(19) Bureau voor de Industriële Eigendom Nederland

(11) **1021632**

(12) C **OCTROOI**[20]

(21) Aanvrage om octrooi: **1021632**

(22) Ingediend: **11.10.2002**

(51) Int.Cl.[7]
G07C13/00, G06F17/60

(41) Ingeschreven:
14.04.2004

(47) Dagtekening:
14.04.2004

(45) Uitgegeven:
01.06.2004 I.E. 2004/06

(73) Octrooihouder(s):
N.V. Nederlandsche Apparatenfabriek "Nedap" te Groenlo.

(72) Uitvinder(s):
Johannes Harm Lukas Hogen Esch te Aalten
Vincent Hakvoort te Winterswijk

(74) Gemachtigde:
Geen

(54) **Systeem voor het kiezen op afstand met stemmaskering.**

(57) Een verkiezingssysteem voor het kiezen op afstand waarbij het stemgeheim wordt gewaarborgd door een uitgebrachte stem te maskeren met stemmen op een willekeurig aantal andere kandidaten. De kiezer stelt twee identieke willekeurige lijsten samen waarbij de uit te brengen stem aan een van deze lijsten is toegevoegd. Deze lijsten worden vervolgens door drie of vier computers verwerkt om de identiteit van de kiezer en de door deze kiezer uitgebrachte stem gescheiden te houden. De einduitslag, maar ook een tussenuitslag, kan worden bepaald door alle lijsten zonder de gekozen kandidaten af te trekken van alle lijsten met de gekozen kandidaten. Alle verzonden informatie is beveiligd, doch blijft leesbaar voor zowel de zendende als de ontvangende partij. Malversaties worden opgemerkt en de kiezer beschikt over een gewaarmerkt bewijs met betrekking tot de uitgebrachte stem, waarbij eventueel gecontroleerd kan worden of deze stem heeft meegeteld bij de einduitslag.

NL C 1021632

Systeem voor het kiezen op afstand met stemmaskering.

De uitvinding betreft een systeem voor het kiezen op afstand waarbij de uitgebrachte stemmen zodanig gemaskeerd worden dat het onmogelijk is een verband te leggen tussen de kiezer en de door deze kiezer uitgebrachte stem of stemmen. Het verkiezingssysteem volgens de uitvinding kan worden gebruikt voor bijvoorbeeld landelijke, provinciale of gemeentelijke verkiezingen, waarbij de stemmen op afstand dus bijvoorbeeld via internet, via een point to point modemverbinding, via een telefoonlijn of met behulp van stemzuilen op openbare locaties kunnen worden uitgebracht.

Een van de belangrijkste eisen die gesteld worden aan verkiezingssystemen is waarborging van het stemgeheim. Dit wil zeggen dat het onmogelijk moet zijn om een verband te leggen tussen de kiezer en een uitgebrachte stem. Bij het kiezen op afstand via bijvoorbeeld internet is dit een lastig probleem, omdat tezamen met de uitgebrachte stem ook de identiteit van de betreffende kiezer moet worden overgebracht om te kunnen vaststellen dat deze kiezer gerechtigd is en dat slechts één stem door deze kiezer wordt uitgebracht. Dit laatste wordt ook wel uniciteit genoemd. Verder moet het verkiezingssysteem integer zijn, waarbij de uitslag niet door de beheerders van de verschillende deelsystemen kan worden beïnvloed en uitsluitend wordt bepaald door rechtmatig uitgebrachte stemmen afkomstig van kiezers. Het gehele systeem moet ook controleerbaar zijn zonder dat het stemgeheim in gevaar komt. Tenslotte moet de kiezer het stemproces kunnen begrijpen en vertrouwen.

De onderhavige uitvinding voldoet aan al deze eisen en zal aan de hand van vijf figuren van proces- en datadiagrammen in het vervolg worden verduidelijkt.

Figuur 1 toont globaal het totale proces- en dataflowdiagram van het verkiezingssysteem volgens de uitvinding.

Figuur 2 toont het proces- en dataflowdiagram betreffende de informatie van en naar de kiezer en de verwerking van deze informatie door de computer (PC) van de kiezer.

Figuur 3 toont het proces- en dataflowdiagram en de verwerking van de informatie door een eerste centrale computer 1.

Figuur 4 toont het proces- en dataflowdiagram en de verwerking van de informatie door een tweede centrale computer 2.

Figuur 5 toont het proces- en dataflowdiagram en de verwerking van de informatie door een derde en eventueel een vierde computer 3 en 4.

Aangezien de steminformatie die via een netwerk, zoals bijvoorbeeld internet, wordt verzonden ten behoeve van uniciteit gekoppeld moet worden aan informatie betreffende de identiteit van de kiezer is in het verkiezingssysteem volgens de uitvinding gekozen voor het gebruik van minimaal drie onafhankelijke centrale computers (servers) 1-3, eventueel aangevuld met een vierde computer 4 om de telling te controleren waarbij, zoals aangegeven in figuur 1, computer 1 en computer 2 via het voornoemde netwerk (internet) zijn verbonden met de computer van de kiezer en waarbij alle centrale computers onderling zijn verbonden via een beschermd netwerk zoals bijvoorbeeld intranet. In de beschrijving zal in het vervolg worden uitgegaan van vier centrale computers, omdat dit de beste bescherming tegen frauduleus handelen biedt.

De vier centrale computers worden in het verkiezingssysteem volgens de uitvinding beheerd door vier onafhankelijke partijen, die niet met elkaar over de informatie in de door deze partijen beheerde computers zullen communiceren. Één of enkele van deze partijen zou bijvoorbeeld kunnen worden aangevuld met een internationale waarnemers-

groep. Het systeem is verder zodanig ingericht dat het, met gebruikmaking van alle informatie die, met uitzondering van de computer (PC) van de kiezer, per computer beschikbaar is, onmogelijk is om te bepalen op wie een willekeurige kiezer heeft gestemd. Ook worden malversaties bij zowel de kiezer als bij één van de partijen die de computers beheren opgemerkt door één of meer van de andere partijen.

Een belangrijk kenmerk van het systeem volgens de uitvinding is dat encryptietechnieken worden toegepast om de communicatielijnen te beveiligen en om digitale waarmerken aan te brengen op de informatie tussen de kiezer en de vier computers. De verzonden informatie blijft echter in alle gevallen zowel voor de zendende als voor de ontvangende partij leesbaar, hetgeen de controleerbaarheid en de transparantie vergroot.

Een ander belangrijk kenmerk van de uitvinding is, dat de uitgebrachte stem van iedere kiezer wordt gemaskeerd door een relatief groot aantal stemmen op kandidaten die niet door de betreffende kiezer worden gekozen maar wel voorkomen op het stembiljet van de betreffende kiezer. De kiezer zendt twee lijsten met willekeurige kandidaten in, waarbij de ene lijst één kandidaat meer bevat dan de andere lijst. Deze lijsten zijn volkomen identiek op de ene extra kandidaat na die door de betreffende kiezer gekozen wordt. De lijst met de extra kandidaat wordt in het vervolg de plus-lijst genoemd en de andere lijst de min-lijst. Door bij de verwerking alle min-lijsten af te trekken van alle plus-lijsten blijven de gekozen kandidaten over. De plus-lijsten worden tezamen met de identiteiten van de kiezers verwerkt door computer 2, de min-lijsten worden tezamen met de identiteiten van de kiezers verwerkt door computer 1 en de computers 3 en 4 verrichten de telling zonder te beschikken over de identiteit van de kiezers en genereren onafhankelijk van elkaar dezelfde einduitslag van de verkiezing, die op deze wijze ook controleerbaar is.

Bij het systeem volgens de uitvinding beschikt de kiezer over een geheime code, die uit twee delen bestaat, te

weten, één persoonlijk deel dat de kiezer, voorafgaande aan de verkiezingsdag heeft gegenereerd en aan de verkiezingsinstantie heeft bekend gemaakt en een tweede deel in de vorm van een stemcode die aan de kiezer wordt toegezonden en alleen aan de betreffende kiezer bekend is. Deze stemcode kan bijvoorbeeld op de oproepkaart onzichtbaar onder een kraslak worden aangebracht, waarbij de kiezer bij beschadiging van deze laklaag om een andere stemcode kan verzoeken.

De eerste stap die de kiezer moet doen om via internet te kunnen stemmen is het laden van de verkiezingsapplicatie die op de PC van de kiezer kan draaien. Alle informatie van en naar de kiezer wordt uitgewisseld via een standaard SSL (Secure Sockets Layer) protocol verbinding waarmee de authenticiteit van de verbindingen via internet wordt gewaarborgd. De verkiezingsapplicatie kan bijvoorbeeld bestaan uit een zogenaamde JAVA-applet die kan draaien onder standaard internet browsersoftware, maar kan ook een applicatie zijn die wordt gedownload via internet of die vooraf aan de kiezer wordt verstrekt via een digitaal medium.

Nadat de kiezer de voornoemde applicatie gestart heeft, wordt deze kiezer verzocht zijn of haar persoonlijke identiteit bekend te maken, bijvoorbeeld aan de hand van naam en adresgegevens of aan de hand van een oproepnummer en de twee delen van de geheim code in te toetsen. Tezamen vormt dit de informatie (ID) omtrent de identiteit en de authenticiteit van de kiezer.

Met behulp van deze informatie wordt zoals aangegeven in figuur 2 een stembiljet opgehaald bij computer 1. Dit stembiljet bevat de lijst met digitaal gewaarmerkte kandidaten, die voor het stemdistrict van de betreffende kiezer van toepassing zijn, waarbij alle kandidaten voorzien zijn van een uniek kandidaatnummer, dat voor de gehele verkiezing slechts éénmaal voorkomt. Voornoemd digitaal waarmerk (W1) wordt op bekende wijze gegenereerd met behulp van een asymmetrisch encryptiealgoritme met een publieke en

een geheime sleutel waarbij de publieke sleutel met de informatie meegezonden wordt en de mogelijkheid biedt om deze informatie te lezen, maar voorkomt dat deze informatie ook door de ontvangende partij gegenereerd zou kunnen worden.

Voordat computer 1 het gevraagde gewaarmerkte stembiljet (W1[L]) verstrekt, wordt zoals aangegeven in figuur 3, aan de hand van de identiteit (ID) gecontroleerd of de betreffende kiezer voorkomt in het kiesregister, of de betreffende kiezer al eerder gestemd heeft, een stembiljet heeft ontvangen en of de geheime persoonlijke code klopt.

Als de betreffende kiezer reeds gestemd heeft, dan wordt deze kiezer daarvan in kennis gesteld en het proces beëindigd. Indien al eerder een gewaarmerkt stembiljet (W1[L]) is verstrekt, dan wordt hetzelfde biljet opnieuw verstrekt.

Nadat de kiezer het gewaarmerkte stembiljet, tezamen met de publieke sleutel van waarmerk (W1), heeft ontvangen wordt, zoals aangegeven in figuur 2, met behulp van de verkiezingsapplicatie één kandidaat (s) gekozen door de kiezer.

Het gebruikersinterface van deze applicatie kan bijvoorbeeld worden uitgevoerd zoals aangegeven in de Nederlandse octrooiaanvrage nr. 1019945 (Dynamisch gebruikersinterface voor stemsystemen) van aanvraagster.

Van alle overblijvende kandidaten (W1[L-s]) wordt vervolgens willekeurig "at random" ongeveer de helft uit de lijst verwijderd, waarna de gekozen kandidaat (s) weer aan de resterende lijst (W1[L-R-s]) wordt toegevoegd. De lijst (W1[L-R]) die op deze wijze overblijft is de plus-lijst van de betreffende kiezer, waarin de gekozen kandidaat (s) voorkomt.

Deze plus-lijst (W1[L-R]) wordt vervolgens door de applicatie naar computer 2 gezonden tezamen met de identiteitsinformatie (ID) van de kiezer, waarin ook de geheime persoonlijke code is verwerkt. Op dezelfde wijze als computer 1 controleert, zoals aangegeven in figuur 4, computer 2 aan de hand van het kiesregister, of de

betreffende kiezer al eerder gestemd heeft, een gewaarmerkte plus-lijst heeft ontvangen en of de geheime persoonlijke code klopt.

Als de betreffende kiezer reeds gestemd heeft, dan wordt deze kiezer daarvan in kennis gesteld en het proces beëindigd. Indien al eerder een gewaarmerkte plus-lijst is verstrekt, dan wordt dezelfde gewaarmerkte plus-lijst opnieuw verstrekt.

Het digitaal waarmerken van de plus-lijsten door computer 2 geschiedt eveneens op bekende wijze met een asymmetrisch encryptiealgoritme, waarbij de publieke sleutel met de lijst wordt meegezonden, zodat deze lijst leesbaar blijft voor de ontvangende partij(en) doch niet geproduceerd kan worden door deze ontvangende partij(en).

Computer 2 slaat de ontvangen plus-lijst (W1[L-R]+ID) op in een tijdelijk geheugen en brengt twee digitale waarmerken (W2) en (W3) aan, waarbij waarmerk (W2) wordt aangebracht over de ingezonden plus-lijst (W1[L-R]) en waarmerk (W3) over de met (W2) gewaarmerkte ingezonden plus-lijst (W2[W1[L-R]]) inclusief de identiteitsgegevens (ID) van de kiezer (W3[W2[W1[L-R]]+ID]). Vervolgens wordt deze dubbel gewaarmerkte informatie (W3[W2[W1[L-R]]+ID]) terug-gezonden naar de kiezer tezamen met de publieke sleutels van de waarmerken (W2) en (W3).

Nadat de computer van de kiezer de door computer 2 dubbel gewaarmerkte plus-lijst (W3[W2[W1[L-R]]+ID]) heeft ontvangen genereert deze, zoals aangegeven in figuur 2, de min-lijst voor de betreffende kiezer (W3[W2[W1[L-R-s]]+ID]), door de uitgebrachte stem (s) uit de ontvangen gewaarmerkte plus-lijst te verwijderen. Deze dubbel gewaarmerkte min-lijst (W3[W2[W1[L-R-s]]+ID]) wordt vervolgens, tezamen met de publieke sleutels van de waarmerken (W2) en (W3), naar computer 1 gezonden. Aangezien de kandidaten elk apart gewaarmerkt zijn, kan eenvoudig een gewaarmerkte kandidaat gewist worden uit de lijst maar kunnen er geen nieuwe kandidaten aan toe worden gevoegd.

Computer 1 ontvangt de door computer 2 dubbel

gewaarmerkte min-lijst (W3[W2[W1[L-R-s]]+ID]), controleert aan de hand van de waarmerken of de ontvangen min-lijst authentiek is, verwijdert waarmerk (W3) en slaat, zoals aangegeven in figuur 3, het restant (W2[W1[L-R-s]]+ID) op in een tijdelijk geheugen.

Dit restant van de min-lijst (W2[W1[L-R-s]]+ID) wordt door computer 1 voorzien van een digitaal waarmerk (W4), dus als (W4[W2[W1[L-R-s]]+ID]), teruggezonden naar de computer van de kiezer ter bevestiging van de ontvangst van deze min-lijst. De kiezer beschikt nu over gewaarmerkte bewijzen met betrekking tot de uitgebrachte stem, die bijvoorbeeld via de applicatie op de PC van de kiezer met behulp van een door de kiezer te bedenken versleuteling kunnen worden opgeslagen, zoals aangegeven in figuur 2.

Computer 1 meldt vervolgens via het onderlinge netwerk aan computer 2 dat een min-lijst met (n-1) kandidaten is ontvangen van een kiezer met de identiteitsgegevens (ID) en ontvangt een bevestiging met het aantal kandidaten in de plus-lijst van de kiezer met dezelfde identiteitsgegevens (ID) van computer 2. Na ontvangst van voornoemde bevestiging wordt de data verwerkt door computer 1 en worden de min-lijst stemmen (W2[W1[L-R-s]) zoals aangegeven in figuur 3 zonder identiteit van de kiezer toegevoegd aan het min-lijst geheugen en gewist uit het voornoemd tijdelijk geheugen.

Op dezelfde wijze verwerkt computer 2 zoals aangegeven in figuur 4, na ontvangst van de melding van computer 1 met betrekking tot de betreffende kiezer, de plus-lijst uit het tijdelijk geheugen en plaatst deze stemmen eveneens zonder de identiteit van de kiezer in het plus-lijst geheugen.

Na ontvangst van een vast te stellen minimum aantal stemmen zendt computer 2, zoals aangegeven in figuur 4, "at random" een willekeurig aantal met (W1) gewaarmerkte stemmen uit het plus-lijst geheugen, dus zonder identiteitsgegevens van de kiezers naar de computers 3 en 4. Op dezelfde wijze zendt computer 1, zoals is aangegeven in figuur 3, "at

random" een willekeurig aantal met (W2) en (W1) gewaarmerkte stemmen uit het min-lijst geheugen, dus zonder identiteitsgegevens van de kiezers naar de computers 3 en 4.
Deze gegevens worden door beide computers 3 en 4 bewaard in respectievelijk een plus-lijst geheugen en in een min-lijst geheugen.

Alle kandidaten met hetzelfde unieke kandidaatnummer die zowel in het plus-lijst geheugen als in het min-lijst geheugen voorkomen worden tegen elkaar weggeschrapt en uit de betreffende geheugens verwijderd.
Het plus-lijst geheugen bevat op deze wijze een globale tussenuitslag die afhankelijk van de soort verkiezing, al dan niet bekend gemaakt kan worden.

Nadat de termijn voor het uitbrengen van stemmen is verstreken worden de overblijvende restanten van het plus-lijst geheugen in computer 2 en het min-lijst geheugen in computer 1 ook naar de computers 3 en 4 gezonden, waarna deze computers beide de einduitslag kunnen bepalen door de resterende kandidaten met hetzelfde unieke kandidaatnummer in hun plus-lijst geheugen en in hun min-lijst geheugen tegen elkaar weg te schrappen, waarna de min-lijst geheugens dus leeg moeten zijn en het plus-lijst geheugen de einduitslag bevat.

Nadat de computers 3 en 4 de einduitslag vergeleken hebben en gelijk bevonden, kan deze worden bekendgemaakt.

Het geven van een uniek kandidaatnummer aan elke kandidaat wordt gedaan om te voorkomen dat kopieën kunnen worden gemaakt van de records van de gewaarmerkte kandidaten.

Een bijkomend voordeel hiervan is, dat hetzelfde verkiezingssysteem ook kan worden toegepast voor een duale verkiezing of voor een verkiezing met heel weinig kandidaten, waarbij de kiezer een gewaarmerkt stembiljet ontvangt waarop dezelfde kandidaten meerdere malen voorkomen met telkens een ander uniek kandidaatnummer. De applicatie op de computer van de kiezer geeft in dit geval uiteraard alleen een keuzemogelijkheid tussen de verschillende kandidaten,

waarbij elke kandidaat slechts éénmaal voorkomt.

Omdat alle gekozen kandidaten in de einduitslag een uniek kandidaatnummer hebben is het mogelijk een controleprocedure in te stellen, waarbij de kiezer door een onafhankelijke beroepscommissie kan laten controleren of de door de betreffende kiezer uitgebrachte stem heeft meegeteld in de einduitslag. Hiervoor geeft de kiezer in eerste instantie het door deze kiezer gekozen kandidaatnummer aan de beroepscommissie, die hiermee bij computer 3 of 4 kan nagaan of dit kandidaatnummer meegeteld heeft in de einduitslag zonder dat de naam van de betreffende kandidaat bekend gemaakt hoeft te worden. Is dit niet het geval, dan kan de kiezer via de gewaarmerkte plus-lijst en de gewaarmerkte min-lijst bewijzen dat de betreffende stem door deze kiezer is uitgebracht, waarbij deze stem wel bekend gemaakt moet worden aan de beroepscommissie.

Indien alle centrale computers de gecommuniceerde informatie bewaren tot na het verstrijken van de beroepstermijn, dan is een volledige audit van het verkiezingsproces mogelijk en kunnen hertellingen worden gedaan.

1. Een verkiezingssysteem voor het kiezen op afstand met het kenmerk, dat het stemgeheim wordt gewaarborgd door een uitgebrachte stem te maskeren, doordat de kiezer een plus-lijst met een willekeurig aantal kandidaten, inclusief de te kiezen kandidaat, samenstelt uit een voor deze kiezer geldend stembiljet met, door een eerste computer digitaal gewaarmerkte, kandidaten en vervolgens de kandidaten op deze plus-lijst door een tweede computer digitaal laat waarmerken, waarna de kiezer de te kiezen gewaarmerkte kandidaat uit deze plus-lijst verwijdert en de zo ontstane min-lijst verzendt naar de eerste computer, waarna beide computers, na controle en verwijdering van de identiteit van de kiezer, de ontvangen lijsten doorzenden naar een derde en eventueel een vierde computer, die elk de uitslag kunnen berekenen door per kandidaat het aantal uitgebrachte stemmen via de min-lijsten af te trekken van het aantal uitgebrachte stemmen via de plus-lijsten.

2. Een verkiezingssysteem voor het kiezen op afstand volgens conclusie 1 met het kenmerk, dat het met gebruikmaking van alle informatie die, uitgezonderd de computer van de kiezer, per computer beschikbaar is voor de partij die de betreffende computer beheert, onmogelijk is om te bepalen op wie een kiezer heeft gestemd.

3. Een verkiezingssysteem voor het kiezen op afstand volgens één of beide vorige conclusie(s) met het kenmerk, dat weliswaar encryptietechnieken worden toegepast om de communicatielijnen te beveiligen en om digitale waarmerken aan te brengen op de informatie tussen de computer van de kiezer en de drie of vier centrale computers, maar dat de verzonden informatie in alle gevallen zowel voor de zendende als voor de ontvangende partij leesbaar blijft, hetgeen de controleerbaarheid en de transparantie vergroot.

4. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat malversaties bij zowel de kiezer als bij één van de partijen die de centrale computers beheren opgemerkt worden door tenminste één van de andere partijen.

5. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat de kiezer over een geheime code beschikt, die uit twee delen bestaat, te weten één persoonlijk deel dat de kiezer, voorafgaande aan de verkiezingsdag heeft gegenereerd en aan de verkiezingsinstantie heeft bekend gemaakt en een tweede deel in de vorm van een stemcode die aan de kiezer wordt toegezonden en alleen aan de betreffende kiezer bekend is.

6. Een verkiezingssysteem voor het kiezen op afstand volgens conclusie 5 met het kenmerk, dat deze stemcode op de oproepkaart onzichtbaar onder een kraslak wordt aangebracht, waarbij de kiezer bij beschadiging van deze laklaag eventueel om een andere stemcode kan verzoeken.

7. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat alle informatie van en naar de kiezer wordt uitgewisseld via een standaard "Secure Sockets Layer" protocol verbinding, waarmee de authenticiteit van de verbindingen via internet wordt gewaarborgd.

8. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat de verkiezingsapplicatie bestaat uit een zogenaamde JAVA-applet die kan draaien onder standaard internet browsersoftware.

9. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat de verkiezingsapplicatie door de kiezer wordt gedownload via internet.

10. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat de verkiezingsapplicatie vooraf aan de kiezer wordt verstrekt via een digitaal medium.

11. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat alle gewaarmerkte kandidaten op het stembiljet voorzien zijn van een uniek kandidaatnummer, dat voor de gehele verkiezing slechts éénmaal voorkomt waarmee kopieën van de records van de gewaarmerkte kandidaten kunnen worden ondervangen.

12. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat dit verkiezingssysteem ook kan worden toegepast voor een duale verkiezing of voor een verkiezing met heel weinig kandidaten, waarbij de kiezer een gewaarmerkt stembiljet ontvangt waarop dezelfde kandidaten meerdere malen voorkomen met telkens een ander uniek kandidaatnummer.

13. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat de kiezer beschikt over gewaarmerkte bewijzen met betrekking tot de uitgebrachte stem, die bijvoorbeeld met behulp van een door de kiezer te bedenken versleuteling kunnen worden opgeslagen, waardoor een beroepsprocedure tot de mogelijkheden behoort.

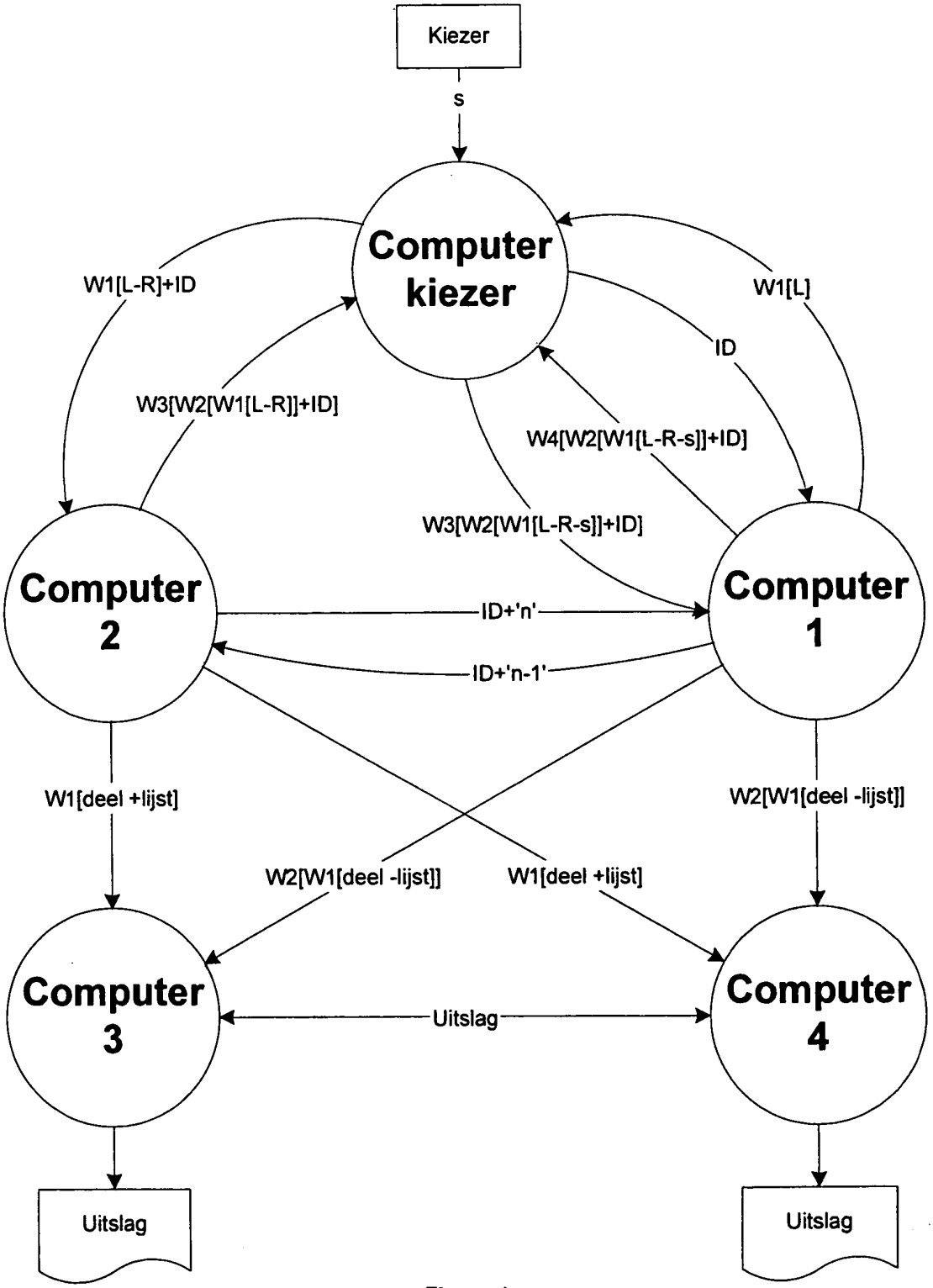
14. Een verkiezingssysteem voor het kiezen op afstand volgens één of meerdere vorige conclusie(s) met het kenmerk, dat de eerste en de tweede computer na ontvangst van een vast te stellen minimum aantal stemmen "at random" een willekeurig aantal verwerkte gewaarmerkte stemmen uit hun geheugens, zonder identiteitsgegevens van de kiezers naar de derde en eventueel een vierde computer zenden om de telling te verrichten en eventueel een globale tussenuitslag te bepalen.

15. Een verkiezingssysteem voor het kiezen op afstand volgans één of meerdere vorige conclusies) met het kenmerk, dat nadat de termijn voor het uitbrengen van stemmen is verstreken de overblijvende restanten van het min-lijst geheugen van de eerste computer en de overblijvende restanten van het plus-lijst geheugen van de tweede computer naar de derde en eventueel naar de vierde computer worden gezonden, waarna de derde en de vierde computer beide de einduitslag kunnen bepalen.

16. Een verkiezingssysteem voor het kiezen op afstand volgans één of meerdere vorige conclusies) met het kenmerk, dat de derde en de vierde computer de einduitslag vergelijken alsvorens deze bekend te maken.

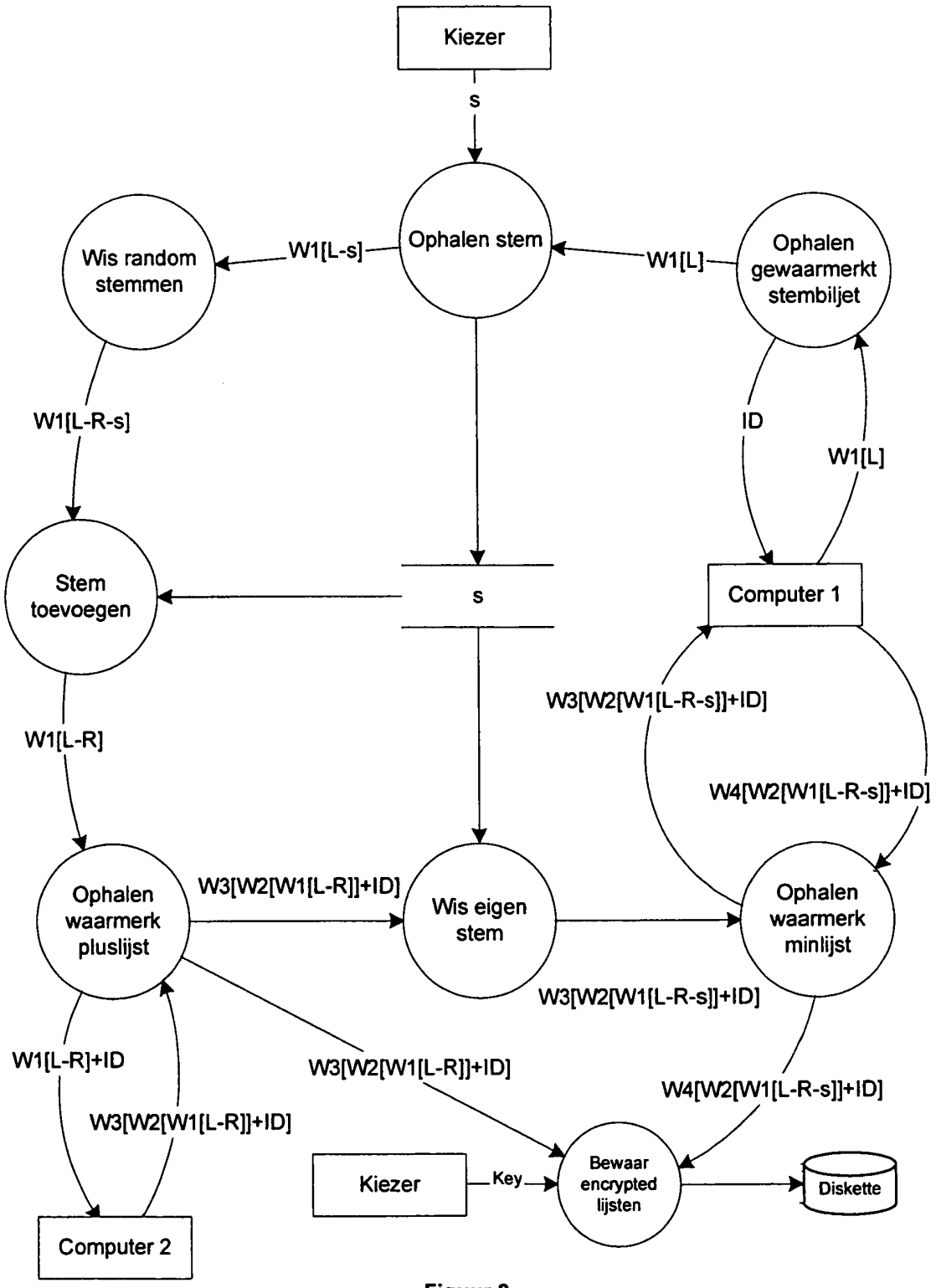
17. Een verkiezingssysteem voor het kiezen op afstand volgans één of meerdere vorige conclusies) met het kenmerk, dat een volledige audit van het systeem mogelijk is.

Overzicht

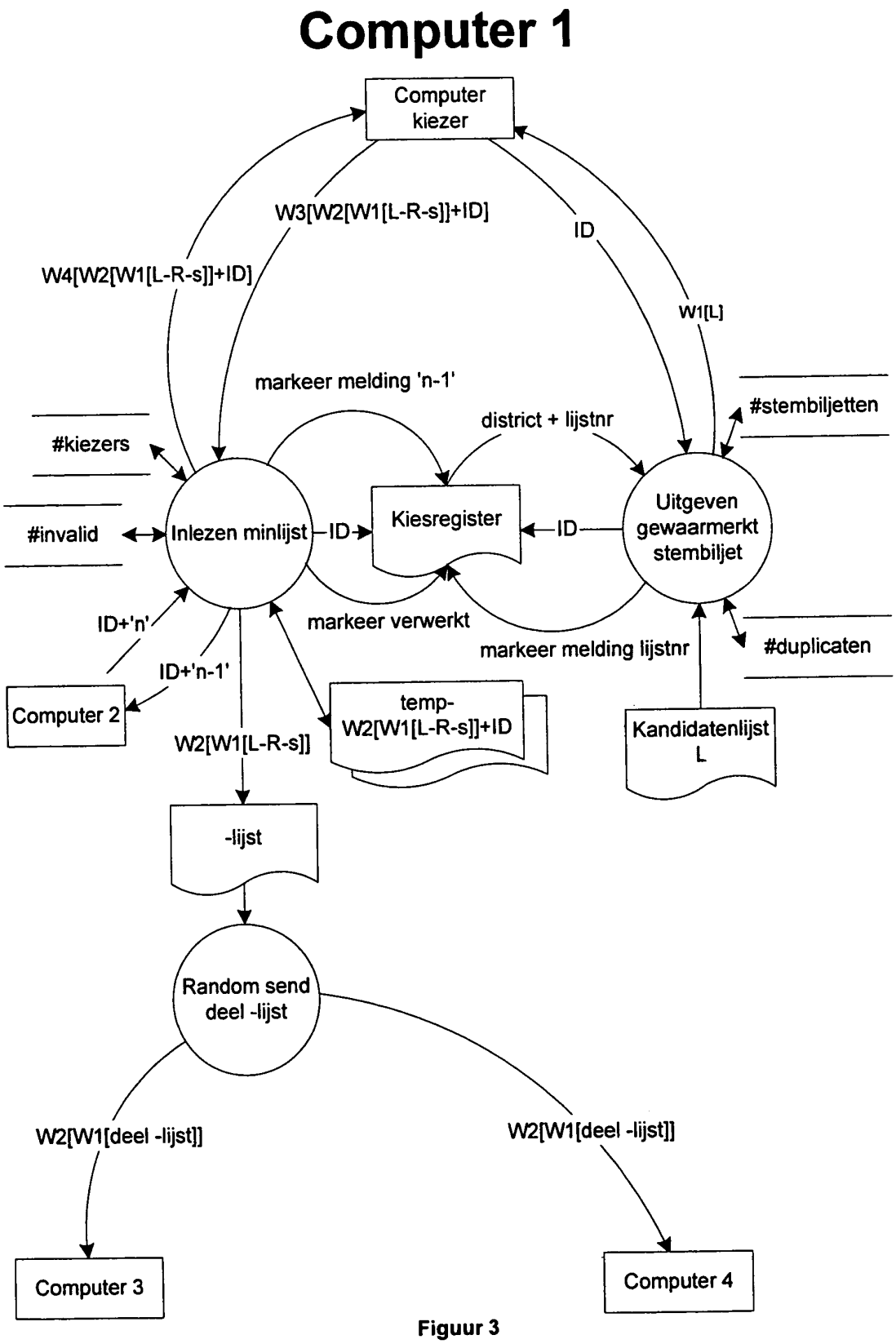


Figuur 1

Computer kiezer

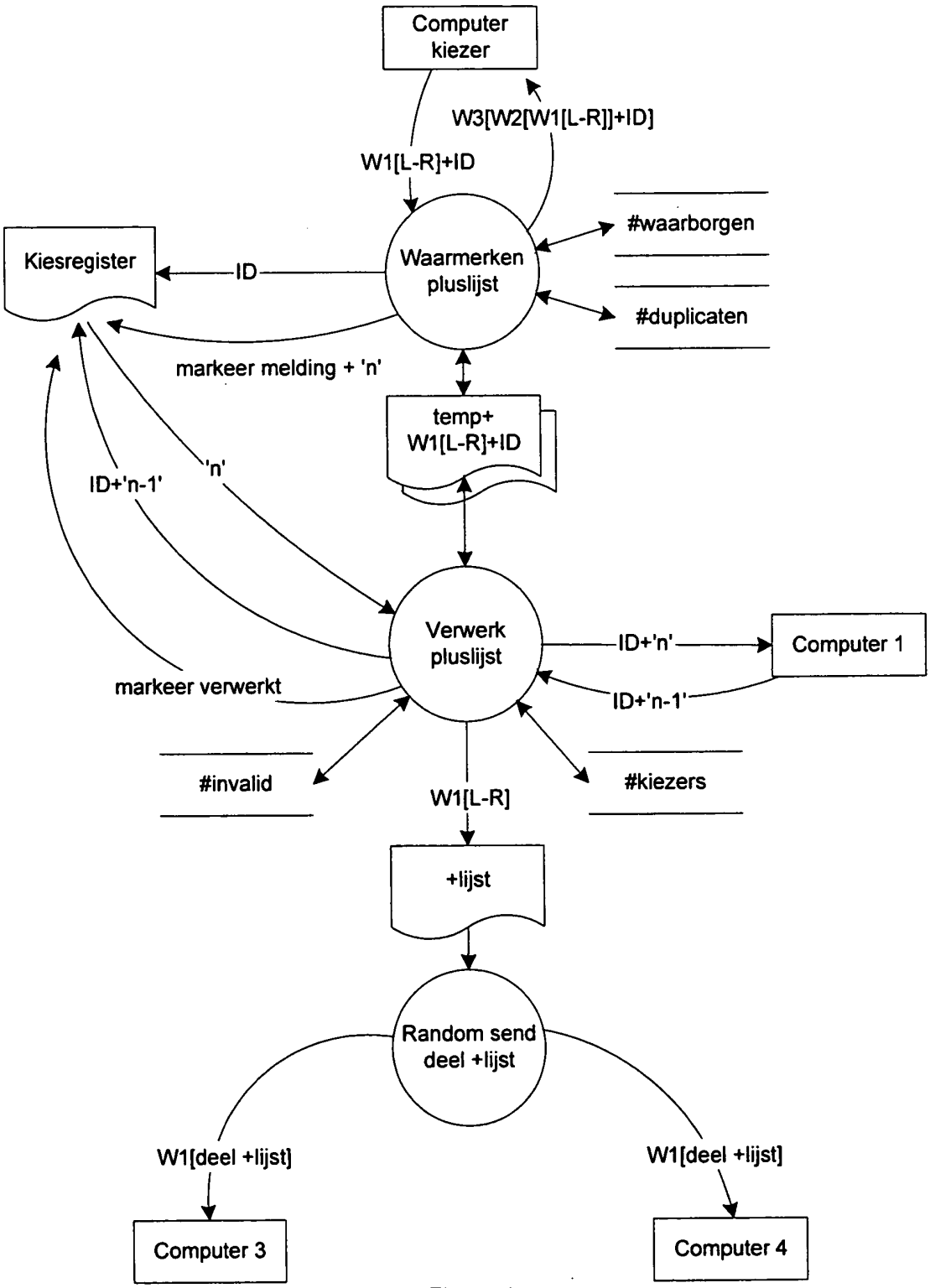


Figuur 2



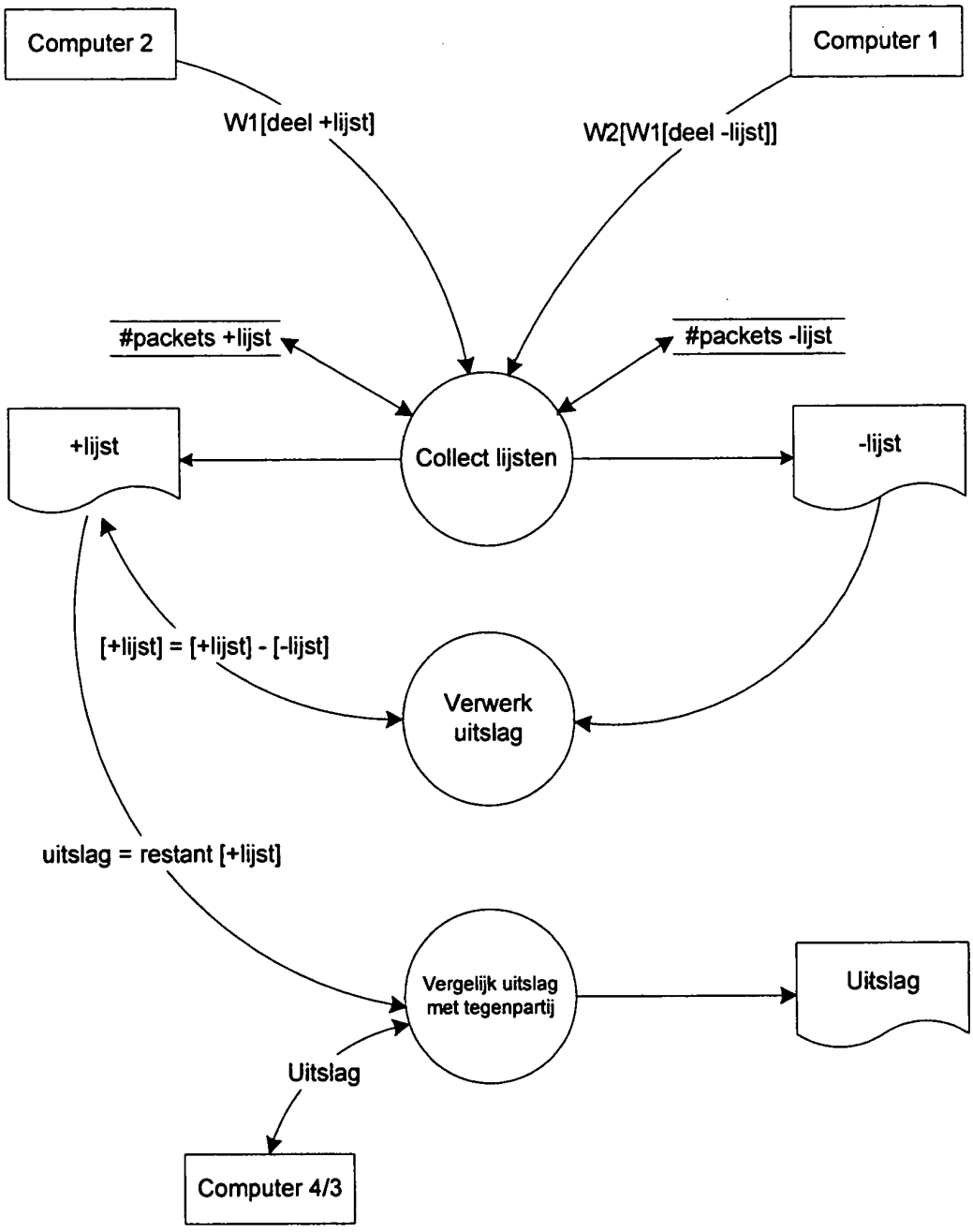
Figuur 3

Computer 2



Figuur 4

Computer 3/4



Figuur 5

SAMENWERKINGSVERDRAG (PCT)

RAPPORT BETREFFENDE NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFICATIE VAN DE NATIONALE AANVRAGE	KENMERK VAN DE AANVRAGER OF VAN DE GEMACHTIGDE NS50/SK
Nederlands aanvraag nr. 1021632	Indieningsdatum 11 oktober 2002
	Ingeroepen voorrangsdatum
Aanvrager (Naam) N.V. Nederlandsche Apparatenfabriek "Nedap"	
Datum van het verzoek voor een onderzoek van internationaal type	Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr. SN39815NL

I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)

Volgens de internationale classificatie (IPC)

Int. Cl 7: G07C13/00 G06F17/60

II. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie

Classificatiesysteem	Classificatiesymbolen
Int. Cl 7:	G07C G06F H04H

Onderzochte andere documentatie dan de minimum documentatie, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

III. ☐ GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)

IV. ☐ GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Demande de recherche No
NL 1021632

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07C13/00 G06F17/60

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07C G06F H04H

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 2002/077885 A1 (KARRO JARED ET AL) 20 juin 2002 (2002-06-20) abrégé; revendications; figures alinéa '0044! - alinéa '0049! alinéa '0074! - alinéa '0122! ---	1-17
A	US 2002/083126 A1 (BEST ROBERT ANGUS ET AL) 27 juin 2002 (2002-06-27) abrégé; revendications; figures alinéa '0005! - alinéa '0063! alinéa '0069! - alinéa '0072! ---	1-17
A	WO 92 03805 A (TECNOMEN OY) 5 mars 1992 (1992-03-05) abrégé; revendications; figures page 9, ligne 2 -page 14, ligne 35 --- -/--	1-17

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche de type international a été effectivement achevée	Date d'expédition du rapport de recherche de type international
17 juillet 2003	

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meyl, D

1

C.(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 021 200 A (FISCHER JEAN-BERNARD) 1 février 2000 (2000-02-01) abrégé; figures colonne 1, ligne 41 -colonne 2, ligne 67	1-17
A	HERSCHBERG: "Secure Electronic Voting Over the World Wide Web" SUBMITTED TO THE DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE AT THE MASSACHUSETTS INSTITUTE OFTECHNOLOGY, XX, XX, 27 mai 1997 (1997-05-27), pages 1-82, XP002215652	
A	US 6 081 793 A (CHALLENER DAVID C ET AL) 27 juin 2000 (2000-06-27)	

1

RAPPORT DE RECHERCHE DE TYPE INTERNATIONAL

Renseignements relatifs aux membres de familles de brevets

Demande de recherche n
NL 1021632

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2002077885 A1	20-06-2002	AU 3258402 A	18-06-2002
		WO 0246883 A2	13-06-2002
US 2002083126 A1	27-06-2002	WO 0062257 A1	19-10-2000
		AU 3648400 A	14-11-2000
		CA 2368121 A1	19-10-2000
		CN 1355908 T	26-06-2002
WO 9203805 A	05-03-1992	FI 904216 A	28-02-1992
		WO 9203805 A1	05-03-1992
US 6021200 A	01-02-2000	FR 2738934 A1	21-03-1997
		CN 1151554 A ,B	11-06-1997
		DE 69605627 D1	20-01-2000
		DE 69605627 T2	06-04-2000
		EP 0763803 A1	19-03-1997
		JP 9179923 A	11-07-1997
		ZA 9607111 A	03-03-1997
US 6081793 A	27-06-2000	AUCUN	