Feasibility Analysis of Prêt à Voter for German Federal Elections

Denise Demirel[1], Maria Henning[2], Peter Y. A. Ryan[3], Steve Schneider[4], and Melanie Volkamer[1]

[1] Technische Universität Darmstadt / Center for Advanced Security Research Darmstadt, Germany
[2] Project Group Constitutionally Compatible Technology Design (provet), Universität Kassel, Germany
[3] University of Luxembourg/ Interdisciplinary Centre for Security and Trust, Luxembourg
[4] University of Surrey, United Kingdom

Abstract. Prêt à Voter is one of the most well-known and most extensively analysed electronic voting systems for polling stations. However, an analysis from a legal point of view has not yet been conducted. The purpose of this paper is to analyse the readiness of Prêt à Voter for legally binding federal elections in Germany. This case is of particular interest as Germany has with the Constitutional Court Decision from 2009 probably the most restrictive requirements on electronic voting in particular regarding the public nature of elections and verifiability respectively. While many aspects are analysed, some remain open for further legal and technical discussions. Thus, a final decision is not yet possible. Aspects analysed are the ballot paper layout, different processes from ballot printing through to the publishing of results, as well as verifiability, and the overall election management.

Keywords: Verifiable Elections, legal requirements, German Federal Elections, Prêt à Voter, Election System Design

1 Introduction

Since the 1960s several attempts have been made in Germany to replace manual casting and counting of votes by mechanical and later electronic voting systems. These efforts have always been based on the ambition to obtain a correct election result within a very short period of time. Electronic voting machines were first deployed in Germany on the occasion of the European elections in 1999. These machines produced by the company of Nedap were used on all election levels. After their usage for the elections of the German Bundestag (Federal Diet) in 2005 two people filed a complaint against this election. These complaints went through several instances and ended up at the Federal Constitutional Court. In 2009, the Federal Constitutional Court declared the used electronic voting machines and the Federal Voting Machine Ordinance which defines the requirements a voting machine has to ensure, to be unconstitutional because both did not meet the requirements emerging from Article 38 in conjunction with Article 20.1 and 20.2 of the German Constitution. From these articles the court deduced that it must be possible to check the essential steps in the election process including the accurate counting of votes [5, page 71]. Now, election authorities are looking for an electronic voting machine that meets these requirements and can therefore be classified as constitutionally compatible.

Prêt à Voter is one of the best known electronic voting systems which implements verifiability, has a prototype actually implemented, and has been successfully used in (test) elections in the U.K. Over time different variations of Prêt à Voter have been published and their security has been analysed. However, an analysis from a legal point of view has not yet been conducted.

This paper analyses which version of Prêt à Voter fits best to the regulations of the Federal Electoral Act, the Federal Electoral Code, and the German Constitution. It also discusses necessary modifications to the system and the processes. In general, we tried to keep the process for voters as similar as possible to what they know and as simple as possible. Such an analysis was possible due to the cooperation and interdisciplinary work between computer scientists and legal researchers. We categorise our discussion into

the following groups: aspects that are relevant for the ballot paper design, the different processes, verifiability, and election management. Voting registration and authentication in the polling station are not taken into account for this paper as these processes do not need to be modified.

The paper is structured in the following way: we first provide an introduction to the German federal elections in Section 2 and then to Prêt à Voter in Section 3. Afterwards, we discuss legal and technical aspects of the ballot paper design in Sections 4 and 5, different processes starting from ballot printing until the publishing of receipts in Section 6, the type of verifiability in Section 7 and the overall election management in Section 8. The paper concludes with a brief summary and remarks for future work (Section 9).

2 German Federal Election

According to Article 38.1 German Constitution/Grundgesetz (GG) the Bundestag is elected in universal, direct, free, equal and secret suffrage. Subject to particular regulations, the elections take place every four years. Voters can cast two votes on one ballot paper (see Fig. 1). With the first vote they select a named candidate from their home county (electoral district). With the second vote they select the list of a party on state level. Half of the delegates move into parliament because of the first vote, half because of the second vote. After §1.1 of the Federal Electoral Act (FEA), the Bundestag generally consists of 598 delegates.

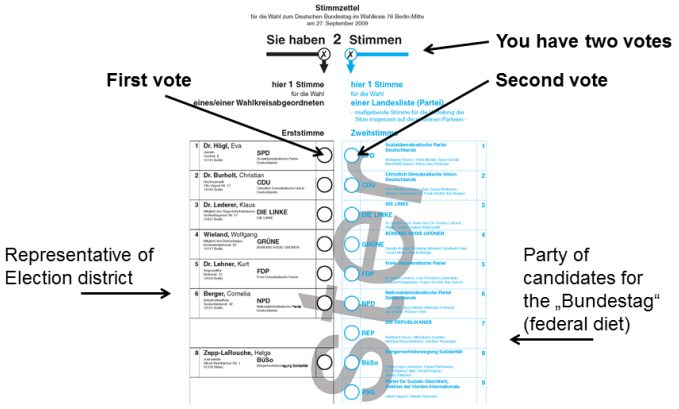

Fig. 1. Ballot paper for the German Federal Election in 2009

According to [6], roughly 62.2 million Germans were eligible to vote in the elections for the Bundestag in 2009. 70.8 percent cast their votes while 1.7 percent of the first votes and 1.4 percent of the second votes were invalid. Based on the handover of empty or crossed ballot papers, it is assumed that nearly 70 percent of them have been spoiled on purpose. For the elections of the Bundestag the territory of the 16 federal states is subdivided into 299 electoral districts. Due to the fact that every electoral district nominates local candidates for the first vote, the ballot papers differ from one district to another. The electoral districts are subdivided into constituencies. After §12.1 of the Federal Electoral Code (FEC) municipalities with no more than 2,500 inhabitants (generally 1,700 voters) usually form one constituency. Altogether there were 75,081 constituencies in Germany in 2009.

According to §31 FEA and §54 FEC everyone (not only eligible voters but everyone who is interested) is allowed to be present at the polling station during the whole election procedure and during the vote counting as long as they do not disturb any processes. Thus, people can observe the correct operation of the election and the correct counting of votes. After §47.1 FEC the polling stations are open from 8am until 6pm on a Sunday. The ascertainment of the results starts right after closing the polling stations. After deciding about

the validity of every vote, the returning committee[5] ascertains the votes cast in the constituency according to §§67–71 FEC. Referring to this, the head of the returning committee informs the local authority and the district election officer who passes the respective district results to the state returning officer. The state returning officer refers the results directly and continuously to the federal returning officer who publishes the provisional curatorial election result. In the elections for the Bundestag in 2009, this result was published at 3.25am Monday morning.

3 Prêt à Voter

Prêt à Voter is an end-to-end verifiable voting system. It provides secrecy of the ballot and integrity of the election, and is designed also to allow verification of the processing of the votes, from casting through to tallying. It achieves this by publishing auditable information for each stage the votes pass through, so that verification rests on the information that is published rather than the processes which generated that information. In fact there are several versions of Prêt à Voter, which vary in terms of the detail of how this is achieved, and an overview of the differences and of the general Prêt à Voter approach is given in [11]. In this paper we focus on elections where a vote is cast against a single candidate. Variants of Prêt à Voter are also able to handle preferential voting, but we will not consider them here.

The key idea is that Prêt à Voter sets up the voting process so that voters cast their vote in a familiar way, but the system accepts their vote in encrypted form. This allows publication of the list of encrypted votes cast, and also allows the voters to retain a record of their cast vote to confirm that it appears on the published list. The system then anonymises the votes, decrypts them, and finally tallies the results. The anonymisation phase means that no decrypted vote can be linked with any encrypted vote cast by a specific voter, preserving ballot secrecy. There are verification mechanisms for each of these phases—anonymisation, decryption, tallying—which mean that the integrity of the election can be verified. A diagrammatic overview of the process is given in Figure 2.

3.1 Vote Casting

The central idea of Prêt à Voter is the use of a particular design of ballot form to capture the vote. In the proposals to date, each ballot form contains the list of candidate names on the left hand side, in a random order which varies between ballot forms. The right hand side has a space against each candidate for the voter to mark their vote, and also (at the bottom) the order of the candidates in encrypted and hashed form[6]. The ballot form is perforated to allow the two sides to be separated. The voter marks their vote against their chosen candidate, and then separates the two halves of the ballot paper and destroys the list of candidates on the left hand side. The right hand side contains a vote marked in some position, and the hash value of the ciphertext containing the order of candidates[7]. The right hand side is then scanned into the election system, the scanner's interpretation (in terms of the position of the mark) is displayed to the voter, the voter confirms this is correct (or else corrects it either on the display or by filling out a new paper ballot), and it is then accepted by the system for inclusion in the published list L_1 of cast votes, which is published on an online Web Bulletin Board (BB) together with the encryption of the corresponding candidate order. The system will only accept a vote in which exactly one selection is made. The system provides the voter with a signed record of the encrypted vote that has been accepted, which contains the cryptographic information on the original right hand side, and the marked position. This can be compared with the one the voter scanned. While the original one is put into a ballot box the printed and signed one is kept by the voter as receipt. The voter can later check it against the published list of votes cast by looking it up on the BB. The record does not reveal which candidate received the vote, since the random order of candidates means it could have been any of them.

[5] The returning committee is the electoral body who takes care of the ordinary run of the election, watches the observance of the electoral principles and counts the votes after closing the election.

[6] The hash is used to keep it short. Instead of the hash value also a serial number could be used while this number is bounded to the ciphertext of the candidate order e.g. via commitments of the Web Bulletin Board.

[7] In the following we will use the term hash value when referring to this ciphertext.

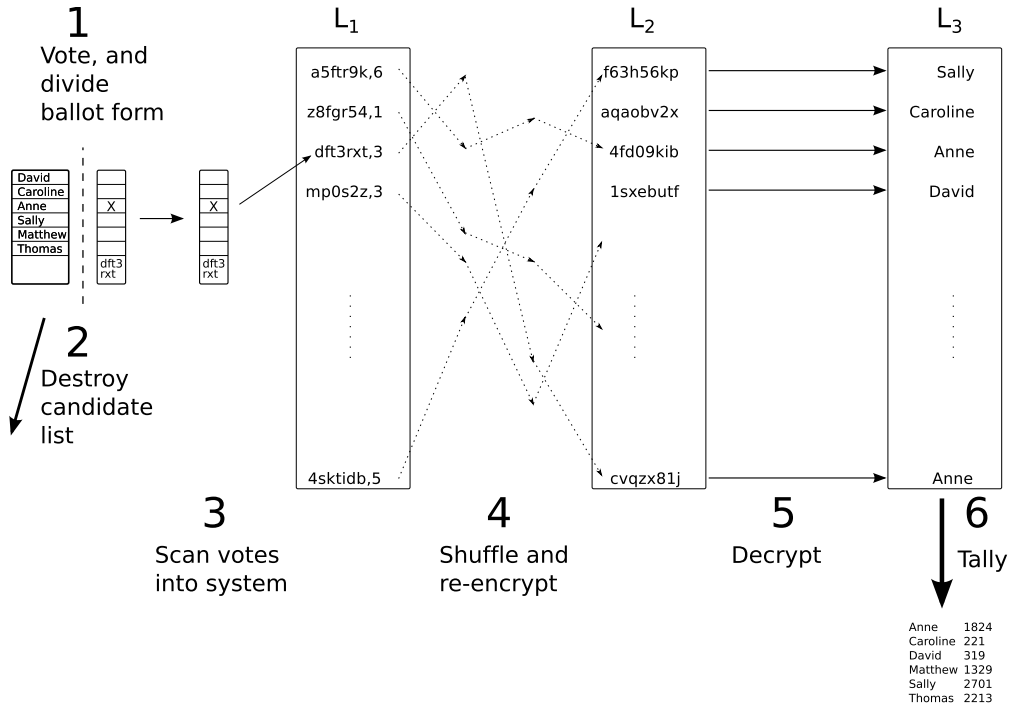

Fig. 2. Overview of the phases of Prêt à Voter vote processing

3.2 Vote Processing

The list of accepted scanned votes L_1 is a list of encrypted votes. They are now processed through a series of stages to yield the final tally. The first stage is *anonymisation*: this is achieved by passing L_1 through a re-encryption mixnet [10], which shuffles the encrypted votes through a series of *mixnet nodes* which perform secret permutations, while re-encrypting the votes. The result is a new list of different ciphertexts which encrypt the same votes as the original list but in a different order. This resulting list L_2 is also published. No vote in L_2 can be linked to any vote in the original list, and hence cannot be linked to any vote record held by a voter. The shuffling and re-encryption can be verified, either by randomised partial checking [8], or through proofs of re-encryption [13,9], depending on the approach taken. Several mix servers are used, each to perform a round of re-encryption and shuffling: secrecy of the shuffle is obtained provided they do not all collude.

The second stage is *decryption*. The resulting list L_2 of encrypted votes can now be decrypted. The decryption key is shared across the election servers, so that a minimum number (threshold set) of them are required to cooperate to decrypt the ballots. The resulting list L_3 is also published. The decryption can be audited against L_2, and verified as valid by the public.

The final stage is *tallying*. The decrypted votes are tallied in order to obtain the result of the election. Since the tallying algorithm is public, and the decrypted votes are published, the tallying process can be checked and verified by any party.

4 General Legal Analysis of Random Candidate Order

In this section we analyse whether shuffling candidates complies with the legal regulations for federal elections in Germany. After §30.3 FEA the order of the party lists on state level depends on the number of the second votes each party achieved in the particular federal state within the last election. The parties that are not

currently represented in parliament follow in alphabetical order. The order of the county proposals presented on the left side of the ballot paper depends on the order of the respective party list. Other county proposals follow in alphabetical order.

Correspondingly the random order of Prêt à Voter is not compatible with the current regulation of the FEA. However, the question if it might be permissible in general, depends on constitutional requirements because the respective regulation can be changed if this is constitutionally compatible. The Federal Constitutional Court abnegated the obligation to provide equal ballot papers in its decision from the 6th October 1970 [4, p. 164]. It pointed out that the regulation relevant to the case ensures the ordinary flow of the election, but is not necessary from a constitutional point of view.

The principle of the equal suffrage according to Article 38.1 GG forms the basis for the organisation of the election and the functionality of the voting system [14, §1, Rn. 42]. After the jurisdiction of the Federal Constitutional Court it contains the equality of counter value[8] for the first and second vote, the equality of result value[9] for the second vote and the equality of opportunity for all candidates [1, p. 246, 247].

The third aspect would be strengthened by the random order. In reference to this every candidate needs to have the same chance to win the election. Although a strict order is not said to violate the principle of the equal suffrage because voters prefer to make their decisions based on the manifesto of the political party [2, p. 18], it brings a psychological benefit to the party that achieved the highest number of second votes within the last election and therefore comes up on the top of the race [14, §30, Rn. 8]. This effect would be lost by using the random order of Prêt à Voter. Therefore, non-established parties would win the benefit to be on top of the list periodically. Consequently, the key idea of Prêt à Voter brings a big advantage over the known paper ballot system. New parties could obtain the benefit of getting registered first by the voters just like the catch-all parties. Through this the constitutional requirement of the equal suffrage would be invigorated. Furthermore, a strict order of the candidates is not compulsory according to the election principles of Article 38.1 GG.

5 Analysis of Design Proposals — Ballot Paper

In this section, we discuss different aspects of the ballot layout including which of the possible types of randomization for candidates and parties is most appropriate, how to design the ballot paper to easily remove the part that is scanned, how to integrate the hash value of the encrypted order of candidates, and how to enable invalid votes.

5.1 Type of Random Order

According to [11], two different types of randomisation can be applied, namely completely arbitrary order or cyclic shifting of candidate order. Chaum et al. point out in [7] that the distance between marks on the receipt can leak some information if entries are only shifted and the voter is allowed to mark more than one entry. This is not the case for arbitrary order of entries as the successor and predecessor of every entry differs from ballot paper to ballot paper. The current ballot paper for the German federal election contains two races on one paper in two columns (compare to Fig. 1) which leads to a similar problem then mentioned in [7]. For instances, two entries in a row leak the information that the voter cast a vote for a direct candidate and the associated party which would violate the principle of the secret suffrage according to Article 38.1 GG. This principle includes that it needs to remain secret whether voters split their votes or cast them based on a single preferred party [14, §1, Rn. 95].

Cyclic shifting has, compared to an arbitrary order, the advantage that it is easier for the voter to find their candidate and party since the sequence of the candidates stays the same on all ballot papers. Therefore, the most appropriate way to randomize the order seems to be the use of cyclic shifting while each race is shifted with its own value. Note, in case where one race has more entries (candidates or parties), the empty

[8] Every person, eligible to vote, has the same number of votes and is able to vote in the same way.
[9] All votes have the same influence on the election result.

columns are not included in the shifting algorithm (compare to Fig. 3). This approach leads to two different shift values which can either be encrypted together to one ciphertext and then hashed or the hash of two separate ciphertexts is computed.

5.2 General Ballot Layout

Using Prêt à Voter it is necessary that the voters can easily detach their markings and destroy the parts with the candidates on. On the current ballot paper for federal elections the candidate list and party list respectively shows up on the left and right hand side and voters mark their decision for both races in the centre of the ballot paper. As approaches like using two different ballot papers, putting the second race below the first race, and swapping the two races are either not practical or do not comply with §30.2 FEA and §45.1 FEC including appendix 26 of FEC respectively, we recommend to keep the ballot paper format from the traditional system but prepare it in a way that it is easy to detach the candidate lists on the left and right hand side. This remaining central part of the ballot paper, containing the marked positions and the hash value is scanned.

5.3 Obscuring Hash Values on Ballots

Although voters are not committed to keep their voting decision secret, they are not allowed to get a receipt of it which can be used as an evidence of the respective vote. Due to the possibility that voters might take a picture of themselves including the marked but not detached ballot paper and the respective hash value which will be published on the BB later, the secrecy of the vote and indirectly also the free suffrage of the election (compare to [14, §1, Rn. 94]) could be violated. The picture together with the corresponding entry on the BB serves as a proof to sell votes. By entering the code on the BB, a potential extortionist could control if voters really cast their vote, which position they marked and correspondingly (by using the picture) for which candidate. Note, also in the traditional system one could take a similar picture but this picture does not serve as proof as the voter might have asked for a new ballot paper afterwards. Correspondingly, the hash value may not be plain as long as it is possible to link it to the particular ballot form and the order of entries on it. This is an issue during the vote casting process.

To solve this problem, the hash value could be hidden by various measures e.g. a scratch strip or invisible ink. Organisational procedures need to ensure that voters first detach the centre part of the ballot, destroy the remaining parts in the polling booth and then reveal the covered hash value outside of the polling booth before scanning it. While this is required from the legal perspective more research on this approach is required including whether voters would feel comfortable with the strict process needed in this case and technical challenges.

5.4 Enabling Invalid Votes

Due to privacy issues Prêt à Voter neither accepts under- and over-votes nor empty votes. In the traditional system any of these possibilities can be used to cast an invalid vote. Also paintings or writings on the ballot paper would result in an invalid vote. If a corresponding vote is scanned by Prêt à Voter the system will inform the voter and reject this vote.

§39 FEA defines the term of invalid votes and ascertains the way to deal with them. According to [14, §1, Rn. 23], the principle of the free suffrage contains the right to cast invalid votes. Otherwise people eligible to vote could be forced to cast a vote for a candidate. In reference to this, voters are allowed to vote the candidate they like, vote invalid while participating in the election, and to abstain from voting as well. In Prêt à Voter this aspect can be addressed by adding one field to the candidate/party list of every race with the option to cast an invalid vote (as proposed in [15]).[10]

From a legal perspective, it needs to be discussed whether voters can be forced to vote invalid in a certain way by marking the respective field. This might violate the principle of the free suffrage. But electronic voting

[10] Note, in order to spoil the whole ballot paper it is required to mark both invalid vote entries.

is discussed in order to reduce the number of invalid votes cast by accident. The voting system of Prêt à Voter is able to support this intention.

All the different aspects of the ballot designed have been combined in an example ballot shown in Fig. 3.

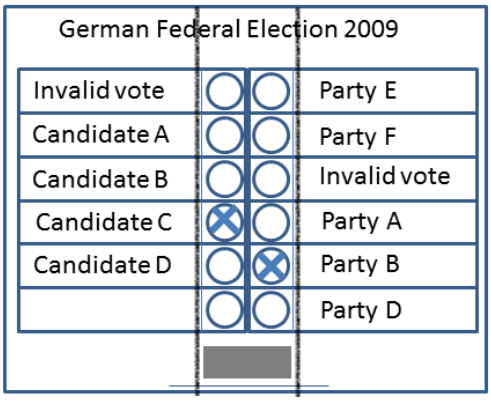

Fig. 3. Proposed ballot paper

6 Analysis of Design Proposals — Processes

In this section, we discuss the relevant processes including ballot printing, vote casting, scanning, and the publishing of the receipts on BB.

6.1 Ballot Printing Process

There are two possibilities to consider for the timing of printing the ballot forms. It can be carried out either on demand in the polling station, or in advance of Election Day. The advantage of printing on demand is that there are no chain of custody issues with respect to the physical ballot forms, since they do not exist in physical form before they are printed for immediate use. However, printing on demand has a number of disadvantages: printers are needed in each polling station and additional effort at local level is required. The inclusion of measures such as scratch strips or invisible ink to mask the hash value will require special equipment. Hence, printing on demand is not appropriate. We therefore recommend that printing of the ballot forms is carried out in advance of the election.

We further recommend that the Election Manager takes responsibility for the printing at the same physical location as the generation of the ballot forms, where they are printed directly as they are generated, so that no electronic file of the ballot forms needs to be created. The ballot form generation system (servers and printers) should also be isolated from any network. A high level of trust is required in the printing provider, since it knows the association of ballot orders and the hash values. This can be mitigated by involving several parties in the printing process and using mechanisms to distribute the information between them, as discussed in [12], though this can become cumbersome.

Once generated, the chain of custody of the ballot forms through to their use in the election must be securely managed, to ensure that the information they contain remains secret, and that ballot forms cannot be added or removed.

6.2 Vote Casting Process

The detached centre part of the ballot form could either be scanned inside or outside of the polling booth. In case of the first variant, voters would have to scan the respective part on their own and without any external help. Irrespective of the question if they might be able and willing to do so, the returning committee could not confirm that the hash value is not revealed until the scanning process starts. This is no option due to the possibility of violating the principle of the secret suffrage (see Section 5.3).

In the second case, voters would have to scan the detached centre part of the ballot paper after having revealed the hash value outside the polling booth in front of the returning committee. Because voters might appreciate the help given by the returning committee, this approach would probably be the more pleasant one from a practical point of view. According to [14, §1, Rn. 95] nobody shall know if voters cast an over, under or empty vote if they do not disclose their voting decision by themselves. It should be noted that the system reveals some information by rejecting the scanned paper.

However, this situation could be improved for voters by providing a separate scanner in the polling booth. Voters could run a test scan before casting their votes outside in order to check whether the system accepts their ballot and whether they agree with the interpretation of the scan. While changing the rules for casting a vote change (in particular for casting an invalid one), we expect people to feel more comfortable pre-scanning their ballot in the voting booth.

Voters could still try to scan an invalid vote in public, disclaim the possibility of checking their filled ballot paper in advance, add marks after they checked the ballot paper or just ignore the feedback. But this situation might be comparable to the one regulated in §56.6 and 8 FEC. After this the returning committee has to rebuff every voter who tries to put an unfolded ballot paper into the ballot box. In case the voter still wants to cast a vote, the returning committee hands out a new ballot form after destroying the old one. Herewith the legislator wanted to assure voters do not waive their right of secret voting. However, further research from a legal point of view is required to back up this comparison.

6.3 Vote Scanning Process

Once the strip with the marks is scanned, there exist several possibilities to interpret the marks as votes. For instance one can detect crossing lines or the degree of blackening in the bubbles. The interpretation algorithm must comply with the legal guidelines.

After §34.2 of the FEA voters cast their votes by marking the particular section of the candidate on the ballot form with a cross or any other sign which indicates the voting decision. Consequently voters are free to choose any mark they like as long as it is not unconstitutional. The secret suffrage for example is violated by using a very individual sign like signatures, which could be attributed to a particular voter. A sign outside of the field is not forbidden if an allocation to a certain candidate is possible [14, §34, Rn. 4]. But according to §39 FEA the votes cast are invalid in certain cases, e.g. when the voter hands in a ballot paper with an addition or a caveat on it. Although both terms are not defined in the FEA, the returning committee needs to decide about the validity of every vote. Therefore decisions can be made differently in different constituencies. After [14, §39, Rn. 12] for example an addition is every verbal annexation on the ballot paper which outruns the allowed annexation according to §34.2 FEA. Admittedly non-verbal terms need to be covered as well, e. g. a skull and crossbones on the ballot paper.

The scanner used by Prêt à Voter needs to be programmed in order to convert the given information while taking these uncertainties into account. Note, as voters still cast their vote on ballot papers it is possible that they could add marks or pictures which make the vote invalid but would be accepted by the system. The system's interpretation of the scan will naturally depend on the thresholds used, for example the degree of blackening accepted as a mark, in the image processing algorithms applied to the scan, and this may differ from the voter's expectation. Therefore the voting system of Prêt à Voter provides a confirmation stage for the voter. This option would show voters how their vote is interpreted, and provide the option to fill in another ballot paper if required. The confirmation stage would solve another problem as well: if voters put a comment into the section for a candidate — even the comment shows the antipathies of the voter — the system would count this as a valid vote for the respective candidate. This can only be acceptable when the

voter confirms the interpretation of the system. On the condition of this confirmation stage, it might be legally compatible that the scanning process ignores additional marks or pictures and accepts ballot papers where exactly one mark per race is detected. Further this solution provides a consistent processing of votes.

6.4 Process of Publishing Receipts

The scanner prints out a signed receipt for each voter to take home. In order to enable voters to verify that their encrypted votes are recorded correctly, the corresponding electronic version of these receipts are published on the BB. These receipts could be published right after casting the vote or after the official end of the election. If they are published during the Election Day, an internet connection in the polling station would be needed. Irrespective of the increasingly higher costs, the risk of manipulation over the internet would come up as well. Therefore, we recommend to take the equipment first to some central places in the election district, count and tally votes, get backups of everything and then publish the receipts containing the position of the marks and the hash value together with the corresponding ciphertext.

The publishing of receipts after the closing of the polling station is also compatible with the current regulations of the FEC. According to §§54, 67 FEC voters can watch the counting of votes in traditional paper based elections only after the closing of the election. In addition, by publishing afterwards, voters would not lose the possibility to appeal against the election or certain election decisions. According to Article 41 GG complaints requesting the scrutiny of an election need to be discussed and adjudicated by the Bundestag. After §2.4 of the Law on the Scrutiny of Elections the complaints have to be submitted within two months after the elections. After the jurisdiction of the Federal Constitutional Court the unobstructed run of parliamentary elections requires that legal control during the election is reserved for complaints requesting the scrutiny of the election afterwards [3].

7 Analysis of Design Proposals — Verifiability

After the verdict of the Federal Constitutional Court from the 3rd March of 2009 the voter himself or herself must be able to verify whether his or her vote as cast is properly recorded as a basis for counting [5, page 72]. It is not sufficient if voters must rely on the functionality of the system without the possibility of personal inspection [5, page 72]. Electronic voting systems need to provide a possibility for the voter to check the essential steps in the election act and in the ascertainment of the results to the same amount as in traditional paper based elections. Here voters are able to watch the entire election procedure — from the opening of the polling station until the vote counting and tallying. Thus, even though only very few people take the opportunity to observe the whole process it is in general possible.

In this section we consider the verifiability aspects of the stages of processing the votes while we distinguish between individual and public verifiability and discuss their compliance with the demands from the court decision.

7.1 Individual Verifiability

Individual verifiability covers well-formedness (to ensure that votes are cast as intended) and the fact that the voter can verify that their hash value appears on the BB (to ensure that votes are stored as cast). *Well-formedness* of the ballot forms requires that the printed candidate list matches the list embedded in the hash value. Ballot forms can be checked by requesting a decryption of the ciphertext belonging to the hash value from the election decryption servers. There will be some random well-formedness checks by independent auditors ahead of and during the election. Due to the legal requirement this event will be announced and will be accessible by the public[11].

Also during the election, voters themselves may request to audit ballot forms that they are given. When given a ballot form, a voter can choose whether to select it for audit, or to use it to cast a vote. In the case

[11] In addition, to enabling them to observe even they cannot be physically present, a live stream could be broadcasted.

of audit, the voter retains an audit copy of the entire ballot form with the visible hash value, and the system retains and logs that ballot form as selected for audit by entering the hash value in a separate interface. This is necessary to prevent the form also being used to vote, since secrecy will be lost. In the post election phase, the audit process will be completed, by decrypting and publishing the list of candidates, for the voter to verify.

If a vote is cast, the voter is provided with a *receipt* of the right hand side, and after the election when the receipts are published, the voter can use this to verify that the information contained on it has been included on the published list of cast votes, which will next become mixed and decrypted.

If voters detect a problem with either of these two lists, then the voter's receipt and the entire ballot form respectively are evidence that can be used as a basis for a challenge to the election. It is important that receipts and the entire ballot form for auditing cannot easily be forged, since that would enable voters to mount fake challenges.

7.2 Public Verifiability

The cast votes are submitted in encrypted form. The next stage of the process is to pass them through several rounds of a re-encryption mix, where each round re-encrypts and shuffles all of the votes. The output of that process is another list of encrypted votes, which can then be decrypted and tallied.

Re-encryption mixes allow several approaches to verification, as described earlier. The legal requirement that it must be possible to check the essential steps in the election process inclines us towards the randomised partial checking approach, rather than using proofs of re-encryption: the mechanism of random sampling and checking is more intuitive and comprehensible to the public, and in principle any observer can contribute to the random audit checks. Each stage of the mix, i.e. each intermediate list of encrypted votes, is made public. A check involves challenging a particular re-encryption link in the mix and obtaining evidence of the re-encryption (i.e. the randomisation introduced in that step) that can be independently checked. In a mix, half of the links will be randomly checked, but in a way that ensures that no receipt can be traced through the mix. More precisely, the audits, while essentially random, can be carefully constrained to ensure that there are numerous breaks in the chain from receipt to decrypted vote.

Several re-encryption mixes can be run, in parallel or at any later time on request, which on decryption of the output should all yield the same result. The confidence level can be made as high as required by adding parallel mixes and audits. For a winning margin of n votes, the probability that a different candidate was in fact the winner but no altered votes were found by the audit, will be at most $2^{-n/2}$, which decreases exponentially as n increases: for example, a winning margin of only 40 votes is 99.9999% certain to be correct if the randomised partial checking audit on a single re-encryption net is successful, i.e. does not find any incorrect re-encryptions. If a higher level of certainty is required, then further mixnets can be generated and audited.

The remaining steps of the process are all publicly verifiable: the decryption of the outputs from the mix along with proofs of correctness of the decryptions is published, and can be verified by anyone. The tallying of the decrypted votes is also published and can also be checked independently.

With this proposed verifiability of the election, the level of verifiability can be increase compared to the level of verifiability in traditional paper based election systems. However, what remains for future work is to deduce an acceptable certainty for both individual and public verifiability from both legal requirements and the accepted error rate in traditional paper based elections.

8 Analysis of Design Proposals — Election Management

The election can be run centrally, or it can be distributed. The advantage of running the election from a single central location is that the system needs to be set up only once, and one single election system is likely to reduce costs in terms of equipment and management in comparison to a number of smaller ones. However, the disadvantage is that a single system will be a bottleneck, both in terms of setting up the election in

the first place, including the generation and printing of the ballot forms, and in terms of the length of time needed to process the large number of cast ballots.

Alternatively the election may be decentralised, and run across a number of locations. This can be achieved by setting up completely independent Prêt à Voter systems, each to run the election for a number of constituencies, and collating their results. This has the advantage of processing the cast votes in parallel, obtaining the result more quickly than a single central system would be able to. Another advantage of decentralisation is that challenges can be handled more efficiently at a more local level.

The election naturally separates into smaller races which can be run and processed separately: The ballot forms differ for every electoral district, so the preparation before the election is different for each district and can be distributed. Furthermore, the results of each electoral district must in any case be reported separately, meaning that the votes from each electoral district must be processed and tallied separately. The Prêt à Voter system is able to manage this by processing the votes in batches and reporting separately on the results, one district at a time, and this task distributes naturally across a number of such systems.

Our recommendation is therefore to decentralise the election management. The optimal level of decentralisation balances the overall resources required against the gains achieved in terms of efficient management of the election and speed of reporting the result, and in this context we would recommend decentralisation to the level of federal states.

9 Conclusion and Future Work

The paper analyses Prêt à Voter regarding its readiness for German federal elections and discusses different design proposals in order to decide which of the many different variations of Prêt à Voter fits best. While already a lot of different aspects from the legal perspective are covered and ensured by the proposed version, some others need to be discussed in future work. The main one is the requirement of [5, page 39] that all essential steps in an election are subject to public examinability (unless other constitutional interests justify an exception). This needs to be possible without any special expert knowledge [5, page 39]. Against this background, it needs to be discussed whether and how a system like Prêt à Voter can fulfil this requirement. Therefore, it is first necessary to further analyse the judgement regarding the question whether voters need to be able to check the election manually or whether tool support is acceptable as well as understanding the general idea, or whether it is necessary to follow all mathematical steps (which would obviously not be possible for a system like Prêt à Voter). Besides this, future work includes discussions about data storage (which data for how long) and responsibilities (who prints and keeps the ballot papers, how many key holders, election servers, and mix nodes as well as who they are). Although the receipt gives no information about the particular voter, long term secrecy needs to be broached as well. Furthermore, an acceptable certainty for both individual and public verifiability needs to be deduced from legal requirements and the accepted error rate in traditional paper based elections. Besides that we have to view the fact that visually handicapped people cannot cast their votes by using a plastic template (with Braille on it to put the ballot paper in) anymore when introducing Prêt à Voter. Therefore, it needs to be discussed whether a particular amount of ballot papers with Braille needs to be available in each polling station.

In addition to these legal aspects, there are also usability and acceptance issues, for instance regarding whether detaching is feasible without destroying the centre part of the ballot paper and destroying the other parts, as well as accepting that only test ballots can be audited but not the one to cast and the strict processes demanded in the polling station.

Another challenge is extending a suggestion regarding the vote scanning process and enabling voters to check the signature on their receipt, to ensure their receipt is genuine evidence of their cast ballot. This requires additional equipment, perhaps provided by independent organisations. If this is not feasible then it may be appropriate to use conventional anti-counterfeiting measures, such as special paper for the receipts, special patterns, rubber stamping, and so on. This challenge is the subject of current research.

This paper shows that it is worth analysing systems with an interdisciplinary team to ensure that they are not only secure from a cryptographic point of view but also conform to elections laws for particular elections.

Acknowledgements 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) and conducted in cooperation of provet (Project Group Constitutionally Compatible Technology Design at the University of Kassel) and CASED (Center for Advanced Security Research Darmstadt). Peter Ryan thanks the FNR Luxembourg for funding the SeRTVS project. Steve Schneider is grateful for funding through the Trustworthy Voting Systems project under UK EPSRC grant EP/G025797/1.

References

1. Bundesverfassungsgericht: Judgment. BVerfGE 1, 208 - 261 (April 1952), http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv001208
2. Bundesverfassungsgericht: Judgment. BVerfGE 13, 1 - 20 (May 1961), http://sorminiserv.unibe.ch:8080/tools/ainfo.exe?Command=ShowPrintVersion&Name=bv013001
3. Bundesverfassungsgericht: Judgment. BVerfGE 14, 154 (June 1962)
4. Bundesverfassungsgericht: Judgment. BVerfGE 29, 154 165 (October 1970)
5. Bundesverfassungsgericht: Judgment. BVerfGE 123, 39 - 88 (March 2009), http://www.bverfg.de/entscheidungen/rs20090303_2bvc000307en.html
6. Bundeswahlleiter, D.: Wahl zum 17. Deutschen Bundestag am 27. September 2009, Heft 5, Textliche Auswertung der Wahlergebnisse (November 2010), http://www.bundeswahlleiter.de/de/bundestagswahlen/BTW_BUND_09/veroeffentlichungen/Heft5_komplett.pdf
7. Chaum, D., Ryan, P.Y.A., Schneider, S.A.: A practical, voter-verifiable election scheme. In: European Symposium on Research in Computer Security, number 3679 in Lecture Notes in Computer Science. Springer- Verlag (2005)
8. Jakobsson, M., Juels, A., Rivest, R.L.: Making mix nets robust for electronic voting by randomized partial checking. In: USENIX Security Symposium. pp. 339–353 (2002)
9. Neff, C.A.: A verifiable secret shuffle and its application to e-voting. In: ACM Conference on Computer and Communications Security. pp. 116–125 (2001)
10. Park, C., Itoh, K., Kurosawa, K.: Efficient anonymous channel and all/nothing election scheme. In: EUROCRYPT. LNCS, vol. 765, pp. 248–259. Springer (1993)
11. Ryan, P.Y.A., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à Voter: a voter-verifiable voting system. IEEE Transactions on Information Forensics and Security 4(4), 662–673 (2009)
12. Ryan, P.: Prêt à Voter with Paillier encryption. In: Journal of Mathematical and Computer Modelling, Volume 48, Issues 9-10, November 2008. pp. 1646–1662. Elsevier (2008)
13. Sako, K., Kilian, J.: Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In: EUROCRYPT. LNCS, vol. 921, pp. 393–403. Springer (1995)
14. Schreiber, W.: Bundeswahlgesetz Kommentar. Carl Heymanns Verlag (March 2009)
15. Xia, Z., Schneider, S.A., Heather, J., Ryan, P.Y., Lundin, D., Peel, R., Howard, P.: Prêt à voter: All-in-one. In: Proceedings of IAVoSS Workshop on Trustworthy Elections (WOTE 2007). pp. 47 – 56 (2007), ottawa, Canada