

Hoogheemraadschap van
Rijnland

MINUUT/afschrift aan:
hJBZ

BIJLAGE
2.4



07.12220

uw kenmerk:

Aan het hoofdbestuur van de VVD
Postbus 30836
2500 GV Den Haag

uw brief van:

ons kenmerk:

07.12220

bijlagen:

1

inlichtingen:

mr. drs. A.R. van Kampen

doorkiesnummer:

3366

onderwerp:

octrooi internetstemmen

Leiden,

17 APR. 2007

Geacht bestuur,

Eén van de leden van het algemeen bestuur van het Hoogheemraadschap van Rijnland heeft het college van dijkgraaf en hoogheemraden erop geattendeerd dat uw organisatie bij de kandidaatstelling voor de statenverkiezingen gebruik heeft gemaakt van een systeem, waarbij uw leden ondermeer middels post en internet hun stem konden uitbrengen.

Op 29 juni 2005 is het hoogheemraadschap, tezamen met de heer P.G. MacLaine-Pont te Wickel, octrooi verleend voor de vinding "systeem en werkwijze voor een elektronische verkiezing". Een kopie van het octrooibewijs voeg ik voor de goede orde hierbij.

De heer MacLaine Pont heeft uw organisatie eind 2006 benaderd met de vraag of hij inzicht kon krijgen in het systeem, dat u bij de stemmingen in het kader van o.m. de kandidaatstelling hanteert; er zou immers sprake kunnen zijn van een - onbewuste - inbreuk op de rechten van de octrooihouders.

Helaas werd hem het gevraagde inzicht niet geboden; derhalve richt het Hoogheemraadschap zich thans, mede namens de heer MacLaine Pont, tot u met dezelfde vraag.

Het hoogheemraadschap verzoekt u vriendelijk hem zo snel mogelijk - doch uiterlijk 1 juni a.s. - zoveel inzicht te geven in het systeem, dat uw organisatie bij de stemming per post en via internet in het kader van uw kandidaatstellingen hanteert, dat kan worden beoordeeld of er sprake is van een inbreuk op het octrooi. Bij gebreke daaraan gaat het hoogheemraadschap er noodgedwongen van uit dat er inderdaad sprake is van een inbreuk op zijn octrooi en zullen nadere acties worden overwogen.



Hoogheemraadschap van
Rijnland

U kunt er overigens van op aan dat het hoogheemraadschap de door u te verstrekken systeem informatie strikt vertrouwelijk zal behandelen.

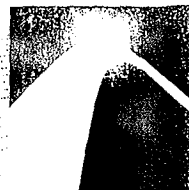
Hoogachtend,

Namens dijkgraaf en hoogheemraden,

drs. A.R. van Kampen,
hoofd Juridische en Bestuurlijke Zaken



OCTROOICENTRUM NEDERLAND



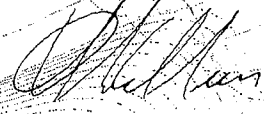
Koninkrijk der Nederlanden



Hierbij wordt verklaard, dat in Nederland op 11 januari 2005 onder nummer 1023861,
ten name van:
Pieter Gerard MACLAINE PONT
te Wijckel en
HOOGHEEMRAADSCHAP VAN RIJNLAND
te Leiden
een octrooi werd verleend, voor:
"Systeem en werkwijze voor een elektronische verkiezing",
en dat de hieraan gehechte stukken overeenstemmen met het uitgegeven octrooischrift.

Rijswijk, 29 juni 2005

De Directeur van Octrooi Centrum Nederland,
voor deze


D.H. de Haas

Hoogheemraadschap van Rijnland
bijlage bij nr. 105.16456



(19)



Octrooi Centrum
Nederland

(11) 1023861

(12) C OCTROOI²⁰

(21) Aanvraag om octrooi: 1023861

(51) Int.Cl.7
G07C13/00

(22) Ingediend: 08.07.2003

(41) Ingeschreven:
11.01.2005 I.E. 2005/03(47) Dagtekening:
14.03.2005(45) Uitgegeven:
02.05.2005 I.E. 2005/05(73) Octrooihouder(s):
Pieter Gerard Maclaine Pont te Wijkkel.
Hoogheemraadschap van Rijnland te Lelidn.(72) Uitvinder(s):
Pieter Gerard Maclaine Pont te Wijkkel(74) Gemachtigde:
lr. J.M.G. Dohmen c.s. te 5600 AP Eindhoven.

(54) Systeem en werkwijze voor een elektronische verkiezing.

(57) Elektronisch openbaar verkiezingssysteem en -werkwijze op basis van een virtueel stembiljet dat met behulp van een symmetrisch cryptografisch algoritme wordt gecreëerd. Iedere kiezer ontvangt vooraf een persoonlijke, geheime cryptografische sleutel. Deze sleutels worden vooraf in een vertrouwelijk en besloten proces berekend en gereedgemaakt voor veilig transport en er wordt een uitslagreferentiebestand berekend, door voor iedere kiezer met diens persoonlijke sleutel iedere mogelijk uit te brengen stem te berekenen. Dit uitslagreferentiebestand wordt vooraf gepubliceerd. De kiezer brengt zijn stem uit door met behulp van bijvoorbeeld zijn PC-Internetbrowser, smartcard of GSM-telefoon met zijn persoonlijke sleutel een berekening uit te voeren over zijn gekozen onderwerp of combinatie van onderwerpen en identiteiten van de verkiezing. Dit vormt zijn virtuele stembiljet dat bij het stembureau elektronisch of per post kan worden ingeleverd. De uitvinding voorziet daarin, dat wanneer een stel van twee of meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een enkel virtueel stembiljet van het stel wordt gevalideerd als een geldige stem en de overige virtuele stembiljetten van het stel worden aangemerkt als duplicaat, mits de virtuele stembiljetten van het stel identiek zijn voor het door de kiezer gekozen onderwerp of een combinatie van onderwerpen, anders worden alle virtuele stembiljetten van het stel aangemerkt als ongeldig. Na afloop worden alle ontvangen virtuele stembiljetten gepubliceerd. Iedereen kan zelf de uitslag berekenen of kijken of zijn stem is meegeteld. Daarmee is een eenvoudig en betrouwbaar verkiezingssysteem mogelijk.

NL C 1023861

De inhoud van dit octrooi wijkt af van de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekening(en). De oorspronkelijk ingediende stukken kunnen bij het Octrooi Centrum Nederland worden ingezien. Octrooi Centrum Nederland is het Bureau voor de Industriële Eigendom, een agentschap van het ministerie van Economische Zaken

Korte aanduiding: Systeem en werkwijze voor een elektronische verkiezing.

De uitvinding heeft betrekking op elektronische verkiezingen en in
5 het bijzonder op elektronische verkiezingen waarbij stemmen worden uitgebracht en
verzameld via een openbaar datacommunicatienetwerk, zoals het Internet.

Onder verkiezing wordt hierna verstaan: een vorm van
opinieonderzoek, zoals een openbare verkiezing voor een overheidslichaam, een
referendum of een verkiezing voor een democratische vertegenwoordiging in een
10 organisatie of bedrijf, waaraan alleen vooraf geregistreerde personen
(stemgerechtigden, kiezers) mogen deelnemen, waarbij hun opinie of keuze (hierna
aangeduid als stem) gevraagd wordt uit vooraf volledig openbaar gemaakte tekst, te
kiezen kandidaten of referendumtekst (hierna aangeduid als kandidatenlijst), waarbij
de door hun afgegeven stem vertrouwelijk is en zonder dwang kan worden ingediend
15 gedurende een beperkt tijdsperiode (hierna aangeduid als verkiezingsvenster) bij een
vooraf aangekondigde vertrouwde partij, waarbij iedere door een kiezer ingediende
stem als keuze voor een kandidaat tenminste en maximaal éénmaal telt en waarbij de
uitslag van de verkiezing openbaar is en door onafhankelijke derden te controleren
dient te zijn.

20 Een verkiezingssysteem via een openbaar datacommunicatienetwerk
is een systeem, dat een kiezer in staat stelt deel te nemen aan een verkiezing vanaf een
door hem zelf te kiezen plaats, van waaruit hij met de daartoe benodigde middelen of
apparatuur via het openbare datacommunicatienetwerk zijn stem kan uitbrengen. Zo'n
systeem zal hierna worden aangeduid als locatie-onafhankelijk verkiezingssysteem.

25 Een elektronisch verkiezingssysteem is een locatie-onafhankelijk
verkiezingssysteem, waarbij de kiezer gebruikmaakt van digitale, elektronische
middelen om zijn keuze kenbaar te maken en gebruik wordt gemaakt van een digitaal
en elektronisch openbaar communicatienetwerk. Voorbeelden hiervan zijn: SMS via
mobiele of vaste telefoon, WAP-telefoon en een personal computer via het Internet.

30 Uit de Europese octrooiaanvraag EP 1 291 826 A1 is een
elektronisch verkiezingssysteem bekend, waarbij het Internet wordt gebruikt als
communicatiemiddel tussen de kiezers, die op afstand, bijvoorbeeld thuis, een stem
uitbrengen en het stembureau dat de door de kiezers uitgebrachte stemmen verzamelt.

Hierbij worden maatregelen getroffen om de juiste identiteit van de kiezer te waarborgen, fraude te voorkomen, en het gevaar van een virus of een kwaadwillende hacker, die inbreekt op het stemproces om de elektronische stemmen te wijzigen, te weren. Bij dit verkiezingssysteem kan de kiezer kiezen om eenmalig de stem uit te brengen langs elektronische weg of door het deponeren van een stembiljet (per post) bij een stembureau.

Uit de afstudeerscriptie "Electronic elections employing DES smartcards" door H. Robers, December 1998, IBM Student Chipcard Innovation Team, is een elektronisch verkiezingssysteem met een verkiezingsprotocol voor locatie- onafhankelijk stemmen bekend, waarbij gebruik wordt gemaakt van het Internet.

In dit verkiezingssysteem wordt gewerkt met individuele, onpersoonlijke (virtuele) stembiljetten, die pas bij het uitbrengen van de stem op de locatie van de kiezer met een symmetrische cryptografische techniek, zoals Data Encryption Standard, DES, worden berekend met gebruikmaking van een persoonlijke chipkaart, die is ingevoerd in een met een persoonlijke computer gekoppeld chipkaartlezer. Aan iedere kiezer is daartoe vooraf, langs vertrouwelijke weg, een unieke persoonlijke cryptografische 3DES-sleutel, die alleen voor de te houden verkiezing kan worden gebruikt, in zijn /haar chipkaart verstrekt.

De voor de berekening van het stembiljet benodigde functionaliteit voor de Internet-browser van de met de chipkaartlezer gekoppelde personal computer, wordt tijdens het verkiezingsvenster via het Internet verschaft, bij het opvragen van de lijst van te kiezen onderwerpen. Met deze functionaliteit wordt met behulp van de persoonlijke sleutel van de kiezer voor de verkiezing en het gekozen onderwerp het virtuele stembiljet van de kiezer berekend.

Voorafgaand aan de verkiezing worden alle unieke persoonlijke sleutels voor de ingeschreven kiezers gegenereerd en voor verzending klaar gemaakt. Ook wordt een referentiebestand met de cryptografisch berekende referentie van alle, door iedere kiezer mogelijk uit te brengen stemmen gegenereerd en openbaargemaakt.

Na het sluiten van het verkiezingsvenster worden alle ontvangen virtuele stembiljetten gepubliceerd in samenhang met het vooraf openbaargemaakte referentiebestand voor algemeen onderzoek naar het verloop van de verkiezing.

In dit verkiezingssysteem kan de stem alleen langs elektronische weg worden ingediend door gebruikmaking van een unieke sleutel, die vooraf is vastgelegd in een persoonlijke chipkaart. Het gebruik van een chipkaart vergt dat een personal computer moet zijn voorzien van een chipkaartlezer om als stemapparaat in
 5 een verkiezing te kunnen worden gebruikt.

Voor een kansrijke invoering van elektronisch stemmen moet het verkiezingssysteem voldoen aan algemene formele voorwaarden voor een verkiezing van overheidswege, waarbij ook het uitbrengen van stemmen per post mogelijk moet zijn. Bovendien moeten de toe te passen technische middelen zodanig zijn, dat ten
 10 minste 95% van de potentiële kiezers in staat is aan het verkiezingssysteem deel te nemen door middel van een met een datacommunicatienetwerk, zoals het Internet, gekoppelde personal computer zonder te moeten voldoen aan bijzondere aanpassingen of functievereisten, zowel wat betreft hardware- als softwarematig.

Daarnaast is het gewenst dat de kiezer bij twijfel over het welslagen
 15 van het elektronisch verzenden van het stembiljet over een datanetwerk, opnieuw zijn/haar stem uit kan brengen door een nieuw stembiljet met dezelfde keuze te verzenden over hetzelfde datacommunicatienetwerk of een over een ander datacommunicatienetwerk dat voor de verkiezing is opengesteld. De mogelijkheid om een stem uit te brengen door de keuze te markeren op het vooraf ontvangen
 20 stembericht en het stembericht vervolgens (per post) te deponeren bij het stembureau dient, ook na het elektronisch uitbrengen van de stem, te kunnen worden benut.

Via bijvoorbeeld het Internet en betrokken Internet-servers aan het stembureau overgedragen stemmen kunnen problemen ontstaan wanneer als gevolg van bijvoorbeeld technische storingen en onderbrekingen tijdens de overdracht, een
 25 uitgebrachte stem door een server twee of meer keer wordt herhaald en als zodanig door het stembureau wordt ontvangen en verzameld.

Een en ander heeft tot gevolg dat vanwege verschillende oorzaken meer dan één stembiljet van dezelfde kiezer wordt ontvangen en verzameld, waar niet meer dan een geldige stem kan worden toegekend.

30 De hierboven aangeduide elektronische verkiezingssystemen kennen geen voorzieningen om de problemen van het ontvangen van twee of meer stemmen van dezelfde kiezer te ondervangen.

De uitvinding beoogt te voorzien in een elektronisch verkiezingssysteem dat de kiezer in staat stelt om zijn/haar stem met beschikbare elektronische middelen naar het stembureau te verzenden door middel van een datacommunicatienetwerk en om zijn/haar stem in de vorm van een fysiek stembiljet
 5 (per post) te deponeren bij het stembureau, waarbij de stem, die door de kiezer op regelmatige wijze is uitgebracht als zodanig wordt onderkend en gewaardeerd, zodat dubbeltelling wordt voorkomen.

Volgens een eerste aspect verschaft de uitvinding hiertoe een elektronisch verkiezingssysteem voor het verzamelen en tellen van stemmen van
 10 individuele kiezers die gebruikmaken van een elektronisch stemapparaat in een verkiezing met een lijst van te kiezen onderwerpen waaruit een onderwerp wordt gekozen door een individuele kiezer waarbij de stemmen worden verzonden door middel van een datanetwerk, omvattende:

middelen voor het genereren van een unieke persoonlijke sleutel voor
 15 iedere kiezer op een lijst van voor de verkiezing ingeschreven kiezers, welke unieke persoonlijke sleutel aan de individuele kiezer wordt verstrekt;

middelen voor het genereren van een unieke onderwerpcodes voor
 ieder onderwerp op de lijst van te kiezen onderwerpen;

middelen voor het genereren van een referentie-uitslag voor iedere
 20 individuele kiezer bevattende alle virtuele stembiljetten voor de individuele kiezer, waarbij een unieke kiezerreferentie-identiteit wordt berekend uit een unieke verkiezingscode voor de verkiezing en de unieke persoonlijke sleutel van de kiezer, waarbij voor ieder onderwerp op de lijst van de door de kiezer te kiezen onderwerpen een unieke onderwerpreferentie-identiteit wordt berekend uit de unieke
 25 onderwerpcodes en de unieke persoonlijke sleutel van de kiezer en waarbij de berekende referentie-identiteiten deel uitmaken van de virtuele stembiljetten;

middelen voor het opslaan van de referentie-uitslagen van de
 individuele kiezers;

middelen voor het laden van instructies in het stemapparaat van de
 30 individuele kiezer om het stemapparaat in te richten voor het berekenen van een unieke kiezeridentiteit uit de unieke verkiezingscode voor de verkiezing en de unieke persoonlijke sleutel van de kiezer die aan de kiezer is verstrekt, voor het berekenen

van een unieke onderwerpidentiteit van het door de kiezer gekozen onderwerp uit de unieke onderwerpcodes van het gekozen onderwerp en de unieke persoonlijke sleutel van de kiezer en voor het genereren van het virtuele stembiljet met de, met gebruikmaking van het stemapparaat berekende identiteiten;

5 middelen om het virtuele stembiljet door het stemapparaat te verzenden over het datanetwerk;

middelen voor het ontvangen en verzamelen van het door het stemapparaat verzonden virtuele stembiljet;

10 middelen voor het verifiëren van elk verzameld virtueel stembiljet met betrekking tot de aanwezigheid in de referentieuitslagen van de kiezers;

middelen voor het tellen van de stemmen;

middelen voor het vaststellen van de verkiezingsuitslag, gekenmerkt door middelen voor het valideren van de stemmen van de ontvangen virtuele stembiljetten, welke middelen zodanig zijn ingericht dat, wanneer een stel van twee of
15 meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een virtueel stembiljet van het stel wordt gevalideerd als een geldige stem van de betreffende kiezer en de overige virtuele stembiljetten worden aangemerkt als duplicaat, mits de virtuele stembiljetten van het stel identiek zijn voor het door de kiezer gekozen onderwerp, anders worden alle virtuele stembiljetten van het stel
20 aangemerkt als ongeldig.

Volgens een tweede aspect van de uitvinding is een werkwijze verschaft voor een elektronische verkiezing voor het verzamelen en tellen van de stemmen van individuele kiezers die gebruikmaken van een elektronisch stemapparaat in een verkiezing met een lijst van te kiezen onderwerpen waaruit een onderwerp
25 wordt gekozen door een individuele kiezer, en de stemmen worden verzonden door middel van een datanetwerk, omvattende de stappen van:

het genereren van een unieke persoonlijke sleutel voor iedere individuele kiezer op een lijst van voor de verkiezing ingeschreven kiezers;

30 het verstrekken van de unieke persoonlijke sleutel aan de individuele kiezer;

het genereren van een unieke onderwerpcodes voor ieder onderwerp op de lijst van in de verkiezing te kiezen onderwerpen;

het genereren van een referentie-uitslag voor iedere individuele kiezer bevattende alle mogelijke virtuele stembiljetten voor de individuele kiezer, waarbij voor ieder individuele kiezer een unieke kiezerreferentie-identiteit wordt berekend uit een unieke code voor de verkiezingen en de unieke persoonlijke sleutel van de kiezer, voor ieder onderwerp op de lijst van te kiezen onderwerpen een unieke
 5 onderwerp referentie-identiteit wordt berekend uit de unieke onderwerpcodes en de unieke persoonlijke sleutel van de kiezer, waarbij de berekende referentie-identiteiten deel uitmaken van de virtuele stembiljetten;

het opslaan van de referentie-uitslagen van de individuele kiezers;

10 het laden van instructies in het stemapparaat van de kiezer;

het kiezen van een onderwerp uit de lijst van te kiezen onderwerpen met gebruikmaking van het stemapparaat van de individuele kiezer door de unieke persoonlijke sleutel, die aan de kiezer is verstrekt, en de unieke onderwerpcodes voor het gekozen onderwerp in te voeren in het stemapparaat;

15 het genereren van een virtueel stembiljet met gebruikmaking van de in het stemapparaat geladen instructies, waarbij een unieke kiezeridentiteit wordt berekend uit de unieke code van de verkiezing en de unieke persoonlijke sleutel van de kiezer en een unieke onderwerpidentiteit wordt berekend uit de unieke onderwerpcodes van het gekozen onderwerp en de unieke persoonlijke sleutel van de
 20 kiezer en waarbij de berekende identiteiten deel uitmaken van het virtueel stembiljet;

het verzenden van het virtueel stembiljet over het datanetwerk;

het ontvangen en verzamelen van het door het stemapparaat verzonden stembiljet;

25 het verifiëren van het verzameld virtueel stembiljet met betrekking tot de aanwezigheid in de referentie-uitslagen van de kiezers;

het tellen van de stemmen, en

het vaststellen van de verkiezingsuitslag op basis de getelde stemmen van de kiezers, gekenmerkt door de stap van het valideren van de stemmen van de verzamelde virtuele stembiljetten op een zodanige wijze dat, wanneer een stel van
 30 twee of meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een virtueel stembiljet van het stel wordt gevalideerd als een geldige stem en de overige virtuele stembiljetten van het stel worden aangemerkt als duplicaat, mits de

virtuele stembiljetten van het stel identiek zijn voor het door de kiezer gekozen onderwerp, anders worden alle virtuele stembiljetten van het stel aangemerkt als ongeldig.

5 De middelen respectievelijk de stap voor het valideren van de stemmen van de ontvangen virtuele stembiljetten kunnen ook worden toegepast bij een systeem respectievelijk een werkwijze voor een elektronische verkiezing met een lijst van te kiezen onderwerpen, waaruit een combinatie van onderwerpen door een individuele kiezer wordt gekozen.

10 Door deze maatregelen is het verkiezingssysteem in staat meerdere virtuele stembiljetten van dezelfde kiezer als één stem te herkennen en zodanig te valideren dat dubbeltelling wordt voorkomen. Daarmee is de uitkomst van het verkiezingssysteem ongevoelig voor storingen en onderbrekingen tijdens het verkiezingsvenster en mogen de kiezers bij twijfel een zelfde stem met herhaling uitbrengen, zelfs met gebruikmaking van andere technieken.

15 Bij een elektronisch verkiezingssysteem kan gebruik worden gemaakt van een symmetrisch cryptografisch algoritme, waarbij de voor een vercijferingsbewerking gebruikte sleutel gelijk is aan de sleutel die voor de ontcijfering nodig is. Deze sleutel dient geheim te worden gehouden (behalve voor de partijen die de vercijfer- en ontcijferbewerkingen dienen uit te voeren). Een
20 bijzondere eigenschap van dit soort algoritmen is, dat de daarbij toe te passen sleutels relatief kort zijn, de berekeningen relatief snel kunnen worden uitgevoerd en de bewerkingen van het algoritme relatief eenvoudig en compact zijn te realiseren in programmatuur. Met een symmetrisch cryptografisch algoritme kan men informatie vercijferen. Om de betrouwbaarheid ervan te waarborgen, kan men de informatie
25 voorzien van een Message Authentication Code (MAC) om deze informatie te beschermen tegen wijzigingen door anderen dan de oorspronkelijke verzender of ontvanger en van een Modification Detection Code (MDC), ook wel "hash" genoemd, om zonder gebruik van een geheime sleutel de integriteit van de gegevens te controleren en beschermen.

30 Tenslotte kan men met een symmetrisch cryptografisch algoritme een beheerssysteem maken voor de opslag en distributie van symmetrische cryptografische sleutels. Ziet men kans de geheime sleutels inderdaad geheim te

1023861 -

houden, dan zijn de diverse, publiek gestandaardiseerde cryptografische algoritmen veilig toepasbaar voor de hierboven beschreven functies. In de praktijk betekent dit dat symmetrisch cryptografische algoritmen goed toepasbaar zijn, als één enkele partij optreedt als hoofdverantwoordelijke en de basisopzet en inrichting van de te

5 beveiligen toepassing geheel kan bepalen.

Verdere uitvoeringsvormen van het systeem en de werkwijze volgens de uitvinding zijn in de afhankelijke conclusies geformuleerd.

De werking van een elektronisch verkiezingssysteem voor locatie-onafhankelijk stemmen met gebruikmaking van een virtueel stembiljet, waarbij

10 middelen worden toegepast om de geldigheid van ontvangen virtuele stembiljetten van dezelfde kiezer te onderzoeken en zodanig vast te stellen dat dubbeltelling wordt voorkomen wordt hierna toegelicht.

Bij een verkiezing met een elektronisch verkiezingssysteem onderscheiden we de volgende partijen en functies:

- 15 • Centrale verkiezingscommissie: een openbare, daartoe ingestelde partij, die de voor de elektronische verkiezingen noodzakelijke voorbereidingen treft, waaronder:
- De vaststelling en publicatie van een kiezersregister (waarin vastligt welke kiezers aan de verkiezing mogen deelnemen)
 - 20 ○ De vaststelling en publicatie van de informatie waarover de opinie of keuze van de kiezer gevraagd (de kandidatenlijst)
 - De organisatorische en technische voorbereiding van de elektronische verkiezingen, waaronder het voorzien van alle kiezers van specifieke informatie, die het hun mogelijk moet maken veilig en zonder
 - 25 persoonlijk bekend te worden (onpersoonlijk) aan de elektronische verkiezingen deel te nemen, waaronder:
 - Een document, zoals een poststembiljet, met een onpersoonlijke identiteit voor een specifieke kiezer om aan deze verkiezing mee te mogen doen, waarop de persoonlijke sleutel Kp van de
 - 30 kiezer is vermeld op een manier, die intoetsen met een toetsenbord mogelijk maakt; men zou dat bijvoorbeeld in twee alfanumerieke groepen kunnen doen, respectievelijk de

(vertrouwelijke) Verkiezing Pseudo Identiteit of VPID en een geheim wachtwoord (PW); eventueel kan men er voor kiezen de voor Internet stemmen te gebruiken data elementen op een apart document (de Stemkaart) te vermelden, of

- 5 ▪ Een geheime, persoonlijke sleutel Kp voor iedere individuele kiezer, die op veilige wijze geladen wordt op diens smartcard of SIM-kaart van zijn GSM-telefoon
- De daartoe noodzakelijke regelingen en afspraken met derde partijen, zoals dienstverleners, telecommunicatiebedrijven en
- 10 anderen.

- De vaststelling en publicatie van alle informatie die noodzakelijk is om op veilige en betrouwbare wijze het resultaat van de verkiezingen te kunnen vaststellen.

- Kiezer (hiervoor reeds gedefinieerd), in het bezit van een instrument om aan
- 15 de elektronische verkiezing mee te doen, waaronder:

- Een document met de voor hem bestemde onpersoonlijke identiteit (zoals het eerder beschreven Poststembiljet of de Stemkaart met daarop zijn Pseudo Verkiezing Identiteit of VPID en zijn wachtwoord (PW) om aan deze verkiezing mee te mogen doen), of
- 20 ○ Een persoonlijke smartcard (zoals bijvoorbeeld zijn Studenten ChipKaart, een hem door de overheid verstrekte identiteit smartcard, of een hem door zijn bank verstrekte smartcard zoals de ChipKnip) of
- De smartcard (SIM) in zijn persoonlijke GSM telefoon

- Stem Unit (of stemapparaat waarmee de kiezer zijn stem kan indienen,
- 25 bijvoorbeeld:

- Zijn PC met Internet-browser
- Zijn PC met smartcardlezer
- Zijn GSM-telefoon
- Zijn pen, om daarmee zijn stemkeuze aan te kunnen geven op zijn
- 30 poststembiljet

- Stembureau (of wel de Stemverwerking centrale): de instantie waar de kiezer zijn stem via een netwerk moet indienen tijdens het verkiezingsvenster
- Toezichthoudend en controlerend orgaan: een openbaar en van de verkiezingen volledig onafhankelijk orgaan, belast met het toezicht op de verkiezing
- Terugvalsysteem: systeem dat in geval van een storing (of andere vorm van interruptie) die deelname door de kiezer aan de verkiezing onmogelijk maakt, deze toch in staat stelt op andere wijze (bijvoorbeeld per post) zijn stem uit te brengen.

Bij een verkiezing met een elektronisch verkiezingssysteem onderscheiden we de volgende fasen:

- Voorbereidingsfase
 - Centrale verkiezingscommissie stelt het volgende samen:
 - Verkiezingsnaam of -identiteit (EIID)
 - Kiezersregister (dat bevat de kiezers $V_1 \dots V_n$)
 - Publicatie daarvan en mogelijke aanpassingen door de kiezer
 - Kandidatenlijst (dat bevat de kandidaten $C_1 \dots C_m$)
 - Na vaststelling en bevestiging van kiezersregister en kandidatenlijst in een afgeschermd, vertrouwelijk proces:
 - Per kiezer de generatie van K_p of $VPID$ en PW (in dat geval is $K_p = \text{functie } \{VPID, PW\}$)
 - Berekenen of bepalen van een veilige transportvorm naar de kiezer van K_p of van $VPID$ en PW
 - Ingeval K_p door cryptografische vercijfering onder een transportsleutel KEK_t , die uitsluitend transport naar en laden van K_p in de smartcard of SIM van de kiezer mogelijk maakt
 - Ingeval $VPID$ en PW door productie van set verkiezingsbescheiden in gesloten enveloppe (waaronder het voor deze kiezer bedoelde onpersoonlijk Poststembiljet, eventueel met een

aparte Stemkaart), waarbij identiteit en adres van de kiezer alleen buiten op de enveloppe staat en VPID en PW, samen met algemene informatie over de verkiezing, zich binnen de enveloppe bevindt. Zoals eerder gesteld, kan het Poststembiljet ook worden gebruikt voor briefstemmen door die kiezers, die daar voorkeur aan geven of als terugvalsysteem. Op dit Poststembiljet zijn VPID, PW en EIID in ieder geval in machineleesbare vorm gecodeerd en is een overzicht van alle kandidaten vermeld met de mogelijkheid er één als stem te kunnen markeren.

- Berekening van een uitslagreferentiebestand en wel als volgt:
 - Voor iedere kiezer wordt een referentie-uitslag berekend $RnPotVote$
 - Per kiezer n bestaat $RnPotVote$ uit
 - Een kiezerreferentie-identiteit $RnPID = MDC [DES_{mac}(K_p, \text{functie}\{EIID\})]$
 - Voor iedere kandidaat m uit de kandidatenlijst een onderwerpreferentie-identiteit $RnCm = MDC [DES_{mac}(K_p, \text{functie}\{Cm, EIID\})]$
 - Transport naar buiten het afgeschermd, vertrouwelijke proces van
 - Het uitslagreferentiebestand
 - De veilige transportvorm van K_p (of VPID en PW) voor transport naar de kiezer

10238613

- 5

 - Het wissen van alle vertrouwelijke, kiezersgerelateerde informatie waaronder Kp (of VPID en PW)), dan wel opslag daarvan onder een uitsluitend aan het Toezichthoudend en controlerend orgaan bekende cryptografische sleutel KEKctrl
- 10

 - MDC staat voor een cryptografische hash-functie, zoals de op DES gebaseerde Modification Detection Code
 - DES staat voor een symmetrisch cryptografisch algoritme, zoals DES, 3DES of EAS
 - DESmac staat voor een Message Authentication Code berekening met een symmetrisch cryptografisch algoritme, zoals de in ANSI gestandaardiseerde MAC met DES
- 15

 - Het veilig verzenden van Kp of het Poststembiljet naar de juiste kiezer
- 20

 - Publicatie (via een openbaar netwerk) voor de start van de verkiezing van
 - De identiteit van de te houden verkiezing (EIID)
 - Het bevroren kiezersregister
 - De vastgestelde kandidatenlijst
- 25

 - Het referentieuitslagbestand RnPotVote voor alle kiezers
- 30

 - Bij gebruik van GSM-telefoons: automatische installatie bij alle kiezers van de noodzakelijke extra functionaliteit voor stemberekening in hun GSM-telefoon (m.b.v. SIM Tool Kit functionaliteit)

1023861-

- 5 ○ De kiezer stelt (tijdig) vast of hij daadwerkelijk en correct in het kiezersregister is opgenomen, of hij vooraf de beschikking krijgt over de informatie (Kp of VPID en PW, de kandidatenlijst en de EIID) en middelen (afhankelijk van het geboden systeem: PC-browser, smartcardlezer, smartcard, correcte versie SIM en GSM-telefoon), noodzakelijk om aan de verkiezing deel te nemen
- 10 • Het Stembureau (of wel de Stemverwerkingcentrale) installeert een aantal netwerkserverns om tijdens de verkiezingen de stem van iedere kiezer te kunnen ontvangen en wel zodanig, dat de toekomstige verbinding met de Stem Unit van iedere kiezer zal worden beschermd met SSL (of een functioneel vergelijkbare techniek bij gebruik van SMS via GSM-telefoons), waarbij de kiezer eveneens eenduidig zal kunnen vaststellen werkelijk zijn stem bij het Stembureau in te leveren; tevens installeert het Stembureau het referentie-uitslagbestand. Daarnaast voorziet het Stembureau in mogelijkheden om de

15 belasting en het gebruik van het netwerk tussen de Stem Units van kiezers en het Stembureau te kunnen bewaken. Daarnaast installeert het Stembureau een aparte Stemontvangstbevestigingsserver, die aan hetzelfde netwerk is verbonden en ook alleen via SSL toegang van kiezers toestaat.

 - 20 ○ Het Toezichthoudend en controlerend orgaan controleert steekproefsgewijs en via klachtprocedures of de kiezer vooraf van de juiste informatie is voorzien
 - Het Toezichthoudend en controlerend orgaan en ieder ander controleert of omvang en structuur van het referentie uitslagbestand overeenkomen met het kiezersregister en de kandidatenlijst
- 25 • Het verkiezingenvenster zelf

 - De kiezer (n) zelf

 - Stelt vast wat de identiteit van de verkiezing is (EIID)
 - Bepaalt zijn keuze op grond van de publieke kandidatenlijst (Cx)
 - 30 • Maakt met zijn Stem Unit verbinding met het Stembureau

1023861-

- Overtuigt zich ervan dat aan de andere zijde van het netwerk werkelijk het stembureau aanwezig is en de verbinding is beveiligd (standaardfuncties van SSL)
 - Afhankelijk van zijn Stem Unit:
 - Bij een PC-browser, al dan niet in combinatie met een smartcard: ontvangt automatisch als onderdeel van een normale webpagina de noodzakelijke functionaliteit voor het berekenen van zijn stem (als script-taal)
 - Bij een GSM-telefoon: schakelt het vooraf ontvangen SIM Tool Kit programma in om deel te nemen aan deze verkiezing
 - Geeft zijn keuze voor Cx aan zijn Stem Unit. Zijn Stem Unit berekent zijn stem, die uit de volgende twee elementen bestaat en zo samen zijn virtuele stembiljet vormen:
 - zijn kiezeridentiteit $VnPID = DESmac(Kp, functie\{EID\})$
 - zijn specifieke keuze voor kandidaat Cx: $VnC_x = DESmac(Kp, functie\{C_x, EID\})$
 - Zorgt dat zijn Stem Unit zijn virtuele stembiljet daadwerkelijk doorgeeft aan het Stembureau door aanklikken van de juiste functie of intoetsen van de juiste toets
 - Controleert of zijn virtuele stembiljet is aangekomen, door (automatisch) te kijken op de Stemontvangst bevestigingsserver; is dat zo, dan is hij zeker dat zijn stem tijdig is uitgebracht (zijn stemunit berekent $RnPID = MDC(VnPID)$, die weer gelijk is aan $MDC[DESmac(Kp, functie\{EID\})]$, en kijkt of dezelfde RnPID op de Stemontvangst bevestigingsserver aanwezig is); hij bewaart een door de Stemontvangst bevestigingsserver voor hem berekende ontvangstbevestiging (Sign(Kconf, RnPID)).
 - Herhaalt bij twijfel of storingen van het proces of enig onderdeel daarvan zijn stemprocedure als hiervoor beschreven

- Stemt eventueel bij onmogelijkheid dit via het netwerk te doen per post met behulp van zijn Poststembiljet.
 - Weet, dat bij het meermalen indienen van zijn virtuele stembiljet deze als één telt als allen voor dezelfde kandidaat Cx zijn uitgebracht en als ongeldig als ze voor verschillende kandidaten zijn uitgebracht.
- Stembureau (ofwel de Stemverwerkingcentrale, eventueel als taak uitbesteed aan een Onafhankelijke Vertrouwde Derde Partij (TTP))
 - Vervult de rol in de communicatie met de kiezer als hiervoor beschreven
 - Ontvangt ieder virtuele stembiljet als vertrouwelijke informatie, ontdoet deze van iedere tijd- en netwerkinformatie, berekent $RnPID = MDC(VnPID)$, geeft RnPID met het ontvangen virtuele stembiljet door aan de Stemontvangst-bevestigingsserver en slaat het virtuele stembiljet zelf als vertrouwelijke informatie op in een vertrouwelijk Ontvangen Netwerk Stemmen bestand
 - Zorgt dat de Stemontvangst-bevestigingsserver voortdurend alle ontvangen RnPID's na een (kort) tijdsinterval publiceert en kwiteert bij opvragen
 - Verwerkt de (tijdig) binnengekomen Poststembiljetten met dezelfde berekening als die voor de elektronisch uitgebrachte stemmen, voegt deze poststemmen toe aan een vertrouwelijk Ontvangen Post Stemmen-bestand
- Het Toezichthoudend en controlerend orgaan stelt vast of het Stembureau zijn taken correct vervult en bereikbaar is voor alle kiezers
- De Centrale verkiezingscommissie heeft geen specifieke taak tijdens het verkiezingsvenster zelf
- Uitslagfase
 - Het Stembureau (of wel de Stemverwerkingcentrale)

- Sluit de toegang tot het Ontvangen Netwerk Stemmen bestand aan het eind van de verkiezingen en publiceert dit
 - Sluit de toegang tot het Ontvangen Post Stemmen-bestand aan het eind van de verkiezingen of de tijdige inzendtermijn en publiceert dit
 - Publiceert statistische informatie over ontvangen stemmen, kiezers, RnPID's en Poststembiljetten
- De Centrale verkiezingscommissie (en ieder ander)
 - berekent nu de uitslag als volgt:
 - Berekent alle Ontvangen Post Stemmen en Ontvangen Netwerk Stemmen om naar Ontvangen Stem-referenties RnRecVote, door ieder virtuele stembiljet om te rekenen volgens de berekening $RnRecVote = [MDC(VnPID)] // [MDC(VnC_x)]$
 - Zoekt in het uitslagreferentiebestand met RnRecVote de daar aanwezige RnPotVote gegevens
 - Ontdubbelt (dezelfde RnPID en RnC_x combinatie komt meerdere malen voor) en verwijdert onduidelijke keus stemmen (twee of meer RnPID's met verschillende, op zich geldige RnC_x combinaties komen voor)
 - Zoekt in het uitslag referentiebestand met RnRecVote de daar aanwezige RnPotVote gegevens op en bepaalt zo voor welke Kandidaat deze stem telt.
 - Publiceert de verkiezingsuitslag en start daarmee de uitslag beroepstermijn (om kiezers en derden in staat te stellen de uitslag zelf te berekenen en daarna eventueel protest aan te tekenen)
 - Ontvangt tijdens de uitslag beroepstermijn klachten van kiezers over door hun uitgebrachte stemmen die niet voorkomen in de Ontvangen Stemmen bestanden, terwijl ze wel over een geldige ontvangstbevestiging van de stem bevestigingsserver beschikken

1023861~

- Verklaart de uitslag als correct na afloop van de uitslag beroepstermijn, indien geen geldige klachten zijn binnengekomen
 - Verklaart de uitslag als ongeldig na afloop van de uitslag beroepstermijn, indien geldige klachten zijn binnengekomen (de verkiezingen zullen opnieuw moeten worden gehouden)
- De kiezer zelf controleert – desgewenst – of zijn stem, waarvoor hij een ontvangstbevestiging heeft ontvangen, daadwerkelijk voorkomt in de gepubliceerde Ontvangen Stemmen bestanden; indien onjuist, dan dient hij een klacht in
- Derden en de kiezer zelf controleren de uitslagberekening met behulp van de gepubliceerde informatie; indien onjuist, dan dienen zij een klacht in.
- Het Toezichthoudend en controlerend orgaan
 - Controleert de berekeningen van het stembureau op correctheid en plausibiliteit
 - Controleert de juiste afwikkeling van de klachten tijdens de uitslagberoepstermijn
 - Verklaart op grond daarvan of een door de Centrale verkiezingscommissie correct bevonden uitslag ook daadwerkelijk bindend is.

Een uitvoeringsvorm van het elektronische verkiezingssysteem volgens de uitvinding is zodanig ingericht dat de Stemontvangst-bevestigingsserver de anonimiteit van de kiezer beschermt door op ieder verzoek van een kiezer een groep RnPID's te verstrekken i.p.v. alleen de RnPID van de kiezer.

Een andere uitvoeringsvorm van het elektronische verkiezingssysteem volgens de uitvinding is voorzien van middelen voor iedere individuele kiezer om, voorafgaand aan de verkiezing, de faciliteiten te testen met behulp van een teststem en een verdere controle door de kiezer in de vooraf gepubliceerde referentie-uitslag van de kiezer.

Asymmetrisch sleutelgebruik van geheime DES- of 3DES- transportsleutels en KEKctrl kan worden toegepast op basis van de Control Vector-

architectuur voor DES of een vergelijkbare oplossing. Daarmee kunnen risico's over het in verkeerde handen raken van Kp aanzienlijk worden beperkt en beheerst.

Elektronische verkiezingssystemen op basis van een DES-virtueel stembiljet, aangeduid met DVSS, met de hierboven beschreven opbouw hebben de

5 volgende eigenschappen:

1. Relatief eenvoudig verkiezingssysteem, dat volledig is te realiseren binnen op dit moment op grote schaal aanwezige technische voorzieningen (Internet-browsers, DES en 3DES smartcards, GSM-telefoons met SIM-kaarten die DES- en 3DES-berekeningen doen en eenvoudig met SIM Tool Kit van
10 nieuwe functies kunnen worden voorzien).
2. Verkiezingsprotocol is gebaseerd op bekende, reeds gestandaardiseerde cryptografische functionaliteit (MAC en MDC) van een symmetrische algoritme. Door toepassing van deze functies op een andere wijze, dan tot nu voorzien, worden voor dit verkiezingsprotocol functies gecreëerd, waarvoor
15 normaal publieke sleutel algoritmen toegepast zouden moeten worden. Aangezien de laatste technische faciliteiten vereisen, die grootteorden liggen boven die voor een symmetrisch algoritme, is toepassing daarvan binnen de huidige infrastructuren praktisch onmogelijk of ongewenst.
3. Door de eenvoudige opzet is het systeem geheel als "store-and-forward"
20 systeem op te zetten (via SMS bij GSM-telefoon of eenvoudige server contacten bij gebruik van Internet servers en -clients). Daarmee is het systeem met eenvoudige middelen op grote schaal inzetbaar, is extra of reserve capaciteit eenvoudig te realiseren en is het systeem inherent ongevoelig voor aanvallen of allerlei vormen van misbruik.
- 25 4. Gestemd wordt met behulp van een virtueel stembiljet, dat alleen door de kiezer zelf kan worden berekend. Het systeem is in staat meerdere virtueel stembiljetten van dezelfde kiezer als één stem te herkennen. Daarmee is het mogelijk om op eenvoudige wijze het systeem ongevoelig te maken voor storingen of interrupties en mag de kiezer bij twijfel zijn (zelfde) stem
30 nogmaals uitbrengen, zelfs met een andere techniek als waarmee hij het de eerste maal deed.
5. Openbare controle op het verkiezingssysteem is (op grote schaal) mogelijk.

6. Er is een volledige scheiding tussen bij de verkiezing betrokken partijen, zoals die van organisator, stembureau, controleorgaan, kandidaat en kiezer.
7. Het systeem voldoet aan alle eisen, die daaraan bij verkiezingen voor overheidsorganen worden gesteld of kan daar op eenvoudige wijze aan voldoen.
8. Individuele cryptografische stemberekening per stemgerechtigde wordt uitgevoerd door de standaard Internetbrowser zonder verdere bijzondere Internet technologie, anders dan toepassing van een script-taal in die browser, waarbij alle geheime, individuele, maar onpersoonlijke informatie uitsluitend door hemzelf via het toetsenbord wordt ingegeven en de betrokken Internet server, die de verkiezingen verzorgt, uitsluitend algemene, niet vertrouwelijke informatie verstrekt.
9. Controle op voorbereiding, plausibiliteit, telling en uitslag door een ieder, onafhankelijk van de organisator van de verkiezingen.
10. Controle voor individuele stemgerechtigde op correcte verwerking van zijn stem in de uitslag, onafhankelijk van de organisator van de verkiezingen.
11. Het verkiezingssysteem maakt combinaties met andere vormen van stemmen (zoals bijvoorbeeld stemmen per stembus, per post, per (GSM) telefoon met SMS mogelijk, zonder dat de stemgerechtigde vooraf zijn keuze kenbaar maakt; het systeem staat toe, dat een stemgerechtigde zijn stem langs verschillende kanalen uitbrengt, waarbij – als dat correct is gebeurd – dat toch maar als één stem telt.
12. De stemgerechtigde stemt op basis van een hem verstrekt Poststembiljet of Stemkaart (hierna aangeduid als “stembescheiden”), waarop zich alle geheime, individuele, maar onpersoonlijke informatie bevindt die hij nodig heeft om zijn stem uit te brengen; de stembescheiden kunnen de stemgerechtigde per post worden toegezonden.
13. Het verkiezingssysteem heeft sterke eigenschappen, die de invloed van storingen of onderbrekingen van of aanvallen op Internet of netwerk of client of server componenten minimaliseren, dan wel eenvoudige vormen van back-up/vervanging toestaan.

1023861-

14. Het verkiezingssysteem staat toe dat een stemgerechtigde zijn keuze voor een kandidaat meer dan éénmaal doorgeeft, bijvoorbeeld om te compenseren voor storingen of overbelasting van Internet; daarbij kan deze ook besluiten zijn keuze d.m.v. een andere techniek kenbaar te maken (die voor deze verkiezing is toegestaan, bijvoorbeeld een poststem).

- Het systeem biedt daarmee een hoge weerstand tegen storingen en onderbrekingen van een netwerk als Internet.

- Het systeem staat toe dat de servers, die belast zijn met het ontvangen van de stemmen op meerdere plaatsen en netwerklocaties kunnen worden ingericht, zonder dat daartoe speciale voorzieningen nodig zijn om de uitgebrachte stemmen na afloop te kunnen consolideren

- Het systeem staat toe dat bij storingen, onderbrekingen of herstarts van enig bij de verkiezing betrokken server men niet hoeft te voorkomen dat individuele stemmen dubbel voorkomen; alle reeds in buffers van servers aanwezige stemmen kunnen eenvoudig worden doorgezonden naar de server(s) waarin alle stemmen worden verzameld; er is namelijk geen risico van dubbeltellingen.

15. Het verkiezingssysteem kent een kritische initialisatiefase, maar deze is eenvoudig te isoleren op een aparte, off-line server of PC in een geïsoleerde ruimte, eventueel uitbesteed aan of bediend door een Onafhankelijke Vertrouwde Derde Partij (TTP); zowel de invoer als de uitvoer van dit initialisatie proces omvatten geen vertrouwelijke gegevens, anders dan de gegevens van de af te drukken stembescheiden na. Deze dienen volgens de bij poststemmingen gebruikelijke procedures aan een vertrouwde drukker, die normaal diensten aanbiedt bij poststemmen, ter hand te worden gesteld.

16. Het Verkiezingssysteem staat toe meerdere kanalen voor de stemgerechtigde te implementeren om zijn stem uit te brengen, waaronder

- zijn Internet-PC met toetsenbord en beeldscherm, via een hem toegezonden stembescheiden

- zijn Internet-PC met toetsenbord, beeldscherm en gekoppelde chipkaartlezer, via een 3DES chipkaart, die reeds in zijn bezit is en die

automatisch wordt voorzien van de voor de verkiezing noodzakelijke
geheime, individuele, maar onpersoonlijke gegevens

- 5 ○ zijn Internet-PC met toetsenbord, beeldscherm en niet gekoppelde
chipkaartlezer, via zijn bankkaart met ChipKnip-technologie en hem
toegezonden stembescheiden
- Via zijn GSM-telefoon, een daarmee te maken SMS-bericht en hem
toegezonden stembescheiden
- Via zijn moderne telefoon die SMS toestaat, een daarmee te maken
SMS-bericht en hem toegezonden stembescheiden
- 10 ○ Via zijn GSM-telefoon, een daarmee uit te voeren WAP-conversatie en
hem toegezonden stembescheiden
- Via een hem vooraf verstrekt, individueel stembiljet, dat door hem per
post kan worden ingezonden
- 15 ○ Via een hem vooraf verstrekt, individueel stembiljet, dat door hem in
een stembus kan worden gedeponneerd.

1023861-

CONCLUSIES

1. Elektronisch verkiezingssysteem voor het verzamelen en tellen van stemmen van individuele kiezers die gebruikmaken van een elektronisch stemapparaat
5 in een verkiezing met een lijst van te kiezen onderwerpen waaruit een onderwerp wordt gekozen door een individuele kiezer waarbij de stemmen worden verzonden door middel van een datanetwerk, omvattende:

middelen voor het genereren van een unieke persoonlijke sleutel voor iedere kiezer op een lijst van voor de verkiezing ingeschreven kiezers, welke
10 unieke persoonlijke sleutel aan de individuele kiezer wordt verstrekt;

middelen voor het genereren van een unieke onderwerpcodes voor ieder onderwerp op de lijst van te kiezen onderwerpen;

middelen voor het genereren van een referentie-uitslag voor iedere individuele kiezer bevattende alle virtuele stembiljetten voor de individuele kiezer,
15 waarbij een unieke kiezerreferentie-identiteit wordt berekend uit een unieke verkiezingscode voor de verkiezing en de unieke persoonlijke sleutel van de kiezer, waarbij voor ieder onderwerp op de lijst van de door de kiezer te kiezen onderwerpen een unieke onderwerp-referentie-identiteit wordt berekend uit de unieke onderwerpcodes en de unieke persoonlijke sleutel van de kiezer en waarbij de
20 berekende referentie-identiteiten deel uitmaken van de virtuele stembiljetten;

middelen voor het opslaan van de referentie-uitslagen van de individuele kiezers;

middelen voor het laden van instructies in het stemapparaat van de individuele kiezer om het stemapparaat in te richten voor het berekenen van een
25 unieke kiezeridentiteit uit de unieke verkiezingscode voor de verkiezing en de unieke persoonlijke sleutel van de kiezer die aan de kiezer is verstrekt, voor het berekenen van een unieke onderwerpidentiteit van het door de kiezer gekozen onderwerp uit de unieke onderwerpcodes van het gekozen onderwerp en de unieke persoonlijke sleutel van de kiezer en voor het genereren van het virtuele stembiljet met de, met
30 gebruikmaking van het stemapparaat berekende identiteiten;

middelen om het virtuele stembiljet door het stemapparaat te verzenden over het datanetwerk;

1023861-

middelen voor het ontvangen en verzamelen van het door het stemapparaat verzonden virtuele stembiljet;

middelen voor het verifiëren van elk verzameld virtueel stembiljet met betrekking tot de aanwezigheid in de referentieuitslagen van de kiezers;

5 middelen voor het tellen van de stemmen;

middelen voor het vaststellen van de verkiezingsuitslag, gekenmerkt door middelen voor het valideren van de stemmen van de ontvangen virtuele stembiljetten, welke middelen zodanig zijn ingericht dat, wanneer een stel van twee of meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een
10 virtueel stembiljet van het stel wordt gevalideerd als een geldige stem van de betreffende kiezer en de overige virtuele stembiljetten worden aangemerkt als duplicaat, mits de virtuele stembiljetten van het stel identiek zijn voor het door de kiezer gekozen onderwerp, anders worden alle virtuele stembiljetten van het stel aangemerkt als ongeldig.

15 2. Elektronisch verkiezingssysteem voor het verzamelen en tellen van stemmen van individuele kiezers die gebruikmaken van een elektronisch stemapparaat in een verkiezing met een lijst van te kiezen onderwerpen waaruit een combinatie van onderwerpen wordt gekozen door een individuele kiezer waarbij de stemmen worden verzonden door middel van een datanetwerk, omvattende

20 middelen voor het genereren van een unieke persoonlijke sleutel voor iedere kiezer op een lijst van voor de verkiezing ingeschreven kiezers, welke unieke persoonlijke sleutel aan de individuele kiezer wordt verstrekt;

middelen voor het genereren van een unieke combinatiecode voor iedere combinatie van onderwerpen op de lijst van te kiezen onderwerpen;

25 middelen voor het genereren van een referentie-uitslag voor iedere individuele kiezer bevattende alle virtuele stembiljetten voor de individuele kiezer, waarbij een unieke kiezerreferentie-identiteit wordt berekend uit een unieke verkiezingscode voor de verkiezing en de unieke persoonlijke sleutel van de kiezer, waarbij voor iedere combinatie van onderwerpen op de lijst van de door de kiezer te
30 kiezen onderwerpen een unieke combinatie-referentie-identiteit wordt berekend uit de unieke combinatiecode en de unieke persoonlijke sleutel van de kiezer en waarbij de berekende referentie-identiteiten deel uitmaken van de virtuele stembiljetten;

middelen voor het opslaan van de referentie-uitslagen van de individuele kiezers;

middelen voor het laden van instructies in het stemapparaat van de individuele kiezer om het stemapparaat in te richten voor het berekenen van een
 5 unieke kiezeridentiteit uit de unieke verkiezingscode voor de verkiezing en de unieke persoonlijke sleutel van de kiezer die aan de kiezer is verstrekt, voor het berekenen van een unieke combinatie-identiteit van de door de kiezer gekozen combinatie van onderwerpen uit de unieke combinatiecode van de gekozen combinatie van onderwerpen en de unieke persoonlijke sleutel van de kiezer en voor het genereren
 10 van het virtuele stembiljet met de, met gebruikmaking van het stemapparaat berekende identiteiten;

middelen om het virtuele stembiljet door het stemapparaat te verzenden over het datanetwerk;

middelen voor het ontvangen en verzamelen van het door het
 15 stemapparaat verzonden virtuele stembiljet;

middelen voor het verifiëren van elk verzameld virtueel stembiljet met betrekking tot de aanwezigheid in de referentie-uitslagen van de kiezers;

middelen voor het tellen van de stemmen;

middelen voor het vaststellen van de verkiezingsuitslag, gekenmerkt
 20 door middelen voor het valideren van de stemmen van de ontvangen virtuele stembiljetten, welke middelen zodanig zijn ingericht dat wanneer een stel van twee of meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een virtueel stembiljet van het stel wordt gevalideerd als een geldige stem van de betreffende kiezer en de overige virtuele stembiljetten worden aangemerkt als
 25 duplicaat, mits de virtuele stembiljetten van het stel identiek zijn voor de door de kiezer gekozen combinatie van onderwerpen, anders worden alle virtuele stembiljetten van het stel aangemerkt als ongeldig.

3. Elektronisch verkiezingssysteem volgens conclusie 1 of 2, met het kenmerk, dat de middelen voor het valideren van de stemmen deel uitmaken van de
 30 middelen voor het verifiëren van de ontvangen virtuele stembiljetten.

4. Elektronisch verkiezingssysteem volgens conclusie 1 of 2, met het kenmerk, dat de middelen voor het valideren van de stemmen deel uitmaken van de middelen voor het tellen van de stemmen.

5. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, gekenmerkt door middelen voor het genereren van een ontvangstbewijs waarin is aangeduid dat een virtueel stembiljet van het stemapparaat van de kiezer is ontvangen en middelen voor het leveren van het ontvangstbewijs met een unieke ontvangstbevestigingswaarde in leesbare vorm aan het stemapparaat van de kiezer.

6. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, gekenmerkt door middelen voor het openbaar maken van de lijst van voor de verkiezing ingeschreven kiezers, de lijst van te kiezen onderwerpen en de referentie-uitslagen van de individuele kiezers om gelegenheid te geven voor algemeen onderzoek voorafgaand aan de verkiezing en middelen voor iedere individuele kiezer om de referentie-uitslag van de individuele kiezer te onderzoeken.

7. Elektronisch verkiezingssysteem volgens conclusie 5 of 6 in afhankelijkheid van conclusie 5, gekenmerkt door middelen voor het openbaar maken van de verkiezingsuitslag bevattende de geldige stemmen die na het verifiëren en het valideren zijn toegekend voor de verzamelde virtuele stembiljetten om gelegenheid te geven voor algemeen onderzoek, en middelen voor iedere individuele kiezer om met gebruikmaking het verkregen ontvangstbewijs de aanwezigheid van het door het stemapparaat van de kiezer verzonden virtueel stembiljet te onderzoeken.

8. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, gekenmerkt door communicatiemiddelen voor het communiceren van de unieke persoonlijke sleutel naar iedere kiezer op de lijst van voor de verkiezing ingeschreven kiezers, welke communicatiemiddelen tenminste een uit de groep bevattende middelen voor het elektronisch opslaan van de unieke persoonlijke sleutel in een chipkaart van de kiezer, data-communicatiemiddelen voor het communiceren van de unieke persoonlijke sleutel naar de kiezer zoals het Internet of een vast en/of mobiel datacommunicatienetwerk, waaronder een Short Message Service, en middelen voor het verschaffen van de unieke persoonlijke sleutel in een voor mensen en/of machines leesbare vorm op een fysieke drager, zoals een tekstbericht op papier voor communicatie per post naar de kiezer, omvatten.

1023861-

9. Elektronisch verkiezingssysteem volgens conclusie 8, met het kenmerk, dat het stemapparaat is ingericht om werkzaam te zijn verbonden met middelen voor het invoeren van data, welke invoermiddelen tenminste een uit de groep bevattende een chipkaartlezer, een toetsenbord, een muis, een scherm, een streepjescode-lezer en spraakomzettingmiddelen, omvatten.

10. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, met het kenmerk, dat de middelen voor het ontvangen en verzamelen van virtuele stembiljetten zijn ingericht voor het ontvangen en verzamelen van virtuele stembiljetten die anders dan door het stemapparaat van de kiezer zijn verzonden, zoals fysieke stembiljetten die per post zijn ontvangen en in virtuele stembiljetten zijn omgezet door middelen voor het automatisch lezen en omzetten van stembiljetten.

11. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies in afhankelijkheid van conclusie 1, met het kenmerk, dat de middelen voor het genereren van een unieke onderwerpcodes voor ieder onderwerp op de lijst van te kiezen onderwerpen voor de verkiezing, de middelen voor het genereren van een unieke persoonlijke sleutel en de middelen voor het genereren van een referentie-uitslag voor iedere kiezer op de lijst van de voor de verkiezing ingeschreven kiezers zijn voorzien van middelen voor het uitvoeren van cryptografische bewerkingen en berekeningen.

12. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies in afhankelijkheid van conclusie 2, met het kenmerk, dat de middelen voor het genereren van een unieke combinatiecode voor iedere combinatie van onderwerpen op de lijst van te kiezen onderwerpen voor de verkiezing, de middelen voor het genereren van een unieke persoonlijke sleutel en de middelen voor het genereren van een referentie-uitslag voor iedere kiezer op de lijst van voor de verkiezing ingeschreven kiezers zijn voorzien van middelen voor het uitvoeren van cryptografische bewerkingen en berekeningen.

13. Elektronisch verkiezingssysteem volgens conclusie 15 of 16, met het kenmerk, dat de middelen voor het uitvoeren van cryptografische bewerkingen en berekeningen zijn ingericht voor symmetrische encryptie.

14. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, met het kenmerk, dat middelen voor het bij het stemapparaat van de kiezer

aanbieden van de lijst onderwerpen waarvan een onderwerp of combinatie van onderwerpen door de kiezer wordt gekozen met het stemapparaat, de middelen voor het laden van de instructies in het stemapparaat van de kiezers, de middelen voor het ontvangen en verzamelen van het door het stemapparaat verzonden virtuele stembiljet en de ontvangstbevestigingsmiddelen worden ondersteund door een computersysteem met tenminste een computerserver.

15. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, met het kenmerk, dat de middelen voor het laden van de instructies in het stemapparaat van een kiezer, de middelen voor het ontvangen en verzamelen van het door het stemapparaat verzonden virtuele stembiljet, de ontvangstbevestigingsmiddelen en het stemapparaat, zijn ingericht om met elkaar of afzonderlijk te voorzien in beveiligde datatransmissie over het datanetwerk.

16. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, met het kenmerk, dat de middelen voor het genereren van de unieke persoonlijke sleutel voor iedere individuele kiezer, de middelen voor het genereren van de unieke onderwerpcode of de unieke combinatiecode voor ieder onderwerp of combinatie van onderwerpen van de lijst van in de verkiezing te kiezen onderwerpen, de middelen voor het genereren van de referentie-uitslag voor iedere kiezer op de lijst van de voor de verkiezing ingeschreven kiezers, de middelen voor het verifiëren van het verzamelde virtuele stembiljet van de kiezer met betrekking tot de aanwezigheid in de referentie-uitslag van de kiezer, de middelen voor het valideren van de verzamelde virtuele stembiljetten, de middelen voor het tellen van de stemmen en de middelen voor het vaststellen van de verkiezingsuitslag op basis van de getelde stemmen worden ondersteund door een computersysteem dat is ingericht om te worden bedreven onder supervisie van een onafhankelijke toezichthouder.

17. Elektronisch verkiezingssysteem volgens een van de voorgaande conclusies, met het kenmerk, dat het stemapparaat tenminste een uit de groep bevattende een persoonlijke computer en vaste en mobiele communicatie-apparaten voor het verschaffen van toegang tot het datanetwerk, omvat.

18. Werkwijze voor een elektronische verkiezing voor het verzamelen en tellen van de stemmen van individuele kiezers die gebruikmaken van een elektronisch stemapparaat in een verkiezing met een lijst van te kiezen onderwerpen

waaruit een onderwerp wordt gekozen door een individuele kiezer, en de stemmen worden verzonden door middel van een datanetwerk, omvattende de stappen van:

- het genereren van een unieke persoonlijke sleutel voor iedere individuele kiezer op een lijst van voor de verkiezing ingeschreven kiezers;
- 5 het verstrekken van de unieke persoonlijke sleutel aan de individuele kiezer;
- het genereren van een unieke onderwerpcodes voor ieder onderwerp op de lijst van in de verkiezing te kiezen onderwerpen;
 - het genereren van een referentie-uitslag voor iedere individuele
- 10 kiezer bevattende alle mogelijke virtuele stembiljetten voor de individuele kiezer, waarbij voor ieder individuele kiezer een unieke kiezerreferentie-identiteit wordt berekend uit een unieke code voor de verkiezingen en de unieke persoonlijke sleutel van de kiezer, voor ieder onderwerp op de lijst van te kiezen onderwerpen een unieke onderwerp referentie-identiteit wordt berekend uit de unieke onderwerpcodes en de
- 15 unieke persoonlijke sleutel van de kiezer, waarbij de berekende referentie-identiteiten deel uitmaken van de virtuele stembiljetten;
- het opslaan van de referentie-uitslagen van de individuele kiezers;
 - het laden van instructies in het stemapparaat van de kiezer;
 - het kiezen van een onderwerp uit de lijst van te kiezen onderwerpen
- 20 met gebruikmaking van het stemapparaat van de individuele kiezer door de unieke persoonlijke sleutel, die aan de kiezer is verstrekt, en de unieke onderwerpcodes voor het gekozen onderwerp in te voeren in het stemapparaat;
- het genereren van een virtueel stembiljet met gebruikmaking van de in het stemapparaat geladen instructies, waarbij een unieke kiezeridentiteit wordt
- 25 berekend uit de unieke code van de verkiezing en de unieke persoonlijke sleutel van de kiezer en een unieke onderwerpidentiteit wordt berekend uit de unieke onderwerpcodes van het gekozen onderwerp en de unieke persoonlijke sleutel van de kiezer en waarbij de berekende identiteiten deel uitmaken van het virtueel stembiljet;
- het verzenden van het virtueel stembiljet over het datanetwerk;
- 30 het ontvangen en verzamelen van het door het stemapparaat verzonden stembiljet;

1023861-

het verifiëren van het verzameld virtueel stembiljet met betrekking tot de aanwezigheid in de referentie-uitslagen van de kiezers;

het tellen van de stemmen, en

het vaststellen van de verkiezingsuitslag op basis de getelde
 5 stemmen van de kiezers, gekenmerkt door de stap van het valideren van de stemmen van de verzamelde virtuele stembiljetten op een zodanige wijze dat, wanneer een stel van twee of meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een virtueel stembiljet van het stel wordt gevalideerd als een geldige stem en de overige virtuele stembiljetten van het stel worden aangemerkt als duplicaat, mits
 10 de virtuele stembiljetten van het stel identiek zijn voor het door de kiezer gekozen onderwerp, anders worden alle virtuele stembiljetten van het stel aangemerkt als ongeldig.

19. Werkwijze voor een elektronische verkiezing voor het verzamelen en tellen van de stemmen van individuele kiezers die gebruikmaken van een
 15 elektronisch stemapparaat in een verkiezing met een lijst van te kiezen onderwerpen waaruit een combinatie van onderwerpen wordt gekozen door een individuele kiezer, en de stemmen worden verzonden door middel van een datanetwerk, omvattende de stappen van:

het genereren van een unieke persoonlijke sleutel voor iedere
 20 individuele kiezer op een lijst van voor de verkiezing ingeschreven kiezers;

het verstrekken van de unieke persoonlijke sleutel aan de individuele kiezer;

het genereren van een unieke combinatiecode voor iedere combinatie van onderwerpen op de lijst van in de verkiezing te kiezen onderwerpen;

25 het genereren van een referentie-uitslag voor iedere individuele kiezer bevattende alle mogelijke virtuele stembiljetten voor de individuele kiezer, waarbij voor ieder individuele kiezer een unieke kiezerreferentie-identiteit wordt berekend uit een unieke code voor de verkiezing en de unieke persoonlijke sleutel van de kiezer, voor iedere combinatie van onderwerpen op de lijst van te kiezen
 30 onderwerpen een unieke combinatie-referentie-identiteit wordt berekend uit de unieke combinatiecodes en de unieke persoonlijke sleutel van de kiezer, waarbij de berekende referentie-identiteiten deel uitmaken van de virtuele stembiljetten;

1023861-

het opslaan van de referentie-uitslagen van de individuele kiezers;

het laden van instructies in het stemapparaat van de kiezer;

- 5 het kiezen van een combinatie van onderwerpen uit de lijst van te kiezen onderwerpen met gebruikmaking van het stemapparaat van de individuele kiezer door de unieke persoonlijke sleutel, die aan de kiezer is verstrekt, en de unieke combinatiecode voor de gekozen combinatie van onderwerpen in te voeren in het stemapparaat;

- 10 het genereren van een virtueel stembiljet met gebruikmaking van de in het stemapparaat geladen instructies, waarbij een unieke kiezeridentiteit wordt berekend uit de unieke code van de verkiezing en de unieke persoonlijke sleutel van de kiezer en een unieke combinatie-identiteit wordt berekend uit de unieke combinatiecode van de gekozen combinatie van onderwerpen en de unieke persoonlijke sleutel van de kiezer en waarbij de berekende identiteiten deel uitmaken van het virtueel stembiljet;

- 15 het verzenden van het virtueel stembiljet over het datanetwerk;

het ontvangen en verzamelen van het door het stemapparaat verzonden stembiljet;

het verifiëren van het verzameld virtueel stembiljet met betrekking tot de aanwezigheid in de referentie-uitslagen van de kiezers;

- 20 het tellen van de stemmen, en

- 25 het vaststellen van de verkiezingsuitslag op basis de getelde stemmen van de kiezers, gekenmerkt door de stap van het valideren van de stemmen van de verzamelde virtuele stembiljetten op een zodanige wijze dat, wanneer een stel van twee of meer virtuele stembiljetten met een identieke kiezeridentiteit is verzameld, een virtueel stembiljet van het stel wordt gevalideerd als een geldige stem en de overige virtuele stembiljetten van het stel worden aangemerkt als duplicaat, mits de virtuele stembiljetten van het stel identiek zijn voor de door de kiezer gekozen combinatie van onderwerpen, anders worden alle virtuele stembiljetten van het stel aangemerkt als ongeldig.

- 30 20. Werkwijze voor een elektronische verkiezing volgens conclusie 18 of 19, gekenmerkt door de stap van het genereren van een ontvangstbewijs met een unieke ontvangstbevestigingswaarde in leesbare vorm om aan te duiden dat een over

1023861-

het datanetwerk verzonden virtueel stembiljet is ontvangen en waarbij het ontvangstbewijs wordt geleverd aan het stemapparaat van de kiezer.

21. Werkwijze voor een elektronische verkiezing volgens een van de conclusies 18 tot en met 20, gekenmerkt door de stap van het openbaar maken van de
 5 lijst van voor de verkiezing ingeschreven kiezers, de lijst van de te kiezen onderwerpen in de verkiezing, de referentie-uitslagen van de individuele kiezers om gelegenheid te geven voor algemeen onderzoek voorafgaand aan de verkiezing en de stap van het verschaffen van middelen voor iedere individuele kiezer om de referentie-uitslag van de individuele kiezer te onderzoeken.

10 22. Werkwijze voor een elektronische verkiezing volgens een van de conclusies 20 of 21 in afhankelijkheid van conclusie 20, gekenmerkt door de stap van het openbaar maken van de verkiezingsuitslag bevattende de geldige stemmen die na het verifiëren en het valideren zijn toegekend voor de verzamelde virtuele stembiljetten om gelegenheid te geven voor algemeen onderzoek, en de stap van het
 15 verschaffen van middelen voor iedere individuele kiezer om met gebruikmaking van het verkregen ontvangstbewijs de aanwezigheid van het door het stemapparaat van de kiezer verzonden virtueel stembiljet te onderzoeken.

23. Werkwijze voor een elektronische verkiezing volgens een van de voorgaande conclusies 18 tot en met 22, gekenmerkt door de stap van het ontvangen
 20 en verzamelen van virtuele stembiljetten die anders dan door het stemapparaat van de kiezer zijn verzonden, zoals stembiljetten die per post worden ontvangen, waarbij de ontvangen fysieke stembiljetten met gebruikmaking van middelen voor het automatisch lezen worden omgezet in virtuele stembiljetten.

24. Werkwijze voor een elektronische verkiezing volgens een van de
 25 conclusies 18 tot en met 23, met het kenmerk, dat de unieke identiteit voor ieder onderwerp of iedere combinatie van onderwerpen van de te kiezen onderwerpen, de unieke kiezeridentiteit en de referentie-uitslag voor iedere individuele kiezer op de lijst van voor de verkiezing ingeschreven kiezers cryptografisch worden gegenereerd en berekend.

30 25. Werkwijze voor een elektronische verkiezing volgens conclusie 24, met het kenmerk, dat de identiteiten en de referentie-uitslag worden gegenereerd en berekend voor symmetrische encryptie.

26. Werkwijze voor een elektronische verkiezing volgens een van de conclusies 18 tot en met 25, met het kenmerk, dat de stappen van het genereren van een unieke persoonlijke sleutel voor iedere individuele kiezer op de lijst van voor de verkiezing ingeschreven kiezers, de unieke identiteit voor ieder onderwerp of iedere combinatie van onderwerpen op de lijst van te kiezen onderwerpen, de referentie-uitslag voor iedere individuele kiezer en de stappen van het verifiëren van een verzameld virtueel stembiljet van een individuele kiezer met betrekking tot de aanwezigheid in de referentie-uitslag van de kiezer, het valideren van de verzamelde virtuele stembiljetten, het tellen van de stemmen en het vaststellen van de verkiezingsuitslag worden uitgevoerd onder supervisie van een onafhankelijke toezichthouder.

27. Werkwijze voor een elektronische verkiezing volgens een van de conclusies 18 tot en met 26, met het kenmerk, dat de stap van het verstrekken van de unieke persoonlijke sleutel aan de individuele kiezer op de lijst van voor de verkiezing ingeschreven kiezers tenminste een stap omvat uit een groep van stappen omvattende het elektronisch opslaan van de unieke persoonlijke sleutel in een chipkaart van de kiezer, het aan de kiezer verstrekken van de unieke persoonlijke sleutel door middel van een datanetwerk zoals het Internet of een vast en/of mobiel datacommunicatienetwerk, waaronder een Short Message Service, SMS, en het verschaffen van de unieke persoonlijke sleutel in een voor mensen en/of machines leesbare vorm op een fysieke drager, zoals een tekstbericht op papier voor toezending per post naar de kiezer.

28. Werkwijze voor een elektronische verkiezing volgens conclusie 27, met het kenmerk, dat de fysieke drager geschikt is om te worden gebruikt als fysiek stembiljet met de lijst van te kiezen onderwerpen of combinaties van onderwerpen, welk stembiljet, nadat de kiezer een keus heeft gemaakt, wordt gedeponéerd bij een stembureau.

29. Werkwijze voor een elektronische verkiezing volgens een van de conclusies 18 tot en met 28, met het kenmerk, dat het stemapparaat tenminste een omvat van een groep omvattende een persoonlijke computer en vaste en mobiele datacommunicatie apparatuur die is ingericht om met gebruikmaking van browser-

1023861-

software toegang te verschaffen tot het datanetwerk en waarbij de instructies automatisch van het datanetwerk in het stemapparaat worden geladen.

30. Werkwijze voor een elektronische verkiezing volgens conclusie 29, met het kenmerk, dat het datanetwerk het Internet omvat en het stemapparaat een
- 5 persoonlijke computer omvat die werkzaam is gekoppeld met het Internet waarbij de instructies in de persoonlijke computer worden geladen door middel van een Java-applet dat is opgenomen in een web-pagina die door de kiezer wordt geselecteerd om deel te nemen aan de verkiezing.
31. Werkwijze voor een elektronische verkiezing volgens conclusie 30,
- 10 met het kenmerk, dat het stemapparaat GSM-communicatieapparatuur met een Subscriber Identity Module-SIM-kaart omvat en waarbij de instructies in de SIM-kaart van de communicatieapparatuur worden geladen voor een kiezer die met gebruikmaking van genoemde communicatieapparatuur deelneemt aan de verkiezingen.
- 15 32. Computerprogramma-product omvattende programmacodemiddelen die zijn opgeslagen op een voor een computer leesbaar medium voor het verrichten van de of een deel van de stappen van de werkwijze volgens conclusies 18 tot en met 31, indien geladen in het intern werkgeheugen van de computer en uitgevoerd door de computer.
- 20 33. Computerprogramma-product omvattende programmacodemiddelen die zijn opgeslagen op een voor een computer leesbaar medium, ingericht als een stel instructies die worden geladen in een computerprogramma dat werkzaam is op een door een computer gestuurd stemapparaat voor het verrichten van de stappen volgens een van de conclusies 18, 19 en 29 tot en met 31, indien geladen in een intern
- 25 werkgeheugen van de computer en uitgevoerd door de computer.

