

Algemeen Octrooi- en Merkenbureau

OCTROOIEN • MERKEN • MODELLEN
KWEKERSRECHTEN • LICENTIES



05.05121

Hoogheemraadschap van Rijnland
T.a.v. de heer Bouwman
Archimedesweg 1
2333 CM LEIDEN

Hoogheemraadschap van Rijnland

25 FEB. 2005 0505121

9 074

A	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10	11

DIV 1 2 3 4 5 6 7 8 9 10 11

Octrooigemachtigden

*Ir. J.M.G. Dohmen
Ir. C.G.C. Veldman
Ir. P. Dorna
Ir. A. Blokland
Ir. R. Valkonet
Dr. E.L.C. Piot*

Adviseurs

*Ir. J.J.H. Van kan
Ir. C.J. Vollebregt*

*Merken- en
modellengemachtigden*

*F.M. Verguld
Mr. S.X.F. Schuit
Mr. J. Meuwissen*

Kwekersrecht

Drs. R. Koronstra

Onze ref.: 210010/JD/vn

Eindhoven, 18 februari 2005

Betreft: Uw Internationale (PCT) octrooiaanvraag PCT/NL2004/000496 ten name van Hoogheemraadschap van Rijnland en P.G. MacLaine Pont "System and method for electronic voting".

Geachte heer Bouwman,

In uw bovengenoemde Internationale octrooiaanvraag ontvingen wij het nieuwheidsrapport met een eerste beoordeling van de octrooieerbaarheid van de aanvraag door een nieuwheidsonderzoeker van het Europees Octrooibureau. Een afschrift van het nieuwheidsrapport en de daarin genoemde documenten vindt u bijgesloten. Tevens ontvangt u een afschrift van de aanvraag zoals gepubliceerd onder het nummer WO 2005/000423 A1 en onze reactie aan de heer MacLaine Pont inzake de bezwaren van de nieuwheidsonderzoeker.

Tevens sluit ik onze nota bij voor de met het bestuderen en rapporteren van het nieuwheidsonderzoek gemoeide kosten, inclusief kopieer- en verzendkosten.

Met vriendelijke groeten,

Algemeen Octrooi- en Merkenbureau

J. Dohmen

- Bijlagen:
- afschrift aanvraag zoals gepubliceerd onder nummer WO 2005/000423 A1;
 - afschrift internationaal nieuwheidsrapport;
 - afschriften geciteerde documenten (4);
 - afschrift brief aan de heer MacLaine Pont;
 - nota.

Besloten Vennootschap Algemeen Octrooi- en Merkenbureau B.V.

*Eindhoven John F. Kennedylaan 2, 5612 AD Eindhoven, Postbus 645, 5600 AP Eindhoven, Telefoon 040-2433715, Fax 040-2434557,
mail@oomb.nl http://www.oomb.nl*

*Rijswijk Vraartlaan 4, 2288 GM Rijswijk, Telefoon 070-3906397, Fax 070-3950759, mail@oomb.nl
Sittard Poststraat 10-12, Postbus 5041, 6130 PA Sittard, Telefoon 046-4200420, Fax 046-4585456, mail@oomb.nl
Rabobank 18 82 48 005, F. van Lanschot Bankiers 22 69 09 948, Postbank 151052 Handelsregister Eindhoven 17074382.
Algemene Voorwaarden - bij de K.v.K. Eindhoven gedeponeerd onder nr. 4938 98 - worden op verzoek toegezonden*

Algemeen Octrooi- en Merkenbureau

OCTROOIEN • MERKEN • MODELLEN
KWEKERSRECHTEN • LICENTIES

De heer P.G. Maclaine Pont
Lynbaen 9
8563 AZ WIJCKEL (F)

Onze ref.: 210010/JD/vn

Eindhoven, 18 februari 2005

Betreft: Uw Internationale (PCT) octrooiaanvraag PCT/NL2004/000496 ten name van Hoogheemraadschap van Rijnland en P.G. Maclaine Pont "System and method for electronic voting".

Geachte heer Maclaine Pont,

In uw bovengenoemde Internationale octrooiaanvraag ontvingen wij het internationale nieuwheidsrapport, opgesteld door het Europees Octrooibureau. Een kopie van het nieuwheidsrapport en afschriften van de geciteerde documenten sluit ik bij. Tevens is bij het rapport een eerste missive gevoegd van de nieuwheidsonderzoeker, waarin hij zijn bevindingen ten aanzien van het belang van de diverse publicaties voor octrooiverlening uiteenzet. Een afschrift van dit rapport is ook bijgesloten. Tevens sluit ik een afschrift bij van de aanvraag zoals gepubliceerd onder het nummer WO 2005/004023 A1.

Het Internationale nieuwheidsrapport noemt een viertal publicaties, in het bijzonder de Europese octrooiaanvraag EP 1 291 826 van de Katholieke Universiteit Nijmegen, bij u bekend en in de octrooiaanvraag genoemd.

De andere geciteerde documenten zijn door de nieuwheidsonderzoeker in de categorie "A" gerangschikt, hetgeen betekent dat deze slechts van ondergeschikt belang voor het beoordelen van de uitvinding worden geacht.

De conclusies van uw Internationale octrooiaanvraag zijn gericht op het voorkomen van dubbel telling, zoals eerder reeds besproken. De nieuwheidsonderzoeker is dan ook van mening dat dit een nieuw onderwerp is, dat niet door de in het nieuwheidsrapport genoemde documenten wordt geopenbaard. Daarentegen is de nieuwheidsonderzoeker van mening dat de conclusies niet inventief zijn ten opzichte van het document van de

Besloten Vennootschap Algemeen Octrooi- en Merkenbureau B.V. 0505121

Eindhoven John F. Kennedylaan 2, 5612 AB Eindhoven. Postbus 645, 5600 AP Eindhoven. Telefoon 040-2433715. Fax 040-2434557.
mail@aomb.nl http://www.aomb.nl

Rijswijk Veraartlaan 4, 2288 GM Rijswijk. Telefoon 070-3906397. Fax 070-3950759. mail@aomb.nl
Sittard Poststraat 10-12. Postbus 5041, 6130 PA Sittard. Telefoon 046-4200420. Fax 046-4585456. mail@aomb.nl
Rabobank 18 82 48 005. F. van Lanschot Bankiers 22 69 09 948. Postbank 151052. Handelsregister Eindhoven 17074382.
Algemene Voorwaarden - bij de K.v.K. Eindhoven gedeponeerd onder nr. 4938/98 - worden op verzoek toegezonden

Algemeen Octrooi- en Merkenbureau

OCTROOIEN • MERKEN • MODELLEN
KWEKERSRECHTEN • LICENTIES

Universiteit van Nijmegen, ook aangegeven als referentie D1. Ik verwijs in het bijzonder naar paragraaf 3 van de bijgesloten missive.

De nieuwheidsonderzoeker geeft aan dat het probleem van de dubbel telling naar zijn mening geen technisch probleem is. Hierin verschillen wij van mening met de nieuwheidsonderzoeker omdat, zoals in de aanvraag aangegeven, het probleem van de dubbel telling kan worden veroorzaakt door fouten op het communicatiepad tussen de stemmer en de organisator van de verkiezing, hetgeen wel degelijk een technisch probleem is. Naar onze mening geeft de uitvinding hier een oplossing voor in de zin van het vermijden van deze dubbel telling, zoals ten principale in conclusie 1 is aangegeven.

De Examiner geeft verder aan dat naar zijn mening het slechts tellen van één stem ook bekend is uit de Internationale octrooiaanvraag WO 02/42974 (2) in het bijzonder pagina 7, regels 11-17. Hier wordt echter naar onze mening een inderdaad simpele maatregel genoemd om geen verdere stemmen toe te laten, zodra er één stem geregistreerd is. Hiermee kan een stemmer dan zijn keuze niet meer wijzigen, hetgeen volgens de oplossing van de uitvinding wel toelaatbaar is.

Graag zou ik uw reactie hierop hebben, in het bijzonder de nadelen die verbonden zijn met de in D2 genoemde manier voor het eenvoudigweg uitsluiten van verdere stemmen, gebaseerd op de unieke code voor elke stemmer.

Een ander punt dat de nieuwheidsonderzoeker aan de orde stelt en dat ik ook al kort telefonisch aan u heb doorgegeven, is aangegeven in paragraaf 2. van de missive.

Zoals beschreven op bladzijde 27, regel 4 van uw aanvraag onder f. is het noodzakelijk dat de stemmer de parameters ExtParGp, VPID en PW vanaf de stemkaart op het scherm invult.

Zoals aangegeven op bladzijde 35, regel 5 onder e. van uw aanvraag worden op de stemkaart de waarden VPID, PW en ELID leesbaar afgedrukt. De nieuwheidsonderzoeker vraagt zich nu af hoe de stemmer de waarde ExtParGp kan invoeren, wanneer deze niet aan hem of haar is medegedeeld.

Ik wijs erop dat de code ExtParGp (Extended Participation Group) oftewel de deelnamegroep, niet als zodanig in de oorspronkelijk ingediende octrooiaanvraag voor komt. Voor deelname aan de verkiezing lijkt derhalve

Algemeen Octrooi- en Merkenbureau

OCTROOIEN • MERKEN • MODELLEN
KWEKERSRECHTEN • LICENTIES

ExtParGp niet per se noodzakelijk en dus niet essentieel voor het uitvoeren van de uitvinding.

Wanneer wij geen wijze kunnen aangeven waarop de stemmer in het bezit kan komen van de parameter ExtParGp, gestuurd door de tekst zoals ingediend, stel ik voor om deze uit de aanvraag te schrappen. Graag uw reactie.

Verder maakt de nieuwheidsonderzoeker nog wat bezwaar tegen de gebruikte termen, maar dat kan gemakkelijk worden opgelost door ofwel het toevoegen van een lijst met afkortingen en definities, een soort concordantielijst, zoals reeds door u geproduceerd (RIES ABBREVIATIONS AND DEFINITIONS V1.2 4 april 2004) dan wel door in de conclusies de betreffende parameternamen te noemen.

De eerstvolgende stap in deze Internationale octrooiaanvraag is het eventueel aanvragen van een verdere beoordeling van de octrooieerbaarheid door het Europees Octrooibureau, hetgeen dan kan leiden tot een niet-bindend advies omtrent de octrooieerbaarheid. Deze stap is niet verplicht en wordt door ons alleen geadviseerd wanneer het nieuwheidsonderzoek en de bijbehorende missive positief zijn dan wel met eenvoudige wijzigingen tot een positief resultaat kunnen leiden. Of deze stap in uw octrooiaanvraag zinvol is, kunnen wij pas beantwoorden naar aanleiding van uw reactie. De termijn voor de eerstvolgende stap verloopt op **8 mei 2005**.

Uw reactie zien wij graag zo spoedig mogelijk van u tegemoet, bij voorkeur vóór 4 maart 2005, zodat wij eventueel ook nog wijzigingen in de Nederlandse octrooiaanvraag kunnen aanbrengen op basis van uw reactie op het nieuwheidsrapport en de bezwaren van de nieuwheidsonderzoeker in deze PCT-octrooiaanvraag.

Met vriendelijke groeten,
Algemeen Octrooi- en Merkenbureau

J. Dohmen

Bijlagen: - afschrift aanvraag zoals gepubliceerd onder nummer
WO 2005/0040023 A1;
- afschrift internationaal nieuwheidsrapport;
- afschrift in het nieuwheidsrapport genoemde documenten (4)

cc: Hoogheemraadschap van Rijnland, ter attentie van de heer
Bouwman

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 January 2005 (13.01.2005)

PCT

(10) International Publication Number
WO 2005/004023 A1

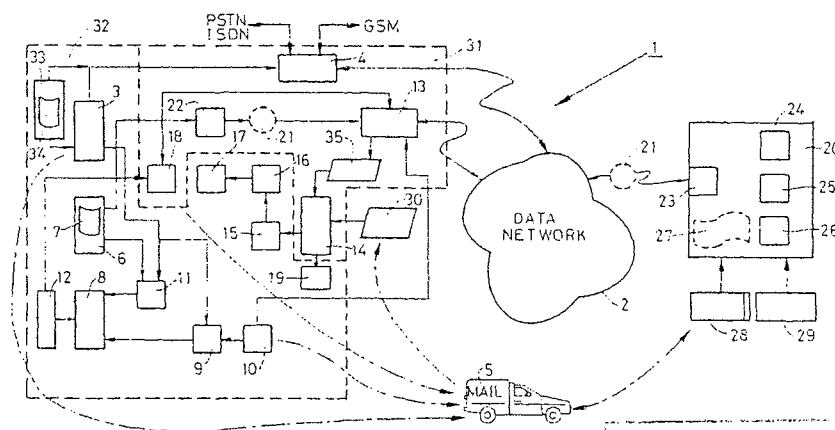
- (51) International Patent Classification⁷: G06F 17/60, G07C 13/00
- (21) International Application Number: PCT/NL2004/000496
- (22) International Filing Date: 8 July 2004 (08.07.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 1023861 8 July 2003 (08.07.2003) NL
- (71) Applicant (for all designated States except US): HOOGHEEMRAADSCHAP VAN RIJNLAND [NL/NL]; Archimedesweg 1, NL-2333 CM Leiden (NL).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): MACLAINE PONT, Pieter, Gerard [NL/NL]; Lynbaen 9, NL-8563 AZ Wijckel (NL).
- (74) Agents: DOHMEN, Johannes, Maria, Gerardus et al.; Algemeen Octrooi- en Merkenbureau, P.O. Box 645, NL-5600 AP Eindhoven (NL).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR ELECTRONIC VOTING



Hoogheemraadschap van Rijnland

bilans nr. 0505121

(57) Abstract: Electronic voting system (1) and method for collecting and counting votes from individual voters using electronic polling equipment (20). The system (1) comprises means (15) for validating votes from collected virtual ballot forms (27). The validating means (15) are arranged in such way that if a set of two or more virtual ballot forms (27) associated with an identical voter is collected, one virtual ballot form (27) of said set is validated as one valid vote of said voter. The remaining virtual ballot forms (27) of said set are marked as duplicate, provided said virtual ballot forms (27) of said set are identical as to the subject elected by said voter. Otherwise all virtual ballot forms (27) of said set are marked invalid. Thereby effectively preventing double counting of valid votes, among others, due to network problems causing a virtual ballot form (27) to be forwarded twice or even many more times.

WO 2005/004023 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Title

System and Method for Electronic Voting.

5

Field of the Invention

The present invention generally relates to electronic voting and, more particularly, to electronic voting in an election via a public data network such as the Internet.

10

Background of the Invention

In the context of the present invention, an election is to be construed as an election for a public or governmental body, an opinion poll, a referendum, a company election for an employees council or the like and any other type of election wherein persons may choose between two or more alternatives or options and communicate their choice as a vote to a vote collecting authority.

An important aspect is that the participation to the election is restricted to persons which have been registered beforehand as voters entitled to participate in the voting.

At present, an election for a public body, for example, requires that a person has to report himself at a polling station for filling in a ballot form or to vote electronically by pushing one or more buttons on a voting machine. For expats, that is voters who live abroad, for example, the votes may be forwarded by mail to a central polling station and will be counted together with the collected ballot forms and electronic votes in the total election result.

Although electronic voting machines have improved the speed of counting the votes, for example, they still require that the voters report themselves at a polling station for making their choices.

With the advent of modern electronic communication techniques, in particular the Internet, methods and systems have been developed by which voters can vote from their homes, using electronic communication equipment like Personal Computers (PC's), landline and mobile telephones, and the like.

European patent application EP 1 291 826 discloses an electronic voting system wherein the Internet is used as a communication medium between the remote home voters and the vote collecting authority. Several measures have been proposed and implemented to guarantee the correct identity of the voter, to avoid fraude and to reduce the risk of a virus or a malicious hacker to intercept and amended the electronic votes, for example.

In a paper "Electronic elections employing DES smartcards", by Robers, H., December 1998, IBM Student Chipcard Innovation Team, a location independent electronic voting system is disclosed, using chipcard technology.

In the context of the present invention, the term "electronic vote" has to be construed as a vote electronically communicated via an electronic voting system from a remote voter to a vote collecting authority.

For a successful implementation of electronic voting, the system should meet the requirements that can be expected for a formal government election system, for example, in which voting by mail is allowed as well. In addition, the technology used should be such, that more than 95% of the expected potential of users should be able to use the system on their regular Internet connected PC, without any changes or installation requirements to be performed by the users.

Such PC's can expected to be equipped with a regular Internet browser, like Microsoft's Internet Explorer®, with features like Java® and acceptance of cookies typically turned off. In addition, most of them will be connected to the Internet with either a dial-up or a slow

ADSL or cable connection. In addition, the system should behave for the user like a "normal" interactive Internet application, with "normal" response properties, since the use of the election system will be a "one-time shot" over longer periods such as months or years.

5 Given the relative low turnout, there is a high risk of losing the potential voter in case his Internet access to the election is behaving "funny" in his or hers observation. So the client environment will put a serious limitation on the actual possibilities at the client side for an electronic voting system.

10 Not only the client environment, but also the Internet itself and the intermediate providers may cause problems while a vote is being communicated to the vote collecting authority.

 As will be recognized by most of the users of email messages, for example, sometimes a message will not arrive at all and is
15 lost on the Internet, and sometimes a single message will be delivered twice or many more times due to an erroneous behavior of the communication equipment involved from the voter up to the vote collecting authority.

 The electronic voting system as disclosed by European
20 patent application EP 1 291 826 and Robers, H., amongst others, has no provisions how to deal with electronic votes from the same remote voter that arrive at the vote collecting authority twice or even repeatedly.

 Other shortcomings of the cited prior art comprise:

25 - no vote and result validation of the final election results, both for each voter and other parties to an election;

 - difficult to combine with other voting manners (mail, electronically, GSM, SMS, etc. to one result with manageable priority;

30 - no facilities to provide for an alternative election package for voters who claim not to have received the original one, for example, which package contains the initial secrets, required by each voter to take part in the elections, and

- no capability to implement an election scheme in such a way that each voters secret remains in his/hers possession or at least in his polling equipment, without any other requirement then the use of a regular internet browser on that PC.

5 Further, systems entirely based on intelligent chip card (or smart card), such as described by Robers, H., require that the user must have a chip card interface device attached to his/hers PC. This is a major cost factor, in particular for election on a large scale, many entitled voters, such as a governmental election. Practically, such
10 voting systems are only feasible for a minor group of (specialized) voters. Further, on each smart card the organizer of the elections needs to pose a secret cryptographic key-distribution key. Although feasible in practice, this too adds significantly to the costs and complexity of the system.

15

Summary of the Invention

In the light of the above disclosed conditions, it is an object of the present to provide an improved electronic voting system, by
20 which remote users can electronically communicate their votes to a vote collecting authority, and meeting as much as possible all major theoretical requirements that can be defined in view of a well controllable democratic election system.

In practice, there will be a trade off between requirements
25 which will be met by a proper design and implementation of the electronic voting system, and requirements which can be met through organizational measures. However, the electronic voting system according to the invention should be expected to be designed and applied in such a way that an optimum between system functions and organizational measures is
30 obtained at reasonable costs.

The following goals should at least be met, either by the

electronic voting system itself, or by a combination with other, organizational, measures:

- only eligible persons can vote;
- no person can vote more than once;
- 5 - the vote is secret;
- each (correctly cast) vote gets counted, and
- the voters trust that their vote is counted.

Based on the location independent electronic voting system described in the above-mentioned paper by Robers, H., these objects and others are achieved, in accordance with a first aspect of the present invention, by an electronic voting system for collecting and counting votes from individual voters using electronic polling equipment in an election comprising a list of subjects to be elected, from which list one subject is to be elected by an individual voter, wherein the votes being

10 forwarded by means of a data network, and the voting system comprises:

15

- means for generating a unique personal key for each individual voter entitled to the election, which unique personal key is to be communicated to the individual voter;
- means for generating a unique subject code for each
- 20 subject on the list of subjects to be elected in the election;
- means for generating a reference election record for each individual voter comprising all potential virtual ballot forms for the individual voter, wherein a unique voter identity code for the individual voter is calculated from a unique code for the election and the unique
- 25 personal key of the voter, wherein a unique subject identity code for each subject on the list of subjects to be elected by the voter in the election is calculated from the unique subject codes and the unique personal key of the voter, and wherein the calculated identity codes form part of the virtual ballot forms;
- 30 - means for storing the reference election records for the individual voters;

- means for loading a tool in the polling equipment of the individual voter wherein the tool comprises means for calculating the unique voter identity code of the voter from the election code and the unique personal key communicated to the voter, for calculating the unique
5 subject identity code of the subject elected by the voter from the unique subject code of the subject elected by the voter and the unique personal key of the voter and for generating the virtual ballot form comprising the calculated identity codes by using the polling equipment;

10 - means for forwarding the virtual ballot form by the polling equipment over the data network;

- means for receiving and collecting the virtual ballot form forwarded by the polling equipment;

15 - means for verifying each collected virtual ballot form with respect to its presence in the reference election records of the voters;

- means for counting votes, and

20 - means for establishing an election result, characterized by means for validating votes from the collected virtual ballot forms, which validating means are arranged in such way that if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of the set is validated as one valid vote of the voter and the remaining virtual ballot forms of the set are marked as duplicate, provided the virtual ballot forms of the set are identical as to the subject elected by the voter, otherwise all virtual
25 ballot forms of the set are marked invalid.

In the context of the present invention, the term "virtual ballot form" is to be construed as an electronic or "soft" ballot form, contrary to a paper or "hard" ballot form, for example.

30 To avoid double counting of votes, in accordance with the present invention, a set of virtual ballot forms collected by the means for receiving and collecting are validated in a such a manner that if

multiple virtual ballot forms are received from the same voter, these ballot forms will be counted as a single valid vote, provided the received virtual ballot forms are identical. Otherwise, all received virtual ballot forms of the set are marked invalid and no valid vote will
5 be counted for this voter.

The election system according to the invention is now capable to deal with communication irregularities causing two or more identical votes from the same votes being collected, for example, such that no person can vote twice. That is, can provide multiple electronic
10 votes that are all validly counted.

As will be appreciated by those skilled in the art, with the election system according to the invention, by generating a personal key for each voter, by calculating a unique voter identity code for the individual voter from a unique code for the election and the unique
15 personal key of the voter, by generating unique subject codes for each subject taking part in the election and by calculating unique subject identity codes of the subjects to be elected by a particular voter from his/hers personal key and the subject identity codes, which identity codes form part of the virtual ballot form, a very secure and safe voting
20 system is provided.

Security is particularly strengthened by when using cryptographic algorithms and encryption techniques such as, but not limited to, symmetric cryptographic algorithms, like the Data Encryption Standard (DES), triple DES, or the Advanced Encryption Standard (AES),
25 using Message Authentication Codes (MACs) and Modification Detection Codes (MDCs), also called hashing codes.

The reference election record provides a first check whether collected virtual ballot forms are indeed a possible vote for a respective voter, whereas the means for validating the votes in
30 accordance with the invention effectively prevent double voting of virtual ballot forms which are within the reference election record of

that particular voter.

Accordingly, the electronic voting system according to the invention can be safely used even with distorted public network facilities, while meeting the requirements of preventing double counting
5 of the same or different votes of a voter.

In a further embodiment of the invention, the electronic voting system is arranged for collecting and counting votes in an election wherein one combination of subjects is to be elected by an individual voter, comprising validating means, arranged in such way that
10 if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of the set is validated as one vote of the voter and the remaining virtual ballot forms of the set are marked as duplicate, provided the virtual ballot forms of the set are identical as to the one combination of subjects elected by
15 the voter, otherwise all virtual ballot forms of the set are marked invalid.

In accordance with further embodiments of the invention, the validating means may form part of the means for verifying the collected virtual ballot forms or may form part of the means for counting
20 the votes. This, reducing the number of means actually involved in the election and thereby reducing the risk of malicious attacks on multiple parts of the system, for example.

To inform the voter of the receipt of his or hers vote, in a yet further embodiment of the invention, the voting system comprises
25 confirmation means for generating a receipt indicating that a virtual ballot form has been received from the polling equipment of the voter and means for delivering the receipt comprising a unique receipt confirmation value in readable form at the polling equipment of the voter.

A very important aspect of electronic voting or election
30 systems for use in public elections, for example, is the possibility that voters have an opportunity to inspect whether they have been correctly

registered and which votes they can make. This is achieved, in yet another embodiment of the invention, by comprising means for publishing the list of voters entitled to the election, the list of subjects to be elected in the election and the reference election records for the individual voters, enabling public inspection before the date of the election, and by entry means for each individual voter using the unique personal key for inspection of the reference election record for the individual voter.

It will be appreciated that voters also have to be provided with an opportunity to inspect, once they have voted, whether their votes are correctly counted. To this end, in a further embodiment of the invention, the voting system comprises means for publishing the election-result comprising the record of the valid votes as awarded for the collected virtual ballot forms after they have been submitted for verification and validation, enabling public inspection, and entry means for each individual voter using the unique personal key for inspection of the account of the virtual ballot form forwarded by the polling equipment of the individual voter.

In another embodiment of the invention, the system further comprises means for generating and storing a reference service identity code for each individual voter entitled to the election, which reference service identity code is calculated from a fixed part of the unique personal key of the voter and information related to the election and means for keeping a status record of the voter at the means for receiving and collecting the virtual ballot forms, wherein the status record is associated with the reference service identity code of the voter.

In a preferred embodiment of the invention, the tool to be loaded in the polling equipment of the voter is arranged for calculating a service identity code from the fixed part of the unique personal key of the voter and the information related to the election and for forwarding the service identity code to the means for receiving and collecting the

virtual ballot forms.

The status record provides a possibility to track whether a voter has already taken part in the vote, whether the voter has or has not completed the voting, etc. by comparing the stored reference service
5 identity code and the calculated service identity code, all this without revealing the voter's identity.

The personal keys have to be communicated to the voters. In accordance with a yet further embodiment of the invention, communication means for communicating the unique personal key to each individual voter
10 entitled to the election are provided, the communication means comprises at least one of a group including means for electronically storing the unique personal key in a chip card of the voter, data communication means for communicating the unique personal key to the voter by a data network such as the Internet or a fixed and/or mobile data communication network
15 including a Short Message Service, and means for providing the unique personal key in a human and/or machine readable form on a hard copy, such as a text message on paper, for communicating by mail to the voter.

In order to enter the personal key, in another embodiment of the invention, the polling equipment is arranged for operatively
20 connecting same to data input means comprising at least one of a group including a chip card reader, a keyboard, a mouse, a screen, a bar code reader and voice conversion means.

An important advantage of this embodiment according to the invention is that the electronic voting system can be combined with an
25 existing ordinary mail or postal election system. All eligible voters may receive both the capability to vote by mail or to vote electronically, by forwarding an election package by mail. In this election package they will find a postal ballot-form and an Internet Voting Card. The voter will have the free choice to select the best option for himself without
30 any prior registration.

Accordingly, the design of the electronic voting system of

the invention has to reflect the combination of Internet and mail voting and should be capable of coping with all kind of potential discrepancies, created by the combination of these two systems, e.g. voters who take part using both channels, i.e. the mail and the Internet, etc. In
5 addition, the individual voter should have the possibility to validate that also his mail vote is reflected in the final outcome.

In another embodiment of the electronic voting system according to the invention, the means for receiving and collecting virtual ballot forms are arranged for receiving and collecting virtual
10 ballot forms other than forwarded by polling equipment of a voter, such as physical ballot forms received by mail, and comprising reading and conversion means for converting the physical ballot forms into virtual ballot forms.

To avoid double voting, i.e. double counting of votes of
15 the same voter, the means for verification and validating are arranged in such way that if a set of two or more virtual ballot forms associated with an identical voter identity code is collected and the virtual ballot forms are collected from means of different kinds that have been appointed different values of priority, only the virtual ballot forms
20 collected from the means of the kind with the higher value of priority are submitted for verification and validation.

That is, the invention provides the possibility of allocating a processing priority to virtual ballot forms received via different channels. That is, for example, directly via the Internet, for
25 example, or indirectly via the mail and scanning and conversion of the physical ballot forms.

In a yet further embodiment of the invention, the means for verification and validation are arranged in such way that physical ballot forms received by mail and which are converted into virtual ballot forms,
30 are appointed the lower value of priority.

Thus, virtual ballot forms directly received via the

Internet, for example, will be calculated as the eventually valid vote, in case the voter has used both the mail and the data network opportunity to vote.

It will be appreciated that the system according to the invention supports voting, by different means either electronically and by mail. However, by using the validating means according to the invention, always a single vote will be counted. Also in the case of voting by different electronic means. Note that the election is to be performed in a set time window. Votes received outside the time window will be invalid, of course.

As already disclosed above, to enhance the security of the system, the means for generating a unique subject identity code for each subject to be elected in the election, the means for generating a unique voter identity code and the means for generating a reference election record for each individual voter entitled to the election preferably comprise cryptographic generator and calculator means.

Likewise, the means for generating a unique subject combination identity code for each combination of subjects to be elected in the election, the means for generating a unique voter identity code and the means for generating a reference election record for each individual voter entitled to the election preferably comprise cryptographic generator and calculator means.

The cryptographic generator and calculator means are preferably arranged for symmetric encryption, such as DES, triple DES and AES, for example.

In a practical embodiment of the electronic voting system according to the invention, the means for presenting the list of subjects from which one subject or one combination of subjects is to be elected by the voter at the polling equipment, the means for loading the tool in the polling equipment of a voter, the means for receiving and collecting the virtual ballot form forwarded by the polling equipment and the

confirmation means are supported by computer equipment comprising at least one computer server.

In a preferred embodiment of the invention, in order to enhance safety and security, to prevent fraud as much as possible, the or each of the means for loading the tool in the polling equipment of a voter, the means for receiving and collecting the virtual ballot form forwarded by the polling equipment, the confirmation means and the polling equipment are arranged for providing secure data transmission over the data network.

The invention further provides that the means for generating a unique personal key for each individual voter, the means for generating the unique voter identity code for each individual voter, the means for generating the unique identity code for each subject or combination of subjects to be elected in the election, the means for generating the reference election record for each individual voter entitled to the election, the means for verifying the collected virtual ballot form of the individual voter with respect to its presence in the reference election record of the voter, the means for counting votes of the voters, the means for validating votes from the collected virtual ballot forms and the means for establishing an election-result based on the counted votes are supported by computer equipment arranged to be operated under the supervision of an election authority.

This provides as much as possible control and inspection, to ensure anonymity of the user and to avoid tampering with the election results.

The polling equipment comprises at least one of a group including a personal computer and fixed or mobile data communication equipment arranged for providing access to the data network, such as the Internet.

In a second aspect, the inventions provides a method for electronic voting, for collecting and counting votes from individual

voters using electronic polling equipment in an election comprising a list of subjects to be elected, from which list one subject is to be elected by an individual voter, the votes being forwarded by means of a data network, the method comprising the steps of:

- 5 - generating a unique personal key for each individual voter entitled to the election;
- communicating the unique personal keys to the individual voters;
- generating a unique subject code for each subject on the
- 10 list of subjects to be elected in the election;
- generating a reference election record for each individual voter comprising all potential virtual ballot forms for the individual voter, wherein a unique voter identity code is calculated for the individual voter from a unique code for the election and the unique
- 15 personal key of the voter, a unique subject identity code for each subject on the list of subjects to be elected by the voter in the election is calculated from the unique subject codes and the unique personal key of the voter, the calculated identity codes forming part of the virtual ballot forms;
- 20 - storing the reference election records for the individual voters;
- loading a tool in the polling equipment of a voter;
- electing one subject from the list at the polling equipment of the individual voter, by inputting the unique personal key
- 25 communicated to the voter and the unique subject code for the one elected subject into the polling equipment;
- generating a virtual ballot form using the tool loaded into the polling equipment of the voter, wherein a unique voter identity code is calculated from the election code and the unique personal key of
- 30 the voter, wherein a unique subject identity code is calculated from the unique subject code for the one subject elected by the voter from the

unique subject code of the one subject elected and the unique personal key of the voter and wherein the calculated identity codes form part of the virtual ballot form;

- forwarding the virtual ballot form over the data network;
- 5 - receiving and collecting the virtual ballot form forwarded by the polling equipment;
- verifying each collected virtual ballot form with respect to its presence in the reference election records of the voters;
- counting votes, and
- 10 - establishing an election-result based on the counted votes, characterized by a step for validating votes from the collected virtual ballot forms in such way that, if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of the set is validated as one single
- 15 valid vote of the voter and the remaining virtual ballot forms of the set are marked as duplicate, provided that the virtual ballot forms of the set are identical as to the one subject elected by the voter, otherwise the virtual ballot forms of the set are marked invalid.

In the case of collecting and counting votes from

20 individual voters using electronic polling equipment in an election comprising a list of subjects to be elected, from which list one combination of subjects is to be elected by an individual voter, in accordance with an embodiment of the method according to the invention, the step for validating votes from the collected virtual ballot forms is

25 arranged such that if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of the set is validated as one valid vote of the voter and the remaining virtual ballot forms of the set are marked duplicate, provided that the virtual ballot forms of the set are

30 identical as to the one combination of subjects elected by the voter, otherwise all virtual ballot forms of the set are marked invalid.

The method according to the invention, in various embodiments thereof, further provides delivery of a receipt after voting, publication of a list of voters entitled to the election, publication of the election result for checking by a voter whether his or hers vote has
5 been properly counted in the result, providing a reference service identity and a service identity for checking the status of the voting process of a user, voting by mail and/or electronically, priority vote counting and cryptographic algorithms and codes, election under supervision of an election or vote counting authority, the use of modern
10 communication means like SMS, Internet, mobile and fixed telephone facilities, as well as providing hard copies of ballot forms to the registered voters. In the case of a hard copy of the ballot form, the hard copy is suitable to be cast as a physical ballot form comprising the subjects or the combinations of subjects to be elected by the voter. Such
15 as disclosed above in relation to the electronic voting equipment.

In the case of communicating the personal key to the voters by mail, using the above-mentioned election package comprising a postal ballot-form and an Internet Voting Card, replacement election packages should be offered to complaining eligible voters, who claim to have not
20 received their package.

In such a case, in accordance with an embodiment of the method according to the invention, a reserve-list of a limited number of unique reserve keys is generated and the reference election record is generated to comprise virtual ballot forms for the number of unique
25 reserve keys, and wherein a reserve key of the reserve-list is issued to a voter who applies for a fresh unique key replacing the unique personal key initially appointed to the voter, wherein the reserve key is appointed to the voter after the initially appointed unique personal key and the corresponding reference election record is withdrawn, and wherein
30 the issue of the reserve key from and the withdrawal of the initially appointed unique personal key are taken into account for the verification

of the validity of collected virtual ballot forms. Original voting capabilities are marked as invalid.

The replacement procedure should allow for the translation of voters real identity into the proper impersonal reference identity of that voter, in such a way, that the voter's election identity will remain secret. Proper publication of the activities around the replaced packages is required.

It will be appreciated that the replacement process is likewise applicable if the unique voter identity is not delivered by mail, i.e. as an election package, but by SMS, email, or otherwise.

The invention further provides that the tool is loaded automatically into the polling equipment from the data network. In an embodiment of the invention, wherein the data network comprises the Internet and the polling equipment comprises a personal computer operatively connected to the Internet, the tool is loaded into the personal computer by means of a Java applet included in a web-page to be selected by a voter for participating in the election.

Actually, the tool may be loaded in parts to avoid annoyance of the voters in the case of slow internet connections, for example. The parts may be divided such that, while a second part is downloaded, the voter is requested to respond to an already loaded first part, for example by inputting his personal key in two or more parts. In practice, the Java applet will be as small as a few kbytes.

In accordance with another embodiment of the method of the invention, the tool is loaded in a SIM-card of a GSM communication equipment, for example, for participating in the election by a voter using this communication equipment.

In a third aspect, the invention relates to a computer program product, comprising program code means stored on a computer readable medium, for performing the or part of the steps according to the invention as disclosed above, if loaded into an internal working memory

of a computer and operated by the computer.

In accordance with the invention, the computer program product may be arranged as a tool for loading into a computer program running on a computer controlled polling equipment for performing the steps of the invention as disclosed above, if loaded into an internal working memory of a computer and operated by the computer.

The invention will now be disclosed in more detail, in a non-limiting manner, using a schematic drawing of the electronic voting system as whole.

10

Brief Description of the Drawing

The figure shows, in a general and schematic manner, an embodiment of an electronic voting system according to the invention.

15

Detailed Description of the Invention

In the figure, reference numeral 1 indicates, as a whole, in a general and schematic manner, an electronic voting system for collecting and counting votes from individual voters, in accordance with the present invention. The equipment operated and controlled by a vote collecting authority or a polling office or a polling committee or the like, and the polling equipment of the voters connect, in the embodiment shown, via a data network 2, such as the Internet.

25

Reference numeral 3 designates means for generating a unique personal key for each individual voter entitled to the election. Such voters are defined in means 33, the eligible voters file, which relate to means 34, the eligible voters list. This personal key is to be communicated in protected form to the individual voter. To this end, the personal key generator means 3 connect to communication means 4, for communicating the personal key in protected form via the data network 2,

30

via a mobile radio network, such as GSM-network, via a landline telephone network, such as the PSTN (Public Switched Telephone Network) or the ISDN (Integrated Services Digital Network) or any other means, including mail
5 for communicating the personal key by a mail package to the individual
5 voter. Therefore, the means 33 connect to the communication means 4 as well.

Reference numeral 6 denotes means for generating a unique subject code for each subject on a list of subjects to be elected in the election. Subjects in accordance with the present invention, may be
10 persons, such as for an election of a public body, but can be also opinions to be elected in an opinion pole and the like. The list of subjects is schematically indicated with reference numeral 7.

For generating a reference election record, means 8 are provided which cooperate which means 9, for generating a unique voter
15 identity code for the individual voter, calculated from a unique election code, schematically indicated by reference numeral 10, and the unique personal key of the voter as generated by the means 3 for generating the personal key. Further, the means for generating the reference election record 8 cooperate with means 11 for generating a unique subject identity
20 code for each subject on the list of subjects 7 to be elected by the voter. The means 11 connect to the means 6 for generating the subject codes and the means 3 for generating the personal key of a voter.

The means 8 connect to memory means 12 for storing the reference value of all potential virtual ballot forms for each individual
25 voter, which reference values are associated with the identity codes generated by the means and 9 and 11.

In accordance with the present invention, each user which would like to avail himself of the possibility of electronic voting, has to use a polling equipment 20, such as the personal computer (PC) of a
30 voter. However, it will be appreciated that other electronic equipment by which a voter is able to communicate via the data network 2 and which

provides means 29 for inputting data, such as a keyboard or any other means for making a vote, such as a touch screen or pointing device, can be used with the present invention.

In order to take part in the election, a tool 21 has to be loaded in the polling equipment 20 of the individual voter, such as schematically indicated by broken lines 21. The tool 21 is to be communicated from the vote collecting authority via the data network 2 to the polling equipment 20. To this end, the vote collecting authority is provided with means 22 for forwarding the tool 21 to the polling equipment 20. The means 22 could, for example, be a tool to make both the tool 21 and the list of subjects 7 of the subject codes generator means 6 as a part of, for example, Web-server means 13, i.e. the ballot-box server. The polling equipment 20 is provided with means 23 for receiving and downloading the tool 21 into the polling equipment 20. The tool 21 can be communicated, for example, using known Web browser software and could, for example, be a script, running in the Web browser.

The tool 21, which is in fact a software program of a few kbytes, will be loaded into the polling equipment 20, before the voter enters any secret or personal information, like or his/hers choice for a subject in the election. The personal key may be loaded into several parts, in order to facilitate the downloading of the tool 21. It will be appreciated that the tool 21 may be loaded directly into the polling equipment 20, in the case of data network connections with are sufficiently fast. The tool must guarantee that the voters personal key will only be entered in the polling station itself and never be transmitted out of that, for instance never transmitted to the polling server. The tool will only transmit the virtual ballot and status identity information to the polling server.

With the tool 21 loaded into the polling equipment of the voter, means 24 are established in the polling equipment 20 for calculating the unique voter identity code of the voter, from the unique

personal key communicated to the voter and the election code 10, which can be communicated to the voter by mail 5, for example, or electronically via the communication means 4, or be incorporated in the tool 21.

5 The voter is now able to elect a subject or a combination of subjects, which are presented on the polling equipment 20 by the vote collecting authority, to which end Website means or a ballot-box server 13 may be installed at the voter collecting authority or another body which is responsible for the election. The means 13 are arranged for
10 presenting a subject to be elected by a voter and - if desired - as well as the transfer of the tool 21. It will be appreciated that the means 13 may be coupled or integrated in the means 8 for generating the reference election.

 The means 25 incorporated with the polling equipment 20 by
15 the tool 21, now calculate a unique subject identity code of the subject elected by the voter and the unique personal key of the voter and a virtual ballot form is generated comprising the calculated identity codes. To this end, the tool 21 may incorporate means 25 and 26 into the polling equipment or the means 24 or 25 may be arranged for calculating
20 the virtual ballot form. In the figure, the virtual ballot form is indicated by reference numeral 27 for illustration purposes. Note that the virtual ballot form 27 exists electronically.

 The polling equipment 20 further is arranged for communicating the virtual ballot form 27 over the data network 2 to the
25 vote collecting authority. To this end, the means 23 may be used by which the tool 21 is loaded into the polling equipment or separate means. The vote collecting authority is provided with means 14 for receiving a virtual ballot form, or the means 13 have the capability to receive the virtual ballot form 27 and to store the virtual ballot form 27 in means
30 35, a "received virtual ballot forms" file

 The means 14 could connect to means 15 if so desired, for

verifying each collected virtual ballot form with respect to its presence in the reference election record of the voters stored in the storage means 12. To this end, the means 15 may communicate with the means 8 and/or can be integrated into each other.

5 In accordance with the present invention, means 16 are provided, which connect to the verification means 15, for validating collected virtual ballot forms. The validating means 16 are arranged in such a way that, if a set of two or more virtual ballot forms 27 associated with an identical voter identity code is collected, only one
10 virtual ballot form 27 of the set is validated as one valid vote of the voter and the remaining virtual ballot forms 27 of the set are marked as duplicate, provided that the virtual ballot forms of the set are identical as to the subject elected by the voter. Otherwise, all virtual ballot forms 27 of the set are marked invalid.

15 A set of ballot forms 27 can be collected by the means 14 due to data network problems, for example resulting therein that the virtual ballot form 27 of a voter is delivered twice or many more times at the votes collecting means 14.

20 The validating means 16 connect to means 17 for counting valid votes and for publishing the election result.

25 For confirmation of the receipt of a received vote, means 18 are provided, connecting to the means 17 for counting a valid vote. The means 18 may be arranged to communicate directly via data network 2 to the polling equipment 20 of the user or may use, for example the server means 13 to this end. The receipt confirmation may be also
delivered by mail 5 to the voter. In the figure, mail transport is schematically indicated by dot-dashed lines.

30 For safety purposes, the list 7 can be arranged for publishing of the voters entitled to the election and for publishing the election result comprising the record of the valid votes as awarded for the collected virtual ballot forms 27. Of course, separate means may be

used for this purpose.

The system 1 comprises also scanning and conversion means 30, for scanning and converting hard ballot forms, received by mail. The means 30 connect to the means 14

5 At the polling equipment 20, means 28 may be provided, for entering the personal key by other means than by keyboard, for example using a smart card reader, a credit card reader, or the like.

For control and safety purposes, means 19 may be provided, in a further embodiment of the invention, for generating and storing a reference service identity code for each individual voter entitled to the
10 election. These means 19 are further arranged for keeping a status record of the voter, and connect to the means 14 for receiving the virtual ballot forms. It will be appreciated that the means 19 may comprise two or more separate means for this purpose.

15 In the figure, a single polling equipment 20 is shown. One skilled in the art will appreciate that a plurality of voters using his or hers polling equipment can be connected to the data network 2 for taking part in the election.

Further, it will be appreciated that several of the means
20 used by the vote collecting authority can be combined into a single processing means, for example, such as a single computer server.

For example, the means 13, 35, 14, 18, 22 could be arranged into a single computer server 31. Further, the means 3, 6, 8, 9, 10, 11, 12, 15, 16, 17, 19, 33, 34 may be arranged in a further computer server
25 or computer equipment 32, such as schematically indicated by broken lines.

Further, the word "means" as used in the present specification may be construed as one or both hardware and software means, such as, but not limited to, a computer program product to be
30 loaded into a working memory of a computer or polling equipment.

Those skilled in the art will appreciate that other

groupings or more than two servers can be used, without departing from the invention. The invention is not limited to the means shown, nor to their internal/external connections and functions.

5 The method according to the invention, in a preferred embodiment thereof, wherein the personal voter keys are forwarded by ordinary mail and wherein mail and electronic voting via the Internet are allowed, using DES cryptographic techniques, also called DES Virtual Ballot System (DVBS) comprises the following steps.

Initialize Voter Secrets (Initial preparation).

10 The Central Election Committee defines or establishes the following items:

1. Public operations:

a. EIID (Election Identity) name or election code for these elections.

15 b. Voters registry (that contains all eligible Voters V_1 ... V_n) with their public identities V_nID and per voter the proper value of ParGp (Participation Group), if applicable.

c. List of candidates C_1 ... C_m for this election.

2. Secret operations:

20 a. Generate per voter a personal key K_p (Personal Voter Key) comprising, for example, two parts:

$$K_p = DESe (K_{genvoterkey}, \{V_nID // ParGp // EIID\})$$
, wherein DESe means DES encryption and $K_{genvoterkey}$ is a Triple DES (3DES) 16 byte encrypted key generated by a vote key generator.

25 b. Calculate per voter: VPID, a voters secret voting code, and PW, a password, where both values are 34AN translations of both halves of K_p . (34AN is an AlfaNumeric 34 coding).

30 c. Checking on double VPID values and allocating VPID sequence numbers in a ParGp field of each voter, transforming that to an ExtParGp field (Extended Participation Group).

d. Calculating the proper, cumulative check digits/-

characters for the ExtParGp, VPID and PW fields and adding these values to those fields.

5 e. Production of Postal Ballot-forms and Voting Cards, in a closed envelope, addressed on the outside to the proper voter Vn; on the Postal Ballot-forms VPID, PW and EIID have been coded in machine-readable form, on the Voting Cards these values are printed in good, readable format.

f. Calculation of RnPotVote (Reference Virtual Ballot Form) for each Vn, existing of two parts:

10 i. Per voter one RnPID = MDC [DESmac (Kp, f(EIID))], a Reference Pseudo Identity for Voter n (reference security identity code), wherein DESmac is an MAC (Message Authentication Code) calculated with DES and MDC stands for Modification Detection Code.

15 ii. Per voter for each possible vote for candidate Cm in this election RnCM = MDC [DESmac (Kp, f(Cm,EIID))], wherein RnCM is a Reference Candidatechoice m by voter .

g. Calculation of ReSPID (Reference Service Identity Code) per voter (ReSPID = MDC[DESmac{Kp, (EIID//ExtParGp)}]) and creation of an (empty) status-tracking file with ReSPID as key.

20 h. Generation and production of similar materials for Replacement Election Packages (RepElPac), with the following properties.

i. All with a special series of VnID's, referred to as VrID (a VnID out of a special series for RepElPac's).

25 ii. With the related VrID printed on the outside of the closed envelope.

iii. With a file or list of all VrID's of the produced RepElPac's (RepElPac Stock File).

iv. To be stored in a specially managed storage.

30 v. All related RnPotVote (Reference Potential Voter for Voter n) records are marked "not_issued".

i. Total deletion and removal of all voter-related secret

information, other than the closed envelope with the ballot forms.

3. Publication of the RnPotVote file, signed with the public key. This public key and its related root-certificate to validate it should be such that the validation will be done automatically in the
5 client of the voter, without additional public key installation activities. An acceptable alternative will be to just hash the file with SHA-1 and to publish the proper hash through an out-of-band channel.

4. Mailing of all closed envelopes with the ballot-forms to all voters.

10 5. Proper start of one or more ballot-box and ballot-box-status servers and the reception point for postal ballots.

Vote Collecting (submitting votes by voters)

As soon as the voter receives his closed envelope with the ballot-forms, he is or could be involved in the following actions:

15 1. He or she validates that the envelope is undamaged and unopened (if that is not the case he or she files for the Replacement Election Packages procedure).

2. He or she decides to vote by mail or by Internet (or not to vote at all).

20 3. In case of a postal vote, he or she marks the proper candidate on the postal ballot, puts the ballot in the supplied response-envelope and mails that envelope.

4. In case of an Internet vote he or she is engaged in following events:

25 a. Selects his Voting Card.

b. Starts a PC, connected to the Internet and an Internet browser.

c. Surfs to the proper Internet site (URL) for this election.

30 d. Observes the proper start of SSL (Reference Security Identity Code) and the proper authentication of the ballot-box server.

e. Receives through his browser automatically the first election page, containing a tool in JavaScript coding to operate the system.

5 f. Enters his ExtParGp, VPID and PW from his Voting Card in the proper fields of the first screen. The proper values are validated with the check digits/characters.

g. The JavaScript of the system calculates the ReSPID (Reference Service Identity Code) value for this voter and sends that to the ballot-box-status server; that server responds with a status record
10 for this voter: either "votes received for one or more election-categories" or "open to vote".

h. The ExtParGp field, in conjunction with the status information, now defines the proper sequence for his voting: one or more screens with candidates are presented to the voter.

15 i. In every screen the voter marks his choice.

j. When all choices are made a screen is presented that invites the voter to enter his PW once more. The proper value is validated with the check character.

k. The JavaScript program tool now calculates Kp (or
20 Personal Voter Key) for this user and his Virtual Ballot, by calculating VnPID (Voter Identity Code) and VnCx (Subject Identity Code) for each election category, then sends the Virtual Ballot form to the ballot-box server.

l. The ballot-box server stores the received values VnPID
25 and VnCx as a pair in sequential file. After storing the values it calculates a Vote Receipt Confirmation (VotRecCon):

VotRecCon = DESmac (Kbbs_b, (VnPID//VnCx)) and stores the first (high order) 4 bytes of that value (VotRecConSvr) in a file, to be published after the elections. The last (low order) 4 bytes (VotRecConCnt) are
30 transferred to the JavaScript program in the PC of the voter. Kbbs_b is a 3DES MAC generation key for BBS_b, i.e. Ballot Box server with identity

b.

m. The JavaScript program tool produces the proper status to the voter.

5 n. In the last screen for the voter, the JavaScript program presents the filed Voting Pair(s) (or Virtual Ballot Form(s)) VnPID (Voter Identity Code) and VnCx (Subject Identity Code) values, in combination with the received VotRecConCnt. The voter can use this complete information after the election are closed to validate his contribution to the elections and is referred to as his Receipt
10 Confirmation Value (VotValVal).

o. The voter is invited either to write down or print out the VotValVal for each category he voted for.

5. Due to network problems or heavy congestion at the ballot-box-status or ballot-box servers, long response times for the initial
15 status or VotValVal might occur. (The initial status and the VotRecConCnt value in VotValVal are the only interactive elements in this Vote Collecting process). In practice this can result in two different cases:

a. At the beginning of the voting sequence the status information is not received, so the client is unclear if there has been
20 an earlier (partly) completed voting session with the ballot-box server.

b. At the end of the voting sequence the voter does not see (timely enough) the proper status of completion and the related VotValVal values and is not convinced that his vote(s) were properly received at the ballot-box server.

25 To cope with these situations the voter is entitled to perform one of the following actions (or both if he or she prefers to do so):

1. He or she performs the entire voting sequence once more through a URL entry point that does not validate his previous status.

30 2. He or she files a postal vote.

As long as all his/hers votes are for the same

candidate(s), the tally system will clearly detect his proper choice and count his/hers vote as one for the proper candidate.

Replacement Election Packages procedure.

5 Any eligible voter, who claims not to have received his closed envelope with the ballot-forms or the reception of a damaged envelope, is entitled to request a Replacement Election Package. The following organizational and technical provisions will be in place to submit such a package to the voter and to mark the ballots form his original package as invalid.

- 10 1. At a Central Election Committee Helpdesk:
- a. The complaining voter approaches the Central Election Committee Helpdesk and files his complaint.
 - b. The Helpdesk validates voters' identity, his eligibility as voter and establishes his VnID.
 - 15 c. The Helpdesk reports the VnID to a Polling Office or Polling Committee, providing the election services under supervision of the Central Election Committee, called TTP Internetstemmen.
 - d. The Helpdesk issues the voter a closed RepElPac envelope and marks the corresponding VrID in the RepElPac Stock File as "issued".
 - 20 e. Note is taken that the combination VnID and VrID is NOT recorded in any way (e.g. this can be handled by two different, separated elements of the helpdesk)
 - f. All the Helpdesk activities in this matter are logged, but anonymously.
- 25 2. At TTP Internetstemmen:
- a. The proper RnPotVote records are marked "invalid".
 - i. From the Helpdesk the reported VnID's are received.
 - ii. Using an automated procedure, the corresponding Kp is calculated, then the related RnPotVote records.
 - 30 iii. These records are marked "invalid".
 - iv. A logging file is maintained, containing only

impersonal information.

b. The proper RnPotVote records are marked "valid, issued".

i. From the Helpdesk (through the RepElPac Stock File) the issued VrID's are received.

5 ii. Using an automated procedure, the corresponding RnPotVote records are accessed and marked "valid, issued".

iii. A logging file is maintained, containing only impersonal information.

Tally (Calculating the voting results)

10 1. At the end of election TTP Internetstemmen performs the following actions;

a. Internet Votes:

15 i. They close all ballot-box and ballot-box-status servers, after receiving the proper order to close from the Central Election Committee.

ii. They sign the Internet-Received-Votes (IRecVote) and the VotRecConSvr files.

iii. They publish those files with their signature.

b. Postal Votes:

20 i. Close of the point for the postal ballots.

ii. Processing of all postal ballots:

1. Counting all ballots.

2. Automatic reading of all ballots, creating a Received Postal Ballot (RecPostBal) record per form, making a RecPostBal File.

25

3. Correcting/ adding records to this file of forms that create automatic processing problems.

4. Discrepancy reporting on all reading problems and manual corrections.

30 5. Sending the RecPostBal File and all reports in a secure way to TTP Internetstemmen Tally processing.

6. TTP Internetstemmen calculates per RecPostBal record a proper VnPID-VnCx pair and appends that to the Postal-Received-Votes (PRecVote) File.

5 7. Validation of the number of records processed with the received number of postal ballots and the reported discrepancies.

8. Creation of a complete signed PRecVote file.

iii. Publication of that file with their signature.

c. Republication of the changed RnPotVote file.

10 d. Forwarding of all invalid votes to the Central Election Committee.

e. Forwarding of logs and discrepancy reports to the Central Election Committee.

2. The Central Election Committee performs the following actions:

15 a. Validation of logs, reports and invalid votes.

b. Proper calculation of the voting results by processing Received-Votes files in relation to the current RnPotVote file.

i. Proper processing and counting rules are observed:

20 1. Combination of all RecVote files in one file; in this total RecVote file the complete origin and status of the Tally process is registered per voting pair.

2. Sorting all vote pairs in this file in the order of VnPID, VnCx.

25 3. Comparing every vote pair (after hashing the values with MDC to a RnRecVote) with the RnPotVote file and updating the status of the vote pair as found per group with equal RnPID.

a. All invalid votes (with either an invalid VnPID or an invalid VnCx) are marked as 'invalid'.

30 b. In case of one valid vote pair for this VnPID: update vote record as countable vote.

c. In case of multiple valid vote pairs for this

VnPID:

i. All from one source (internet or postal)?

1. Yes; in case all equal: mark first as countable vote with proper Cm, all others as duplications

5

2. No: mark all as invalid because of different votes

ii. All valid votes from two sources: mark all votes from the source with the lowest priority as overruled, process the votes of the source with the highest priority as described in the step above.

10

4. Perform a count of all countable vote records.

c. Publication of provisional election results.

d. Formal complaint steps.

15

e. Correction steps in the Votes-Received files as required.

f. Publication of these corrections.

g. Publication of the permanent election results.

Validating the results of the election

20

For validation purpose each voter should retain his Receipt Confirmation Value (VotValVal), which is presented to him at the last screen of his voting process in hexadecimal format and can then be printed.

25

At the beginning of the election the Reference Potential Votes (RnPotVote) published can be used by anyone to validate the number of potential voters and the number of candidates. In addition each individual voter can verify that his VPID can be validated through the file and that all his potential votes can be validated through the file.

30

The Tally process as conducted by the Central Election Committee can be performed by anyone with access to the published RnPotVote and Votes-Received files and the published rules for the elections.

Each individual voter can validate that his vote (the Virtual Ballot Form retained in his Receipt Confirmation Value (VotValVal)) is present in the RecVote file and therefore part of the formal outcome of the election.

5 In addition, all published logs and discrepancy records can be used by anyone to validate that operating procedures have been conducted as required. In particular the Replacement Election Packages procedure should be verified (e.g. the number of complaining voters should match the number of issued VrID's and the number of updates in the
10 RnPotVote file; plausibility checks should be done on the number of complaining voters).

Handling of Vote Receipt Confirmation in respect to complains by voters

In case of a complaint by a voter, that his vote is not
15 present in the RecVote file, it is of major importance that his VotRecConCnt (the last part in his Receipt Confirmation Value or VotValVal) is validated. Since this is a DESmac, created by a 3DES key, this validation is a sensitive operation that should and could not be performed by any party with some kind of interest in the election
20 results. In case of, the system TTP Internetstemmen will perform this task. TTP Internetstemmen is the party that is responsible for the generation, installation and management of the 3DES keys in the first place and can do the validation in total independence of The Central Election Committee or any other authority.

25 If indeed the voter can present a valid vote pair (Virtual Ballot Form) with proper VotRecConCnt (Vote Receipt Confirmation for Client), that is not present in the RecVote file, then this is an absolute proof that votes have disappeared. TTP Internetstemmen will report that to the Central Election Committee, so the later can make a
30 final decision on the validity of the total election result.

To prevent abuse by TTP Internetstemmen, the published

VotRecConSvr (Vote Receipt Confirmation for Server) file creates an opportunity to validate that indeed the same DESmac key is used in the validation process as was used during the election.

5 A Pki based VotRecCon would allow for an easier validation process, but would require a significantly more powerful ballot-box server process. In the current view of the peak load on this server this is considered not to be acceptable.

Specific requirements of the system and its supporting organization.

10 The Internet Election system, in combination with the supporting organizations, should provide for the following features. In addition, the major measures to obtain the features are shortly described. In some cases this description applies to several requirements.

15 1. Authentication: Only authorized voters should be able to vote.

a. All eligible voters receive a Voting Card by mail, that contains an impersonalized 8 alphanumeric character Voters secret Voting Code (VPID) and a randomly selected 8 alphanumeric character Password (PW), both unique to each voter.

20 b. In case of a complaint of an authorized user about the reception of his Voter Card, a new one will be made available to him. The original Voting Card will be rendered invalid and cannot be used to produce valid votes any more.

25 c. The voter can validate his VPID and PW before the election begins on the Internet through a published Reference Potential Votes (RnPotVote) file.

2. Convenience: Voters should be able to cast votes with minimal equipment and skills.

30 a. There is no requirement for the voter to register in advance the way he will cast his vote. At any moment the voter can decide

to drop his effort to vote through the Internet and use his conventional ballot paper through the mail, as long as the latter is turned-in on time.

5 b. The system is based on the regular Internet facilities that are currently used by over 95% of the potential voters.

c. The actual Internet voting process for the voter is based on short directions on his Voting Card and a normal, interactive sequence of screens through his Internet browser.

10 d. During the sequence of screens the voter is free to interrupt his voting activities; a status screen gives him a simple and complete picture of the actual situation at a each moment of interruption and at the end of his voting session.

15 e. At the completion of his voting session, the voter receives an 8 alphanumeric character long Vote Receipt Confirmation (VotRecConCnt), that he can printout or write down in addition to his Virtual Ballot Form (VnPID//VnCx) and use in case of disputes about his voting action.

3. Secrecy: No one should be able to determine how any individual voted.

20 a. His or hers unique and impersonalized Voter Identity Code VnPID protects the actual voting identity of each voter; his Voting Card just contains impersonalized information about him.

25 b. The actual calculation and generation of the several sensitive voter-related data (e.g. VPID, PW) and the related Reference Potential Votes (RnPotVote) file is sensitive; the system allows for isolated processing of this data in a short time interval by an independent party (TTP Internetstemmen).

30 c. The preparation of Voting Cards and the mailing to the individual voter is sensitive as well and will be handled by an independent, specialized printing company.

d. Each vote of a specific voter for a specific candidate

consists of a unique 16-byte string and can only be generated by the voter. The system (and anyone else) is able to determine its validity, but without any reference to the real identity of the voter.

5 e. During voters communication with the voting server the exchanged information is protected by SSL.

f. The voting server itself is set-up in a way, that neither Internet address information, nor any other information related to the sender of a vote is retained with that vote. TTP Internetstemmen will manage that server.

10 4. Uniqueness: No voter should be able to vote more than once.

5. Integrity: Votes should not be able to be modified without detection.

6. Accuracy: Voting systems should record the votes correctly.

15 7. Reliability: Systems should work robustly, even in the face of numerous failures.

a. In the system an individual vote is calculated by a script program in the browser of the client, based on secret information coming from the Voting Card. The main task of the election server is to initiate a reliable and confidential session with the client, to provide
20 the client with the script program and candidate information, to receive and store the vote and to return a Vote Receipt Confirmation (VotRecConCnt) message. In addition, all messages are short. Both on the client and the server side there is no dependency on critical and complex components, like database technology, detailed interactivity, point-of-
25 no-return counters and commit-roll-back mechanisms. Finally there is no need to concentrate all election traffic in one server, since there is no need to guard the voters activities at a single place; votes could even be received in parallel in different servers and all be combined at the end of the election. By nature this allows for the creation of a robust
30 server setup in a simple and straightforward way.

b. In a multi component, Internet based election system one

should take into account that the same message could arrive more than once. That could be caused accidentally by system components or on purpose in case of a system (component) restart or a voter that repeats his voting action in case of disturbances. The system allows for the reception of one or more votes for one election by the same voter, as long as all his valid votes are all the same.

5 c. The system counts all the same votes of one voter as one; valid, but different votes by one voter for several candidates are invalid (since that is comparable with a ballot paper with more than one box marked by the voter in the case where he can only vote for one candidate).

10 d. The system allows for the use of both mail and Internet votes by the same voter. First all invalid votes for this voter are dropped. In case the valid votes of a specific voter arrived both by mail and by Internet, the system will neglect the mail votes and compare the Internet votes. In case there is only one Internet vote or a set of equal votes, then one is counted as a vote for a specific candidate. In case of just valid mail votes from a specific voter have arrived, they are processed in a similar way. This way, mail voting could even be used as a back up for Internet voting.

15 e. The voting session is protected by SSL. This is done to protect against eavesdropping and to ensure the voter, that he is casting his vote with the proper ballot authority.

8. Verifiability: Should be possible to verify that votes are correctly counted for in the final tally.

25 a. At the beginning of the election the Reference Potential Votes (RnPotVote) file is published; this file can be checked by anyone on:

- 30 i. Its origin and integrity
ii. Its size (that should reflect the number of potential voters and the number of candidates)

and by each individual voter on:

iii. The fact that his VPID can be validated through the file.

5 iv. The fact that all his potential votes can be validated through the file.

b. At the end of the election all received votes (RecVotes) are published; this file can be checked by anyone on:

i. It's origin and integrity.

10 ii. Its size (that should reflect the published turn-out for the election).

iii. The actual published election results, in combination with the earlier published RnPotVote file,

and by each individual voter, in combination with the earlier published RnPotVote file on.

15 iv. The fact that his vote is present in the RecVote file and therefore part of the formal outcome of the election.

v. The validation of the received Vote Receipt Confirmation (VotRecConCnt), through the Empire function of TTP Internetstemmen, in case of discrepancies.

20 9. Audit ability: There should be reliable and demonstrably authentic election records.

In addition to the features mentioned in relation to Verifiability, TTP Internetstemmen adds the following reports:

25 a. Reports on proper initiation of the election data and systems

b. Reports on proper Voting Card reissuing procedures

c. Reports on proper processing of the mail votes

d. Reports on all discrepancies handled by the Empire activities

30 e. Reports on the presentation of the formal results

f. File containing all VotRecConSvr values to validate all

VotRecConCnt values and visa-versa

- g. Presentation of (all) valid and invalid votes on request.
10. Non-coercibility: Voters should not be able to prove how they voted.
- 5 11. Flexibility: Equipment should allow for a variety of ballot question formats.
- a. The system meets this requirement.
12. Certifiability: Systems should be testable against essential criteria.
- 10 a. Due to technical shortcomings, created by the given voter environment, the system by itself is unable to meet all requirements; therefore, just certifying the system will not guarantee a proper election process.
- 15 b. Some parts and functions of the system and its subsystems are certifiable.
- c. Other parts out of the scope of the system should be judged as well, to obtain a complete impression on the reliability and controllability of the complete election process.
- 20 13. Transparency: Voters should be able to possess a general understanding of the whole process.
- a. Any system with technical components will be hard to understand for the general public and at least will not come close to the understandability of a ballot-box election system.
- 25 b. In case the technical components could be validated and certified by an independent party; once that is accepted, the general public can have a general understanding and trust in the system design, since all functions map well on the basic interests of the individual voter.
- 30 14. Cost-effectiveness: Systems should be affordable and efficient.

a. The system can be performed with general Internet-browser type systems at the client site and relatively simple server components.

5 Above, the invention has been disclosed with reference to a preferred embodiment thereof. Those skilled in the art will appreciate that several modifications and additions can be made within the scope of the present invention as defined in the attached claims.

CLAIMS

1. Electronic voting system for collecting and counting votes from individual voters using electronic polling equipment in an election comprising a list of subjects to be elected, from which list one subject is to be elected by an individual voter, said votes being forwarded by means of a data network, said voting system comprising:
- 5
- means for generating a unique personal key for each individual voter entitled to said election, which unique personal key is to be communicated to said individual voter;
- 10
- means for generating a unique subject code for each subject on said list of subjects to be elected in said election;
 - means for generating a reference election record for each individual voter comprising all potential virtual ballot forms for said individual voter, wherein a unique voter identity code for said individual voter is calculated from a unique code for said election and the unique personal key of said voter, wherein a unique subject identity code for each subject on said list of subjects to be elected by said voter in said election is calculated from said unique subject codes and said unique personal key of said voter, and wherein said calculated identity codes form part of the virtual ballot forms;
- 15
- means for storing said reference election records for said individual voters;
 - means for loading a tool in said polling equipment of said individual voter wherein said tool comprises means for calculating the unique voter identity code of said voter from said election code and the unique personal key communicated to said voter, for calculating the unique subject identity code of the subject elected by said voter from the unique subject code of said subject elected by said voter and said unique personal key of said voter and for generating the virtual ballot form comprising said calculated identity codes by using said polling equipment;
- 20
- 25
- 30

- means for forwarding said virtual ballot form by said polling equipment over said data network;

- means for receiving and collecting said virtual ballot form forwarded by said polling equipment;

5 - means for verifying each collected virtual ballot form with respect to its presence in said reference election records of said voters;

- means for counting votes, and

- means for establishing an election result,

10 characterized by means for validating votes from said collected virtual ballot forms, which validating means are arranged in such way that if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of said set is validated as one valid vote of said voter and the remaining virtual
15 ballot forms of said set are marked as duplicate, provided said virtual ballot forms of said set are identical as to the subject elected by said voter, otherwise all virtual ballot forms of said set are marked invalid.

2. Electronic voting system for collecting and counting votes from individual voters using electronic polling equipment in an election
20 comprising a list of subjects to be elected, from which list one combination of subjects is to be elected by an individual voter, said votes being forwarded by means of a data network, said system comprising:

- means for generating a unique personal key for each individual voter entitled to said election, which unique personal key is
25 to be communicated to said individual voter;

- means for generating a unique subject combination code for each combination of subjects on said list of subjects to be elected in said election;

- means for generating a reference election record for each
30 individual voter comprising all potential virtual ballot forms for said individual voter, wherein a unique voter identity code for said

individual voter is calculated from a unique code for said election and the unique personal key of said voter, wherein a unique subject combination identity code for each combination of subjects on said list of subjects to be elected by said voter in said election is calculated
5 from the unique subject combination code for said combination of subjects and said unique personal key of said voter, and said calculated identity codes and wherein said calculated identity codes form part of the virtual ballot forms for said individual voter;

10 - means for storing said reference election records for said individual voters;

- means for loading a tool in said polling equipment of said individual voter wherein said tool comprises means for calculating the unique voter identity code for said voter from said election code and the unique personal key of said voter, means for calculating the unique
15 subject combination identity code for the combination of subjects elected by said voter from the unique subject combination code for said combination of subjects elected by said voter and the unique personal key of said voter, and means for generating the virtual ballot form comprising said calculated identity codes by using said polling
20 equipment;

- means for forwarding said virtual ballot form by said polling equipment over said data network;

- means for receiving and collecting said virtual ballot form forwarded by said polling equipment;

25 - means for verifying each collected virtual ballot form with respect to its presence in said reference election records of said voters;

- means for counting votes, and

- means for establishing an election result,

30 characterized by means for validating votes from said collected virtual ballot forms, which validating means are arranged in such way that if a

set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of said set is validated as one vote of said voter and the remaining virtual ballot forms of said set are marked as duplicate, provided said virtual ballot forms of said set are identical as to said one combination of subjects elected by said voter, otherwise all virtual ballot forms of said set are marked invalid.

3. Electronic voting system according to claim 1 or 2, wherein said validating means form part of said means for verifying said collected virtual ballot forms.

4. Electronic voting system according to claim 1 or 2, wherein said validating means form part of said means for counting said votes.

5. Electronic voting system according to any of the previous claims, further comprising confirmation means for generating a receipt indicating that a virtual ballot form has been received from said polling equipment of said voter and means for delivering said receipt comprising a unique receipt confirmation value in readable form at said polling equipment of said voter.

6. Electronic voting system according to any of the previous claims, further comprising means for publishing the list of voters entitled to said election, the list of subjects to be elected in said election and said reference election records for said individual voters, enabling public inspection before the date of said election, and entry means for each individual voter using said unique personal key for inspection of the reference election record for said individual voter.

7. Electronic voting system according to any of the previous claims, further comprising means for publishing the election-result comprising the record of the valid votes as awarded for said collected virtual ballot forms after been submitted for verification and validation, enabling public inspection, and entry means for each individual voter using said unique personal key for inspection of the

account of said virtual ballot form forwarded by said polling equipment of said individual voter.

8. Electronic voting system according to any of the previous claims, further comprising means for generating and storing a reference
5 service identity code for each individual voter entitled to said election, which reference service identity code is calculated from a fixed part of said unique personal key of said voter and information related to said election and means for keeping a status record of said voter at said means for receiving and collecting said virtual ballot
10 forms, wherein said status record is associated with said reference service identity code of said voter.

9. Electronic voting system according to claim 8, wherein said tool to be loaded in said polling equipment of said voter is arranged for calculating a service identity code from said fixed part of said unique
15 personal key of said voter and said information related to said election and for forwarding said service identity code to said means for receiving and collecting said virtual ballot forms.

10. Electronic voting system according to any of the previous claims, further comprising communication means for communicating said
20 unique personal key to each individual voter entitled to said election, said communication means comprises at least one of a group including means for electronically storing said unique personal key in a chip card of said voter, data communication means for communicating said unique personal key to said voter by a data network such as the Internet or a
25 fixed and/or mobile data communication network including a Short Message Service, and means for providing said unique personal key in a human and/or machine readable form on a hard copy, such as a text message on paper, for communicating by mail to said voter.

11. Electronic voting system according to claim 10, wherein
30 said polling equipment is arranged for operatively connecting same to data input means comprising at least one of a group including a chip card

reader, a keyboard, a mouse, a screen, a bar code reader and voice conversion means.

12. Electronic voting system according to any of the previous claims, wherein said means for receiving and collecting virtual ballot forms are arranged for receiving and collecting virtual ballot forms other than forwarded by polling equipment of a voter, such as physical ballot forms received by mail and converted into virtual ballot forms by automatic ballot form reading and conversion means.

13. Electronic voting system according to claim 12, wherein said means for verification and validating are arranged in such way that if a set of two or more virtual ballot forms associated with an identical voter identity code is collected and said virtual ballot forms are collected from means of different kinds that have been appointed differing values of priority only the virtual ballot forms collected from the means of the kind with the higher value of priority are submitted for verification and validation.

14. Electronic voting system according to claim 13 wherein said means for verification and validation are arranged in such way that the means in which physical ballot forms received by mail are converted into virtual ballot forms are appointed the lower value of priority.

15. Electronic voting system according to any of the previous claims dependent on claim 1, wherein said means for generating a unique subject identity code for each subject to be elected in said election, said means for generating a unique voter identity code and said means for generating a reference election record for each individual voter entitled to said election comprise cryptographic generator and calculator means.

16. Electronic voting system according to any of the previous claims dependent on claim 2, wherein said means for generating a unique subject combination identity code for each combination of subjects to be elected in said election, said means for generating a unique voter identity code and said means for generating a reference election record

for each individual voter entitled to said election comprise cryptographic generator and calculator means.

17. Electronic voting system according to claim 15 or 16 wherein said cryptographic generator and calculator means are arranged
5 for symmetric encryption.

18. Electronic voting system according to any of the previous claims, wherein said means for presenting said list of subjects from which one subject or one combination of subjects is to be elected by said voter at said polling equipment, said means for loading said tool in said
10 polling equipment of a voter, said means for receiving and collecting said virtual ballot form forwarded by said polling equipment and said confirmation means are supported by computer equipment comprising at least one computer server.

19. Electronic voting system according to any of the previous
15 claims, wherein the or each of said means for loading said tool in said polling equipment of a voter, said means for receiving and collecting said virtual ballot form forwarded by said polling equipment, said confirmation means and said polling equipment are arranged for providing secure data transmission over said data network.

20. Electronic voting system according to any of the previous
20 claims, wherein said means for generating a unique personal key for each individual voter, said means for generating said unique voter identity code for each individual voter, means for generating for generating said unique identity code for each subject or combination of subjects to be
25 elected in said election, said means for generating said reference election record for each individual voter entitled to said election, said means for verifying the collected virtual ballot form of said individual voter with respect to its presence in said reference election record of said voter, said means for counting votes of said voters, said means for
30 validating votes from said collected virtual ballot forms and said means for establishing an election-result based on said counted votes are

supported by computer equipment arranged to be operated under the supervision of an election authority.

21. Electronic voting system according to any of the previous claims, wherein said polling equipment comprises at least one of a group
5 including a personal computer and fixed and mobile data communication equipment arranged for providing access to said data network.

22. Method for electronic voting, for collecting and counting votes from individual voters using electronic polling equipment in an election comprising a list of subjects to be elected, from which list one
10 subject is to be elected by an individual voter, said votes being forwarded by means of a data network, said method comprising the steps of:

- generating a unique personal key for each individual voter entitled to said election;
- 15 - communicating said unique personal keys to said individual voters;
- generating a unique subject code for each subject on said list of subjects to be elected in said election;
- generating a reference election record for each
20 individual voter comprising all potential virtual ballot forms for said individual voter, wherein a unique voter identity code is calculated for said individual voter from a unique code for said election and the unique personal key of said voter, a unique subject identity code for each subject on said list of subjects to be elected by said voter in said
25 election is calculated from said unique subject codes and said unique personal key of said voter, said calculated identity codes forming part of the virtual ballot forms;
- storing said reference election records for said individual voters;
- 30 - loading a tool in said polling equipment of a voter;
- electing one subject from said list at said polling

equipment of said individual voter, by inputting said unique personal key communicated to said voter and said unique subject code for said one elected subject into said polling equipment;

5 - generating a virtual ballot form using said tool loaded into said polling equipment of said voter, wherein a unique voter identity code is calculated from said election code and said unique personal key of said voter, wherein a unique subject identity code is calculated from said unique subject code for said one subject elected by said voter from said unique subject code of said one subject elected and
10 said unique personal key of said voter and wherein said calculated identity codes form part of said virtual ballot form;

 - forwarding said virtual ballot over said data network;

 - receiving and collecting said virtual ballot form forwarded by said polling equipment;

15 - verifying each collected virtual ballot form with respect to its presence in said reference election records of said voters;

 - counting votes, and

 - establishing an election-result based on said counted votes, characterized by a step for validating votes from said collected
20 virtual ballot forms in such way that, if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of said set is validated as one single valid vote of said voter and the remaining virtual ballot forms of said set are marked as duplicate, provided that said virtual ballot forms of
25 said set are identical as to said one subject elected by said voter, otherwise said virtual ballot forms of said set are marked invalid.

23. Method for electronic voting, for collecting and counting votes from individual voters using electronic polling equipment in an election comprising a list of subjects to be elected, from which list one
30 combination of subjects is to be elected by an individual voter, said votes being forwarded by means of a data network, said method comprises

the steps of:

- generating a unique personal key for each individual voter entitled to said election;
- communicating said unique voter identity code to each
5 individual voter;
- generating a unique subject combination code for each combination of subjects on said list of subjects to be elected in said election;
- generating a reference election record for each
10 individual voter comprising all potential virtual ballot forms for said individual voter wherein a unique voter identity code is calculated from a unique code for said election and said unique personal key of said voter, a unique subject combination identity code for each combination of subjects on said list of subjects to be elected by said voter in said
15 election is calculated from said unique subject combination code and said unique personal key of said voter, said calculated identity codes forming part of said virtual ballot forms;
- storing said reference election records for said individual voters;
- loading a tool in said polling equipment of a voter;
- electing one combination of subjects from said list at
20 said polling equipment of said individual voter, by inputting said unique personal of said voter and said unique subject combination code for said one elected combination of subjects into said polling equipment;
- generating a virtual ballot form on said polling
25 equipment using said tool loaded into said polling equipment of said voter wherein a unique voter identity code is calculated from said election code and said unique personal key of said voter, wherein a unique subject combination identity code is calculated from said subject combination code for said one combination of subjects elected and said
30 unique personal key of said voter and wherein said calculated identity

codes form part of said virtual ballot form;

- forwarding said virtual ballot form over said data network;

5 - receiving and collecting said virtual ballot form forwarded by said polling equipment;

- verifying each collected virtual ballot form with respect to its presence in said reference election records of said voters;

- counting votes, and

10 - establishing an election result based on said counted votes, characterized by a step for validating votes from said collected virtual ballot forms in such way that, if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of said set is validated as one valid vote of said voter and the remaining virtual ballot forms of said set are
15 marked duplicate, provided that said virtual ballot forms of said set are identical as to said one combination of subjects elected by said voter, otherwise all virtual ballot forms of said set are marked invalid.

24. Method for electronic voting according to any of the claims 22 - 23, further comprising the step of generating a receipt comprising a
20 unique receipt confirmation value in readable form indicating that a virtual ballot form forwarded over said data network has been received, and wherein said receipt is delivered at said polling equipment of said voter.

25. Method for electronic voting according to any of the claims 22 - 24, further comprising the step of publishing the list of voters entitled to said election, the list of subjects to be elected in said election and said reference election records for said individual voters, enabling public inspection before the date of said election, and the step for providing entry means for each individual voter using said unique
30 personal key for inspection of the reference election record for said individual voter.

26. Method for electronic voting according to any of the claims 22 - 25, further comprising the step of publishing the election result comprising the record of said valid votes as awarded for said collected virtual ballot forms after been submitted for verification and validation, enabling public inspection and the step for providing entry means for each individual voter using said unique personal key for inspection of the record of said vote for said virtual ballot form forwarded by said polling equipment of said individual voter.

27. Method for electronic voting according to any of the claims 22 - 26, further comprising the steps of generating and storing a reference service identity code for each individual voter entitled to said election wherein said reference service identity code is calculated from a fixed part of said unique personal key of said voter and information related to said election, and the step of keeping a status record for each individual voter associated to said reference service identity code.

28. Method for electronic voting according to any of the claims 22 - 27, further comprising the step of generating a service identity at said polling equipment of said voter wherein said service identity code for said voter is calculated from said first part of said unique voter identity code of said voter and information related to said election using said tool been loaded in said polling equipment of said voter, and the step of forwarding said service identity code to said means for receiving and collecting said virtual ballot form.

29. Method for electronic voting according to any of the claims 22 - 24, further comprising the step of receiving and collecting virtual ballot forms other than forwarded by said polling equipment of a voter, such as physical ballot forms forwarded by mail, and converting said physical ballot forms into virtual ballot forms using automatic ballot form reading and conversion means.

30. Method for electronic voting according to claim 29, wherein

the step of validating is arranged in such way that if two or more virtual ballot forms associated with an identical voter identity code are collected and said virtual ballot forms are collected from means of different kinds having been appointed differing values of priority, only
5 the virtual ballot forms collected from the means with the higher value of priority are submitted for validation.

31. Method for electronic voting according to claim 30, wherein the step of validating is arranged in such way that the means in which physical ballot forms received by mail are converted into virtual ballot
10 forms are appointed the lower value of priority.

32. Method for electronic voting according to any of the claims 22 - 31, wherein said unique identity code for each subject or each combination of subjects to be elected, said unique voter identity code and said reference election record for each individual voter entitled to
15 said election are cryptographically generated and calculated.

33. Method for electronic voting according to claim 32, wherein said identity codes and reference election records are generated and calculated for symmetric encryption.

34. Method for electronic voting according to any of the claims 20 22 - 33, wherein said steps of generating said unique personal key for each individual voter entitled to said election, said unique voter identity code for each individual voter, said identity code for each subject or each combination of subjects to be elected, said reference election record for each individual voter entitled to said election, and
25 said steps of verifying the validity of a collected virtual ballot form of an individual voter with respect to its presence in said reference election record of said voter, validating said collected virtual ballot forms, counting votes and establishing said election-result are performed under the supervision of an election authority.

30 35. Method for electronic voting according to any of the claims 22 - 34, wherein said step of communicating said unique personal key to

each individual voter entitled to said election comprises at least one of a group of steps including electronically storing said unique personal key in a chip card of said voter, communicating said unique personal key to said voter by a data network such as the Internet or a fixed and/or
5 mobile data communication network including a Short Message Service, and providing said unique personal key in a human and/or machine readable form on a hard copy, such as a text message on paper, for communicating by mail to said voter.

36. Method for electronic voting according claim 35, wherein
10 said hard copy is suitable to be cast as a physical ballot form comprising said subjects or said combinations of subjects to be elected by said voter.

37. Method for electronic voting according to any of the claims
22 - 36, wherein a reserve-list of a limited number of unique reserve
15 keys is generated and said reference election record is generated to comprise virtual ballot forms for said number of unique reserve keys, and wherein a reserve key of said reserve-list is issued to a voter who applies for a fresh unique key replacing said unique personal key initially appointed to said voter, wherein said reserve key is appointed
20 to said voter after said initially appointed unique personal key and said corresponding reference election record are withdrawn, and wherein said issue of said reserve key from and said withdrawal of said initially appointed unique personal key are taken into account for the verification of the validity of collected virtual ballot forms.

38. Method for electronic voting according to any of the claims
25 22 - 37, wherein said polling equipment comprises at least one of a group including a personal computer and fixed and mobile data communication equipment arranged for providing access to said data network using browser software, and wherein said tool is loaded automatically into said
30 polling equipment from said data network.

39. Method for electronic voting according to claim 38, wherein

said data network comprises the Internet and said polling equipment comprises a personal computer operatively connected to the Internet, wherein said tool is loaded into said personal computer by means of a Java applet included in a web-page to be selected by a voter for participating in said election.

5

40. Method for electronic voting according to claim 39, wherein said polling equipment comprises GSM communication equipment having a SIM-card and wherein said tool is loaded in said SIM-card of said communication equipment for participating in said election by a voter using said communication equipment.

10

41. Computer program product, comprising program code means stored on a computer readable medium, for performing the or part of the steps according to any of claims 22 - 40, if loaded into an internal working memory of said computer and operated by said computer.

15

42. Computer program product, comprising program code means stored on a computer readable medium, arranged as a tool for loading into a computer program running on a computer controlled polling equipment for performing the steps according to any of the claims 22, 28 and 37 - 40 if loaded into an internal working memory of said computer and operated by

20

said computer.

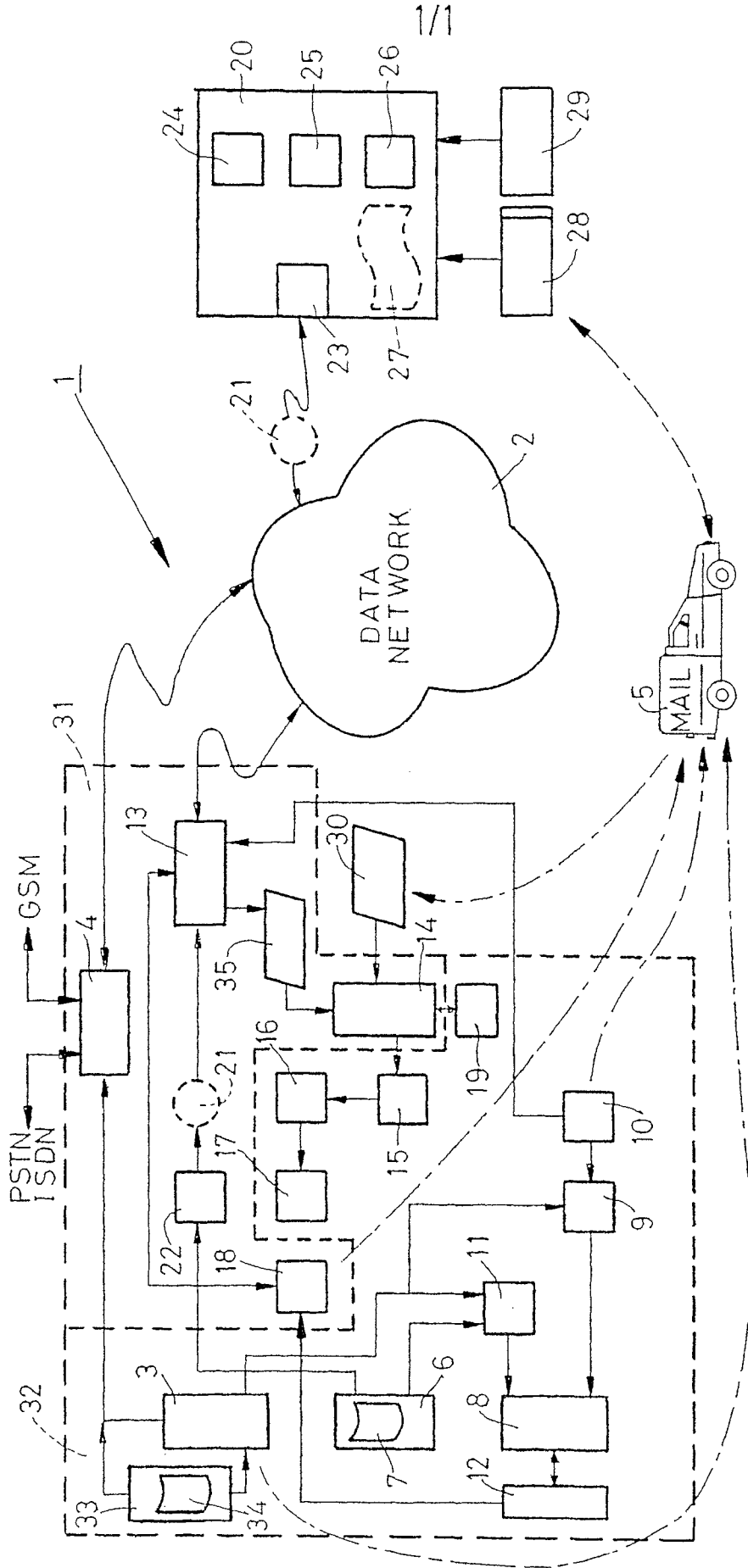


FIG.

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/NL2004/000496

A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06F17/60 G07C13/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC 7 G06F G07C		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 291 826 A (UNIV NIJMEGEN) 12 March 2003 (2003-03-12) cited in the application paragraph '0019! paragraph '0028! paragraph '0035! paragraph '0036! - paragraph '0039! -----	1-42
A	WO 02/42974 A (DAVIES CATHERINE RITA ; REEVES BRUCE HASBROUCK DICKSON (NZ)) 30 May 2002 (2002-05-30) page 7, line 11 - line 17 -----	1-42
A	WO 03/037008 A (LEE EUN-WOO) 1 May 2003 (2003-05-01) page 9, line 24 - page 10, line 12; figure 3 ----- -/--	1-42
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents:		
A document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed		*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family
Date of the actual completion of the international search 22 October 2004		Date of mailing of the international search report 03/11/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Stenger, M

INTERNATIONAL SEARCH REPORT

Int. Patent Application No.
PCT/NL2004/000496

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 148 447 A (MICROFLIGHT S R L ; E I S S P A (IT)) 24 October 2001 (2001-10-24) the whole document	1-42

INTERNATIONAL SEARCH REPORT

Int. nat Application No
PCT/INL2004/000496

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1291826	A	12-03-2003	EP 1291826 A1	12-03-2003
			US 2003042305 A1	06-03-2003
WO 0242974	A	30-05-2002	AU 1285802 A	03-06-2002
			EP 1348187 A1	01-10-2003
			GB 2380033 A ,B	26-03-2003
			WO 0242974 A1	30-05-2002
			US 2003171983 A1	11-09-2003
WO 03037008	A	01-05-2003	WO 03037008 A2	01-05-2003
EP 1148447	A	24-10-2001	EP 1148447 A1	24-10-2001

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 210010/EP/he	FOR FURTHER ACTION		see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/NL2004/000496	International filing date (day/month/year) 08/07/2004	(Earliest) Priority Date (day/month/year) 08/07/2003	
Applicant HOOGHEEMRAADSCHAP VAN RIJNLAND			

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 4 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (See Box II).

3. **Unity of invention is lacking** (see Box III).

4. With regard to the **title**,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regards to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

as suggested by the applicant.

as selected by this Authority, because the applicant failed to suggest a figure.

as selected by this Authority, because this figure better characterizes the invention.

b. none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/NL2004/000496

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 G06F17/60 G07C13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 IPC 7 G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 291 826 A (UNIV NIJMEGEN) 12 March 2003 (2003-03-12) cited in the application paragraph '0019! paragraph '0028! paragraph '0035! paragraph '0036! - paragraph '0039! -----	1-42
A	WO 02/42974 A (DAVIES CATHERINE RITA ; REEVES BRUCE HASBROUCK DICKSON (NZ)) 30 May 2002 (2002-05-30) page 7, line 11 - line 17 -----	1-42
A	WO 03/037008 A (LEE EUN-WOO) 1 May 2003 (2003-05-01) page 9, line 24 - page 10, line 12; figure 3 -----	1-42
	-/--	

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

22 October 2004

Date of mailing of the international search report

03/11/2004

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel: (+31-70) 340-2040, Tx: 31 651 epo nl
 Fax: (+31-70) 340-3016

Authorized officer

Stenger, M

INTERNATIONAL SEARCH REPORT

international Application No
PCT/NL2004/000496

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 148 447 A (MICROFLIGHT S R L ; E I S S P A (IT)) 24 October 2001 (2001-10-24) the whole document -----	1-42

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/NL2004/000496

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1291826	A	12-03-2003	EP 1291826 A1	12-03-2003
			US 2003042305 A1	06-03-2003
WO 0242974	A	30-05-2002	AU 1285802 A	03-06-2002
			EP 1348187 A1	01-10-2003
			GB 2380033 A , 8	26-03-2003
			WO 0242974 A1	30-05-2002
			US 2003171983 A1	11-09-2003
WO 03037008	A	01-05-2003	WO 03037008 A2	01-05-2003
EP 1148447	A	24-10-2001	EP 1148447 A1	24-10-2001

PATENT COOPERATION TREATY

210010

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

PCT

see form PCT/ISA/220

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/NL2004/000496

International filing date (day/month/year)
08.07.2004

Priority date (day/month/year)
08.07.2003

International Patent Classification (IPC) or both national classification and IPC
G06F17/60, G07C13/00

Applicant
HOOGHEEMRAADSCHAP VAN RIJNLAND

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Stenger, M

Telephone No. +49 89 2399-7353



WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/NL2004/000496

Box No. II Priority

1. The following document has not been furnished:

copy of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(a)).

translation of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(b)).

Consequently it has not been possible to consider the validity of the priority claim. This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

2. This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-42
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	1-42
Industrial applicability (IA)	Yes: Claims	1-42
	No: Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/NL2004/000496

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
 - This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).
2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material:
 - a sequence listing
 - table(s) related to the sequence listing
 - b. format of material:
 - in written format
 - in computer readable form
 - c. time of filing/furnishing:
 - contained in the international application as filed.
 - filed together with the international application in computer readable form.
 - furnished subsequently to this Authority for the purposes of search.
3. In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:

Section V:

1. Cited documents:

The following documents (D) are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: EP1291826

D2: WO02/42974

2. Article 5:

The application contravenes Article 5 PCT. There is only one embodiment disclosed in the description (p.24, I.4-p.34, I.7). According to this embodiment, the values VPID, PW and EIID are printed on the voting cards (p.25, I.5). However, the voter is required to enter VPID, PW and ExtParGp into his polling equipment (p.27, I.4). Since the voter is not in the possession of ExtParGp, he is not capable of entering this code. Thus, in the absence of any working embodiment, the description does not disclose the invention in a manner sufficiently clear and complete to enable the person skilled in the art to carry out the invention (Article 5 PCT).

In addition, the terminology used in the description of the mentioned only embodiment is completely different from the one used in the claims and the general description of the invention (p.1, I.1-p.24, I.3). Thus, it is not possible for the person skilled in the art to associate the various "unique codes/keys" of the claims to the different values/key/codes mentioned in the description of the embodiment.

Therefore also, the requirements of Article 5 PCT are not met.

Moreover, according to the independent claims, the calculated identity codes are comprised in the virtual ballot form. The subject codes are not mentioned. However, there is no teaching in the present application how the votes can be counted if the subject codes themselves are not comprised in the virtual ballot form. Therefore also, the requirements of Article 5 are not met.

In addition, there is no embodiment comprised in the description that would disclose to the person skilled in the art how a combination of subjects could possibly be elected. Therefore also, the requirements of Article 5 are not met.

3. Inventive step of independent claims 1, 2, 22 and 23:

Notwithstanding the above objection concerning Article 5, the independent claims, as far as they could be understood, also lack an inventive step according to Article 33(3)

PCT.

D1 discloses systems and methods according to the preamble of each of the independent claims of the present application (see par.s 19, 28, 35.3), 36-39).

The subject-matter of the independent claims of the present application differs from D1 by the characterizing features, namely that

- if a set of two or more virtual ballot forms associated with an identical voter identity code is collected, one virtual ballot form of said set is validated as one single valid vote of said voter and the remaining virtual ballot forms of said set are marked as duplicate if said virtual ballot forms of said set are identical concerning the subject/the combination of subjects elected by said voter, and otherwise (all) said virtual ballot forms of said set are marked invalid.

These characterizing features merely reflect a choice concerning the rules of the election which has to be decided upon by the organisers of that election (please see also D1, par. 41). It has to be noted that the specific choice defined in the independent claims of the present application does not, per se, solve any particular technical problem.

Instead, the objective technical problem to be overcome by the person skilled in the art of computer and network science would be to implement the rule about the counting of double votes defined by the organisers of the election into a computerised election system according to D1. Such a straightforward implementation, however, comes within the scope of the customary practice followed by persons skilled in the art of computer and network science.

Please note that the application does not contain any information which would help the person skilled in the art of computer and network science when implementing the above mentioned rule.

Consequently, the subject-matter of the independent claims 1, 2, 22 and 23 lacks an inventive step according to article 33 (3) PCT.

Moreover, even the purely organisational possibilities of either counting only one vote or of discarding all votes originating from one and the same source is already disclosed in D2 (p.7, I.11-17).

4. Dependent Claims:

The features of the dependent claims, insofar as they are not known from the documents cited in the Search Report for the same purpose as in the present application, are generally known to a person skilled in the art, and therefore, do not produce an inventive step.

Section VII:

1. If new independent claims are to be filed, they should still be correctly limited against D1 as required by Rule 6.3(b).
2. The relevant prior art known from D2 should be cited in the description (Rule 5.1(a)(ii) PCT).
3. The features of the claims should be provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 6.2(b) PCT). This applies to both the preamble and characterising portion (see the Guidelines 5.11 PCT). This reference signs should not only include the numbers used in the figure, but should also comprise the values/codes/keys used throughout the description of the embodiment on p.24, l.4-p.34, l.7.
4. The description and the dependent claims should be adapted to the new independent claims.
5. In the event that more than one independent claim (e.g. a method and an apparatus claim) is filed, **all claims should comprise the same or corresponding "special technical features" to meet the requirements of Rules 13.1 and 13.2.** The applicant is requested to identify these "special technical features" in his accompanying letter.

Section VIII:

1. Claims 41 and 42 are each directed to a computer program product for performing a part of the steps of certain dependent claims. Please note that dependent claims always comprise all the features of the (independent) claims they refer to. Thus, it is not clear what is actually claimed in claims 41 and 42 and these claims should be deleted.

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING
AUTHORITY (SEPARATE SHEET)

International application No.

PCT/NL2004/000496

Further remarks:

The examiner doubts that the above Article 5 objections can be overcome by the applicant. If, however, the applicant disagrees on this point, he is requested to file an amended application taking account of all above objections and the following remarks.

The applicant should clearly point out the basis in the original PCT application for every amendment made in the claims (Article 34(2)b PCT).

In his letter of reply, the applicant should clearly point out which combination of features taken from different former dependent claims or from the description, now forming part of the characterizing features in the independent claim, solves a technical problem in a non-obvious way.

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.03.2003 Bulletin 2003/11

(51) Int Cl.7: G07C 13/00, G07C 13/02

(21) Application number: 01203355.1

(22) Date of filing: 05.09.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(72) Inventors:
• Jacobs, Bartholomeus Paulus Franciscus
6524 SJ Nijmegen (NL)
• Oostdijk, Martijn Diederik
6512 JT Nijmegen (NL)

(71) Applicant: KATHOLIEKE UNIVERSITEIT
NIJMEGEN
6525 ED Nijmegen (NL)

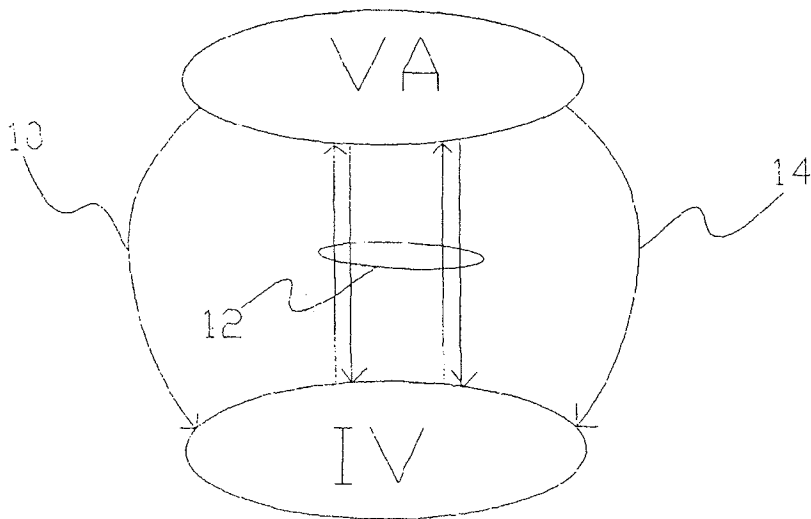
(74) Representative: Prins, Adrianus Willem et al
Vereenigde,
Nieuwe Parklaan 97
2587 BN Den Haag (NL)

(54) Electronic voting system

(57) An electronic voting process sends votes that have been entered via a general purpose user interface such as the keyboard of a PC to a vote collecting system. To prevent viruses between the interface and the vote collecting system from entering fraudulent votes, individualized ballot forms are used. Each for a different voter and each containing entries for respective ones of the options that can be made in the vote. Entries for different options within each one of the forms contain mutually different identifiers, identifiers in entries for equal

options in different ones of the forms containing mutually different identifiers. Each ballot forms is sent to the voter for which it was individually generated. The voter enters the identifiers for his or her option and a voting system compares the identifier with the information about the identifiers for the identified voter stored in the vote collecting system. The vote is counted for the option, if any, that corresponds to the data for the identified voter according to the information stored in the vote collecting system

FIGURE 1



EP 1 291 826 A1

Description

[0001] The invention relates to an electronic system and process for collecting votes and to a set of ballot forms for use in such a system and process. As used herein "voting" will refer to any process in which a human user makes a selection between options and communicates that selection to a vote collecting authority.

[0002] The advent of modern electronic communication techniques has made it possible to hold elections in which voters don't need to go to conventional polling stations where officials receive voters and collect votes. For example, instead of entering his or her vote at a polling station, the voter may enter his or her vote at home using a PC, whereupon the PC transmits the vote to a server that counts votes from a plurality of voters and reports the result. Without a polling station, however, there are also no officials to check the identity of the voters and to ensure that the votes are cast by the identified voters.

[0003] For electronic voting these guarantees against fraud have to be replaced by technical measures to ensure that no fraud is possible. Most possibilities of fraud can be counteracted by the use of electronic signatures. An electronic signature adding device incorporates the vote into an electronic message in such a way that it can be verified that a specific voter has sent the message. A typical example of a signature adding device is a smart card. The voter is provided with a smart card that contains unique, secret information. The user enters his or her option in the vote, the smart card encodes (e.g. encrypts) the vote in a message using the secret information and the encoded vote is sent to the server. Upon reception of the message, the server verifies that the message has been encoded with the secret information of the voter and enters the vote only if this is so. Such a protection ensures that only legal voters, that are in possession of appropriate smart cards can send votes that will be counted.

Of course, smart cards have only limited user interface facilities. Therefore, it is desirable that the user enters his or her option via the general input facilities of the PC, for example using the keyboard, the mouse or voice recognition etc. and that the PC feeds the option to the smart card to encode it in the message.

[0004] It has been found that this use of a general purpose user interface leads to another susceptibility to fraud. If the PC, or more generally any device that contains the user interface, is infected with a virus that intercepts communication between the PC and the smart card, there is a risk that such a virus can substitute a fraudulent vote for the vote entered by the voter, have the smart card encode this fraudulent vote and send a message with the fraudulent vote to the server. Thus, the fraudulent vote would be counted at the server.

[0005] Amongst others it is an object of the invention to provide for measures that reduce the risk that a virus that has infected the path between the user interface

and the signature device can fraudulently select the voting option. The invention provides for an electronic voting system according to Claim 1. According to the invention individualized ballot forms are used, in which the possible options that can be voted for correspond to identifiers that are different for different voters. Without knowledge of the ballot form, a virus in the path between the user interface and the vote collecting system is unable (or more precisely, very unlikely to be able) to insert valid fraudulent votes by inserting an identifier for a pre-determined option.

[0006] Information about the identifiers is also stored in the vote collecting system. To vote, the voter enters the identifier for his or her option at the user interface.

The identifier is compared with the stored identifiers for the voter. The vote is sent to a vote collecting system, which counts the vote for the option corresponding to the identifier. Preferably, the comparison between the stored identifiers and the entered identifier is performed in the vote collecting system.

[0007] The identifiers are for example numbers, or letter combinations that can be entered at a user interface. In an embodiment the identifiers are encoded as bar codes on a paper ballot form, or more generally as any machine readable code, so that the voter can enter the identifier for example by scanning it with a bar code scanner. Preferably, the identifiers are assigned randomly, or pseudo randomly, to the different options and voters, so that it is impossible (or more precisely very unlikely) to guess which identifier is assigned to a specific option for a specific user. It may be noted that the identifiers for the same option need not be different for all voters. Some voters may have the same identifier for one or more option. This is no problem as long as it is impossible to know which voters have the same identifiers.

[0008] Preferably, the identifier entered at the user interface is encoded with a signature adding device such as a smart card to make it possible for the vote collecting system to ensure that the vote really involves the identified voter. However, for protection against fraud by a virus this is not strictly necessary, since the use of the individualized ballot form already provides protection against fraud in this case. The signature adding device provides protection against voting after theft of the ballot form.

[0009] Preferably, the ballot form is sent to the voter outside the channel through which the identifier is sent back. For example, the ballot form is a paper form sent by normal mail, the identifier being sent back via a computer network like the Internet. Thus, the risk that a virus can access the ballot form to commit fraud is minimized. In principle, the invention can even be applied to votes where there is only a single voter.

[0010] In an embodiment, a closing identifier is included in the ballot form. When it receives the closing identifier the vote collecting system makes the vote final, foreclosing any possibility of changing the vote. Before

the closing identifier is received, the voter may change his or her option, by sending the identifier for a different option to the vote collecting system. The vote collecting system will count the vote only for the option corresponding to the last received identifier. The closing identifier reduces the possibility of fraud by tampering with the vote after it has been cast.

[0011] Preferably, the closing identifier is included in a paper ballot form under a removable seal, which may be scratched out for example. This makes it possible to use the ballot form at a conventional ballot station as well. In this case, the officials at the ballot station should accept a vote from the voter only if the closing identifier on the ballot form has not been made accessible. Thus it can be ensured that no votes are entered into the ballot box for which electronic votes have already been finally cast.

[0012] In another embodiment the vote collecting system is arranged to send a confirmation message back to the user after receiving an identifier. The confirmation message identifies the option selected by the voter. Preferably, the confirmation message is sent prior to reception of the closing identifier. Thus, the voter is able to check whether the correct vote has been registered by the vote collecting system prior to finalizing the vote by sending the closing identifier. The confirmation message is sent for example by fax or telephone, to a telephone number specified by the voter during the vote.

[0013] In a further embodiment, the ballot form contains an opening identifier and the vote collecting system is arranged to accept votes for the voter only after receiving the opening identifier from the ballot form of the voter. Thus, it is ensured that someone without the ballot form can try to start casting votes for the voter.

[0014] The invention also relates to a voting process that uses the system according to the invention and a set of ballot forms for use in such a voting process.

[0015] These and other advantageous aspects and advantages of the system, method and set of forms according to the invention will be described in more detail using the following figures.

- Figure 1 shows communications between a voting authority and a voter
 Figure 2 shows a voting system
 Figure 3 shows communication between devices in a voting system
 Figure 4 shows a ballot form

[0016] The invention uses a protocol - called VSVPP for Voter-Side Virus Protection Protocol - for protecting electronic voting mechanisms against viruses that may be active on the computer of a voter. This protocol makes it extremely unlikely that such a voter-side virus can disrupt the voter transmitting the intended vote to the (on-line) voting authority, without detection. And in case such a disruption is detected, a new attempt on another computer can be made, or an ordinary vote can

be cast in a physical voting station.

[0017] Figure 1 illustrates messages 10, 12, 14 involved in the VSVPP protocol. The VSVPP involves multiple messages 10, 12, 14 between the voting authority (VA) and each individual voter (abbreviated as IV), which is assumed to be a human being. These messages will use the following three channels, in the given order.

- 10 - Ordinary mail. This is used for sending a message 10 with a special ballot paper (or poll card) from the VA to each IV.
- A Computer network. This is used for the electronic communications 12 between the VA and the IV, and in particular for transferring the actual vote from each IV to the VA.
- 15 - Phone connection, possible wireless. This is used for transmitting a confirmation 14 of the vote from the VA to each IV who cast his/her vote via the computer network.
- 20

[0018] Transfer of messages 14 that include the electronic vote is indicated by multiple arrows, because this may involve multiple messages.

- 25 [0019] The key idea behind the VSVPP is to use a large collection of special identifiers to denote the possible options in an election. For each IV there is a unique subset of identifiers, in a one-one-correspondence with the options that is only known to the VA, and that is printed on a special ballot paper that is only usable by the IV. A virus that tries to influence the outcome of a vote will have to change identifiers. But since the correspondence between identifiers and options (for each IV) is a secret, the virus cannot change identifiers in a goal-directed manner - so that a particular option results.
- 30
- 35

VSVPP Assumptions

- 40 [0020] Preferably, the VSVPP works under the following assumptions.

- There is an unspecified computer network, such as the Internet or a company network or some other network, which enables exchange of electronic messages between the VA and IVs, in both directions. There is no assumption that the computer network is reliable. For example, it may lose messages, or messages may be altered when transported by the computer network.
- 45
- 50 - A vote is a special but unspecified message from an IV to the VA. It may for example contain a choice for a candidate or for a certain course of action, or something else. If a vote is transported from an IV to the VA via the computer network, it is called an electronic vote. Such a vote is typically encapsulated or encoded, so that it cannot be read or modified by others (than IV and VA), see below.
- 55
- The actual processing of the votes that have been

- received by the VA - e.g. in order to determine the end result - is outside the scope of the VSVPP.
- The VA is in control of voting stations whose purpose is to collect votes. There are both on-line voting stations connected to the computer network, and physical voting stations, where an IV can actually go to in order to cast his/her vote.
 - Each IV is known to the VA. The VA knows the ordinary mail address of each IV.
 - Each IV who wishes to cast an electronic vote is in possession of a (tamper-resistant) Individual Computing Device (abbreviated as ICD), such as a smart card, or an ibutton, or something else. Each ICD belongs to precisely one IV, called its owner. Each ICD carries a (electronic / digital) signature (or key), which enables the VA to link the ICD to its owner. Access to an ICD by others than the owner may be prevented via a Personal Identification Number (PIN), or via biometric identification, or via other such means.

[0021] For example, the secret key in an ICD may be the private key in a key pair <private key, public key> associated with the IV, as used in public-key cryptography; in this case the VA knows the (publicly known) link between IVs and their public keys, and can thereby link an ICD to its owner.

[0022] ICDs may be distributed as general citizen identity smart cards, or as company cards, or as something similar. Their use need not be restricted to just one election.

- An ICD need not have an interface for direct communication with its owner. But it can be connected to a so-called host computer (or HC, for short). This may for instance be a personal computer at the home or work of an IV, with an Internet connection and a smart card reader. The HC is assumed to:

- 1) be connected to the computer network, so that it can send and receive messages;
- 2) provide an interface for the IV to communicate with the IDC (via the HC);
- 3) enable the IDC to send messages to the VA and receive messages from the VA, via the computer network (and via the HC).

[0023] Figure 2 depicts the system used to collect votes. This system contains a user interface 10, a host computer 12, an individual computing device 14, a vote collecting system 16 and a memory device 18. There need not be a relation between an HC and an IV, like between an ICD and its owner IV: an IV should be able to use his/her ICD together with any appropriate HC. Also, an HC need not be reliable.

[0024] Figure 3 illustrates the communications within the system of figure 2. An IV casts an electronic vote by means of entry of an identifier at the user interface 2,

which performs a communication 31 by communicating the appropriate identifier for the vote via the HC 22, which performs a communication 32 of the identifier to the IDC 34, which performs a communication 33 back to the HC 32. The host then performs a communication 34 to the vote collecting system 26. The HC is assumed to be equipped with software which can (seem to) perform these transmission tasks, with appropriate input and output facilities (typically with keyboard and screen), as part of the interface with the IV.

- The secret signature (or key) on the ICD is used for encoding and decoding messages on the ICD. Via such en-/decoding the ICD and VA can exchange encapsulated messages which (in principle) no-one else can read or modify - unless the secret signature on the ICD is compromised. Thus the integrity of messages 12 sent between the VA and ICD via HC is guaranteed. The VSVPP does not prescribe which kind of encoding/decoding should be used in order to ensure the integrity of communication between ICDs and the VA.
- An election is an event when IVs may send their votes to the VA. An election has a beginning and an end. The voting stations under the control of the VA are open to receive votes from the beginning until the end of the election, but not outside this interval.

Voter-side viruses

[0025] In this context, a virus is a special computer program running on the host computer (HC) 22 that may disrupt the voting process. The HC is then said to be infected. Because the virus runs on HCs that are used by IVs to express their votes, it is called a voter-side virus. The IV need not be aware of the possible presence of a virus on the HC that he/she uses for casting his/her electronic vote. (There may also be viruses on the side of the VA, but they are outside the scope of the VSVPP).

[0026] A concrete example scenario is the following. Voters are given the chance to decide on a certain issue by voting 'yes' or 'no'. Before the election begins, a special election-disrupting "yes" virus may spread via the computer network, or via other means, and install itself on many HCs. The presence of such a virus may not even be noticed, because it need only become active during the election, and not before. When, during the election, an IV uses an infected HC to express his/her vote via the HC, the yes-virus may disregard this vote and cause the HC to always pass on 'yes' to the ICD, which passes this yes-vote on to the VA, after encoding it.

[0027] The purpose of the VSVPP is to detect a possible disruption of vote casting by such voter-side viruses. Upon detection of a disruption an IV can retry to cast his/her vote, either by using another (hopefully uninfected HC), or by physically casting the vote in an actual

voting station. Since the VSVPP can detect possible disruptions, it may discourage undermining proper electronic voting.

VSVPP ballot paper

[0028] For convenience we assume that an election involves one or more choices among a number of options, say (option₁, ..., option_n). For such an election the VSVPP prescribes a special ballot paper.

[0029] Figure 4 shows a ballot paper 40 containing the different options of the election. Before the beginning of the election the VA sends by ordinary mail to each IV an individual ballot paper 40, which forms both an invitation to participate in the election and a means to vote. The ballot paper 40 may contain a header 41, with information about the nature of the election, the election date and the voter for which the ballot paper is valid. The information about the kind and date of the election on the ballot is irrelevant for the VSVPP.

[0030] The ballot paper 40 contains entries 44, 46 for the various options in the election. Each entry contains a printout 46 of the election option represented by the entry (for example ycs or no, or the name of a candidate) and a generic printable identifier 44, such as a number, a word, a barcode, or something similar. The number of possible identifiers should be much larger than the number of options. An IV makes his/her choice for an option 46 by passing on the corresponding identifier 44, on the personal ballot paper for the IV, to a HC, which should pass it on to the IVs ICD, so that it can be transferred to the VA, as the vote of IV. This requires that the identifiers 44 related to options 46 should all be pairwise different on the ballot paper, so that the identifier can indeed be used to indicate a choice for individual options 46.

[0031] The listed options are (in principle) the same for all ballot papers of IVs, but the n+2 identifiers should be different between ballot papers 40 for different voters, or at least there should be a considerable number of ballot papers 40 with different identifiers.

[0032] The main point about the ballot paper for a particular IV is that it contains especially generated identifiers for this IV, which are known (only) to the VA. Especially, the relation identifier-option for this IV is known to the VA. Thus, if the VA knows IV, it knows which identifier corresponds to which option. In order to do this, the vote collecting system 26 of the VA is required to keep a secret database in memory device 28 in which this connection between each IV and the pairs (identifier-option) on his/her ballot paper are stored.

[0033] The ballot paper also contains first and last identifiers 42, 48, copies of which are also stored in the vote collecting system 26.

[0034] If the VA guards its secrets, a virus will never know the relation identifier-option for an IV. It will be able to change identifiers in an arbitrary way, but not in an intentional way, so that a specific option appears to be

chosen. Moreover, if the number of identifiers is sufficiently large, there is a very small change that a virus will change an identifier chosen by an IV into another identifier which is actually related to another option for this IV. This is the essence of the protection against voter-side viruses offered by the VSVPP.

The role of the first and last identifiers 42, 48 on the ballot paper 40, called will be explained in the following. Preferably these identifiers 42, 48 are covered (or sealed or stamped) with some removable (e.g. scratchable) layer, for indicating whether this identifier has been read. These covers should be such that, once removed, they cannot be restored without noticing.

VSVPP Voting procedure

[0035] We consider an arbitrary IV with intention to vote in an election, in possession of his/her personal ballot paper, after the beginning of an election, but before the end. The VA organises two options for IV:

1) Non-electronic voting. In this case the IV actually goes to a physical voting station with his/her ballot paper to express his/her vote there, in an unspecified but standard non-electronic way (But a voting station may of course also offer HCs for electronic voting). Such a non-electronic vote is only allowed if the covering of the last identifier 48 on the IVs ballot paper is still there. In this process of voting, a representative of the VA removes the cover, and stores the vote as 'confirmed' in the database of the VA. This removal of the cover of the last identifier 48 is proof that the IV has cast his/her vote.

2) Electronic voting. In this case the IV is assumed to have access to a host computer HC 22, linked as in Figure 2 to the computer network and IV with his/her ICD 24, and equipped with voting software which seemingly regulates the voting process. But note that this software (or the entire HC) may be infected with a virus. The IV then goes through the following series of steps, constituting an (electronic) voting session. If anything at any stage does not work as being described below, the IV should consider this attempt to vote disrupted, and abort the attempt. Then (s)he can either proceed to non-electronic voting as in 1. above, or look for another HC and restart the sequence of steps below.

3) The IV connects his/her own ICD to the HC, and starts the voting software that is assumed to be available on HC - either via downloading (securely) from the web, or via a special floppy from the VA, or via some other way.

4) The IV is asked to remove the cover of the first identifier 42 on the ballot paper, and pass this on to the HC 22, either by typing it on the keyboard in the user interface 20, or by reading it via a barcode reader in that interface 20, or by some other appropriate means.

[0036] The HC 22 passes this identifier 42 on to the ICD 24, which encodes it together with at least the ICD's 24 own identity (more information may be added like a time-stamp or nonce so that this voting session can be identified). The ICD 24 passes the encoded information to the HC 22. The HC 22 sends the resulting message over the computer network to the VA 26. The VA 26 decodes the message, and checks in its database in memory 28 whether the identifier 42 from the ballot box belongs to the IV - whose identity it can derive from the identity of his/her ICD 24. Also, the VA 26 checks that there is no confirmed vote yet for the IV. The VA 26 sends a reply message to the HC 22, containing a unique identification for this voting session, and saying either 'proceed', if the identifier that was sent belongs to the IV and there is no confirmed vote, and 'abort' otherwise. In the latter case the IV is not using the right ballot paper or has already cast his/her vote, and the current voting session is terminated. The step checking of the first identifier 42 is not really essential to the VSVPP, but is included to decrease the chance of disruption. Also, the covering of the first identifier 22 on the ballot paper 40 is not essential; it can only tell the IV whether or not someone has tried to misuse his/her ballot paper.

- Assuming the 'proceed' message is sent by the VA, decoded by the ICD, and displayed by the HC, the IV can proceed to enter, at interface 20 of HC 22, his/her identifier 44 corresponding to the option 46 chosen by IV from his/her ballot paper 40. One or more identifiers may have to be entered, depending on the kind of election that is taking place. At the end of this, the IV also enters the phone (or fax) number at which he/she wants to receive confirmation of his/her vote from the VA 26.

[0037] All this information is passed on by the HC to the ICD, which again encodes it together with an identification tag of this voting session, and sends it via the HC to the VA. The VA decodes this message, and checks that it belongs to a currently running voting session via the identification tag. It looks if the identifier(s) contained in the message really belong to an option - using the relations identifier-option that VA stores for IV in its database. If not, the VA terminates the voting session, possibly after sending an abort message to the ICD. If the identifier(s) match options stored in memory 28 for the IV, these options are stored as the vote of IV. At this stage, the VA considers the voting session to be 'unconfirmed'. This means that it can still be altered, but only as part of a new (electronic or non-electronic) voting session.

[0038] (As described above, the VA checks whether the given identifier(s) really correspond to options for the IV. Such a check may also be done by the ICD, if the VA tells in a previous (encoded) message to the ICD which of all the possible identifiers are appropriate. In this case the ICD can already abort a voting session, and will only

send an acceptable identifier, if any, to the VA. But this alternative is less secure, because the list of appropriate identifiers is secret information, and should not leave the VA. However, it does not affect the main idea of the VSVPP). Also it is not necessary that the database contains the full identifier. Instead it may contain the result of evaluating a "one-way" function (as known from encryption techniques) with the identifier as argument. In this case the one-way function with the identifier as argument is evaluated and the result is compared with the stored information. This allows additional security, since it makes it difficult to cheat even if the virus has access to the database.

[0039] Once the VA has received the identifier and translated it into a valid option, the VA does two things:

- It uses the phone number given by IV to transfer a message (for example voice / fax / sms / other) to IV telling him/her what the option(s) are that are currently stored as his/her vote.
- It sends a message to the ICD asking for confirmation.
- In case the phone message contains the same option(s) that the IV has chosen, the IV removes the cover from the last identifier 48 at his/her ballot paper 40 and enters it to the HC at this stage. The HC passes this identifier on to the ICD, which transmits it securely as part of the current voting session to the VA. Upon successful decoding of this message and successful checking of this last identifier (against the one in the database for IV), the VA consider this vote to be confirmed. It can then no longer be altered.

[0040] This removal of the covering of the last identifier is the physical sign that IV has voted. So it should only be removed at the very last stage, after the phone message coincides with the vote intended by IV. If the covering is still present, the IV can still change his/her vote, or start a new voting session, either electronically or non-electronically.

[0041] An interesting question is what to do with the votes which are still unconfirmed at the end of the election. One option is to discard them, but another is to count them, but only at the end of the election when they can no longer be changed. The latter seems reasonable, but the choice between these alternatives is best decided by the organisers of an (electronic) election. Also, the organisers may want to limit the number of times that a vote can be changed.

Claims

1. An electronic voting system for collecting votes for one or more options from a plurality of voters, the system comprising

- means for generating individualized ballot forms, each for a respective one of the voters, each containing entries for respective ones of the options, each entry containing an identifier, the identifiers being selected so that entries for different options within each one of the forms contain mutually different identifiers, identifiers in entries for equal options in different ones of the forms containing mutually different identifiers;
 - a memory device for storing information about the identifiers entered for different options for different voters in a vote collecting system;
 - a user interface for entering data purportedly representing one of the identifiers from a voting voter;
 - an input device for receiving an identification of the voting voter;
 - a vote translating unit arranged to compare the data with the information from the memory about the identifiers for the identified voter;
 - a vote collecting system to count a vote for the option, if any, that corresponds to the data for the identified voter according to the information.
2. An electronic voting system according to Claim 1, wherein the means for generating individualized ballot forms are arranged to add a closing identifier to each form, mutually different closing identifiers being selected for different forms, the transmitter being arranged to send further data captured from the user interface and purportedly representing the closing identifier to the vote collecting system, the vote collecting system being arranged to allow changes of the vote, but only up to reception of the closing identifier.
 3. An electronic voting system according to Claim 1 or 2, wherein the means for generating individualized ballot forms are arranged to add an opening identifier to each form, the transmitter being arranged to send further data captured from the user interface and purportedly representing the opening identifier to the vote collecting system, the vote collecting system being arranged to enter into a vote reception protocol only upon reception of the opening identifier.
 4. An electronic voting system according to Claim 1, 2 or 3, wherein the vote collecting system is arranged to send a vote confirmation message identifying the option corresponding to the identifier received by the voting system back to the voter upon reception of the identifier.
 5. An electronic voting process for collecting votes for one or more options from a plurality of voters, the process comprising
 - generating individualized ballot forms, each for a respective one of the voters, each containing entries for respective ones of the options;
 - including identifiers in the entries, so that entries for different options within each one of the forms contain mutually different identifiers, identifiers in entries for equal options in different ones of the forms containing mutually different identifiers;
 - storing information about the identifiers entered for different options for different voters in a vote collecting system;
 - sending each ballot form to the voter for which that form was generated;
 - entering data purportedly representing one of the identifiers from a voting voter via a user interface at a remote station;
 - entering an identification code of a voter;
 - comparing the data with the information from the vote collecting system about the identifiers for the identified voter;
 - counting a vote for the option, if any, that corresponds to the data for the identified voter according to the information stored in the vote collecting system.
 6. An electronic voting process according to Claim 5, wherein a closing identifier is included in each of the forms, mutually different closing identifiers being included for different forms, the vote collecting system being arranged to allow changes of the vote, but only up to reception of the closing identifier.
 7. An electronic voting process according to Claim 6, wherein the ballot forms are printed on paper, an area of the form where the closing identifier is printed being covered by a irreversibly removable seal.
 8. An electronic voting process according to Claim 5, 6 or 7, wherein an opening identifier is added to each form, the transmitter being arranged to send further data captured from the user interface and purportedly representing the opening identifier to the vote collecting system, the vote collecting system being arranged to enter into a vote reception protocol only upon reception of the opening identifier.
 9. An electronic voting process according to Claim 5, 6, 7 or 8, comprising sending a vote confirmation message back to the voter from the vote collecting system upon reception of the identifier, the vote confirmation identifying the option selected corresponding to the identifier.
 10. A set of ballot forms for use in a vote for a plurality

of options, each ballot form being for a different voter, each ballot form comprising a plurality of entries, each for a possible option in a vote, each entry comprising an identifier identifying the option, the identifiers for a same option on ballot forms for different voters being mutually different. 5

- 11. A set of ballot forms according to Claim 10, printed on paper, each ballot form comprising a closing identifier covered by an only irreversibly removable seal. 10

15

20

25

30

35

40

45

50

55

8

FIGURE 1

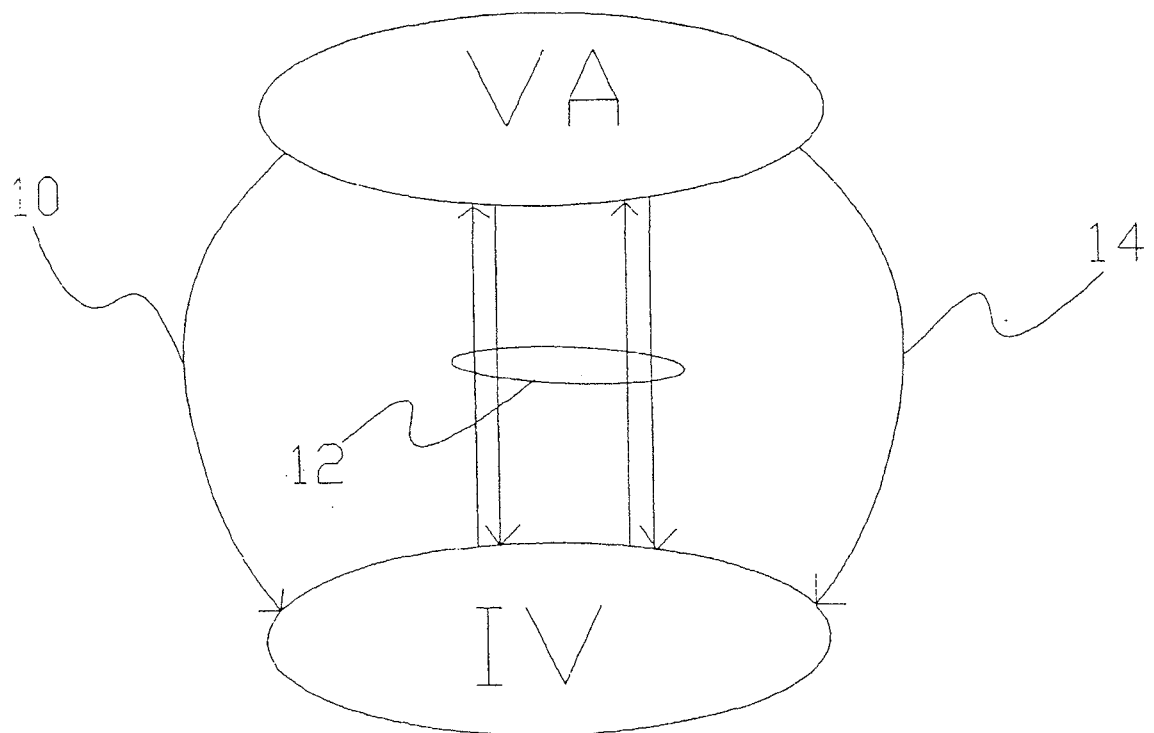


FIGURE 2

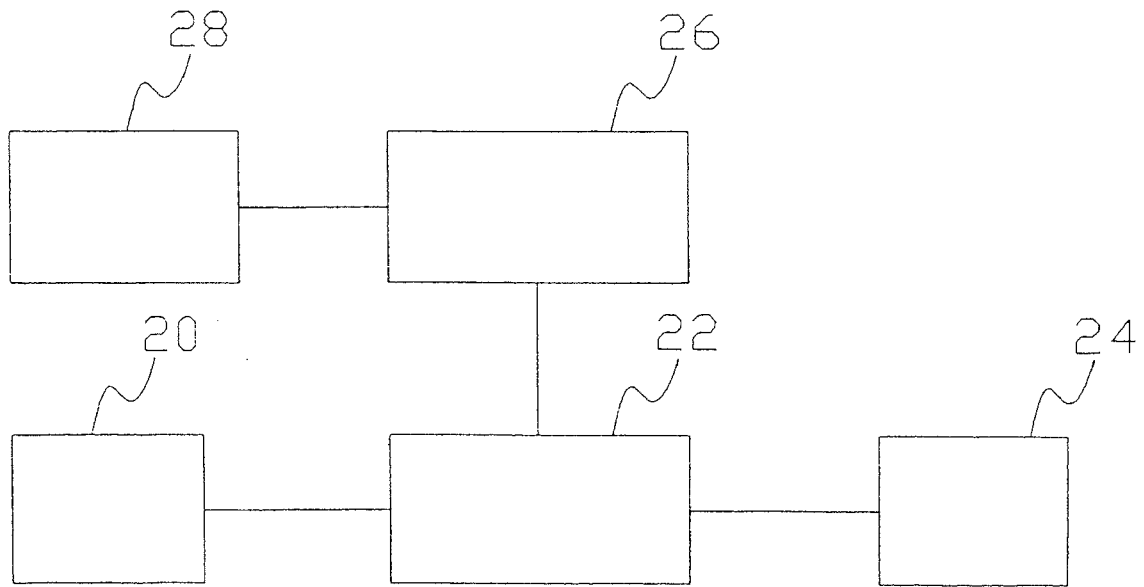


FIGURE 3

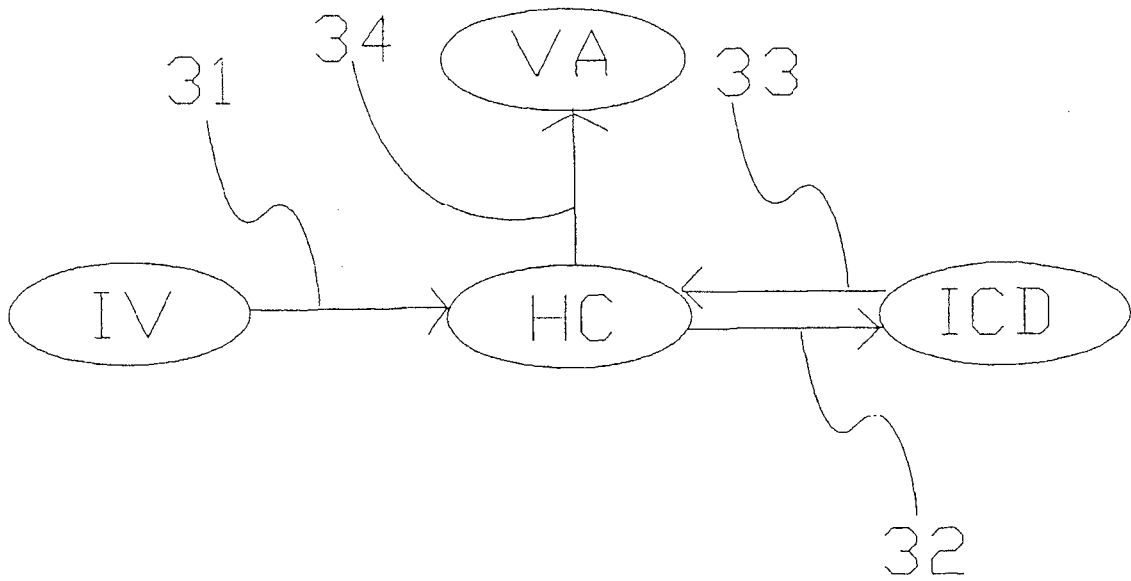
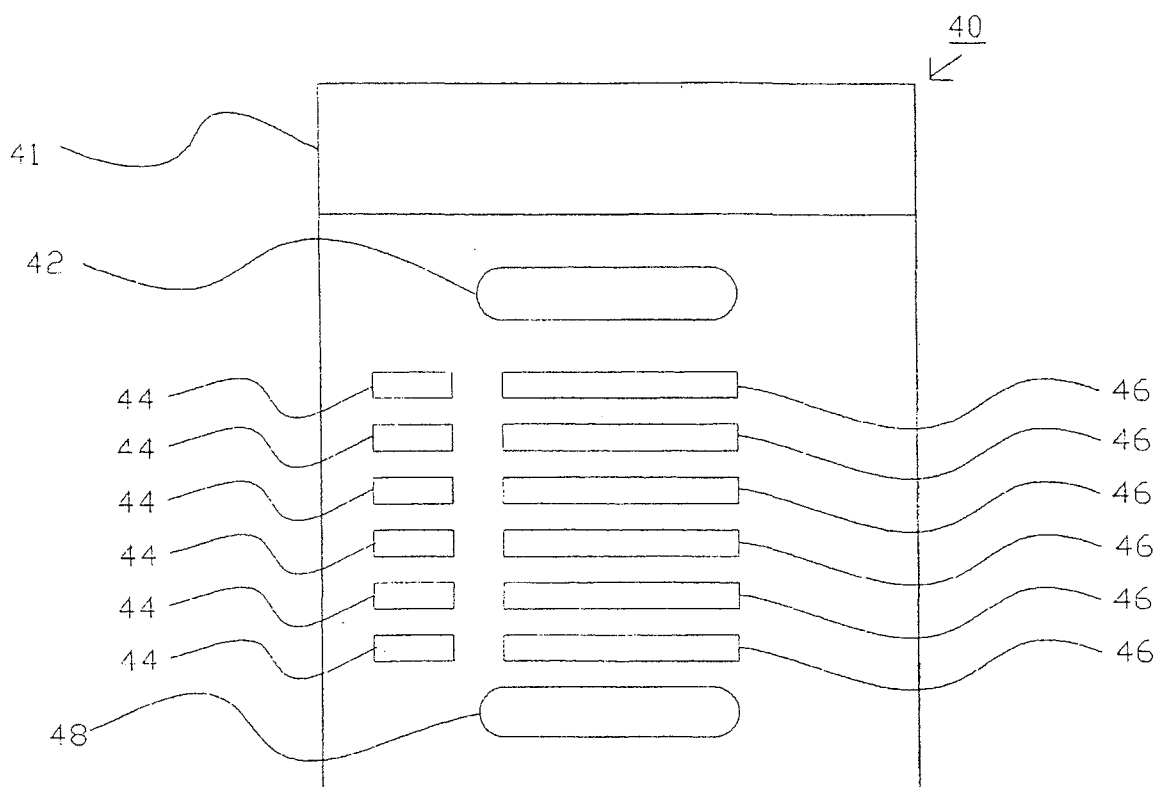


FIGURE 4





European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 20 3355

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 5 875 432 A (SEHR RICHARD PETER) 23 February 1999 (1999-02-23) * column 5, line 58-62; claims 1,5,7,8 *	1-11	G07C13/00 G07C13/02
A	US 4 010 353 A (MOLDOVAN JR MICHAEL TERRANCE ET AL) 1 March 1977 (1977-03-01) * abstract; claim 3 *	2	
A	US 4 025 757 A (MCKAY RICHARD H ET AL) 24 May 1977 (1977-05-24) * abstract *	2	
A	US 6 250 548 B1 (LOHRY KERMIT ET AL) 26 June 2001 (2001-06-26) * abstract *	2	
A	US 5 758 325 A (ROSS ALAN R ET AL) 26 May 1998 (1998-05-26) * column 6, line 58-62 *	4	
A	WO 99 33029 A (WAY IAN) 1 July 1999 (1999-07-01) * abstract *	11	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07C
The present search report has been drawn up for all claims			
Place of search MUNICH		Date of completion of the search 7 December 2001	Examiner Laub, C
CATEGORY OF CITED DOCUMENTS		1 theory or principle underlying the invention 2 earlier patent document, but published on, or after the filing date 3 document cited in the application 4 document cited for other reasons 5 member of the same patent family, corresponding document	
X particularly relevant to taken alone Y particularly relevant if combined with another document of the same category A technological background O non-written disclosure P intermediate document			

EP 1 291 826 A1 (01.02.02)

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 01 20 3355

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on the European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-12-2001

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5875432	A	23-02-1999	NONE	
US 4010353	A	01-03-1977	NONE	
US 4025757	A	24-05-1977	CA 1078065 A1 JP 52126145 A	20-05-1980 22-10-1977
US 6250548	B1	26-06-2001	NONE	
US 5758325	A	26-05-1998	NONE	
WO 9933029	A	01-07-1999	AU 1893499 A EP 1046139 A1 WO 9933029 A1	12-07-1999 25-10-2000 01-07-1999

PAC FORV 12/01/01

For more details about this annex, see Official Journal of the European Patent Office, No. 12/82

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
30 May 2002 (30.05.2002)

PCT

(10) International Publication Number
WO 02/42974 A1

(51) International Patent Classification: G06F 17/60

(NZ). DAVIES, Catherine, Rita [NZ/NZ]; 155 The Esplanade, Petone. 6008 Lower Hutt (NZ).

(21) International Application Number: PCT/NZ01/00238

(74) Agents: CUNNINGHAM, Annette, Jean et al.; c/o Pipers. 29 Waterloo Road, 6009 Lower Hutt (NZ).

(22) International Filing Date: 26 October 2001 (26.10.2001)

(25) Filing Language: English

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(26) Publication Language: English

(30) Priority Data:
508465 27 November 2000 (27.11.2000) NZ
511392 27 April 2001 (27.04.2001) NZ
512918 11 July 2001 (11.07.2001) NZ

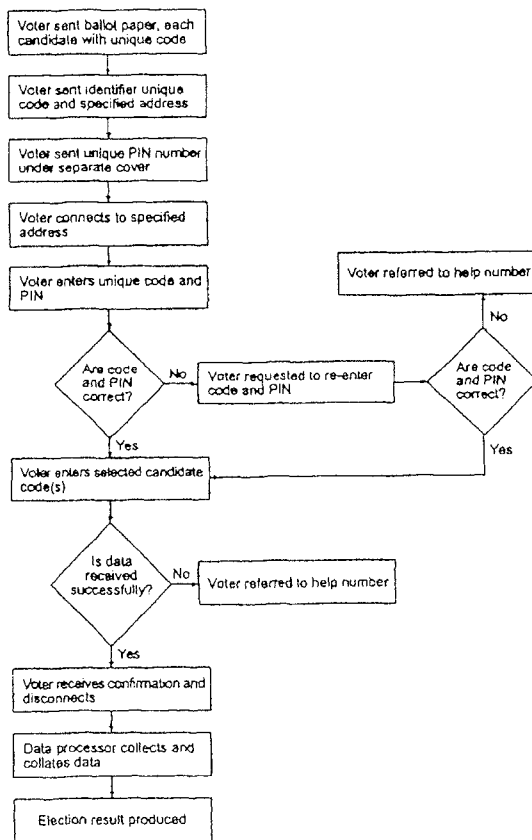
(71) Applicants and

(72) Inventors: REEVES, Bruce, Hasbrouck, Dickson [NZ/NZ]; 155 The Esplanade, Petone. 6008 Lower Hutt

(84) Designated States (regional): ARIPO patent (GI, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: METHOD FOR COLLECTION AND COLLATION OF DATA



(57) Abstract: The invention provides a method of collecting and collating data including the steps of: a) providing each user with an option or question paper where each option or question has a unique transmittable signal or code; b) assigning each user with a unique transmittable signal or code; c) assigning each user a specified address for receiving information to be transmitted by the user by any telecommunications means, or any other means for the transmitting and/or receiving of any signal or code; d) instructing the user to connect to the said specified address and enter the user signal or code, and signal or code or signals or codes for the selected options or questions (the data); e) receiving the entered user data; and f) processing and/or collating some or all of the user data. A computerised data processor is preferably used for receiving and processing the data. The method is particularly suitable for conducting an election, and the preferred telecommunication means is the telephone. Preferably voter identity checks and checks for multiple voting are provided for.

WO 02/42974 A1

0505121



IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— with international search report

Field of Invention

5 This invention relates to a method for the collection and subsequent collation of information, and in particular relates to a method for the collection and collation of information from individuals or collectives and conveyed by way of a telecommunications link to a specified receiving address in such as a census, a survey, a referendum, an election or the like.

10

Background

It is well-known that situations arise where it becomes necessary to receive information from a number of individuals or collectives, and where it is desirable for that information to be efficiently collated for the purpose of achieving a result, or
15 some statistical knowledge. For example, it is the practise of many governments to conduct a census of the citizens of their country for the purposes of planning for the future. Referenda are often conducted by governments or organisations and it is well-known to survey a sample of the population by way of polls and the like to obtain a consensus of opinion.

20

One of the most important events in any country is the conduction of a general election to determine the government for the country, and in most countries and communities the need to elect representatives at all levels of governance is a regular occurrence. Election of representatives, especially at government level, requires
25 receiving and counting the votes of all eligible citizens, and can be an enormous exercise in logistics with respect to providing the means for the votes to be made, and subsequently collating, counting and recording the results of the voters' preferences.

In addition, any voting process, referendum, census, survey or the like, must usually
30 be organised in such a way that it is open, yet secure, and ensures the secrecy of the recorded information. A means should be incorporated for detecting and invalidating the votes of voters who attempt to vote more than once. Usually, in an election, the progress of the results should not be available until such time as the ballot has closed

and voting is complete. However, thereafter it is desirable that a count can be completed as rapidly and accurately as possible.

The process of voting, to date, usually requires voters to attend at designated voting sites, where votes are recorded by way of marking each voter's preference(s) on a prepared voting card or sheet. Prior to the vote being made the voter is identified on an electoral roll, and if that voter attempts to make a second vote this can be traced and the votes consequently invalidated. The cards or sheets are then collected and counted after the ballot has ended. Alternatively voters may be posted ballot papers for completion and return by mail. The tasks of vote counting, and voter identification are laborious and expensive, and are not as accurate as is desirable.

In addition, many votes are not recorded because voters cannot or do not, for a variety of reasons, make their way to the designated voting sites, in spite of the fact that in any election it is always a priority to maximise voter turn-out.

Object

It is an object of the present invention to address the foregoing identified problems, or at least to provide the public with a useful choice.

It is a further object of the invention to provide an improved method for collecting and collating data by way of a telecommunications link, or any other means for the transmitting or receiving of any signal or code, from individuals or collectives to a receiving address or central collecting agency in such as a census, a survey, a referendum, an election or the like.

It is a further object of the invention to provide a telecommunications system in association with a data processing system which is networked and adapted for use in the above improved method of collecting and collating data.

Statement of Invention

According to a first aspect of the invention there is provided a method of collecting and collating data including the steps of:

- a) providing each user with an option or question paper where each option or question has a unique transmittable signal or code;
- b) assigning each user with a unique transmittable signal or code;
- c) assigning each user a specified address for receiving information to be transmitted by the user by any telecommunications means, or any other means for the transmitting and/or receiving of any signal or code;
- d) instructing the user to connect to the said specified address and enter the user signal or code, and signal or code or signals or codes for the selected options or questions (the data);
- e) receiving the entered user data; and
- f) processing and/or collating some or all of the user data.

15

According to a second aspect of the invention there is provided a method of voting including the steps of:

- a) providing each voter with an option paper wherein each option has a unique transmittable signal or code;
- b) assigning each voter a unique transmittable signal, code, or identifier;
- c) assigning each voter a specified address for receiving information to be transmitted by the voter by any telecommunications means, or any other means for the transmitting and/or receiving of any signal or code;
- d) instructing the voter to connect to the said specified address and enter the voter signal or code, and signal or code or signals or codes for the selected option or options (the data);
- e) receiving the entered voter data; and
- f) processing and/or collating some or all of the voter data.

Preferably each voter or user is additionally supplied with a unique transmittable PIN number which must be entered in addition to the unique voter transmittable signal or code.

Preferably the user or voter data is processed by a centralised computer data processing system.

- 5 Preferably the data processing system is enabled to generate a response on completion of the entry of data by the user or voter, to confirm that the data has been processed and the user or voter may now disconnect.

- 10 Preferably the data processing system is adapted to identify the incorrect matching of an entered PIN number with the user or voter unique transmittable signal or code, and to generate a response requesting the re-entry of the unique transmittable signal or code, and the PIN number.

- 15 Preferably the data processing system is adapted to recognise when a user or voter unique transmittable signal or code is entered more than once for the purposes of re-entering selected options or voting more than once, and to invalidate all data entered at any time by that user or voter.

- 20 Preferably a summary of all, or selected portions of the received user or voter data is produced.

- 25 Preferably the user or voter signal or code, and the signal or code, or signals or codes for the selected option or options are entered such as to embrace the selection interactively, manually or via fixed or dynamically allocated means and processes;

- Preferably the user or voter data and selected options are received and recorded manually, interactively, and/or via any automated process.

- 30 By specified address is meant any receiving address to which the user or voter may connect to transfer, by the appropriate telecommunication means, the user or voter signal, code or identifier, and signals or codes for the selected option or options, and if required, the unique transmittable PIN number.

In one embodiment of the invention the telecommunication means is a telephone and the specified address is a telephone number.

- 5 In another embodiment of the invention the telecommunication means is the internet by way of computer, internet enabled phone or interactive TV access, and the specified address is an email address, or website or other suitable receiving site.

- 10 In another embodiment of the invention the telecommunication means is networking-enabled phones and the specified address is a unique address made available by the service provider.

- 15 In another embodiment of the invention the telecommunications means is a voice activated computer enabled to communicate the voice activated selected option to the specified receiving address which may be an email address, website or other suitable receiving site.

- 20 It will be appreciated that while the above known means of telecommunication have been provided by way of example, that any means which enables data to be entered at one location for telecommunication to a receiving address is envisaged as within the scope of the invention. It will be further appreciated that as technology advances other suitable telecommunications means may be developed including any method for the transmitting or receiving of any signal or code. The method of the invention is not to be limited to only those telecommunication means presently available, but is
25 intended to encompass any and all appropriate and relevant advances in technology.

- 30 It is envisaged for example that included within the scope of the invention are all card based applications, interactions and procedures via any communications method whatsoever. This includes magnetic swipe cards, smart cards, chip cards of any sort, transponders or any integrated circuit, RF circuit, micro-processor, stored memory, inducted loop process or technology, any transmitter or receiver process inclusive of bar code, infra-red or laser reader, writer or transmitter.

The means of communications transfer are envisaged as including existing fixed line telecommunications, mobile, cellular, satellite, microwave, radio frequency, or laser transmission or reception. Suitable mediums may include telephonic communications
5 of any sort, copper, xDSL, ADSL, fibre optic, satellite of any sort, cards of any sort, card reader or writer, Point Of Sale (POS), kiosk, internet or personal data transmitter or receiver.

The process of data transmission is envisaged as including any circuit based or packet
10 switching process of any kind.

It should also be appreciated that the method of this invention may be used in association with previously known methods of receiving and recording information, or previously known systems of voting, as, for example, in situations where a
15 referendum, or election is conducted and where some of the users or voters do not have access to the telecommunications systems required to use the method of the invention.

In addition it should be appreciated that the method of the invention may incorporate
20 the use of one, or any number of the above-mentioned means for the telecommunication of data in any one election, referendum, survey, census or the like.

While the following description of the invention specifically relates to voters in a general election it will be appreciated that this is by way of example only, and the
25 method of the invention may similarly be applied to the responding by individual or collective users to other forms of survey or questionnaire such as those described above, and the method of the invention is not to be construed as limited to the recording of votes in an election.

30 EXAMPLE

In this example the method of the invention enables the individual voter to participate in an election from the privacy of their own homes, or any publicly available

appropriate telecommunications system. The option for most voters to vote without having to leave home should have the desired effect of enhancing voter turn-out.

5 It will be appreciated that the uniquely specified addresses to which data is sent will be connected to a computer data processing system which has the appropriate software and hardware for receiving the data, collating, sorting and counting votes, and producing summary results as required. In addition the data processing system should preferably be enabled to generate a response to the voter after all the data has been entered to confirm that the data has been processed, and that the voter may disconnect.

10

The use of a voter signal or code unique to each voter can be readily used to identify any voters who attempt to vote more than once. It is a relatively simple matter, when information is received and processed electronically, to adapt systems to receive information from a signal or coded source once, and once only, and to thereafter
15 extinguish that signal or code so that any subsequent information from that source could not be accepted. Furthermore, any first votes recorded from that source could also be cancelled, should a second attempt to vote by the same voter be detected.

Voter security in this example is guaranteed by way of the voter allocated PIN signal
20 or code. Should any voter fail to supply the correct PIN signal or code allocated to its voter identifying signal or code, no vote would be allowed. Alternatively, if the voter code and PIN number do not match, then in a preferred embodiment of the example a response would be generated requesting that the voter re-enter the voter code and PIN number.

25

Should the laws of the nation or organisation conducting the election allow it, the data processing system of this example would enable progressive counting and reporting on the progress of the election, and as soon as the ballot closes the technology is available to enable an extremely rapid collation, count and reporting of the data
30 received.

It will further be appreciated that the hardware and software for this kind of electronic processing does exist, and can be readily assembled by personnel skilled in this area of computing.

- 5 The preferred example of the invention will now be described by way of example only, in which the forms and instructions referred to are those of Figures 1, 2 and 3.

In this preferred example, preparatory to the voting each eligible voter will be posted an information package which includes:

- 10
- the details of the election to take place;
 - an individual voting form, as shown in Figure 1;
 - an option form which includes a listing of candidates or options which may be voted for, together with any relevant supplementary information. An example of a suitable form is given as Figure 2;
- 15
- a return envelope for the return of documentation which may be used in the event that a recount is required;
 - under separate cover, and after the initial documentation has been posted, but prior to election date, a voter PIN number.

20 By way of specific example a voter (John Doe) receives at some time prior to election day, a mail out including the Forms of Figures 1 and 2. The form of Figure 1 provides:

- 25
- the voter name, 1;
 - the specified address to which voter information is to be sent 2, in this case a telephone number;
 - the voter unique signal or code 3;
 - a space for the subsequent addition of a PIN number 4;
 - electoral information 5;
 - voter information, 6;

30

The form of Figure 2 provides:

- a list of options for voter selection, 7. In this case the options are candidates, but it is envisaged as within the scope of the invention that the options may be of any form, eg choices in a referendum;
- unique signal or code identifiers for each candidate 8;
- 5 • a space for the voter to record the preferred candidate signal or code 9;
- voter information 10.

Subsequent to the receipt of the above forms a second mail out supplies the voter with information as shown in Figure 3.

10

In this embodiment of the invention Figure 3 is a combined form 11, and set of instructions for voting day 12.

15 In the form 11, the voter is notified of its allocated PIN number (supplied in a separate envelope), and a space 13, in which to record this number. In the information portion 12, instructions 14, for voting day itself are provided.

20 The voter can summarise all the information required for voting, on the form of Figure 1, and in one option of the invention this form may subsequently be returned to the electoral authorities for use in a recount, or as required.

25 The voter is then instructed to connect to the designated telephone number, and enter both its identifying signal or code and linked PIN number, and then the preferred candidate signal or code. The voter then waits to receive confirmation that the information has been successfully processed, and disconnects from the address. Should the voter have incorrectly entered the identifying signal or code and linked PIN number it will receive a response prompting re-entry of the code and PIN. Should there be any error in transmission of the data, so that the required confirmation is not received, the voter is referred to the help desk number 15, given on form of
30 figure 1..

A flow chart describing the sequence of events of the method of the invention is described in Figure 4.

It will be appreciated that various departures and modifications may be made on the
5 aforementioned example without departing from the scope of the invention.

CLAIMS

- Claim 1. A method of collecting and collating information data the steps of:
- 5 a) providing each user with an option or question paper where each option or question has a unique transmittable signal or code;
 - b) assigning each user with a unique transmittable signal or code;
 - c) assigning each user a specified address for receiving information to be transmitted by the user by any telecommunications means, or any other means for the
 - 10 transmitting and/or receiving of any signal or code;
 - d) instructing the user to connect to the said specified address and enter the user signal or code, and signal or code or signals or codes for the selected options or questions, (the data);
 - e) receiving the entered user data; and
 - 15 f) processing and/or collating some or all of the user data.

- Claim 2. A method of voting including the steps of:
- a) providing each voter with an option paper wherein each option has a unique transmittable signal or code;
 - 20 b) assigning each voter a unique transmittable signal, code, or identifier;
 - c) assigning each voter a specified address for receiving information to be transmitted by the voter by any telecommunications means, or any other means for the transmitting and/or receiving of any signal or code;
 - d) instructing the voter to connect to the said specified address and enter the voter
 - 25 signal or code, and signal or code or signals or codes for the selected option or options (the data);
 - f) receiving the entered voter data and; and
 - g) processing and/or collating some or all of the voter data.

- 30 Claim 3. The method of either claim 1 or claim 2 wherein the user or voter is provided with a unique transmittable PIN number which must be entered in addition to the unique user or voter transmittable signal or code.

Claim 4. The method of any one of the preceding claims wherein the user or voter data is processed by a centralised computer data processing system.

5 Claim 5. The method of any one of the preceding claims wherein after entering all of the user or voter data the user or voter receives a response confirming that the data has been successfully processed and the user or voter may disconnect from the receiving address.

10 Claim 6. The method of any one of the preceding claims wherein if there is incorrect matching of the user or voter unique transmittable PIN number with the unique transmittable user or voter signal or code the user or voter receives a response requesting the re-entry of the unique transmittable user or voter signal or code and the unique transmittable PIN number.

15 Claim 7. The method of any one of the preceding claims wherein all data entered by a user or voter is invalidated if the user or voter attempts to connect to the specified address more than once for the purpose of re-entering selected options.

20 Claim 8. The method of any one of claims 1, 3, 4, 5, 6 or 7 wherein at least one summary of some or all of the processed and collated user data and/or selected options is produced.

25 Claim 9. The method of any one of claims 2, 3, 4, 5, 6 or 7, wherein at least one summary of some or all of the processed and collated voter data and/or selected options is produced.

30 Claim 10. The method of any one of the preceding claims in which the user or voter signal or code, and the signal or code, or signals or codes for the selected option or options are entered such as to embrace the selection interactively, manually or via fixed or dynamically allocated means and processes.

Claim 11. The method according to any one of the preceding claims in which the user or voter data and selected options are received and recorded manually, interactively, and/or via any automated process.

5 Claim 12. The method of any one of the preceding claims wherein the telecommunication means is a telephone and the specified address is a telephone number.

10 Claim 13. The method of any one of claims 1 to 11 wherein the telecommunication means is the internet by way of computer, internet enabled phone or interactive TV access, and the specified address is an email address, or website or other suitable receiving site.

15 Claim 14. The method of any one of claims 1 to 11 wherein the telecommunication means is networking-enabled phones and the specified address is a unique address made available by the service provider.

20 Claim 15. The method according to any one of claims 1 to 11 wherein the telecommunications means is a voice activated computer adapted to communicate the voice activated selected option to the specified receiving address which may be an email address, website or other suitable receiving site.

25 Claim 16. The method according to any one of claims 1 to 11 wherein the means for the transmitting and/or receiving of any signal or code includes a card, chip or transponder based process inclusive of an appropriate transmitting and/or receiving process.

30 Claim 17. The method according to any one of the preceding claims when used in association with any previously known system for voting or for the collection and collation of data.

Claim 18. The method according to any one of the preceding claims where more than one telecommunications means or any other means for the transmitting and receiving of any signal or code is used.

- 5 Claim 19. A telecommunications system in association with a data processing system which is networked and adapted to perform the method of any one of the preceding claims.

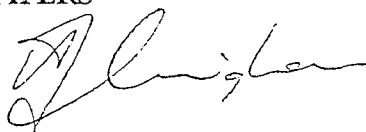
- 10 Claim 20. A method for collecting and collating information or voting substantially as hereinbefore described with reference to the accompanying drawings.

BRUCE HASBROUCK DICKSON REEVES, and

CATHERINE RITA DAVIES

By their Authorised Attorneys

- 15 **PIPERS**



1 3 4 5 2 5

John Doe
 Your telephone booth number is: 04 568 578 373
 Please dial 04 568 578 373 followed by the following numbers:
 123 456 789 001 0 (_ _ _ _) 0001 00012 (_ _ _ _)
 Electoral voters unique Voters PIN Electoral Electorate Candidates unique
 number (e.g. fax number) Code number numbers

If you have entered all the above numbers correctly your vote will be registered and counted.

6 { Did you receive confirmation that your vote has been registered YES / NO
 If YES you need do no more.

If NO please phone the following Help Desk Number: 04 568 578 374 15

N.B. YOU CAN CAST YOUR VOTE BY TELEPHONE ANYTIME
 FROM: 9.00 a.m. on Thursday November 16,
 TO: 7.00 p.m. on Saturday November 17.

FIGURE 1

CANDIDATES:

Candidate Number	Candidate Name	Party Membership
000001	Jane Doe	Republican
000002	Michael Dukakis	Labour
000003	John Anyone	National
000004	Betty Clinton	Democrat

8 { Enter the number of your candidate here: (_ _ _ _) 9

10 { Are you sure that that is the correct number YES / NO
 If NO re-enter correct number
 If YES then transfer this number to your voting sheet in the brackets MARKED CANDIDATES UNIQUE NUMBER.

FIGURE 2

13

11

Enter your PIN number which arrived in a separate envelope in the following space: (_____)

Are you sure this is the correct number, YES / NO
If NO re-enter correct number

If YES then transfer this number to your voting sheet in the brackets MARKED VOTERS PIN.

Your voting slip is now ready for your voting to be registered.
Is this the designated voting day, YES / NO

If NO then wait until the designated voting day has arrived

If YES then proceed to register your vote.

1. Telephone (Television or Computer) connect to your local polling booth phone number
2. Phone the polling booth number listed on your voting form and then enter the full list of numbers listed on your voting form in the order they appear.
3. Wait to listen for confirmation that your vote has been successfully registered.
4. Hang up. Your vote has been cast and will be counted for your selected candidate.

IF YOU DID NOT RECEIVE CONFIRMATION THEN YOU SHOULD CALL THE HELP LINE NUMBER LISTED ON YOUR VOTING FORM.

5. If you have been instructed to return your voting papers then place them in the envelope supplied, seal the envelope and post back to the electoral authority.

NO STAMP REQUIRED.

THANK YOU FOR VOTING AND HELPING TO MAINTAIN OUR DEMOCRACY

FIGURE 3

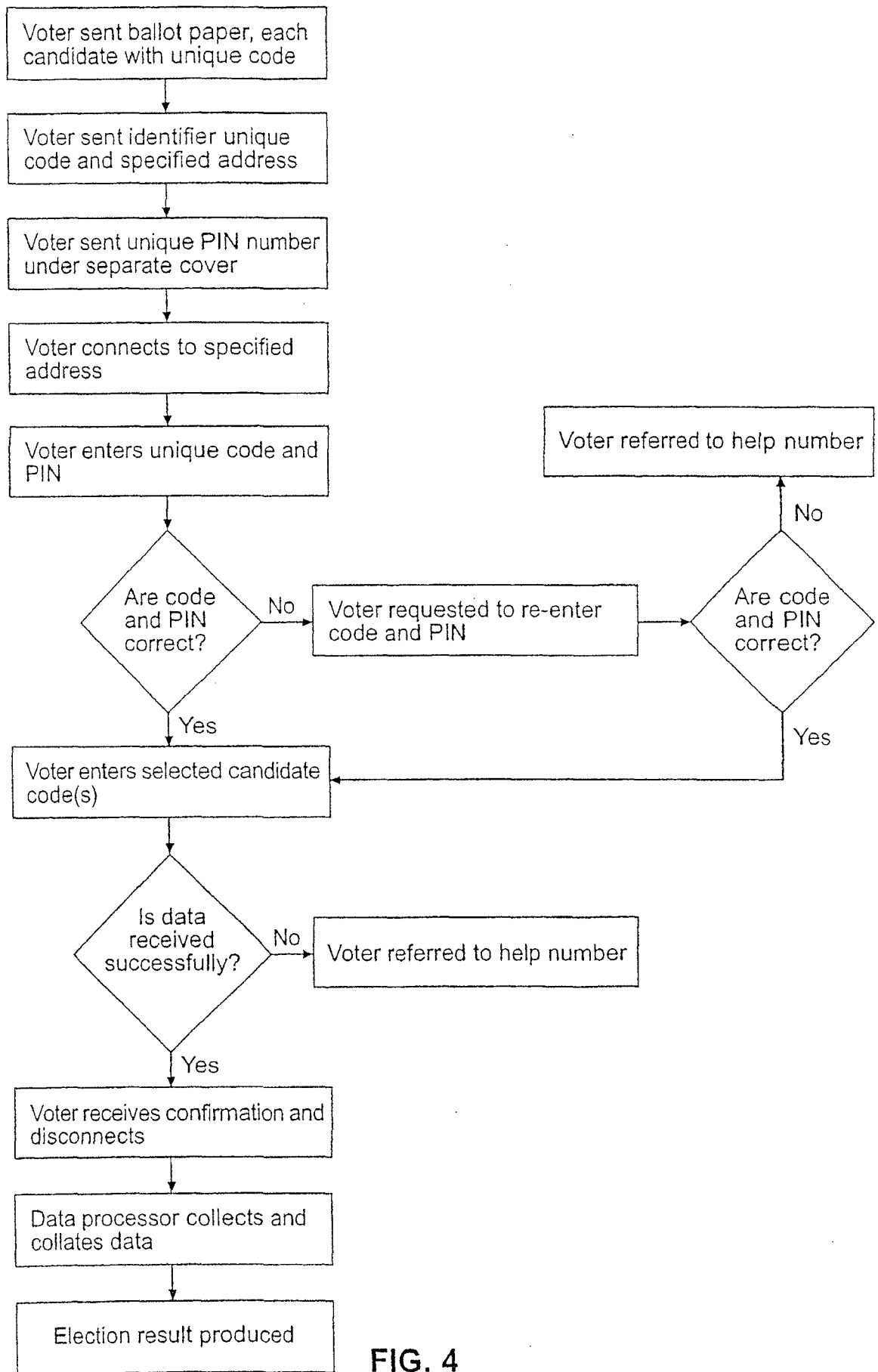


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ01/00238

A. CLASSIFICATION OF SUBJECT MATTER		
Int. Cl. ⁷ : G06F 17/60		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F 17/60 19/00 AND KEYWORDS: VOTE, ELECTRONIC, COUNT, CODE AND SIMILAR TERMS		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6081793 A (Challener et al.) 27 June 2000 Abstract; Figure 1A	1-20
X	US 5898399 A (Peralto) 2 March 1999 Abstract; column 3, lines 44-46; column 5, lines 16-21	1-20
X	US 6021200 A (Fischer) 1 February 2000 Column 1, lines 9-17 and lines 40-53; column 3, lines 20-55	1-20
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex		
* Special categories of cited documents:		
"A"	document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search 21 December 2001		Date of mailing of the international search report 4 JAN 2002
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustrialia.gov.au Facsimile No. (02) 6285 3929		Authorized officer ROSEMARY LONGSTAFF Telephone No : (02) 6283 2637

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/NZ01/00238

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Derwent Abstract Accession No. 1999-454220, JP 11191131 (YAMAHA CORP.) 13 July 1999 Abstract	1-20

Form PCT/ISA/210 (continuation of Box C) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/NZ01/00238

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	6081793	NONE					
US	5878399	NONE					
US	6021200	CN	1151554	EP	763803	FR	2738934
		JP	9179923	ZA	9607111		
JP	11191131	NONE					

END OF ANNEX

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
1 May 2003 (01.05.2003)

PCT

(10) International Publication Number
WO 03/037008 A2

(51) International Patent Classification: H04Q 7/24

(21) International Application Number: PCT/KR01/01947

(22) International Filing Date:
15 November 2001 (15.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2001/59469 25 September 2001 (25.09.2001) KR

(71) Applicant and

(72) Inventor: LEE, Eun-Woo [KR/KR]; P & P Research,
7th Floor, 63 Bldg, 60 Yeouido-dong, Youngdeungpo-gu,
Seoul 150-763 (KR).

(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA,
ZW.

(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,
GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,
NE, SN, TD, TG).

Published:

with declaration under Article 17(2)(a); without abstract;
title not checked by the International Searching Authority

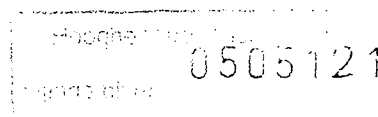
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 03/037008 A2

(54) Title: A SURVEY METHOD UTILIZING MOBILE INTERNET PHONES ENABLED WITH WIRELESS APPLICATION PROTOCOL (WAP)

(57) Abstract:



【DESCRIPTION】**【NAME OF INVENTION】**

A survey method utilizing mobile Internet phones enabled with Wireless Application Protocol (WAP)

5

【BRIEF DESCRIPTION OF THE DRAWINGS】

FIG. 1 is a flow chart illustrating a survey method by utilizing members of mobile subscribers;

10 FIG. 2 is a flow chart illustrating a survey method by utilizing Short Message Service (SMS) sent to panels of surveys;

FIG. 3 describes that how the present invention conducts surveys on its mobile phone display;

15

FIG. 4 shows that the present invention is able to embody a variety of survey questionnaires on its display including even essay-type questions;

FIG. 5 and FIG. 6 demonstrate extended ways of survey methods by utilizing
20 sounds and graphics offered by this invention; and

FIG.7 illustrates "Free survey corner" by which any mobile subscribers joining a membership can create their own survey questionnaires with choices on the present invention to get the results.

[BACKGROUND OF THE PRESENT INVENTION]

The present invention is designed to conduct surveys by utilizing mobile Internet phones enabled with Wireless Application Protocol (WAP) that offers sounds, graphics and moving graphics as well as Short Message Service (SMS). In
5 recent years, the numbers of domestic mobile subscribers are up to 26,895,763(persons) according to the Ministry of Information and Telecommunication in November 2000 following many wireless communication devices, including mobile phones, have spread to people. The number of this coverage is 10.12 percents bigger than conventional telephones.

10

The numbers of mobile Internet phone users was 15,785,000 out of total number of mobile phone users, and the number is on the rise according to the Ministry of Information and Telecommunication in November 2000.

15 So the competition was fierce to dominate the mobile phone market, and accordingly mobile service providers required seeking not just the sound but new telecommunication media in an effort to attract their new subscribers. The demand for new mobile service has led the market to create new mobile phone contents.

20

Therefore all sorts of contents provided by the conventional Internet have moved to the mobile Internet, and the contents have also become diverse. In order to use various mobile Internet contents, we need to have IWF (Inter Working Function) and browsers installed at the mobile Internet devices just like

we need the Internet browsers such as Internet Explorer and Netscape Navigator that help us access the conventional Internet.

There are several kinds of mobile Internet browsers such as ME (Mobile Explorer) produced by Microsoft in the U.S.A., i-mode by NTT DoCoMo in Japan and Anyweb by Samsung in South Korea. However, the browsers can be classified into two types--HTML (Hyper Text Markup Language) and WAP (Wireless Application Protocol)--in terms of their languages written at mobile Internet devices.

10

We adopted a mobile Internet phone utilizing Wireless Application Protocol (WAP) to embody the present invention because that device is able to provide many advantages: first, we can embody the most appropriate mobile contents, comparing to HTML type of language; second, there are many companies manufacturing WAP-based mobile Internet devices such as UP, AUR, Ericsson, Nokia, MSMB and SK Telecom.

15

Since the number of mobile phone users is bigger than that of conventional telephone users, and the mobile device has shifted into a WAP-based mobile Internet rather than just a mobile phone, many survey companies have considered it as important survey method; numbers of sample population is one of the most important factors to survey companies.

20

Mobile Internet has been overwhelming conventional telephone market in

recent years in terms of the number of its subscribers and awakening many survey companies to inform them of an arrival of new survey solution.

Conventionally there have been two kinds of survey methods--the online and
5 offline survey. For example, the Internet survey utilizing the conventional wired
Internet is a kind of online survey, while offline surveys include an interview, a
focus group interview, a telephone survey and a mail survey etc. The most
appropriate survey method to get the fastest and accurate results has been
considered as an online survey utilizing the Internet following the advent of wide
10 spread use of the Internet. Through this survey method, a survey company is
able to instantly collect answer data from its samples and analyzes them.

But online survey has had two disadvantages--limits in its time and space. All
the respondents participating in a survey must sit in front of computers to
15 access the survey corner and answer to the questionnaires almost at the same
time. That way, survey companies can get the results during a specific survey
duration.

Because of the previous inconveniences, a new survey solution called a mobile
20 survey enabled with Short Message Service (SMS) has emerged to solve the
problems even though it seemed to be very similar to a conventional telephone
survey in terms of its survey solution.

A mobile survey is the same as the present invention with regard to sending

Short Message Service to its subscribers in order to request a survey. But this invention does not conduct a survey by only utilizing Short Message Service. Even though this invention uses SMS, it just informs participants of an arrival of survey request. If a mobile subscriber wants to take part in the survey, he/she
5 needs to press a "send" button of mobile phones to connect Automatic Response System (ARS) that sends them survey questionnaires with voice. In this way, participants are able to answer to the survey by pressing buttons on the mobile phones.

10 But this survey system limits its users to a specific time and space: (a) the participants cannot give their answers until they completely understand what the question says; (b) the voice message provided by ARS is a limited communication medium in terms of sending and receiving only by voice because some participants might have a problem with hearing.

15

[DISCLOSE OF INVENTION]

There are two survey methods by utilizing this invention in terms of ways of participating in surveys that include: (a) a survey corner that is accessed and answered by mobile Internet subscribers called "Non-panel members" who
20 joined a membership of survey companies as sample population even though they are not obligated to respond to all surveys; (b) a survey corner that is accessed and answered by mobile Internet subscribers called "Panel members" who joined a membership of survey companies as panelists and agreed to answer to all surveys after receiving Short Message Service (SMS).

In addition to that, this invention has other features. The answer data collected from participants is instantly transferred to server computers belonging to a survey company through wired or wireless telecommunication system just after answering to the survey questionnaires. The server computers, then, statistically analyze the answer data on real time to get the instant results, and finally send them to clients who requested the survey.

There are twelve procedures required embodying this invention, which follow:

- (1) a survey company must secure a large number of samples who have their own mobile Internet devices enabled with WAP browser and join a membership of the company;
- (2) a server computer pertaining to a survey company must classify members' individual information into their demographic categories in order to efficiently conduct surveys;
- (3) classifying our members into panels and general members in the process of categorizing by members' demographical information;
- (4) sharing members' information with a mobile telecommunication company and a survey company by transferring members' data each other;
- (5) extracting the most appropriate panels from members' data in conducting surveys based on their information;
- (6) transferring panels' data to a mobile telecommunication company;
- (7) sending Short Message Service to panel members in order to inform them of arrival of survey questionnaires;
- (8) a mobile telecommunication company must store survey questionnaires at its server computers and send them to WAP-based mobile Internet devices for a specific period of time in order for general members to answer to them;
- (9) answer data obtained from members should be stored at server computers

belonging to a mobile telecommunication company; (10) the answer data should be transferred to server computers belonging to a survey company; (11) a survey company must analyze the answer data transferred from a mobile telecommunication company; (12) sending the survey result to client who
5 requested the survey.

A survey company providing the present invention is considered as one of many Contents Providers (CP) belonging to a mobile telecommunication company that utilizes a WAP-based mobile Internet device to provide such services,
10 however, this invention is designed to conduct only surveys. This invention has to follow such procedures to embody its purpose. That way, a survey company can provide its clients with the fastest and accurate results.

[DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS]

15 In order to achieve a purpose of the present invention, we need several stages that include: (1) a survey company must secure at least over 1,000 panel member of mobile subscribers who agreed to respond to all surveys; (2) classifying the members data into demographic categories such as ages, genders and occupations etc.; (3) sharing categorized members' data with a
20 mobile telecommunication company and a survey company via wired or wireless telecommunication; (4) extracting the most appropriate samples from panels' data to carry out specific surveys; (5) a mobile telecommunication company must send SMS (Short Message Service) including Call Back URL to panel members located in specific regions, at the same time; (6) a mobile

telecommunication company must store survey questionnaires at its server computers for a specific period of time and send the survey data to non-panel members' mobile Internet devices in order for them to access the survey corner and answer to that at any time convenient; (7) a mobile telecommunication company must receive the answer data and store it at its server computers; (8) the answer data should be transferred to server computers pertaining to a survey company via wired or wireless telecommunication; (9) a survey company should analyze the answer data by utilizing its statistical analysis program; (10) a survey company must send the survey result to its clients following appropriate procedures required making a refined report.

The disclosed invention will be described with reference to the accompanying drawings, which show important embodiments of the invention.

FIG. 1 describes an operating system of panel research utilizing SMS (Short Message Service) by which a survey company is able to request surveys to its panel members. The SMS is sent to only a panel member who agreed to answer the survey.

First, a WAP-based mobile subscriber (1) should register as a panel member of survey company (2) by accessing conventional or mobile Internet. And there are two methods to register as a panel member that follow: (1) a mobile subscriber must input his/her personal information and agree with articles pertaining to a survey company by accessing a survey company's homepage; or (2) a mobile

subscriber must input his/her personal information and agree with articles pertaining to a survey company by accessing mobile Internet devices.

When the registration procedure is over, members' personal information is
5 stored at server computers of a survey company or a mobile telecommunication company.

In this process, a survey company needs a specific number of members that is necessary to carry out surveys. Appropriate ways to attract the members are
10 promotion events or refunding services provided by a survey company; for instance, giving them out some type of gifts or deducting a specific amount of money from their monthly mobile phone charge by their mileage or point obtained from answering to survey questionnaires.

15 A deduction of monthly mobile phone charge is, particularly, a good method to improve an answering rate or answerers' loyalty to survey questionnaires. This is a good way to attract them comparing to a conventional telephone survey that only demands sample's answers without any refunding service.

20 And a survey company has to specify a refunding service to the members by showing articles as well as their rights and duties before they register as members.

All members' personal information is stored at server computers pertaining to a

survey company as database, and is classified into their demographic information. A survey company extracts (4) the most appropriate samples' data from panel members' data stored at server computers and transfers it to a mobile telecommunication company that eventually sends SMS to the panel
5 members in order for them to be aware of arrival of survey request.

This SMS must include Call Back URL that makes panel members easily access to survey corners embodied in mobile Internet devices. We will find our mobile phones showing the displays like FIG. 3 when we access the survey
10 corner. Then the panel members directly participate in the survey without a certification procedure because they are already certified as panel members by sending SMS.

There are five types of survey questionnaires as appeared in FIG. 4, which
15 include: (1) essay type questions without choices; (2) questions with multi-choices to choose just one answer; (3) questions mixed with both (a) and (b) type; (4) questions with multi-choices to choose more than one answer; (5) questions with two possible choices.

20 Through this invention, a survey company is able to obtain more reliable results by asking various types of questionnaires to its sample population. In some aspects, these types of survey questionnaires are very similar to conventional offline surveys such as telephone surveys or face-to-face interviews etc.

The data stored at the procedure (7) is transferred (8) from a mobile telecommunication company to server computers belonging to a survey company.

- 5 The data transferred to a survey company is analyzed by a social statistics program on real time (9). But the result obtained from the program is just a raw data that does not include any detailed consulting advices. Therefore, a survey company utilizes its consultants and survey analysts to make more detailed and refined report before sending to clients (10).

10

But the present invention does not include the procedure (10) because it can be taken much time and efforts to complete this procedure according to the quality of reports. However, this invention demands the shortest time to get a raw data obtained from panel members, comparing to existing other survey solutions.

15

A panel research ensures the accuracy of survey results because a survey company extracts the most appropriate samples' data classified into their demographic information. And this type of extracted samples' data is very useful for a survey company to conduct specific surveys.

20

FIG. 2 describes the other type of survey method embodying in this invention in which a survey company requests surveys to its non-panel members by providing survey corners embodied in mobile Internet devices. One of the features in this survey method is that non-panel members can access to survey

corners to respond to that at anytime, anywhere convenient as long as the survey duration permits.

All mobile Internet subscribers who want to become members of a survey
5 company can join a membership by accessing conventional or mobile Internet.
And server computers pertaining to a survey company automatically classifies
(3) the member's information into their demographic categories (2) based on
their ages, genders, regions and monthly incomes etc.

10 As for the procedure of joining a membership, articles containing members'
rights and duties as well as promotion events and refunding services are also
shown to mobile Internet subscribers just like a panel research appeared on
FIG. 1.

15 Giving them out some gifts or deducting a specific amount of money from their
monthly mobile phone charge is good examples to attract them.

After acknowledging the articles, the members go to a certification procedure to
identify themselves (2 of FIG. 3) by returning to the first menu (1 of FIG. 3)
20 following joining a membership.

After completing the certification procedure, members are able to choose one of
the surveys to participate in it. There are various kinds of surveys such as CSI
(Consumer's Satisfaction Index), marketing research, public opinion polls and

survey on broadcastings and newspapers (3 of FIG. 3).

But to some specific surveys such as on "the Teenagers' Consciousness" appeared on 4 of FIG. 3 demands specific samples categorized by their demographic information. Only teenagers can participate in this survey. If a participant is not a teenager, he/she cannot participate in the survey and receives error message at the stage of 4 of FIG. 3. The reason for receiving error message is that the participant's personal information stored at server computers does not fit for accessing to the survey corner that is programmed to respond to only teenagers.

So the survey utilizing non-panel members also keeps its accuracy that fits for the purpose of survey. The rest of the procedures are the same as FIG. 1.

FIG. 5 and FIG. 6 describe the most extended ways of surveys by utilizing this invention. One of the features of WAP-based mobile Internet devices is that they utilize new telecommunication media--SMS, graphics, moving graphics as well as voice--to help their subscribers communicate each other or connect them to a mobile telecommunication company and a survey company. It is because this device is basically designed to embody all possible communication media in mobile Internet phones by shifting conventional Internet services to the new device.

A survey company is able to conduct more various surveys by the help of above

advantages that range from a survey on new design to a survey on background music of game (FIG. 5) and (FIG. 6).

FIG. 7 describes that the present invention does not limit its uses to helping its
5 subscribers communicate each other or connecting them to a mobile telecommunication company and a survey company. The uses of this invention are limitless by shaping a cyber space called a mobile community, for instance, just like the Internet community in which members can share their ideas to form opinions.

10

To begin with, mobile subscribers who passed a certification procedure (1, 2 of FIG. 7) choose "Free survey corner" at the stage of 3, then access to "Current Surveys"(1 of 4 on FIG. 7) to check out current conducting surveys or to choose
2 of 4 to create their own surveys by indicating appropriate number of questions
15 and choices as they intended.

After indicating each number for questions and choices, the display creates exact number of blanks and subscribers input their questions and choices in the blanks. When the subscribers complete that procedure, the "Free survey" data
20 they created is stored at 1 of 4 directory. In that way, other members who randomly access to the corner will respond to that. And the subscribers who created their own surveys are able to check the result out any time convenient. But "Free survey" corner does not ensure the accuracy of results or fit for the

purpose of surveys because participants responding to the survey corner only passed a certification procedure that only ensures their membership.

The "Free survey corner" is designed to provide mobile subscribers with a cyber
5 community in which the mobile Internet subscribers share their ideas and information to shape their opinions. Therefore, this corner limits its uses in terms of the accuracy of surveys and promptness to get results.

This invention utilizes all possible communication media such as voice, letter,
10 graphics and moving graphics to carry out surveys. But this invention does not limit its uses to such communication media, as mentioned above. Other possible forms of communication media can be included in the devices by a survey company, a mobile telecommunication company, producers of mobile Internet devices and software providers, if necessary, as long as it does not
15 breach the idea of present invention. Even though the drawings of this invention only introduce a part of its applications, it additionally includes all kinds of surveys as long as it utilizes WAP-based mobile Internet devices within the intention of this invention.

20 According to previous descriptions of the present invention, WAP-based mobile Internet phone subscribers are able to access to survey corners embodied in the devices at anytime, anywhere convenient as long as they hold the devices, or answer to surveys after receiving SMS (Short Message Service) sent by a mobile telecommunication company.

In conclusion, a survey company is able to conduct all kinds of surveys by utilizing the present invention because WAP-based mobile Internet devices can provide its subscribers with every possible communication media by which the subscribers communicate each other or connect to a survey company and a
5 telecommunication company at anytime, anywhere convenient.

10

15

20

【CLAIMS】

What is claimed is:

1. at least over 1,000 mobile Internet subscribers who own WAP-based mobile
5 Internet devices and join a membership of a survey company:
 - (a) at least over 1,000 members are the minimum number of samples that
are statistically required to conduct all kinds of surveys;
 - 10 (b) there are two kinds of methods to join a membership; 1) by accessing to
the registration corner embodied in the Internet homepage pertaining to a
survey company, or 2) by accessing to the registration corner embodied
in the mobile Internet devices pertaining to a mobile telecommunication
company.
- 15 2. promotion events or refunding services to attract the mobile Internet
subscribers as samples belonging to a survey company which include;
 - (a) deducting a specific amount of money from members' monthly mobile
20 phone charge according to their mileage or points obtained from their
responding to surveys;
 - (b) giving them presents or money as compensation for responding to
surveys;

3. all possible communication media in conducting surveys provided by WAP-based mobile Internet devices:

as previously mentioned, the communication media includes voice, graphics, letter and moving pictures, however, it does not exclude other possible communication media that can be embodied in WAP-based mobile Internet devices by utilizing current or future technologies.

4. a method that is able to instantly obtain a survey result in the process of sending SMS through getting the survey result:

in the process of analyzing the survey result, the answer data obtained from members is stored at server computers pertaining to a mobile telecommunication company and is sent to server computers of a survey company through conventional or mobile Internet;

the answer data is analyzed by a social statistics program installed at server computers pertaining to a survey company in order to obtain the survey result;

the survey result is embodied in the Internet homepage pertaining to a survey company or in the display of WAP-based mobile Internet phones pertaining to a mobile telecommunication company;

“the survey result” is not a form of refined report, but just a raw data that is not

properly processed by survey analysts or consultants belonging to a survey company.

5

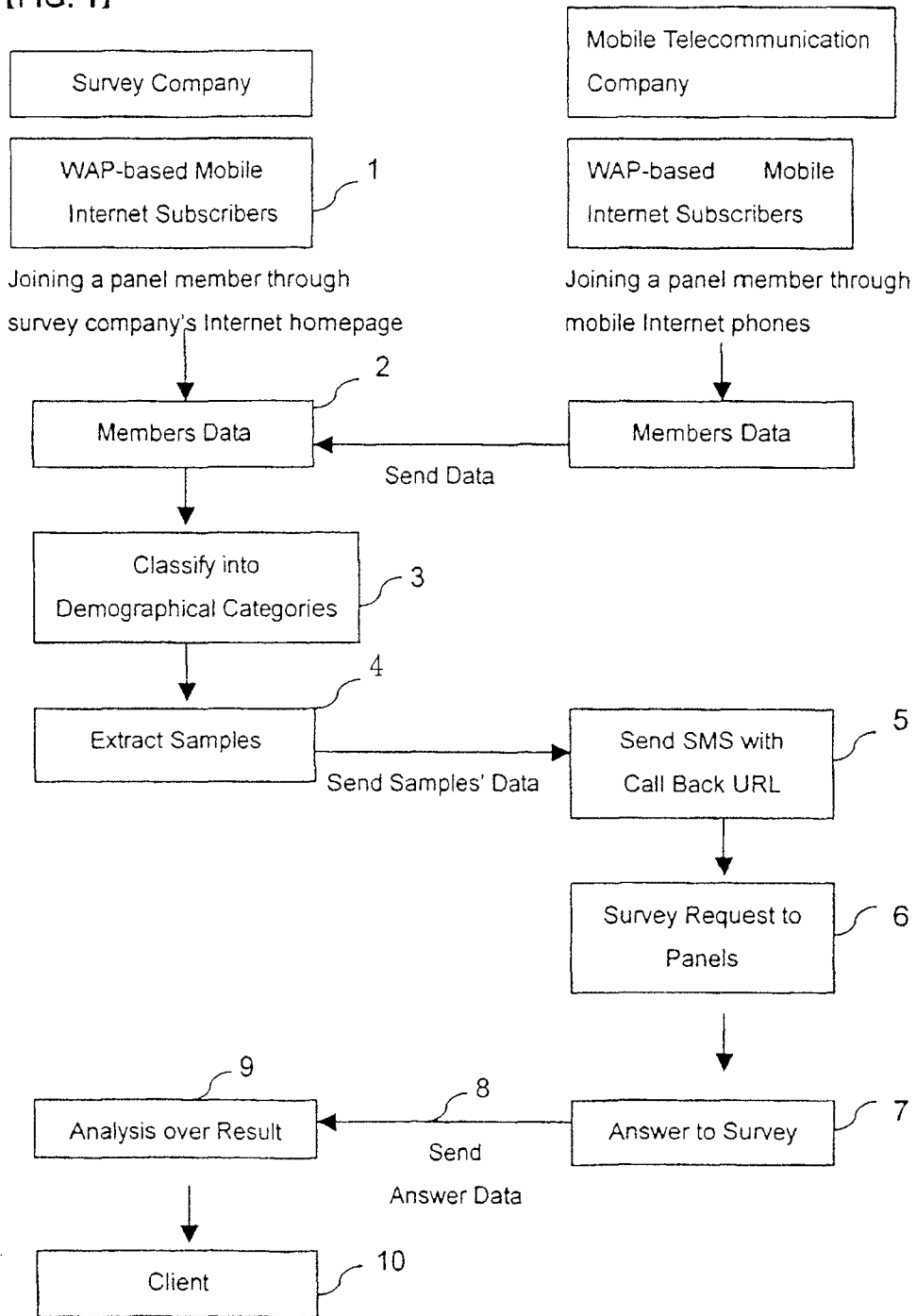
10

15

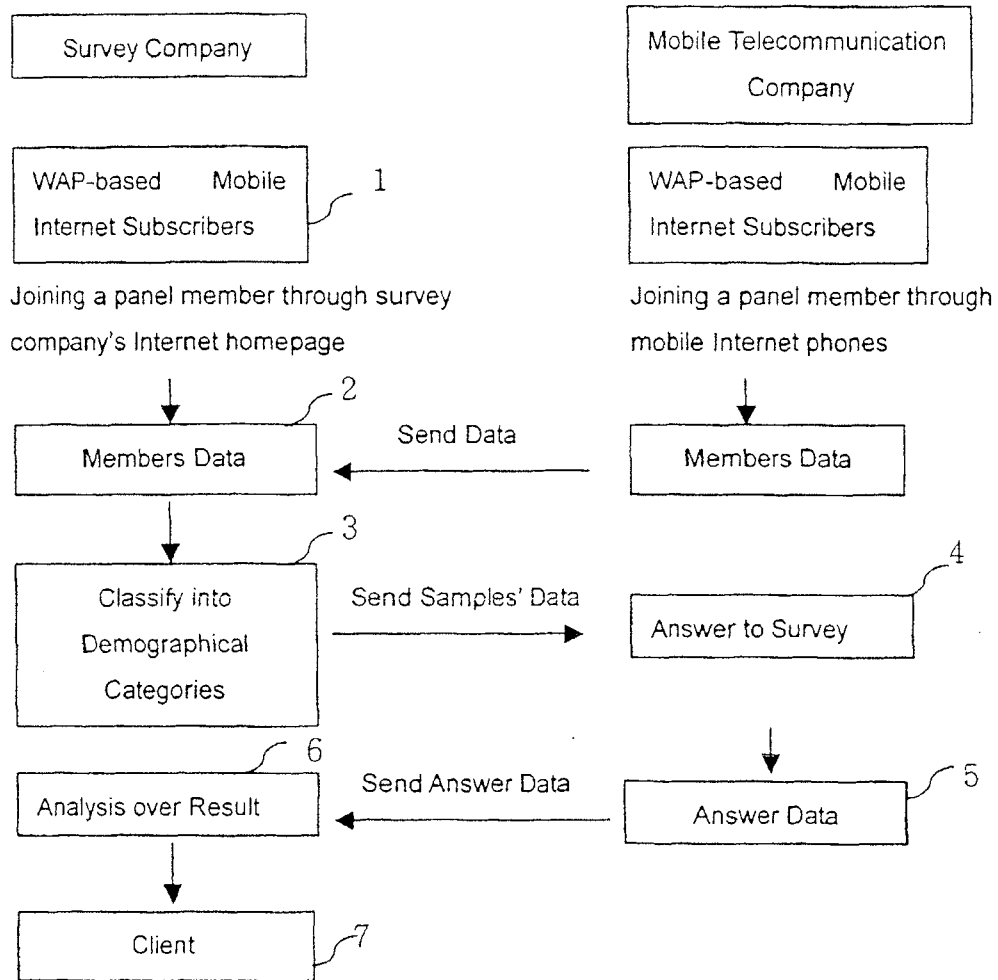
20

[DRAWINGS]

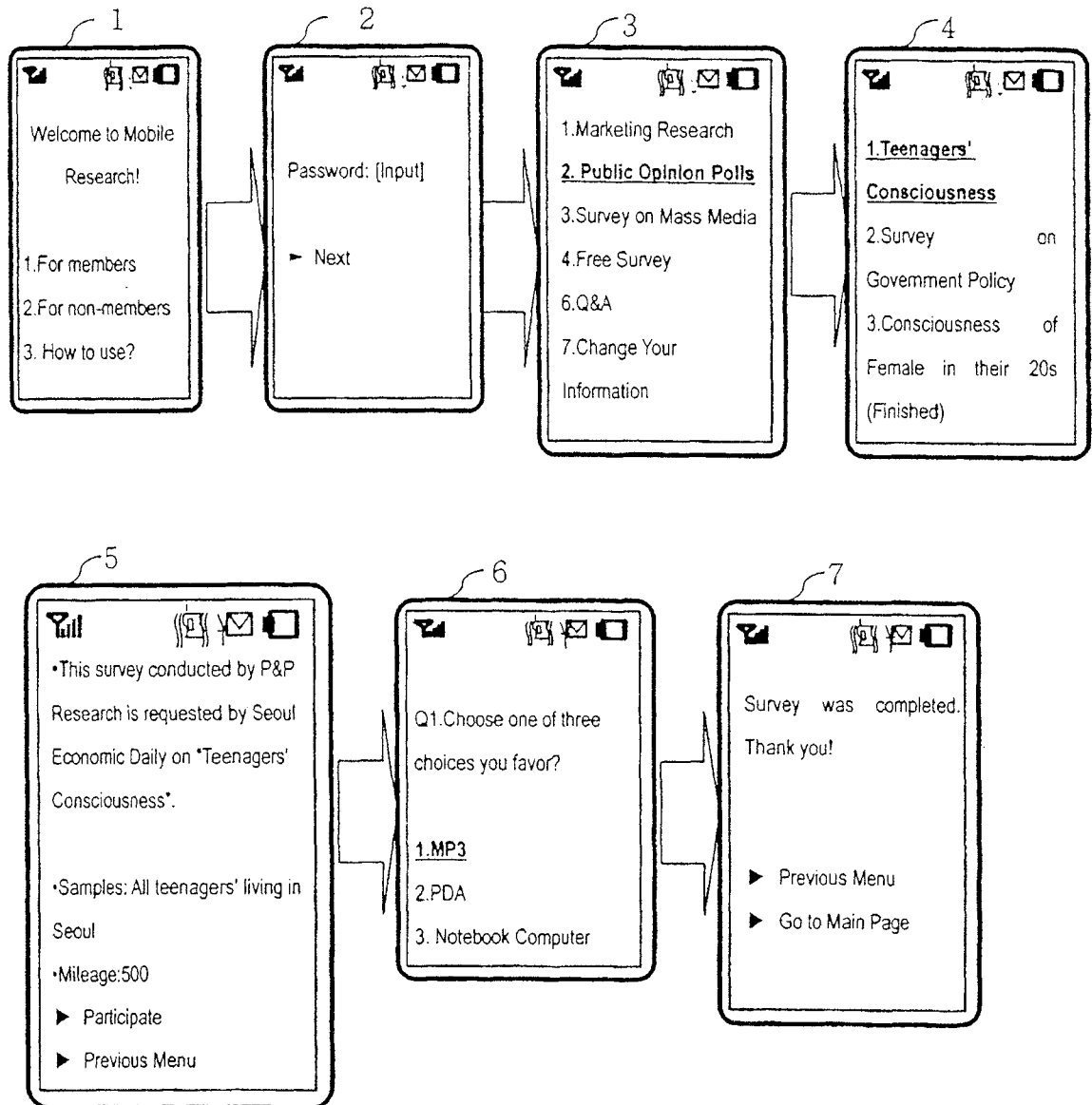
[FIG. 1]



[FIG. 2]



[FIG. 3]



[FIG. 4]

1. Question with multi-choices to choose one answer

Q1. Do you have a refrigerator?

1. Yes

2. No

2. Question with multi-choices to choose more than one answer

Q1. What's the reason of current economic depression?

Company's managerial failure

Government policy

Foreign products

Low in export

▶ Next

3. Essay-type question

Q1. Who is your favorite female model for cosmetics commercials?

[Input]

4. Question Mixed with 2 and 3 type above

Q1. What is your favorite transaction bank?

S Bank

J Bank

K bank

Y bank

Others

▶ Next

Please input other banks if you have any.

[Input]

▶ Next

5. Question with Two Possible Choices

Q1. Have you ever traded stocks?

1. Yes

2. No

1. If you chose "yes"

Q2. How about the result of stock trading?

1. Got profits

2. Lost money

3. No profit no lost

Q3. What do you think about stock trading?

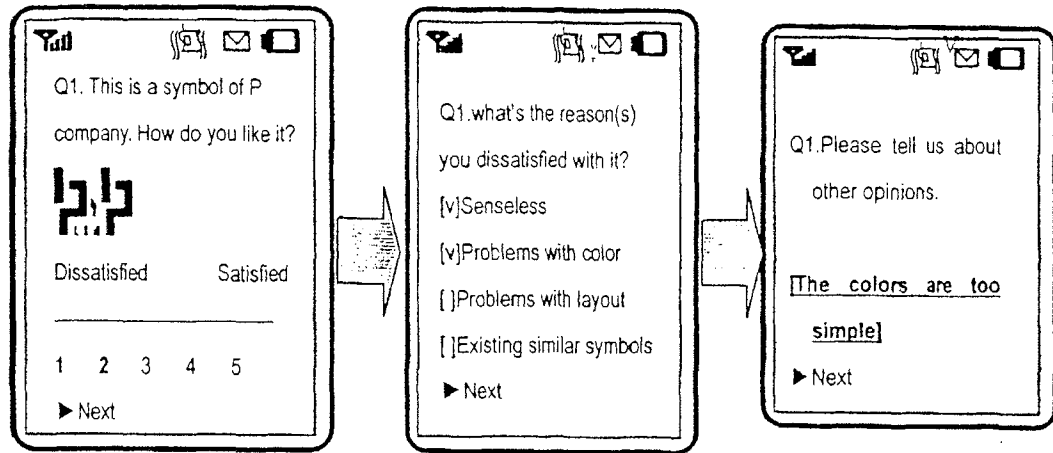
.....

.....

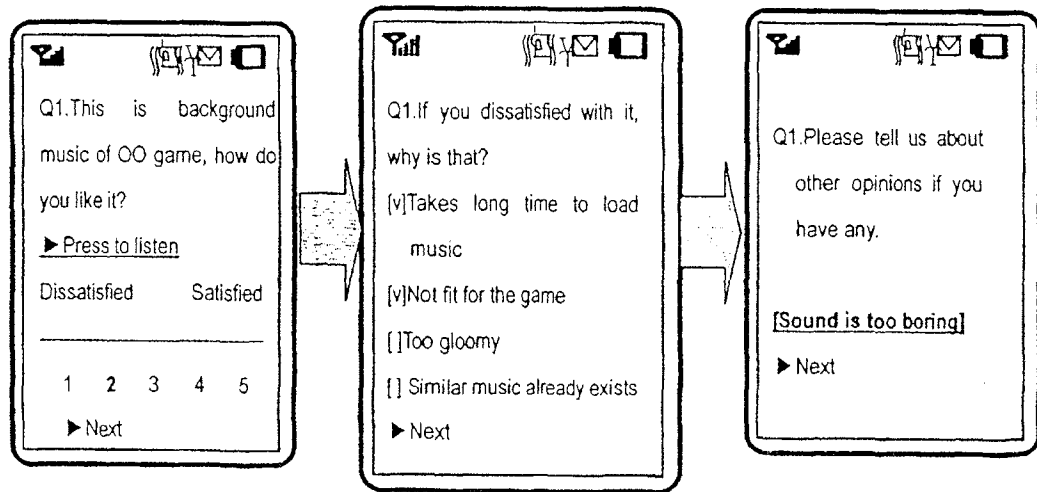
.....

2. If you chose "no"

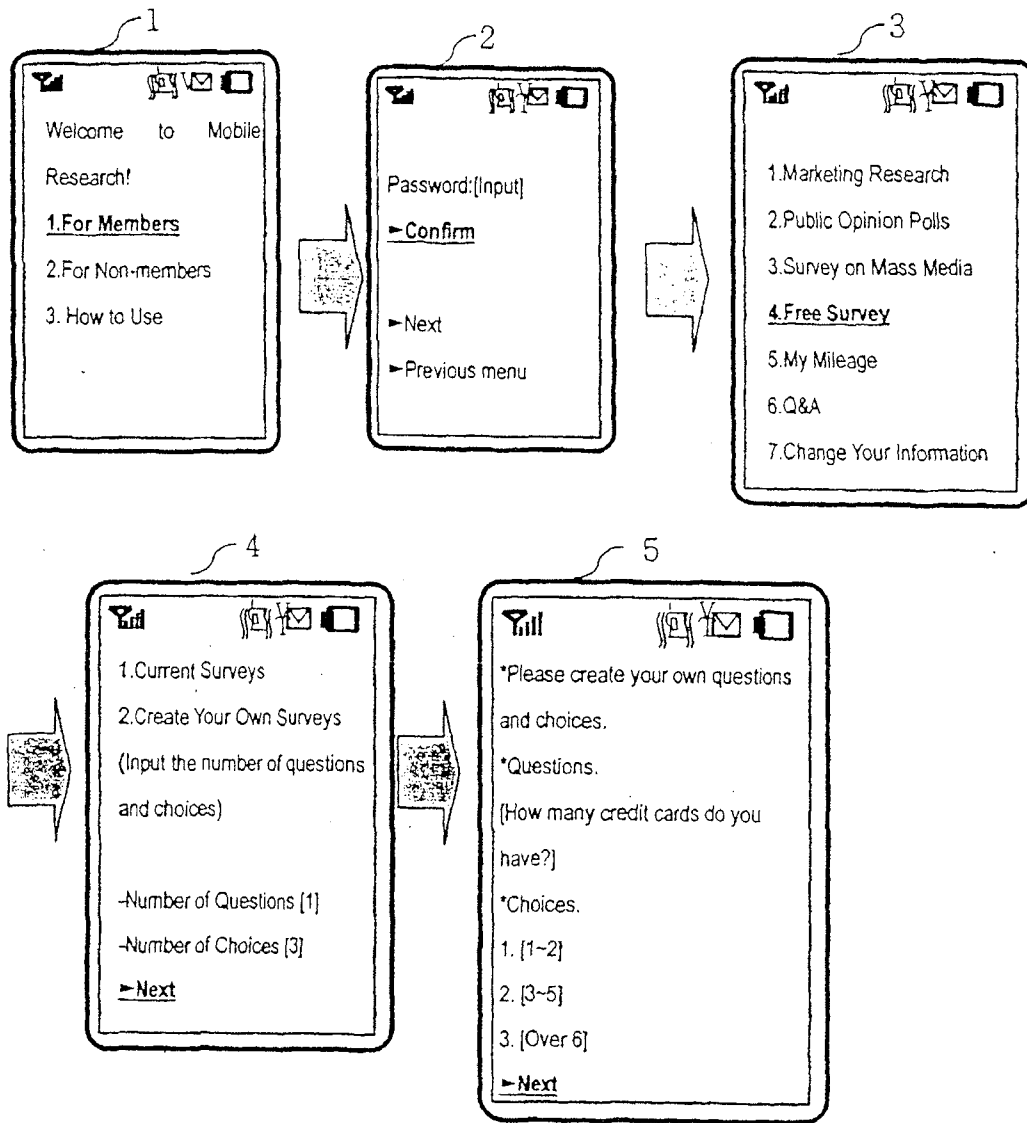
【FIG. 5】



【FIG. 6】



[FIG. 7]



PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT
(PCT Rule 17(2)(a), Rules 13ter.1(c) and 39)



Applicant's or agent's file reference pandp2001	IMPORTANT DECLARATION	Date of mailing (day/month/year) 28 JUNE 2002 (28.06.2002)
International application No. PCT/KR01/01947	International filing date (day/month/year) 15 NOVEMBER 2001 (15.11.2001)	(Earliest) Priority date (day/month/year) 25 SEPTEMBER 2001 (25.09.2001)
International Patent Classification (IPC) or both national classification and IPC IPC7 H04Q 7/24		
Applicant LEE, Eun-Woo		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. The subject matter of the international application relates to:
 - a. scientific theories.
 - b. mathematical theories.
 - c. plant varieties.
 - d. animal varieties.
 - e. essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
 - f. schemes, rules or methods of doing business.
 - g. schemes, rules or methods of performing purely mental acts.
 - h. schemes, rules or methods of playing games.
 - i. methods for treatment of the human body by surgery or therapy.
 - j. methods for treatment of the animal body by surgery or therapy.
 - k. diagnostic methods practised on the human or animal body.
 - l. mere presentation of information.
 - m. computer programs for which this International Searching Authority is not equipped to search prior art.
2. The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

the description the claims the drawings
3. The failure of the nucleotide and/or amino acid sequence listing to comply with the standard for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:

the written form has not been furnished or does not comply with the standard.
 the computer readable form has not been furnished or does not comply with the standard.
4. Further comments:
 Claims 1-2 relate to the methods of doing business, and claims 1-4 are so unclear that the scope of these claims are indefinite, therefore no meaningful search could be carried on said claims.

Name and mailing address of ISA/KR  Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer BAE, Soon Goo Telephone No. 82-42-481-5742 
---	--

Form PCT/ISA/203 (July 1998)



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
 24.10.2001 Bulletin 2001/43

(51) Int Cl.7: **G07C 13/00, G06M 1/00**

(21) Application number: 00830309.1

(22) Date of filing: 21.04.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
 Designated Extension States:
AL LT LV MK RO SI

• **E.I.S. S.p.A.**
 20099 Sesto S. Giovanni MI (IT)

(72) Inventor: **Faita, Marco**
 20092 Cinisello Balsamo MI (IT)

(71) Applicants:
 • **Microflight S.r.l.**
 20092 Cinisello Balsamo MI (IT)

(74) Representative: **Concone, Emanuele et al**
Società Italiana Brevetti S.p.A.
 Via Carducci 8
 20123 Milano (IT)

(54) **Method and apparatus for collecting and transmitting the results of votes**

(57) An apparatus for collecting and transmitting the data of votes includes a central server S connected through a mobile phone network C to a plurality of n portable units U located one in each polling station. Each portable unit U includes a keyboard, a display, a memory and a digital transceiver system and is directly programmed by server S according to the operational coordinates transmitted to the server upon activation of the

unit. During the counting process, the user only has to strike the key corresponding to the value of the scrutinized ballot and as soon as the counting session is completed he can send immediately to server S the relevant results. Thanks to this method of centralized programming and automatic vote counting, both the risks of errors and the time required for collecting and forwarding the data are greatly reduced.

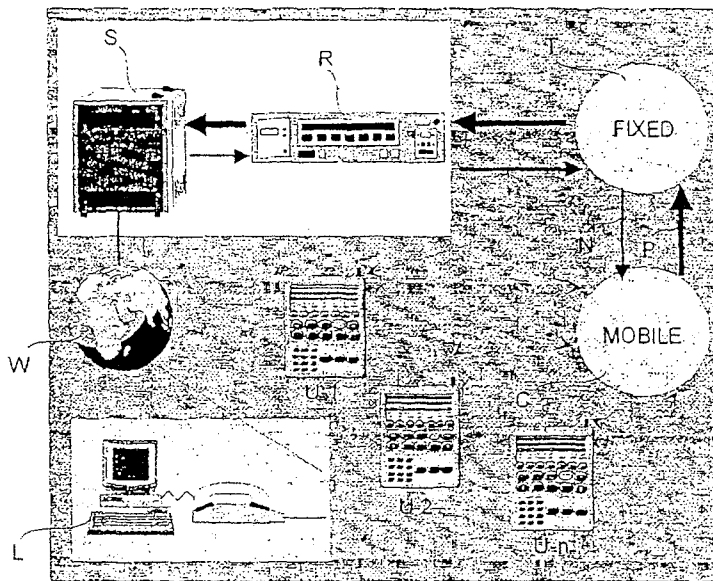


FIG. 2

EP 1 148 447 A1

Hochschulbibliothek
 0505121

Description

[0001] The present invention relates to systems for collecting and transmitting data, and in particular to a method and apparatus intended for collecting and transmitting the data of votes such as elections, referendums, political and commercial surveys, etc. Reference will be made hereafter specifically to the application of the present invention to the counting of votes of administrative elections, but it is clear that what is being said is readily adaptable to other types of votes such as referendums, regional, provincial, municipal elections and the like and to any type of political and commercial survey.

[0002] It is known that, upon conclusion of the voting, inside the polling station there is provided the step of checking and counting the votes, and there is the need to know and list the result of the vote as soon as possible and to transmit it to a data collecting headquarter.

[0003] In practice, this means that during the counting process someone must open the ballot-papers, read their content, assign a value (valid vote, void vote, blank ballot) by declaring it out loud and subsequently recording it in a report, file it and, at the end of the counting session, transmit it outside the polling station.

[0004] This process of collecting, filing and listing the data is carried out completely manually with evident drawbacks as to lengthiness and possibility of errors in the counting and/or in the sending of the results.

[0005] Therefore the object of the present invention is to provide a method and apparatus suitable to overcome said drawbacks.

[0006] This object is achieved by means of a method and apparatus which automatize the process of counting the votes and forwarding the data while leaving to the scrutinizer only the task of assigning to each ballot the relevant value.

[0007] A first evident advantage of the present invention is that it greatly reduces the risk of errors in counting and forwarding the data, in that the only remaining source of error is the erroneous assigning of the value by the scrutinizer.

[0008] Another clear advantage is the greater velocity in collecting and forwarding the data which allows to have the results almost in real time.

[0009] These and other advantages and characteristics of the method and apparatus according to the present invention will be clear to those skilled in the art from the following detailed description of an embodiment thereof, with reference to the annexed drawings wherein:

Fig. 1 shows a portable unit which makes part of the present apparatus; and

Fig. 2 diagrammatically illustrates the complete apparatus and its operation.

[0010] With reference to fig. 1, there is illustrated a

portable unit which substantially includes a keyboard K, a display D, a memory and a digital transceiver system indicated by antenna A, e.g. a GSM module. In particular, keyboard K is preferably of the membrane type and divided into an upper portion including a plurality of programmable function keys F (F1-F7 in the illustrated example) and other operational keys, and a lower portion including a numerical keyboard and three system keys. The use of these keys will be made clear later on upon explanation of the operation of the apparatus.

[0011] As shown in fig. 2, the above-described portable unit makes part of a plurality of n units U located one in each polling station and connected through the transceiver module to a central unit S (server). This connection is preferably achieved through a mobile phone network C, which forwards the transmission to the fixed phone network T to which server S is connected through a router R which handles the lines. The communications from the portable units U to server S are represented by the thick black arrows P whereas those in the opposite direction by the thin arrows N. Also, server S is preferably connected to a global communication network W (typically the Internet) so as to allow access to the collected data also to remote users L.

[0012] The operation of the apparatus above will now be described also with reference to the method devised for the intended object.

[0013] The first step of the present method is the creation of an electronic database, stored in server S, of the lists of all parties, coalitions and candidates which enter the electoral competition, said lists being possibly multiple depending on the voting system in use and on the type of vote. For example, for administrative elections in Italy you would presently have a list of the parties entered in the proportional share of the House of Representatives, a list of the coalitions and candidates entered in the majority share of the House of Representatives and a list of the coalitions and candidates entered in the majority share of the Senate.

[0014] In every list an arbitrary code is assigned to each party, coalition or candidate, according to the various candidatures applied for in each electoral ward and constituency. In this way it is possible to unambiguously identify the corresponding political entity and to add up the vote results of every polling station without possibility of error. Moreover, the preliminary preparation of the electronic lists in a single place, carried out by qualified personnel, eliminates the possibility of making errors in assigning the code to the political entity.

[0015] Server S also stores a list of identification codes of each portable unit U to which corresponding user-settable keywords are coupled. Together with the data relating to the number of the electoral ward and of the polling station, these codes make up the operational coordinates which allow server S to select from the database the pertinent lists to be sent to each unit U.

[0016] In practice, every user in order to be able to receive the electronic lists on his unit U must first input

the relevant user identification code, the keyword, the electoral ward number and the polling station number. This input is carried out by means of the numerical keyboard and "ENTER" key in the lower portion of keyboard K, and once these data have been input it is sufficient to strike the "SEND" key to send them to server S (arrows P). The latter receives and checks the operational coordinates and picks out from its general electronic lists all and only the useful elements and information relating to the desired electoral ward (abbreviations of the parties, names of the candidates for Senate and House, etc.).

[0017] The transmission from server S to unit U (arrows N) of the thus selected lists results therefore in the complete programming of the unit in a simple and error-free way. Each of the F1-F7 function keys is coupled with the abbreviation of one of the parties present in that specific electoral ward, thus allowing to take into account also local or regional parties. It is clear that when the number of parties is greater than that of the available function keys each key will be coupled to more than one party, and the choice of the relevant series of parties will take place through the left/right shifting keys (horizontal arrows). The other keys are used for counting the blank ballots (BLANK), the void votes (VOID) and for the functions of correction, selection, setup, etc.

[0018] During the counting process, the user only has to strike the key corresponding to the value of the scrutinized ballot (F1-F7, BLANK, VOID) and in the memory of unit U there will be an automatic increase of one unit in the number of votes previously stored in relation to the corresponding code.

[0019] This activity is defined "session" and in the course of each vote there may be several sessions, as in the case of counting the ballots relating to the proportional share at the House of Representatives (first session, illustrated in fig.1) or to the majority share at the House of Representatives (second session) or to the majority share at the Senate (third session). At the end of each session, the user can indicate its conclusion through the relevant "END SESSION" key and then proceed to a new session through the "CHANGE SESSION" key, or immediately send to server S the data relating to the completed session through the "SEND" key.

[0020] In the case of void vote it is preferable to show up on display D a list of reasons among which to select the most pertinent (e.g. multiple vote, irregular signs, etc.) so as to obtain an even more accurate report of the count.

[0021] The data collected by all units U-1, U-2, ..., U-n are then forwarded (arrows P) almost in real time to server S which subsequently processes them in order to obtain the results at national, regional, provincial level and the like.

[0022] It is clear that the above-described and illustrated embodiment of the apparatus according to the invention is just an example susceptible of various modifications. In particular, the members making up unit U

may be of any kind suitable for the purpose and/or replaced by other equivalent elements.

[0023] For example, the programmable function keys F could be replaced by a sensitive display of the "touch-screen" type on which the abbreviations of the parties are displayed, and also the other keys could be different in number or have a different arrangement. Similarly, the communication system could be different from a GSM module (e.g. UMTS) and possibly provide a direct connection to server S, e.g. through a satellite link.

Claims

1. An apparatus for collecting and transmitting the data of votes **characterized in that** it includes a central unit (S), containing a database, connected through a telecommunication network to a plurality of portable units (U), each of said portable units (U) including a transceiver system for the connection to said central unit (S), a keyboard (K), a display (D) and a memory which can be directly programmed by the central unit (S).
2. An apparatus according to claim 1, **characterized in that** the connection between the central unit (S) and the portable units (U) is achieved through a mobile phone network (C).
3. An apparatus according to claim 2, **characterized in that** each of said portable units (U) includes a GSM module.
4. An apparatus according to one or more of the preceding claims, **characterized in that** the keyboard (K) of each of said portable units (U) is of the membrane type.
5. An apparatus according to one or more of the preceding claims, **characterized in that** the keyboard (K) of each of said portable units (U) includes a plurality of programmable function keys (F).
6. An apparatus according to one or more of the preceding claims, **characterized in that** the display (D) of each of said portable units (U) is a sensitive display of the "touch-screen" type.
7. A method for collecting and transmitting the data of votes, **characterized in that** it includes the following steps:
 - a) creating an electronic database with all the data relating to the vote, such as lists of parties, coalitions, candidates and so on in the various electoral wards, polling stations and the like;
 - b) assigning a univocal arbitrary code to each record of the database;

- c) creating a list of identification codes univocally corresponding to a plurality of portable units (U);
- d) storing the data of points a), b) and c) in a central unit (S) connected to said portable units (U) through a telecommunication network; 5
- e) sending from each portable unit (U) to the central unit (S) a request for activation containing the operational coordinates of the portable unit (U), which include the identification code and the number of electoral ward, polling station or the like; 10
- f) sending from the central unit (S) to each portable unit (U) a reply to the request for activation containing the instructions for the programming of the portable unit (U) with all and only the data relating to the operational coordinates thereof; 15
- g) increasing by one unit the count of the code mentioned at point b), stored in the memory of the thus programmed portable unit (U), according to the value assigned to each scrutinized ballot; 20
- h) sending from each portable unit (U) to the central unit (S) the total result of the completed counting session. 25

30

35

40

45

50

55

4

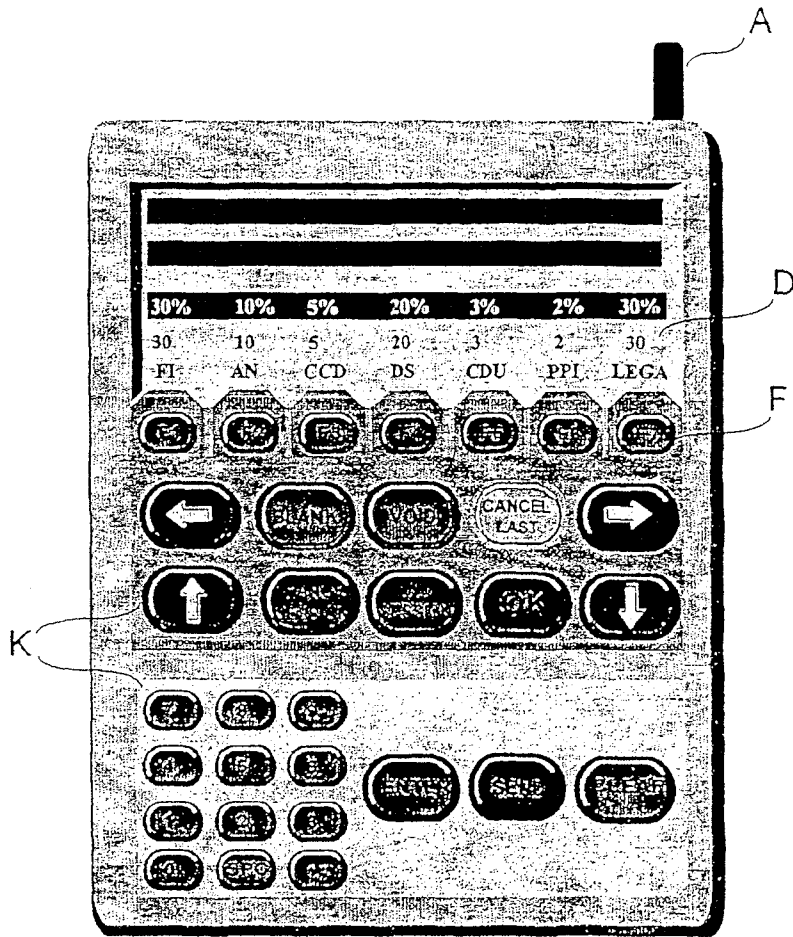


Fig. 1

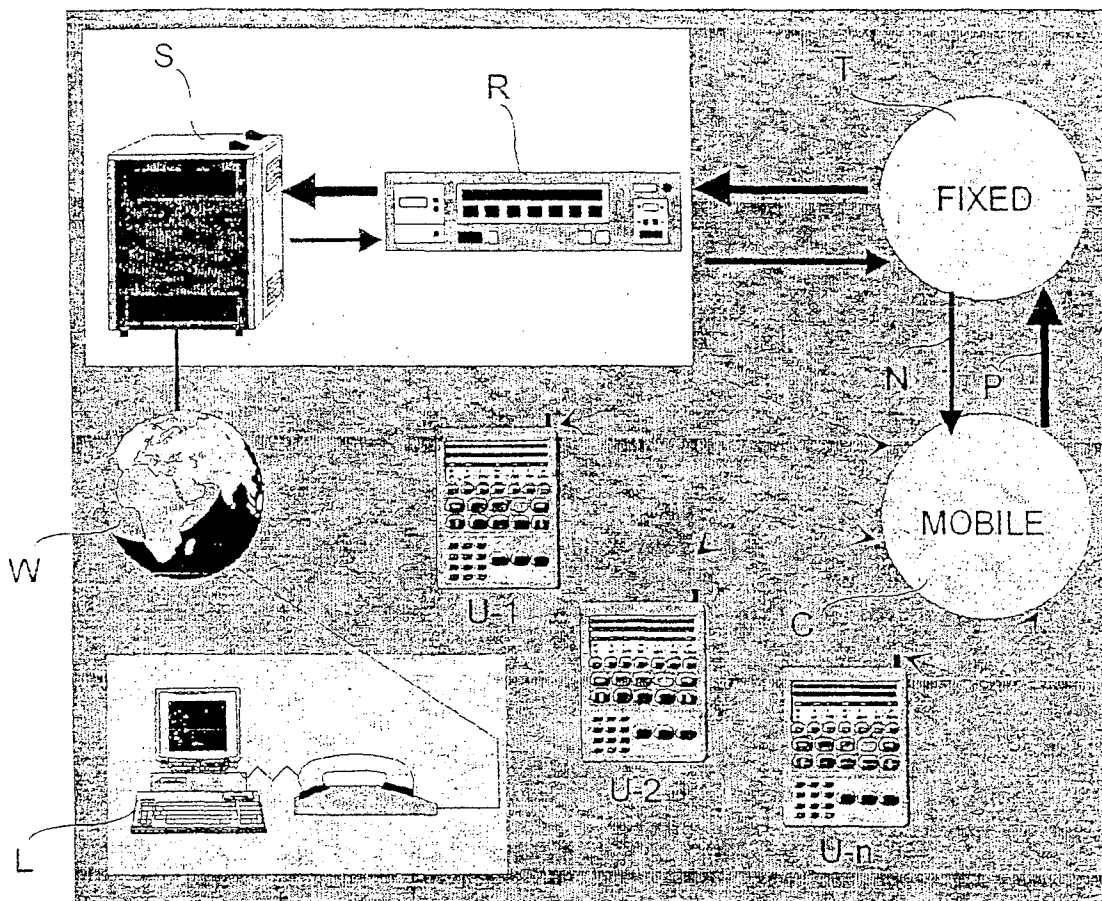


Fig. 2



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 83 0309

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 201 067 A (PARMELEE STEVEN G ET AL) 6 April 1993 (1993-04-06) * abstract; figures 1-4 * * column 2, line 52 - column 3, line 18 * * column 4, line 25 - column 5, line 46 *	1-5	G07C13/00 G06M1/00
A	WO 99 23607 A (INGF I HAGLOEF AB ;HAGLOEF STEFAN (SE)) 14 May 1999 (1999-05-14) * abstract; figures * * page 1, line 29 - page 2, line 11 * * page 4, line 9 - line 13 *	7	
A	US 4 774 665 A (WEBB KENNETH D) 27 September 1988 (1988-09-27) * abstract; figures * * column 3, line 27 - line 63 * * column 4, line 55 - column 6, line 36 *	7	
A	DE 44 46 728 A (MUELLER & LORENZ GMBH) 27 June 1996 (1996-06-27) * abstract; figures 1,5 * * column 3, line 10 - line 42 *	7	
A	US 5 153 826 A (JOHNSON ROBERT) 6 October 1992 (1992-10-06) * abstract; figures 1,2 * * column 2, line 16 - column 3, line 30 * * column 6, line 50 - line 54 * * column 7, line 51 - line 68 * * column 8, line 9 - line 31 *	1,5,7	G07C G06M G06F
A	EP 0 743 620 A (NIPPON ELECTRIC CO) 20 November 1996 (1996-11-20) * abstract; figure 1 * * column 2, line 34 - column 3, line 10 *	7	
A	US 5 117 358 A (WINKLER PETER M) 26 May 1992 (1992-05-26)		
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 21 September 2000	Examiner Buron, E
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 (03.02) (P46/01)

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 00 83 0309

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-09-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5201067 A	06-04-1993	DE 69230364 D	05-01-2000
		EP 0541772 A	19-05-1993
		KR 9505862 B	31-05-1995
		WO 9220167 A	12-11-1992
WO 9923607 A	14-05-1999	SE 511220 C	23-08-1999
		EP 1025545 A	09-08-2000
		SE 9703818 A	21-04-1999
US 4774665 A	27-09-1988	CA 1280825 A	26-02-1991
DE 4446728 A	27-06-1996	NONE	
US 5153826 A	06-10-1992	NONE	
EP 0743620 A	20-11-1996	US 6092051 A	18-07-2000
		AU 702945 B	11-03-1999
		AU 5235196 A	28-11-1996
		CA 2176990 A	20-11-1996
		JP 8315053 A	29-11-1996
US 5117358 A	26-05-1992	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82