used for the generation of the Restricted-ID and for securing the Internet communication, are broken. Besides intercepting the data transferred over the network to the electoral register, an attacker also needs to know the public key of each German e-ID card and the public key of the electoral register (eID-Server) [17].

Furthermore, if the electoral register (eID-Server) and the Certification Authority of the German e-ID cards cooperate, even today they can assign each Restricted-ID stored on the electoral register to the identity of the voter [4]. Therefore, storing the Restricted-IDs on the electoral server permanently must be forbidden and the deletion of the stored Restricted-IDs must be verified by the corresponding data protection expert. A long-term storage of data might only be acceptable in case of a pending complaint requesting the scrutiny of an election. However, the storage must be set up by the Federal Returning Officer and controlled by the responsible data protection expert.

The authentication with the German e-ID card has a number of advantages with respect to data privacy in comparison with the classical approach. Instead of the voter's personal data a pseudonym is transferred over the network. As the Restricted-ID is unique in the context of the election, a voter trying to vote more than once will easily be detected. Furthermore, citizens who have lost their right to vote according to § 13 of the Federal Electoral Act can easily be identified as well. Therefore, the so-called Country Verifying Certificate Authority (CVCA) can publish a corresponding revocation list, which contains all election-specific Restricted-IDs that are not allowed to exercise their right to vote. Depending on the implementation, the successful checking of the eligibility to vote could either be accepted by the electoral committee or by a voting machine which then might enable the voter to start the vote casting process.

In addition, the electoral committee is not expected to enter the personal data of voters manually, which is error prone and time consuming. However, it must be considered that currently not all citizens are in possession of a German e-ID card and therefore not all citizens can use the German e-ID card in the context of checking their eligibility to vote. But the authentication with the German e-ID card could optionally be offered to those eligible voters, who already possess this document and have activated the eID-Functionality. Although, the principle of the equal elections requires that every citizen shall be able to exercise his right to vote in the same formal way (besides the equality of counter value and result value), this does not mean that there can be only one option for vote casting. In that regard, postal voting provides a different way of voting too but it is constitutionally compatible since it is offered as an option and it strengthens the principle of universal elections (ref. to page 125 in [13]). Finally, it has to be said that since 11/1/2010 citizens applying for an identification document only receive the German e-ID card. However, there is no obligation to exchange the "old" identity card. According to identity card law (ref. to § 6.1 in [22]), German identity cards are valid for ten years. Therefore, "old" identity cards will be present until 10/31/2020. After this date, all eligible voters shall possess

a German e-ID card and could subsequently use it for authentication, if the eID-Functionality has been activated. However, even after 10/31/2020, an additional option besides the German e-ID card must be provided for identification and authentication.

A regulation, which requires that voters can only be identified by providing the German e-ID card, is not compatible with Article 38.1 sentence 1 Basic Law because it violates the principle of universal elections. Thus, it is possible that voters lose their German e-ID card just before the election or the German e-ID card is stolen or missing. Therefore, the submission of another official document which is suitable and intended for proving the identity of the owner shall be considered. Since the election technique proposed in this work allows vote casting in any preferred constituency within the electoral area, the identification document must contain the place of residence of the voter as well. This is necessary in order to identify the corresponding electoral district, thus the votes will count for the intended candidates. In this context, a German driving license is not appropriate because it does not provide information of the place of residence of the owner. Thus, the election notification could still be sent to all eligible voters in order to enable identification and authentication. The personal data of voters on the election notification could be entered manually into the system by the electoral committee. This is not objectionable from a legal point of view, because according to § 14.1 sentence 2 Federal Electoral Code, the electoral register can be maintained through an automatic process. Thereby, it must be ensured that necessary data for checking the eligibility to vote is used only for the intended purpose and can be transferred securely, for instance, by using cryptography.

Table 1 summarizes the advantages and disadvantages of using manual (Poll Workers) or automatic (German e-ID card) electronic voters' identification and authentication.

Table 1. Manual v.s. automatic electronic voters' identification and authentication.

Manually (Poll Workers)	**Automatically (German e-ID)**
Advantages	*Disadvantages*
Compliant with the principle of universal elections	- (not all citizens posses it)
Disadvantages	*Advantages*
Not long-term secure	+ (adversary needs more effort)
Error prone	+
Time consuming	+
–	Transmit a pseudonym instead of voter's identity
–	Neither the PC of the electoral committee nor the electoral register knows the voter's identity
–	Eligibility check can be performed by the electronic voting machine

4 Vote Casting and Tallying

While maintaining the current election system and providing vote casting in any preferred constituency, it must be ensured that each voter is provided with the corresponding ballot of her constituency and that her vote is also counted in her constituency.

4.1 Paper Ballot

In case vote casting is still done with paper ballots, there are two possibilities to provide the corresponding voting ballot: either each constituency keeps enough paper ballots from all electoral districts or the electoral committee prints the corresponding paper ballot on demand. The first approach requires that each constituency provides enough paper ballots from all electoral districts in order to enable vote casting for all eligible voters. This approach appears impractical, because in Germany there are approximately 299 different ballots, and therefore not further considered. The tallying of votes can take place either in the constituency, where the voter casts her vote or in the constituency the voter is registered in. The first option violates the principle of the secret ballot in case only one voter (or few voters) casts her vote in a foreign constituency. In this case, the electoral committee knows what the respective voter voted for. The second approach requires that the paper ballot is sent to the constituency the voter is assigned to. Sending the paper ballot by post is not recommended because of the associated time delay. Another possibility would be to transfer the paper ballot electronically over the Internet. In that regard, the only remaining option is to scan and subsequently transfer the paper ballot to the respective constituency. In order to ensure the principle of free and secret elections the paper ballots would have to be scanned and transferred by the voter personally. Afterwards, the electronically recorded ballot must be encrypted right after scanning and transferred to the respective constituency over a secure channel, e.g. using standard cryptographic protocols for secure communication over the Internet, like SSL/TLS[7]. The votes (cast paper ballots) of other constituencies must finally be sent to a central location, whereas ballot secrecy must be ensured, for instance similar to postal voting.

This approach can be implemented in two ways: either using canonical ballots or encoded ballots, like in [27], [23], and [10]. In the canonical ballot approach, two major disadvantages are identified: First, electronic emissions might leak the voter's choice, thereby violating ballot secrecy. Second, it is technically not possible for the voter to verify, if the scanner has encrypted and sent her cast vote without changing it. The major disadvantage in the encoded ballot approach are the costs for special purpose equipment, special printers that are able to print scratch fields, like in [27], or two layered paper ballots, like in [23]. Furthermore, the verifiability of the proper ballot encoding is difficult to implement,

[7] In this context, tow technical "unresolved" issues must be considered: First, poll workers must be able to check the SSL/TLS server's certificate. Second, secrecy is provided only as long as the used cryptographic mechanisms remain unbroken.

as poll workers must have access to the corresponding private key(s) of foreign constituencies.

4.2 Electronic Ballot

As an alternative, voters could cast their vote electronically, directly on an electronic voting machine. In this case, the electronic vote could be transferred to the respective constituency just at the point of voting or afterwards. In order to ensure the principle of free and secret elections, the cast vote must be encrypted subsequently. For the sake of not interfering with ballot secrecy, two different machines should be used for voter authentication and vote casting and transmission.

A number of technical proposals for end-to-end verifiable electronic voting schemes/systems, which enable electronic vote casting, can be considered for directly implementing this approach, for example [5], [18], and [28].

In section 4.1, electronic emissions are an issue with respect to ballot secrecy. Furthermore, costs for the provision and maintenance of electronic voting machines arise.[8] However, end-to-end verifiable electronic voting schemes/systems provide an increased level of verifiability in comparison with postal voting and the traditional voting in the "home constituency". By using electronic voting ballots, voters could also comprehend the impact of their cast vote much better as the system provides appropriate feedback (e.g. regarding invalid votes). Furthermore, this approach enables visually impaired people to cast their vote personally. This strengthens the principle of direct elections as well as the principle of secret elections, because these voters - in contrast to the regulations in § 57 of the Federal Electoral Code - do not need to take an auxiliary person into the voting booth. Thus, they can cast their vote secret and personally. Thus, it is conceivable that voters are informed about the validity of their vote.

Table 2 summarizes the advantages and disadvantages of using canonical paper ballots or electronic ballots on electronic voting machines for vote casting.

Table 3 summarizes the advantages and disadvantages of using encoded paper ballots or electronic ballots on electronic voting machines for vote casting.

The comparisons in table 2 and 3 show that electronic ballots on electronic voting machines have more advantages, especially with respect to cryptographic verifiability.

5 Summary and Discussion

In this paper we have analysed the application of vote casting in any preferred constituency using the German parliamentary elections as an example. Thereby,

[8] Note, these costs are lower than the one for special printers.

Table 2. Canonical paper v.s. electronic ballot on electronic voting machine.

Canonical Paper Ballot (on demand)	**Electronic Ballot**
Advantages	*Disadvantages*
Established method	–
+	Costs for the provision and maintenance of electronic voting machines
Disadvantages	*Advantages*
–	Provides an increased level of cryptographic verifiability
–	Enables visually impaired people to cast their vote personally
Time for returning the ballots to the appropriate constituency	+
–	Voters can comprehend the impact of their cast vote much better

we have shown that a centralised electoral register cannot be declined in general. Different approaches of voter identification and authentication, and checking the eligibility to vote were discussed. The ballot record and the telephone are no adequate solutions, while the manual input of personal data and the use of the German e-ID card have both their advantages and disadvantages. With regard to the vote casting and tallying, we have shown that both processes shall be carried out electronically in order to provide vote secrecy towards the electoral committee or any third party (e.g. an eavesdropping attack over the Internet) in the best way. In this case cryptographic mechanisms are essential. This means that the cast votes must be transferred in an encrypted form. Thus, the question remains whether this approach complies with the principle of the public nature of elections which has been modified by the Federal Constitutional Court of Germany in 2009. Thereafter, it must be possible for the citizen to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge [14].

Cryptography is based on mathematical processes, which can be visualized to some extent, but until now these processes cannot be illustrated in a way that everyone is able to understand them, regardless of expert knowledge. Thus, the principle of the public nature of elections - just as the election principles in Article 38.1 sentence 1 Basic Law - is guaranteed without any reservation. However, the nature of things entails that not all election principles can be fulfilled in total purity (ref. to page 124 in [13]). Insofar, the restriction of one election principle is not unconstitutional per se, but may be justified as long as the constitution contains a respective authorisation, the deviation ensures the national political objectives or if the restriction is necessary in the interests of another election principle (ref. to page 369) in [15]). Vote casting in any preferred constituency could strengthen the principle of universal elections significantly. Thereby, those people, who decided to travel on Election Day in the short term or to be ab-

Table 3. Encoded paper v.s. electronic ballot on electronic voting machine.

Encoded Paper Ballot (on demand)	**Electronic Ballot**
Advantages	*Disadvantages*
Electronic emissions do not endanger ballot secrecy	–
Disadvantages	*Advantages*
Cryptographic verifiability is difficult to implement	+
–	Enables visually impaired people to cast their vote personally
Higher costs for special printers	+ (less costs for electronic voting machines)
–	Voters can comprehend the impact of their cast vote much better

sent because of any other reason, are given the opportunity to participate in the election. Postal voting cannot provide this opportunity, as it requires an early application for a ballot paper. Furthermore, in contrast to postal voting, the moment of casting a vote would not be carried out in a private environment, but would remain in a controlled environment.[9] While voting in any preferred constituency, the compliance with all election principles could be ensured and controlled by the public, because everyone can see that the voter enters and leaves the polling booth alone. Although postal voting is an indispensable voting channel for all citizens who are not able to visit a constituency within the electoral area, it can be assumed based on the increasing number of postal voters, that this voting channel is also used by citizens who would not actually need it. However, in order to ensure the election principles in the best possible way, vote casting in any preferred constituency should be considered as an additional voting channel.

In future work we will further analyse, if its application is constitutionally compliant also in the context of regional and local elections. In that regard it needs to be said that German states often establish the active right to vote with a certain period of residence in the particular state.[10] Furthermore, it must be noticed that regional and local elections do not take place at the same time. Therefore, vote casting outside the corresponding federal state or municipality is only possible with very large organisational effort. Based on the findings of this work, we aim to concretise the legal requirements for the establishment of a centralised electoral register and to provide a practical solution for accessing the currently distributed electoral register infrastructure. Thereby, we will focus on both options for identification and authentication of voters, namely by using the election notification, the German e-ID card or a combination of both. Finally, we will analyse, if existing proposals for end-to-end verifiable electronic voting

[9] This criticises Richter [25].

[10] For example § 2.1 No. 3 Electoral Act for the parliament of the State of Hessen.

schemes/systems, namely [5], [18], and [28] that could implement the approach treated in section 4.2, comply with the findings of this work and fulfill the technical and legal requirements for electronic voting in Germany.

Acknowledgments. This paper has been developed within the project 'VerkonWa' - Verfassungskonforme Umsetzung von elektronischen Wahlen - which is funded by the Deutsche Forschungsgemeinschaft (DFG, German Science Foundation).

References

1. Austrian Ministry for Science and Research: Evaluierungsbericht: E-Voting bei den Hochschülerinnen- und Hochschüler- schaftswahlen 2009. E-voting evaluation report, Wien (2010) (in German)
2. Briefwahl, http://www.bundeswahlleiter.de/de/glossar/texte/Briefwahl.html, Online: accessed 10 May, 2013 (in German)
3. Bräunlich, K., Kasten, A., Grimm, R.: Der neue Personalausweis zur Authentifizierung bei elektronischen Wahlen. In: Der 12. Deutsche IT-Sicherheitskongress - Sicher in die digitale Welt von morgen, pp. 211–225. (2011) (in German)
4. Bräunlich, K., Grimm, R., Kasten, A., Vowé, S., Jahn, N.: Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen. (2011) (in German)
5. Budurushi, J.: End-to-End Verifiable and Coercion Resistant Electronic Voting Protocol for Distributed Voting Machines in Polling Stations. Master thesis. Darmstadt (2012)
6. Budurushi, J., Neumann, S., Volkamer, M.: Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally binding Elections and Approaches Proposed in Scientific Papers. In: Kripp. M.J., Volkamer, M., Grimm, R. (eds.) 5th International Conference on Electronic Voting 2012, vol. 205, pp.257–270. Gesellschaft für Informatik, Bregenz (2012)
7. Bundesgesetzblatt I, No. 21, 9.5.1956, pp. 383–388, http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl&bk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl156s0383.pdf%27%5D, Online: accessed 10 May, 2013 (in German)
8. Bundesgesetzblatt I, No. 26, 26.4.2002, pp. 1342–1350, http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl&bk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl102s1342.pdf%27%5D, Online: accessed 10 May, 2013 (in German)
9. Carracedo Gallardo, J., Belleboni, P.E.: Use of the New Smart Identity Card to Reinforce Electronic Voting Guarantees. In: 4th International Conference for Internet Technology and Secured Transactions, pp.1–6. IEEE Press, London (2009)
10. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, T. A., Vora, L. P.: Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting. In IEEE Security & Privacy, pp. 40–46. (2008)
11. Deutscher Bundestag, Drucksache 17/10158, http://dipbt.bundestag.de/dip21/btd/17/101/1710158.pdf, Online: accessed 10 May, 2013 (in German)
12. Estonian National Electoral Committee: E-voting System General Overview, http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf, Online: accessed 10 May, 2013

13. Federal Constitutional Court of Germany: Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 59, pp. 119–128, (1981)
14. Federal Constitutional Court of Germany: Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 123, pp. 39–88, (2009)
15. Federal Constitutional Court of Germany: Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 95, pp. 335–407, (1996)
16. Federal Office for Information Security: Advanced Security Mechanism for Machine Readable Travel Documents - Part 2. Technical report, BSI-TR-03110-2, (2012)
17. Federal Office for Information Security: Functional Specification eID-Server - Part 1. Technical report, BSI-TR-03130-1, (2012)
18. Gibson, J. P., Lallet, E., Raffy JL.: Engineering a Distributed e-Voting System Architecture: Meeting Critical Requirements. In: Giese, H. (eds.) First International Symposium Architecting Critical Systems, vol. 6150, pp. 89–108. Springer, Prague (2010)
19. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, `http://tools.ietf.org/html/rfc5280`, Online: accessed 10 May, 2013
20. Meister, G., Hühnlein, D., Araujo, R.: eVoting with the European Citizen Card. In: Brömme, A., Busch, C., Hühnlein, D. (eds.), Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, vol. 137, pp. 67–78. Gesellschaft für Informatik, Darmstadt (2008)
21. Mishra, A., Gupta, B. B., Joshi, R.C.: A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques. In: Intelligence and Security Informatics Conference (EISIC) European, pp. 286–289. (2011)
22. Personalausweisgesetz (PAuswG), `http://www.gesetze-im-internet.de/pauswg/BJNR134610009.html`, Online: accessed 10 May, 2013 (in German)
23. Popoveniuc, S., Hosp, B.: An Introduction to PunchScan. In: Towards Trustworthy Elections, pp. 242–259. (2010)
24. Referentenentwurf Bundesmeldegesetz (MG), `http://philipbanse.de/docs/Referenenentwurf_Meldegesetz.pdf`, Online: accessed 10 May, 2013 (in German)
25. Richter, P.: Briefwahl für alle? - Die Freigabe der Fernwahl und der Grundsatz der Öffentlichkeit der Wahl. In: Die Öffentliche Verwaltung, pp. 606–610. W. Kohlhammer GmbH, (2010) (in German)
26. Rössler, T.: Electronic Voting Using Identity Domain Separation and Hardware Security Modules. In: 9th IFIP WG 6.1 Conference on E-Business, E-Services and E-Society, pp. 1–12. Springer, Nancy (2009)
27. Ryan, Y. A. P., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à voter: a voter-verifiable voting system. In: IEEE Transactions on Information Forensics and Security, pp. 662–673. (2009)
28. Sandler, D.R., Wallach, D.S.: The case for networked remote voting precincts. In: Proceedings of the 3rd USENIX/ACCURATE Electronic Voting Technology Workshop. San Jose, CA, (2008)
29. Schreiber W.: Bundeswahlgesetz: Kommentar. Carl Heymanns Verlag, Köln (2009) (in German)
30. Subramani, S.: Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis. In: SANS Institute InfoSec Reading Room, `http://www.sans.org/reading_room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi_33764`, Online: accessed 10 May, 2013
31. The Transport Layer Security (TLS) Protocol Version 1.2, `http://tools.ietf.org/html/rfc5246`, Online: accessed 10 May, 2013