(19) DANMARK

(10) **DK/EP 3249616 T3**

(12) Oversættelse af europæisk patentskrift

Patent- og Varemærkestyrelsen

(51) Int.Cl.: ***G 07 C 13/00 (2006.01)*** *H 04 L 9/32 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2022-01-31**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2021-11-03**

(86) Europæisk ansøgning nr.: **15878324.1**

(86) Europæisk indleveringsdag: **2015-01-21**

(87) Den europæiske ansøgnings publiceringsdag: **2017-11-29**

(86) International ansøgning nr.: **CL2015000004**

(87) Internationalt publikationsnr.: **WO2016115646**

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

(73) Patenthaver: **Correa Parker, Cesar Ramón Juan, San Olav 6440 Dpto. 204, Las Condes, Santiago, Chile**

(72) Opfinder: **Correa Parker, Cesar Ramón Juan, San Olav 6440 Dpto. 204, Las Condes, Santiago, Chile**

(74) Fuldmægtig i Danmark: **O3C Konsult AB (A Questel Company), PO Box 6088 , 17106 Solna, Sverige**

(54) Benævnelse: **ELEKTRONISK AFSTEMNINGSFREMGANGSMÅDE OG -SYSTEM IMPLEMENTERET I EN BÆRBAR ENHED**

(56) Fremdragne publikationer:
WO-A1-2010/048295
WO-A1-2013/182252
US-A1- 2004 046 021
US-A1- 2005 269 406
US-A1- 2006 294 387
US-A1- 2007 185 761
US-A1- 2011 089 236
US-A1- 2012 328 104
None

DESCRIPTION

SPECIFICATION

[0001] The present application relates to a method and system for electronic voting capable of being implemented in portable devices, such as smartphones, meeting the basic requirements of anonymity, verifiability and security in voting, as well as other well-known requirements for electronic voting systems. It should be noted that the method and system proposed in the application meet the six requirements set in the assessment dimensions for voting systems and methods. The dilemma of allowing voters to verify the correct issue and vote counting while ensuring anonymity is resolved, as well as preventing the risks associated with malicious third parties, fraud, failure or errors in computer systems, thus giving the transparency needed to encourage participation and ensure the integrity of the voting results.

[0002] Furthermore, the invention of the present application improves voting rates by providing a method and system implemented in portable devices, which are currently widely used allowing the vote to be cast remotely without going to a determined polling place, ensuring voting is secure for both the process itself and to the voter.

Background of the Invention

[0003] The methods and systems for electronic voting have begun to be widely used in various instances, both in particular votes, such as those including analysis of trends and opinion polls, and large popular votes, e.g. related to elections of public office or referendums.

[0004] Indeed, the early history of massive implementation of electronic voting dates back to 1964, with the United States being one of the pioneers in implementing such a system. At that time, electronic voting systems were installed directly in the polling stations, using punch cards and counting computer machines. Such devices have evolved over time in order to comply with the requirements of security, anonymity and transparency, as well as to improve the administration and counting of mass votes thanks to automation.

[0005] In 1996 the US government implemented the first election in which various voting mechanisms were offered, including Internet, mail and telephone voting. However, the first parliamentary election offering voting capacity by Internet was conducted in Estonia, in 2007, where the voter used a smart identification card as authentication agent. At that time, the objective was to make the voting process easier releasing the polling place at voter's choice; about 4% of votes was cast by accessing the Internet. Advanced examples of such electronic voting systems are found in US patent applications 2011/0238463 and US 2012/0095811, where electronic voting systems and methods are proposed that integrate various mechanisms for voter identification, management of voting and counting of votes cast, in addition to security

mechanisms to authenticate the vote and results.

[0006] In this respect, during parliamentary votes in Europe in 2011, the highest percentage of Internet voting was obtained, with 24% of total votes. This high percentage was attributable to the provision of mobile phones as voter identification equipment, as proposed in the patent application US 2014/0207537, a document that also considered portable computers as an interface comprising the ballot.

[0007] Considering the above background, the patent application US 2002/0077886 discloses a system, a method and apparatus for electronic voting that is installed in the polling place, wherein said apparatus provides independent systems for recording and counting, and printing the ballot papers issued. In this context, the apparatus provides separate storage means for storing redundant voting information, with the storage of, at the very least, voting information in electronic memories, used by the system for counting, as well as information on paper voting, usually used to audit the voting process. Furthermore, the apparatus of the application uses a display device in which an interface is implemented for the voter that provides a voting session identifier. This provides transparency in every vote and maintains anonymity between each vote and the voter. However, the method, system and apparatus of the application consider printing the votes with identification codes assigned to the user, which facilitates the association of a vote with the applicable voter. Moreover, the voting machines are installed in polling places; thus, remote secure voting is not possible. Therefore, the solution proposed by the application US 2002/0077886 does not address issues related to remote voting or how to facilitate voting so as to stimulate the number of votes; in addition, it has serious security problems associated with voting, mainly anonymity and non-coercion. These problems result from the random printing of the code in the voting paper, thus allowing for the possibility of associating the code with the voter and, therefore, associate the voter with the vote cast.

[0008] Moreover, the publication of patent application WO 2012/137035 defines the use of GMS networks for a mobile voting system based on nationwide location, where the GMS network is used to access all citizens of a region and to provide real-time connection to a central database platform. This central database collects the online votes, counting those votes securely, taking into consideration the voter's anonymity by avoiding the storage of information associated with their identity, and providing the possibility of accessing the system for audit. In short, the system proposed by the publication is to use the GMS network to collect the votes of the voters and to obtain their location. While this solution allows releasing the voter from the polling place, it does not ensure the protection of the vote and the voter with respect to the main requirements or pillars where electronic voting is framed. Indeed, the system proposed by the WO 2012/137035 does not include features to prevent electoral fraud, which becomes relevant in electronic systems due to the management of information and the possibility that malicious third parties, for example hackers, gain access to it.

[0009] Regarding the above, it is identified that security in electronic voting systems is of high relevance. In this regard, the document JP 2011028376 provides an electronic voting system using cell phones, with the system comprised of a server arranged in a network and cellular

phones; each phone includes an identifier corresponding to the IMSI number associated with the device's SIM card. Said system comprises various programs to cast a vote, including a program preventing double vote in the same cell phone through the identification of the identifier. In this context, the document in question only takes care of voting security with respect to doubling the vote, without proposing security mechanisms that may avoid, among other things, electoral fraud by malicious third parties. Moreover, users with multiple SIM cards may attempt to violate the security of the system by introducing such cards in the device used for voting.

[0010] In addition, the document EP 2455919 describes an electronic voting method that uses a mobile communications network. This method considers various security mechanisms, among which a PIN number known by the voter is sent to the authority in charge of the election to verify and authorize the electronic voting of said voter. Such approval takes place with a code received by the voter, who also receives information to vote. A random number is generated by a trusted authority and sent to the voter, so that the encrypted voting information and the random number are sent to the authority in charge of the election process. Considering the above, the document EP 2455919 proposes a complex security system that increases the voting security but it is not able to prevent malicious third parties accessing the information found online and handle or disclose it without authorization. Indeed, the single method of protection against third party access is encryption of information, a methodology that is currently vulnerable because of the great capabilities computers have in processing information, which allows the deciphering of even the most advanced encryptions. In addition, the voting verification system is cumbersome and complex, increasing the chances of failure during operation. Regarding anonymity, the document EP 2455919 states that this requirement is achieved by associating the vote with an encrypted random number and not with the information of the voter; however, this association prevents voters from verifying themselves the cast vote.

[0011] The document patent application US 2014/0089062 provides a voting system that uses smartphones, indicating that this provides a safe and quick method to vote. In this regard, this document uses different modules including a certificate management module and a module for managing aspects of voting, such as management of voter information, voter registration and identity, generation and verification of voting certificate, among others. In this context, the system and method proposed by this document considers the constant communication between the voter and a server that verifies the identity of the voter and, after verification, it issues a voting certificate authorizing the vote. In addition, the secret voting system proposed in the document US 2014/0089062 is comprised of a series of steps and involves various modules which complicate voting, making it unfriendly for the voter. Finally, the system and method proposed in the document does not propose a simple and effective solution to prevent voter fraud by malicious third parties, since the only barrier facing such fraud is encryption of information, which is not secure when validating a vote. In addition, secrecy in voting is only insured by the certification of the voter registration, which -added to the non-verifiability of the method of the vote- increases the uncertainty of the system.

[0012] In this context, many systems use similar methodologies to those described in US 2014/0089062, such as US 2008/0105742 and US 2005/101307 documents in which identification mechanisms are used as comparison between transaction identifiers and identification and encryption as a primary means of security against fraud. Indeed, most of the solutions that propose the use of portable devices, such as smart phones as a means of voting, take over security aspects related to voting secrecy and anonymity of the voter, without addressing other risks associated with voting, such as verifiability and non-coercion, among others that are discussed below.

[0013] In addition, the document US 2004/046021 describe an electronic voting apparatus, system and method which provides at least two independently means for recording and counting votes, e.g., one associated with the voting apparatus and one separate therefrom. A preferred voting apparatus, system and method may provide triple data redundancy in that each vote is recorded by three independent and verifiable means: i.e. by recording in one or more electronic memory devices included in the voting machine and/or system, by recording in the memory of a smart card separate from the voting machine and/or system, and/or by a confirmatory printed record for each voter. The invention may utilize a voting session identifier to provide transparency of the vote and to maintain the anonymity of the votes and voters.

[0014] Although it has been shown that electronic voting systems have been used for several years, these systems are not free from errors that can lead to invalidate an election. Among these errors, the most relevant ones relate to the authentication of the voter, the registration of voter preferences by voting intention, the counting of preferences and security in the sense that data are not altered, being these some of the pillars that a voting system must ensure. Moreover, more complex voting systems have the disadvantage of relying on the operation of elements of such systems, such as identification devices by fingerprint and network capabilities, among others.

[0015] As already indicated, the alteration of the electronic voting records from malicious third parties, fraud, failure or errors in computer systems is a risk inherent in the use of electronic systems, primarily due to the possibility that such events will not be detectable when the methods and systems prevent voting traceability in order to protect anonymity. Furthermore, methods and systems that maintain traceability of the vote to detect such events do not guarantee anonymity. In this respect, a relevant problem to be solved by electronic voting systems is to maintain the anonymity of the voter, preventing a particular vote to be traced to a voter, while allowing verifiability, and detection of attempts on security from malicious third parties, fraud, failures or errors in computer systems in order to ensure voting integrity is not compromised.

[0016] In this context, experts have reached consensus that a method and system for electronic voting should be evaluated on the basis of six dimensions, which also apply to traditional voting systems. Here, the requirements established relate to:

- Ensuring the legitimacy of the vote,

- Preventing coercion (non-coercion)
- Capturing the voter's intention,
- Safeguarding of voter's privacy (anonymity),
- Security and transparency of the voting system, and
- Verifiability of the cast votes.

[0017] These requirements are necessary to achieve the objective of proposing a secure voting system both for the process itself and for the voter. In this respect, in an electronic voting system, the requirement for verifiability has replaced the supervision of vote counting used in traditional voting processes by allowing each voter to verify whether their vote was properly considered, but taking into account that this could facilitate bribery if the process allows a third party to also verify the vote of each voter.

[0018] Despite the facilities provided by an electronic voting method and system, there is a cultural barrier to the use of such systems, which results in relatively low percentages compared to traditional voting. In this context, the main barrier refers to the voters' distrust of voting in electronic devices at the time of voting, due to the fact that involvement in the process and / or performance is unrelated to the user.

[0019] Regarding the above, today the use of personal high-performance portable devices such as smartphones, has increased considerably, with those devices being part of the daily lives of users. Indeed, today's portable devices offer users multiple features, including Internet access, online banking, handling emails and storing personal information, where such features often involve sensitive user information. In this sense, safe handling of sensitive or critical information on mobile portable devices has been the object of major developments; thus, at present there are security systems that greatly reduce the possibility of critical information leakage, achieving acceptable safety levels, as those associated with the use of smart cards for authentication purposes. However, considering the flexibilities in the electronic environment, the risk will always exist that malicious third parties may overcome the security systems, thus gaining access to alter sensitive or critical information, which can be countered by providing voter verifiability and ensuring its anonymity.

[0020] It is therefore necessary to implement an electronic voting system and method able to simultaneously meet the six dimensions previously stated, while encouraging use by implementing a reliable and familiar interface for the voter, wherein said voter can verify the correct issue and vote counting, safeguarding the privacy of the voter, and containing the risk associated with malicious third parties, fraud, failure or errors in computer systems.

Brief Description of the Invention

[0021] The present invention comprises an electronic voting method that allows voting through

a network such as Internet or Intranet using portable devices, such as smartphones, capable of data transmission. An objective of the invention is to solve the problem of allowing voters to verify their vote was properly considered in the count, and avoiding the risk of disclosing the identity of the voter, i.e. ensuring their anonymity and preventing the risks associated with malicious third parties, fraud, failure or errors in computer systems. This, in combination with the high safety standards of current portable devices and the user experience offered by these devices, enables a transparent, quick method and a system that encourages the participation of portable device users.

[0022] In this context, the first stage or step of the electronic voting system and method proposed in the application is having voters duly registered in a database. The registration of voters is an essential component of the invention, widely used in all kinds of voting, whether electronic or not. In this respect, the method and system of the present invention first requires voters to be registered as such in a database, where such registration is done by associating the identity of the voter with a portable device identifier to be used by the voter when voting, with such identifier being, in the case of smartphones and cell phones, the International Mobile Equipment identifier associated with each mobile device, known as IMEI. The identifier is a unique electronic universal code that differentiates a portable device from another, even if they correspond to the same model.

[0023] Additionally, the method and system of the invention allow only a single identifier or portable device IMEI to be associated per voter, having the same number of voters as portable electronic devices registered to vote.

[0024] As a result, a database of registered voters is obtained and associated with the portable device identifier or IMEI to be used in the voting, all of them being potential voters by the method and system proposed by the invention.

[0025] Once the voter is registered or the universe of registered voters has been established for an electronic vote according to the method and system proposed in this application, the voting process can start, where each voter can cast their vote, for example through internet or intranet, from the portable device registered, with voting information received by at least one voting server in two separate sets or batches of information. Each separate set or batch of information is comprised of different data, preventing the association between the two batches of information since they are separate from each other, thereby preventing the disclosure of the voter identity to preclude the association of a specific vote with the identifier of the portable device or IMEI of the device registered where such vote was cast. In this sense, at least a first separate batch of information, called identifier set, is comprised of the identifier of the portable device or IMEI as obtained from the portable device that was used to vote, which must be registered through said identifier for the vote to be processed by at least one voting server, and a code A selected by the voter to cast the vote in its portable device, wherein said code A is selected from a first plurality of codes randomly generated and already predefined to allow authentication of the portable device identifier or IMEI with the information provided by the voter through a code module. The IMEI or identifier or portable device with the code A provides

confirmation that all votes cast come from voters registered in the database and verifies that there is no duplication of votes. This code A, which is only known by the voter at the time of its selection, as well as the identifier of the portable device or IMEI, allows the voter to verify that their participation was recorded properly once the results are published on the Internet and / or Intranet, with IMEIs being referenced to code A selected by each voter.

[0026] Moreover, at the very least a second separate batch of information, called set of voting, is comprised of the vote cast and a code B different from code A, also selected by the voter when casting the vote on their portable device, wherein said code B is selected from a second plurality of codes randomly generated and already predefined by a code module to allow authentication of votes. This code, which is only known by the voter at the time of its selection, allows the voter to verify that their vote was counted correctly, once the results are published on the Internet and / or Intranet, with all votes cast being referenced to the code B chosen by each voter.

[0027] The first and second plurality of randomly generated codes is predefined and equal for all voters comprised of a number of permutations that make it almost impossible for two voters to select the same code for the same voting. For example, for a group of voters grouped in a virtual polling station of 400 voters, where they must select from 9-digit numeric codes, there is less than 0.01% probability to choose the same code. When the system operates in online mode, the first and second plurality of random codes can be generated for each new group of voters (i.e. 400 voters) excluding those codes already used in the voting (i.e. by any of the 400 voters), before being sent to the new voter for its selection and subsequent authentication. In this way, the possibility of two voters, from the group of 400 voters, selecting the same code for the same voting is eliminated.

[0028] As part of the methodology and system implemented, the separate batches of information, the voting set and the identifier set are received by the voting server and randomly arranged, so that they cannot be associated on the basis of the sequence in which they were received by the voting server. Printing of separate batches of information is generated randomly by the voting server and / or by a printing device that randomly compiles said information, making the association between different paper traces of the voting impossible. For the voting set, the voting server begins random printing only once a first vote is recorded that expresses a different preference to previously recorded votes, so that the first votes that express the same preference cannot be associated with voters; for example, if 10 sets of voting have been received and number 11 is the first to include a vote that is different from the previous opinions, it is only from vote number 11 when random print of sets of vote starts. In the case of the printing device, the random compilation is achieved when the output of prints is received in a receptacle that does not allow maintaining the print sequence.

[0029] Thus, finally, as part of the methodology and system implemented, results are verified. In this sense, once the results are published on the Internet and / or Intranet, the voter may query using codes A and B previously selected to confirm their vote and participation were correctly recorded. In this context, according to one embodiment of the invention the voter

sends their confirmation or verification from their portable device, with the verification information being received by the voting server, wherein the verification information is called verification set. The verification set includes the verification and the identifier of the portable device or IMEI that is obtained from the portable device used to complete the verification, which must be the same as the device used to vote that has already been registered in order to allow authentication of the verification with the ID of the portable device or IMEI. In addition, the printouts of the votes, identifier set and verification set, leave a paper trail that acts as a backup to the electronic voting, which can also be used to verify the validity of the results; vote counts, participation counts and verification counts by the voting server, for example, in audits performed to the process or by public scrutiny.

[0030] All temporary files that the system may have created during the voting process, containing information that allows association of the voter with the vote, for example the set of voting and ID group, are deleted to prevent third party accessing them.

[0031] Considering the above, it is possible to determine that the methodology and system proposed in the application allow at the least:

- Safeguarding the voter anonymity, by preventing the association of the voter to the vote cast,
- Verification for voters that their vote was properly considered and counted, as votes are made public along with the code associated with that vote, which is chosen and known only by that voter,
- The prevention of attempted fraud by malicious third parties, as well as failure or errors in computer systems, by being able to trace the vote and the voter participation in the election with information given by the voter; by codes A and B predefined and authenticated, which are independent from the operation of the electronic voting system, and by the paper back-up which should match the electronic voting results that are also published on the Internet and / or Intranet.

[0032] The table below shows the qualities of the method and system for the six dimensions established to evaluate voting systems and methods, particularly for electronic voting.

Table 1. Dimensions of evaluation methods and voting systems

Dimension	**Requirement**	**Characteristic of the method and system proposed**
Vote legitimacy	Only legitimized voters can cast their vote.	Only the identifier of the portable device registered by the voter is entitled to cast one single vote by the method and system of the invention.
	Each voter may cast only one vote in each election.	
		Voters select a code A from a first plurality of randomly generated codes as they cast their vote in the portable device where said

Dimension	Requirement	Characteristic of the method and system proposed
		code A is associated with the identifier or IMEI obtained from the portable device (identifier set) allowing authentication of the origin of the identifier of the portable device with information provided by the voter and not only by the system.
		Voters select a code B from a second plurality of randomly generated codes different from code A as they cast their vote in the portable device where said code B is associated with the vote (voting set) allowing authentication of the origin of the vote with information provided by the voter and not only by the system.
		Random codes are predefined by a code module to allow the server authenticate the vote.
Verifiability	Each voter must be able to verify the validity of the vote cast.	The user or voter verifies their vote and participation in the voting process, once the results are published on the Internet and / or Intranet, using selected codes A and B, which are independent of the electronic voting system operation.
	Voters must be authorized to verify that their vote was properly counted.	
	The results of the election must be verifiable by the public, being this requirement a way to ensure that the process has been performed in the right way.	Prints of the voting set, identifier set and verification set leave a paper trail that acts as a backup to the electronic voting, which can also be used to verify the validity of the results; count of votes, count of participation and count of verification by the voting server, for example, in audits performed to the process or by public scrutiny
Anonymity	For an anonymous electronic election to be achieved, only the voter can know their votein the voting process.	Only the voter knows the selected codes A and B, which were generated randomly.
	The protection of private information is one of the most important requirements of electronic voting.	The voter does not receive an official record or print of the portable device identifier or IMEI with selected code A (set of identifiers) or vote and selected code B (voting set) that could compromise anonymity.
		Separate batches of information, voting set

Dimension	Requirement	Characteristic of the method and system proposed
		and identifier set are received and sorted randomly by the voting server, so that they cannot be associated based on the sequence in which they were received by the voting server.
		Printing of separate batches of information is generated randomly by the voting server and / or by a printing device that compiles them randomly, making the association between different paper trails of the vote impossible. For the voting set, the voting server starts the random printing only once a first vote expressing a different preference to the votes previously recorded is received, so that the first votes that express the same preference cannot be associated with voters.
		All temporary files that the system may have created during the voting process, containing information that allows the association of the voter with a vote, for example the voting set and the identifier set, are deleted to prevent a third party from having access to them.
Non Coercion	Each voter should be able to cast their vote according to their own decision, i.e., no voter can be forced to vote in a particular way.	Voting takes place in the privacy chosen by each voter using the portable device registered or in the privacy determined by the appropriate authority; thus, voting premises are established where access to the voting system can be controlled and only given through an Intranet network available on these premises.
		The codes are generated randomly (code A and code B) and they can be chosen only at the time the vote is issued, preventing voters from being coerced to compromise their vote.
		The voter does not receive an official record or print of their vote or codes, therefore when these are made public on the Internet and / or Intranet, the voter may not be assigned authorship of a particular vote.
		All temporary files that the system may have created during the voting process, containing information that allows

Dimension	Requirement	Characteristic of the method and system proposed
		association of the voter with a vote, for example the voting set and the identifier set, are deleted to prevent a third party from having access to them.
Voting intention	The voting process should be as simple as possible for the voter so to ensure that the vote cast is consistent withthe vote intent.	The voter uses its own portable device, wherein the method of voting is implemented.
	A friendly electronic voting interface is preferred, not requiring the learning of sophisticated techniques or the use of additional equipment.	Before completing the vote, this is confirmed by the voter as part of the selection process of codes. This gives the voter another opportunity to reflect their intended selection.
Security and transparency	A secure electronic voting system should prevent the vote count from being altered, duplicated or removed by third parties.	The security of the method and system proposed employs cutting edge security technology for portable devices, communication and servers, helping prevent the vote from being altered, duplicated or removed by someone and enabling the correct counting of legitimate votes.
	Every legitimate vote should be counted correctly.	
	The possibility for an illegitimate vote to be considered is completely eliminated.	However, in case of alteration of electronic records by malicious parties, fraud, failure or errors in computer systems, the verifiability of votes by voters with the predefined A and B codes -randomly generated but selected by the voter- provides an independent means to identify problems in the integrity of the process, thus ensuring the accuracy of the method and system proposed.
	The alteration of electronic records by malicious parties, fraud, failure or errors in computer systems should become clear, preventing any negative impact on the integrity of the process.	
		Prints of the voting set, the identifier set and the verification set leave a paper trail that acts as a backup to the electronic voting that can also be used to reveal whether the results of the vote have been altered, as well as the vote count, participation count and verification count by the voting server, for example, in audits performed to the process or by public scrutiny.

[0033] Considering the above, it follows that the method according to claim 1, proposed in the application is an electronic voting method implemented in portable devices, which improves transparency and speed in voting, and encourages participation therein. In its general aspects, said method is comprised of the following steps:

- Registering the identifier of the portable device used by the voter in casting their vote, and associating said identifier with the identity of the voter.
    - The voter registration with the identifier of the portable device consists of storing the identifier of the portable device along with the voter identification in a database.
    - The identifier of the portable device must correspond to the IMEI of the device.
    - Start the voting process where the portable device used by the voter is authenticated when establishing the connection by comparing the identifier of the portable device registered with the ID obtained from the portable device.

        ▪ The identification and verification module, which manages the identification interface, can be implemented on the portable device.

    - Generate the vote by the voter in the portable device registered.

        ▪ The vote includes the choice made by the voter.

        ▪ The vote may be multiple in the case of several elections, for instance candidates or questions to be answered, to which the elector is subject.

        ▪ The vote may include one or more texts written by the voter stating a position or opinion.

        ▪ The vote is generated at a voting interface proposed by a voting module.

        ▪ The voting module can be implemented in the portable device.

    - Select -by the voter- two of a first and second plurality of random codes received in the portable device.

        ▪ Before voting, a first and second plurality of random codes are received in the portable device, wherein said codes are predefined or generated by a module of codes.

        ▪ The module of codes can be implemented in the portable device.

    - Issue the vote at the voting interface, associating it with a code B selected by the voter from a second plurality of random codes received in the portable device.
    - Issue participation at the identification interface, associating it with a code A selected by the voter from a first plurality of random codes received in the portable device, which is different from code B.

- Send at least to one voting server the voting information comprising two separate batches of information, wherein:

  ▪ A first separate batch of information comprising the vote and code B selected by the voter from a second plurality of random codes received in the portable device, and

  ▪ A second separate batch of information including the identifier obtained from the portable device used in the casting of votes and code A selected by the voter from a first plurality of random codes received in the portable device, which must be different from code B.

  ▪ The separate batches of information are not associable with each other, preventing the vote and selected code B, generated by the voting module, and the identifier obtained from the portable device and selected code A, generated from an identification and verification module, from being associated.

  ▪ The voting module, as already indicated, can be implemented in the portable device.

  ▪ The identification and verification module, which manages the identification interface, can be implemented in the portable device.

- Receive the separate batches of information in at least one voting server, responsible for processing the information contained in each batch.

  ▪ First, the voting server authenticates the votes cast confirming that the selected code B belongs to one of the predefined codes, and processes the vote count.

  ▪ In addition, the voting server verifies that the identifiers obtained from the portable devices that have issued votes are duly registered in the database, confirming that the selected code A belongs to one of the predefined codes, and processes the voter participation.

  ▪ The separate batches of information are sorted randomly by the voting server, making impossible the association among different batches by the sequence in which they are received by the voting server.

- Print in at least one printing device, the separate batches of information received in the voting server, leaving a paper trail that acts as support for the electronic voting.

  ▪ Printing of separate batches of information is generated randomly by the voting server and / or randomly compiled by the printing device, making the association between different paper trails of the vote impossible.

[0034] Furthermore, an embodiment of the invention may comprise the step of:

- Verification, by the voter, that its vote and participation were properly recorded once the results are published on the Internet and / or Intranet.

  ▪ Once the results are published on the Internet and / or Intranet, the voting server notifies the voter, for example through email, to consult on the Internet and / or Intranet, using codes A and B previously selected, if their vote and participation were correctly recorded.

  ▪ The voter issues their verification at the verification interface.

  ▪ The verification information that includes the verification and the identifier obtained from the portable device used is sent to at least one voting server.

  ▪ At least one voting server receives the verification information, and is responsible for processing the information. The voting server authenticates the verifications issued, confirming that the identifiers obtained from the portable devices that have issued verification are properly registered in the database, and processes the verification counting.

  ▪ Print in at least one printing device, the batch of verification information, leaving a paper trail that acts as support for electronic voting.

  ▪ The verification interface may be implemented in the identification and verification module, or in a separate module.

  ▪ The identification and verification module, as already indicated, can be implemented in the portable device.

[0035] As you may notice, the method described above is implemented in a system according to claim 10, associated with that method, wherein said system is comprised of:

- A portable device for each voter;
- At least one database for recording and storing of identifiers of portable devices associated with the identity of voters and other data relating to the voting process, developed in accordance with the requirements of the authority responsible for the vote, which may be comprised of, but is not limited to, data of candidates, data of the positions for which they are running, data of questions to be voted on, data of the voter registry, data of the clustering of voters by sector or station, etc.
- At least one module of codes in which a first and second plurality of codes are randomly generated for each batch;

  ▪ The module of codes can be implemented in the portable device.

  ▪ The module of codes can obtain the first and second plurality of random codes from a

database of codes.

- At least one voting module where the information on vote cast and code B, selected by the voter from a second plurality of random codes received in the portable device, is entered by the voter;

  ▪ The voting module can be implemented in the portable device.

- At least one identification and verification module that gets the identifier from the portable device and the code A, selected by the voter from a first plurality of random codes received in the portable device, is entered by the voter together with the verification information;

  ▪ The identification and verification module can be implemented in the portable device.

- At least one voting server that coordinates voting and receives the separate batches of information issued from the portable device and orders them randomly and where printing of separate batches of information is generated randomly, thus making the association among different paper trails of voting impossible.
- At least one printing device wherein the printing of separate batches of information is compiled randomly, making the association among different paper trails of voting impossible.

[0036] Considering the above, it is noted that the method and system proposed in the application meets the requirements of the six dimensions of assessment established for voting systems and methods, solving the problem of allowing voters to verify the right cast and count of their vote, avoiding the risk of disclosing the identity of the voter, i.e. ensuring their anonymity and providing the transparency required to prevent the realization of possible malicious attempts, fraud, failure or errors in computer systems. In addition, thanks to the high levels of security of current portable devices and the user experience offered by these devices, the proposed solution allows a quick, participation-encouraging voting system and method.

Brief Description of the Figures

[0037] As part of the present application the following representative figures of the invention are presented, which teach preferred embodiments thereof and, therefore, should not be construed as limiting the definition of the application.

Figure 1 shows a scheme of the system according to an embodiment of the invention wherein the system operates in on-line mode.

Figure 2 shows a scheme of the system according to an embodiment of the invention including the verification process as part of the system, wherein the system operates in on-line mode.

Figure 3 shows a scheme of the system according to an embodiment of the invention wherein the system operates in an offline mode.

Figure 4 shows a scheme of the system according to an embodiment of the invention including the verification process as part of the system, wherein the system operates in an offline mode.

Figure 5 shows a scheme of the method of the invention implemented in the system of Figure 1.

Figure 6 shows a scheme of the method of the invention implemented in the system of Figure 2.

Description of the Preferred Embodiment

[0038] Figure 1 shows a scheme of an embodiment of an electronic voting system proposed by the application, wherein the system operates in on-line mode, that is, in direct and instant communication through a network. In this scheme, a portable device 1 is shown, which is in communication with at least one code module 2, at least one module of identification and verification 4 and at least one voting module 3. Communication between the modules and the portable device 1 is such that:

- The at least one identification and verification module 4 is comprised of an identifier code (ID code) of the portable device 1, which is previously stored in the module and is verified with the ID code contained in the portable device 1, for establishing the communication.

  ◦ This module via an interface of identifier 40a receives a set of identifier 10a comprised of the identifier code obtained from the portable device 1 associated with the code A, selected by the voter from a first plurality of random codes received in the portable device, as part of the voting process.

  ◦ In an alternative embodiment shown in Figure 2, this module via an interface check 50a receives a set of verification 10c comprised of the identifier code obtained from the portable device 1 together with verification of the voter.

- The at least one code module 2 sends to the portable device 1 a first and second plurality of random codes 20a and 20b, respectively, which must be different from each other and which have been generated in the module of codes 2 and from which the voter will select one of each, code A and code B. The random codes may be comprised of numeric, alphanumeric and / or image codes.

  ◦ In one embodiment, the first plurality of random codes 20a is displayed on the screen of device 1, before generating the vote but after communication is established, so that the voter may select code A, which will be associated with the identifier code obtained

from the portable device 1 creating the identifier set 10a, and then again a second plurality of random codes 20b is displayed on the screen of device 1 after generating the vote, for the voter to select a code B, where code B will be associated with the vote, thus creating the voting set 10b.

◦ In a second embodiment, the first and second plurality of random codes 20a and 20b, respectively, is displayed on the screen of device 1 after generating the vote, for the voter to select code A, which will be associated with the identifier code obtained from portable device 1 creating the identifier set 10a, and the code B to be associated with the vote, creating the voting set 10b.

- The at least one voting module 3 allows a voting interface 30a to be displayed in the portable device. After the vote, said module receives the voting set 10b comprised of the vote cast, which can be a written text, by the voter associated with the random code B that said voter has selected, which is different from the code A that is associated with the identifier code obtained from portable device 1 according to the above.

[0039] Additionally, in one embodiment of the invention, modules 2, 3 and 4 are implemented in a single voting management module, which can be in turn implemented in the portable device 1 or, at least, in a voting server 6. Here, one embodiment of the invention contemplates that each module can be implemented separately in the portable device 1 or in, at the least a voting server 6. In addition, each module mentioned corresponds to a computer program responsible for carrying out the actions associated with each module.

[0040] Moreover, Figure 1 shows that the identification and verification module 4 and voting module 3 sends two separate batches of information 30b and 40b to a network 5, where the first separate batch of information 30b includes the voting set 10b, while the second separate batch of information 40b includes the identifier set 10a of portable device 1. In this context, it is worth noting that the network 5 can be any network that allows data transfer through portable devices such as type networks 2G and subsequent generation, or Intranet or Internet connections, such as wireless communication technologies. In an alternative embodiment, shown in Figure 2, three separate batches of information are implemented, wherein one separate batch of information 50b is comprised of a set of verification 10c.

[0041] Furthermore, in an alternative embodiment of the invention, the at least one voting server 6 communicates with the portable device 1 via the network 5, sending information to said portable device. In particular, according to the present embodiment, the voting server 6 sends the first and second plurality of random codes 6a to the module of codes 2, information on identifiers of registered portable devices 6b and alternatively as shown in Figure 2, information on the verification interface 6d to the identification and verification module 4 and / or information concerning the voting interface 6c to the voting module 3; these embodiments are illustrated with dotted lines in Figures 1 and 2. Moreover, at least one voting server 6 can operate as coordinating voting unit and at the same time, as a counting, printing entity, as well

as serving other functions relating to the voting process for both modes online and offline. However, alternative systems embodiments of the online and offline modes consider the use of separate servers or machines to coordinate voting, count the results and print the separate batches of information.

[0042] In the online mode shown in Figure 1, the two separate batches of information 30b and 40b are instantly communicated after the user casts its vote to the at least one voting server 6 via network 5 wherein said at least one voting server 6 receives each separate batch of information and processes them separately for validation, authentication and counting, and sorts them randomly to prevent the vote and the voter from being associated with the sequence in which the batches of information are received by the voting server 6. In this context, for the first separate batch of information 30b, which includes the voting set 10b, the at least one voting server 6 authenticates that the selected code B associated with the vote belongs to one of the codes of the second plurality of random codes 20b, counting the votes correctly issued or authenticated. Additionally, the at least one voting server 6 can count the unauthenticated votes. Moreover, for the second separate batch of information 40b, containing the identifier set 10a of the portable device 1, the at least one voting server 6 validates that said identification code obtained from the portable device 1 is registered in at least one database 7 containing the record of identifiers of portable devices associated with the identity of the voter, and that the selected code A associated with the identifier belongs to one of the codes of the first plurality of random codes 20a. Additionally, the at least one voting server 6 can count the unauthenticated identifiers. Finally, according to the embodiment of the invention shown in Figure 2 there is one separate batch of verification information 50b, which together with the two separate batches of information 30b and 40b forms a third separate batch of information, where said third separate batch of information 50b is comprised of the verification set 10c. In this context, the at least one voting server 6 authenticates that the identifier code obtained from the portable device 1 is registered in at least one database 7 containing the record of identifiers of portable devices associated with the voter identity, counting the authenticated verifications. Additionally, the at least one voting server 6 may count the unauthenticated verifications.

[0043] The at least one database 7 can be implemented in at least one voting server 6 or be in direct communication with the server via the network 5. Said database shall be construed as any means for storing information, whether tangible or intangible, which contains information on voting; for example, at least one database of codes, database of candidates, database of offices to which they are running, database of questions to be voted, database of the registry of voters, database voters clusters by sector or station, etc., where said databases may be comprised of independent databases or one and the same general database. Furthermore, communication between the at least one voting server 6 and the at least one database 7 is such that the at least one voting server 6 queries and / or writes over the at least one database 7 after the voting process has started.

[0044] According to Figures 1 and 2, the at least one voting server 6 can randomly order the separate batches of information 30b, 40b and alternatively 50b for their later sending to at

least one printing device 8, wherein said at least one printing device prints and randomly compiles each separate batch of information, leaving a paper trail 8a, 8b and alternatively 8c of voting. Said paper trail separately comprises a first paper trail 8a corresponding to the first separate batch of information 30b, a second paper trail 8b corresponding to the second separate batch of information 40b and, alternatively, a third paper trail 8c corresponding to the third separate batch of information 50b. Moreover, this mechanism allows backing up the electronic voting that is counted in at least one voting server 6. Alternatively, the at least one printing device 8 deposits the paper trail in at least one printing receptacle 9, as shown in Figure 2, wherein said printing receptacle can be used in any of the embodiments of the present invention.

[0045] In one embodiment of the invention, both for online and offline operation, there are groups of printing devices, wherein said printing device groups are separately designated to print each separate batch of information.

[0046] Figure 3 shows an embodiment of the system according to the invention operating in offline mode. Here, the main difference from the system shown in Figure 1 is that voting is performed in the portable device 1 without being in direct and instantaneous communication with the network 5. In fact, in this embodiment of the invention, the voting server 6 communicates to the portable device 1 the information concerning voting (6a, 6b, 6c and alternatively 6d) only when the process is started, where only after the voting and verification has taken place, the portable device 1 sends separate batches information 30b, 40b and alternatively 50b to the at least one voting server 6 which can act as coordinating unit and / or counting unit. Then, both in online and offline mode, the at least one voting server 6 acting as counting unit proceeds to record the voting results electronically and, by at least one printing device 8, to print paper trails 8a, 8b and alternatively 8c corresponding to the separate batches of information 30b, 40b and 50b, respectively. Furthermore, as it can be derived from the above description, the off-line mode shown in Figure 3 can also operate by incorporating the verification set 10c as shown in Figure 4.

[0047] Figure 5 shows a diagram associated with the electronic voting method proposed in the application, wherein the steps of registering (100) the identifier of the portable device 1, which can be a cell phone, smartphone or any device proposed with a universal unique identifier of the IMEI type. Such registration is performed by associating the portable device identifier with the identifier of a voter, wherein said portable device identifier may correspond to the IMEI of the device. This means that the invention considers that a single portable device 1 is associated with each voter.

[0048] Once the registration is complete, the voter is authorized to use their portable device 1 in the electronic voting process. In one embodiment, the information on the registration of portable devices and voters is stored in at least one database 7 by means of at least one voting server 6 which communicates with the portable device 1.

[0049] Subsequently, the voter can generate (200) the vote in the portable device 1 registered

using said device for voting. The vote includes the choice that the voter has made, which can be a text written by the voter, preferably being generated at the voting interface 30a that is displayed on the screen of the portable device 1. Said voting interface is generated through the voting module 3, which may or may not be implemented in the portable device 1 or in the voting server 6.

[0050] Before casting the vote from the portable device, the voter must select (300) two distinct codes, A and B, from the first and second plurality of random codes 20a and 20b received in the portable device 1, wherein said first and second plurality of random codes 20a and 20b has been generated in the module of codes 2, which may or may not be implemented in the portable device 1 or in the voting server 6.

[0051] Once the codes have been selected, the voter is authorized to cast (400) its vote and to issue (450) its identifier. The set of information including the vote and the code B selected from the second plurality of random codes 20b is called voting set 10b. The information set comprised of the identifier obtained from the portable device that may correspond to the IMEI of the device and code A selected from the first plurality of random codes 20a is called identifier set 10a.

[0052] With the casting of the vote by the voter, the system gets the identifier set 10a of the portable device and sends (500) the voting information to the at least one voting server 6 that is in communication with the portable device 1 through the network 5. Said voting information includes two separate batches of information 30b and 40b, wherein the first batch of separate information 30b includes the voting set 10b and the second batch of separate information 40b comprises the identifier set 10a of the portable device used in casting the vote. Such separate batches of information are not associable with each other. In one embodiment, the voting set 10b is sent from the voting module 3 and the identifier set of the portable device 10a is sent from the identification and verification module 4, wherein said modules 3 and 4 may or may not be implemented in the portable device 1 or in the voting server 6.

[0053] By sending the voting information in two separate batches of information 30b and 40b, the method is further comprised of receiving (600) the separate batches of information in the at least one voting server 6 that is in charge of processing the information contained in each batch. In this context, according to one embodiment, the at least one voting server 6 authenticates the votes cast, confirming that the selected code B associated with the vote belongs to one of the predefined codes, registers the batches at random and processes the voting count. Moreover, the at least one voting server 6 verifies that the identifiers of the portable devices 1 that have issued a vote are duly registered in the database 7 corroborating that the selected code A associated with the identifiers of the portable devices 1 belongs to one of the predefined codes, registers the batches at random and processes the attendance count. In this regard, the at least one voting server 6 acts as coordinating voting unit and counting unit, and separate servers or machines can be used for such work.

[0054] In the next step, the method of the invention consider printing (700), in the at least one

printing device 8, the separate batches of information received in at least one voting server 6, leaving a paper trail 8a and 8b, where the paper trail is randomly generated by the voting server and / or printing device that randomly compiles them, making impossible the association between the different paper trails, which act as a backup to the electronic voting.

[0055] One embodiment of the method of the invention, shown in Figure 6 and which is complemented by the method of Figure 4, provides for the verification (800) by the voter, that their vote and participation were recorded correctly once the results are published on the Internet and / or Intranet. Once the results are published on the Internet and / or Intranet, the voting server 6 notifies the voter - for example through email - to consult the Internet and / or Intranet using the codes A and B previously selected, and determine if their vote and participation were properly recorded.

[0056] Then, the voter generates (900) their verification in the portable device 1 registered. The verification is comprised of the voter's confirmation or rejection of the results published, preferably generated at the verification interface 50a that is displayed on the screen of the portable device 1. The identification and verification module 4, which may or may not be implemented in the portable device 1, generates such verification interface.

[0057] Once the voter verifies their vote and participation, the voter casts (1000) their verification. The set of information including the verification and the identifier of the portable device is called verification set 10c.

[0058] With the issuance of the verification by the voter, the system retrieves the set of verification 10c of the portable device and sends (1100) the verification information to the at least one voting server 6 that is in communication with the portable device 1 by network 5. Such verification information is comprised of at least one batch of information 50b, which includes the set of verification 10c of the portable device used in the issuance of the verification. In one embodiment, the verification set 10c is sent from the identification and verification module 4 wherein said identification and verification module 4, as already mentioned, may or may not be implemented in the portable device 1 or in the voting server 6.

[0059] By sending the verification information in at least one separate batch of information 50b, the method is further comprised of receiving (1200) the separate batch of information in at least one voting server 6 that is in charge of processing the information contained in the batch. In this context, according to one embodiment, the at least one voting server 6 authenticates the verification, confirming that the identifiers of portable devices 1 that have issued the verification are duly registered in the database 7, registers the batch and processes the verification counting. In this regard, the at least one voting server 6 acts as coordinating voting unit and counting unit, and separate servers or machines can be used for such work.

[0060] In the last step, the method of the invention consider printing (700'), all separate batches of information received in at least one voting server 6, in the at least one printing device 8, leaving a paper trail 8a, 8b and 8c, which acts as a backup to the electronic voting. In

this context, the paper trails 8a and 8b correspond to those generated from the sending (500) of the voting information, while the paper trail 8c corresponds to that generated by the sending (1000) of the verification information according to the present embodiment.

[0061] In addition, alternative embodiments of the invention consider that in order to access the voting interface 30a and verification interface 50a, the user must log into this voting interface 30a and verification interface 50a using a secure connection to initiate communication with the at least one voting server 6. In the online mode, connection is initially established to carry out the whole process of voting in direct connection with the at least one voting server 6, using the portable device 1 to verify that the portable device is properly registered and as a means of entering information, while in the offline mode the connection is initially performed to verify that the portable device is properly registered by its identifier, for voting, with the voting or verification being performed without a direct connection with the at least one voting server 6.

[0062] Considering this, the online mode requires that communication between the portable device 1 and the voting server 6 is set during voting and verification, with the information being sent and received according to the method proposed. Here, after the separate batches of information have been generated that correspond to the identifier set of the portable device 10a, the voting set 10b and the verification set 10c, said batches of information are instantly communicated by the at least one voting server 6, with the voting set acting as a coordinating unit or the machine acting as counting unit, where such units may be part of the same voting server 6. The counting unit updates the electronic voting results and coordinates the printing of the paper trails 8a, 8b and 8c corresponding to separate batches of information 30b, 40b and alternatively 50b, respectively, where such coordination is performed by the voting server 6 or directly with the at least one printing device 8.

[0063] Instead, the offline mode comprises that communication between the portable device 1 and at least one voting server 6 may be established only for sending information, which means that the portable device 1 becomes much more relevant in the voting process acting as a voting interface itself rather than an input device as in the online mode. Indeed, in the offline mode the portable device 1 is validated in communication with the poling server 6 acting as a voting coordinating unit, which, according to one embodiment, sends information (6a, 6b, 6c and alternatively, 6d) necessary for the voting process to be started in the portable device 1. Then, the connection between the voting server 6 and the portable device 1 may be ended. Once the modules 2, 3 and 4 of the portable device receive the information 6a, 6b, 6c, and alternatively, 6d, the voting process is initiated using the voting interface 30a to cast the vote. Then, the portable device, through modules 3 and 4, generates the separate batches of information 30b and 40b corresponding to the voting set 10b and the identifier set 10a, and alternatively, the separate batch of information 50b for the set of verification 10c. Said batches of information are then communicated to the at least one voting server 6 acting as counting unit, starting a new secure connection, wherein the said at least one voting server 6 starts the process of updating the results of the electronic voting and printing paper trails corresponding to the separate batches of information.

[0064] Furthermore, the invention considers that communication between the at least one voting server 6 and the portable device 1 is performed by a software implemented in the portable device 1 or in the at least one voting server 6 wherein said software consists of the modules of the present invention.

[0065] It should be noted that the present invention is applicable both for voting and opinion or preference polls. Thus, the terms "electors", "voters" and "vote" used in the present application should be considered as synonyms or including such terms as "respondents," "opinion" or "preference" as used in the processes of surveys.

REFERENCES CITED IN THE DESCRIPTION

Cited references

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

- US20110238463A **[0005]**
- US20120095811A **[0005]**
- US20140207537A **[0006]**
- US20020077886A **[0007]** **[0007]**
- WO2012137035A **[0008]** **[0008]**
- JP2011028376B **[0009]**
- EP2455919A **[0010]** **[0010]** **[0010]**
- US20140089062A **[0011]** **[0011]** **[0012]**
- US20080105742A **[0012]**
- US2005101307A **[0012]**
- US2004046021A **[0013]**

PATENTKRAV

1. Elektronisk afstemningsfremgangsmåde under anvendelse af en bærbar enhed (1), der forbedrer en afstemnings transparens og hastighed, hvilket opmuntrer til deltagelse i afstemningsprocessen, hvilken afstemningsfremgangsmåde består af:

- registrering (100) i mindst én database (7) af en identifikatorkode for den bærbare enhed (1), som anvendes af en vælger til at stemme, hvilket associerer identifikatoren med vælgerens identitet, hvor den bærbare enhed er i kommunikation med mindst ét modul af koder (2), mindst ét identifikations- og verifikationsmodul (4) og mindst ét afstemningsmodul (3);

- generering (200) af en stemme afgivet af vælgeren i den registrerede bærbare enhed (1), hvor stemmen er vælgerens valg under afstemningsprocessen;

- valg (300), foretaget af vælgeren, af en kode A fra en første flerhed af vilkårlige koder (20a), der modtages i den bærbare enhed (1), og en kode B fra en anden flerhed af vilkårlige koder (20b), der modtages i den bærbare enhed (1), hvor den første og den anden flerhed af vilkårligt genererede koder, i offline-modus, er foruddefineret og ens for alle vælgere, idet de består af et antal permutationer, der gør det næsten umuligt for to vælgere at vælge den samme kode for den samme afstemning, og den første og den anden flerhed af vilkårlige koder genereres, i online-modus, for hver ny gruppe af vælgere, undtagen de koder, som allerede er anvendt i afstemningen, inden de sendes til nye vælgere med henblik på valg og efterfølgende autentificering;

- afgivelse (400) af stemmen i en afstemningsgrænseflade (30a), der associerer den med koden B, der vælges af vælgeren, hvor associeringen af stemmen og den valgte kode B benævnes afstemningssæt (10b);

- udstedelse (450) af identifikatoren for den bærbare enhed i en identifikatorgrænseflade (40a), der associerer den med kode A, der vælges af vælgeren, hvor associeringen af identifikatoren for den bærbare enhed og den valgte kode A benævnes identifikatorsæt (10a);

- afsendelse (500) via et netværk (5) til mindst én server (6) af afstemningsinformationerne, der består af to separate batcher af informationer, som ikke kan associeres med hinanden, hvor:

  - en første separat batch af informationer (30b) består af afstemningssættet (10b); og

  - en anden separat batch af informationer (40b) består af identifikatorsættet (10a);

- modtagelse (600) af de separate batcher af informationer i den mindst ene server (6), der er ansvarlig for at behandle og vilkårligt registrere de informationer, som er indeholdt i hver batch, hvor den mindst ene server (6) autentificerer den afgivne stemme, hvilket bekræfter, at den valgte kode B tilhører én af koderne for den anden flerhed af vilkårlige koder og behandler stemmeoptællingen, og hvor den mindst ene server (6) verificerer, at de identifikatorer, der opnås fra de bærbare enheder, som har afgivet stemmen, registreres behørigt, hvilket bekræfter, at den valgte kode A tilhører én af koderne for den første flerhed af vilkårlige koder; og

- udprintning (700) i mindst én udprintningsenhed (8) af de separate batcher af informationer, der modtages i den mindst ene server (6), hvilket efterlader et papirspor (8a, 8b), der fungerer som backup for den elektroniske afstemning, hvor den første flerhed af vilkårlige koder (20a) og den anden flerhed af vilkårlige koder (20b) modtages fra det mindst ene modul af koder (2), hvor den første og den anden flerhed af vilkårlige koder (20a, 20b) er foruddefineret eller genereres i det mindst ene modul af koder (2), og de er forskellige, og hvor det mindst ene modul af koder (2) opnår den første og den anden flerhed af foruddefinerede vilkårlige koder (20a, 20b) fra den mindst ene database (7), der er implementeret i den mindst ene server (6) eller er tilgængelig på netværket (5), og hvor den mindst ene server (6) vilkårligt registrerer de to separate batcher af informationer (30b, 40b), hvilket gør associeringen mellem de forskellige batcher umulig ifølge den sekvens, i hvilken de blev modtaget i serveren (6), hvor udprintningen af de separate batcher af informationer (30b, 40b) genereres vilkårligt af serveren (6) og/eller den mindst ene udprintningsenhed (8), der vilkårligt kompilerer dem, hvilket gør associeringen mellem de forskellige papirspor for afstemningen umulig, og hvor

serveren (6), for afstemningssættet (10b), kun begynder den vilkårlige udprintning, når der er registreret en første stemme, som udtrykker en forskellig præference i forhold til tidligere registrerede stemmer.

2. Elektronisk afstemningsfremgangsmåde ifølge krav 1, hvor registreringstrinnet (100) består af lagring af identifikatoren for den bærbare enhed (1) sammen med identifikationen af vælgeren og andre data relateret til afstemning i den mindst ene database (7).

3. Elektronisk afstemningsfremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor den mindst ene server (6) behandler optællingen af identifikatorer.

4. Elektronisk afstemningsfremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor udprintningstrinnet udføres i mindst to grupper af udprintningsenheder (8), hvor de mindst to grupper af udprintningsenheder er separat udpeget til at printe hver separat batch af informationer.

5. Elektronisk afstemningsfremgangsmåde ifølge et hvilket som helst af de foregående krav, hvor den også består af følgende trin:

- kommunikation (800) ved hjælp af serveren (6) til den bærbare enhed (1) af afstemningsresultaterne som offentliggjort på internettet og/eller et intranet;

- generering (900) af verificeringen af vælgeren i den registrerede bærbare enhed (1);

- udstedelse (1000) af verificeringen i en verificeringsgrænseflade (50a), der associerer den med den identifikatorkode, som blev opnået fra den bærbare enhed, hvor associeringen benævnes verificeringssæt (10c);

- afsendelse (1100) via netværket (5) til mindst én server (6) af verificeringsinformationer, der består af mindst én informationsbatch (50b), som omfatter verificeringssættet;

- modtagelse (1200) af informationsbatchen i den mindst ene server (6), der er ansvarlig for behandling og registrering af de informationer, som er indeholdt i hver batch;

- udprintning (700') i mindst én udprintningsenhed (8) af batchen af informationer, der modtages i mindst én server (6), hvilket efterlader et papirspor (8c), der fungerer som backup for elektronisk afstemning, hvor udprintningen af de separate batcher af informationer genereres vilkårligt af afstemningsserveren og/eller en udprintningsenhed, der vilkårligt kompilerer dem, hvilket gør associeringen mellem de forskellige papirspor for afstemning umulig og efterlader et papirspor (8a, 8b, 8c), der fungerer som backup for elektronisk afstemning.

6. Elektronisk afstemningsfremgangsmåde ifølge krav 5, hvor den mindst ene server (6) ved hjælp af netværk (5) også sender informationer relateret til verificeringsgrænsefladen (6d).

7. Elektronisk afstemningsfremgangsmåde ifølge kravene 5 eller 6, hvor serveren (6), til den bærbare enhed (1), kun kommunikerer de informationer, der er relateret til afstemningsverificeringen (6d), når afstemningsresultaterne er blevet optalt.

8. Elektronisk afstemningsfremgangsmåde ifølge et hvilket som helst af kravene 5 til 7, hvor verificering svarer til bekræftelsen foretaget af vælgeren om, at resultaterne, der er offentliggjort på internettet og/eller et intranet, korrekt afspejler deres stemmer og deltagelse, hvor verificeringen genereres på verificeringsgrænsefladen (50a), hvor verificeringsgrænsefladen (50a) foreslås af det mindst ene identifikations- og verificeringsmodul (4), og hvor verificeringssættet (10c) kommer fra det mindst ene identifikations- og verificeringsmodul (4).

9. Elektronisk afstemningsfremgangsmåde ifølge et hvilket som helst af kravene 5 til 8, hvor den mindst ene server (6) behandler optællingen af verificeringer.

10. Elektronisk afstemningssystem under anvendelse af bærbare enheder (1), der omfatter:

- en bærbar enhed (1) hos hver vælger,

- mindst ét modul af koder (2),

- mindst ét identifikations- og verificeringsmodul (4) og

- mindst ét afstemningsmodul (3),

hvor den bærbare enhed er til kommunikation med det mindst ene modul af koder (2), det mindst ene identifikations- og verificeringsmodul (4) og det mindst ene afstemningsmodul (3), hvor:

○ modulet af koder (2) er konfigureret til at generere en første og en anden flerhed af vilkårlige koder (20a, 20b) til hver afstemning, der sendes til den bærbare enhed (1) hos hver vælger med henblik på valg;

○ det mindst ene afstemningsmodul (3) er konfigureret til at tillade en afstemningsgrænseflade (30a) at blive vist i den bærbare enhed (1), og efter afstemningen konfigureres modulet til at modtage et afstemningssæt (10b), der består af den stemme, som afgives af hver vælger, der er associeret med en kode B, der er valgt af vælgeren ud fra den anden flerhed af vilkårlige koder, som modtages i den bærbare enhed hos hver vælger;

- det mindst ene identifikations- og verificeringsmodul (4) er konfigureret til at tillade en identifikationsgrænseflade (40a) at blive vist i den bærbare enhed (1), inden eller efter afstemningen, og modulet er konfigureret til at modtage et identifikatorsæt (10a), som består af den enkelte identifikator, der opnås fra den bærbare enhed (1) med en kode A, som vælges af vælgeren ud fra den første flerhed af vilkårlige koder, der modtages i den bærbare enhed hos hver vælger, hvor kode A er forskellig fra kode B, og hvor den første og den anden flerhed af vilkårligt genererede koder, når systemet fungerer i offline-modus, er foruddefineret og ens for alle vælgere, idet de består af et antal permutationer, der gør det næsten umuligt for to vælgere at vælge den samme kode for den samme afstemning, og når systemet fungerer i online-modus, genereres den første og den anden flerhed af vilkårlige koder for hver ny gruppe af vælgere undtagen de koder, der allerede er anvendt i afstemningen, inden de sendes til nye vælgere med henblik på valg og efterfølgende autentificering;

- mindst én server (6), der er forbundet med et netværk (5) og konfigureret til at modtage to separate batcher af informationer, som er udstedt fra den

bærbare enhed (1), hvor en første separat batch af informationer (30b) består af afstemningssættet (10b), og en anden separat batch af informationer (40b) består af identifikatorsættet (10a) af den bærbare enhed (1), hvor den mindst ene server (6) er konfigureret til at autentificere den afgivne stemme, hvilket bekræfter, at den valgte kode B tilhører én af koderne af den anden flerhed af vilkårlige koder, og at behandle stemmeoptællingen, og hvor den mindst ene server (6) er konfigureret til at verificere, at identifikatorerne, der opnås fra de bærbare enheder, som har afgivet stemmen, registreres behørigt, hvilket bekræfter, at den valgte kode A tilhører én af koderne af den første flerhed af vilkårlige koder;

- mindst én udprintningsenhed (8) er konfigureret til at printe et papirspor for de separate batcher af informationer, der modtages i den mindst ene server (6); og

- mindst én database (7), der er implementeret i den mindst ene server (6) eller tilgængelig på netværket (5), hvor den første flerhed af vilkårlige koder (20a) og den anden flerhed af vilkårlige koder (20b) modtages fra det mindst ene modul af koder (2), hvor den første og den anden flerhed af vilkårlige koder (20a, 20b) er foruddefineret eller genereres i det mindst ene modul af koder (2), og de er forskellige, og hvor det mindst ene modul af koder (2) er konfigureret til at opnå den første og den anden flerhed af foruddefinerede vilkårlige koder (20a, 20b) ud fra den mindst ene database (7), der er implementeret i den mindst ene server (6) eller tilgængelig på netværket (5), og hvor den mindst ene server (6) er konfigureret til vilkårligt at registrere de to separate batcher af informationer (30b, 40b), hvilket gør associeringen mellem de forskellige batcher umulig ifølge den sekvens, i hvilken de blev modtaget i serveren (6), hvor udprintningen af de separate batcher af informationer (30b, 40b) genereres vilkårligt af serveren (6), og/eller den mindst ene udprintningsenhed (8) er konfigureret til vilkårligt at kompilere dem, hvilket gør associeringen mellem de forskellige papirspor for afstemningen umulig, og hvor serveren (6), for afstemningssættet (10b), kun begynder den vilkårlige udprintning, når der er registreret en første stemme, som udtrykker en forskellig præference i forhold til tidligere registrerede stemmer.

11. Elektronisk afstemningssystem ifølge krav 10, hvor den mindst ene database (7) er konfigureret til at registrere og lagre identifikatorerne af de

bærbare enheder, der er associeret med hver vælgers identitet, hvor databasen (7) er implementeret i den mindst ene server (6) eller tilgængelig på netværket (5).

12. Elektronisk afstemningssystem ifølge krav 11, hvor databasen (7) indeholder informationer relateret til afstemning, for eksempel den mindst ene database over vilkårlige koder, databasen over kandidater, databasen over positioner, til hvilke de opstiller, databasen over de spørgsmål, der skal stemmes om, databasen over vælgerregister, databasen over vælgergrupperne efter sektor eller station osv., hvor databaserne kan omfatte uafhængige databaser eller én og samme generelle database.

13. Elektronisk afstemningssystem ifølge et hvilket som helst af kravene 10 til 12, hvor de to separate batcher af informationer (30b, 40b) kommunikerer med den mindst ene server (6) via netværket (5), hvor den mindst server (6) er konfigureret til at modtage hver separat batch af informationer (30b, 40b) og, separat, at behandle med henblik på validering, autentificering og optælling og at registrere de første to batcher (30b, 40b) vilkårligt, hvilket således gør associeringen mellem de to forskellige batcher umulig ifølge den sekvens, i hvilken de blev modtaget af serveren.

14. Elektronisk afstemningssystem ifølge et hvilket som helst af kravene 10 til 13, hvor papirsporet, separat, består af: et første papirspor (8a) svarende til den første separate batch af informationer (30b) og et andet papirspor (8b) svarende til den anden separate batch af informationer (40b).

15. Elektronisk afstemningssystem ifølge krav 14, hvor det består af to udprintningsenheder (8), der er konfigureret til at printe begge papirspor (8a, 8b) hver for sig, og udprintningen af de separate batcher af informationer kompileres vilkårligt, hvilket således gør associeringen mellem de forskellige papirspor for afstemning umulig.

16. Elektronisk afstemningssystem ifølge et hvilket som helst af kravene 10 til 15, hvor det mindst ene identifikations- og verificeringsmodul (4) også er konfigureret til at tillade en verificeringsgrænseflade (50a) at blive vist i den bærbare enhed (1) efter afstemning, og modulet er konfigureret til at modtage et verificeringssæt (10c) bestående af verificeringen, som udstedes af hver vælger, der er associeret med identifikatoren, som opnås fra den bærbare enhed (1).

17. Elektronisk afstemningssystem ifølge krav 16, hvor den mindst ene server (6), der er forbundet med et netværk, også er konfigureret til at modtage én separat batch af informationer (50b), der udstedes fra den bærbare enhed (1), hvor den separate batch af informationer (50b) består af verificeringssættet (10c), og hvor den ene separate batch af informationer (50b) kommunikerer med den mindst ene server (6) via netværket (5), hvor den mindst ene server (6) er konfigureret til at modtage den ene separate batch af informationer (50b) og at behandle den separat med henblik på validering, autentificering og optælling.

18. Elektronisk afstemningssystem ifølge krav 17, hvor papirsporet også består af et tredje papirspor (8c) svarende til den tredje separate batch af informationer (50b).

DRAWINGS

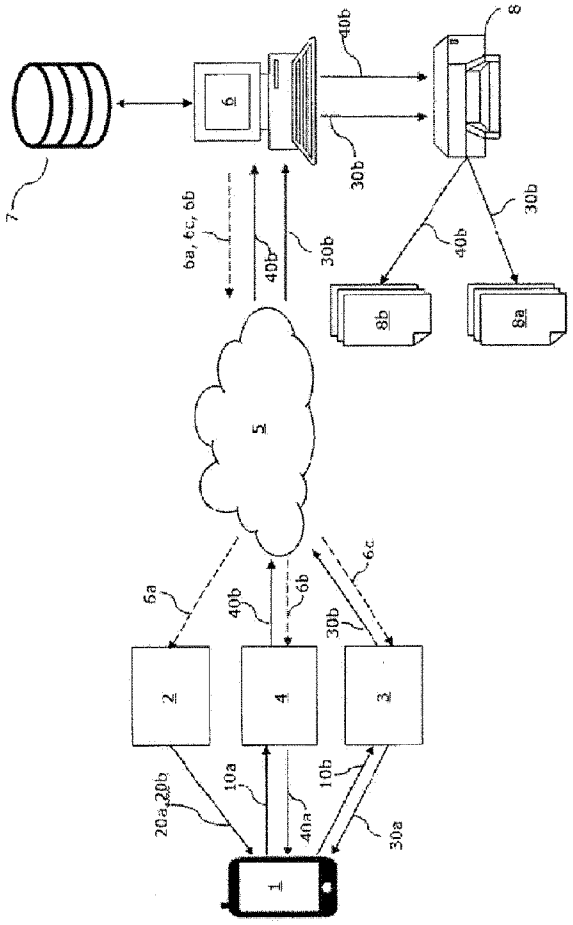

FIG.1

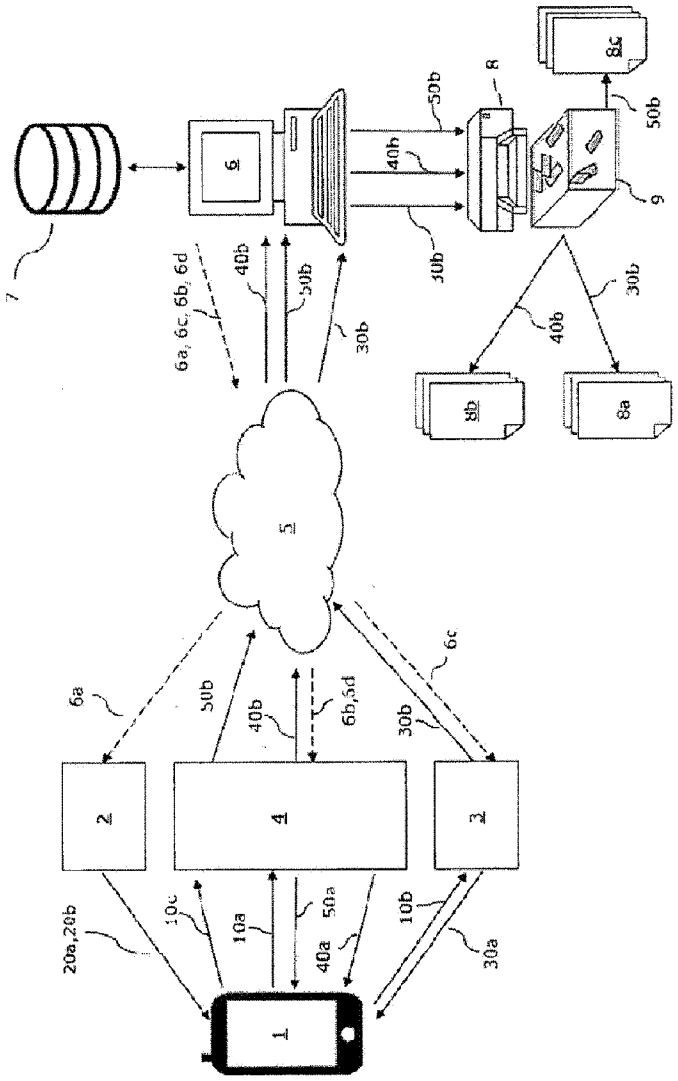
7
9
8c
8b
8a
8
5
6a, 6c, 6b, 6d
40b
50b
30b
6a
6c
6b,6d
2
4
3
1
20a,20b
10c
10a
50a
40a
10b
30a

FIG.2

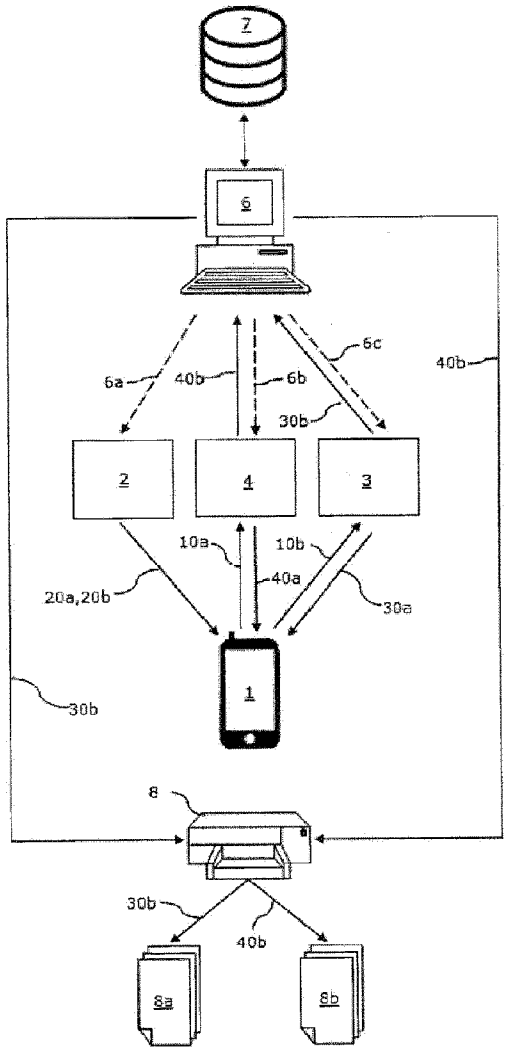
7
6
6a
40b
6b
6c
40b
30b
2
4
3
10a
10b
40a
20a,20b
30a
1
30b
8
30b
40b
8a
8b

FIG.3

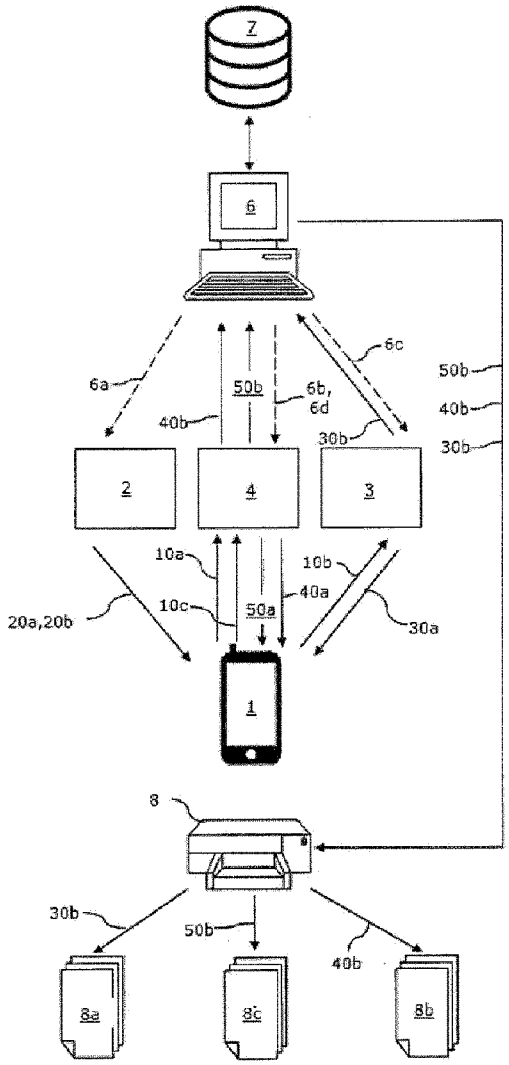
7
6
6a
50b
6b,
6d
6c
50b
40b
30b
40b
30b
2
4
3
10a
10b
40a
10c
50a
20a,20b
30a
1
8
30b
50b
40b
8a
8c
8b

FIG.4

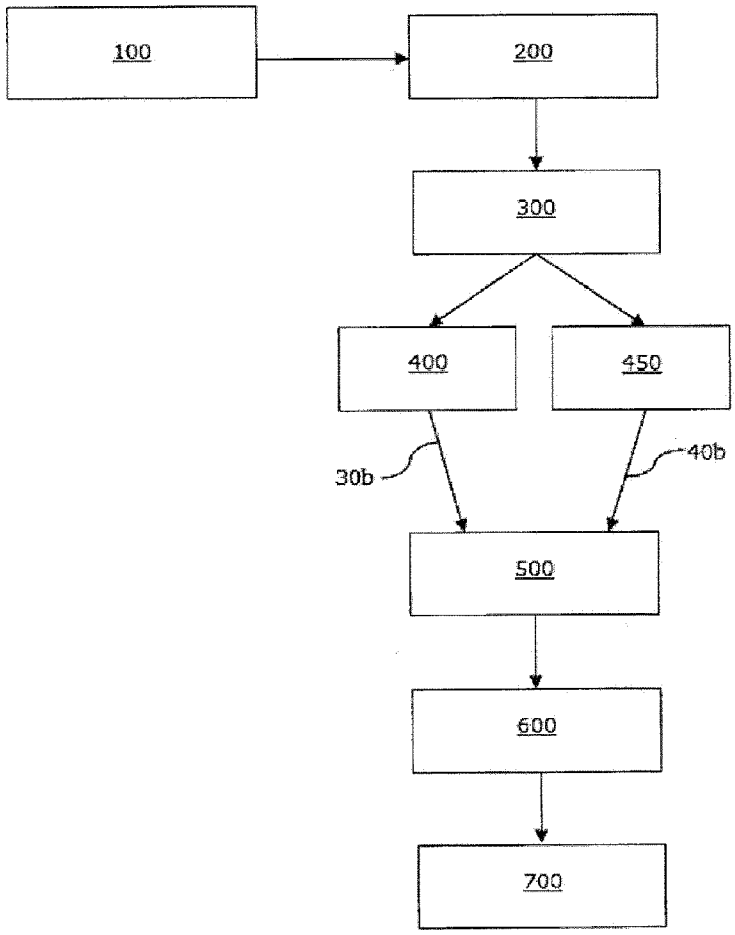

FIG.5

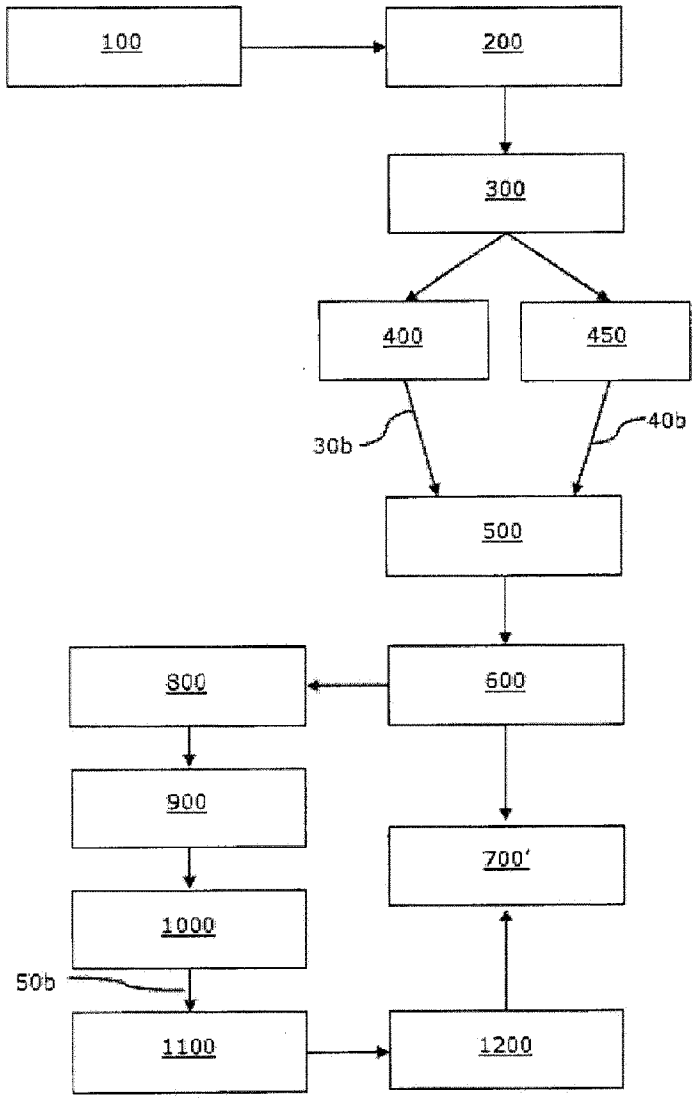
100
200
300
400
450
30b
40b
500
600
800
900
700'
1000
50b
1100
1200

FIG.6