

PROGRAMMA VAN EISEN HERTELPROGRAMMATUUR  
KIEZEN OP AFSTAND



# PROGRAMMA VAN EISEN HERTELPROGRAMMATUUR KIEZEN OP AFSTAND

**4 februari 2004**

**Status** Definitief

**Versie** 1.0

# Inhoudsopgave

<b>1 Inleiding.....</b>	<b>3</b>
1.1 Afbakening.....	3
1.2 Versies.....	3
<b>2 Functioneel Ontwerp.....</b>	<b>4</b>
2.1 Doel van de (her)telprogrammatuur.....	4
2.2 Te ondersteunen processtappen.....	4
<b>3 Randvoorwaarden.....</b>	<b>7</b>
<b>A Bijlage Specificaties stemmen en exportbestand.....</b>	<b>9</b>
<b>B Bijlage Specificaties Rapportages.....</b>	<b>10</b>
B.1 Definitie rapport "Resultaat van de stemming".....	10
B.2 Voorbeeld rapport "Resultaat van de stemming".....	10
B.3 Definitie rapport "Verwerkingsverslag".....	11
B.4 Voorbeeld rapport "Verwerkingsverslag".....	12

# 1 Inleiding

## 1.1 Afbakening

In opdracht van het ministerie van BZK (BZK) is door een leverancier een stembienst ontwikkeld om het stemmen per internet en telefoon mogelijk te maken. Deze stembienst voorziet er uiteraard in dat de uitgebrachte stemmen worden geteld.

BZK wil dat het tellen (en hertellen) van de uitgebrachte stemmen ook buiten deze stembienst om kan geschieden.

Voor het (her)tellen buiten de stembienst om is het nodig om een aanvullend programma te ontwikkelen. Dit document de eisen waaraan dit programma dient te voldoen.

## 1.2 Versies

<b>Versienummer</b>	<b>Toelichting</b>
1.0	Eerste versie (d.d. 4 februari 2004)

## 2 Functioneel Ontwerp

### 2.1 Doel van de (her)telprogrammatuur

De (her)telprogrammatuur (hierna: het Programma) dient om de versleutelde stemmen die in de elektronische stembus zijn opgenomen te ontsleutelen en vervolgens te tellen.

### 2.2 Te ondersteunen processtappen

Het Programma kent een hoofdmenu met daarin de volgende functies:

Wissen Gegevens
Importeren Kandidatenbestand
Importeren Export stembus
Importeren sleutel
Ontsleutelen
Tellen
Rapportage

Het Programma kent daarnaast een helpfunctie en een functie om het Programma te beëindigen.

#### 2.2.1 Stap 1: Wissen gegevens

De gebruiker selecteert uit het menu de functie Wissen gegevens.

Na bevestiging verwijdert het Programma alle gegevens over kandidaten, lijsten, sleutels, versleutelde en ontsleutelde stemmen en rapporten uit het intern geheugen en van de harde schijf. Daarnaast worden alle tellers op nul gezet. Indien de actie is geslaagd toont het Programma een melding op het scherm dat het geheugen leeg is en alle gegevens verwijderd zijn.

#### 2.2.2 Stap 2: Importeren kandidatenbestand

De gebruiker selecteert uit het menu de functie Importeren kandidatenbestand.

Middels een dialoogscherf wordt de gebruiker gevraagd de locatie van het kandidatenbestand op te geven.

Het Programma verifieert of het kandidatenbestand een geldig XML bestand is en de juiste header bevat. Zo niet dan wordt het hele bestand geweigerd onder vermelding van de reden. Er worden in dat geval geen lijsten, kandidaten, of kandidaatcodes ingelezen.

Als het een geldig XML bestand is, dan meldt het Programma op het scherm hoeveel lijsten zijn aangetroffen en hoeveel kandidaten per lijst. Het Programma vraagt een bevestiging aan de gebruiker om het bestand in te lezen. Zo ja, dan worden de gegevens over de lijsten, kandidaten en kandidaatcodes ingelezen. De gebruiker wordt gevraagd of hij een overzicht op het scherm wil krijgen van lijsten, kandidaten en kandidaatcodes.

Zo nee, dan keert de gebruiker terug naar het hoofdmenu.

### 2.2.3 Stap 3: Importeren Export stembus

De gebruiker selecteert uit het menu de functie Importeren Export stembus.

Middels een dialoogscherf wordt de gebruiker gevraagd de locatie van het exportbestand (zie § 3.1 in bijlage A) op te geven.

Het Programma verifieert of het exportbestand een geldig XML bestand is en de juiste header bevat. Zo niet dan wordt het hele bestand geweigerd onder vermelding van de reden. Er worden in dat geval geen records ingelezen.

Als het een geldig XML bestand is dan, meldt het Programma op het scherm hoeveel versleutelde records (met vermoedelijk stemmen) zijn aangetroffen.

Het Programma vraagt een bevestiging aan de gebruiker om het bestand in te lezen. Zo ja, dan worden de stemmen ingelezen. Zo nee, dan keert de gebruiker terug naar het hoofdmenu

### 2.2.4 Stap 4: Importeren sleutel

De gebruiker selecteert uit het menu de functie Importeren sleutel.

Middels een dialoogscherf wordt de gebruiker gevraagd de locatie van het bestand met daarin de privé RSA sleutel op te geven. Daarna wordt de gebruiker gevraagd de bij de sleutel behorende passphrase op te geven. Het Programma verifieert of het bestand een geldige RSA sleutel bevat. Zo niet dan wordt het sleutelbestand geweigerd onder vermelding van de reden. Zo ja, dan verifieert het Programma of de juiste passphrase is ingegeven.

Vervolgens wordt de gebruiker gevraagd om de locatie van het bestand met daarin de publieke RSA sleutel op te geven. Daarna wordt de gebruiker gevraagd de bij de sleutel behorende passphrase op te geven. Het Programma verifieert of het bestand een geldige RSA sleutel bevat. Zo niet dan wordt het sleutelbestand geweigerd onder vermelding van de reden. Zo ja, dan verifieert het Programma of de juiste passphrase is ingegeven.

Als beide sleutelbestanden succesvol ingelezen zijn verifieert het Programma of de publieke sleutel en de private sleutel bij elkaar horen. Zo niet dan worden de sleutels alsnog geweigerd onder vermelding van de reden.

### 2.2.5 Stap 5: Ontsleutelen

De gebruiker selecteert uit het menu de functie Ontsleutelen.

Het Programma zal vervolgens elke ingelezen stem ontcijferen. Zie hiervoor ook § 3.2 uit bijlage A. Tijdens het ontsleutelen wordt de voortgang (in termen van aantal nog te ontsleutelen te stemmen of middels een voortgangsbalk) getoond op het scherm.

Het Programma meldt het aantal succesvol ontsleutelde stemmen op het scherm.

### 2.2.6 Stap 6: Tellen

De gebruiker selecteert uit het menu de functie Tellen.

Het Programma zal vervolgens per lijst en daarbinnen per kandidaat het aantal op die kandidaat uitgebrachte stemmen tellen.

Tijdens het tellen wordt de voortgang (in termen van aantal nog te tellen stemmen of middels een voortgangsbalk) getoond op het scherm.

In het telrapport dient voor elke kandidaat van elke lijst vermeld te worden hoeveel stemmen deze heeft gekregen. Dus ook als een kandidaat geen stemmen heeft gekregen, dient deze vermeld te worden. Noot: in de systematiek van de stembus is een blanco stem een stem op de 'kandidaat blanco'.

Het Programma meldt het aantal succesvol getelde stemmen op het scherm.

#### 2.2.7 Stap 7: Rapportage

De gebruiker selecteert uit het menu de functie Rapportage.

De gebruiker krijgt de keuze uit twee rapporten:

- a) "Resultaat van de stemming" en
- b) "Verwerkingsverslag"

Na aanklikken van de keuze wordt de inhoud van het rapport op het scherm getoond met behulp van een PDF-viewer (Adobe Acrobat).

De exacte voorwaarden waaraan de rapporten dienen te voldoen zijn vastgelegd in bijlage B.

De rapporten kunnen worden afgedrukt middels Adobe Acrobat en de standaard Windows Print Manager (zodat elke printer gebruikt kan worden).



### 3 Randvoorwaarden

#### 3.0.1 Wettelijke regelingen

De (her)telling dient te worden uitgevoerd met inachtneming van de daarop van toepassing zijnde wet- en regelgeving (Experimentenwet Kiezen op Afstand, Kieswet en de op die beide wetten gebaseerde algemene maatregelen van bestuur en ministeriële regelingen<sup>1</sup>).

#### 3.0.2 Gebruikers

Het Programma zal gebruikt worden door leden van het stembureau en/of derden die in opdracht van het stembureau danwel het ministerie van BZK handelen. In geval van hertellen zal dit geschieden zoals dat in de Kieswet is beschreven, door het **centraal** stembureau (i.c. de Kiesraad) (art. P 21 Kieswet) of door het vertegenwoordigend orgaan (i.c. niet het Europees Parlement, maar de Tweede Kamer). Bij de opzet van het Programma moet er vanuit gegaan worden dat deze personen noch uitvoerige ICT deskundigheid hebben noch langdurige getraind zijn in het gebruik van het Programma.

Dit betekent dat functies in het hoofdmenu alleen getoond worden wanneer daaraan voorafgaande stappen afgerond zijn.

Dit betekent ook dat voor elke stap in het proces een contextsensitieve helpfunctionaliteit geboden moet worden, waarin uitgelegd wordt wat de werking en betekenis is van de door het Programma geboden functies en meldingen.

#### 3.0.3 Performance

Het Programma dient in staat te zijn om binnen 5 minuten 25.000 stemmen te verwerken. Hierbij dient uitgegaan te worden van een configuratie van minimaal Pentium 4, 2+ Mhz, 256 Mb intern geheugen.

Het Programma dient in staat te zijn om te gaan met een exportbestand met 600.000 stemmen.

#### 3.0.4 ICT-omgeving

Het Programma dient te functioneren op een computer met de volgende specificaties:

Pentium 4, 2 Mhz of beter

256 Mb geheugen

Operating systeem: Linux of Windows98SE, Windows2000, Windows2000 Professional, Windows XP

#### 3.0.5 Installatie / verwijderen programma

Het Programma dient geleverd te worden met een installatie programma. Het Programma dient ook op die wijze verwijderd te kunnen worden.

---

<sup>1</sup> Actuele wetsteksten zijn opvraagbaar via <http://wetten.overheid.nl>.

### 3.0.6 Overige voorwaarden

- Het bestand met kandidaten zal diakritische ketens bevatten. Deze tekens dienen in het rapport “Resultaat van de stemming” exact overgenomen te worden.
- De XML bestanden maken gebruik van de UTF-8 (ookwel Unicode genaamd) tekenset.
- Het Programma dient opgeleverd te worden met een gebruikershandleiding.
- Het Programma dient opgeleverd te worden met technische documentatie (technisch ontwerp én niet-gecompileerde broncode).

## A Bijlage Specificaties stemmen en exportbestand

Rapport LogicaCMG.

## B Bijlage Specificaties Rapportages

### B.1 Definitie rapport “Resultaat van de stemming”

#### Resultaat van de stemming

Kieskring: [bron: XML exportbestand, tag <KIESKRING NUMMER & NAAM>]  
 Stembureau: [bron: XML exportbestand, tag <GLOBAAL STEMBUREAU>]  
 Stemperiode: [bron: XML exportbestand, tag <GLOBAAL PERIODE\_START>]  
 Verkiezing: Verkiezing van de leden van het Europees Parlement  
 Starttijd stemming: [bron: XML exportbestand, tag <GLOBAAL PERIODE\_START>]  
 Eindtijd stemming: [bron: XML exportbestand, tag <GLOBAAL PERIODE\_EIND>]  
 Aantal kiesgerechtigden: [leeglaten, met de hand invullen]  
 Aantal stemmen: [bron: aantal getelde stemmen door Programma]

[grijze balk met daarin Lijstnummer]

**Lijstnaam:** [Naam van de Lijst]

totaal aantal stemmen op lijst: [aantal]

[tabel met de stemmen per kandidaat, gesorteerd op oplopend positienummer]

[positienummer]	[voorletters kandidaat] [Achternaam kandidaat]	[aantal stemmen]
-----------------	---	---------------------

### B.2 Voorbeeld rapport “Resultaat van de stemming”

#### Resultaat van de stemming

Kieskring: 12 - Gemeente 's-Gravenhage  
 Stembureau: Internet- en telefoonstembureau  
 Stemperiode: 1 juni 2004 - 10 juni 2004  
 Verkiezing: Verkiezing van de leden van het Europees Parlement  
 Starttijd stemming: 1 juni 2004 9:01  
 Eindtijd stemming: 10 juni 2004 21:00  
 Aantal kiesgerechtigden:  
 Aantal stemmen: 9

**Lijstnummer:** 1

**Lijstnaam:** Partij van de Vliegtuigen

totaal aantal stemmen op lijst: 7

1.	K.L. Miloot	3
2.	S. Brokken	2
3.	P. Vleugel	2
4.	L. Gestel	0

Lijstnummer: 2

**Lijstnaam: Partij van de Kleuren**

totaal aantal stemmen op lijst: 1

1.	P. Impelpáárs	1
2.	F. Elrood	0
3.	L. Blauw	0

Lijstnummer: 99

**Lijstnaam: Blanco**

totaal aantal stemmen op lijst: 1

1.	Blanco	1
----	--------	---

### B.3 Definitie rapport “Verwerkingsverslag”

#### Verwerkingsverslag

Verslag opgemaakt op: [systeemdatum, systeemtijd]

---

 Kandidatenbestand [succesvol/niet succesvol] geïmporteerd.

[reden niet succesvol importeren]

 Locatie en naam kandidatenbestand: [locatie, naam, datum/tijdstempel  
kandidatenbestand]

Referentienummer: [referentienummer kandidatenbestand]

Aantal aangetroffen lijsten (excl. blanco): [aantal excl. lijst blanco]

Aantal aangetroffen kandidaten (excl. blanco): [aantal excl. kandidaat blanco]

Aantal blanco stemmen: [aantal]

---

 Stembusbestand [succesvol/niet succesvol] geïmporteerd.

[reden niet succesvol importeren]

Naam en locatie stembusbestand: [locatie, naam, datum/tijdstempel stembusbestand]

Aantal aangetroffen kieskringen: [aantal]

Aantal aangetroffen versleutelde stemmen: [aantal]

---

 Private sleutel [succesvol/niet succesvol] geïmporteerd.

[reden niet succesvol importeren]

Naam en locatie sleutelbestand: [locatie, naam, datum/tijdstempel sleutelbestand]

Publieke sleutel [succesvol/niet succesvol] geïmporteerd.

[reden niet succesvol importeren]

Naam en locatie sleutelbestand: [locatie, naam, datum/tijdstempel sleutelbestand]

De private sleutel en publieke sleutel behoren [wel/niet] tot hetzelfde sleutelpaar.

---

Ontsleutelen gestart op [datum / tijdstempel].

[Ontsleutelen is afgebroken wegens ...]

Ontsleutelen gestopt op [datum / tijdstempel].

Er zijn [aantal] stemmen ontsleuteld.

---

Tellen gestart op [datum / tijdstempel].

[Tellen is afgebroken wegens ...]

Tellen gestopt op [datum / tijdstempel].

Er zijn [aantal] stemmen geteld.

Einde verwerkingsverslag

## B.4 Voorbeeld rapport “Verwerkingsverslag”

### Verwerkingsverslag

Verslag opgemaakt op: 10 juni 2004 21:29:02

---

Kandidatenbestand succesvol geïmporteerd.

Locatie en naam kandidatenbestand: A:\koa\kandidatenlijst-export57.xml 28 april  
2004 19:15:00

Referentienummer: 57

Aantal aangetroffen lijsten (excl. blanco): 2

Aantal aangetroffen kandidaten (excl. blanco): 8

Aantal blanco stemmen: 1

---

Stembusbestand succesvol geïmporteerd.

Naam en locatie stembusbestand: A:\koa\exportstembus.xml 10 juni 2004 21:01:34

Aantal aangetroffen kieskringen: 1

Aantal aangetroffen versleutelde stemmen: 7

---

Private sleutel succesvol geïmporteerd.

Programma van Eisen hertelprogrammatuur Kiezen op afstand

Locatie en naam sleutelbestand: A:\koa\sleutels\privatekey.prc 29 mei 2004  
13:10:00

Publieke sleutel succesvol geïmporteerd.

Locatie en naam sleutelbestand: A:\koa\sleutels\publickey.prc 29 mei 2004 13:10:00

De private sleutel en publieke sleutel behoren wel tot hetzelfde sleutelpaar.

---

Ontsleutelen gestart op 10 juni 2004 21:10:00

Ontsleutelen gestopt op 10 juni 2004 21:12:45

Er zijn 7 stemmen ontsleuteld.

---

Tellen gestart op 10 juni 2004 21:15:00.

Tellen gestopt op 10 juni 2004 21:15:40.

Er zijn 7 stemmen geteld.

Einde verwerkingsverslag