

Gesellschaft für Informatik (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into the fields of

- Seminar
- Proceedings
- Dissertations
- Thematics

current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

ISSN 1617-5468

ISBN 978-3-88579-225-3

The 2008 Conference on Electronic Voting took place in Castel Hofen near Bregenz at the wonderful Lake Constance from 6th to 9th August.

This volume contains 17 papers selected for the presentation at the conference out of more than 30 submissions. To assure a scientific quality, the selection was based on a strict and anonymous double-blind review process.



Robert Krimmer, Rüdiger Grimm (Eds.): Electronic Voting 2008

# GI-Edition

## Lecture Notes in Informatics

**Robert Krimmer, Rüdiger Grimm (Eds.)**

### 3<sup>rd</sup> international Conference on **Electronic Voting 2008**

**Co-organized by Council of Europe,  
Gesellschaft für Informatik and E-Voting.CC**

**August 6<sup>th</sup>- 9<sup>th</sup>, 2008  
In Castle Hofen, Bregenz, Austria**

# Long-term Retention in E-Voting – Legal Requirements and Technical Implementation

Rotraud Gitter<sup>1</sup>, Lucie Langer<sup>2</sup>, Susanne Okunick<sup>3</sup>, Zoi Opitz-Talidou<sup>1</sup>

<sup>1</sup>Universität Kassel  
– provet –  
Wilhelmshöher Allee 64-66  
34119 Kassel, Germany  
[r.gitter | z.talidou}@uni-kassel.de](mailto:{r.gitter | z.talidou}@uni-kassel.de)

<sup>2</sup>Technische Universität Darmstadt  
Cryptography and Computeralgebra  
Hochschulstraße 10  
64289 Darmstadt, Germany  
emailadresse@autor1  
[langner@cdc.informatik.tu-darmstadt.de](mailto:langner@cdc.informatik.tu-darmstadt.de)

<sup>3</sup>pawisda systems GmbH  
Robert-Koch-Straße 9  
64331 Weiterstadt, Germany  
[susanne.okunick@pawisda.de](mailto:susanne.okunick@pawisda.de)

**Abstract:** Legally binding elections require retention of specified election data such as balloting material. This applies to paper-based as well as electronic elections. However, in Germany, legal requirements on retention in e-voting have not been issued so far. Based on the German legal framework for governmental as well as non-governmental paper-based elections, we give recommendations on long-term retention in e-voting, applying our results to a state-of-the-art e-voting scheme. We also review technical measures to meet the security requirements of long-term retention in e-voting.

## 1 Introduction

In the context of governmental actions and democratic elections especially, secure long-term storage is an important issue. Strict regulations apply here and compliance with these obligations must be documented as a proof of correct process implementation. Turning to e-government and e-voting in particular, new challenges have to be faced in this area: While the classical paper-based form of documentation just needs to be stored in a safe place once and for all, long-term retention of electronic data truly is a long-term task. Electronic data can easily be changed, therefore issues like integrity and authenticity must be addressed. Furthermore, due to hardware and software obsolescence, difficulties in terms of readability emerge.

With respect to democratic elections, the ballots must be retained over a specific period (usually several years) to allow recounting in case of contestations. Hence, for legally binding elections there exist legal obligations regarding long-term retention. This applies to common paper-based as well as electronic elections. But unlike the paper-based variant, legal regulations for remote electronic elections have not yet been issued in general. In its recommendation on legal, operational and technical standards for e-voting [Cou04], the Council of Europe states that “the e-voting system shall maintain the availability and integrity of the electronic ballot box,” which means that “the information kept in the electronic ballot box must be securely saved for as long as this is necessary to permit any recount or legal challenge or for the period after the election required by the electoral process in the member state in question” [Cou04, Standard No. 99]. Concrete measures are a matter for national legislature. The German Informatics Society (Gesellschaft für Informatik – GI) has developed a catalogue of requirements for online elections in non-governmental organizations [Ges05], presuming that there exist no regulations regarding long-term retention of election results. At the same time, the GI as well as the German Research Foundation (Deutsche Forschungsgemeinschaft – DFG) have adopted their own regulations for online elections, which comprise also regulations regarding long-term retention of election records (cf. [Ges04], [Deu06]).

The different issues of long-term retention in general have been addressed by a lot of research projects. The projects nestor [nes] and PADI [PAD] brought together and made available competences and information regarding technical, organizational, and legal aspects of long-term archiving. InterPARES [Int] is a major international research initiative that aims at developing the knowledge necessary to provide policies, strategies and standards capable of ensuring the longevity and trusted authenticity of digital material. In Germany the DOMEA concept [DOM] defines requirements for document management and electronic archiving in e-government. The long-term conservation of electronically signed documents has been addressed by the European Telecommunications Standards Institute [ETS03] and the projects ArchiSig [Arc] and TransiDoc [Tra]. The LTANS group [LTA] brings forward the standardization in this area. However, long-term retention in the context of e-voting has not yet been addressed before and the question as to which data should be retained is unanswered. [VK06] focuses on the challenge of providing everlasting privacy for online elections that, at the same time, are based on cryptosystems that may be broken at some point in the future. But to the best of our knowledge, long-term retention in the case of electronic elections has not yet been studied thoroughly before.

Our paper is structured as follows. In Section 2 we review the regulations for paper-based elections in Germany and transfer them to online voting, providing legal requirements regarding long-term retention of election data in e-voting. In Section 3 we apply our results to a state-of-the-art e-voting protocol and evaluate which data must be retained in particular to meet the legal requirements we have derived. Following a more technical approach, we report on specific requirements regarding retention in e-voting in Section 4: Which security objectives must be achieved? Which measures should therefore be applied? We also provide concrete recommendations regarding the technical implementation, referring to the protocol we have analyzed in Section 3. Concluding remarks are given in Section 5.

## **2 Legal Framework**

In the following we analyze the legal regulations that apply to selected election types in Germany, reaching from governmental elections for democratic decision-making to non-governmental elections in civil society.

## **2.1 Legal Requirements for Conventional, Paper-based Elections**

### **Parliament.**

Elections of the German Bundestag take place every four years [Sch98]. They are subject to the Federal Electoral Law (Bundeswahlgesetz – BWG) and specified by the Federal Election Ordinance (Bundeswahlordnung – BWO), which contains provisions for documentation and safekeeping of the election material. According to Art. 72 BWO, the election board has to keep a record of the election process, the vote counting and the election results. Discarded ballot papers must be enclosed in the record as well as envelopes and polling cards whose validity has been questioned. The record has to be approved and signed by the members of the election board. All documents are handed over to the municipality hereafter. The municipal authorities have to retain the election documents for a period determined by Art. 90 BWO. Protection against unauthorized access must be ensured. The following election documents have to be retained for six months, as long as no scrutiny procedure is pending and no law enforcement authority needs to investigate regulatory offences: the electoral roll, the polling card register, the register of invalid polling cards, and the register of persons (for example in hospitals or monasteries) who according to Art. 29 (1) BWO, were allowed to vote by a moving election board; furthermore, the form letters containing the signatures assisting the nomination of candidates. All the other documents such as voting papers, voting envelopes, and the documents of the postal vote have to be retained in accordance with Art. 90 (3) BWO for the whole legislative period of the Bundestag, until 60 days before the elections of a new Bundestag.

The longest retaining period for elections documents amounts to four years. This period may be extended if pursuant to Art. 49 BWG scrutiny procedures are pending or when regulatory offences (see Art. 107-108e StGB) need to be investigated by the law enforcement authorities. Consequently, the appropriate election documents may be needed for a period of longer than four years to be used as evidence material for the hearing or the proceedings.

### **Works Council.**

Elections of the works council are held every four years. The election process is governed by Art. 7-20 of the German Works Constitution Act (Betriebsverfassungsgesetzes – BetrVG) and, in detail, determined by a special election ordinance (Wahlordnung – WO). Documentation requirements are stipulated in Art. 18 BetrVG, Art. 16 and 19 WO. According to Art. 18 (3) BetrVG the election board has to establish a record of the election process subsequently to the termination of the election. The record must contain the total of the ballot envelopes handed in, the total of valid and invalid votes, the number of valid votes for every list of candidates, the distribution of seats to the lists, the names of the elected candidates, and finally, any incidents or matters that might affect the validity of the election. The record must be signed by the chairman and at least one different member of the election board (*writing requirement*). According to Art. 19 BetrVG an election may be contested if any of the essential rules regarding the right to vote, eligibility or the electoral procedure have been infringed and no subsequent correction has been made. In this case only infringements that verifiably could not have altered or influenced the election results will not affect the validity of the election. As a rule, contestations must be filed within two weeks of the announcement of the election results.

However, severe infringements exceptionally may be claimed even hereafter, whereupon the election result might be declared void at any time. Art. 19 WO therefore stipulates that the newly elected works council has to retain all relevant election documents at least until the end of its term of office. These documents are, in addition to the record of the election board, any other documents in the broadest sense that might be relevant in case of election contest: for example ballots, announcements of the election board and the envelopes of late postal votes that were not counted.

### **Governing Boards of Social Security Institutions.**

Elections of the governing boards of the social pension funds as well as for the health, nursing and accident insurances take place every six years. The election process is governed by Art. 43 et sqq. of the Social Security Code (SGB IV) and by the special Electoral Ordinance for that sector (SVWO). According to Art. 91 SVWO there is a general obligation to retain the election documents for the whole term of office of the governing boards. However, the voter's election pass, the ballot papers, the ballot envelopes and the postal voting envelopes can be discarded if the election is not contested one month after the announcement of the final results (see Art. 57 (3) SGB IV). In case of an election contest, these documents have to be retained for at least two months after the court decision has become legally binding, as far as no special reasons demand further retaining.

## **Executive Committee of an Association.**

The executive committee of an association is elected at the annual general membership meeting [Kur04]. The election procedure is organized pursuant to the provisions of Art. 28 et sqq. of the German Civil Code (BGB), if the articles of association do not stipulate something else (Art. 40 BGB). Details of the electoral procedure, for example the voting principles, the eligibility requirements, or the modality of the election performance, may be regulated according to the discretion of the body setting down a separate voting statute of the association [Rei07].

On the association level, elections have already been carried out electronically: The German Informatics Society as well as the German Research Foundation have issued their own e-voting statutes (cf. [Ges04], [Deu06]). Both of them comprise provisions concerning the retention of electronic election documents and the voting software which provide for a retention period according to the term of office of the executive committee, i.e. two and four years, respectively.

## **2.2 Obligations for Documentation and Retention in E-Voting**

Legal rules governing elections demand a thorough documentation of the election process and the retrieval of the results. Even if it is not explicitly stipulated (as for the elections of the executive committee of an association), a preservation of these documents is necessary to prove the dual process of the election and the correct calculation of results. As a rule these documents should be stored at least for the term of office of the elected body. E-Voting systems must provide for an appropriate electronic documentation to prove the compliance with basic voting principles. The election host therefore must be able to demonstrate how the technical or organizational processes which could alter or influence the election results work in general and if the system functions properly. For this purpose the election host must be able to prove the security of the relevant components and applications of the voting system. The tallying process must be verifiable and hence repeatable. Thus, in particular the number of cast and counted ballots – including the number of valid and invalid ballots – must be documented, as well as logging files that can exclude any manipulation of the system. It should be possible to recount the election results by a trustworthy counting program. If legal norms require paper-based documentation (e.g. for the record of the election board), printouts can be generated and signed by the responsible authority. According to German law, it is also possible to replace the handwritten signature by a qualified electronic signature. In any case, qualified signatures should be used to provide for the integrity and authenticity of the electronic documentation [Siga].

### 3 Implementing Legal Requirements: A Concrete Example

In the following, we apply our results regarding legal stipulations on long-term retention to the e-voting scheme designed by Juels, Catalano, and Jakobsson (JCJ) [JCJ05]. First we give a short description of the protocol. Hereafter we investigate which of the occurring data must be retained in order to meet the legal requirements we have identified in Section 2.

#### 3.1 Protocol Description

The scheme proposed by JCJ was the first one to offer coercion-resistance, which means that a voter cannot be forced to abstain from voting or to vote in a particular way. In effect, a potential adversary cannot learn whether the coerced voter complied with his demand. To achieve this, the JCJ scheme is designed such that the identity of the voter remains hidden during vote-casting and validity of the ballot is verified by blind comparison against an electoral roll. For this, secret anonymous credentials are distributed among the voters during registration phase. These credentials serve two purposes: Firstly, they are employed for authentication and authorization of the voters. Secondly, they mark a “free” vote in the sense that this vote indeed expresses the voter’s will; if a voter wants the vote to be accounted, she includes her valid credential. If she casts the vote under coercion, she attaches an invalid credential. The coercer is not able to distinguish invalid credentials from valid ones and hence cannot know if the voter has complied with his demand. Since multiple voting is allowed, the voter can hereafter cast a valid vote. In the end, only the latest vote with a valid credential is accounted in the tallying process.

##### **Registration.**

The identity and eligibility of each voter is first verified by the registration authority. Upon successful verification, voter  $v_i$  receives a unique valid credential  $\sigma_i$  from the registration authority over an untappable channel. An encrypted version  $S_i$  of this credential is published on the bulletin board. At the end of registration phase, the electoral roll  $L$  contains all valid encrypted credentials alongside the plaintext names of registered voters and is signed by the registration authority. The registration authority is assumed to be trustworthy, but can also prove to a voter that  $\sigma_i$  is authentic, i.e. that  $S_i$  is a valid encryption of  $\sigma_i$ . However, it must be assumed that the registration authority does not leak credentials to an adversary.

##### **Voting.**

The registration authority publishes an integrity-protected candidate list  $C$ . For voting, the voter  $v_i$  casts a ballot over an anonymous channel. The ballot comprises the following parts:

1. A probabilistic encryption of the chosen candidate  $c_j$ , hereafter referred to as the *vote*
2. A probabilistic encryption of the voter's credential  $\sigma_i$
3. A non-interactive zero-knowledge proof (cf. [BSMP91]) that  $c_j$  is in  $C$
4. A non-interactive zero-knowledge proof of knowledge of  $\sigma_i$  and  $c_j$

Voter  $v_i$  encrypts her valid credential  $\sigma_i$  if she wants her vote to be accounted, otherwise she encrypts a fake credential  $\sigma_i'$ . The proof that  $c_j$  indeed marks a valid candidate is necessary since casting write-in votes could compromise coercion-resistance. Knowledge of  $\sigma_i$  and  $c_j$  must be proved to prevent replay-attacks by simply re-encrypting votes that have already been cast.

### Tallying.

**1. Proof checking.** The tallying authority first checks that all proofs included in each ballot are correct. Ballots containing invalid proofs are discarded. For all the remaining ballots, let  $A_1$  denote the list of encrypted votes and  $B_1$  the list of encrypted credentials.

**2. Duplicate removal.** Next, the tallying authority removes ballots with credential duplicates via plaintext equivalence test (see [JJ00]). Only the latest credentials in  $B_1$  are kept, resulting in a weeded list  $B_2$ . The ciphertexts in  $A_1$ , which correspond to duplicate credentials are also removed, resulting in a weeded list  $A_2$ . Now there is no more than one vote per given credential.

**3. Mixing.** The list of encrypted votes as well as the list of encrypted credentials is mixed using the same, secret permutation.

**4. Validity checking.** The credentials from  $B_2$  are compared with the ones in  $L$  via plaintext equivalence test, eliminating those which do not correspond to valid credentials in  $L$ . The corresponding invalid votes from  $A_2$  are eliminated as well. Let  $A_3$  and  $B_3$  denote the final lists. These now correspond to authentic ballots cast freely by eligible voters with no more than one vote per voter.

**5. Vote counting.** Finally the votes in  $A_3$  are decrypted and tallied.

### 3.2 Meeting Legal Requirements

We now investigate which data should be retained in order to meet the legal obligations specified in 2.2. Here we only specify *which* data is to be stored. Comments on the question *how* this should be done will be given in Section 4.

First of all, the list  $L$  is to be kept; it denotes the eligible voters and contains their valid, encrypted credentials. Furthermore, the list  $C$  should be stored since it contains the names of the candidates including unique identifiers used for vote-casting.

Let  $N$  denote the total number of ballots cast in the election. This value includes also multiple ballots cast by single voters under valid as well as invalid credentials. In 2.2 we have stated that that the number of cast and counted ballots – including the number of valid and invalid ballots – must be documented. Hence, we first have to determine what “invalid” votes actually are with regard to the analyzed voting scheme. As mentioned before, for the JCJ scheme to remain coercion-resistant, it is excluded that voters cast write-in votes, which means that they vote for candidates that are not on list  $C$  and hence are invalid. This implies that voters cannot cast invalid votes, i.e. ballots that have been invalidated by the content of the vote and not by using an invalid credential. A ballot can thus only be invalid for one of the following reasons:

- (a) It contains an invalid proof
- (b) It has been cast under a valid credential, which was later on re-used to vote
- (c) It was cast under an invalid credential

The number of ballots corresponding to the these categories are the following:

- (a)  $N - |B_1|$  (see phase 1 of the tallying procedure)
- (b)  $|B_1| - |B_2|$  (see phase 2 of the tallying procedure)
- (c)  $|B_2| - |B_3|$  (see phase 4 of the tallying procedure)

According to 2.2 the retrieval of the election result shall be documented, which includes also ballots that have been declared invalid. In particular, ballots that contain invalid proofs and hence are to be discarded in phase 1 of the tallying procedure should not be deleted but rather kept for retention and just eliminated from the tally. For being able to exclude replay attacks, the valid proofs of knowledge of the tallied votes should be kept as well.

Subtracting the number of invalid ballots specified above from the total of  $N$  ballots gives  $N - (N - |B_1| + |B_1| - |B_2| + |B_2| - |B_3|) = |B_3|$  valid ballots. This is no surprise since  $B_3$  contains the valid, unique credentials under which votes have been cast. This list should be retained, as it must be verifiable that only eligible voters have cast a ballot.

Re-tallying of the votes requires retaining list  $A_3$  since it contains encrypted votes, which correspond to the valid, unique credentials in  $B_3$ .

Besides protocol-specific data we have just considered, additional material must be retained. According to the legal stipulations, it must be provable that the system functions properly and no manipulations have been performed. System auditing files as well as logging files of intrusion detection systems in use should therefore be retained in addition to the material specified above.

## 4 Technical Implementation of Long-Term Retention

In this section we address the technical realization of long-term retention. First we appoint the technical requirements for electronic and electronically signed voting material to meet legal obligations. Next we outline suitable technical protection methods. Finally we apply the results to the scheme proposed by JCJ, which we have introduced in Section 3.

### 4.1 Requirements for E-Voting

General requirements for the technical implementation of long-term retention are specified in [RFDJ07] and [WPB07]. In the following these requirements are transferred to e-voting:

**Integrity.** Any kind of retention is targeted at preserving the integrity of a document, i.e. preserving it as it originally has been created. Undetected modification or deletion of any election document, in particular the electronic ballots, must be prevented. Integrity – and hence the whole election – is compromised otherwise.

**Authenticity.** The authenticity of the documents must be preserved to keep the originator of the document identifiable. In case of electronic elections, special attention must be paid to the task of ensuring authenticity of the ballots (e.g. confirmed by a validating authority) on the one hand while providing for strict anonymity of the vote on the other hand.

**Completeness.** Since the whole election process has to be documented, the connection of the single election documents should be preserved.

**Confidentiality.** Voting material containing personal data of the voters must be protected against unauthorized knowledge. For instance the voter's signature includes the voter's certificate, which may contain sensitive personal data of the voter.

**Negotiability.** A document is negotiable if it is possible to transfer it if from one system to another without losing the possibility to check the characteristics of the document, for example, its integrity. In case of contestations, the evidential voting material has to be presented before the court without any quality loss.

**Readability.** The voting documents have to be readable, i.e. hardware to access the stored data must be available as well as software to interpret and present it. We assume that permanent availability of the voting data during the retention period is not required.

### 4.2 Technical Protection Methods

In the following, we present existing technical protection methods and evaluate them on the basis of the requirements defined above. The protection methods are divided into the following categories according to [RFDJ07]:

**System-oriented.** Data access is controlled by a technical system. By configuring the archiving system accordingly, access is restricted to certain components or persons. An example is write protection on a file system defining groups with reading and writing privileges.

**Medium-oriented.** This category includes storage media for which the overwriting or manipulating of the stored information is not possible, e.g. WORM (write once read many) or other non-rewritable media.

**Document-oriented.** This comprises technologies to preserve documents against unauthorized extraction of content and undetected modifications, for example encryption and qualified signatures.

In [RFDJ07] some protection methods out of every category are evaluated. At this point we pick up this evaluation and work out recommendations for the retention of e-voting documents.

### **Using Qualified Signatures.**

As mentioned in Section 2 qualified signatures should be used to provide provability of the integrity and authenticity of the election documentation. A qualified signature proves that the data has not been modified and ensures that the originator of the signed document can be identified.

Signatures are also a suitable method to ensure completeness and negotiability. Completeness may be guaranteed by pooling all voting documents and signing this collection. Furthermore, a signed document is negotiable because any third person is able to verify the signature and thus prove the integrity and authenticity of the document. In contrast to signatures, system-oriented methods limit the negotiability of a document: An unsigned document protected by access control in a given system loses this protection when given to a third party. The third party is not able to verify the integrity of the document and has to trust the applied system or must verify its security.

### **Using Well-Known, Standardized Signature and Data Formats.**

To ensure negotiability, accepted or standardized data formats should be used. If a rare and unknown format is used, the court will have to consult an expert opinion, which may cause great costs. Well-known or standardized signature formats are:

1. CMS (Cryptographic Message Standard) [Hou04]
2. XML signatures [ERS02]
3. PDF/A (ISO 19005-1:2005, this ISO standardization of the PDF/A specification includes the electronic signature)

General usage of standardized formats increases the probability that appropriate software is available and hence contributes to long-term readability.

### **Access Restriction During the Retention Period.**

As previously mentioned, qualified signatures conserve the provability of signed documents, but they do not protect against modifications during the retention period. Therefore, additional protection methods are necessary. Suitable are non-rewritable media or system-oriented methods for the file system, document management systems or archive systems where the document is stored, e.g. access control software or a read-only mode for the documents. An alternative is the usage of any portable storage media as DVD or USB, which are deposited at a place accessible only by authorized persons. By access restriction the confidentiality of retained sensitive voting data can be achieved as well.

### **Redundant Data Management.**

In general it is useful to hold the data redundant to safeguard against loss in case of unexpected impacts such as theft or fire. For this purpose, backups should be provided and kept in at a different place.

## **4.3 Long-Term Aspects**

The retention period has great influence on the realization of retention since all technical protection methods are subject to an aging process and require an update. In the following we select long-term aspects important for e-voting.

Generally, obsolete archive systems and storage media have to be replaced by state-of-the-art technologies. During the replacing process data must not be modified or lost. We assume that currently available hardware that meets the minimal quality standard is durable for the expected retention time in e-voting.

In the case of electronic signatures, an aging process applies as well. After a certain time, the underlying cryptographic algorithms and parameters become insecure. Thus signatures lose their integrity and authenticity and hence their probative value. This process may be significant after six years and therefore concerns signed e-voting documents. In Germany, according to §6 of the Signature Act [Siga] and §17 of the Signature Ordinance [Sigb] electronic signatures have to be renewed by a new qualified electronic signature before the used algorithms lose their security suitability. In the concept of signature renewal the new signature is performed by a time stamp. A time stamp is issued by a time stamp service, which signs the document after adding a date. In the ArchiSig project [Arc] a concept has been developed in which a lot of documents are renewed by one time stamp [RS06]. At first the documents are merged in a hash tree in accordance with Merkle [Mer80]. Then a time stamp for the root hash value of the tree representing all documents is requested. This procedure is independent of document formats and more cost-efficient since qualified time stamps usually require a fee. The concept complies with the German and European Signature Law [Roß04]. The LTANS group [LTA] brings forward the standardization in this area, cf. [BPG07]. However, only few products exist which handle signature renewal.

E-Voting protocols such as the JCJ scheme mentioned in Section 3 usually employ encryption to ensure confidentiality. The aging process of cryptographic algorithms also influences the encrypted data. With the decreasing security suitability of the used algorithms, the encrypted document loses its confidentiality. Therefore additional measures should be taken during the retention period to ensure confidentiality.

#### **4.4 Applying the Results to the JCJ Scheme**

Finally, we briefly comment on long-term retention methods for the JCJ scheme discussed in Section 3.

While, for example the electoral roll  $L$  is supposed to be signed by the registration authority, most of the other data which is to be retained such as the lists  $A_3$  and  $B_3$  are a priori not signed. However, it is not sufficient to store the data unsigned since both data integrity and authenticity has to be provable before the court. Therefore it is inevitable to sign the material. Signing all lists including  $L$  by one authority additionally proves the completeness of the voting material. As recommended in Section 2, qualified signatures should be used.

To ensure negotiability, a non-proprietary format should be chosen for the lists. Otherwise the lists can only be interpreted and presented by appropriate proprietary software. To prove the compliance with essential voting rules, the security of the software must be examined. To ensure confidentiality, the encrypted credentials in the lists have to be protected against unauthorized access before the encryption parameters and algorithms become insecure.

## **5 Conclusion**

Long-term retention is an important issue in e-government and e-voting in particular. Electronic elections can only become legally binding if legal obligations on long-term retention are met. We have transferred the legal regulations on paper-based elections in Germany to the scenario of online elections, providing guidelines for long-term retention in e-voting. Following an exemplary e-voting protocol we have analyzed which data must be retained concretely. We have also provided technical requirements for retaining voting documents and recommended technical protection methods. Our work shows that the requirements of long-term retention should be taken into account already when designing an e-voting protocol or selecting a scheme to be used for a practical implementation. We believe that we hereby contribute to building the foundations of e-voting and help advancing online elections, not only in Germany.

## References

- [Arc] The ArchiSig Project. <http://www.archisig.de/>, last checked 26.02.2008.
- [BPG07] Ralf Brandner, Ulrich Pordesch, and Tobias Gondrom. Evidence Record Syntax (ERS). RFC, 4998, August 2007. <http://www.ietf.org/rfc/rfc4998.txt>, last checked 25.02.2008.
- [BSMP91] Manuel Blum, Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Noninteractive Zero-Knowledge. *SIAM J. Comput.*, 20(6):1084–1118, 1991.
- [Cou04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11, September 2004. [http://www.coe.int/T/e/integrated\\_projects/democracy/02\\_Activities/02\\_e-voting/](http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/), last checked 13.02.2008.
- [Deu06] Deutsche Forschungsgemeinschaft. Wahlordnung für die Wahl der Mitglieder der Fachkollegien der Deutschen Forschungsgemeinschaft (DFG), 2006. [http://www.dfg.de/forschungsfoerderung/formulare/download/70\\_01.pdf](http://www.dfg.de/forschungsfoerderung/formulare/download/70_01.pdf), last checked 25.02.2008.
- [DOM] DOMEA-Konzept. [http://www.kbst.bund.de/cln\\_011/nn\\_836960/Content/Standards/Domea\\_Konzept/domea\\_node.html\\_nnn=true](http://www.kbst.bund.de/cln_011/nn_836960/Content/Standards/Domea_Konzept/domea_node.html_nnn=true), last checked 28.02.2008.
- [ERS02] Donald Eastlake, Joseph Reagle, and David Solo. (Extensible Markup Language) XML-Signature Syntax and Processing. RFC, 3275, March 2002. <http://www.ietf.org/rfc/rfc3275.txt>, last checked 26.02.2008.
- [ETS03] ETSI TS 101 733 V1.5.1, 2003.
- [Ges04] Gesellschaft für Informatik. Ordnung der Wahlen und Abstimmungen, 2004. <http://www.gi-ev.de/fileadmin/redaktion/OWA/gi-owa.pdf>, last checked 24.02.2008.
- [Ges05] Gesellschaft für Informatik. GI-Anforderungen an Internetbasierte Vereinswahlen (“GI requirements for Internet based elections in non-governmental organizations”), August 2005. [www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen\\_Vereinswahlen.pdf](http://www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf), last checked 13.02.2008.
- [Hou04] Russ Housley. Cryptographic Message Syntax (CMS). RFC, 3852, July 2004. <http://www.ietf.org/rfc/rfc3852.txt>, last checked 26.02.2008.
- [Int] The InterPARES Project. <http://www.interpares.org/>, last checked 25.02.2008.
- [JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, WPES, pages 61–70. ACM, 2005.
- [JJ00] Markus Jakobsson and Ari Juels. Mix and Match: Secure Function Evaluation via Ciphertexts. In Tatsuki Okamoto, editor, ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, pages 162–177. Springer, 2000.
- [Kur04] Kurt Stöber. Handbuch zum Vereinsrecht. Otto Schmidt, München, 2004.
- [LTA] Long-Term Archive and Notary Services (Itans). <http://www.ietf.org/html.charters/ltans-charter.html>, last checked 26.02.2008.
- [Mer80] Ralph C. Merkle. Protocols for Public Key Cryptosystems. In IEEE Symposium on Security and Privacy, pages 122–134, 1980.
- [nes] nestor – The German Network of Expertise in Digital Long-Term Preservation. <http://www.langzeitarchivierung.de/index.php?newlang=eng>, last checked 28.02.2008.
- [PAD] PADI – Preserving Access to Digital Information. <http://www.nla.gov.au/padi/>, last checked 28.02.2008.
- [Rei07] Bernhard Reichert. Vereins- und Verbandsrecht. Luchterhand Verlag, 2007.

- [RFDJ07] Alexander Roßnagel, Stefanie Fischer-Dieskau, and Silke Jandt. Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, August 2007. <http://www.bmwi.de>, last checked 25.02.2008.
- [Roß04] Alexander Roßnagel. Signaturgesetzkonformität des Standardisierungsvorschlags “Long-Term Conservation of Electronic Signatures” für die ISIS-MTT Spezifikation vom 30.6.2004, July 2004. [http://www.teletrust.de/fileadmin/files/ag8\\_isis-mtt-gutachten-langzeitsig.pdf](http://www.teletrust.de/fileadmin/files/ag8_isis-mtt-gutachten-langzeitsig.pdf), last checked 28.02.2008.
- [RS06] Alexander Roßnagel and Paul Schmücker. Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit? Economica Verlagsgruppe Hüthig Jehle Rehm GmbH, Heidelberg, 2006.
- [Sch98] Wolfgang Schreiber. Handbuch des Wahlrechts zum Deutschen Bundestag. 1998.
- [Siga] German Electronic Signature Act (Gesetzliche Rahmenbedingungen für elektronische Signaturen, SigG). [http://bundesrecht.juris.de/sigg\\_2001/index.html](http://bundesrecht.juris.de/sigg_2001/index.html), last checked 13.02.2008.
- [Sigb] German Electronic Signature Ordinance (Verordnung zur elektronischen Signatur, SigV). [http://bundesrecht.juris.de/sigv\\_2001/index.html](http://bundesrecht.juris.de/sigv_2001/index.html), last checked 13.02.2008.
- [Tra] Legally Secure Transformations of Signed Documents. <http://www.transidoc.de>, last checked 20.01.2008.
- [VK06] Melanie Volkamer and Robert Krimmer. Online-Wahlen und die Forderung nach zeitlich unbegrenzt geheimen Wahlen. Working Paper Series on Electronic Voting and Participation, 02/2006, 2006.
- [WPB07] Carl Wallace, Ulrich Pordesch, and Ralf Brandner. Long-Term Archive Service Requirements. RFC, 4810, March 2007. <http://www.ietf.org/rfc/rfc4810.txt>, last checked 25.02.2008.