(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 053 565 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
29.04.2009 Bulletin 2009/18

(51) Int Cl.:
G07C 13/00 *(2006.01)*

(21) Application number: **08159636.3**

(22) Date of filing: **03.07.2008**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA MK RS

(30) Priority: **03.07.2007 NL 1034079**

(71) Applicant: **N.V. Nederlandsche Apparatenfabriek NEDAP**
7141 DC Groenlo (NL)

(72) Inventors:
- **Hakvoort, Vincent**
  c/o N.V Nederlandsche Apparatenfabriek NEDAP
  7141 DC Groenlo (NL)
- **Hogen Esch, Johannes Harm Lukas**
  7122 ZN Aalten (NL)

(74) Representative: **Hatzmann, Martin et al**
Vereenigde
Johan de Wittlaan 7
2517 JR Den Haag (NL)

(54) Transparent election system with double vote rotation

(57) An Internet election system which consists of two independent servers, wherein the number of the chosen candidate is changed into the number of a different candidate with the aid of a double rotation offset. Both servers have a parameter for this rotation offset which is exclusively known to the respective server and the voter. The identity of the voter is known to the first server, which receives the vote, then converts it to the number of a different candidate by means of the first secret parameter and sends on this number together with an anonymous identification number to the second server. This second server converts this number to the number of the candidate which was chosen by the voter with the aid of the second secret parameter. The second server publishes the chosen candidate together with a verification number which is exclusively known to the second server and the voter, who can verify with this that the vote cast counts. With the original or a replacement polling card, the voter can also vote at a polling place, where a vote cast via the Internet is overwritten or revoked. The votes cast at the polling place can be processed in the same manner as the Internet votes, so that they can be verified as well and the outcome can be calculated.

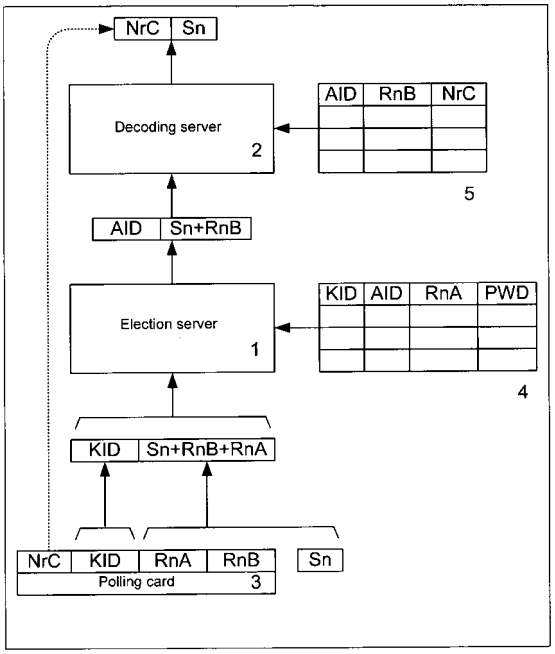


Fig. 1

EP 2 053 565 A2

Description

[0001] The invention relates to an election system, where the integrity of the vote is *inter alia* guaranteed by using a double vote rotation instead of the conventional encryption techniques. In the elections for parliament, the Provincial States and the local councils, a great transparency and verifiability of the system is desired and, despite the stringent certification, the trust in closed voting machines decreases. At the same time, the demand increases for more modern means, such as for instance the Internet, to be able to vote at a location and a time the voter chooses.

[0002] One of the most important requirements imposed on election systems is guarantee of the secret ballot. This means that it must be impossible to find a connection between the voter and a vote cast. With remote voting via, for instance, the Internet, this is a difficult problem, because, together with the vote cast, the identity of the respective voter needs to be transmitted as well to be able to determine that this voter is entitled and that only one vote is cast by this voter. The latter is also referred to as uniqueness. Further, the election system needs to be incorruptible, where the result cannot be influenced by the administrators of the different subsystems and is exclusively determined by the lawfully votes cast coming from voters. The whole system also needs to be verifiable without the secret ballot being jeopardized. Finally, the voter needs to be able to understand and trust the voting process.

[0003] In Dutch patent no. 1021632 of applicant, a system is described where the secret ballot is guaranteed by disguising a vote cast with votes for a random number of other candidates. In this solution, encryption techniques are likewise no longer necessary, but it is not possible to publish the contents of the ballot box in such a manner that the voter can determine whether his or her vote is in the ballot box without violating the secret ballot.

[0004] This verification by the voter is possible in the system according to Dutch patent application no. 1029723 of applicant, but here the voter cannot verify whether the overall outcome also matches the total of all votes cast.

[0005] The present invention contemplates a complete transparency and publication of all information with regard to the votes cast, so that a voter can determine whether his or her vote is in the ballot box, without it being possible to find a connection between these votes and the voters who have cast these respective votes. The system according to the invention further provides the possibility to make the votes cast at a polling place visible and verifiable for the voter as well and any citizen can calculate the outcome of the election on the basis of the published information.

[0006] The basis of this election system is that, with sufficient processing power and time, any form of cryptographic encryption of a vote can be converted, so that, with the exception of the standardized SSL (Secured Socket Layer) authentication of the servers, this is abandoned. Even all communication over the network being known must not result in violating the secret ballot. According to the invention, the election system is characterized in that this election system is provided with at least two independent computer servers, which are administered by independent trusted parties, wherein the designation of the candidate or blank vote that the voter wishes to vote for is changed into a voting code by the voter by means of a mathematical function, for instance with the aid of an election application on the voter's computer or with the aid of a polling card, wherein the election system is arranged such that, prior to the elections, each of the independent servers provides at least one secret parameter of this mathematical function for at least one voter, which is then, in the election system, exclusively known to the respective server and which is communicated to the at least one voter and wherein, during the elections, at least one first secret parameter of these secret parameters together with information about the identity of the at least one voter associated therewith are exclusively known to a first server of the at least two servers, an anonymous voter identification number of the at least one voter is exclusively known to the first and a second server of the at least two servers and the anonymous voter identification number and at least one second secret parameter of the anonymous parameters associated with the anonymous identification number of the at least one voter are exclusively known to the second server, wherein the first server operatively receives the voting code of the at least one voter, then converts the voting code to an intermediate code with the aid of the inverse mathematical function and the at least one first secret parameter known to the first server, and sends on this intermediate code together with the anonymous identification number associated with the at least one voter to the second server, which converts this information to the designation of the candidate that was chosen by the at least one voter with the aid of the inverse mathematical function and the at least one second secret parameter known to the second server, associated with the anonymous voter identification number of the at least one voter.

[0007] In particular, it holds that the voter can apply for a replacement polling card in case of damage or loss. Further, it particularly holds that, with the original polling card, the voter can also cast a vote at the polling place, while a vote cast via the network is overwritten and is cancelled. It also particularly holds that the voter can also cast a vote at the polling place with a replacement polling card, while a vote cast via the network is revoked and is cancelled. It also particularly holds that all transactions are stored in the servers so that, after the election, an audit is possible to verify whether the election process has proceeded properly.

[0008] Preferably, the system is further provided with a polling card for the at least one voter, the polling card being designed to cast a vote with the first server, via the Internet with the aid of the doubly rotated voting code,

where this double rotation per digit of a candidate number or preference number is stated on the polling card so that, in a simple manner, on the basis of the candidate number or preference number and this stated double rotation, a voting code can be deduced by the voter on the polling card, which voting code can be inputted into the voter's PC and can be passed on via the Internet and which represents the vote cast by the respective voter, without information being present or being sent on the voter's PC or via the Internet, from which the vote cast can be converted on the basis of the voting code. Here, inputting the voting code may be done with an application on an Internet server and a standard browser on the voter's PC, while no program needs to be downloaded. Also, in particular, voting can be done on information columns, for instance at stations or in other public places.

[0009] Preferably, the polling card is assembled from two parts glued together, of which the voter can simply remove one part, so that information which was covered first becomes visible, to prevent the individual parties involved in producing and printing the polling cards from having information with which a vote could be converted. Instead of two parts glued together, use may also be made of scratch varnish to cover information. Instead of two parts glued together, information which needs to be covered may also be printed through a closed envelope and only become visible after opening of the envelope. The designation of the candidate to be chosen or the designation of the preference of one or more options in a referendum can be represented by one or more digit (s), letter(s), icon(s) or a combination of these symbols. The polling card is, for instance, per digit of a number of a candidate, provided with a pair of columns which each comprise a first and second column, while, for each pair of columns, it holds that the possible values of a digit are included in the first column in a predetermined vertical order and while, viewed in horizontal direction, in the second column, behind each digit of the first column, there is a new digit or new character while, in use, for each digit of a number of a candidate, in the pair of columns associated with this digit, the voter looks for this digit in the first column and then determines which new digit or new character in the second column is behind this digit in the first column, while the new digits or new characters thus obtained are then combined by the voter to form the voting code associated with the vote. Here, the polling card may be provided with two side edges or information strips, which are provided with information relevant to the respective server by the decoding server and by the election server, respectively and can be kept as a physical counterfoil with the respective server to be able to demonstrate which information these respective servers have added to the polling card. At least one of the parts of the polling card may be printed partly black or with black figures on the side glued together, to prevent the covered information from being read out through the polling card or through the envelope. The polling card may be provided with a strip with which one can vote by proxy at a polling place, while, for determining the voting code, use is made of the double rotation of the proxy holder and where the principal can optionally verify via the Internet whether the vote or option agreed upon has actually been cast. On the polling card, the relevant information may not only be in a readable form, but also in a machine-readable form, such as for instance in the form of a bar code or OCR.

[0010] The election system according to the invention will be described hereinbelow with reference to some Figures, in which:

Fig. 1 schematically shows the system in which a vote is cast via a communication network such as for instance the Internet with the aid of an election application with the voter;
Fig. 2 schematically shows the principle of the double rotation of the vote cast;
Fig. 3 shows the substitution of the vote by an intermediate code, the substitution of the intermediate code by a voting code and vice versa;
Fig. 4 shows the front and the back side of part 1 of the polling card according to the invention, as it is manufactured by the printer and for substituting a vote by a voting code according to the principle of Fig. 3;
Fig. 5 shows the front and the back side of part 2 of the polling card, as it is manufactured by the printer;
Fig. 6 shows the front and the back side of the parts 1 and 2 of the polling card glued together;
Fig. 7 shows the front side of the card, after the Anonymous IDentification number (AID) has been provided by the decoding server;
Fig. 8 shows the front and the back side of the polling card as it is supplied to the election server;
Fig. 9 shows the front and the back side of the polling card after the Voter IDentification number (KID), the name and address information, the table with rotated options, the password and corresponding bar codes have been provided;
Fig. 10 shows the polling card as it is received by the voter in a window envelope;
Fig. 11 shows the back side of the polling card, after the strip which makes the verification number, the rest of the table and the bar code of the random second rotation RnB visible has been removed; and
Fig. 12 shows an example of a completed card, where the proxy strip for the polling place has also been torn loose, so that, with the remaining bar codes, a voting machine may optionally be released.

[0011] The secret ballot is guaranteed in the election system according to the invention by using at least two independent computer systems or servers, which are administered by independent trusted parties, such as for instance the municipality and a notary, while these individual parties cannot find a connection between the voter and the vote cast by this voter.

[0012] In the diagram of Fig. 1, the election server (1), which is located with the municipality, has linked the voter's name and address information to a voter identification code, in this example a voter identification number KID. The decoding server (2), which is located with the notary, has a list of random unique anonymous identification numbers AID, while this server generates at least one second secret parameter per AID, in this example in the form of a random rotation number (rotation value) RnB, prior to the election process. This also includes random selection by the server (2) of a number from a list with numbers or values generated elsewhere. This server also generates a unique verification number NrC prior to the election process. Also prior to the elections, for all voters, the polling card (3) is printed with an AID, an associated RnB and NrC by decoding server (2), where AID and RnB are printed both in a readable form and in the form of a bar code, or a similar code which can be machine-read. These numbers are stored in a table (5) by the decoding server (2). A part of the card is then folded double and sealed up, so that RnB and NrC together with the bar code of RnB are not readable anymore.

[0013] Then the polling cards are sent to the administrator of the election server (1), with which, with the aid of a bar code reader, the bar codes of the AID numbers of the cards are read out and stored in this election server (1) in table (4), together with a random KID to be issued by the municipality, at least one first secret parameter RnA, and a password PWD, with which the voter can obtain access to the election server (1). In this example, the at least one secret parameter is in the form of a random rotation number RnA. In this example, the random number is generated by the election server. This also includes random selection by the server (1) of a number from a list of numbers generated elsewhere. This information is printed on the card together with a machine-readable code, for instance bar code, for KID, PWD and RnA. The part of the card with RnA, PWD and the bar code of RnA and PWD is folded double and sealed up here as well, so that this information becomes unreadable as well.

[0014] The part of the polling card on which the AID number with associated bar code is printed is separated from the polling card, after the associated KID number is printed on this part as well, and is stored until after the election.

[0015] Finally, with the aid of the KID number, which is also on the remaining part of the card, the associated name and address information is printed on the card and the polling cards are sent to the voters.

[0016] In addition to folding double and sealing up a part of the card, it is also possible to send, for instance, the secret information RnB and NrC from the decoding server (2) to the election server (1) in a separate envelope per voter, which secret information is then sent to the voter together with the secret information RnA and PWD from this server in a second envelope. Another possibility is, for instance, applying a scratch varnish on the secret information so that it becomes unreadable for unauthorized persons.

[0017] The function of RnA and RnB is a rotation offset (rotation value) for the vote cast in order to disguise it therewith. So, the vote Sn is subjected to a mathematical function for obtaining a voting code Sn'. The voting code Sn' can be obtained with the aid of a special application on a voter's computer. The voter then inputs the KID, RnA and RnB stated on the polling card into his computer. On the basis of the vote cast, RnA an RnB, the computer determines the voting code Sn' with the special application. This voting code Sn' is then supplied to the election server (1) together with the KID and optionally the password associated with this KID, for instance via the Internet.

[0018] Also, the voting code can be obtained with the aid of a special polling card of the voter. Examples will be explained hereinafter.

[0019] So, the obtained voting code is inputted into the election server by the voter (directly or via the Internet with his computer). The election server and the decoding server subject the voting code to an inverse mathematical function (an opposite rotation offset on the basis of the rotation values of RnA and RnB) to obtain the vote. All this will hereinafter be explained in more detail on the basis of an example as an example.

[0020] Fig. 2 schematically shows the method of rotation disguise, where an election with six candidates is taken as an example. In this example, the designation for a vote to be cast consists of a number for the candidate. Since, in addition to a vote for the candidates, a blank vote is also possible, there are seven options in this example. The rotation with the aid of RnA and RnB is now carried out by calculating, per rotation, the modulus of the number of options over the sum of the candidate number of the chosen candidate or blank vote and RnA and RnB, respectively. In case of a vote for candidate number 4, according to the example in Fig. 2, with an RnB of 3, the first rotation (4+3) mod 7 = 0 will yield a blank vote (this vote is also referred to as an intermediate code Sn" for the designation of the candidate) and after a second rotation with an RnA of 5 (0+5) mod 7 = 5, it will yield a vote for candidate number 5, which is sent to the election server (1) together with the voter's KID. So, the sent vote is a code for the vote actually cast and is also referred to as the voting code. Election server (1) then receives the vote (voting code) for candidate number 5, then rotates back the RnA of 5 known to this server for this KID (5-5) mod 7 = 0 (= intermediate code), substitutes the voter's KID by the anonymous AID and then sends this AID together with the blank vote found (candidate number 0) to the decoding server (2). The decoding server (2) receives the vote for candidate number 0 (the intermediate code), then rotates back the RnB of 3 known to this server for this AID (0-3) mod 6 = 4 (the designation for the candidate) and publishes the vote cast for candidate number 4 after the election together with the verification number NrC, which is asso-

ciated with the respective AID.

[0021] The voter can now verify on the basis of this published verification number NrC whether his or her vote for candidate number 4 has actually been received and counts in the election.

[0022] Of course, instead of the above-mentioned double rotation offset (rotation value) with the modulus of the number of options, it is also possible to use a different mathematical function between the number of the chosen candidate and the number of the candidate sent to the election server (1), while the election server (1) and the decoding server (2) each administer one or more secret parameter(s) of this mathematical function, which are exclusively known to these servers and to the voter. Also, instead of two servers, multiple servers may be used to increase the number of trusted parties, while each of these parties adds one or more secret parameters. These modifications are understood to fall within the scope of the present invention.

[0023] As can be seen in Fig. 1, in this manner, the relation between the vote Sn and the voter cannot be demonstrated at any moment during the communication or by one of the servers or after the publication. RnA, RnB and NrC are not sent via the network and can therefore not be known to third parties so that any candidate number may be correct on the basis of the known information.

[0024] Should the polling card be damaged on receipt, then a new card with different random numbers can be applied for to the municipality prior to the election. These extra cards are provided with an AID, RnB and NrC by the decoding server (2) and are prepared in advance and sent to the municipality together with the polling cards for the voters.

[0025] Because, with the aid of the polling card (3), one can also vote at a polling place stated on this polling card, in the election system according to the invention, there is the possibility to revoke a vote cast, for instance via the Internet. As described before by applicant in Dutch patent application no. 1019120, it is important in a system for democratic elections where votes count which have been cast outside a polling place, that these votes are not cast under duress or that the voter has not sold his or her vote to the highest bidding party.

[0026] By passing on the KID numbers of the voters at the polling place to the election server (1), this server can pass on the AID numbers associated with these KID numbers to the decoding server (2), after which this server can remove the votes associated with the respective AID numbers from the outcome and can indicate per candidate, in the publication of the votes cast, how many revoked votes there are for the respective candidate. This information is not published per voter, because a vote via the Internet may have been cast under duress.

[0027] In case of loss, damage, renunciation under duress or sale of a polling card, the voter can always apply for a new card to the municipality, so that the vote cast with the original polling card is automatically revoked, which is not noticed by a possible other user of the original polling card.

[0028] If the original polling card is also used to vote at the polling place, the vote cast via the network will be overwritten in the publication.

[0029] In order to guarantee the uniqueness of the votes cast, only the first vote cast per KID is stored. In case of a second vote, the election application on the voter's computer receives back the first stored vote as a response from the election server (1).

[0030] By designing a voting computer at a polling place such that the voter can have the voting computer read in his KID, PWD, RnA and RnB via a suitable, for instance bar code, reader, to then store a table in the voting computer with, per KID, the doubly rotated vote cast as well as the PWD, the outcome of the polling place can also be verified by the voter after the election. To this end, the table with KID and doubly rotated votes is sent to the election server (1) and processed in the same manner as the votes cast via the network. Here, the voter can also verify with the aid of the verification number NrC whether his or her vote cast at the polling place has been received and counts in the election and also calculate the overall outcome. In addition to storing above-mentioned table, the voting computer may also store the votes actually cast anonymously, so that the outcome of the respective polling place can be calculated on the spot after the election.

[0031] In order to realize a greatest possible security of the system, the information is transmitted from the election server (1) to the decoding server (2) with the aid of a CD (compact disc) or another information carrier not connected with a network.

[0032] Prior to the election, the voter's election application can be loaded on the voter's computer via the network.

[0033] Because all transactions are logged in the servers, it is always possible to carry out an audit afterwards if, for instance, a voter does not agree with the outcome. For this, an independent authority can be established which is to monitor the proceedings of the election and can verify whether a voiced complaint is with good reason or not.

[0034] The chosen encoding for the designation of the candidate, the intermediate code and the voting code may be designated by one or more digit(s), letter(s), icon (s) or a combination of these symbols, digits and letters. The voter identification code and/or the anonymous identification code may also be designated by one or more digit(s), letter(s), icon(s) or a combination of these symbols, digits and letters.

[0035] Hereinafter, an example will be discussed in which the chosen encoding for the candidate is a number and the chosen voting code is a combination of letters.

[0036] The invention further relates to a polling card for elections or indicating a preference in a referendum, which is also suitable for voting via the Internet and provides a supplement to the above-described election sys-

tem.

[0037] The best manner to prevent the vote cast or preference from being discovered in case of tapping the PC on which a voter wishes to cast a vote or preference via the Internet is to ensure that no information about this vote or preference is present on the PC. A special variant of the present invention contemplates providing this by carrying out the double vote rotation as described hereinabove with the aid of the polling card. The candidate number of the candidate to be chosen, or the preference number of one or more preferences in a referendum, is substituted here by a voting code (the above-described doubly rotated vote) which is doubly rotated per digit of the candidate number or the preference number with a rotation value determined per digit (rotation offset determined by the value of a rotation number RnA and RnB, respectively) as shown in Fig. 3. In Fig. 3, the vote to be cast has the number 431. The second secret parameter RnB is 734. RnB comprises the digits 7, 3 and 4 which each represent a rotation value. The digit 4 of the vote is substituted by (4+7) mod 10 is 1. The digit 3 of the vote is substituted by (3+3) mod 10 is 6 and the digit 1 of the vote is substituted by (1+4) mod 10 is 5. Now the intermediate code is 165. In Fig. 3, the first secret parameter RnA is 481. RnA comprises the digits 4, 8 and 1 which each represent a rotation value. The digit 1 of the intermediate code is substituted by (1+4) mod 10 is 5. The digit 6 of the intermediate code is substituted by (6+8) mod 10 is 4 and the digit 5 of the intermediate code is substituted by (5+1) mod 10 is 6. Now the voting code is 546. As will be discussed hereinafter, such an encryption of the vote can be carried out by a voter 50 with the aid of a polling card. However, it is also possible that this encryption is carried out with the aid of the computer of the voter 50 after which the voting code is sent to the election server together with the KID, for instance via the Internet.

[0038] Upon receipt of the voting code (directly or via the Internet), the election server then carries out an inverse mathematical operation on the basis of the first secret parameter known to the election server, associated with the respective KID. The election server (1) receives the voting code 456 and the KID. On the basis of the KID, the election server selects the first secret parameter RnA associated with this server (1) is 481. On the basis of the digits 4, 8 and 1 of the first secret parameter RnA, the election server (1) carries out the following: the digit 5 of the voting code of the vote is substituted by the election server by (5-4) mod 10 is 1. The digit 4 of the voting code of the vote is substituted by the election server by (4-8) mod 10 is 6 and the digit 6 of the voting code Sn' is substituted by the election server by (6-1) mod 10 is 5. Now the intermediate code is 165. The election server sends the intermediate code to the decoding server (2). On the basis of the KID, the election server determines the associated AID and sends this AID to the decoding server as well. On the basis of the received AID, the decoding server (2) determines the second secret parameter RnB associated therewith = 734. On the basis of the digits 7, 3 and 4 of the second secret parameter RnB, the decoding server carries out the following: the digit 1 of the intermediate code is then substituted by the decoding server by (1-7) mod 10 is 4. The digit 6 of the intermediate code is then substituted by the decoding server by (6-3) mod 10 is 3 and the digit 5 of the intermediate code is substituted by the decoding server by (5-4) mod 10 is 1. Now the obtained vote Sn is 431 again.

[0039] In addition to the advantage that no information about the candidate or preference to be chosen is present on the PC, less input by the voter is sufficient, because the two offset values (RnA and RnB) for the double vote rotation, as described hereinabove, do not need to be inputted and are replaced by a simple voting code.

[0040] A further advantage is that the input of the voting code on the voter's PC can work with an application on an Internet server and a standard browser on the voter's PC and therefore no program needs to be downloaded, as is for instance done with the tax declaration.

[0041] This also makes it possible to cast a vote on, for instance, information columns at stations or in other public places.

[0042] In order to ensure that the individual parties involved in the production and printing of polling cards have no information with which a vote could be converted, the polling card consists of two parts glued together, of which the voter can simply remove one part, so that information which was covered first becomes visible. In addition to using two parts glued together, of course this may also be achieved in a different manner, for instance by applying a scratch varnish or by printing the information from the outside through a closed envelope, as is often done when issuing PIN codes, this information only becoming visible after opening the envelope.

[0043] The design and production of the polling card according to this special variant according to the invention will be described hereinafter with reference to some Figures, where the chosen encoding with digits and letters is fictional and arbitrary and where the designation of the candidate to be chosen or the designation of the preference for one or more options in a referendum can be represented by one or more digit(s), letter(s), icon(s) or a combination of these symbols.

[0044] The basic idea behind this special embodiment is that, if no convertible information with regard to the vote cast or option is present on the voter's PC and no information is sent over the Internet either, then compromising these parts will not make any information about the vote cast or option available.

[0045] The printer who receives the order to print the polling cards produces two rolls with printed parts 1 and 2 of the polling card separated by perforations, of which only one specimen is shown in Fig. 3 and Fig. 4. An example is given with reference to Figs. 4-12. The principle of the encryption of the vote according to Figs. 4-12 is similar to the system of Fig. 3. In both cases, the vote Sn and the intermediate code Sn" are designated by digits.

In Figs. 4-12, however, the voting code Sn' is designated by letters instead of digits. However, with respect to content, this makes no fundamental difference. If, in Fig. 3, the digits 0-9 of the voting code were replaced by the letters A-J, respectively, a system similar Figs. 4-12 would be obtained, except for the fact that, for Fig. 3 on the one hand and Figs. 4-12 on the other hand, the secret parameters RnA and RnB differ.

[0046] The front side (101) of part 1 in Fig. 4 is the side where, after combining part 1 and part 2 to form the final polling card, the voter's name and address details will be printed. Part 1 is provided with the tear perforations (102), (103), (104) and (105). The back side (106) of part 1 is provided with a unique verification number (107) and a table (108) with ten rows of numbers 0 to 9 in the left part, which are, for instance, divided into three decimal columns depending on the number of candidates or options and are rotated per decimal column with a rotation value between 0 and 9 which is random per decimal column. The decimal values of these second rotations are represented by a random number RnB (109), for instance by indicating, per column, the first digit in the respective column. The value thus obtained of the second rotation RnB (109) is also printed on the back side (106) of part 1, both in a readable form and in a bar code form.

[0047] Anywhere in the description where the term bar code is used, of course a different machine-readable code may be used as well, such as for instance dot code or codes for OCR (Optical Character Recognition).

[0048] In addition to on the back side, both the verification number (107) and the second rotation number RnB (9) are also printed on the front side of part 1, both of them both readable and in a bar code form and in the side edge or information strip (110), which is separated from the center portion of part 1 by perforation (102). This side edge or information strip (110) is later rolled up as a physical counterfoil and kept with the decoding server, in order to be able to demonstrate which information has been added to the polling card by the decoding server. The unique verification number (107) serves to verify after the election whether the vote cast is also in the ballot box and therefore counts in the election. The front side (111) of part 2 of the polling card, as shown in Fig. 5, later forms the back side of the polling card, after the parts 1 and 2 have been glued together. On this, information is printed for the voter, such as for instance the Internet address where a vote can be cast and instructions for casting such an Internet vote. Part 2 contains tear perforations (112), (113) and (114) similar to the perforations (102), (103) and (104) of part 1, and a finger-shaped tear perforation (115). The table (108) of Fig. 4 is repeated on the front side of part 2 in the form of a table (116) but then without entering anything in this. The back side of part 2 is provided with a glue layer (117) which is activated upon combining part 1 and part 2, for instance by heating. This glue layer (117) covers the whole back side of part 2 except for the portion located within the finger-shaped perforation (115) and a line corresponding with perforation (105) of Fig. 4. Under the glue layer (117) and within the finger-shaped perforation (115), a part (118) is printed black or with black figures to prevent the table (108) of Fig. 4 and later the table (116) from being read out through the polling card or the envelope.

[0049] After the parts 1 and 2 are ready, they are glued together as shown in Fig. 6. Here, the information of the table (108), the verification number (107) and the second rotation RnB (9) in Fig. 4 are then completely covered and invisible. However, the verification number (107) and the second rotation RnB (108) on the front side of the polling card can still be read out in the side edge or information strip (119) which is later rolled up and kept with the decoding server as a physical counterfoil. Exactly registering the parts 1 and 2 can take place in a known manner with the aid of optical means or optionally by providing a chain perforation (not drawn) on the sides of both parts in advance.

[0050] The polling cards, being separated by perforations and in a roll form, then go from the printer to the administrator of the decoding server, which administrator provides the cards with a unique AID (121). As shown in Fig. 7, this AID (121) is printed per polling card in a readable form and in the form of a bar code on the side edge or information strip (119) and on the other side edge or information strip (120). Further, in the decoding server, a file is made in which it is recorded per AID (121) what the associated verification number (107) and the associated second rotation RnB (109) are. Then, with the decoding server, the side edge or information strip (119) is removed along the perforations (102) and (112) of Figs. 4 and 5 and rolled up and kept as a physical verification means for the link between the AID (121), the verification number (107) and the second rotation RnB (109).

[0051] The roll of polling cards separated by perforations of which, of one specimen, the front and back side are shown in Fig. 8 then goes to the administrator of the election server. On the outside of the cards now no information can be observed anymore about the verification number (107), the second rotation RnB (109) and the information in the table (108) of Fig. 4 in relation to the AID (121).

[0052] With the aid of the election server, the roll of polling cards separated by perforations is then provided with information about the voter. To this end, as shown in Fig. 9, the voter's name and address details are printed on the front side of the polling card, both on the part (122) intended for the voter and on the part (123) intended for the polling place. On the side edge or information strip (120), also a unique Voter Identification number (KID) (124) as well as a random first rotation RnA (125) are printed, which indicates, per digit of the candidate number or option number, the rotation of, for instance, the ten letters A to J which are printed on the back side (126) of the part of the polling card intended for the voter, in the right part of the table (116). Here, the value of the first rotation RnA (125) represents, for instance, per col-

umn, the position of the letter in the alphabet, starting with 0 for A. On this part, the KID (124), the first rotation RnA (125) and a password (129) for the voter are printed as well, both in a readable form and in a bar code form. On the back side (127) of the part of the polling card intended for the polling place, likewise the KID (124) and the name and address details of the voter are printed. Further, a file is made in the election server, in which, per KID (124) it is recorded what the associated AID (121) and the associated first rotation RnA (125) are.

[0053] Then, the side edge (120) is removed and rolled up and kept with the election server as a physical counterfoil to be able to demonstrate which information has been added to the polling card by the election server. On this, the link between AID (121), KID (124) and the associated first rotation RnA (125) can be read out.

[0054] After the side edge or information strip (120) has been removed along the perforations (103) and (104) of Figs. 4 and 5 and has been rolled up, the polling cards are individually separated from the roll along the perforations (128) and packed in a window envelope as shown in Fig. 10. On the front side of the polling card, via the window of the envelope, in addition to any general information, now exclusively the voter's name and address details can be seen.

[0055] The voter who wishes to vote via the Internet takes the polling card and, as shown in Fig. 11, removes the non-glued part along the finger-shaped perforation (115) and along perforation (105) so that the verification number (107), the second rotation RnB (109) and the rest of the table (108) become visible. By entering the number of the candidate to be chosen or option number at the top of the table, as shown in the example of Fig. 12, the associated voting code can be copied from the table and be entered at the bottom. So, it holds in this example that, per digit of a number of a candidate, the polling card is provided with a pair of columns each comprising a first and second column. For each pair of columns, it holds that the possible values of a digit are included in the first column in a predetermined vertical order and where, viewed in horizontal direction, in the second column, there is a new digit or new character behind each digit of the first column. In this example, this is a new character. In use, for each digit of a number of a candidate, in the pair of columns associated with this digit, the voter looks for this digit in the first column. Then, the voter determines which new digit or new character is in the second column behind this digit in the first column. The new digits or new characters thus obtained are then combined by the voter on the card to form the voting code associated with the vote. With the aid of the KID (124) and the password (129), the voter can then report to the election server and cast his or her vote or choice by inputting the respective voting code. Because no information about the rotations used is known on the PC of the voter, it cannot be deduced on the basis of the voting code what the vote actually cast or choice is.

[0056] Should a voter decide to go to a polling place, then, with the aid of the bar code information of the first rotation RnA (125), the second rotation RnB (109), KID (124) and the password (129), the voting machine can be released and a vote or choice can be cast in the conventional manner. The associated voting code can then be calculated by the voting machine and passed on to the election server, so that the voter can verify on the basis of the verification number (107) whether his or her vote or choice also counts in the ballot box, in the same manner as with an Internet vote.

[0057] If voting is done by proxy, then this can only be done at a polling place. The principal then gives the strip (127) provided with a signature to the proxy holder. With this, the proxy holder can cast a vote or choice at the polling place after the name and address details of the proxy holder have been entered and after a signature has been put thereto. When casting a vote or choice, the first rotation RnA and the second rotation RnB of the proxy holder himself are used to encode the vote or choice and to send it to the election server. However, the publication of the vote cast or choice on the Internet takes place under the verification number of the principal, so that he can also verify the vote cast or choice.

[0058] By not showing or giving the part (126) intended for the voter to the proxy holder, he can cast no vote or choice via the Internet, because the password required for this is missing. Further, then the rotations of the tables (108) and (116) of Figs. 4 and 9, respectively, are missing, so that the proxy holder does not know which voting code needs to be used for which vote or choice. So, when voting with the polling card, it holds that, per server, the mathematical function consists of a rotation offset per digit of a number of a chosen candidate or blank vote, while each digit is smaller than X and the rotation offset of a digit is, for instance, in the form of a modulus-X over the sum of the digit and the at least one secret parameter, while the at least one secret parameter is, for instance, for each server, a random number between zero and X-1 and while, for instance, per digit, a secret parameter is provided and while, optionally the outcome of the double rotation of the digit is substituted by a letter or other designation and while X=10. Other values of X are possible as well. If X=16, for instance, for each digit, a hexadecimal encoding (0, 1,..9, A, B, ... F) can be used. Such variants are also understood to be part of the invention.

Claims

1. An election system for elections via a network, **characterized in that** this election system is provided with at least two independent computer servers, which are administered by independent trusted parties, wherein the designation of the candidate or blank vote for which at least one voter wishes to vote, is changed into a voting code by the at least one voter, for instance with the aid of an election application on the computer of the at least one voter or

with the aid of a polling card of the at least one voter, by means of a mathematical function, in which secret parameters are used, wherein the election system is arranged such that, prior to the elections, for the benefit of the at least one voter, each of the independent servers provides at least one secret parameter of this mathematical function, which is then, in the election system, exclusively known to the respective server and which is communicated to the at least one voter and wherein, during the elections, at least one first secret parameter of these secret parameters together with information associated therewith about the identity of the at least one voter are exclusively known to a first server of the at least two servers, an anonymous identification code such as an anonymous identification number of the at least one voter is exclusively known to the first and a second server of the at least two servers, and at least one second secret parameter of the secret parameters associated with the anonymous identification code of the at least one voter is exclusively known to the second server, wherein, in the first server, the information about the identity of the at least one voter, the at least one secret first parameter associated with the at least one voter and the anonymous identification code of the at least one voter are stored such that it is known to the first server that they belong together, and, in the second server, the at least one second secret parameter associated with the at least one voter and the anonymous identification code of the at least one voter are stored such that it is known to the second server that they belong together, wherein the first server operatively receives the voting code of the at least one voter together with the information about the identity of the at least one voter, for instance via the Internet with the aid of a computer of the at least one voter, and then converts the voting code to an intermediate code with the aid of an inverse mathematical function of the mathematical function and the at least one first secret parameter known to the first server, associated with the information about the identity of the at least one voter, and sends on this intermediate code together with the anonymous identification code associated with the information about the identity of the at least one voter to the second server, which converts this information to the designation of the candidate, which was chosen by the at least one voter, with the aid of the inverse mathematical function and the at least one second secret parameter known to the second server, associated with the anonymous identification code of the at least one voter received by the second server from the first server.

2. An election system according to claim 1, **characterized in that** the election designation is provided with a number for the candidate, wherein the number of the candidate or blank vote for which the voter wishes to vote, is changed into the number of a different candidate or blank vote by the at least one voter, for instance with the aid of an election application on the computer of the at least one voter or with the aid of a polling card, by means of the mathematical function, which other number forms the voting code, wherein the first server operatively receives the changed vote of the at least one voter, then converts the changed vote to a number of a different candidate or blank vote acting as an intermediate code with the aid of the inverse mathematical function and the at least one first secret parameter known to the first server and sends on this number to the second server, together with the anonymous identification code associated with the at least one voter, which second server converts this information to the number of the candidate which was chosen by the at least one voter, with the aid of the inverse mathematical function and the at least one second secret parameter known to the second server, associated with the anonymous identification code of the at least one voter.

3. An election system according to claim 2, **characterized in that,** per server, the mathematical function consists of a rotation offset in the form of the modulus of the number of options over the sum of a number of the chosen candidate or blank vote and the at least one secret parameter, wherein the at least one secret parameter is, for each server, for instance a random number from zero to the maximum of the number of options.

4. An election system according to claim 1, **characterized in that,** per server, the mathematical function consists of a rotation offset per digit of a number of a chosen candidate or blank vote, wherein each digit is smaller than X and the rotation offset of a digit is, for instance, in the form of a modulus-X over the sum of the digit and the at least one secret parameter, wherein the at least one secret parameter is, for each server, for instance a random number which is between zero and X-1 and wherein optionally the outcome of the double rotation of the digit is substituted by a letter or another designation and wherein in particular X=10.

5. An election system according to any one of the preceding claims, **characterized in that** the election system is arranged such that the second server, or if the election system is provided with at least three servers, a last server of the at least three servers, discloses the chosen candidates, each provided with a unique verification number which is, on the one hand, exclusively known to the second server or the last server and is, on the other hand, known to the at least one voter until the disclosure, so that the at least one voter can verify whether the vote cast has been received and counts in the election and, in ad-

dition, can also calculate the outcome of the election on the basis of the published information.

6. An election system according to any one of the preceding claims **characterized in that** the information about the identity of the at least one voter which is exclusively known to the first server and the at least one voter is a voter information code such as a voter information number and comprises an identity of the at least one voter such as name and address details of the at least one voter and optionally a password, wherein the election system is arranged such that, in use, the at least one voter is identified in the first server on the basis of the voter identification code and the password, if any, wherein the at least one voter is identified in the second server on the basis of the anonymous identification code associated with the at least one voter, wherein the information about the identity of the at least one voter is not known to the second server and wherein the link between the at least one voter and the anonymous identification code is known to the first server only and wherein, after the first server has identified the voter on the basis of the voter identification code and the password, if any, the first server sends the anonymous identification code to the second server together with the intermediate code which has been obtained with the aid of the inverse mathematical function and the at least one first secret parameter known to the first server on the basis of the voting code cast by the at least one voter.

7. An election system according to claim 6, **characterized in that** the system is arranged such that, prior to the elections, the first server links a voter identification code and a password, if any, to the information about the identity of the at least one voter and that, prior to the elections, the second server generates at least one second secret parameter and links this to an anonymous identification code and sends on the anonymous identification code to the first server which links this anonymous identification code to the information about the identity of the at least one voter, wherein the sending on of the anonymous identification code may, for instance, comprise the second server printing the anonymous identification code and the associated at least one secret second parameter on a polling card and the first server then reading and storing the anonymous identification code for linking it to information about the identity of the at least one voter and wherein, prior to the elections, preferably, the first server generates at least one first secret parameter and links this to the information about the identity of the at least one voter.

8. An election system according to any one of the preceding claims, **characterized in that** the election system is arranged such that, prior to the election, the polling card of the at least one voter is provided by the servers with the information needed for voting by the at least one voter, including the secret parameters of the servers associated with the at least one voter, the information about the identity of the at least one voter and optionally the anonymous identification number of the at least one voter.

9. An election system according to claim 5 and 8, **characterized in that** the election system is arranged such that, prior to the election, the polling card is provided by the servers with the information needed for voting by the at least one voter, including the verification number.

10. An election system according to any one of the preceding claims, **characterized in that** the secret parameters, the password, if any, and the verification number, if any, are covered on the polling card in such a manner that they are unreadable for unauthorized persons.

11. An election system according to claim 10, **characterized in that** this covering is done by folding a part of the polling card double over this information and sealing it up, and/or by putting a part of the polling card with this information in a separate envelope and sending this envelope to the voter together with the rest of the polling card in a second envelope and/or by covering this information with a scratch varnish.

12. An election system according to any one of the preceding claims, **characterized in that** the system is arranged to print the relevant information on the polling card for casting a vote, including the secret parameters of the servers, both in a readable and in a machine-readable form, such as for instance a bar code, to be able to automate the reading of this information in places appropriate for this.

13. An election system according to claim 6, **characterized in that** the system is arranged to provide the polling card with the anonymous identification code of the at least one voter as well as twice the voter identification code of the at least one voter so that the part of the polling card with the anonymous identification code which, prior to the elections, the first server needs to link to the information about the identity of the at least one voter and one of the two voter identification codes provided can be separated from the polling card prior to the elections before the polling card is sent to the at least one voter, wherein the separated part with the anonymous identification code and the voter identification code can be kept until after the election.

14. An election system according to any one of the preceding claims, **characterized in that** the system is

arranged such that, in use, with a voting computer designed for this purpose, at a polling place, the machine-readable secret numbers of the polling card and the voter identification code are read in, after which the voter identification code together with the doubly rotated vote cast by the voter is stored in the voting computer in order to be sent to the first server after the election in order to be processed in a manner identical to a vote which is, for instance, inputted into the first server via the Internet and the computer of the at least one voter, so that the voter can verify that the vote cast has been received and counts in the election and, in addition, can also calculate the outcome of the election of the polling place on the basis of the published information.

15. An election system according to any one of the preceding claims, **characterized in that** the system is further provided with a polling card for the at least one voter, wherein the polling card is arranged to cast a vote with the first server with the aid of the doubly rotated voting code, for instance via the Internet, wherein this double rotation per digit of a candidate number or preference number is stated on the polling card, so that, in a simple manner, on the basis of the candidate number or preference number and this stated double rotation, a voting code can be deduced by the voter on the polling card, which voting code can be inputted into the voter's PC and can be passed on via the Internet and which represents the vote cast by the respective voter, without information being present or being sent on the PC of the voter or via the Internet, from which the vote cast may be converted on the basis of this voting code.

16. A polling card of the system according to claim 15.

17. An election system for elections via a network, **characterized in that that** this election system consists of at least two independent computer systems or servers, which are administered by independent trusted parties, wherein the number of the candidate or blank vote, for which the voter wishes to vote, is changed into the number of a different candidate or blank vote by the election application on the voter's computer with the aid of a mathematical function, wherein each of the independent servers provide at least one secret parameter of this mathematical function, which is exclusively known to the respective server and the voter and wherein the identity of the voter is exclusively known to the first server, which receives the changed vote of the voter, then converts it to the number of a different candidate or blank vote with the aid of the inverse mathematical function and the secret parameter known to the first server and sends on this number together with an anonymous identification number to the second server, which also converts this information to the number of the candidate which was chosen by the voter with the aid of the inverse mathematical function and the secret parameter known to the second server.

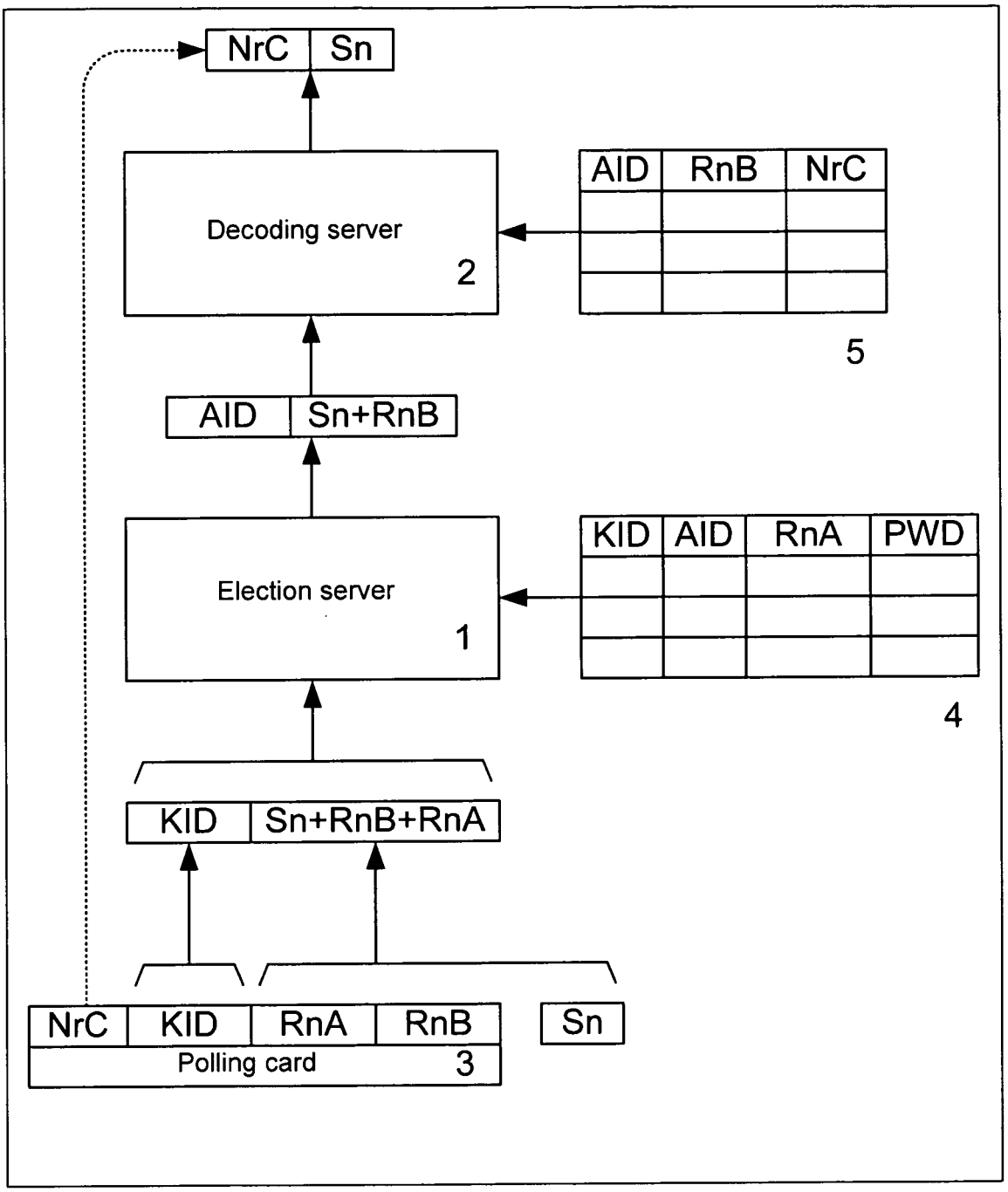

NrC
Sn
Decoding server
2
AID
RnB
NrC
5
AID
Sn+RnB
Election server
1
KID
AID
RnA
PWD
4
KID
Sn+RnB+RnA
NrC
KID
RnA
RnB
Polling card
3
Sn

Fig. 1

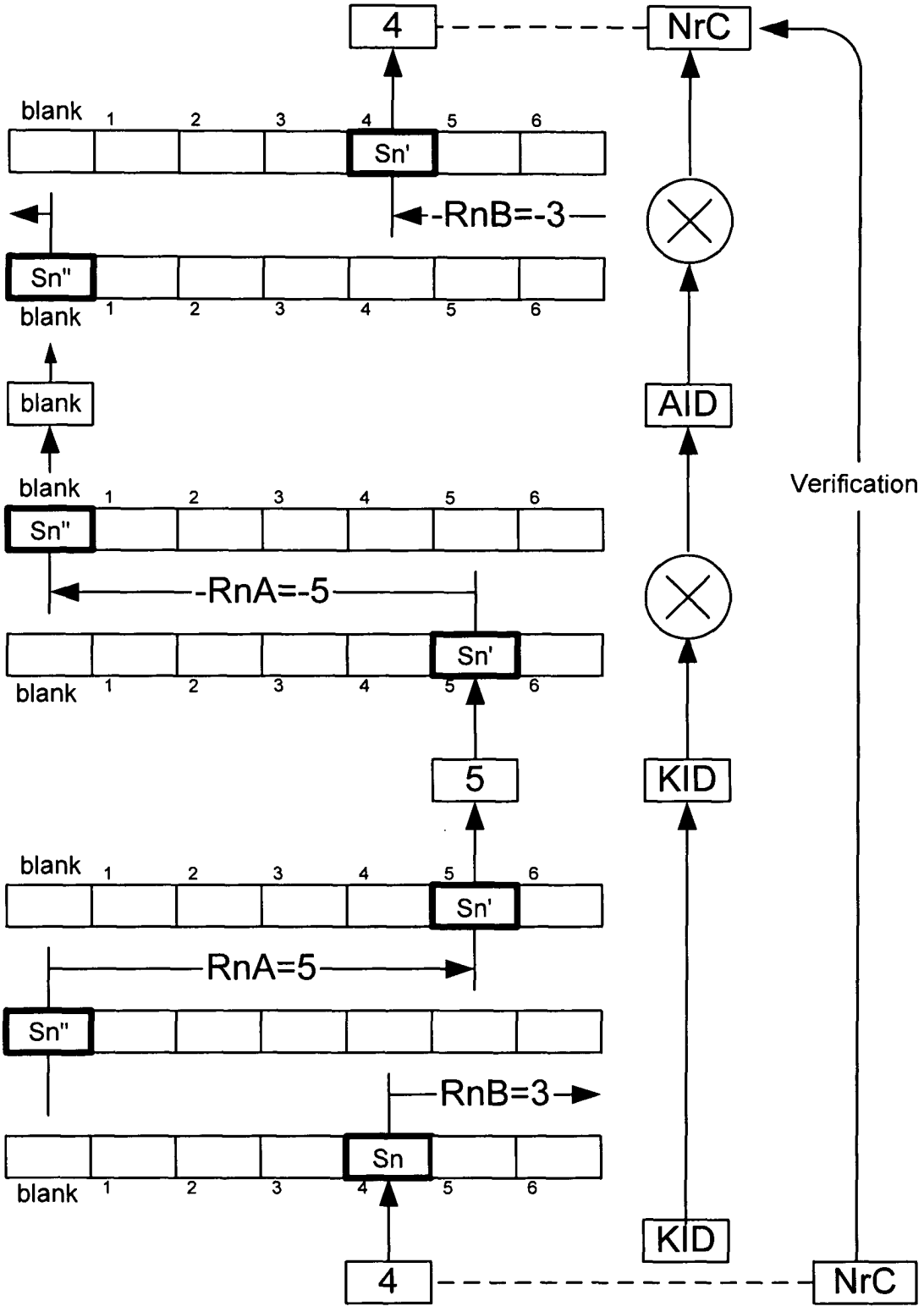

4
NrC
blank
1
2
3
4
5
6
Sn'
-RnB=-3
Sn"
blank
blank
AID
Verification
blank
Sn"
-RnA=-5
Sn'
blank
5
KID
blank
Sn'
RnA=5
Sn"
RnB=3
Sn
blank
KID
4
NrC

Fig. 2

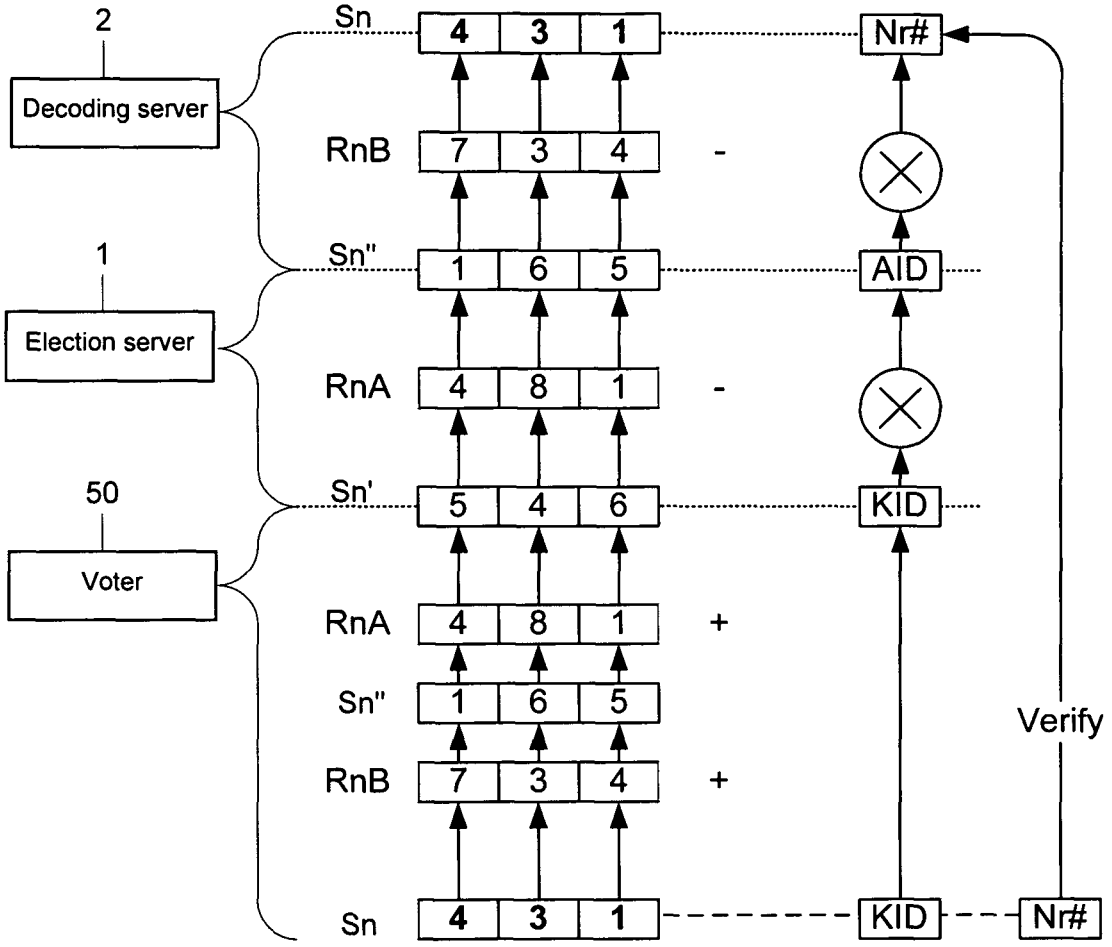

2
Decoding server
1
Election server
50
Voter
Sn
4 3 1
Nr#
RnB
7 3 4
-
Sn"
1 6 5
AID
RnA
4 8 1
-
Sn'
5 4 6
KID
RnA
4 8 1
+
Sn"
1 6 5
RnB
7 3 4
+
Sn
4 3 1
KID
Nr#
Verify

Fig. 3

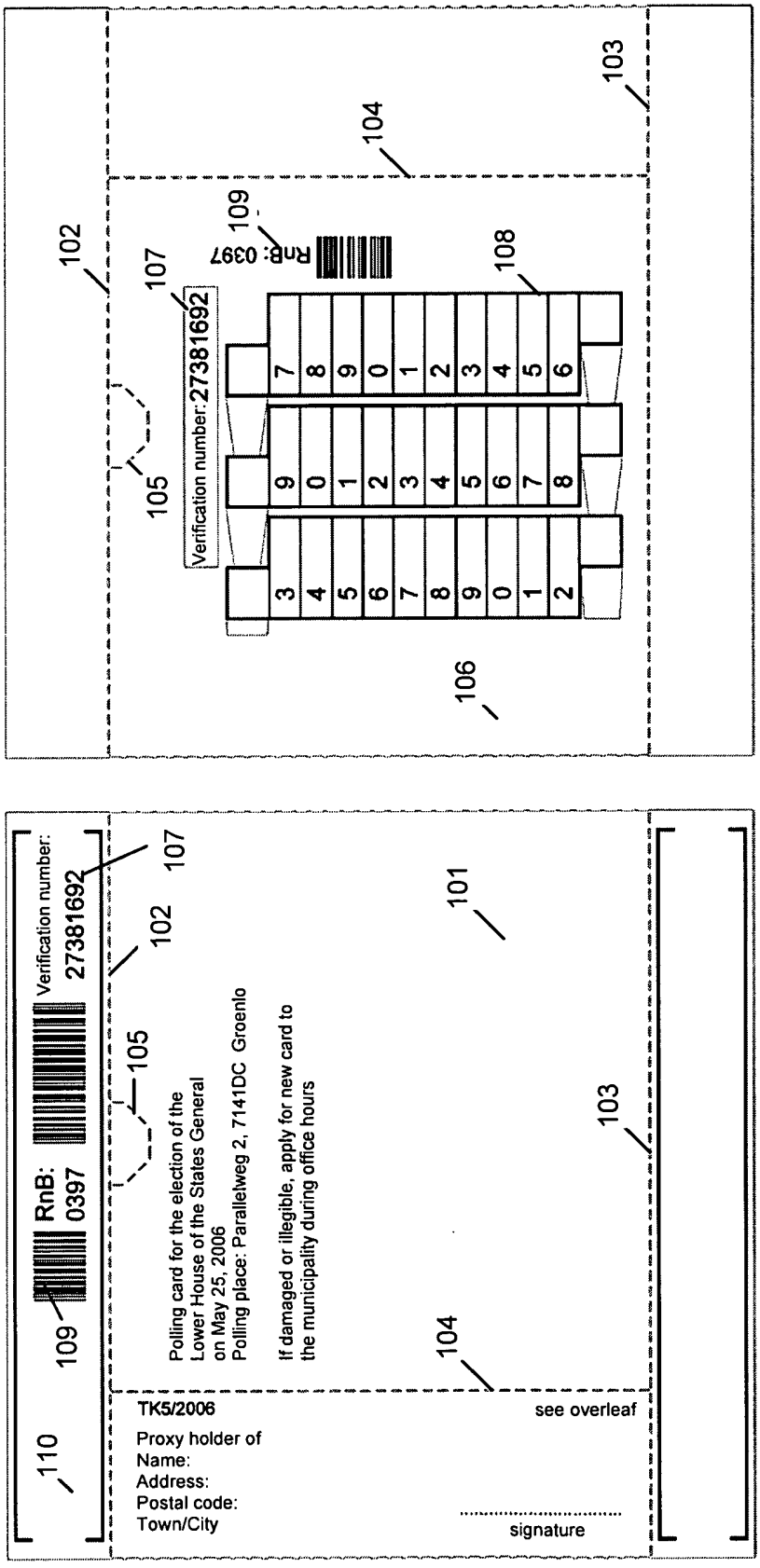

102
103
104
105
106
107
108
109
RnB: 0397
Verification number: 27381692
110
RnB: 0397
Verification number: 27381692
Polling card for the election of the Lower House of the States General on May 25, 2006
Polling place: Parallelweg 2, 7141DC Groenlo
If damaged or illegible, apply for new card to the municipality during office hours
TK5/2006
see overleaf
Proxy holder of
Name:
Address:
Postal code:
Town/City
signature

Fig. 4

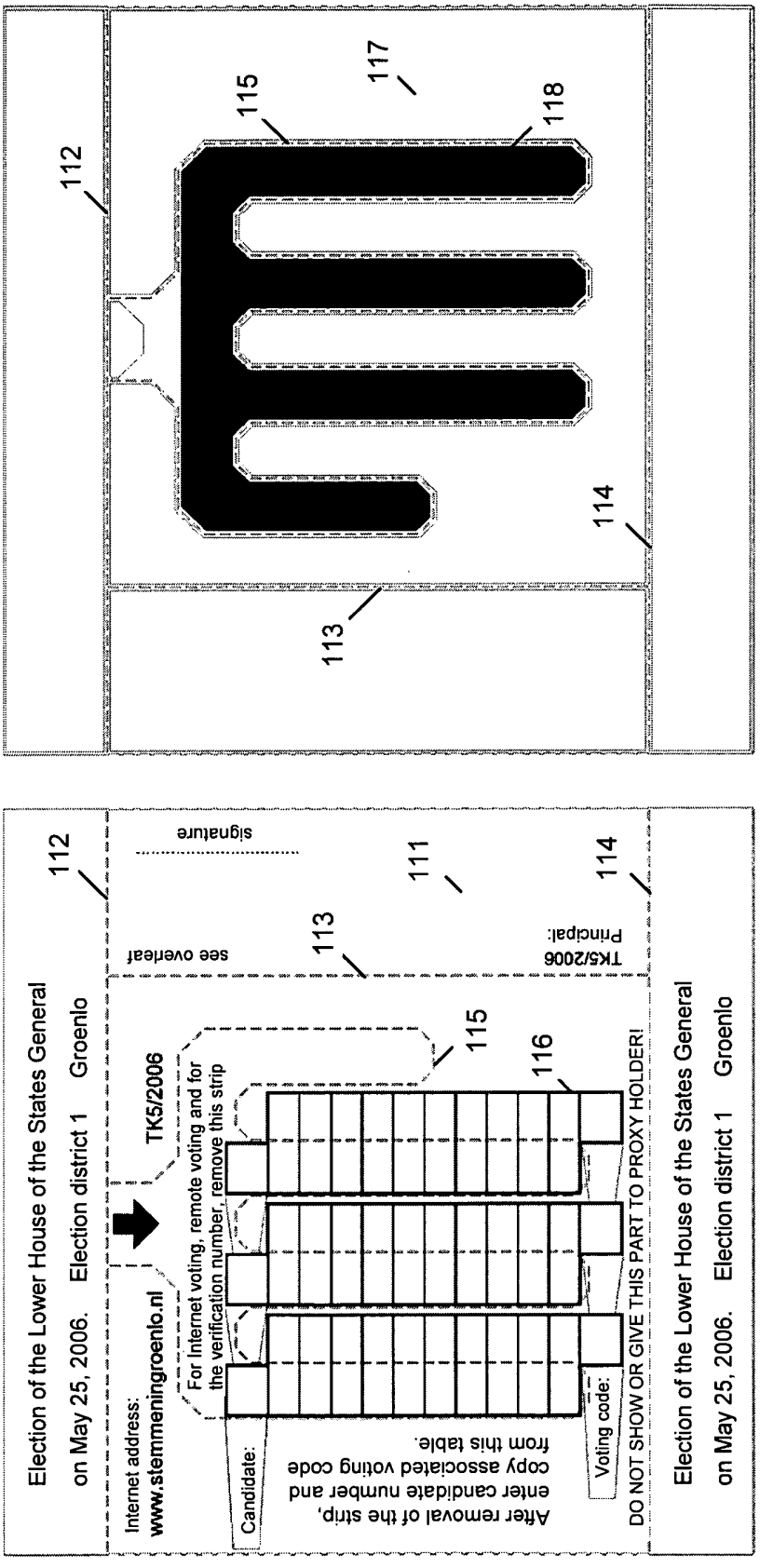
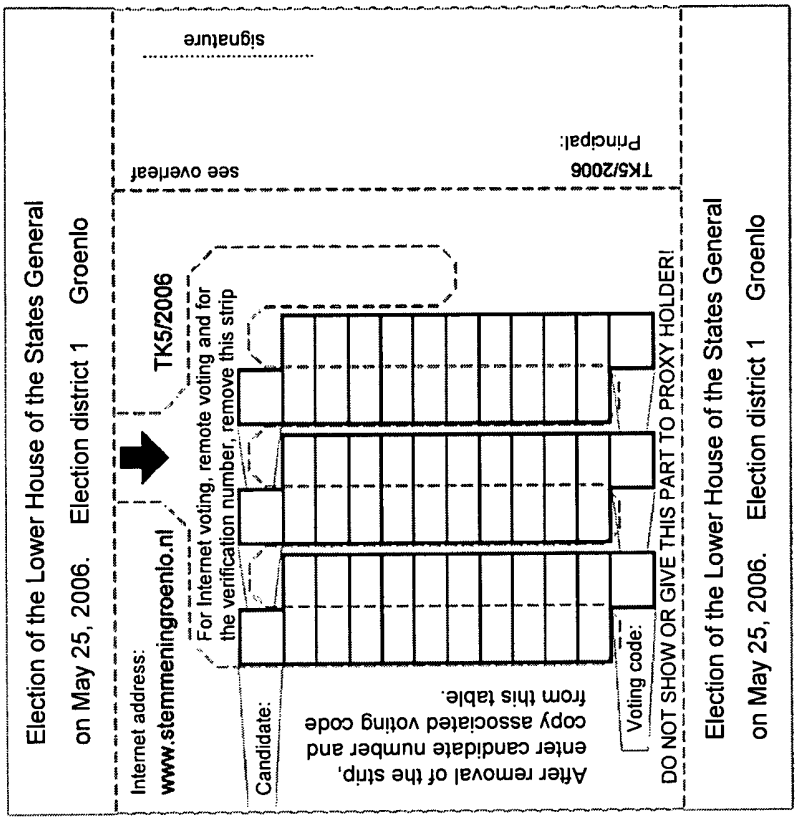

112
115
117
118
114
113
Election of the Lower House of the States General
on May 25, 2006. Election district 1 Groenlo
Internet address:
www.stemmeningroenlo.nl
TK5/2006
For Internet voting, remote voting and for the verification number, remove this strip
Candidate:
Voting code:
After removal of the strip, enter candidate number and copy associated voting code from this table.
DO NOT SHOW OR GIVE THIS PART TO PROXY HOLDER!
see overleaf
signature
111
116
TK5/2006
Principal:

Fig. 5


Election of the Lower House of the States General
on May 25, 2006. Election district 1 Groenlo
Internet address:
www.stemmeningroenlo.nl
TK5/2006
For Internet voting, remote voting and for the verification number, remove this strip
Candidate:
After removal of the strip, enter candidate number and copy associated voting code from this table.
Voting code:
DO NOT SHOW OR GIVE THIS PART TO PROXY HOLDER!
see overleaf
TK5/2006
Principal:
signature
Election of the Lower House of the States General
on May 25, 2006. Election district 1 Groenlo

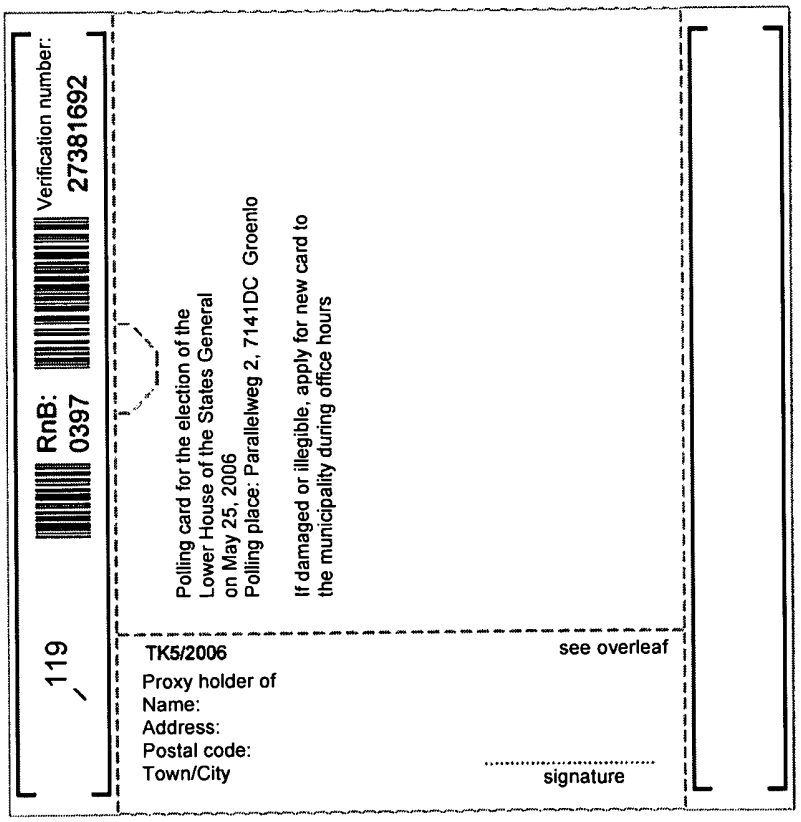

119
RnB: 0397
Verification number: 27381692
Polling card for the election of the Lower House of the States General on May 25, 2006
Polling place: Parallelweg 2, 7141DC Groenlo
If damaged or illegible, apply for new card to the municipality during office hours
TK5/2006
see overleaf
Proxy holder of
Name:
Address:
Postal code:
Town/City
signature

Fig. 6

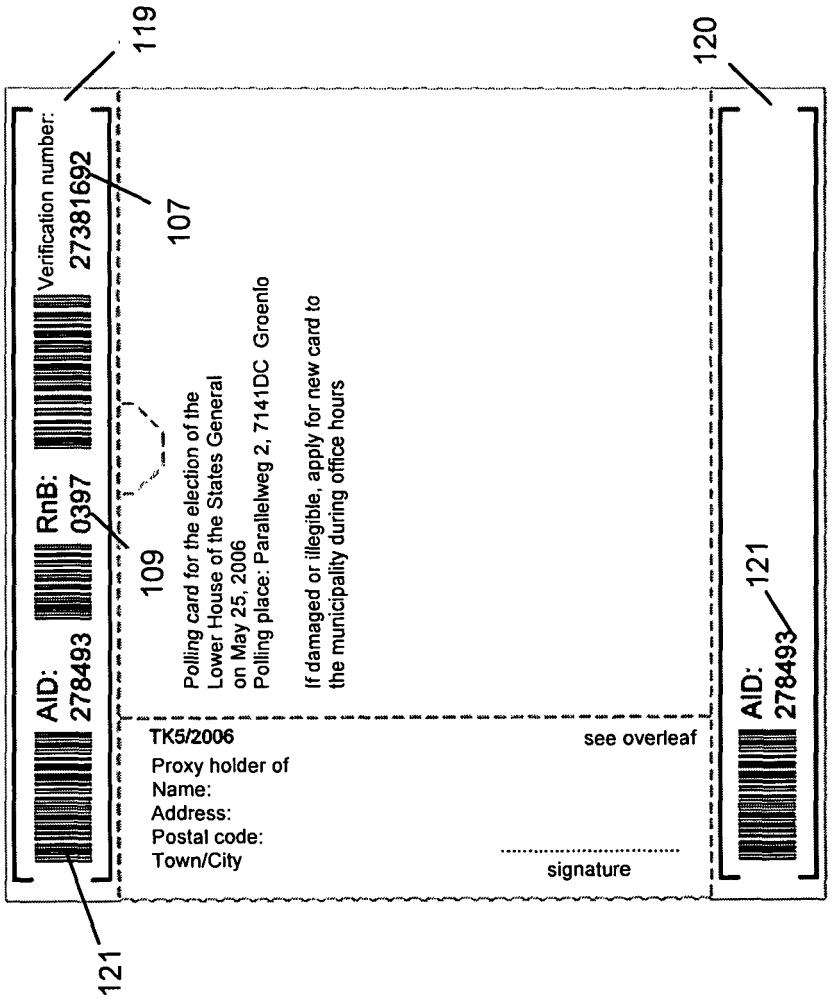

119
120
Verification number:
27381692
107
RnB:
0397
AID:
278493
109
Polling card for the election of the
Lower House of the States General
on May 25, 2006
Polling place: Parallelweg 2, 7141DC Groenlo
If damaged or illegible, apply for new card to
the municipality during office hours
TK5/2006
see overleaf
Proxy holder of
Name:
Address:
Postal code:
Town/City
signature
AID:
278493
121
121

Fig. 7

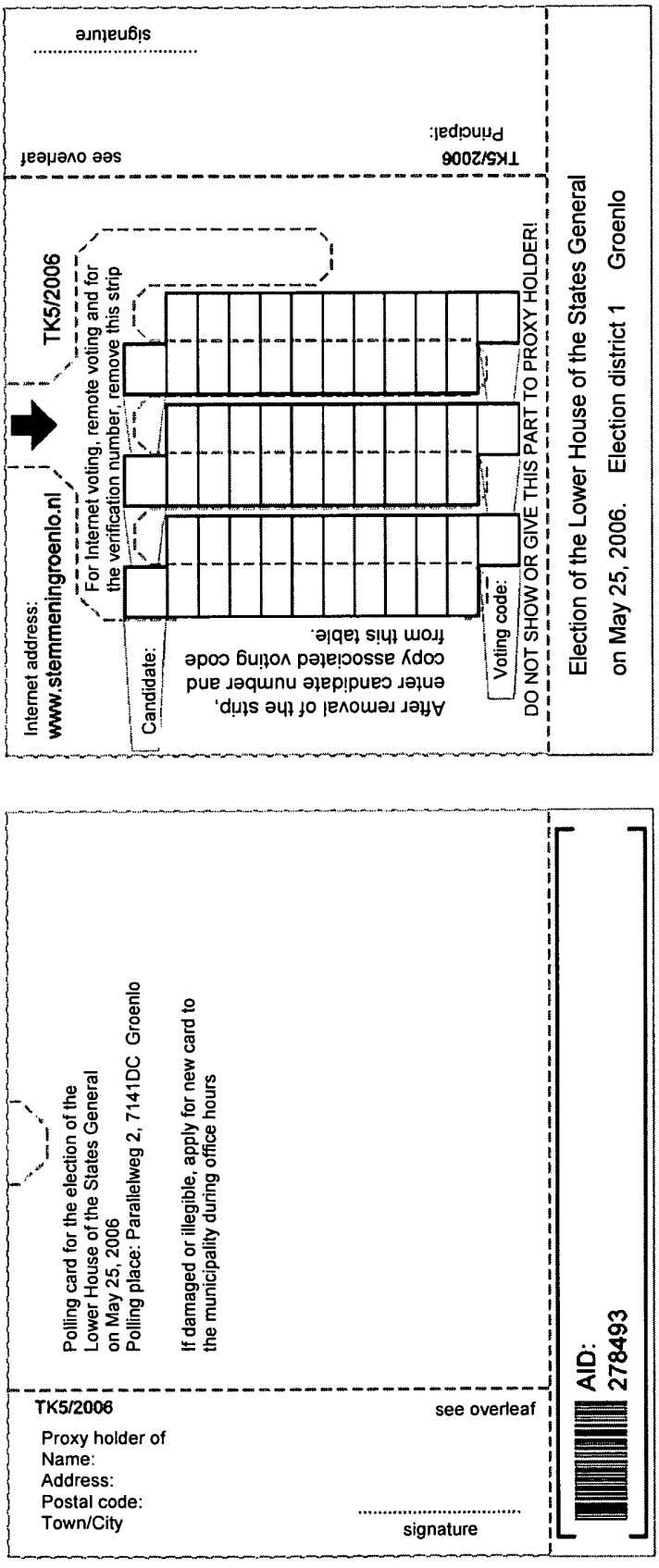

Election of the Lower House of the States General
on May 25, 2006. Election district 1 Groenlo
DO NOT SHOW OR GIVE THIS PART TO PROXY HOLDER!
Voting code:
After removal of the strip,
enter candidate number and
copy associated voting code
from this table.
Candidate:
Internet address:
www.stemmeningroenlo.nl
For Internet voting, remote voting and for
the verification number, remove this strip
TK5/2006
TK5/2006
Principal:
see overleaf
signature
AID:
278493
Polling card for the election of the
Lower House of the States General
on May 25, 2006
Polling place: Parallelweg 2, 7141DC Groenlo
If damaged or illegible, apply for new card to
the municipality during office hours
TK5/2006
see overleaf
Proxy holder of
Name:
Address:
Postal code:
Town/City
signature

Fig. 8

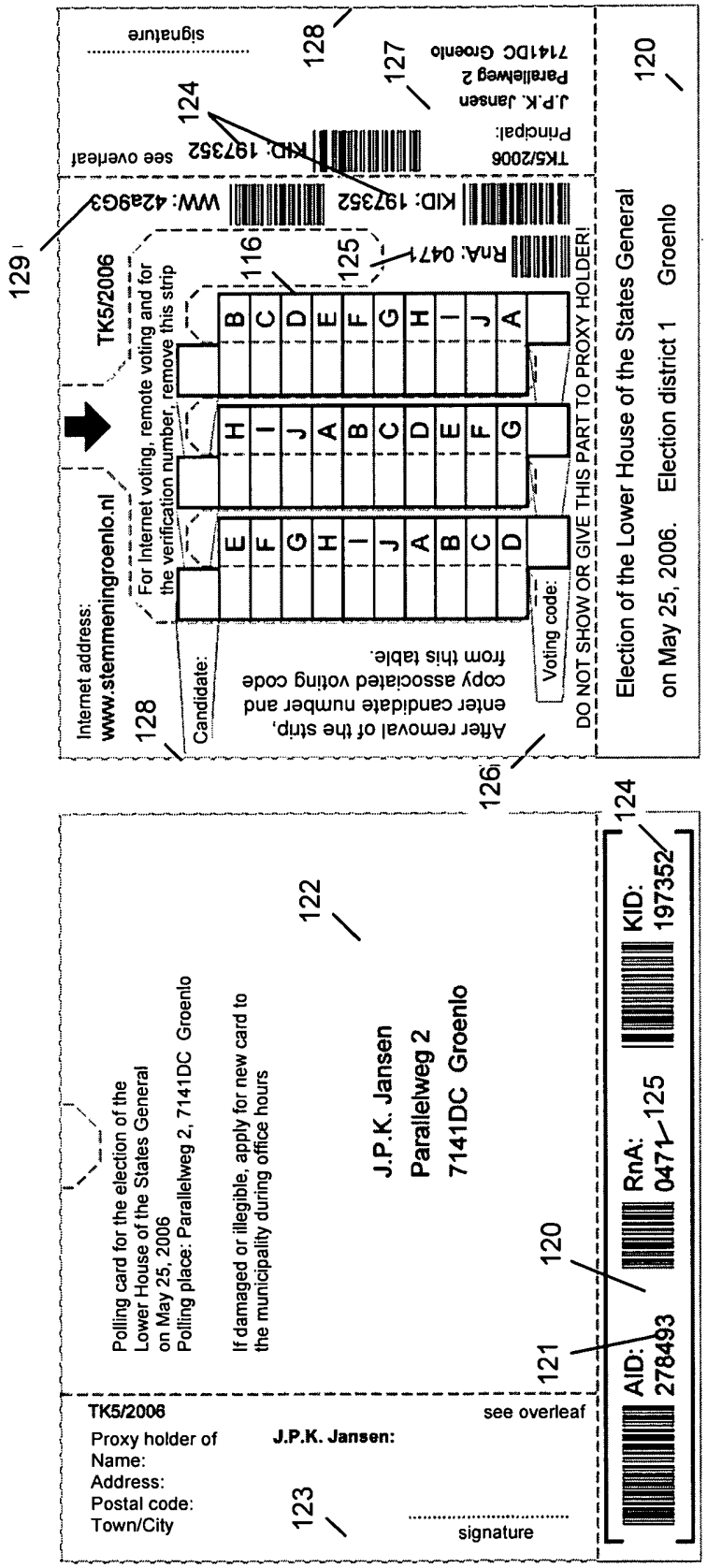

Polling card for the election of the Lower House of the States General on May 25, 2006
Polling place: Parallelweg 2, 7141DC Groenlo
If damaged or illegible, apply for new card to the municipality during office hours
J.P.K. Jansen
Parallelweg 2
7141DC Groenlo
TK5/2006
Proxy holder of
Name:
Address:
Postal code:
Town/City
J.P.K. Jansen:
see overleaf
signature
AID: 278493
RnA: 0471
KID: 197352
Election of the Lower House of the States General
on May 25, 2006. Election district 1 Groenlo
DO NOT SHOW OR GIVE THIS PART TO PROXY HOLDER!
Internet address:
www.stemmeningroenlo.nl
For Internet voting, remote voting and for the verification number, remove this strip
Candidate:
Voting code:
After removal of the strip, enter candidate number and copy associated voting code from this table.
TK5/2006
WW: 42a9G3
KID: 197352
RnA: 0471
120
121
122
123
124
125
126
127
128
129

Fig. 9

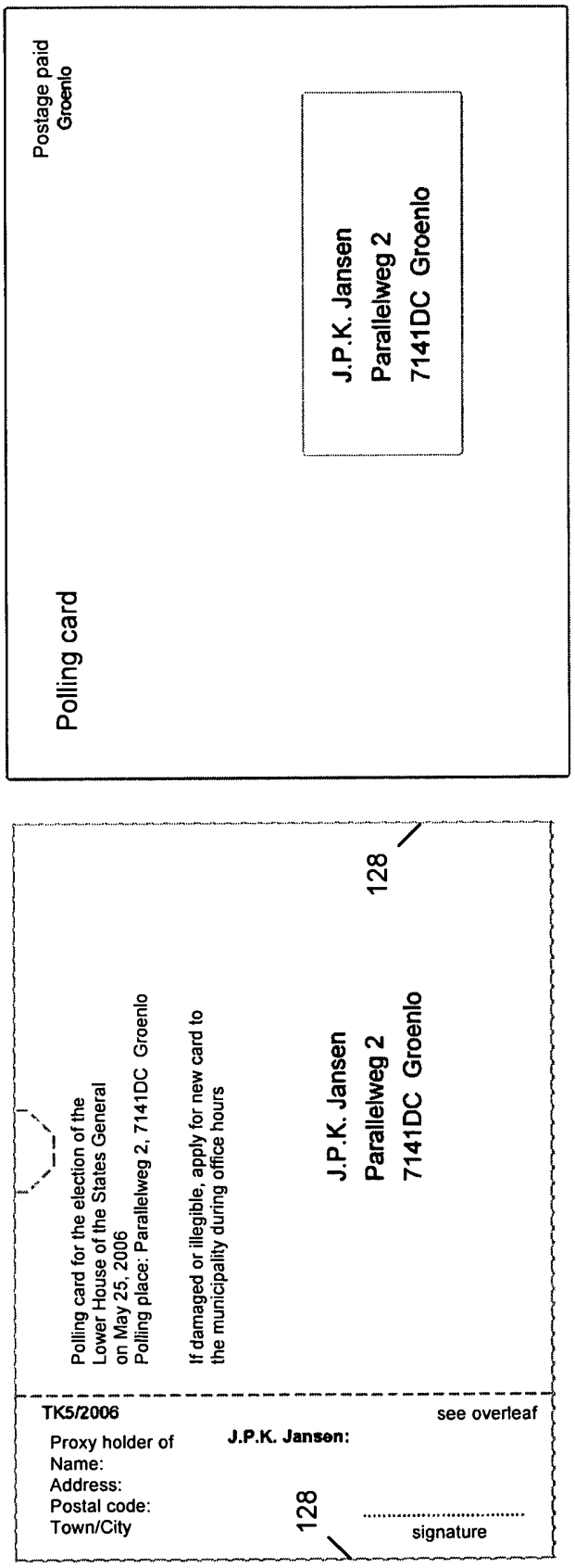

Postage paid
Groenlo
J.P.K. Jansen
Parallelweg 2
7141DC Groenlo
Polling card
Polling card for the election of the
Lower House of the States General
on May 25, 2006
Polling place: Parallelweg 2, 7141DC Groenlo
If damaged or illegible, apply for new card to
the municipality during office hours
J.P.K. Jansen
Parallelweg 2
7141DC Groenlo
128
TK5/2006
see overleaf
Proxy holder of
Name:
Address:
Postal code:
Town/City
J.P.K. Jansen:
128
signature

Fig. 10

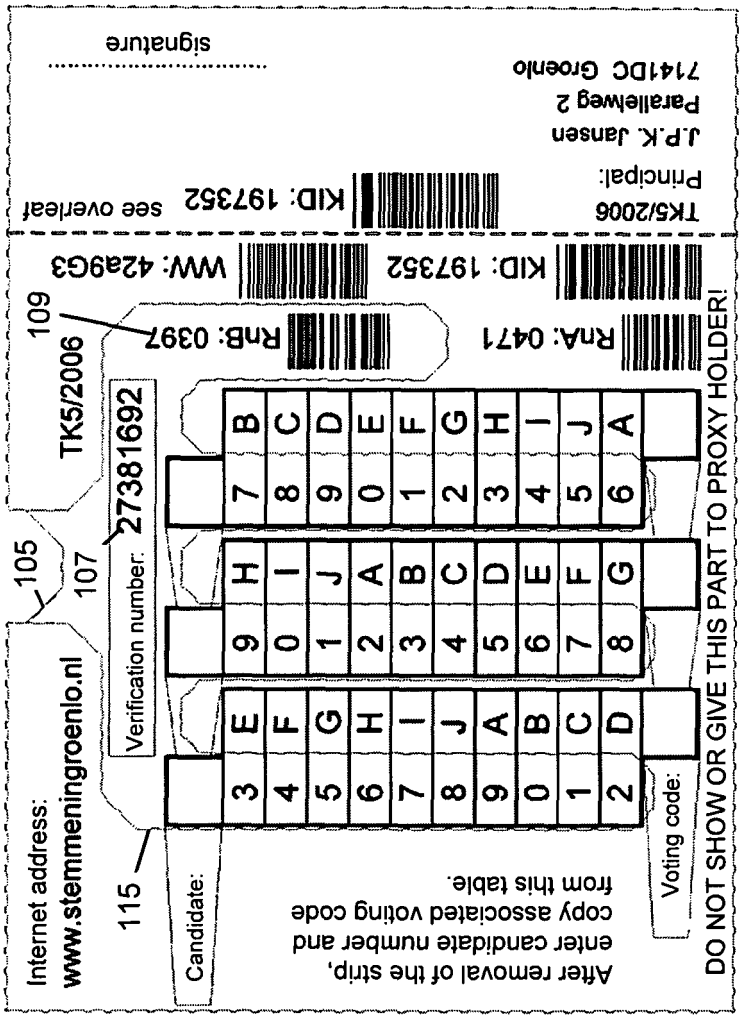
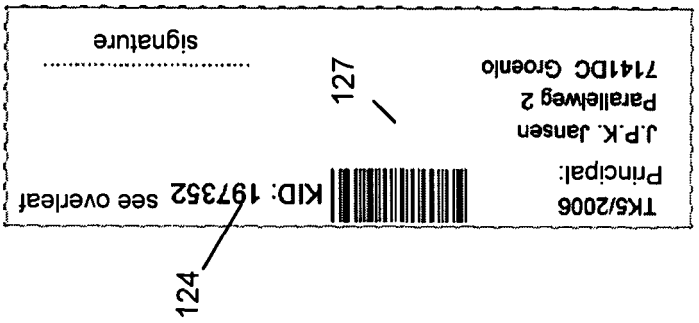

DO NOT SHOW OR GIVE THIS PART TO PROXY HOLDER!
RnA: 0471
KID: 197352
WW: 42a9G3
RnB: 0397
109
TK5/2006
105
107
Verification number: 27381692
Internet address:
www.stemmeningroenlo.nl
115
Candidate:
Voting code:
After removal of the strip,
enter candidate number and
copy associated voting code
from this table.
TK5/2006
Principal:
J.P.K. Jansen
Parallelweg 2
7141DC Groenlo
KID: 197352
see overleaf
signature

Fig. 11


TK5/2006
Principal:
J.P.K. Jansen
Parallelweg 2
7141DC Groenlo
127
signature
KID: 197352 see overleaf
124

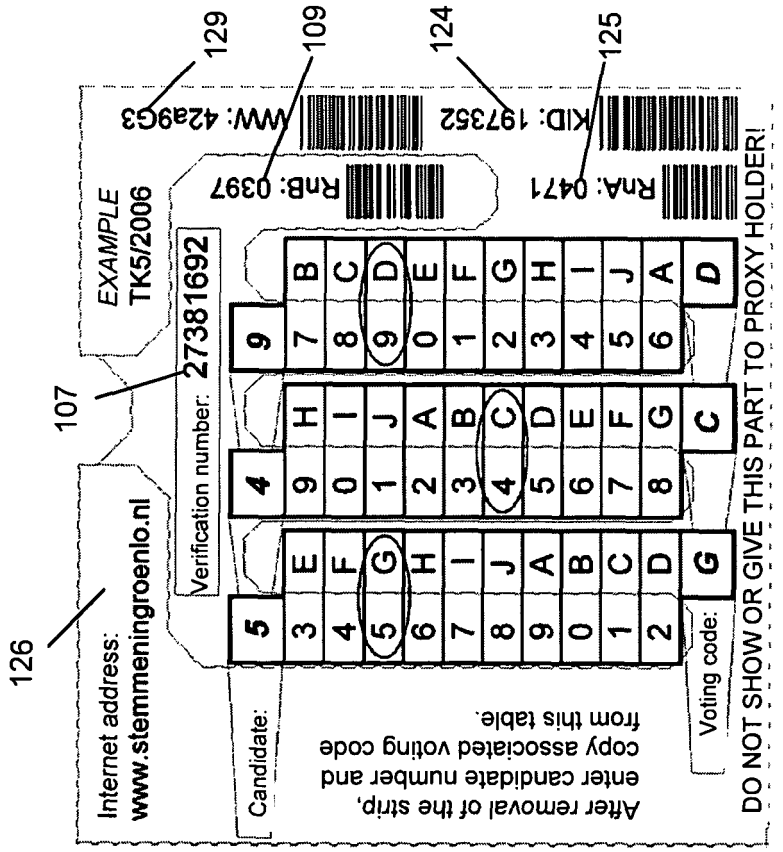

EXAMPLE
TK5/2006
MW: 42a9G3
129
109
RnB: 0397
124
KID: 197352
125
RnA: 0471
Internet address:
www.stemmeningroenlo.nl
126
107
Verification number: 27381692
Candidate:
Voting code:
After removal of the strip,
enter candidate number and
copy associated voting code
from this table.
DO NOT SHOW OR GIVE THIS PART TO PROXY HOLDER!

Fig. 12

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- DE 1021632 **[0003]**
- DE 1029723 **[0004]**
- DE 1019120 **[0025]**