Gebruikershandleiding Hertelapplicatie Kiezen op Afstand

Security of Systems Groep
Katholieke Universiteit Nijmegen

Release v1.3

Inhoudsopgave

1 Toelichting

Deze applicatie behelst een telsysteem voor elektronisch uitgebrachte stemmen. Doel is om de uitvoer die door de programmatuur van LogicaCMG wordt gegenereerd, te kunnen controleren. Vandaar de benaming 'hertelapplicatie'. Uiteraard kan dit programma ook als gewoon telprogramma gebruikt worden om de uitslag van de betreffende verkiezingen te bepalen.

Het programma is specifiek geschreven voor de Europese verkiezingen van 2004. Het kan echter zonder wijzigingen ook voor andere verkiezingen gebruikt worden.

2 Installatie

De totale distributie is een `.zip` file. Na uitpakken levert dit een subdirectory `koa`. Deze directory bevat de files `koa.jar`, `koa.sh` en `koa.bat`. De eerste file bevat het echte programma. De andere twee files zijn scriptfiles die de applicatie goed opstarten.

Onder Windows moet men `koa.bat` uitvoeren. En onder Linux `koa.sh`.

Deze twee files kunnen overigens met een standaard editor aangepast worden om de prestaties van de hertelapplicatie te verbeteren. In deze files wordt namelijk een parameter gebruikt die de maximale heapsize voor Java aangeeft. Standaard staat deze ingesteld op 180Mb. Indien de applicatie meer dan 180Mb gebruikt, zal de garbage collector aan het werk worden gezet om niet meer gebruikt geheugen vrij te geven. Op een machine met 256Mb RAM betekent dit dat Java 180Mb mag gebruiken, zodat er nog genoeg overblijft voor het operating system zelf. Indien de machine meer geheugen heeft, kan deze parameter navenant aangepast worden.

Uiteraard werkt dit alleen maar als ofwel de J2SE Java Runtime Environment (JRE) ofwel de J2SE Software Development Kit (SDK) op het systeem geïnstalleerd is. Onze applicatie is gebaseerd op Java versie 1.4.2. Zie [2].

3 Graphical User Interface

De GUI is zeer simpel van opzet. Conform [3] bestaat het programma uit een serie knoppen die stapsgewijs tot de einduitslag van de verkiezingen zullen leiden.

Het programma dwingt af dat de verschillende functies alleen maar in de juiste volgorde kunnen worden uitgevoerd.

Zie figuur 1 voor het hoofdmenu zoals dat eruitziet na het opstarten van het programma. De extra informatie wordt telkens via popup schermen aan de gebruiker getoond.

4 Handleiding

4.1 Opnieuw Beginnen

Deze knop is toegevoegd om het mogelijk te maken om tijdens een sessie opnieuw te kunnen beginnen. Op het moment van indrukken wordt er overigens nog geen informatie gewist. Dat gebeurt pas bij het indrukken van 'Wissen Gegevens'. Deze functie is uiteraard altijd actief. Het is echter niet mogelijk om na het indrukken van deze knop nog bij de oude gegevens in het geheugen te kunnen.

Figuur 1: Hoofdmenu na opstarten

Men kan dan alleen nog gebruik maken van de rapporten die op de harde schijf zijn weggeschreven.

4.2 Wissen Gegevens

Deze functie wist het interne geheugen en verwijdert eventuele rapporten die als file zijn weggeschreven van de harde schijf. Voor dat er echt iets gewist wordt, moet de gebruiker eerst deze functie bevestigen in een dialoogscherm. Als er files op de harde schijf staan worden deze files opgesomd in het dialoogscherm waar de gebruiker de bevestiging moet geven. Zie figuur 2. Na bevestiging volgt

Figuur 2: Wissen Gegevens

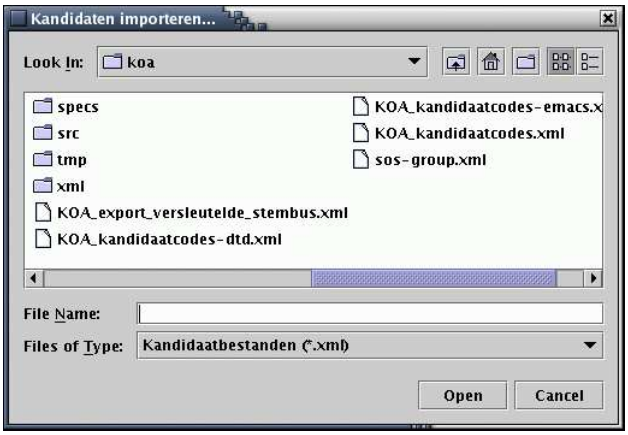
een mededeling of het wissen gelukt is of niet.

4.3 Importeren Kandidatenbestand

Er wordt een filebrowse scherm getoond waarin de gebruiker de gewenste XML file moet kiezen. Er wordt standaard een filter toegepast zodat er alleen maar files met `.xml` extensie worden getoond.

Aangezien dit een standaard component is, is dit scherm helaas in het Engels. Maar gezien het feit dat de functionaliteit zeer universeel is, mag dit geen

probleem opleveren.



Figuur 3: Importeren Kandidatenbestand

Na keuze van de file, wordt geprobeerd die file in te lezen. Afhankelijk van de grootte van de file, zal er een voortgangsbalk tevoorschijn komen. Op het moment dat op de daarbij getoonde 'Cancel' gedrukt wordt, worden de op dat moment reeds ingelezen gegevens gewist.

Als het opgegeven bestand niet van het juiste type is, zal er een foutmelding worden getoond. Is het bestand wel een echt kandidatenbestand dan zal er een scherm getoond worden met daarin een overzicht van de gevonden kieskringen en kieslijsten. Per kieslijst wordt aangegeven hoeveel kandidaten er zijn gevonden. Zie figuur 4.

De knop 'OK' zorgt ervoor dat de gegevens geaccepteerd worden en dat er vervolgens een bestand met stemmen kan worden ingelezen.

De knop 'Annuleren' zorgt ervoor dat de gegevens niet gebruikt worden. Te gebruiken als men per ongeluk een geldig maar verkeerd kandidatenbestand heeft ingelezen.

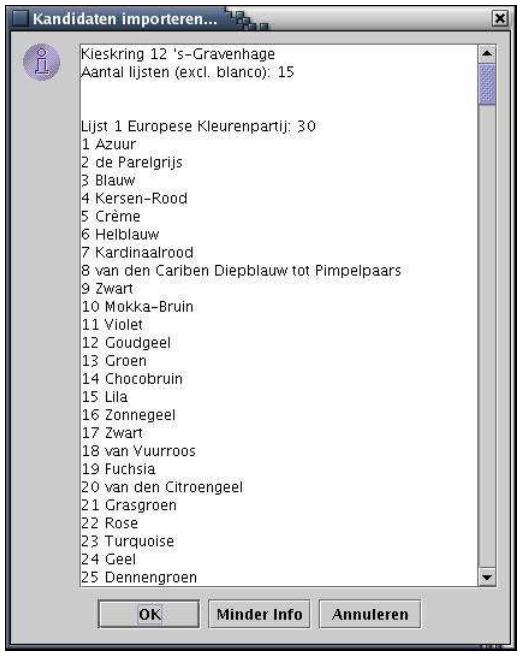
De knop 'Meer Info' geeft de gebruiker een lijst te zien met alle kandidaten. Is voor deze optie gekozen, kan men via 'Minder Info' weer terug naar het vorige scherm. De knoppen 'OK' en 'Annuleren' werken hetzelfde als in het scherm met de beperkte informatie. Zie figuur 5.

4.4 Importeren Export Stembus

Ook nu wordt er een filebrowser geopend. Het filter staat weer op `.xml` ingesteld, maar er wordt wel duidelijk gemaakt dat het nu om stembusbestanden gaat.

Is de gekozen file van een ongeldig formaat, wordt er weer een foutmelding getoond. Is het wel een goede file wordt vervolgens een overzicht getoond waarin het aantal aangetroffen kieskringen en het aantal aangetroffen mogelijke stemmen wordt getoond. Zie figuur 6.

Figuur 4: Importeren Kandidatenbestand resultaat



Figuur 5: Meer Info

Figuur 6: Importeren Export Stembus

Ook hier kan weer via 'OK' danwel 'Annuleren' door de gebruiker gekozen worden om deze gegevens te accepteren of niet.

Afhankelijk van het aantal in te lezen stemmen, kan deze actie erg lang duren. Na enkele seconden verschijnt er dan ook een voortgangsbalk met daarbij de geschatte tijd die het nog duurt om deze actie af te ronden. Zie figuur 7. Doordat deze tijd gebaseerd is op een schatting van de uit te voeren taak, is de informatie met name aan het begin niet altijd even nauwkeurig. Wordt op de 'Cancel' knop gedrukt, dan worden alle tot dan toe ingelezen stemmen weggegooid.

Figuur 7: Importeren Export Stembus voortgangsbalk

4.5 Importeren Private Sleutel

De getoonde filebrowser heeft het filter ingesteld op `.key` bestanden. Na selectie van het bestand met de private sleutel, wordt de gebruiker gevraagd om het bijbehorende wachtwoord te geven. Zie figuur 8.

De gebruiker krijgt een melding op het scherm of het inlezen van deze sleutel gelukt is of niet.

4.6 Importeren Publieke Sleutel

Voor de gebruiker werkt dit hetzelfde als bij de private sleutel. Op de achtergrond is er echter een verschil. Na het kijken of het inlezen van deze publieke sleutel gelukt is, wordt een extra test gedaan om te bepalen of de private en publieke sleutel ook een zogenaamd sleutelpaar vormen. Is dat niet het geval dan wordt hier melding van gemaakt. De gebruiker kan dan direct een nieuwe publieke sleutel inlezen. Zat het probleem echter in de keuze van een verkeerde private sleutel, zit er niets anders op dan de knop 'Opnieuw Beginnen' te gebruiken.

Figuur 8: Importeren Private Sleutel

Figuur 9: Importeren Publieke Sleutel mislukt

In het bijzonder betekent de melding dat importeren gelukt is, dus automatisch ook dat er nu een geldig sleutelpaar is ingelezen. Zie figuur 9.

4.7 Ontsleutelen

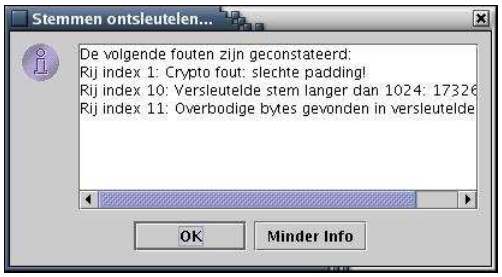
Deze functie gebruikt de ingelezen sleutels om de ingelezen versleutelde stemmen te ontsleutelen. Op het scherm wordt het aantal ontsleutelde stemmen getoond. Zie figuur 10. Dit kan kleiner zijn dan het aantal ingelezen stemmen als bij sommige stemmen de ontsleuteling mislukt is. De knop 'Meer Info' toont de

Figuur 10: Ontsleutelen

eventuele problemen per stem. Zie figuur 11.

Deze functie kan niet geannuleerd worden. In het bijzonder betekent dit dat de 'Cancel' optie die onder de voortgangsbalk staat geen echte annulering inhoudt. Bij een volgende poging tot ontsleutelen worden de inmiddels ontsleutelde stemmen uit de vorige run overgeslagen en direct geteld als reeds ontsleuteld. Wat dat betreft is deze 'Cancel' meer een onderbreking dan een annulering. Echter een zij-effect is dat eventuele foutmeldingen bij het ontsleutelen worden gewist.

Er wordt een file `tmp/decrypted.txt` aangemaakt met daarin de ontsleu-



Figuur 11: Ontsleutelen foutmeldingen

telde stemmen. Elke stem staat op een aparte regel. Als dit allemaal geldige stemmen zijn, zullen de verschillende velden van elkaar gescheiden zijn door een ';'. Op het moment dat er iets anders dan een geldige stem tevoorschijn is gekomen uit de ontsleuteling, is er niets te zeggen over de inhoud van zo'n regel.

4.8 Tellen

Deze functie telt de ontsleutelde stemmen. Aan de hand van de kandidaatcode in de stem, wordt een kandidaat gezocht in de lijst met kandidaten. Vervolgens wordt de redundante informatie in de stem vergeleken met de informatie die bij die kandidaat hoort. Verder wordt gecontroleerd of de kieskring correct is. Wordt deze validatie doorstaan, dan zal het aantal uitgebrachte stemmen voor

Figuur 12: Tellen

deze kandidaat met één opgehoogd worden. Gaat er iets mis met deze validatie wordt er niets gedaan met deze stem en gaat het programma gewoon verder met de volgende stem.

Na afloop wordt het aantal stemmen dat geldig was getoond. Zie figuur 12. De knop 'Meer Info' toont weer de eventuele problemen per stem. Zie figuur 13. Merk hierbij op dat rijen waarbij de ontsleuteling al mislukt was, er nu niet opnieuw geprobeerd is om deze stemmen te tellen en er hier dus ook geen foutmelding over die rijen te zien is.

Als het tellen eenmaal is afgerond, kan deze functie niet meer geannuleerd worden. Als het tellen echter zo lang duurt dat er een voortgangsbalk verschijnt,

Figuur 13: Tellen foutmeldingen

kan via de dan ook getoonde 'Cancel' knop de actie wel onderbroken worden. Door de vastgelegde toestandsovergangen, betekent dat echter alleen dat de gebruiker verder weinig keus heeft: ofwel kan er opnieuw geteld worden met dezelfde invoer, ofwel kan er helemaal opnieuw begonnen worden, ofwel kan het programma afgesloten worden. In elk geval is het zo dat bij elke keer dat het tellen opnieuw wordt gestart, alle tellers bij de kandidaten en partijen weer op 0 worden gezet.

4.9 Rapporteren

Deze functie biedt de gebruiker een popup scherm met daarin de keuze tussen 'Verwerkingsverslag' danwel 'Resultaat stemming' en 'Annuleren'. Zie figuur 14.

Figuur 14: Rapporteren

Voor 'Verwerkingsverslag' zijn inmiddels alle gegevens bekend. Vandaar dat de machinerie automatisch aan het werk gaat. Als het goed is komt er een melding dat het verslag is aangemaakt en is weggeschreven op de harde schijf. Indien de applicatie er in slaagt een PDF viewer te vinden op het systeem, zal die automatisch gestart worden om dit verslag op het scherm te tonen.

Merk op dat in figuur 16 bij het ontsleutelen en het tellen de foutmeldingen per stem worden getoond.

Voor 'Resultaat stemming' zijn nog niet alle gegevens bekend en daarom komen er nog twee popup schermen langs. Bij het eerste scherm (figuur 17) wordt de gebruiker gevraagd om de stemperiode te geven. Standaard wordt hier de periode specifiek voor de Europese verkiezingen van 2004 genoemd. Bij het tweede scherm (figuur 18) wordt de gebruiker gevraagd om het aantal stemgerechtigde kiezers in te geven. Standaard wordt hier het aantal ingelezen stemmen getoond. Het ingevoerde getal mag niet lager zijn dan dit voorgestelde getal. Uiteraard

Figuur 15: Rapporteren resultaat

is het de verwachting dat het in te voeren getal duidelijk hoger zal zijn dan het aantal ingelezen stemmen, daar de opkomst meestal geen 100% is. Na het invoeren van een correct aantal, wordt het PDF bestand aangemaakt. Dit kan even duren. Evenals bij 'Verwerkingsverslag' wordt het bestand opgeslagen op schijf en indien mogelijk direct getoond op het scherm.

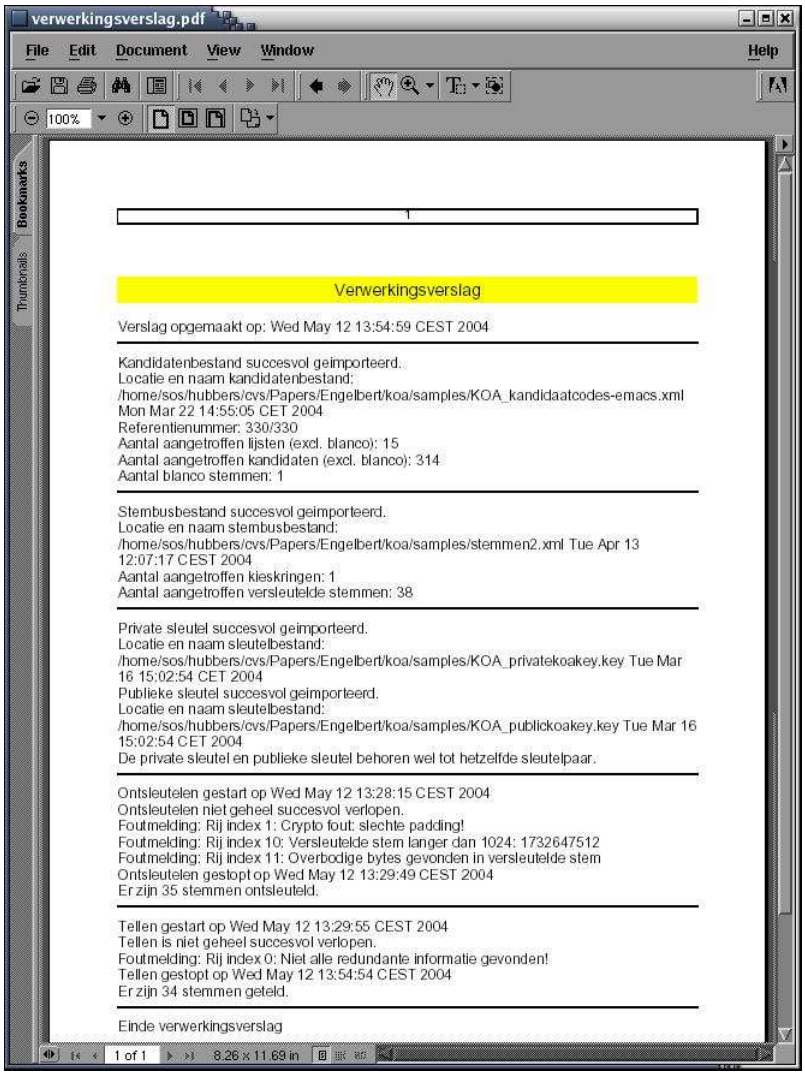
Na het succesvol aanmaken van een rapport, kan men vervolgens nog een keer kiezen voor 'Rapporteren' om het andere rapport te maken.

4.10 Help

De beschikbaarheid is onafhankelijk van de toestand van het proces. Vandaar dat deze knop ook op een aparte plaats staat. Er wordt telkens een tekst getoond die specifiek uitlegt wat er op dat moment allemaal nog gedaan kan worden. Zie figuur 21. Als dit window niet gesloten wordt, zal de inhoud zich automatisch aanpassen aan de uitgevoerde acties.

4.11 Sluiten

Ook deze functie is altijd beschikbaar en sluit het programma af. Hierbij wordt eerst om een bevestiging gevraagd. Zie figuur 22. Gegevens in het geheugen worden uiteraard gewist bij het afsluiten. De PDF rapporten die op schijf zijn opgeslagen worden niet gewist en blijven dus beschikbaar. Bij een volgende 'run' van het programma zullen deze PDF bestanden gewist worden bij de optie 'Wissen Gegevens', maar ook dan zal er eerst nog om een bevestiging worden gevraagd.

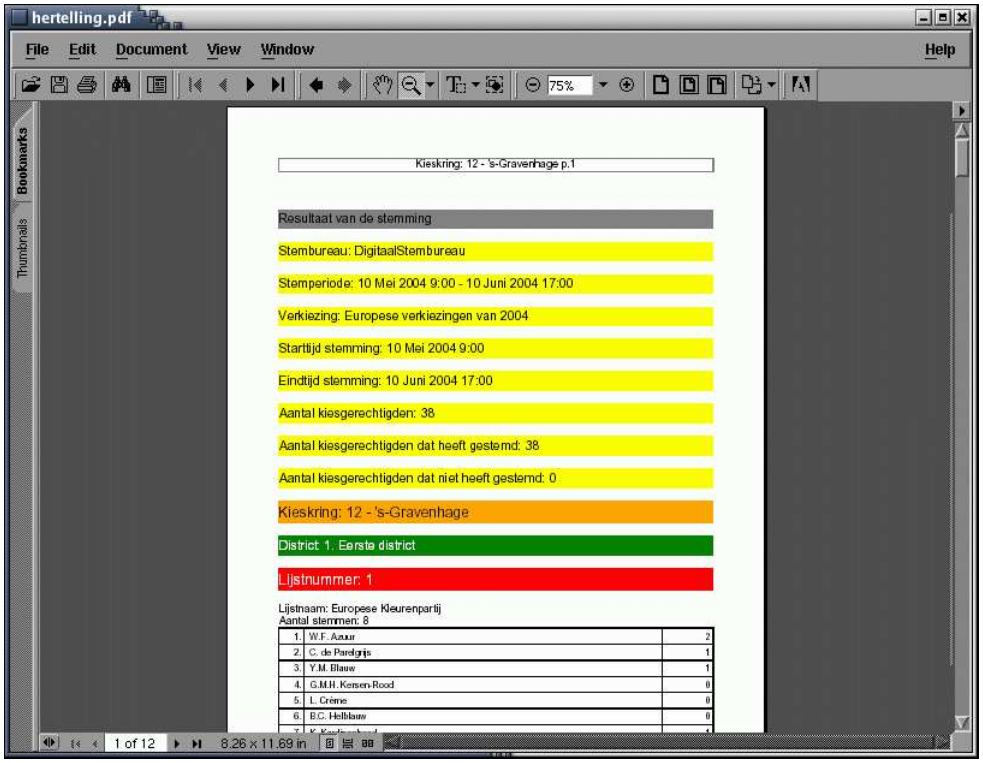


Figuur 16: Rapporteren Verwerkingsverslag

Figuur 17: Rapporteren stemperiode

Figuur 18: Rapporteren kiesgerechtigden

Figuur 19: Rapporteren Resultaat stemming



Figuur 20: Rapporteren Resultaat stemming

Figuur 21: Help

Figuur 22: Sluiten

5 Contact

Voor vragen over deze programmatuur, neem contact op met:

Engelbert Hubbers
Security of Systems groep
Katholieke Universiteit Nijmegen
Postbus 9010
6500 GL Nijmegen
hubbers@cs.kun.nl
+31 24 3652713
http:www.cs.kun.nl/sos/

Referenties

[1] LogicaCMG, KoA Team. Kiezen op afstand - hertellen stemmen. Versie A(3), 2004.

[2] SUN Microsystems. Java Runtime Environment en Software Development Kit. http://java.sun.com/j2se/1.4.2/download.html/.

[3] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Programma van Eisen Hertelprogrammatuur Kiezen op Afstand. Versie 1.0, 2004.

A Afwijkingen

Op sommige plaatsen wijkt ons programma af van de oorspronkelijke documentatie in [3] en [1]. Meestal is dit in overleg met BZK gebeurd; soms puur op eigen initiatief als het om eenvoudige zaken gaat. In deze sectie geven we een overzicht van deze punten.

1. De teksten in het hoofdmenu zijn zo gemaakt dat er bij alle acties een werkwoord staat. De helpfunctionaliteit wordt niet als actie gezien.

2. Er is een knop 'Opnieuw Beginnen' toegevoegd. Dit omdat [3] niet voorzag in de optie om een lopende sessie te onderbreken en opnieuw te beginnen.

3. Bij 'Importeren Kandidatenbestand' wordt in [3] alleen gevraagd om het aantal kandidaten per lijst. Omdat de naam van de lijst op dat moment toch al bekend is, tonen wij hier ook die naam.

4. Bij 'Importeren Kandidatenbestand' wordt gevraagd om een lijst op het scherm te krijgen met alle kandidaten en hun codes. Daar er rekening gehouden moet worden met 1000 codes per kandidaat wordt dit een enorm grote lijst. Daarom worden nu niet de codes genoemd maar alleen de kandidaten.

5. De optie van het importeren van sleutels is in ons programma expliciet opgesplitst in de keuze voor 'Importeren Private Sleutel' en 'Importeren Publieke Sleutel'. De reden hiervoor is dat het nu voor de gebruiker duidelijker moet zijn welk type sleutelbestand geselecteerd moet worden. Omdat er na het succesvol importeren van een private sleutel geen extra informatie op het scherm getoond wordt, kan de gebruiker verbaasd raken door de tweede filebrowser voor de publieke sleutel. De expliciete splitsing voorkomt dit probleem.

6. Het aangeleverde testbestand met de kandidaatcodes was niet geldig ten opzichte van de DTD in [1]. Afgezien van het probleem met de '"' bij 'Partij van de "sport", bleek ook dat het geslacht niet altijd 'M' of 'V' was zoals vereist in de DTD. Daarnaast beschikt de DTD niet over het veld 'codecount' terwijl dat wel in de file staat. Hierom hebben wij besloten niet strikt die DTD te gebruiken, maar een iets soepelere versie.

7. Ook het stembusbestand voldeed niet aan de DTD in [1]. Dit had te maken met de hoofdletters. Wij gebruiken hier dan ook niet de gegeven DTD maar de versie die werkt met het testbestand.

8. In het verwerkingsverslag wordt volgens de definitie het referentienummer van het kandidatenbestand getoond. Daar het niet geheel duidelijk is of het hier om de 'request' dan wel 'response' referentie gaat, tonen wij beide.

9. In het verwerkingsverslag hebben we bij alle files waar om een timestamp wordt gevraagd, gezorgd dat de begeleidende tekst hetzelfde was. Dat is in [3] niet het geval.

10. In het eindverslag met het resultaat van de stemming wijken wij ook af van de definitie in [3]. In de definitie staat namelijk dat de regel voor aantal stemmen leeg moet blijven om later met de hand in te vullen. Wij hebben dit opgelost door bij het aanmaken van dit rapport de gebruiker dit aantal stemgerechtigden in te laten voeren. Motivatie hiervoor is dat in het ons ter beschikking gestelde voorbeeldbestand dit getal ook al is ingevuld.

11. Verder bevat het voorbeeldrapport dat wij gekregen hebben ook een regel voor het aantal kiesgerechtigden dat niet gestemd heeft die niet in de definitie staat. Wij hebben ook zo'n regel opgenomen waarbij de waarde van dit veld wordt bepaald door het aantal getelde stemmen af te trekken van het ingevoerde aantal kiesgerechtigden.

12. Ons verslag gebruikt kleuren om duidelijk onderscheid te kunnen maken tussen globale informatie als het stembureau en de periode en de informatie per kieskring. Omdat er bij deze vekiezingen slechts één kieskring gebruikt wordt, is de toegevoegde waarde niet echt groot.

13. In het bijzonder is dit ook de reden waarom de regel met 'Kieskring' pas onder de globale informatie staat. Dit om voorbereid te zijn op invoer met meerdere kieskringen.

14. Op speciaal verzoek schrijven wij een file `tmp/decrypted.txt` weg met daarin de ontsleutelde stemmen. Deze file wordt niet gewist na het afsluiten van het programma. Hij wordt wel automatisch gewist bij de functie 'Wissen Gegevens'.