

The Role of Digital Signature Cards in Electronic Voting

Robert Kofler, Robert Krimmer, Alexander Prosser, Martin-Karl Unger

WU Vienna University of Economics and Business Administration

Department of Production Management, Pappenheimgasse 35/5, AT-1200 Vienna, Austria

{robert.kofler | robert.krimmer | alexander.prosser | martin.unger}@wu-wien.ac.at

Abstract

As electronic voting enters the stage of real-world implementations, digital signature cards emerge as a basic infrastructure element for e-voting. The paper focuses on three main functions of such cards: (i) Authentication and (as National ID Card also) identification, (ii) as a storage media and (iii) as a secure processing environment. These properties enable protocols for secure e-voting, which guarantees the General Voting Principles.

However, the diffusion of digital signature cards is still relatively low and in many cases, electronic vote casting has to be implemented without such cards. The paper reports on a test election conducted in Austria in May 2003 using a protocol designed for digital signature cards, which was adapted to a case, where such cards are not (yet) available. The necessary adaptations clearly show the importance of digital signature cards for secure e-voting.

1. Election Protocols

1.1 General Voting Principles

The General Voting Principles as specified, for instance in the Austrian Federal Constitution are [38]:

- General voting specified that nobody is to be excluded from the election; this is achieved by maintaining paper-based voting systems.

- The principle of immediate voting demands that the votes have to reach the central voting-teller directly and non-altered. The principle of equal voting demands that each individual can cast her/his vote only once and that all votes have the same weight. Of course, e-voting is a different media and cannot exactly emulate a paper-based ballot (e.g., the electronic media can guide users through complex and error-prone voting procedures thereby effectively excluding an unintentionally invalid vote; hence, a group that votes electronically has a higher potential to cast valid votes than a paper-based group; does this discriminate one

against the other?). It still remains to be decided, how "equal" the two voting media have to be.

- Much more problems are in the principles of secret, personal and free voting. e-Voting poses similar problems like postal voting. In both the votes are not given within a secure polling booth, but the voters themselves must look for the secret and free voting act. Therefore postal voting is allowed only in some countries and also there only in exceptional cases.

The criteria specific to e-voting were suggested in an Internet Policy Report [18] on e-voting as (i) correctness in counting votes, (ii) dishonest voters cannot disturb the election, (iii) permanent anonymity, (iv) voters can only vote once, (v) only authorised voters may vote, (vi) independence (no undue influence is exercised on the voter), (vii) verifiability, (viii) receipt-freeness (voters cannot prove how they voted).

1.2 E-voting Protocols: Different Approaches

There are several cryptographic approaches in the literature to implement secure e-voting:

Anonymous channel. These approaches date back to Chaum's proposal of a MIX net [7], where the original message is encrypted with the public keys from several servers and then passed from one server to the next, each decrypting with its private key and passing the message on to the next server in large batches with a different order (mixing). The problems with this approach – which Chaum intended for a completely different application – are that at least one of the mix servers has to be honest; if, consequently, the number of servers is increased, the protocol becomes slower and more vulnerable and to prevent mixers to introduce fake votes.

Extensions of the original schema can be found in Park et al. [28] and in Sako and Kilian [33], however, both schemes were broken ([27], [17]). Later approaches by Abe [1] and Jakobsson [19, 20] apart from algorithmic improvements add much to the stability and performance of the protocol and the computational effort in the client is reduced

considerably (one collective key instead of several consecutive keys); however, it still has to be analysed and tested in prototype implementations, whether the basic difficulties in MIX nets have been completely addressed.

All-or-nothing disclosure of secrets (ANDOS). ANDOS protocols provide a sender-anonymous channel. They emulate the anonymous purchase of a bitstring [3]. This could be used in one-stage or two-stage protocols. Nurmi et al. [24] and Salomaa [34] suggested issuing voting tokens using ANDOS, which can then be used anonymously to cast a vote. There are improvements of the protocol in terms of efficiency and complexity by Niemi [22] and Hassler and Posch [15], but one of the main disadvantages of ANDOS protocols still is their limited scalability, also voters can prove how they vote, which enables vote buying.¹

Homomorphism. The vote is cast as a binary yes/no vote, encoded following a homomorphic scheme, and submitted to a number of ballot box servers. Due to the homomorphism the summary count of yes/no votes is possible without having to know the individual votes. [10] This advantageous property is also the main problem of the approach: Only binary votes can be cast.

Blind signature. The best known along these lines is certainly Fujioka, Okamoto and Ohta [14], which has also been implemented several times². This protocol, in spite of its popularity, has some fundamental problems concerning voter anonymity and in that fake votes for non-voters can be introduced by the administration.³ The problem of introducing fake votes was addressed by [4] by introducing voter pseudonyms sent through anonymous channels to all candidate servers, which are then used to authenticate the vote itself.

This adds considerable complexity to the protocol and the paper does not propose the details of the necessary anonymous channel; this would have to be subject to further research. In a later extension proposed by Okamoto [26] the problem is addressed by having several blind signature servers, anonymity relies on the usage of a MIX net with the limitations already mentioned above.⁴

¹ The last issue was addressed by Niemi and Renvall in a later paper, but the algorithm pre-supposes the use of a secure voting booth and involves high computational efforts [23].

² A published reference can be found in [32], [9]; there are a number of commercial prototypes.

³ For a comprehensive criticism cf. [31].

⁴ Performance problems with several, additive blind signatures were solved by the protocol in [16], which uses cascaded multi-signatures.

Schneier proposed an interesting extension to the blind signature voting schemes [36]. The protocol combines registration and voting in one stage and voters generate several empty ballot sheets and submit them to a registration server. The server may request the keys to open some of these ballot sheets; one is returned signed blindly. The protocol ensures that no faulty votes are blindly signed, however, the protocol does not offer any mechanism to protect anonymity other than the [14] protocol. The same applies to [5]. Both make use of MIX channels.

The blind signature approach seems to be the most promising, for it has the potential to preserve voter anonymity and to check election fraud; also, it scales well. Prosser and Müller-Török⁵ developed a blind-signature based protocol, which clearly shows to what extent the realisation of secure e-voting depends on digital signature card infrastructure.

1.3 A Two-stage Voting Protocol

Voting systems do not only have to provide secure (above all, anonymous) Internet voting on the application (=cryptographic) layer, but the system has to be considered in its entirety. Here, any type of fraud on the operating system level has to be considered as well. That is why the protocol strictly separates registration and voting stage:

Registration:

1. The registrator has one blind signature key pair (e, d) per constituency c ; each trust centre participating in the election has its (\mathcal{E}, δ) .
2. The voter sends his voter ID to the registrator, which after checking the voter's eligibility answers with c and the appropriate e . The voter also polls her trust centre for \mathcal{E} .
3. The voter creates random tokens t and τ according to RSA and preparing them for a blind RSA signature $(b(t), b(\tau))$. c , $b(t)$ and a standard text applying for a signed e-voting token is sent to the registrator, which after checking the credentials again blindly signs and returns $d(b(t))$. The voter removes the blinding layer and obtains $d(t)$.
4. The voter obtains $\delta(\tau)$ in a similar way from the trust centre.

Storage:

⁵ [30, 31], which also contain a security analysis; for an earlier version, see [29].

The voter stores $t, d(t), \tau, \delta(\tau), c$ and her voter ID on a secure media.

Voting:

1. Some (all) candidates form RSA key pairs (k, k') and publish their respective k' . The k' are ordered (e.g., corresponding to the order on the ballot sheet).
2. On election day, the voter sends her ID and $t, d(t), \tau, \delta(\tau), c$ to the ballot box server, which knows all relevant e and \mathcal{E} .
3. If the ballot box can authenticate the tokens for the constituency indicated and if they have not already been used, it returns an empty ballot sheet BS and the relevant k' .
4. The voter codes the filled-in BS with k' and untamperably links the tokens to this $k'(BS)$. The ballot box once again checks the tokens and stores the ballot.

After the election finished, the candidates reveal their secret k and the ballot sheets are opened.

2. The Role of Digital Signature Cards

2.1 Authentication and Identification

Digital signature cards serve as a means of authentication based on the European signature directive [11]. Anybody can access the directory server of the respective trust centre to retrieve a person's public signature key and modulus to verify the signature of a document received.

This is to be distinguished from identification, where the person's identity is to be proven. This is the purpose of a National ID Card. Austria has already issued such a card [25] based on the Central Registry (Zentrales Melderegister, ZMR). For every person residing in Austria, address information is stored in the ZMR. Also citizens from other EU countries are stored, who may vote on the municipal level. In addition, also Austrian citizen's living abroad are stored in the ZMR, if their addresses are known (e.g., when they applied for a mail ballot from abroad). Basically, the National ID Card can be any digital signature card, which combines the digital identity of the holder (her trust centre certificate) and the real identity (the ZMR entry). This link is implemented by combining the public key (including the modulus) of the digital certificate and the ZMR number, where the

combination is digitally signed by the ZMR. This is referred to as Personal Identification (PI). Hence, the card can be used as a means of identification where also the constituency can be derived from the ZMR entry. There is no need for voters to specifically register for elections.

The system described above utilises both the authentication and the identification function: In the first step, the PI is sent to the registration server to determine the voter's identity and to derive the relevant constituency. The application for an election token is signed by the cardholder (for more details, see Section 2.3 on secure processing).

2.2 Storage Media

Such separation of registration and voting, however, raises the issue of where to store the election token between registration and election day, when the token is used to request a ballot sheet and to eventually cast a vote. General storage media, such as diskettes, hard disk drives, USB keys etc. are readily available, however, they are not linked to a person, they offer no or limited protection of the data stored, and most are error-prone and may result in loss of data. Also, they enable free replication of an election token. The above protocol does prevent multiple usage of election tokens, however, it is certainly not desirable to have multiple copies of an election token, which may even be produced by a legitimate process, such as a data backup.

Hence, the logical storage media seems to be the digital signature card or the National ID Card, resp. As a suitable storage media it has to fulfil certain privacy criteria:

- The election token has to be stored PIN-protected. This can be achieved: The current card issued by the main supplier a-trust [2], for example, offers at least 2 "info-boxes" which are 2K storage areas in the file system of the card which can be PIN protected. Industry-standard card readers can write and read these areas, once they have been created on card initialisation. Since after the election the token and all other data associated with the election protocol can be deleted from the card, the info-boxes can then be used for other purposes.

- There must be no information stored on the card unprotected, which enables an application to identify the cardholder. This is a decisive qualification, as the current version of the National ID Card stores the Personal Identification and the digital certificate without any protection. This would enable a fraudulent voting application to read personal information when accessing the token.

Due to the last restriction, the current National ID Card in Austria cannot be used for these purposes. Here, it becomes obvious that the card had originally been designed for a totally different paradigm, that there is no legitimate anonymous use of the card. However, since the card has to be renewed after three years to increase key length, the above anonymity requirements can be incorporated in the next generation.

2.3 Secure Processing

One of the main concerns in electronic voting is the possibility of fraudulent manipulations of the voter's PC or voting terminal. In some respects, this seems to be the primary concern in e-voting and the major impediment for implementing e-voting [18].

Digital signature cards, however, have the same problem in their basic function, that is digital signatures: A document could be displayed to the prospective signor and when it comes to the digital signature process⁶ a fraudulent programme resident on the signor's terminal could modify the document that is actually signed. This would undermine the entire system to the same extent as would the possibility to forge digital signature keys.

However, this problem was solved by Secure Viewers, which provide a secure tunnel between a viewing application which displays the document to be signed and the signature card. The signor can be assured that the document displayed and the byte string sent, compared to the digital signature card are identical. Therefore, the argument that e-voting is impossible because the PC is an insecure terminal *per se* cannot be maintained.

The algorithm proposed in Section 1.3 utilises the Secure Viewer delivered with the Austrian National ID card for signing the application for an election token and for displaying critical data stored on the card before it is released. Thereby the decisive elements of the protocol run in the operating system of the National ID Card.

This imposes additional requirements on the command set implemented in the operating system of the card.

3. Substituting the Functions of a Digital Signature Card

Although postal (absentee) voting is not enabled in Austria for National Elections, e-voting has been

⁶ For an introduction to digital signatures, see [37] and [12].

enabled for elections to the student union parliament based on §34 of the Student Union Law (HSG 2001).

For the acceptance of e-voting a study has been conducted right after the last Student Union Elections in June 2001, where two issues were under concern: (i) whether or not the students want to elect their representatives over the Internet and if (ii) e-Voting will replace traditional voting in the near future. In the study of the 1033 participating students 83,6 % prefer e-voting over booth voting and 71 % are of the opinion that e-voting will replace traditional forms of voting. [21]

For the results of the Internet election, e-voting.at defined two hypotheses: (H1) e-voting raises the voter turn out and (H2) e-voting results in the same results in the digital voting process as in the paper based voting process.

Since digital smart cards were not available in sufficient quantities, the implementation of the algorithm described in Section 1.2 was adapted for a test election without using the infrastructure of digital signature cards.

This replacement clearly shows where the value added of signature and National ID Cards is and it reveals the difficulties to realise secure e-voting without them. (Figure 1 provides an overview).

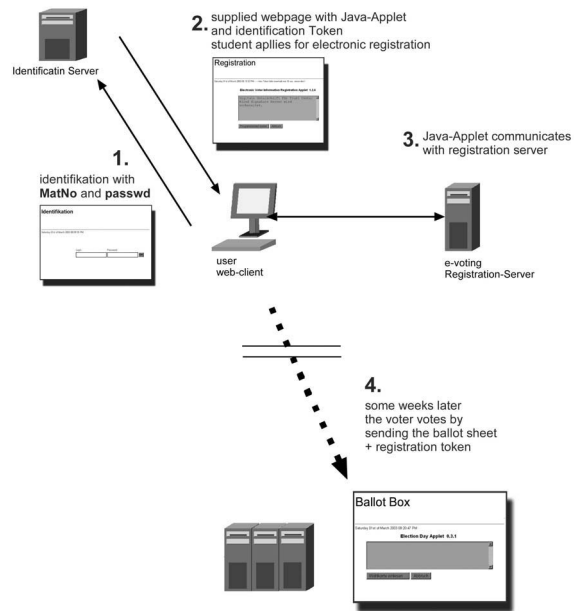


Figure 1: System used for the test elections

3.1 Authentication and Identification

Step 1. In contrast to the original algorithm the student does not use her student ID card with the digital

signature but identifies herself with a standard login procedure. This is done at a webpage of an inhouse identification system by entering the student identification number and their password.

Step 2. This system identifies the students and sends them a different via SSLv3 secured webpage which contains

- (1) The unique identification token and
- (2) The Registration Applet

This unique identification token is used to pass on the identification information from the service provider (in this case the university's IT department) which removes the necessity for the organization conducting the election to pass on individual data to service provider of the voting process. To do so this unique identification token consists out of several components:

(e,d) RSA keypair of identification unit
 MatNo..... Student's identification number
 S.....secret number, only known to the
 identification unit
 tokentime is a Unix timestamp

The unique token is generated by adding the secret number S to the unique student information number MatNo and hashing this information using SHA1, then adding a timestamp and finally signing the data with the private key of the identification unit. This includes the following properties: (i) this identification token can only be created by the identification unit, as it is signed with its private and secret RSA-key (d) so nobody else can calculate it, (ii) the combination of SHA1-encryption and (MatNo+S) guarantees a unique primary key in the registration database which cannot be decrypted and finally (iii) the timestamp is used to prevent resend-attacks by somebody who cracks the SSLv3/TLS-Protocol – therefore the identification unit and the registration unit must synchronize their system time. The timeout is calculated between the token time and the system time of the registration server. Useful values are between 15 and 30 seconds.

This unique token is then passed on to the registration unit.

Step 3. The registration server decrypts the token with the public-RSA key (e) of the identification unit and calculates the validity of the token time. If the token time is valid the registration server compares the "SHA1(MatNo+S)-part" of the token with its registration database and when TRUE it returns the constituency specific public key, so that the Applet can process its numbers for the blind signature and the token can be stored on a medium of choice of the student. The usage of the token is as described in Section 1.3.

3.2 Secure Storage

The test election system uses an arbitrary storage media where PIN protection of files is not available. Hence a different approach was chosen.

The voter chooses a password which is used as a secret key to encrypt and to decrypt the electronic voting permit. The electronic voting permit is encrypted with a user-supplied password before it is written into a file on the storage medium.

After the file which contains the electronic voting permit is read from the storage medium, the user is prompted to enter the password. The password is used to decrypt the electronic voting permit.

The file which contains the electronic voting permit can be accessed without knowledge of the password, but without entering the correct password it will not be possible to use that file for casting a vote.

3.3 Secure Processing

This point clearly shows how essential the use of smart cards for e-voting is. Literally nothing could be supplied to replace the security offered by the combination of a protocol run in the protected environment of the digital signature card and the Secure Viewer on the other.

That is why we hold that full compliance with the General Voting Principles can only be assured by the use of digital smart cards.

4. Summary

The paper outlined a digital signature card-based protocol for remote Internet voting and its requirements in terms of security. The central hypothesis is that secure voting following the General Voting Principles can only be implemented using digital signature cards as a secure processing and storage environment.

The voter turnout for the test election has been 36%; the real paper-based student union election could attract 26%, hence the turn-out in the electronic election was 40% higher than in the conventional, paper-based system.

A “workaround” solution that can be applied in the absence of digital signature cards was proposed. Such a system can substitute a National ID Card to some extent in terms of identification and authentication and secure storage, but it also shows the limitations of a non-smart card-based approach.

References

- [1] Abe M.: Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Centers. In: *Advances in Cryptology - EUROCRYPT '98*, Springer-Verlag, Berlin, 1998, pp. 437-447
- [2] a-trust: Certificate Policy für qualifizierte a.sign Premium Zertifikate für sichere Signaturen, Version 1.0, Vienna, 2003
- [3] Brassard, G., Crepeau, C., Robert, J.-M.: All-or-Nothing Disclosure of Secrets. In: *Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86*, Berlin, Springer Verlag, 1987, pp. 234-238
- [4] Baraani-Dastjerdi A., Pieprzyk J., Safavi-Naini R.: A Practical Electronic Voting Protocol Using Threshold Schemes. In: *Center f. Computer Security Research, Department of Computer Science, University of Wollongong, Australia*, 1994
- [5] Borrell J., Riera A.: Practical Approach to Anonymity in Large Scale Electronic Voting Schemes. In: *Universitat Autònoma de Barcelona, Departament d' Informàtica, Catalonia, Spanien*, 1999
- [6] Chancellerie d'Etat de Genève: Cahier des charges e-voting. In: http://www.geneve.ch/chancellerie/e-government/cahier_charges.html accessed on 2003-03-05
- [7] Chaum, D.: Untraceable electronic mail return addresses and digital pseudonyms in: *Communications of the ACM*, Vol. 24(2), 1981, p. 84-88
- [8] Chaum, David :Blinding for Unanticipated Signatures. In: Chaum, David; Price, Wyn (Ed.):*Advances in Cryptology, EUROCRYPT '87*.Springer-Verlag,Berlin 1987, S.227 –233
- [9] Cranor, L. F., Cytron, R. K.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: *Proceedings of the Hawaii International Conference on System Sciences (HICSS-97)*. Hawaii 1997. <http://lorrie.cranor.org/pubs/hicss/hicss.html> accessed on 2001-02-04
- [10] Cramer R., Gennaro R., Schoenmakers B.: A Secure and Optimally Efficient Multi-Authority Election Scheme. In: *Advances in Cryptology-EUROCRYPT'97, Lecture Notes in Computer Science 1233*, Springer-Verlag, Berlin, 1997, pp. 103-118
- [11] European Union: Directive 1999/93/EC, <http://www.qlinks.net/comdocs/elsig/> accessed on 2002-12-04
- [12] Feghhi, J.; Feghhi, J.; Williams, P.: *Digital Certificates – Applied Internet Security*. Addison-Wesley, Reading 1999
- [13] Gemeinde Fellbach.: *Jugendgemeinderat Fellbach*. <http://www.fellbach.de/wahlen> accessed on 2001-11-20.
- [14] Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: *Advances in Cryptology – AUSCRYPT92*. Springer-Verlag, Berlin 1993, pp.244 –251
- [15] Hassler, V. Posch, R.: A LAN voting protocol. In: *IFIP/SEC 95*, Capetown, 1995, pp.154-167
- [16] Horster P., Michels M., Petersen H.: Blind Multisignatures and their relevance for Electronic Voting. In: *IEEE-Press, 11th Annual Computer Security Applications Conference*, 1995, pp. 149-156
- [17] Horster P., Michels M.: Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme. In: *Asiacrypt'96, LNCS 163*, Springer-Verlag, Berlin, 1996, pp. 125-132
- [18] Internet Policy Institute: Report on the National Workshop on Internet Voting, Issues and Research Agenda. The Internet Policy Institute, Washington (DC), 2001. http://www.internetpolicy.org/research/e_voting_report.pdf, accessed on 2001-11-20
- [19] Jakobsson M.: A Practical Mix. In: *Advances in Cryptology - EUROCRYPT '98*, Springer-Verlag, Berlin, 1998, pp. 448-461
- [20] Jakobsson M.: Flash Mixing. In: *Information Sciences Research Center, Bell Labs, New*

- Jersey, <http://www.bell-labs.com/user/markusj> (2002-11-19)
- [21] Krimmer, R.: e-Voting.at: Elektronische Demokratie am Beispiel der österreichischen Hochschülerschaftswahlen, Thesis, WU Vienna, Vienna, 2002
- [22] Niemi V.: Cryptographic protocols and voting. In: Results and Trends in Theoretical Computer Science, Springer LNCS, Springer-Verlag, Berlin, 1994, pp. 307-316
- [23] Niemi V., Renvall A.: How to Prevent the Buying of Votes. In: Advances in Cryptology-Asiacrypt'94, Springer-Verlag, Berlin, 1995, pp. 164-170
- [24] Nurmi, H., Salomaa, A.; Santean, L.: Secret ballot elections in computer networks. In: Computers and Security 36 (1991) 10, pp. 553 – 560
- [25] OCG: Austrian Computer Society Membership Card, Vienna, <http://members.ocg.at/> accessed on 2002-12-05
- [26] Okamoto T.: An Electronic Voting Scheme: IFIP'96, Advanced IT Tools, Chapman and Hall, London, 1996, pp. 21-30
- [27] Pfitzmann B., Pfitzmann A.: How to Break the Direct RSA-Implementation of Mixes. In: Eurocrypt 89, Springer-Verlag, Berlin, 1989, pp. 373-381
- [28] Park, C., Itoh, K., Kurosawa, K.: All/Nothing Election Scheme and Anonymous Channel. In: Lecture Notes in Computer Science 765, Advances in Cryptology Eurocrypt 93, Berlin, Springer Verlag, 1994, 248-259
- [29] Prosser, A., Müller-Török, R.: Electronic Voting via The Internet. In: 3rd International Conference on Enterprise Information Systems ICEIS-2001, Setubal 2001, pp. 1061–1066
- [30] Prosser, A., Müller-Török, R.: Ein Algorithmus zur sicheren elektronischen Stimmabgabe über das Internet. Proceedings of the International Conference on Operations Research OR 2002, Klagenfurt, 2002
- [31] Prosser, A., Müller-Török, R.: E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. In: Wirtschaftsinformatik 44(2002) 6, pp. 545-556
- [32] Rivest, R.: Cryptography and Information Security Group Research Project: E-Voting. In: <http://theory.lcs.mit.edu/~cis/voting/voting.html> accessed on 2001-11-19
- [33] Sako, K., Kilian, J.: Receipt-Free, Mix-Type Voting Scheme. In: Lecture Notes in Computer Science 921, Advances in Cryptology Eurocrypt 95, Berlin, Springer Verlag 1995, pp. 393-403
- [34] Salomaa, A.: Verifying and Recasting Secret Ballots in Computer Networks. In: Maurer, H.A. (ed.): New Results and New Trends in Computer Science, Springer-Verlag, Berlin 1991, pp.283 –289
- [35] Soundcode VoteHere Inc.; Compaq Computer Corp.; Cisco Systems Inc.; Entrust Inc.: VoteHere Gold.Soundcode Inc.,Bellevue, 2001 <http://www.soundcode.com/voteheregold.html> accessed on 2001-07-20
- [36] Schneier B.: Applied Cryptography, Addison-Wesley, Boston, 1996
- [37] Tilborg van, H.C.A.: Fundamentals of Cryptology. Kluwers Academic Publishers, Boston 2000
- [38] Walter, R; Meyer, H.: Grundriß des österreichischen Bundesverfassungsrechts. 9th ed., Manz Verlag, Vienna 2000