BIJLAGE
1.3

Hoogheemraadschap van
Rijnland

IV

uw kenmerk:

De Verenigde Vergadering.

uw brief van:

ons kenmerk: 03.04446

bijlagen: - 6 -

inlichtingen:

doorkiesnummer:

onderwerp: Waterschapsverkiezing 2004. Leiden, 4 maart 2003

1. Voorstel

Volgens bijgevoegd besluit wordt uw vergadering voorgesteld:

- de verkiezing van 2004 via stemmen per brief te laten plaatsvinden;
- in één kiesdistrict de categorieën ingezetenen, gebouwd, ongebouwd en bedrijven (± 250.000 ingezetenen; ±330.000 stemgerechtigden) – naast het stemmen per brief – ook het stemmen per personal computer (PC) via het Internet aan te bieden;
- een krediet van €2.575.000 ter beschikking te stellen voor de organisatie van de verkiezing per post en via Internet.

2. Inleiding

Vanwege de reorganisatie van de Zuid-Hollandse waterschappen is de reguliere waterschapsverkiezing van het voorjaar van 2003 uitgesteld tot 2004. De verkiezing zal plaatsvinden op een nader door Gedeputeerde Staten te bepalen datum of periode in het vierde kwartaal van 2004. Het algemeen bestuur, het dagelijks bestuur en de voorzitter van het op te heffen hoogheemraadschap van Rijnland oefenen, volgens het Overgangsreglement, de wettelijke taken uit voor de verkiezing van de leden van het algemeen bestuur van het nieuwe hoogheemraadschap. Bijvoorbeeld het algemeen bestuur van Rijnland bepaalt de stemmethode, het dagelijks bestuur houdt het kiezersregister bij en stelt het hoofdstembureau in, en de dijkgraaf is voorzitter van het hoofdstembureau.
De verantwoordelijkheid van Rijnland voor de voorbereiding en organisatie van de verkiezing betekent dat de inliggende waterschappen formeel geen bevoegdheden hebben ten aanzien van de verkiezing. Ten einde de voorbereiding optimaal te laten verlopen worden de inliggende waterschappen hierbij echter wel betrokken. Dit voorstel is bijvoorbeeld voorgelegd aan de dagelijkse besturen van de inliggende waterschappen. Daarnaast heeft ons college de dijkgraven van de inliggende waterschappen uitgenodigd zitting te nemen in het hoofdstembureau, waardoor zij niet alleen betrokken kunnen worden bij de uitvoering van de verkiezing, maar ook tijdens de voorbereiding daarvan.

3. Probleemstelling

In het rapport "Evaluatie waterschapsverkiezingen 1999" is als conclusie opgenomen dat "ondanks de dalende opkomstpercentages van de verkiezingen voor de Provinciale Staten en het Europese Parlement zijn de opkomstpercentages voor de waterschapsverkiezingen gelijk gebleven of zelfs gestegen. Met het behaalde opkomstpercentage van gemiddeld 24% kijkt de stuurgroep dan ook terug op geslaagde waterschapsverkiezingen." "In het totaal heeft

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

Uw vergadering heeft in december 1999 ingestemd met het voorstel in 2001 een onderzoek te houden onder de stemgerechtigden over de stemmethode(n) voor de volgende waterschapsverkiezingen. Hiervoor hebt u het positieve saldo ad. €32.000 van de verkiezingen 1999 gereserveerd. Door het uitstel van de verkiezing is het onderzoek verschoven naar eind 2002.

5.1 Mening kiezers over stemmen in stemlokaal of via Internet
Ondertussen zijn er onderzoeksrapporten verschenen waaruit blijkt dat de Nederlandse kiezer een voorkeur heeft voor het stemmen via Internet ten opzichte van stemmen in een stemlokaal. Dit blijkt onder andere uit een landelijk onderzoek van het Elektronic-highway Platform Nederland onder 3.000 kiesgerechtigden (zie bijlage 3). In februari 2001 gaf tijdens dit onderzoek één op de twee internettende Nederlanders aan, als ze de mogelijkheid zouden hebben tussen Internet of het klassieke stemlokaal, te stemmen via Internet. Een recenter panelonderzoek van Burger@overheid van oktober 2002 geeft aan dat de meerderheid van de niet-stemmers wel zou hebben gestemd als dat via Internet kon (zie bijlage 4).
Bovenstaande onderzoeken hebben het verschil tussen het stemmen op locatie – stembureau – en het locatieonafhankelijk stemmen – stemmen via Internet – met elkaar vergeleken. Er is geen vergelijking gemaakt tussen twee locatieonafhankelijke stemmethoden: stemmen per post en stemmen via Internet. De positieve resultaten uit de onderzoeken kunnen hierdoor niet rechtstreeks worden doorvertaald naar waterschapsverkiezingen.

5.2 Onderzoek elektronisch stemmen door TNO in opdracht van Rijnland
Gezien bovenstaande en andere onderzoeken werd een nader onderzoek door Rijnland onder stemgerechtigden enigermate overbodig. Het aandachtsgebied van het onderzoek is derhalve verschoven naar de gebruikers- en beveiligingsaspecten van het elektronisch stemmen. Om een antwoord te kunnen geven op de eerste twee vraagpunten van de probleemstelling van §3. Eind 2002 heeft TNO in opdracht van Rijnland hiervoor een onderzoek uitgevoerd (zie bijlage 5).

In dit onderzoek is een aantal stemmethoden met elkaar vergeleken. Internetstemmen is vergeleken met eerder toegepaste methoden als stemmen per post en stemmen per telefoon. Daarnaast is een vergelijking gemaakt met internetbankieren.

Onderstaand overzicht uit het rapport geeft de risicoanalyse van internetstemmen weer:

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

dreiging waartegen geen geheel afdoende maatregel genomen kan worden is de installatie van een trojan op de PC van een kiezer die de stemmen manipuleert. De kans hierop is klein. Door elke kiezer een stemkaart te verstrekken met een persoonlijk identificatienummer en bij elke kandidaat een persoonlijk kandidatennummer met een verwachte respons, blijft het stemgeheim gewaarborgd en is het omzetten van een stem naar een andere kandidaat – die een hacker graag gekozen ziet - niet meer mogelijk. Op deze manier wordt een controle ingebouwd, waarin de kiezer zijn stem controleert. De kiezer weet dan zeker dat zijn stem is geteld (zie bijlage 6).

Tegenover deze extra risico's bestaat de mogelijkheid om bij internetstemmen de authenticatie te verbeteren – ten opzichte van stemmen per post en stemmen per telefoon - door het vooraf per post opsturen van een kaartje met gegevens van de kiesgerechtigden. Dit kaartje kan gecombineerd worden met de vooraankondiging, zoals die bij de vorige verkiezing is verzonden. Het levert dus niet een extra verzending op, maar wel meer vooraankondigingen omdat voorheen één vooraankondiging per adres werd bezorgd. Indien een kiezer per Internet wil stemmen, dient hij zich online te registreren. Op de verkiezingssite kan de kiezer door het invoeren van de gegevens van het ontvangen kaartje zich registreren. De kiezer geeft via Internet een zelf gekozen wachtwoord op. Door middel van het opgeven van een hint kan hij zijn wachtwoord opvragen als hij deze is vergeten. Daarnaast kan hij aangeven of hij behoefte heeft aan een e-mailnotificatie. Als hij zijn e-mail doorgeeft wordt hij op de hoogte gehouden van de stemperiode. Geregistreerde kiezers krijgen vervolgens per post een stemcode toegezonden, die ze naast het wachtwoord dienen in te vullen op de verkiezingssite. Vervolgens kunnen ze hun stem uitbrengen.
Een andere mogelijkheid van een hogere beveiliging van de authenticatie bij internetstemmen is het opsturen van een kras-PIN-code. Deze krascode wordt meegezonden met de stembescheiden. Om een stem uit te brengen dient de kiezer de PIN-code zichtbaar te krassen. Op Internet kan hij zich authentiseren door de code in te toetsen, gecombineerd met zijn geboortedatum. Bij deze optie hoeft de kiezer zich niet vooraf te registreren.

6. Stemvarianten

Onderstaand worden vier mogelijke stemvarianten voor de verkiezing 2004 met elkaar vergelijken. Terugvallen op het systeem van stemlokalen is daarbij vanzelfsprekend buiten beschouwing gelaten.

6.1 Stemmen per post

De stemmethode van de verkiezing van 1995. Door de introductie van het stemmen per post werd toen het "opkomstpercentage" verviervoudigd. Nadeel van deze methode is dat de verwerking van de stemmen kostbaar, arbeidsintensief en tijdrovend is. Kostbaar met name vanwege de portikosten van de antwoordenvelop en het scannen van de stembiljetten. Arbeidsintensief omdat bij het openen van de retourenveloppen en scannen van de stembiljetten veel handwerk nodig is. Tijdrovend omdat de uitslag pas na vijf dagen na de sluiting van de stemming kan worden vastgesteld.

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

Meerkosten en extra interne capaciteit t.o.v. stemmen per post (variant 6.1):
Het internetstemmen en stemmen per telefoon besparen in drukwerkkosten en in de kosten voor de stemopneming, maar vergen wel een investering voor het opzetten en exploiteren van het systeem. De netto meerkosten van de volledig elektronische variant bedragen €150.000. Er is voor deze stemvariant 800 uur extra interne capaciteit nodig.

6.4 Stemmen per post en stemmen via Internet
Deze variant is gelijk aan variant 6.2, maar het stemmen per telefoon wordt vervangen door het stemmen per personal computer (PC) via het Internet. Deze combinatie van stemmethoden voldoet aan de vereisten van de probleemstelling van paragraaf 3. Gezien de uitkomsten van het rapport van TNO kan het internetstemmen wellicht niet volledig voldoen aan het beveiligingsniveau van stemmen per telefoon. Echter indien er technische mankementen of andere bezwaren zijn met het internetstemmen, kan de kiezer – gelijk aan variant 6.2 – ook per brief stemmen, zonder dat eerst een schriftelijk verkiezingspakket behoeft te worden aangevraagd. Op deze wijze is het verloop van een verkiezing gegarandeerd en kan de kiezer bepalen – al naar gelang zijn voorkeur – op welke wijze hij stemt. Daarnaast is het mogelijk bij internetstemmen de authenticatie beter te waarborgen.

Meerkosten en extra interne capaciteit t.o.v. stemmen per post (variant 6.1):
Het internetstemmen bespaart in de kosten voor de stemopneming, maar vergt wel een investering voor het opzetten en exploiteren van het systeem. De netto meerkosten voor de stemvariant per post en stemmen via Internet – indien deze variant voor alle categorieën en kieskringen wordt toegepast – bedragen €325.000. Er is voor deze stemvariant 500 uur extra interne capaciteit nodig.

7. Afweging
Voor bovenstaande stemvarianten zijn aan de aspecten van de probleemstelling punten toegekend:

Aspect	**Stemvarianten**			
	6.1 Post	6.2 Post / telefoon	6.3 Internet / telefoon	6.4 Post / Internet
Opkomst	2	3	1	4
Gemak	2	3	2	4
Veiligheid	4	3	1	2
Kosten	*	*	*	*
Totaal	**8**	**9**	**4**	**10**
Ad*: kostenverschil t.o.v. gemiddelde <10%; derhalve niet meegenomen.				

Wij zijn van mening dat het opkomstpercentage positief wordt beïnvloed als de kiezer meerdere stemmethoden krijgt aangeboden. Op deze manier kan tegemoet worden gekomen aan de wensen die de verschillende gebruikersgroepen en leeftijdscategorieën stellen aan stemfaciliteiten (zie §4.3 onderzoek TNO). Het stemmen per telefoon kent een aantal nadelen. Het stemmen per PC via het Internet zien wij als een goede vervanging. Van het

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

8. Experiment kiesdistrict versus geheel gebied per post en via Internet

Onderstaand is een vergelijking gemaakt tussen het houden van een experiment met de stemvariant stemmen per post en via Internet in één kiesdistrict voor alle categorieën en deze variant voor het gehele gebied aan te bieden.

	Experiment in één kiesdistrict	Geheel gebied
Kiezer	Aparte communicatie aan kiezers van één kiesdistrict. Kan voor de overige kiezers in de andere twee districten verwarrend werken. Bijvoorbeeld kiezers uit Leiden boven de Rijn kunnen wel via Internet stemmen, onder de Rijn kunnen ze dat niet.	Helderheid voor kiezer.
Uitvoering	Er zullen twee soorten verkiezingspakketten moeten worden ontwikkeld. Dit vergt extra capaciteit.	Eén verkiezingspakket voor geheel gebied. Besparing is verwerkt in netto meerkosten.
Risico's	De beveiligingsaspecten zijn voor kiesdistrict en geheel gebied gelijk. Kosten herverkiezing voor alle categorieën maximaal: €250.000; - Ingezetenen: €195.000 - Gebouwd: €49.000 - Ongebouwd: €5.000 - Bedrijven: €1.000 Bij een eventuele herverkiezing heeft maximaal eenderde van de bestuursleden een kortere inwerkperiode. Toelating medio december i.p.v. 27 oktober 2004.	De beveiligingsaspecten zijn voor kiesdistrict en geheel gebied gelijk. Kosten herverkiezing voor alle categorieën en kiesdistricten maximaal: €750.000 Bij een eventuele herverkiezing hebben de bestuursleden een kortere inwerkperiode. Toelating medio december i.p.v. 27 oktober 2004.
Financieel	Netto meerkosten €275.000 te vergoeden door BZK, VenW en de Unie	Netto meerkosten €325.000 te vergoeden door BZK, VenW en de Unie. Additionele vergoeding door externen van €50.000, zal mogelijk niet meer kunnen worden gerealiseerd.

Voorshands heeft het college zijn voorkeur bepaald op het experiment model.

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

VERBETERDE EXPEDITIE

11. Kredietvoorstel

Het totale krediet voor de verkiezing bedraagt €2.575.000; waarvan €2.275.000 voor de directe verkiezingen, €25.000 voor de indirecte verkiezingen (o.a. bekendmakingen, drukwerk, verwerking stemmen) en €275.000 voor het internetstemmen. Bij de berekening van de kapitaallasten die uit dit krediet voortvloeien is geen rekening gehouden met de bijdragen van het ministerie van BZK, het ministerie van V&W en de Unie van Waterschappen; deze bijdragen zijn wel een voorwaarde om het internetstemmen te laten doorgaan.

De kapitaallasten van het krediet worden met ingang van 2005 ten laste van de begroting van het nieuwe hoogheemraadschap van Rijnland gebracht. In de meerjarenraming 2003-2007 is rekening gehouden met een krediet van €2.360.000.

Ter vergelijking. In 1999 bedroeg het krediet voor de verkiezingen van de besturen van Rijnland, De Oude Rijnstromen, Groot-Haarlemmermeer en Wilck en Wiericke €2.130.500. De samenwerking tussen Rijnland en de inliggende waterschappen was toen al bijna volledig, derhalve zijn er amper kostenbesparingen te realiseren op drukwerk- en portikosten.

12. Consequenties voor de belastingtarieven

De consequenties voor de belastingtarieven zijn alleen berekend over de kosten van de verkiezingen. De kosten voor het experiment met internetstemmen worden gedekt door bijdragen van derden. Uitgaande van een afschrijvingstermijn van 4 jaar en een rentepercentage van 5% bedragen de kapitaallasten in 2005 €676.000. Uitgedrukt in de kosten per belastingeenheid bedragen de kapitaal- en overige exploitatiekosten vanaf 2005:

ingezetenenomslag:	€0,72	per woonruimte
omslag gebouwd:	€0,0024	per waarde-eenheid
omslag ongebouwd:	€0,09	per hectare
verontreinigingsheffing:	€0,13	per vervuilingseenheid

Dijkgraaf en hoogheemraden,

E.H. van Tuyll van Serooskerken,
dijkgraaf.

J. van Wijk,
secretaris.

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

1e investeringsbesluit 2003

No. 0306577

DE VERENIGDE VERGADERING VAN HET HOOGHEEMRAADSCHAP VAN RIJNLAND;

Gelezen het voorstel van dijkgraaf en hoogheemraden d.d. 4 maart 2003, nr. 03.04446
Gehoord het advies van de commissies Bestuurszaken en Financiën.

BESLUIT:

I. De verkiezing in 2004 van de vertegenwoordigers van de categorieën ingezetenen, gebouwde- en ongebouwde onroerende zaken en bedrijven te laten plaatsvinden via stemmen per brief.

II. Voorshands in één kiesdistrict de categorieën ingezetenen, gebouwd, ongebouwd en bedrijven (±330.000 stemgerechtigden) – naast het stemmen per brief – ook het stemmen per personal computer (PC) via het Internet aan te bieden.

III. Ten behoeve van de organisatie van de waterschapsverkiezing in 2004 een krediet van €2.575.000 beschikbaar te stellen: €2.275.000 voor directe verkiezingen, €25.000 voor indirecte verkiezingen en €275.000 voor het experiment.

IV. Het krediet voor het experiment met internetstemmen beschikbaar te stellen onder de voorwaarde dat kostendekkende bijdragen worden ontvangen van:
- het ministerie van Binnenlandse Zaken en Koninkrijkrelaties;
- het ministerie van Verkeer en Waterstaat;
- de Unie van Waterschappen.

V. De kapitaallasten van het krediet met ingang van 2005 ten laste van de begroting van het nieuwe hoogheemraadschap van Rijnland te brengen en de verkiezingskosten gedurende vier jaar af te schrijven vanaf 2005 conform de volgende verdeling

Aandeel	Totaal	Waterkeringszorg	Waterkwantiteits-beheer	Waterkwaliteits-beheer
Ingezetenen	82%	27,3	27,3	27,4
Gebouwd	17%	8,5	8,5	
Ongebouwd	1%	0,5	0,5	
Totaal	100%	36,3	36,3	27,4

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Hoogheemraadschap van
Rijnland

Bijlage 1: Kostenoverzicht

Bedrag	Specificatie
75.000	Samenstellen kiezersregister, aanpassen GIBS/STUF
35.000	Verkiezingswebsite
15.000	Software kandidaatstelling
25.000	Externe juridische begeleiding
220.000	Bekendmakingen en advertenties verkiezing in diverse media (o.a. krant, radio, tv en billboards)
850.000	Drukwerk verkiezingen: ontwerpen, lithograferen, drukken, printen en couverteren
700.000	Portokosten vooraankondiging, verkiezingspakket en verwerking van de stemmen
80.000	Kosten call center 0800-1321
75.000	Externe begeleiding
200.000	Onvoorzien
25.000	Renteverlies
2.300.000	**SUBTOTAAL**
	Kosten specifiek voor internetstemmen
50.000	Functionele ontwerpen gebruikersapecten, techniek, beveiliging en testen
100.000	Bouw stemapplicatie Internet
75.000	Uitvoeringsexploitatie internetstemmen
35.000	Extra communicatie voor internetstemmen
5.000	Evaluatieonderzoek
10.000	Onvoorzien
275.000	**SUBTOTAAL**
2.575.000	**TOTAAL**

Archimedesweg 1
postadres:
postbus 156
2300 AD Leiden
telefoon (071) 5 168 268
telefax (071) 5 123 916 internet : www.rijnland.net e-mail: post@rijnland.net

Bijlage 3

Panelonderzoek Burger@overheid oktober 2002

1-11-2002

Stemmen via internet

Hieronder volgen in hoofdlijnen de uitkomsten van het onderzoek.

- De vragenlijst is op gesteld in nauwe samenwerking met burger@overheid
- De vragenlijst heeft een week online gestaan van 22 tot 30 oktober 2002.
- Panelprofiel:
    - 55% is man, 45% vrouw
    - 66% doet betaald werk, 13% studeert
    - Het meest worden sites van gemeentes bezocht (86%). De site van de belastingdienst wordt bezocht door 86% van de panelleden62% is het afgelopen half jaar wel eens op een site van een ministerie geweest.
    - De resultaten voor het eerste onderzoek zijn gewogen voor geslacht, leeftijd en opleiding. Dit wil zeggen dat op basis van deze achtergrondvariabelen het panel representatief is voor de Nederlandse internetter.
    - Bij de onderstaande resultaten wordt uit gegaan van de totale steekproef (N=minimaal 759) tenzij anders vermeld.

BLOK C

Hoe groot acht u de kans dat u de komende verkiezingen gaat stemmen?

Zeer klein… zeer groot (5pnts)

Klein/zeer klein	*Weet niet*	*Groot/zeer groot*
(6%)	*(5%)*	*(89%)*

Zeer klein, klein, weet niet

→ Zou u wel gaan stemmen als u via internet zou kunnen stemmen?

N=81

Ja	*(56%)*
Nee	*(19%)*
Weet niet	*(24%)*

Welke manier van stemmen heeft uw voorkeur bij de tweede kamer verkiezingen:

- Stemmen via klassieke stemlokaal *(22%)*
- **Stemmen via internet** *(62%)*
- Geen voorkeur *(16%)*

Opvallende verschillen

- Stemmen via internet is voor alle opleidingscategorieën zeer zeker een optie. Voor MBO en LBO geldt dit het sterkst. Hoger opgeleiden lijken iets voorzichtiger in hun voorkeur voor internet stemmogelijkheid.
- Mannen hebben een sterkere voorkeur om via internet te stemmen dan vrouwen. (67% vs. 58%)

Stel: U zou de mogelijkheid hebben om via internet te stemmen. Hoe groot acht u de kans dat u uw stem uitbrengt via internet?

Klein/zeer klein	*Weet niet*	*Groot/zeer groot*
(14%)	*(10%)*	*(75%)*

Heb je een goed beeld van wat stemmen via internet inhoudt?

- Helemaal geen beeld *(4%)*
- Vaag beeld *(41%)*
- **Duidelijk beeld** *(55%)*

Opvallende verschillen

- Mannen zeggen een duidelijker beeld te hebben van wat stemmen via internet inhoudt dan vrouwen (66% vs. 44%)

BLOK D

Hier volgt een aantal stellingen. Kunt u aangeven in welke mate u het eens bent?

Als ik via internet kan stemmen, wil ik ook meebeslissen bij specifieke belangrijke issues in de politiek

Oneens/zeer mee oneens	*Neutraal*	*Eens/Zeer mee eens*
(12%)	*(38%)*	*(50%)*

Opvallende verschillen

- Dit geldt sterker voor mannen dan voor vrouwen,
- en voor hoger opgeleiden

Stemmen via internet brengt de politiek dichterbij de mensen

Oneens/zeer mee oneens	*Neutraal*	*Eens/Zeer mee eens*
(19%)	*(33%)*	*(48%)*

Opvallende verschillen

- Dit geldt iets sterker voor vouwen dan voor mannen.

Stemmen via internet komt de democratie ten goede

Oneens/zeer mee oneens	*Neutraal*	*Eens/Zeer mee eens*
(15%)	*(42%)*	*(43%)*

Opvallende verschillen

- Er zijn geen opvallende verschillen binnen de groepen.

Nederland moet een voortrekkersrol in Europa vervullen als het gaat om stemmen via internet

Oneens/zeer mee oneens	*Neutraal*	*Eens/Zeer mee eens*
(18%)	*33(%)*	*(49%)*

Opvallende verschillen

- Dit geldt sterker voor mannen dan voor vrouwen.

Hoe lang denkt u dat u nog zal duren voordat we in Nederland via internet zullen kunnen stemmen?

- binnen 1 jaar *(5%)*
- **1-3 jaar** *(48%)*
- 3 – 5 jaar *(32%)*
- langer dan 5 jaar *(14%)*
- nooit *(1%)*

Opvallende verschillen

- 80% van de respondenten verwacht binnen nu en 5 jaar te kunen stemmen via internet, waarvan 48% dit reeds verwacht binnen 3 jaar.
- Vrouwen verwachten dat stemmen via internet sneller mogelijk zal zijn. Mannen zijn iets sceptischer.

In maart zijn de Provinciale Statenverkiezingen. Hoe groot acht u de kans dat u de komende verkiezingen gaat stemmen?

Klein/zeer klein	*Weet niet*	*Groot/zeer groot*
(17%)	*(13%)*	*(70%)*

Zeer klein, klein, weet niet

→ Zou u wel gaan stemmen als u via internet zou kunnen stemmen?

N=221

Ja	*Nee*	*Weet niet*
(59%)	*(27%)*	*(14%)*

Bijlage 4

Persbericht van het Electronic-highway Platform Nederland (EPN)

Zes miljoen Nederlanders verkiezen internet boven stemlokaal

DEN HAAG, 15 maart 2001 – Nederlanders kiezen bij de volgende tweede kamer verkiezingen in 2002 het liefst via internet. Dit blijkt uit een landelijk onderzoek van het Electronic-highway Platform Nederland. Nu al verkiest een op de twee Nederlanders, als ze de mogelijkheid zouden hebben tussen internet of het klassieke stemlokaal, te stemmen via internet. Dit ondanks de gevaren die stemmen via internet nu nog met zich meebrengt zoals identificatie, veiligheid, betrouwbaarheid (fraudegevoeligheid) en privacy.

Vooral het internettende deel van de bevolking, nu 53% zegt massaal (68%) internet te verkiezen boven het traditionele stemlokaal. Opvallend is dat zelfs mensen die zeggen geen toegang te hebben tot internet in een op de vier gevallen toch al via internet willen stemmen.

Problemen die rond stemmen via internet spelen zoals veiligheid, betrouwbaarheid, privacy (het gevaar van family vote) vormen voor het merendeel van de ondervraagden geen beletsel om via internet te stemmen. Van de mensen die zeggen het stemlokaal te verkiezen boven internet geeft 17% aan de veiligheid van stemmen via internet niet te vertrouwen. Slechts 6% geeft privacy redenen op. Met name de mensen die internet niet gebruiken zeggen angst te hebben voor de techniek (45%). Veel van de ondervraagden geven ook aan dat stemmen in het buurthuis, het schoollokaal gewoon gezelliger is. Ook is het behouden van traditie voor veel mensen een belangrijke overweging te blijven stemmen in het stemlokaal.

Het onderzoek wijst tevens uit dat stemmen via internet opkomstverhogend kan werken. Van de ondervraagden zegt 78% bij de vorige 2e kamerverkiezingen gestemd te hebben. Op de vraag aan de niet stemmers of deze wel zouden gaan stemmen als ze dit via internet zouden kunnen, zei 24% in dat geval wel te zullen stemmen.

In het kader van het project Kiezen op Afstand is het ministerie van Binnenlandse Zaken en Koninkrijksrelaties momenteel bezig met proefprojecten op het gebied van identificatiemethoden en wordt gewerkt aan een landelijk digitaal kiezersregister. In 2003 zal bij de provinciale Statenverkiezingen een grootschalig experiment worden gedaan. Op dit moment laat de Kieswet stemmen via internet nog niet toe.

Eerder onderzoek van EPN toonde aan dat een meerderheid van de Nederlandse gemeenten wil deelnemen aan experimenten met stemmen via internet bij verkiezingen. Uit het onderzoek kwam naar voren dat gemeenten meer voordelen zien in stemmen via internet en per telefoon (elektronisch stemmen) dan ouderwets met een potlood of een stemmachine. Gemeenten oordeelden dat elektronisch stemmen sneller en betrouwbaarder is. Bovendien kan er geen misverstand bestaan over de uitgebrachte stem en kan de verkiezingsuitslag snel worden vastgesteld. Gemeenten hopen verder dat het opkomstpercentage stijgt als de kiezer niet meer door weer en wind naar het stemlokaal moet. De gemeenten verwachten dat ze nog ongeveer vijf jaar moeten wachten

Bijlage 5

TNO Technische Menskunde

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek / Netherlands Organisation for Applied Scientific Research

TNO Technische Menskunde
Kampweg 5
Postbus 23
3769 ZG SOESTERBERG

www.tno.nl

T 0346 356 211
F 0346 353 977

TNO-rapport

TM-02-C066

ELS: Beveiligings- en gebruikersaspecten van elektronisch stemmen voor het Hoogheemraadschap van Rijnland

Datum	19 december 2002
Auteur(s)	M.P. van Esch-Bussemakers, J.M.E. Geers*, P.G. Maclaine Pont**, H.J. Vink*
Exemplaarnummer	
Oplage	16
Aantal pagina's	34
Aantal bijlagen	2
Opdrachtgever	De heer S. Bouwman, Hoogheemraadschap Rijland, Leiden
Projectnaam	Rijnland elektronisch stemmen
Projectnummer	013.72192

*Werkzaam bij TNO-FEL; **TNO-TPD

Rap.nr. TM-02-C066

TNO Technische Menskunde
Soesterberg

ELS: Beveiligings- en gebruikersaspecten van elektronisch stemmen voor het Hoogheemraadschap van Rijnland

M.P. van Esch-Bussemakers, J.M.E. Geers, P.G. Maclaine Pont en H.J. Vink

SAMENVATTING

Vraagstelling: Het Hoogheemraadschap van Rijnland wil voor de verkiezingen van 2004 overwegen of overgestapt kan worden naar een combinatie van stemmen per telefoon en stemmen per PC (via Internet). TNO voerde hiervoor een haalbaarheidsonderzoek uit dat zich richtte op twee aspecten, namelijk de techniek en de houding van de burger, waarin onderzocht of een betrouwbaar kiessysteem kan worden aangeboden en werd gekeken naar de gebruiksvriendelijkheid en gebruikersacceptatie van een dergelijk systeem.
Werkwijze: Via workshops en (scenario) analyses (techniek en gebruik) werd informatie verzameld en werden mogelijke problemen in kaart gebracht over door het Hoogheemraadschap van Rijnland aangegeven zwaartepunten. Aan de workshops namen vertegenwoordigers van het Hoogheemraadschap van Rijnland en TNO deel.
Resultaten: Het onderzoek op het gebied van beveiliging laten zien dat de risico's bij Internet stemmen niet groter zijn dan bij telefonisch stemmen of stemmen per post. Wel bestaat bij Internet stemmen een aantal dreigingen die zich niet voordoen bij de andere vormen van stemmen en die kunnen worden opgevangen door bijvoorbeeld het verlengen van de verkiezingstermijn. Wat betreft de gebruikersaspecten laat het onderzoek zien dat de combinatie van stemmen via de telefoon en stemmen via Internet de populatie van stemgerechtigden voldoende in staat stelt een stem uit te brengen. Belangrijk hierbij blijft echter naast het verschaffen van de mogelijkheid tot stemmen, hoe bereid kiezers zijn om te gaan stemmen. De kiezers doordringen van het belang van hun stem en het doel van de verkiezingen zal in de communicatie rond de verkiezingen een extra aandachtspunt moeten blijven.
Conclusie: Aan de ene kant is er op dit moment geen softwarepakket op de markt dat voldoet aan de eisen op het gebied van beveiliging en gebruiksvriendelijkheid, hetgeen betekent dat door het Hoogheemraadschap van Rijnland geïnvesteerd zou moeten worden in de technologie. Het is de vraag of een dergelijke investering rendeert bij de relatief lage frequentie van de verkiezingen (een maal in de 4 jaar). Daarnaast verdient het aanbeveling een andere benadering te kiezen in de communicatie met de uiteenlopende doelgroepen en voor verschillende stemalternatieven (telefoon en Internet). Tevens dient extra aandacht besteed te worden aan de gebruiksvriendelijkheid van het systeem. Hierbij moet o.a. gedacht worden aan het realiseren van een adequate foutafhandeling, terugkoppeling en gebruikerstesten.

1 INLEIDING

Het Hoogheemraadschap van Rijnland dient elke vier jaar verkiezingen uit te schrijven voor het kiezen van een algemeen bestuur. In 2004 zullen wederom verkiezingen gehouden worden[1]. In 1995 en 1999 heeft het Hoogheemraadschap van Rijnland de nieuwe mogelijkheid geboden te stemmen per post in plaats van op een stembureau. Dit was erg populair en het opkomstpercentage werd hierdoor verhoogd van 4% naar 24%. Met dit opkomstpercentage is het Hoogheemraadschap van Rijnland tevreden. In 1999 was het tevens mogelijk telefonisch te stemmen. Van de mogelijkheid per telefoon te stemmen werd toen door 10% van de kiezers gebruik gemaakt (Centrum voor Marketing Analyses, 1999; Lausberg, 2001).

Voor de komende verkiezingen in 2004 wil het Hoogheemraadschap van Rijnland de mogelijkheid bestuderen telefonisch stemmen aan te bieden in combinatie met stemmen via Internet. Dit om de klantvriendelijkheid te verhogen en de kosten te verminderen[2]. Stemmen per post is namelijk kostbaar door de omvangrijke verwerking van de stembiljetten. Mogelijk is elektronisch stemmen (per telefoon en Internet) een goedkoper alternatief. Het Hoogheemraadschap van Rijnland heeft TNO gevraagd om ondersteuning te bieden bij het beantwoorden van een aantal vragen door middel van een haalbaarheidsonderzoek. In dit project heeft TNO expertise geleverd op het gebied van gebruiksvriendelijkheid, gebruikersacceptatie en technische veiligheidsaspecten van stemmen via Internet. Het haalbaarheidsonderzoek heeft zich gericht op twee aspecten van het elektronisch kiezen: de techniek en de houding van de burger. Ten aanzien van de techniek werd onderzocht of een betrouwbaar kiessysteem kan worden aangeboden en ten aanzien van de houding van de burger werd onderzocht of deze toe is aan een nieuwe stemmethode en waar bij de invoering op gelet moet worden.

Belangrijk is dat de objectieve en subjectieve (beleving) betrouwbaarheid van de verkiezingen gewaarborgd is en een zelfde niveau van beveiliging verkregen wordt als bij de eerder gebruikte stemmethoden (stemmen per post en telefoon). De betrouwbaarheid moet zodanig zijn dat de uitslag een representatieve weergave van de intentie van de kiezer is.
Als stemmen via Internet niet haalbaar blijkt, zal in 2004 waarschijnlijk uitsluitend de mogelijkheid van stemmen per post aangeboden worden.

In dit rapport wordt in hoofdstuk 2 de achtergrond gegeven van het stemmen bij het Hoogheemraadschap van Rijnland. In hoofdstuk 3 worden de beveiligingsaspecten nader belicht. In hoofdstuk 4 wordt gekeken naar de stemgerechtigden en of zij met de voorgestelde methodes voldoende in staat worden gesteld hun stem uit te brengen. In hoofdstuk 5 worden de toekomstige technologische mogelijkheden van elektronische verkiezingen beschreven. Als laatste worden in hoofdstuk 6 de conclusies en aanbevelingen van het haalbaarheidsonderzoek gepresenteerd.

---

[1] Deze verkiezingen zijn anderhalf jaar later dan oorspronkelijk gepland vanwege het samengaan van een aantal waterschappen.
[2] Het kosten-aspect zal in dit haalbaarheidsonderzoek niet worden meegenomen.

Het stemmen moet voor de kiezer niet te ingewikkeld zijn. Dit houdt onder meer in, dat

- het niet wenselijk is gebruikersnaam en wachtwoord apart aan de kiezers te versturen;
- het niet wenselijk is, dat de kiezers speciale software moeten installeren om te kunnen stemmen of speciale instellingen moeten doen op hun PC. Er moet uitgegaan worden van een standaard browser en een standaard Internet verbinding;
- het niet wenselijk is, dat de kiezers speciale hardware moeten installeren om te kunnen stemmen, zoals bijvoorbeeld een chipkaartlezer.

2.3 Drempelverlaging

De kiezer is niet gebonden aan thuis stemmen. Daarom moeten de benodigdheden die voor het stemmen noodzakelijk zijn, zoals gebruikersnaam en wachtwoord gemakkelijk mee te nemen zijn. Dit zou bijvoorbeeld kunnen in de vorm van een kaartje van creditkaartformaat, waarop de benodigde gegevens staan en een korte handleiding. Ook zou het drempelverlagend kunnen werken als geen onbekend wachtwoord nodig is, maar de kiezer gebruik kan maken van iets dat bij hem bekend is, zoals verjaardagsdatum of de meisjesnaam van zijn moeder. Dit lijkt echter in de praktijk niet haalbaar. In de eerste plaats moet identificatie van de kiezer plaatsvinden, daarna authentisatie (vaststellen dat de kiezer hoort bij de geclaimde identiteit). Voor identificatie is eenduidig invoeren van een ID, bijvoorbeeld naam, noodzakelijk. Er bestaat echter geen eenduidig ID dat bij kiezer en waterschap bekend is. Het kan bijvoorbeeld zijn, dat de kiezer zijn naam inclusief voorletters anders invoert dan bij het waterschap geregistreerd staat, waardoor identificatie niet mogelijk is. Invoeren van een sofi-nummer biedt weinig voordelen, omdat de meeste kiezers hun nummer niet uit het hoofd kennen. Ook is dit niet direct mogelijk, omdat het sofi-nummer bij het Hoogheemraadschap van Rijnland niet bekend is. Een probleem bij authentisatie is, dat het een bij kiezer en waterschap bekend wachtwoord bij teveel mensen in de omgeving van de kiezer ook bekend is (zoals zijn geboortedatum), waardoor zij in staat zijn in zijn naam te stemmen. In andere gevallen is het wachtwoord niet geregistreerd bij het Hoogheemraadschap van Rijnland (zoals bijv. de meisjesnaam van de moeder).

2.4 Bevestiging en controle

Het is belangrijk dat mensen een bevestiging krijgen van het feit dat hun stem op de verkiezingssite ontvangen is. Anders zullen ze verschillende keren proberen te stemmen en er mogelijk van uitgaan dat het niet gelukt is te stemmen via Internet. Het is echter niet wenselijk, dat in dit responsbericht aangegeven wordt op wie de stem uitgebracht is. Er blijft dan namelijk op de PC een bewijs achter op wie gestemd is en dit zou door iemand anders nagezocht kunnen worden. Het is een discussiepunt of de kiezer in staat moet zijn achteraf zijn stem te controleren en of deze meegeteld heeft in de einduitslag. Enerzijds is het niet wenselijk dat de kiezer in staat is om te bewijzen hoe hij gestemd heeft. Dit om het verkopen van stemmen of het stemmen onder dwang te voorkomen of in ieder geval de kans erop te verminderen. Anderzijds biedt de mogelijkheid zijn stem te controleren de kiezer veel vertrouwen in de stemmethode en (heel belangrijk) is het de mogelijkheid om manipulatie van stemmen te detecteren. Een optie is om de kiezer de mogelijkheid te bieden zijn stem achteraf te controleren, alleen aan te bieden in een

een aanval of fraude over Internet naar verwachting groter. Op een relatief eenvoudige en geautomatiseerde wijze kan locatie-onafhankelijk ingegrepen worden in het stemproces.

3.2 Risicoanalyse beveiliging en maatregelen

In de onderstaande tabel worden de stappen van het telefonisch en Internet verkiezingsproces opgesomd. Daarbij worden de dreigingen benoemd die een rol spelen bij deze verkiezingsmethoden. Ter illustratie wordt het elektronisch stemmen naast een alledaagse Internetapplicatie gezet die ook een hoge betrouwbaarheids- en beveiligingsgraad vereist, namelijk Internet bankieren. Na onderstaande tabel wordt per processtap een toelichting gegeven op de dreigingen en wordt een indicatie gegeven van de kans dat een dergelijke dreiging optreedt en een indicatie van de impact die dit zou hebben. Ook wordt aangegeven welke maatregelen vooraf genomen kunnen worden of welk noodscenario in werking gezet dient te worden als een dergelijke dreiging werkelijkheid wordt. Daarbij is het natuurlijk van belang vast te kunnen stellen dat de dreiging daadwerkelijk optreedt. Indien mogelijk wordt ook aangegeven hoe dit te doen is. Voor de stappen die niet genoemd worden zijn geen dreigingen gedefinieerd.

Telefonisch stemmen	**Internet stemmen**	**Internet bankieren**
1. Kiezer ontvangt gebruikersnaam en wachtwoord *Dreiging: gebruikersnaam en wachtwoord vallen in verkeerde handen*	1. Kiezer ontvangt gebruikersnaam en wachtwoord *Dreiging: gebruikersnaam en wachtwoord vallen in verkeerde handen*	1. Klant ontvangt apparaatje, dat in combinatie met chippas en PIN-code gebruikt kan worden voor authentisatie *Dreiging: chippas en PIN-code worden ontvreemd*
2. Kiezer belt aangegeven telefoonnummer *Dreiging: apparatuur niet beschikbaar wegens storing*	2. Kiezer gaat naar aangegeven website *Dreiging: apparatuur niet beschikbaar wegens storing* *Dreiging: andere website doet zich voor als verkiezingswebsite* *Dreiging: apparatuur niet beschikbaar wegens (Distributed) Denial of Service ((D)DOS) aanval*	2. Klant gaat naar aangegeven website *Dreiging: apparatuur niet beschikbaar wegens storing* *Dreiging: andere website doet zich voor als bankwebsite* *Dreiging: apparatuur niet beschikbaar wegens (D)DOS aanval*
3. Kiezer authentiseert zich via gebruikersnaam en wachtwoord *Dreiging: Valse generatie van gebruikersnaam en wachtwoord*	3. Kiezer authentiseert zich via gebruikersnaam en wachtwoord *Dreiging: Valse generatie van gebruikersnaam en wachtwoord*	3. Klant authentiseert zich via chippas en apparaat.
4. Kiezer maakt keuze voor kandidaat *Dreiging: kiezer wordt gedwongen bepaalde keuze te maken*	4. Kiezer maakt keuze voor kandidtaat *Dreiging: kiezer wordt gedwongen bepaalde keuze te maken*	4. Klant voert transacties in *Dreiging: klant wordt gedwongen bepaalde transacties in te voeren*
5. Kiezer bevestigt keuze *Dreiging: door storing gaat stem verloren*	5. Kiezer bevestigt keuze *Dreiging: door storing gaat stem verloren* *Dreiging: de continuïteit van de sessie wordt doorbroken en hacker voegt andere pagina in* *Dreiging: Trojan op PC van kiezer manipuleert stem, zorgt dat stem niet naar verkiezingssite gaat of stuurt steminfo ook naar andere locatie waardoor anonimiteit verloren gaat*	5. Klant bevestigt transacties met behulp van chippas en apparaat *Dreiging: door storing gaan transacties verloren.* *Dreiging: de continuïteit van de sessie wordt doorbroken en hacker voegt andere pagina in* *Dreiging: Trojan op PC van klant manipuleert transacties, zorgt dat transacties niet naar bank gaan of stuurt transactie info ook naar andere locatie waardoor anonimiteit verloren gaat*
6. Kiezer ontvangt bevestiging van stemmen	6. Kiezer ontvangt bevestiging van stemmen	6. Klant ontvangt bevestiging van bank dat transacties ontvangen zijn
7. Kiezer verbreekt verbinding	7. Kiezer logt uit	7. Klant logt uit

	Bij elke verkiezingsmethodiek bestaat de kans dat stemmen enige tijd onmogelijk is. Bij postale verkiezingen kan bijvoorbeeld gestaakt worden door de post. De kans dat moedwillig storingen gecreëerd kunnen worden is bijzonder klein. De kans dat toevallig storingen optreden is ook klein.
Impact:	Afhankelijk van de duur.
Mogelijke maatregel(en):	Kwalitatief goede centrale apparatuur, zodat deze weinig kans geeft op storingen. Back-up van centrale apparatuur, zodat bij storing back-up apparatuur ingezet kan worden.
Noodscenario:	Verleng verkiezingsperiode, zodat kiezers alsnog hun stem uit kunnen brengen. Biedt alternatieve stemmethode aan, zoals stemmen in stemlokaal. Dit zorgt ervoor dat kiezers kunnen stemmen bij stroomuitval, storing van centrale apparatuur, maar ook bij problemen met hun eigen apparatuur.
Optreden vaststellen:	Monitoren van verkiezingshard- en software tijdens verkiezingen.

Dreiging:	Andere website doet zich voor als verkiezingswebsite (DNS hacking of spoofing).
Kans:	Klein, indien maatregel genomen wordt.
Impact:	Groot
Mogelijke maatregel(en):	Server authentisatie via SSL. De kiezer (of tenminste een aantal kiezers) moet dan wel op de hoogte zijn van de controle die uitgevoerd moeten worden op het SSL server certificaat.
Noodscenario:	Geen
Optreden vaststellen:	Via controle (door aantal kiezers) van SSL server certificaat.

Het 'Report of the National Workshop on Internet Voting' zegt hierover het volgende:
"While technologies such as Secure Socket Layer (SSL) and digital certificates are capable of distinguishing legitimate servers from malicious ones, it is infeasible to assume that all voters will have these protections functioning properly on their home or work computers, and in any event, they cannot fully defend against all such attacks."
Kortom: hoewel de technologie om een betrouwbare verbinding op te zetten voorhanden is kan er niet vanuit worden gegaan dat de kiezer deze technologie in de thuissituatie op een correcte wijze werkend heeft.

Dreiging:	(Distributed) Denial of Service ((D)DOS) attack. Bij een DOS attack genereert één gebruiker of een beperkte groep gebruikers zoveel netwerkverkeer naar een server, dat deze niet meer te bereiken is voor normaal gebruik. Bij een DDOS zijn een heleboel gebruikers PC's geïnfecteerd met een programma dat vanaf een bepaald moment netwerkverkeer gaat genereren naar een bepaalde server. Door de enorme hoeveelheid netwerkverkeer is de server dan niet meer toegankelijk voor normaal gebruik.
Kans:	Middelmatig
Impact:	Middelmatig
Mogelijke maatregel(en):	Gebruik maken van breedbandige aansluiting voor de server, zodat veel netwerkverkeer nodig is om de toegang te blokkeren. Gebruik maken van verschillende server PC's, zodat een (D)DOS attack op één van de servers niet het stemmen op alle servers onmogelijk maakt. Dit werkt echter alleen als kiezers direct contact moeten zoeken met een bepaalde server en naar een alternatieve server uit kunnen wijken als de oorspronkelijke server niet bereikbaar is. Het werkt niet als alle kiezers via één gemeenschappelijke site gaan.

Kans:	Klein. Gelijk voor postale, telefonische en Internet verkiezingen.
Impact:	Klein, aangezien dit niet in grote getale voor zal komen.
Mogelijke maatregel(en):	Geen
Noodscenario:	Geen
Optreden vaststellen:	Via aangifte bij het OM.

3.2.5 Kiezer bevestigt keuze

Dreiging:	Door storing of stroomuitval gaat stem verloren.
Kans:	Klein. Gelijk voor telefonisch en Internet stemmen. Bij elke verkiezingsmethodiek bestaat de kans dat stemmen verloren gaan. Bij postale verkiezingen kunnen bijvoorbeeld stembiljetten kwijt raken in de post. De kans dat moedwillig storingen gecreëerd kunnen worden is bijzonder klein. De kans dat toevallig storingen optreden is ook klein.
Impact:	Afhankelijk van hoeveelheid stemmen die verloren gaat.
Mogelijke maatregel(en):	Goede instantane back-up van uitgebrachte stemmen, bijvoorbeeld door stemmen direct op 2 verschillende systemen op te slaan. Opslag van stemmen op permanent medium. Kwalitatief goede verkiezingsapparatuur.
Noodscenario:	Alternatieve stemmethode aanbieden, zoals stemmen in stemlokaal en bekend maken dat er stemmen verloren gegaan zijn. Dit geeft kiezers de mogelijkheid ook via de alternatieve methode nogmaals hun stem uit te brengen.
Optreden vaststellen:	Monitoren van verkiezingshard- en software tijdens verkiezingen.

Dreiging:	De continuïteit van de sessie wordt doorbroken en hacker voegt andere pagina in. Hierdoor krijgt de kiezer plotseling een andere kandidatenlijst voor zich (met bijv. minder mogelijkheden) of een pagina waarop aangegeven staat dat op iemand anders gestemd wordt. De kiezer kan dit over het hoofd zien en toch zijn stem bevestigen.
Kans:	Klein, indien de juist maatregel genomen wordt.
Impact:	Klein. Het is lastig dit op grote schaal te doen.
Mogelijke maatregel(en):	Gebruik van cookies en SSL.
Noodscenario:	Geen
Optreden vaststellen:	Kiezer de mogelijkheid geven achteraf zijn stem en het meetellen daarvan te controleren.

Dreiging:	Trojan op PC van kiezer manipuleert stem, zorgt dat stem niet naar verkiezingssite gaat of stuurt steminfo ook naar andere locatie waardoor anonimiteit verloren gaat.
Kans:	Klein. Het is lastig op korte termijn een Trojan te maken.
Impact:	Middelmatig. Het is lastig op korte termijn een Trojan uitgebreid te verspreiden.
Mogelijke maatregel(en):	Uitdelen van CD of floppy waarmee PC opgestart wordt met eigen operating system en verkiezingssoftware. (Dit is waarschijnlijk te duur en erg complex gezien de grote variëteit aan hardware.) Geen gebruik maken van standaard verkiezingssoftware waarvoor mogelijk al Trojans bestaan. Korte verkiezingstermijn waardoor het op tijd maken en verspreiden van een Trojan voor de verkiezingssoftware lastig is. Indien gebruik gemaakt wordt van open source software werkt dit niet. On-line virusscanner installeren net voordat kiezer wil gaan stemmen. Nadeel is echter dat dit erg langzaam gaat en dat het moeilijk is de virusscanner actueel te hebben. Virus scanner op disk/CD uitdelen. Grote nadelen hiervan zijn, dat de

Noodscenario:	Geen
Optreden vaststellen:	Audit door onafhankelijke waarnemers.
Dreiging:	Onbetrouwbare communicatie tussen verwerkingssite en officials.
Kans:	Klein, indien juiste maatregel genomen wordt.
Impact:	Groot
Mogelijke maatregel(en):	Betrouwbare communicatie opzetten tussen verwerkingssite en officials, bijvoorbeeld door gebruik te maken van beveiligde e-mail, waarbij authentisatie plaatsvindt door middel van een public-private key mechanisme met een private key die opgeslagen is op een token of smartcard en waarbij de toegang tot de private key eventueel beveiligd is met behulp van biometrie.
Noodscenario:	Uitslag op andere manier versturen tussen verwerkingssite en officials.
Optreden vaststellen:	Schriftelijke of telefonische controle van ontvangen resultaten.
Dreiging:	Uitkomst wordt gemanipuleerd door systeemadministrator.
Kans:	Klein. Afhankelijk van integriteit systeemadministrator.
Impact:	Groot
Mogelijke maatregel(en):	Toegang tot systeem alleen mogelijk door meerdere systeemadministratoren tegelijkertijd. Uitvoeren van audit op systeem voor en achteraf. Alle handelingen op systeem vastleggen (loggen). Monitoren van systeemadministratoren tijdens opzetten en bedienen van systeem.
Noodscenario:	Geen (verkiezingen ongeldig verklaren).
Optreden vaststellen:	Bestuderen van door systeem gegenereerde rapporten.
Dreiging:	Uitkomst wordt gemanipuleerd door systeemprogrammeur of systeem-programmeur zorgt ervoor dat te achterhalen is op wie kiezer gestemd heeft.
Kans:	Klein. Afhankelijk van integriteit programmeur en professionaliteit software.
Impact:	Groot
Mogelijke maatregel(en):	Documentatie van ontwerp, implementatie, operationele procedures en testen. Goede controle op software (white code review/testen met registratie van testen die uitgevoerd zijn en gevonden resultaten) door gespecialiseerde partij. Daarna tekenen van software zodat deze niet meer gewijzigd kan worden. Gebruik maken van open source software. Gebruik van professionele software waarbij de programmeur geen belang heeft bij de einduitslag.
Noodscenario:	Geen
Optreden vaststellen:	--
Dreiging:	Inbraak op centrale verkiezingssysteem manipuleert einduitslag.
Kans:	Klein (indien de juiste maatregelen genomen worden).
Impact:	Groot. Afhankelijk van kennis van inbrekers.
Mogelijke maatregel(en):	Installeren van goede firewall en anti-virus software. Aangezien dit gedaan kan worden door professionele beveiligingsdeskundigen kan de kans op deze dreiging erg klein gemaakt worden.
Noodscenario:	Geen
Optreden vaststellen:	Intrusion Detection Systeem gebruiken.

- bij bankieren bestaat een langdurige relatie tussen de klant en de dienstverlener, stemmen is eenmalig. Daardoor kunnen bij bankieren hogere investeringskosten gemaakt worden, waardoor bijvoorbeeld de authentisatie van de klant veel beter geregeld kan worden
- de resultaten van Internet bankieren zijn achteraf te controleren. Er is terugkoppeling waardoor manipulatie achteraf zichtbaar wordt. Dit kan dan gecorrigeerd worden. Zelfs als bij Internet stemmen achteraf de mogelijkheid bestaat om fraude te detecteren, dan is correctie heel moeilijk. De enige mogelijkheid is het ongeldig verklaren van de verkiezingen en het uitschrijven van nieuwe verkiezingen.

3.3 Conclusie veiligheid Internet stemmen

Veel risico's zijn bij Internet stemmen niet groter dan bij telefonisch stemmen of stemmen per post. Wel bestaat bij Internet stemmen een aantal extra dreigingen die zich niet voordoen bij stemmen per post of telefoon. Sommige van deze dreigingen zijn goed af te dekken door het implementeren van de juiste maatregelen. Tegen een aantal dreigingen is echter weinig te doen. Een Distributed Denial of Service attack (DDOS) is hiervan een voorbeeld. Mocht een dergelijke aanval optreden dan kan wel gekozen worden voor een noodscenario, namelijk het verlengen van de verkiezingstermijn of het aanbieden van een alternatieve stemmethode. Een andere dreiging waartegen geen maatregel genomen kan worden binnen de randvoorwaarden die gesteld zijn is de installatie van een Trojan op de PC van een kiezer die de stemmen manipuleert. De kans hierop is klein. Maar het is lastig om vast te stellen of deze dreiging werkelijk opgetreden is. Door een controle in te bouwen, waarin de kiezer zijn stem controleert, kan wel achteraf worden vastgesteld of het stemproces juist is verlopen. De verkiezingssoftware die momenteel in omloop is (en gebruik maakt van gebruikersnaam en wachtwoord) geeft hier echter nog geen mogelijkheden voor.

4 GEBRUIKERSASPECTEN

4.1 Stemmen per telefoon

Het uitbrengen van een stem per telefoon heeft een aantal belangrijke voordelen ten opzichte van andere stemmethoden. In de eerste plaats is het voor (bijna) iedereen toegankelijk[3]. Tegenwoordig heeft iedereen toegang tot een telefoon, hetzij thuis, hetzij op het werk of via een openbare telefooncel. Ook het gebruik van mobiele telefoon is de laatste jaren sterk toegenomen. Er zijn al verschillende gebruikers die geen zgn. 'vaste' telefoonaansluiting meer hebben en uitsluitend gebruik maken van een mobiel netwerk. Aangezien net als bij de vorige verkiezingen van het Hoogheemraadschap Rijnland het ook mogelijk is via een mobiele telefoon een stem uit te brengen worden de opties waaruit stemgerechtigden bij het stemmen kunnen kiezen alleen maar groter. Een ander voordeel van het stemmen per telefoon ten opzichte van de traditionele manier van stemmen door naar de stembus te gaan of te stemmen per post, is dat kiezers hun huis niet hoeven te verlaten. Met name voor personen die minder mobiel zijn, zoals gehandicapten en ouderen, biedt dit voordelen. Een laatste voordeel van

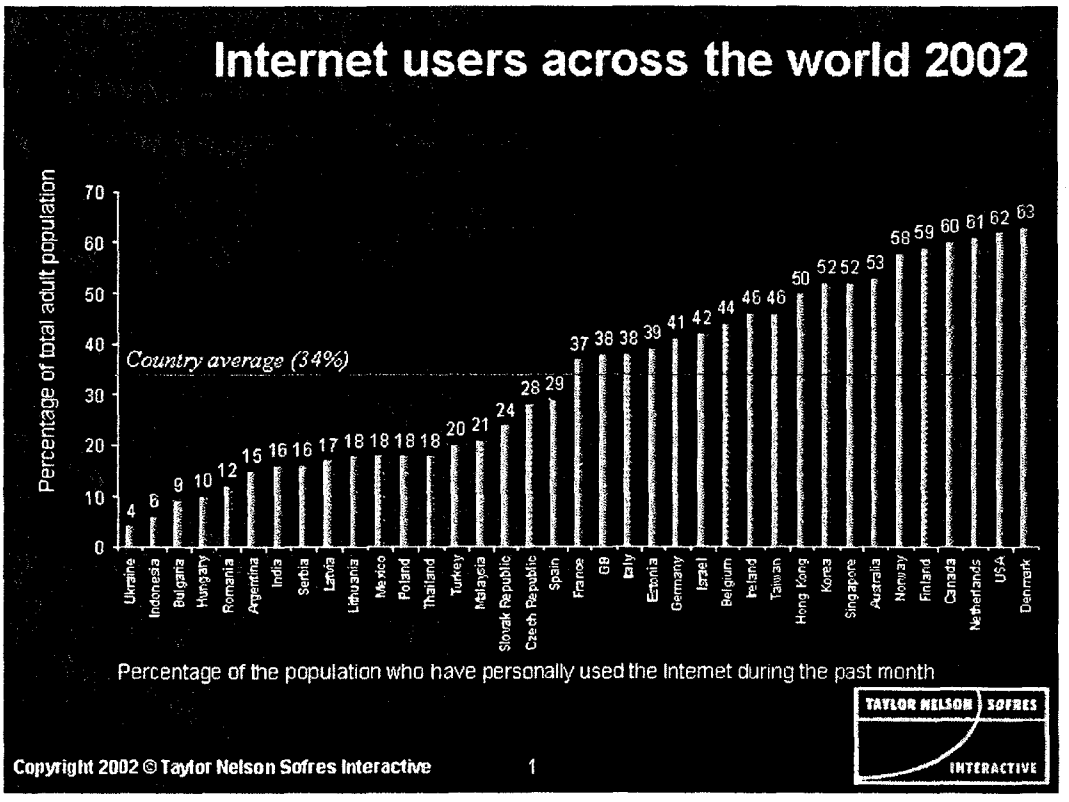


Fig. 1 Percentage van de populatie dat de afgelopen maand gebruik gemaakt heeft van Internet (bron: Taylor Nelson Sofres Interactive).

Stemmen via Internet wordt door gebruikers gezien als een gemakkelijke en prettige manier van stemmen. Het is voor een kiezer mogelijk zelf te beslissen wanneer en waar de stem wordt uitgebracht. Naast vanuit de thuissituatie of de werksituatie, kunnen kiezers in openbare instellingen of zgn. Internetcafés hun keuze kenbaar maken. Een ander belangrijk voordeel van Internet, naast het laagdrempelige karakter van Internet is het feit dat de informatie visueel wordt gepresenteerd aan de kiezer. In tegenstelling tot stemmen via de telefoon is het mogelijk een overzicht te geven van mogelijkheden en instructies. Ook is het voor kiezers minder noodzakelijk om mobiel te zijn in vergelijking met bijvoorbeeld het naar de stembus gaan.

Samengevat is er een aantal, in het verleden moeilijk tot stemmen te bewegen, groepen die met name voordeel hebben bij het stemmen via Internet: de jongeren, 55-plussers en gehandicapten (Internet Policy Institute, 2001).

Er zijn ook nadelen verbonden aan het stemmen via Internet als gekeken wordt naar de gebruikersaspecten. Alhoewel Figuur 1 laat zien dat een groot percentage van de Nederlandse bevolking toegang heeft tot Internet en ook gebruik maakt van deze toegang, betekent dit niet dat iedereen de mogelijkheid heeft om elektronisch een stem uit te brengen. Om alle stemgerechtigden in staat te stellen hun stem uit te brengen, blijven alternatieven naast het stemmen via Internet noodzakelijk. Een tweede nadeel van het stemmen via Internet is dat er bij gebruikers, i.e. stemgerechtigden, een wantrouwen bestaat jegens het verstrekken van gegevens via Internet. In het bijzonder bij gevoelige informatie, zoals een stem, zijn veel mensen zich bewust van de risico's dat hun handelingen zichtbaar gemaakt kunnen worden door derden. Met name in het ontwerp van de applicatie en in de communicatie naar de stemgerechtigden dient

Tabel 1 Overzicht van maatschappelijke segmenten en hun attitude over ICT (Ballon 2001).

	Structurele factoren	Psycho-grafische factoren	Tijdruimte aspecten	Eisen aan diensten
Alleenstaande yup	Jong, geld	Gericht op nieuwe ontwikkelingen	Tijd is schaars	Tijdbesparend, productief
Drukke taak-combineerders	Middelbaar, geld, jonge kinderen	Telefoon/Internet	Tijd is schaars	Functionaliteit, communicatie
Actieve senioren	Geld	Geld voor kwaliteit	Relatief veel tijd	Eenvoudig degelijk
Laaggeschoolde traditionele huishouden	Kinderen, lager inkomen	Traditionele elektronica	Relatief veel tijd	Multimediale passiviteit

De belangrijkste factoren die bepalend zullen zijn voor het gebruik van Internet door deze groepen zijn de psycho-grafische factoren, tijd en eisen. Bij de psycho-grafische factoren is duidelijk te zien dat de alleenstaande yup open staat voor nieuwe apparaten en technologische ontwikkelingen. De mogelijkheid om via Internet een stem uit te brengen zal deze groep zeker aanspreken, vooral als het tijd kan besparen ten opzichte van alternatieve manieren van stemmen (per post of per telefoon). Ook de drukke taakcombineerders zullen naar verwachting geneigd zijn gebruik te maken van de mogelijkheden van Internet. Functionaliteit en communicatie spelen daarbij een grote rol. Voor een dergelijke groep is het uitermate belangrijk voldoende terugkoppeling te geven tijdens en na het stemmen. Voor de actieve senioren is het van groot belang de applicatie, zowel per telefoon als Internet zo eenvoudig en functioneel mogelijk te maken. Deze groep heeft relatief veel tijd, maar haakt ook snel af als iets niet helemaal duidelijk is. Het laaggeschoolde huishouden tot slot zal hoogstwaarschijnlijk meer gebruik maken van de mogelijkheid om te stemmen via de telefoon, aangezien deze groep mensen waarde hecht aan traditionele elektronica (waar de telefoon onder gerekend mag worden).

Bij deze tabel is een aantal opmerkingen te plaatsen. In de eerste plaats is geprobeerd algemene veronderstellingen te doen op basis van eerder onderzoek. Daarbij is het alleen mogelijk algemene trends aan te geven en worden uitzonderingen niet meegenomen. In de tweede plaats zijn niet alle groepen die in een samenleving onderscheiden kunnen worden in deze tabel vertegenwoordigd. Met name de jongeren en de meer 'passieve' senioren ontbreken in dit overzicht. Van jongeren is bekend dat zij met name gebruik maken van Internet. Over het algemeen hebben jongeren zelf weinig geld tot hun beschikking maar kunnen gebruik maken van de faciliteiten van hun ouders of onderwijsinstellingen. Passieve senioren zullen wellicht minder gebruik maken van zowel Internet als de telefoon. Echter eerder is al de mogelijkheid geopperd om op een centraal punt binnen het district een stembus in te richten waar desgewenst een stem kan worden uitgebracht. Van deze groep is het meest waarschijnlijk dat zij hiervan gebruik zullen maken.

4.4 Conclusie gebruikersaspecten Internet en telefoon

Het haalbaarheidsonderzoek laat zien dat het aannemelijk is dat de combinatie van stemmen via de telefoon en stemmen via Internet de populatie van stemgerechtigden voldoende in staat stelt een stem uit te brengen. Daarbij moet wel opgemerkt worden dat er wellicht een kleine groep zgn. 'passieve senioren' van deze beide elektronische stemmethoden weinig gebruik zal maken.

5.2 Compromis

Verstandiger lijkt dan ook om te kijken naar een betrouwbare en persoonlijke technologie, die al in handen is of komt van de kiezer om andere redenen dan de verkiezing zelf. Een voorbeeld daarvan is de eNIK, de elektronische Nationale Identiteits Kaart, die sinds enige tijd door het ministerie van BZK en de PKI (Public Key Infrastructure) taskforce van ICTU wordt bestudeerd. eNIK is een op moderne beveiligtechnologie gebaseerde chipkaart, die op betrouwbare wijze aan alle burgers zou worden verstrekt om veilige communicatie met allerlei overheidsdiensten via een netwerk als het Internet mogelijk te maken. Op het eerste gezicht lijkt het, dat aan de technologische voorwaarden voor de verstrekking van een eNIK vandaag de dag al is voldaan. Bij nadere studie blijken we echter nog jaren af te staan van de praktische mogelijkheden om gewone burgers niet alleen een moderne overheidschipkaart te verstrekken, maar ook te kunnen zorgen, dat ze die daadwerkelijk op hun eigen Internet werkstation (zoals de PC) kunnen gebruiken. Daarnaast blijkt een erg grote discrepantie te bestaan tussen de eisen, die vanuit Europese en nationale regelgeving aan een dergelijke (PKI) technologie worden gesteld en de (diversiteit van) de implementatie ervan in verschillende producten. En tenslotte is er een grote (technische) afstand tussen de economisch op grote schaal inzetbare chipkaarten van vandaag en morgen en de eisen, die "theoretisch juiste" verkiezingssystemen daaraan stellen.

In de praktijk betekent dat voor vandaag en in de komende jaren, dat alleen voor een compromis kan worden gekozen. Daarbij zal men moeten kiezen voor een systeem, waarbij niet alle aspecten van de beveiliging en integriteit van de verkiezingen door de eigenschappen van het systeem zelf kunnen worden gegarandeerd. Men zal dan op andere wijze in dat soort tekortkomingen dienen te voorzien, in de praktijk vaak door het uitvoeren van specifieke organisatorische maatregelen buiten het systeem zelf. Dat is trouwens bij klassieke stembriefje/ stembus/stembureau verkiezingen ook het geval. Men denkt bijvoorbeeld maar eens aan het feit, dat aan een ingevuld stembriefje zelf niet te zien is of het authentiek is (dat wil zeggen: is ingevuld door een rechtsgeldige kiezer als enige stem). De constructie van de stembus, de controle en verzegeling ervan, het toezicht door het heterogeen samengestelde bestuur van een stembureau en speciale door hen uit te voeren procedures dienen dat te compenseren.

5.3 Praktijkvoorbeelden

Bij zo'n compromis kan men kiezen voor verschillende hoofdlijnen. Zo kan men bijvoorbeeld kiezen een chipkaart te gebruiken voor een verkiezing, die om andere redenen al — op betrouwbare wijze — in het bezit van de kiezer is en door deze regelmatig (samen met de bijbehorende PIN) voor andere doeleinden wordt gebruikt. Voorbeelden daarvan zijn: de huidige Chipknip bankkaarten, de SIM kaart, die in iedere GSM telefoon aanwezig is en de in de periode 1994–2001 aan 200.000 studenten uit het hoger onderwijs verstrekte Studenten ChipKaart (SCK). Al deze chipkaarten kennen een vergelijkbare beveiligtechnologie, alle zijn ongeschikt voor de toepassing in een "theoretisch zuiver" verkiezingssysteem, maar toch is een systeem ontwikkeld, waarmee met dit soort kaarten een betrouwbare LOES aanpak is te realiseren. Dit systeem is aanvankelijk bedacht door het ISCIT team van IBM en later onder de naam CHOOSE door het TNO-wISCIT team in de praktijk gerealiseerd en met succes toegepast

6 CONCLUSIES EN AANBEVELINGEN

6.1 Algemene conclusies

In termen van beveiliging levert het stemmen via Internet een aantal risico's op die niet af te dekken zijn. Het is technisch wel mogelijk om achteraf te controleren of er onterechte stemmen zijn uitgebracht, maar dit lijkt niet aan te sluiten bij de huidige procedures waarbij de individuele stem niet gerelateerd mag zijn aan de identiteit van de kiezer.

Vanuit het gebruikersperspectief zal naar verwachting de combinatie van stemmen via telefoon en Internet, plus een centrale mogelijkheid per district om een stembus te bezoeken, stemgerechtigden voldoende in staat stellen hun stem uit te brengen. Grote vraag daarbij blijft natuurlijk wat de bereidheid is van kiezers om te gaan stemmen. Het communiceren van het doel en belang van de verkiezingen speelt daarbij een cruciale rol. Daarbij moet opgemerkt worden dat elke populatie een dynamisch geheel is, d.w.z. voortdurend in beweging, en voor de komende verkiezingen opnieuw gekeken moet worden hoe de verschillende doelgroepen optimaal kunnen worden bereikt.

6.2 Aanbevelingen

In de door TNO uitgevoerde opdracht is gekeken naar de gebruikers- en beveiligingsaspecten van Internetstemmen. Om een afgewogen keuze te kunnen maken over het al dan niet uitvoeren van een proefproject met betrekking tot Internetstemmen bevelen we aan om ook de volgende aspecten in de overweging mee te nemen:

- Verwachte kosten versus besparingen
  Naar verwachting voldoen de huidige software stemsystemen niet aan de gewenste functionaliteiten. Er zal dan ook geïnvesteerd moeten worden in de technologie (aanpassing of ontwikkeling.
- Frequentie verkiezingen t.o.v. marktontwikkelingen
  In combinatie met het vorige punt is het de vraag of een dergelijke investering rendeert bij de relatief lage frequentie van de verkiezingen. Naar verwachting zal de markt van stemsoftware in 2008 (bij de volgende verkiezingen) verder zijn uitgekristalliseerd.
- Beveiliging software
  Ten aanzien van de beveiliging zal ook geïnvesteerd moeten worden (wellicht zelfs gecertificeerd). Daarbij speelt ook een rol dat het achteraf controleren of er onterechte stemmen zijn uitgebracht in de huidige software die op de markt is nog niet is voorzien.
- Geen leverancier met goed pakket
  Op dit moment voldoet geen van de software pakketten die op de markt zijn aan de eisen die zowel op het gebied van beveiliging als op het gebied van gebruiksvriendelijkheid gesteld zijn. Echter, deze pakketten zouden mogelijk als basis kunnen dienen van waaruit verder wordt ontwikkeld.
- Populatie niet op zelfde manier bereiken als 4 jaar geleden
  Op de eerste plaats is de gebruikerspopulatie niet dezelfde als bij de vorige verkiezingen. Daarnaast vereisen de gekozen stemalternatieven (telefoon en Internet) een andere benade-

REFERENTIES

Ballon, P.J.P. (2001). *ICT en de toekomstige thuisomgeving* (TNO rapport STB-01-30b). Delft: TNO Strategie, Technologie en Beleid.

Centrum voor Marketing analyses (1999). *De Waterschapsverkiezingen 1999; bevindingen van de effectmeting (management summary),* augustus 1999. In opdracht van Waterschap Groot Haarlemmermeer, Hoogheemraadschap van Rijnland, Waterschap De Oude Rijnstromen en Waterschap Wilck en Wiericke.

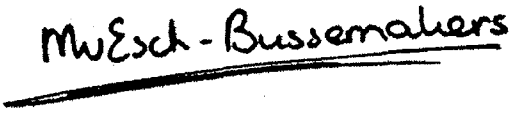
Frissen, V. (2000). X. Paper in opdracht van de Consumentenbond.

Internet Policy Institute (2001). *Report of the National Workshop on Internet Voting; Issues and Research Agenda,* March 2001. Sponsored by the National Science Foundation. Conducted in cooperation with the University of Maryland and hosted by the Freedom Forum.

Lausberg, J. (2001). *Kies digitaal voor droge voeten; onderzoek naar de ontwikkeling van een elektronisch verkiezingssysteem voor het Hoogheemraadschap van Rijnland* (afstudeerscriptie).

Taylor Nelson Sofres Interactive (2002). www.tnsofres.com

Soesterberg, 19 december 2002



Dr. M.P. van Esch-Bussemakers
(1e auteur, projectleider)

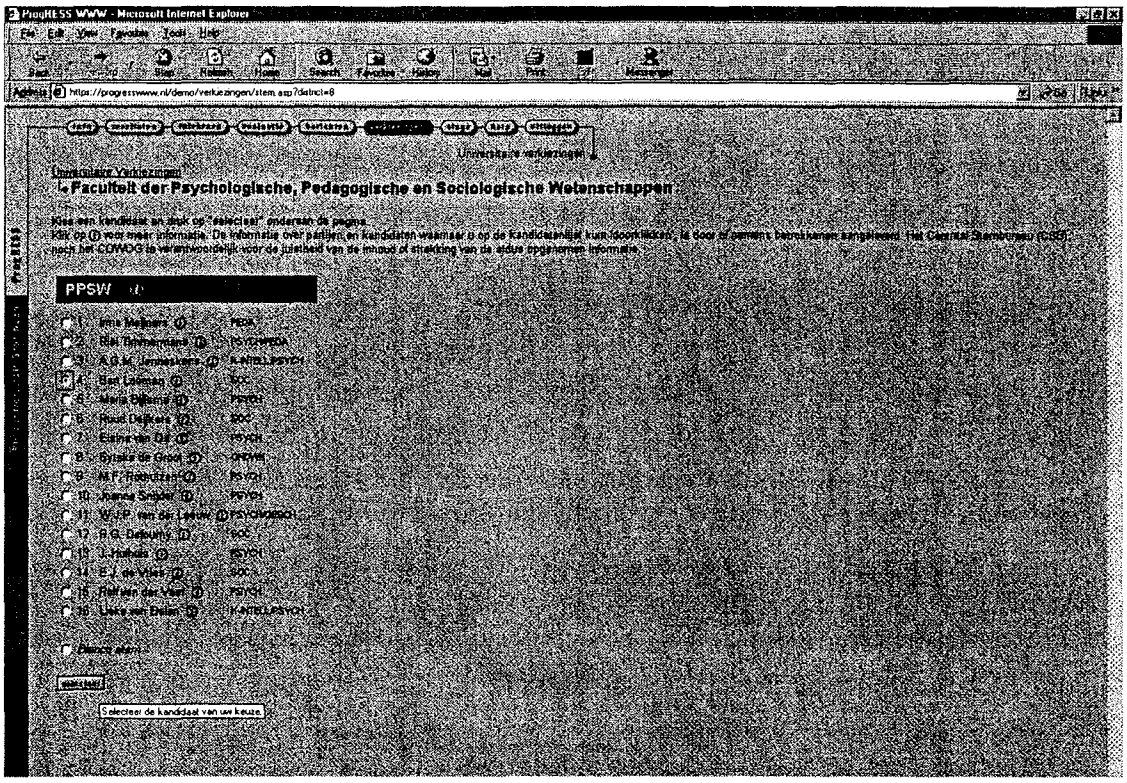


Fig. A.4 De kiezer maakt zijn keuze voor een bepaalde kandidaat door een hokje aan te vinken en op Selecteer te drukken. Eventueel kan informatie over deze kandidaat opgevraagd worden.

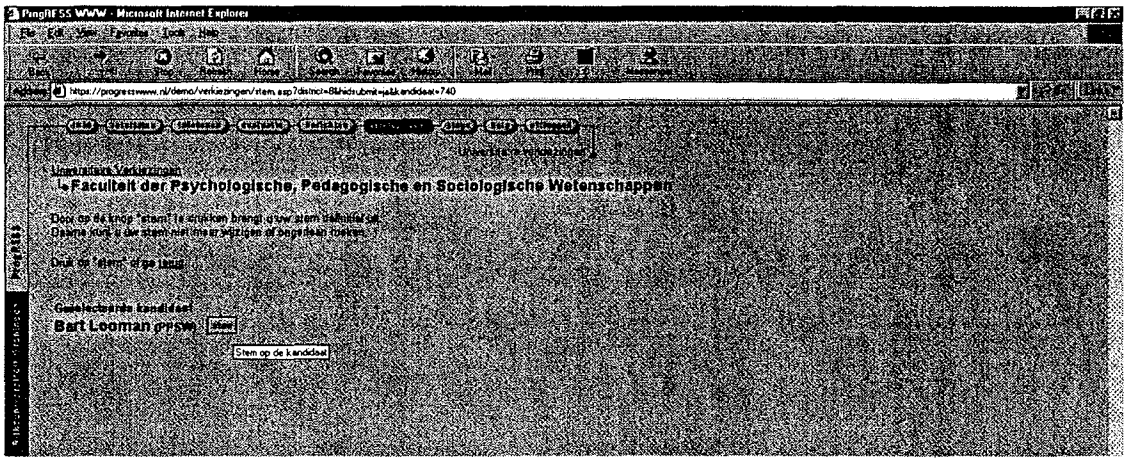


Fig. A.5 De kiezer krijgt een overzicht van zijn keuze en bevestigt deze door op Stem te drukken. Eventueel kan de stem nog aangepast worden.

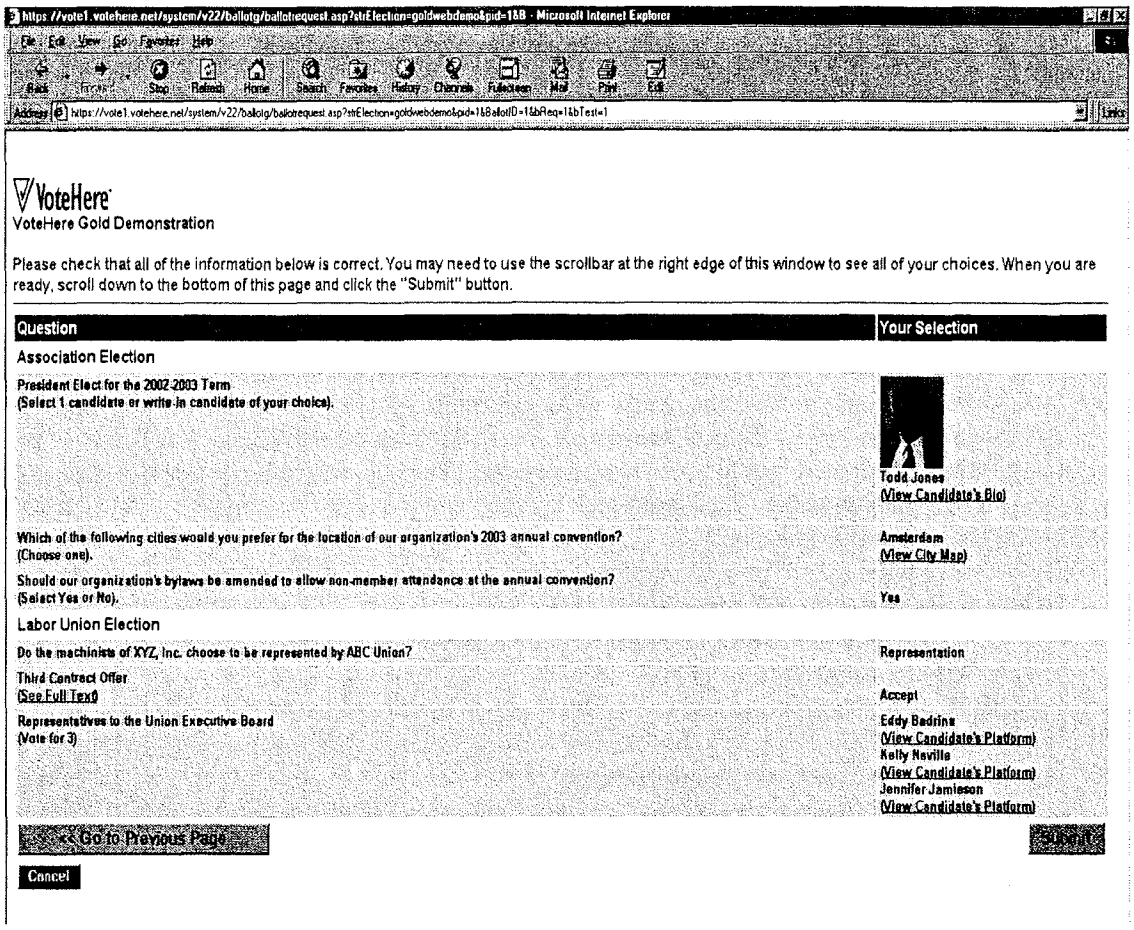


Fig. A.9 De kiezer krijgt een overzicht van zijn keuzes en bevestigt deze door op Submit te drukken. Eventueel kunnen de keuzes nog aangepast worden.

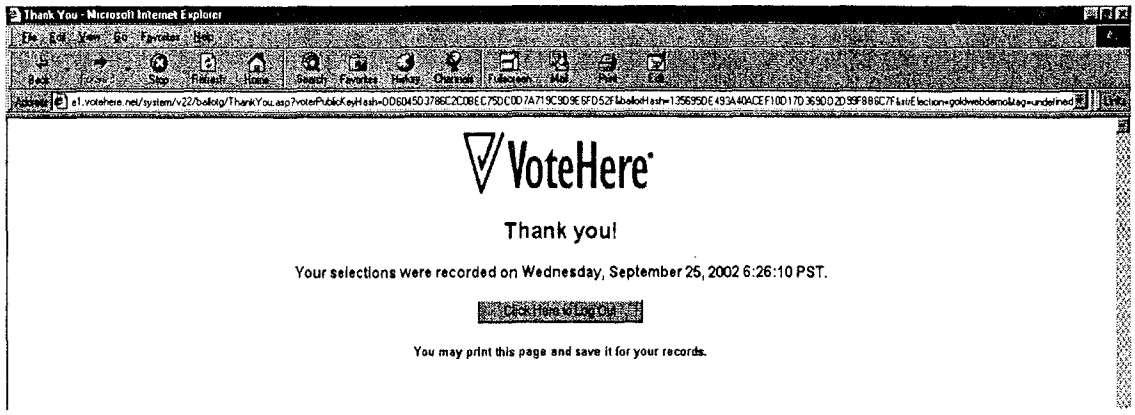


Fig. A.10 De stemsoftware bevestigt dat de stem van de kiezer ontvangen is. Daarna kan de kiezer uitloggen.

- De uitgebrachte stemmen worden opgeslagen in een database. In een tabel worden de uitgebrachte stemmen bijgehouden, in een andere tabel wordt bijgehouden wie een stem heeft uitgebracht. Achteraf valt niet meer te reconstrueren wie welke stem uitgebracht heeft.
- Als back-up maakt het systeem gebruik van meerdere servers, zodat het blijft werken als één webserver uitvalt. De database server is vrijwel geheel redundant uitgevoerd, d.w.z. bij de uitval van een harddisk, voeding, processor, enz. blijft de server werken. Verder wordt elk half uur een back-up gemaakt. Alle servers zijn gekoppeld aan een dubbele UPS.
- Beoordeling van de source code door een onafhankelijke derde partij is onder voorwaarden bespreekbaar.
- Toegang tot het systeem is zodanig aan te passen, dat dit alleen mogelijk is door meerdere personen tegelijkertijd. Momenteel is dit nog niet zo.
- Het aantal te verwachte stemmen lijkt geen probleem voor de ProgRESS WWW stemmodule. Aangezien de server is aangesloten op de backbone van de RUG die weer aan SURFNET gekoppeld is, is de verbinding breedbandig genoeg. De modulaire opbouw van het systeem, zorgt dat de capaciteit gemakkelijk uit te breiden is.
- Het systeem houdt logfiles bij.
- Het is met ProgRESS WWW niet mogelijk om op meer kandidaten dan het toegestane aantal te stemmen. Blanco stemmen is mogelijk
- Het is met ProgRESS WWW niet mogelijk een 2e keer te stemmen. Het systeem houdt bij of iemand al gestemd heeft.
- ProgRESS WWW maakt gebruik van cookies om de sessie continuïteit te garanderen.

Een demo van ProgRESS WWW is te bekijken op: Progresswww.nl/demo.
Login 1 en 2 kunnen stemmen. Password: demo:
Via de administrator login, gebruikersnaam: demo, wachtwoord: demo, kan de stemmodule gereset worden.
Meer informatie over de ProgRESS WWW stemmodule is te verkrijgen bij:
Ed Welling, tel: 050 – 363 36 38 of Herman de Groot, tel: 050 – 363 36 41

VoteHere Gold

VoteHere ontwikkelt verkiezingssoftware voor elektronisch stemmen in stembureaus en kiosken (VoteHere Platinum) en voor elektronisch stemmen via Internet (VoteHere Gold).
VoteHere garandeert:

- de veiligheid van de verkiezing
- de geheimhouding van de stem
- een volledig verifieerbare verkiezing met audit trail.

VoteHere Gold is gebruikt bij een aantal pilot verkiezingen in de publieke sector, onder andere bij de Alaska State Republican Straw Poll in januari 2000 en bij de Presidential Election Online Voting Trial in Arizona en California in november 2000. VoteHere Gold is ook regelmatig gebruikt bij verkiezingen in de private sector onder meer voor vakbondsverkiezingen en op hogescholen en universiteiten. Zo is het gebruikt bij de vakbondverkiezing van Boeing en op Cornell University, Kansas State University, Boston College en Illinois State University.
VoteHere Gold heeft de volgende kenmerken:

- Kiezers hebben geen plug-in software of additionele hardware nodig. Een browser en Internetverbinding is voldoende
- Gebruikersidentificatie kan plaatsvinden via gebruikersnaam en wachtwoord.
- Voor server authenticatie en vercijfering van de gegevens wordt gebruik gemaakt van SSL (128-bit). (Een client certificaat is niet vereist.) Voor het oversturen van de stem wordt dus gebruik gemaakt van HTTPS waardoor deze niet zonder meer te lezen is. De server authenticatie voorkomt dat een andere website zich voordoet als de verkiezingssite.
- De stemmen worden vercijferd en getekend opgeslagen in het VoteHere data centrum.
- Het VoteHere data centrum is een beveiligde omgeving met gecontroleerde, gemonitoorde toegang 24 uur per dag, 7 dagen per week.
- VoteHere genereert log files van de verkiezingen.
- VoteHere Gold maakt gebruik van een multi-authority of distributed trust model voor het berekenen van de einduitslag. Dit wil zeggen dat iedere official een elektronische sleutel heeft en

Distributie rapport

1–5. Opdrachtgever, de heer S. Bouwman, Hoogheemraadschap Rijnland, Leiden

6. Archief TNO-TM in bruikleen aan P.M. van Bergem R.e., TM Communicatie Manager

7. Archief TNO-TM in bruikleen aan dr. M.P. van Esch-Bussemakers, afdeling Informatieverwerking

8. Archief TNO-TM in bruikleen aan dr. J.M.E. Geers, TNO-FEL

9. Archief TNO-TM in bruikleen aan de heer P.G. Maclaine Pont, TNO-TPD

10. Archief TNO-TM in bruikleen aan drs. H.J. Vink, TNO-FEL

11. Archief TNO-TM in bruikleen aan drs. M. Holewijn, hoofd afdeling Informatieverwerking

12–16. Reserve

Gecodeerd stemmen via Internet

Een groep Engelse wetenschappers heeft een systeem bedacht voor het veilig uitbrengen van een internetstem zonder dat daar software of pinpassen voor de kiezer aan te pas komen. Het systeem gaat er van uit dat er geen CD-ROM's of passen worden verstrekt. Vanwege de kosten en het beheer is dat ondoenlijk bij een (waterschaps)verkiezing.

Bijgevoegd is een bijlage van het rapport dat zij hebben opgesteld naar aanleiding van de Engelse experimenten met het elektronisch stemmen in mei 2002.

Het werkt als volgt:

De kiezer krijgt een stemkaart met een persoonlijk identificatienummer: **123456789**

Op de kaart staat bij elke kandidaat een persoonlijk kandidatennummer:

Kandidaat	**Persoonlijk kandidatennummer**	**Verwachte respons**
Verbaan AD	2649	000999
Welleman JA	9485	111888
Weteing Halma CM vd	8282	222777
Wit Lona CM de	1240	333666
Altene STM	1838	222555
Arentshorst J	7482	444777
Bos Frans	9272	111777
Démoed	7827	999555
Blanco stem	8181	666444

Om te stemmen toets de kiezer op de stemapplicatie op het Internet zijn persoonlijk identificatienummer in en het persoonlijk kandidatennummer van de kandidaat van zijn voorkeur. De stemapplicatie bevestigt zijn keuze door het terugsturen van een nummer dat moet overeenkomen met de verwachte respons. De kiezer weet dan zeker dat zijn stem is geteld.

Het uitbrengen van de stem is op deze manier versleuteld zonder dat er software op de computer van de kiezer moet worden geïnstalleerd. Indien een stem op het internet wordt onderschept is nooit duidelijk op welke kandidaat de kiezer stemt. Ook het hacken van het stemproces heeft geen zin. Het stemproces kan ondanks dit systeem nog wel verstoord worden, maar het omzetten van een stem naar een andere kandidaat – die de hacker graag gekozen ziet - is niet meer mogelijk.

Annex C. Possible Security Mechanism

C.1 Introduction

229. In this section we outline a technical approach that may meet the security requirements of a very large-scale election that makes use of Remote Electronic Voting. This solution does not place any trust in the client systems, as it uses pre-encrypted ballots.

230. We start by describing how the election could appear to a voter. It is worth stressing at this point that a number of options will be presented, and some parameter choices are given as illustrative examples only. The approach outlined relies on the use of cryptography to provide security in the system. Alternatively, it would be possible to substitute use the pre-encrypted ballots with pre-generated unique random numbers and the system would work in a very similar manner.

231. For this proposal, it is assumed that the electoral roll would be managed in the normal way. In fact, this Remote Electronic Voting protocol can be implemented independently of any changes in the electoral roll.

232. By default, registered voters would receive credentials for electronic voting through the post. There would, however, be an option for voters who wished not to receive credentials for electronic voting and instead have a postal ballot or only be able to use a physical polling station. It is envisaged that a smaller-than-usual number of physical polling stations would be provided for the election. Voters who receive electronic credentials would still be able to vote in person.

233. The electronic voting credentials would be in two parts:

- A Voter Identification Number (Voter ID). This would be globally unique and might be 16 digits long.
- A list of candidates, corresponding Personalised Candidate Identification Numbers (PCINs) and Response IDs. The PCINs could be 4 digits long and the Response IDs slightly longer at 6 digits.

234. These pieces of information can almost be thought of as almost like a credit card number and a list of several different PIN numbers. They can also be posted separately for security, just as credit cards and PINs are at present.

235. By way of example, John Doe might receive the following:

```
John Doe
Voter ID Number: 1234567890123456
```

Candidate	Party	PCIN	Expected Response
Alice	AliceParty	3344	000999
Bob	BobParty	4455	111888
Charlie	CharlieParty	6677	222777
Dave	DaveParty	8899	333666
Intentionally Spoilt Ballot		1100	444555

236. To vote, John has to send his voter ID number and the PCIN of his chosen candidate. For example the following might be sent as the body of a text message to the election's SMS number:

hash, and the first few bits of the hash used to form the PCIN and some other data used to form a secret function used to generate the Response IDs from the PCINs.

C.3 Ballot Distribution

250. It may, in time, be possible to offer the option of distributing half of the ballot electronically and the other half by post. This would likely save money. However, the basic tenet of distributing a part of the voter's credentials in such a way that computer cannot automatically cast the vote must not be broken.

251. Consider for example what could happen if the Voter ID and PCINs were distributed by email. It would then be possible to steal credentials from people's email by hacking home computers, or even to write a virus to automate voting in a particular way. Distributing credentials on paper prevents such attacks.

C.3.1 Credential Theft

252. Voter education would be required to inform people what to do if their credentials fail to turn up in the post. This would involve contacting a central help desk that would provisionally cancel the voter's ballot, and the voter would be asked to collect a new ballot personally from perhaps their local town hall.

C.4 Vote Casting

253. The basics of the ballot-casting process were outlined in the introduction and are illustrated below:

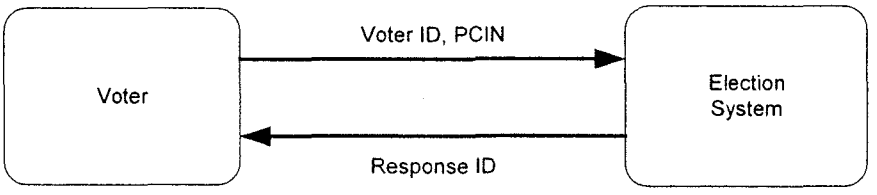


Figure 3: Basic Voting Architecture

254. Sending a vote: this requires the voter to correctly enter their Voter ID and the PCIN corresponding to their chosen candidate in order. It is assumed that some people will be unable to do this correctly first time, so procedural lockouts will be generous enough in a short timeframe.

255. The main threats to this stage are:

- identification of who is being voted for;
- modification of vote in transit;
- deletion of vote in transit.

256. The first two of these threats are met by the secrecy of the Voter ID and PCINs. It is difficult to identify who is being voted for without knowing the PCINs corresponding to a particular Voter ID. The same knowledge is required to replace a vote in transit (and if that data was known, votes could be inserted).

257. The personalised Response ID for each possible vote makes deletion of votes detectable. If a voter does not receive the correct Response ID, or any at all, she should attempt to vote again. Systems that use a generic response message are of course vulnerable to votes being deleted in transit and the generic response being spoofed.

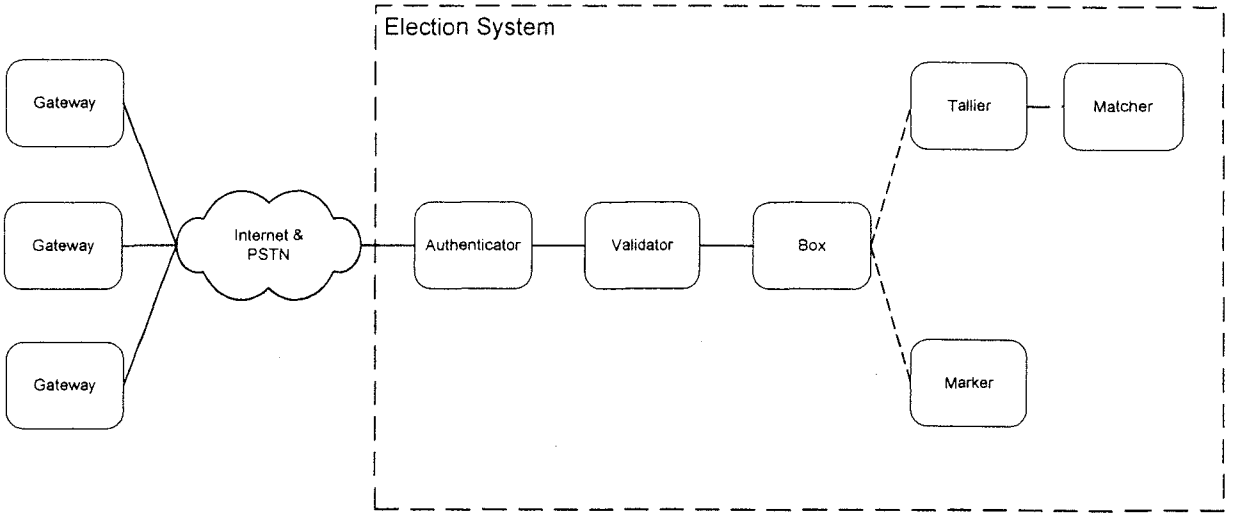


Figure 4: Detailed Voting Architecture

265. We now discuss the components in more detail. The first system that votes enter will be the Gateway.

C.5.1 Gateway

266. As Remote Electronic Voting will potentially use a number of different delivery channels, each will need its own gateway systems. In the case of Internet voting these will be web servers, and similarly there will be computers handling SMS communications, touch-tone telephone and so forth.

267. These systems will be under the control of the election authority, so they will - to a point - be trusted. Gateways will be configured to sign and then encrypt votes passing through them. Applying a digital signature also allows other elements of the system to keep track of where a vote was cast. Votes without valid signatures will not be counted in the final reckoning.

268. Gateways will keep an audit log of all votes sent to them. Note that at this stage no checking has been performed as to the validity of the vote. This function is not carried out by the gateway, so when logged, signed, and encrypted a vote will be passed on to a system known as the Authenticator.

ensure that no one system is in a position to undetectably discard votes, etc., and that no one person is in a position to control enough of the disparate system to alter the tallies of votes.

280. For example, the back-end of the counting architecture will employ comprehensive logging and appropriate cryptographic techniques to make it impossible for single systems to undetectably remove or insert votes.

C.6 Summary

281. In conclusion we have presented a system for practical remote electronic voting that supports multiple voting channels whilst placing no demands on the client systems.