Toetsing eisen
OSV 4 voor Europese Verkiezingen

Rapport t.b.v. de Kiesraad

18 mei 2009

Dr. Sieuwert van Otterloo
+31 20 314 0950
s.vanotterloo@sig.nl

Software Improvement Group

Arent Janszoon Ernststraat 595-H
NL-1082 LD Amsterdam
t +31 (0)20 314 09 50
f +31 (0)20 314 09 55
info@sig.nl
www.sig.nl

Het onderzoek dat in dit rapport is beschreven is uitgevoerd in opdracht van Mw. Mr. J. Schipper-Spanninga, Secretaris-directeur van de Kiesraad

Het rapport is geschreven door Dr. Sieuwert van Otterloo van de Software Improvement Group.

© 2009, Software Improvement Group
A. J. Ernststraat 595-H
1082 LD Amsterdam
The Netherlands

Managementsamenvatting

De Kiesraad heeft programmatuur laten ontwikkelen ter ondersteuning van het verkiezingsproces, en wil deze programmatuur beschikbaar stellen aan de stembureaus voor gebruik bij verkiezingen. De eerste verkiezingen waarvoor de programmatuur gebruikt gaat worden zijn de Europese verkiezingen op 4 juni 2009.
De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties heeft eisen gesteld waaraan deze programmatuur moet voldoen. Eén van deze eisen is dat er door een onafhankelijke instantie een toets gedaan wordt. Het gaat hierbij om toetsing van deel 4 en 5 van de programmatuur *Ondersteunende Software Verkiezingen* (OSV), omdat deze delen gebruikt zullen worden voor de verwerking van verkiezingsresultaten. De Software Improve-ment Group is door de Kiesraad gevraagd om deze toetsing uit te voeren, te beginnen met de programmatuur voor Europese verkiezingen.
Dit rapport geeft de resultaten voor OSV 4 voor gebruik bij de Europese verkiezingen. In een volgend rapport zal ook OSV 5 getoetst worden voor gebruik bij de Europese verkiezingen. Tenslotte zal ook de versie van de programmatuur geschikt voor verkiezingen van de Tweede Kamer, Provinciale Staten en Gemeenteraden getoetst worden in een derde rapport.

Er is vastgesteld dat de programmatuur bovengemiddeld scoort op belangrijke kwaliteitsaspecten waaronder ontwerp en modulariteit. Uit de toetsing aan gestelde eisen is naar voren gekomen dat de programmatuur voor OSV 4 op de volgende kanttekeningen na voldoet aan gestelde eisen:

- Gerelateerd aan eis 3 zijn er op ongeveer 180 plaatsen detailpunten in de broncode gevonden zijn die verbeterd moeten worden. De leverancier heeft toegezegd dit te verbeteren en in het laatste eindrapport zal dit getoetst worden.
- Het is nog te bepalen of er aan eis 4c voldaan wordt. Of de programmatuur conform eis 4c 'open source' ontwikkeld is, wordt bepaald door de licentie waaronder de programmatuur wordt verspreid. Deze licentie moet nog worden gekozen.
- Gerelateerd aan eis 7, valt het op dat er alleen op het moment van installatie een mechanisme is om authenticiteit van programmatuur vast te stellen. Als de programmatuur in een afgeschermde omgeving gebruikt wordt, is hiermee aan eis 7 voldaan.
- Met betrekking tot eis 9 (formele validatie) is vastgesteld dat OSV 4 voor de Europese verkiezingen alleen berekeningen bevat voor het totaliseren van getelde stemmen. Voor deze berekeningen (te weten optellingen) zijn geen bijzonderheden in wet- of regelgeving opgenomen. Hierdoor is deze eis niet van toepassing voor OSV 4. Daadwerkelijke toetsing van eis 9 vindt dus plaats bij beoordeling van OSV 5.

Tijdens het onderzoek zijn verder geen zaken aangetroffen die de Kiesraad zou moeten weerhouden van verspreiding van OSV 4 voor gebruik door stembureaus voor de Europese verkiezingen van 4 juni 2009.

© 2009 Software Improvement Group

© 2009 Software Improvement Group

Inhoudsopgave

© 2009 Software Improvement Group

© 2009 Software Improvement Group

1 Inleiding

1.1 Context

De Kiesraad heeft programmatuur laten ontwikkelen ter ondersteuning van het verkiezingsproces en wil deze programmatuur beschikbaar stellen aan de stembureaus voor gebruik bij verkiezingen. Het gaat om een verzameling programma's genaamd 'Ondersteunende Software Verkiezingen (OSV)'. Deze programmatuur stelt stembureaus in staat om getelde stemmen in te voeren, op te slaan, samen te voegen en tenslotte de gekozen kandidaten te bepalen.
De programma's OSV 4 en OSV 5 zijn de programma's uit OSV die door de verschillende stembureaus gebruikt worden na de verkiezingen voor verwerking van uitslagen. De overige programma's zijn voor het aanmaken van de benodigde informatie (verkiezingsdefinities en kandidatenlijsten) ter voorbereiding van verkiezingen.

1.2 Aanleiding

Door middel van een brief aan de Tweede Kamer op 9 april 2008 heeft de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties eisen gesteld waaraan OSV 4 en 5 moeten voldoen, voordat zij gebruikt kunnen worden in het verkiezingsproces. Eén van deze eisen is dat er door een onafhankelijke instantie een toets gedaan wordt in opdracht van de Kiesraad of de programmatuur aan deze eisen voldoet. Daarnaast heeft de Kiesraad er belang bij om de onderhoudbaarheid van de programmatuur vast te laten stellen. Dit onderzoek heeft als doel om inderdaad deze toetsing te doen en secundair de onderhoudbaarheid vast te stellen.

1.3 Scope

Het gehele onderzoek heeft betrekking op programma 4 en programma 5 van de OSV programmatuur. Aangezien de resultaten van dit onderzoek beschikbaar moeten zijn voor acceptatie van de verschillende delen van de programmatuur, zullen in totaal drie rapporten door de SIG geschreven worden, waarvan de eerste twee een beperkte scope hebben. Het laatste rapport zal alle resultaten van het onderzoek bevatten.

Titel rapport	Scope	Status
Toetsing eisen OSV 4 voor Europese verkiezingen	Toetsing eisen voor OSV 4 voor Europese verkiezingen	Beschikbaar (is dit rapport)
Toetsing eisen OSV 5 voor Europese verkiezingen	Toetsing eisen voor OSV 5 voor Europese verkiezingen	Nog op te leveren
Toetsing eisen OSV 4 en 5	Toetsing eisen voor OSV 4 en 5 voor overige verkiezingen	Nog op te leveren

1.4 Onderzoeksvragen

De primaire vraag voor het uitgevoerde onderzoek is:

© 2009 Software Improvement Group

Toets programma's 4 en 5 van OSV aan de 11 gestelde eisen (omschreven in "Eisen voor programmatuur die gebruikt wordt ..." - brief aan Tweede Kamer van 9 april 2008).

Een secundaire vraag voor dit onderzoek is de volgende:

Bepaal secundair de technische kwaliteit van programma's 4 en 5 en daaruit volgend de mate van onderhoudbaarheid van de programmatuur.

In dit rapport wordt alleen ingegaan op het beantwoorden van de eerste onderzoeksvraag voor OSV 4 voor de Europese verkiezingen. In een volgend rapport zal de eerste onderzoeksvraag beantwoord worden voor OSV 5 voor de Europese verkiezingen. De tweede vraag zal voor OSV 4 en 5 als geheel beantwoord worden in het laatste rapport.

1.5 Structuur van dit rapport

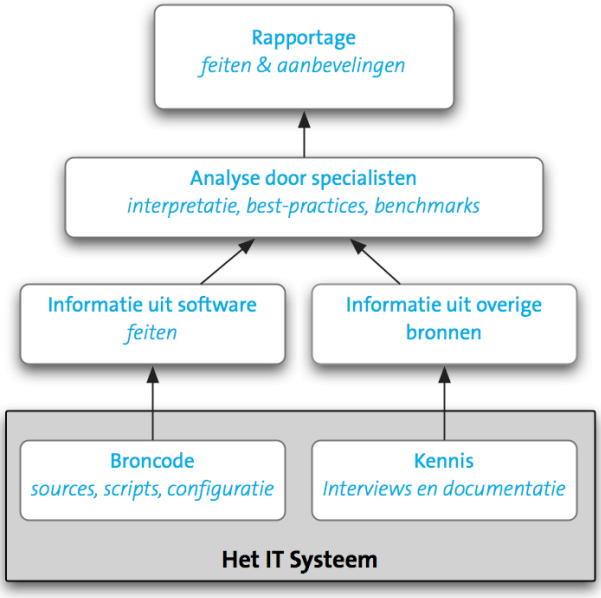
De structuur van dit rapport is als volgt. Hoofdstuk 2 bevat een overzicht van het onderzoeksproces. Hoofdstuk 3 bevat de antwoorden op de eerste onderzoeksvraag rondom de 11 gestelde eisen. Hoofdstuk 4 besluit met conclusies en aanbevelingen. In de appendix is aanvullende, veelal technische, informatie opgenomen over de onderzochte programmatuur.

© 2009 Software Improvement Group

2 Onderzoeksproces

2.1 Uitgangspunten

De SIG is gespecialiseerd in het uitvoeren van onderzoek naar kwaliteit van onderhoudbaarheid van programmatuur op basis van broncode-onderzoek. De basis van het onderzoek wordt daarom gevormd door de feiten verzameld door onderzoek van de aangeleverde broncode. Daarnaast is er aanvullende documentatie als bron gebruikt en zijn gesprekken gevoerd met IVU medewerkers ter verduidelijking.
Op basis van de hieruit vastgestelde feiten is er een interpretatie gedaan door SIG medewerkers om te komen tot antwoorden op de onderzoeksvragen. Deze antwoorden zijn gemotiveerd vanuit de vastgestelde feiten. Deze werkwijze is schematisch weergegeven in Figuur 1.



Figuur 1: Opzet van een onderzoek naar software op basis van broncode. De SIG hanteert een werkwijze waarin eindconclusies gebaseerd zijn op vastgestelde feiten.

2.2 Bronnen

De volgende broncode is door SIG ontvangen en gebruikt als basis voor dit onderzoek:

- Source code OSV 4 en 5, versie van 17 april 2009
- Test source code, versie van 17 april 2009

Naast deze broncode heeft de SIG de volgende ondersteunende documentatie ontvangen ten behoeve van dit onderzoek:

- Gedetailleerde specificatie OSV 1.3.3, ontvangen op 17 april 2009
- Handleiding programma P4 v0.2, ontvangen op 17 april 2009
- Handleiding programma P5 v0.1, ontvangen op 17 april 2009
- 'Determination of the election result', versie van 22 april 2009
- 'List of plausibility checks', ontvangen op 22 april 2009
- Configuratie-bestanden, versie van 22 april 2009

© 2009 Software Improvement Group

Tevens heeft de SIG van de Kiesraad ontvangen:

- Overeenkomst inzake ondersteunende software verkiezingen – overeenkomst tussen de Kiesraad en IVU.
- Verklaring van Destatis over gebruik van de WAS-programmatuur – Brief 26 maart 2009.
- "Eisen voor programmatuur die gebruikt wordt bij de berekening van de uitslag van verkiezingen die vallen onder de werking van de Kieswet" - brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer op 9 april 2008 met daarin de aan de programmatuur gestelde eisen.

De volgende algemeen beschikbare documenten zijn tevens geraadpleegd tijdens dit onderzoek.

- Actieplan 'Nederland open in verbinding' – gepubliceerd door het Ministerie van Economische zaken
- GBA logisch ontwerp versie 3.6
- 'Legal, operational and technical standards', aanbeveling door de Raad van Europa voor elektronisch stemmen
- Open source initiative website - http://www.opensource.org/ - geraadpleegd op 12 mei 2009
- JBoss Enterprise Application platform certified and compatible configurations - http://www.jboss.com/products/platforms/application/testedconfigurations/ - geraadpleegd op 12 mei 2009

2.3 Betrokken personen

Bij dit onderzoek is er contact geweest, direct of per telefoon of email, met de volgende personen.

- Dhr. D. Cosic (IVU),
- Prof. Dr. E. Denert (IVU),
- Dhr. S. Eulitz (IVU),
- Ing R. Mulder (IVU),
- Dhr. J. Nottebaum (IVU),
- Mr. J. Koëter (De Brauw Blackstone Westbroek),
- Mw. Mr. J. Schipper-Spanninga (Kiesraad),
- Mw. Mr. R. Hoorweg (Kiesraad).

Tijdens het onderzoek hebben zijn de volgende meetings gepland als vast contact momenten als onderdeel van de onderzoeksaanpak. Naast deze sessies is er informeel contact geweest tussen de medewerkers van SIG en IVU en met Mr. Koëter.

© 2009 Software Improvement Group

Datum	Meeting	Aanwezig
9 april 2009	Bespreking assessment-aanpak	E. Denert, R. Mulder, S. Eulitz, S. van Otterloo, Y. Kanellopoulos
16 april 2009	Technische sessie - uitleg OSV door IVU experts	S. Eulitz, D. Cosic, S. van Otterloo, Y. Kanellopoulos, J. Heijmans
28 april 2009	Bespreking formele methoden (telefonisch)	J. Nottebaum, S. van Otterloo, Y. Kanellopoulos, J. Heijmans
29 april 2009	Validatiesessie (telefonisch) – validatie van door SIG vastgestelde technische feiten door IVU	S. Eulitz, D. Cosic, J. Nottebaum, S. van Otterloo, Y. Kanellopoulos, J. Heijmans
8 mei 2009	Eindpresentatie	J. Schipper-Spanninga, R. Hoorweg, S. van Otterloo, M. Hissink Muller, J.H. van der Linden

© 2009 Software Improvement Group

3 Antwoorden toetsing aan eisen

In deze sectie is per eis weergegeven of er aan voldaan is en wat de motivatie is voor dit oordeel.

3.1 Eis 1: functionaliteit

3.1.1 Eis en conclusie

Gestelde eis:

> *De programmatuur bevat de functionaliteiten die (conform wet- en regelgeving) nodig zijn voor de berekening van de uitslag (inclusief tussenstappen en tussenresultaten) door het centrale stembureau en de uitvoer daarvan.*

Conclusie:

- Ja, er is voldaan aan deze eis.

3.1.2 Motivatie

- De leverancier heeft per sectie uitgelegd welke functionaliteit bevat is in elke module. De SIG heeft de broncode van iedere module geïnspecteerd om te zien of dit overeenkomt met de uitleg, en heeft nagegaan dat het geheel van de modules voldoende is voor berekening van de uitslag en uitvoer daarvan. In de appendix is de gegeven uitleg van de functionaliteit opgenomen.
- De werking is gedemonstreerd tijdens de technische sessie.
- Er is door de Kiesraad een acceptatietest uitgevoerd waarin de werking van de functionaliteiten is vastgesteld.

3.2 Eis 2: documentatie

3.2.1 Eis en conclusie

Gestelde eis:

> *De functionaliteit van de programmatuur is beschreven en vastgelegd in documenten (functioneel ontwerp, technisch ontwerp, etc.). Deze documenten zijn openbaar.*

Conclusie:

- Ja, er is voldaan aan deze eis.

3.2.2 Motivatie

- De functionaliteit is beschreven in de gedetailleerde specificatie - OSV - Kiesraad, versie 1.3. Dit document zal door de Kiesraad op zijn website gepubliceerd worden.
- De SIG heeft een review gedaan op de gedetailleerde specificatie en per sectie vastgesteld dat de beschreven functionaliteit overeenkomt met de door SIG in de programmatuur aangetroffen functionaliteit.

© 2009 Software Improvement Group

3.3 Eis 3: ontwerp

3.3.1 Eis en conclusie

Gestelde eis:

> *Het ontwerp van de programmatuur voldoet aan geaccepteerde kwaliteitseisen c.q. best practices voor de ontwikkeling van programmatuur: Daartoe:*
>
> *a. Is de programmatuur gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn.*
> *b. Zijn kritische functies in de programmatuur gescheiden.*
> *c. Zijn gegevens die aan verandering onderhevig zijn (configuratieparameters) zonder aanpassingen van programmatuur te wijzigen.*
> *d. Wordt toevallig of opzettelijk foutief gebruik van de programmatuur, voor zover als redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen.*

Conclusie:

- Ja, er is voldaan aan de eis als geheel en de vier in de genoemde deel-eisen.

3.3.2 Motivatie 3a en 3b

Er is een duidelijke module-structuur, die zorgt voor een scheiding van bijvoorbeeld berekening uitslag, data-opslag en in- en uitvoer. Deze modulestructuur is weergegeven in de appendix. Hiermee wordt voldaan aan 3a en 3b.

3.3.3 Motivatie 3c

Door middel van een ‘election definition file’ kan het programma zonder aanpassingen voor een volgende verkiezing gebruikt worden. Door herinstallatie kan het programma in een andere rol of voor een andere regio gebruikt worden zonder aanpassingen aan de code. Hiermee is voldaan aan eis 3c.

3.3.4 Motivatie 3d

Er worden geen nieuwe risico’s geïntroduceerd door gebruik van de programmatuur, omdat het programma niet van buiten toegankelijk is. De programmatuur zal gebruikt worden op een afgezonderde netwerkomgeving die geen verbinding met de buitenwereld heeft. Hiermee wordt misbruik van buitenaf uitgesloten.
Het programma bevat toetsen die onopzettelijke foutieve invoer tegengaan. Deze toetsen zijn weergegeven in de appendix. Opzettelijk foutieve invoer door een stembureaumedewerker is ook zonder programmatuur mogelijk en kan redelijkerwijs technisch niet voorkomen worden.

3.3.5 Motivatie eis 3 als geheel

De hoofdtekst van eis 3 gaat verder dan de genoemde deel-eisen, omdat er ook in het algemeen gesproken wordt over geaccepteerde eisen. De SIG doet daarom een toetsing

© 2009 Software Improvement Group

aan door de SIG gehanteerde kwaliteitseisen voor technische kwaliteit van programmatuur. Er zijn hierbij in de broncode ongeveer 180 detailpunten gevonden die aanpassing behoeven. De leverancier heeft toegezegd dat de broncode op deze punten aangepast zal worden. In het uiteindelijke rapport zal getoetst worden of dit gebeurd is.

3.4 Eis 4: open standaarden en open source

3.4.1 Eis en conclusie

Gestelde eis:

Conform het actieplan Nederland open in verbinding van het kabinet geldt voor de programmatuur:

a. Dat gebruik wordt gemaakt van open standaarden. Voor verkiezingsgegevens (waaronder kandidatenlijsten en zetelverdeling) wordt de open standaard EML gebruikt.

b. Dat deze is geschreven in een gangbare programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler en/of interpreter beschikbaar is.

c. Dat deze als open source ontwikkeld is. De broncode van de programmatuur is openbaar. Indien de programmatuur voor de centrale stembureaus wordt ontwikkeld dan dient het intellectueel eigendom van de broncode van de programmatuur te berusten bij een van de centrale stembureaus.

Conclusie:

- Het is nog te bepalen of aan deze eis wordt voldaan.
  - Ja voor 4a
  - Ja voor 4b
  - Nog te bepalen voor 4c omdat nog te bepalen is of de programmatuur open source ontwikkeld is. De broncode wordt wel openbaar. De programmatuur is niet voor de Kiesraad ontwikkeld, maar alleen voor Kiesraad aangepast.

3.4.2 Motivatie 4a

- De programmatuur maakt gebruik van de open standaard EML en de open standaard PDF.
- Naast deze open standaarden maakt de programmatuur gebruik van de niet-open standaard RTF. Deze standaard wordt niet onafhankelijk beheerd en is daardoor niet open, maar is wel een door veel partijen gebruikte standaard voor bestandsuitwisseling. Omdat de in RTF aangeboden informatie ook in PDF beschikbaar is, gaat dit niet in tegen de eis.

3.4.3 Motivatie 4b

- Het programma is hoofdzakelijk geschreven in de programmeertaal Java. Voor deze taal is een open source compiler beschikbaar, namelijk Eclipse. Het feit dat er een actieve gemeenschap is blijkt uit de activiteiten vermeld onder www.eclipse.org/community
- De overige talen zijn Javascript, JSP en XSLT. Ook hiervoor is aan de eis voldaan.

© 2009 Software Improvement Group

- Voor Javascript is door ECMA een standaard gedefinieerd, en is Firefox beschikbaar als interpreter. Uit de events vermeld op http://www.spreadfirefox.com/news_events blijkt dat er een actieve gemeenschap is.
- JSP is een open standaard. Het JBoss-platform bevat een open source interpreter voor deze taal. Uit de events vermeld op http://www.jboss.org/ blijkt dat er een actieve gemeenschap is.
- XSLT is een open standaard, waarvoor Xalan een open source interpreter is. Hiervoor is een actieve gemeenschap die te bereiken is via http://xml.apache.org/xalan-j/.

3.4.4 Motivatie 4c

- Het actieplan Nederland Open In Verbinding stelt op pagina 28: "*Open source software is software die een door het open source initiative goedgekeurde licentie heeft en daarmee voldoet aan twee kenmerken: de broncode is vrij beschikbaar; in het licentiemodel is het intellectueel eigendom van de software en de bijbehorende broncode dusdanig geregeld dat de licentienemer de broncode mag inzien, gebruiken, verbeteren, aanvullen en distribueren.*"
- Er is nog geen licentie gekozen waaronder de broncode zal worden gepubliceerd, waardoor nog niet te bepalen is of deze licentie voldoet aan de geciteerde definitie van open source.
- De kern van de programma's OSV 4 en OSV 5 is gebaseerd op een eerder voor een derde partij ontwikkeld programma, namelijk een programma ontwikkeld voor het Duitse overheidsorgaan Destatis. Destatis heeft het intellectueel eigendomsrecht op deze kern.
- Er zijn wel afspraken gemaakt met Destatis die de Kiesraad in staat stellen de programmatuur ter inzage te publiceren, te gebruiken en aan te passen. De broncode van de programmatuur zal ook op de website van de Kiesraad worden gepubliceerd. Hiermee wordt aan het tweede deel van eis 4c voldaan.
- De kern van OSV 4 en 5 is niet specifiek voor de kiesraad ontwikkeld, en dus is het derde deel van eis 4c niet van toepassing.

3.5 Eis 5: verschillende besturingssystemen

3.5.1 Eis en conclusie

Gestelde eis:

De programmatuur is beschikbaar op verschillende systeemarchitecturen en verschillende besturingssystemen, waaronder in ieder geval gangbare open source besturingssystemen

Conclusie:

- Ja, er is aan deze eis voldaan.

3.5.2 Motivatie

- Het programma is gebaseerd op het JBoss platform. JBoss is zelf gebaseerd op het Java-platform.
- De leverancier van JBoss geeft aan dat JBoss geschikt is voor alle operating systemen die een juiste versie van het Java-platform bieden en een standaard da-

© 2009 Software Improvement Group

tabase omgeving. Hieraan is voldaan voor onder andere Linux, Windows en Mac OS X
    - Voor zowel Linux, Windows en Mac OS X is er een juiste versie van het Java-platform
    - Voor zowel Linux, Windows en Mac OS X is er een geschikte database
- Als additionele zekerheid biedt de leverancier van JBoss ondersteuning van een groot aantal gecertificeerde configuraties die gebaseerd zijn op het open source besturingssysteem Linux.

3.6 Eis 6: diakritische tekens

3.6.1 Eis en conclusie

Gestelde eis:

Voor naamgeving dient de programmatuur de diakritische tekens van de GBA tekenset te ondersteunen.

Conclusie

- Ja, er is aan deze eis voldaan.

3.6.2 Motivatie

- De programmatuur is geschikt voor verwerking van alle Unicode tekens, omdat het gebruik maakt van de UTF-8 codering voor Unicode.
- In de eisen wordt verwezen naar het logisch ontwerp 3.6 van GBA. Hierin wordt ook Unicode codering genoemd als alternatieve codering in web-omgeving

3.7 Eis 7: authenticiteit programmatuur

3.7.1 Eis en conclusie

Gestelde eis:

Het is mogelijk de authenticiteit van de programmatuur vast te stellen.

Conclusie:

- Ja, er is aan deze eis voldaan.

3.7.2 Motivatie

- Er is een op 'hashcodes' (digitale vingerafdruk) gebaseerde methode om de authenticiteit van de installatiebestanden vast te stellen.
- Het is door middel van de programmatuur niet mogelijk om na installatie de authenticiteit van de programmatuur vast te stellen. Hierdoor is het nodig dat het programma in een afgeschermde omgeving gebruikt wordt. Dit wordt door de Kiesraad voorgeschreven, waardoor aan deze eis is voldaan.

© 2009 Software Improvement Group

3.8 Eis 8: authenticiteit gegevens

3.8.1 Eis en conclusie

Gestelde eis:

> *Alle elektronische communicatie van of naar andere programmatuur, hetzij via een netwerk, via opslagmedia of anderszins, is voorzien van een mogelijkheid om de authenticiteit van de gegevens vast te stellen, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.*

Conclusie:

- Ja, er is aan deze eis voldaan.

3.8.2 Motivatie

- Bij elke uitvoer van gegevens wordt een 'hashcode' berekend en weergegeven in een afdrukbaar document. Door dit afgedrukte document kan de authenticiteit bij inladen van gegevens worden gecontroleerd.
- Er wordt gebruik gemaakt van een cryptografisch sterk hash algorithme (SHA-1) dat voor 2009 voldoende veiligheid biedt. Als in de toekomst nodig mocht blijken om dit algoritme te wijzigen kan dit door wijziging van één regel in de broncode.

In de appendix is een overzicht opgenomen van de opzet van de report generator module, waarin is weergegeven hoe een hashcode berekend wordt.

3.9 Eis 9: formele methodes

3.9.1 Eis en conclusie

Gestelde eis:

> *Met behulp van formele methoden is wiskundig aangetoond dat berekeningen in de programmatuur precies datgene doen wat door de wet- en regelgeving is voorgeschreven.*

Conclusie:

- Deze eis is niet van toepassing op OSV 4.

3.9.2 Motivatie

- OSV 4 voor de Europese verkiezingen bevat alleen berekeningen voor het totaliseren van getelde stemmen. Voor deze berekeningen (te weten optellingen) zijn geen bijzonderheden in wet- of regelgeving opgenomen. Hierdoor is deze eis niet van toepassing voor OSV 4.
- Er is voor OSV 5 een formele definitie gegeven die beschrijft hoe zetels verdeeld worden. Deze zal in de rapportage over OSV 5 worden gebruikt om deze eis te toetsen.

© 2009 Software Improvement Group

3.10 Eis 10: onafhankelijke toetsing

3.10.1 Eis en conclusie

Gestelde eis:

De programmatuur wordt in opdracht van de centrale stembureaus door een of meer onafhankelijke instanties getoetst voordat de centrale stembureaus de programmatuur accepteren en gebruiken. De uitkomst(en) van de toets(en) zijn openbaar.

Conclusie:

- Ja, er is aan deze eis voldaan.

3.10.2 Motivatie

- De SIG voert deze toetsing uit.
- Dit eindrapport mag door de Kiesraad openbaar gemaakt worden als resultaat van toetsing van OSV 4 voor de Europese verkiezingen. Ook de volgende eindrapporten mogen worden openbaar gemaakt.

3.11 Eis 11: elektronisch stemmen

3.11.1 Eis en conclusie

Gestelde eis:

Voor zover nog verder van toepassing dient de programmatuur te voldoen aan de aanbevelingen van de Raad van Europa voor elektronisch stemmen

Conclusie:

- Deze eis is niet van toepassing.

3.11.2 Motivatie

- Er wordt niet elektronisch gestemd door middel van de onderzochte programmatuur. De aanbevelingen zijn daardoor niet van toepassing.

© 2009 Software Improvement Group

4 Conclusies en aanbevelingen

4.1 Conclusies

Uit de toetsing aan gestelde eisen is naar voren gekomen dat de programmatuur voor OSV 4 op de volgende kanttekeningen na voldoet aan gestelde eisen:

- Gerelateerd aan eis 3 zijn er op ongeveer 180 plaatsen detailpunten in de broncode gevonden zijn die verbeterd moeten worden. De leverancier heeft toegezegd dit te verbeteren en in het laatste eindrapport zal dit getoetst worden.
- Het is nog te bepalen of er aan eis 4c voldaan wordt. Of de programmatuur conform eis 4c 'open source' ontwikkeld is, wordt bepaald door de licentie waaronder de programmatuur wordt verspreid. Deze licentie moet nog worden gekozen.
- Gerelateerd aan eis 7, valt het op dat er alleen op het moment van installatie een mechanisme is om authenticiteit van programmatuur vast te stellen. Als de programmatuur in een afgeschermde omgeving gebruikt wordt, is hiermee aan eis 7 voldaan.
- Met betrekking tot eis 9 (formele validatie) is vastgesteld dat OSV 4 voor de Europese verkiezingen alleen berekeningen bevat voor het totaliseren van getelde stemmen. Voor deze berekeningen (te weten optellingen) zijn geen bijzonderheden in wet- of regelgeving opgenomen. Hierdoor is deze eis niet van toepassing voor OSV 4. Daadwerkelijke toetsing van eis 9 vindt dus plaats bij beoordeling van OSV 5.

Tijdens het onderzoek zijn verder geen zaken aangetroffen die de Kiesraad zou moeten weerhouden van verspreiding van OSV 4 voor gebruik door stembureaus voor de Europese verkiezingen van 4 juni 2009.

4.2 Aanbevelingen

Als gevolg van dit rapport zijn er geen verdere adviezen of aanbevelingen. Eventuele adviezen of aanbevelingen voor de langere termijn zullen worden gegeven in het laatste eindrapport over OSV 4 en 5 voor alle soorten verkiezingen.

© 2009 Software Improvement Group

A. Aanvullende informatie

In deze appendix is per eis aanvullende informatie gegeven.

A.1 Algemene informatie: omvang en technologieën

In onderstaande tabel is het volume van de broncode weergegeven. Per gebruikte taal en technologie. Hieruit blijkt dat dit een hoofdzakelijk in Java ontwikkeld systeem is.

Technologie	Regels code
Java	34,000
Javascript	900
Java testcode	2500
JSP	8500
XSLT	200

De Java testcode betreft code die in Java geschreven is en die niet nodig is om het programma te gebruiken, maar controles doet op de werking van delen van het programma. Het beschikbaar hebben van testcode zorgt ervoor dat de werking van het programma automatisch gecontroleerd kan worden, wat de onderhoudbaarheid ten goede komt.

A.2 Eis 1: functionaliteit

De broncode van dit systeem is verdeeld in verschillende modules. Deze modules zijn weergegeven in onderstaande tabel, met daarbij de in de technische sessie gegeven omschrijving van de beoogde functionaliteit van de module.

Module/package	Functionality	Location
Common	Utility functions not only used by part 4 or 5	Business layer
Ejb	Utility functions not only used by part 4 or 5	Business layer
Util	Utility functions not only used by part 4 or 5	Business layer
Wahl.admin	Functionality of administrator role	Business layer
Wahl.anwender	User administration	Business layer
Wahl.auswertung	Reports and screen generation via the generator	Business layer
Wahl.client	Presentation base for interaction with web browser (via JSP)	Business layer
Wahl.dataimport	Importing of election data in EML 230 format and election definition format	Business layer
Wahl.export	Exporting of election data in EML format	Business layer

© 2009 Software Improvement Group

Module/package	Functionality	Location
Wahl.Eingang	Manual input of voting data in EML 150 format. Manual input of voting data.This part contains validity and plausibility checks	P4, P5 specific code
Wah.I18n	Functionality to show program in different languages	Business layer
Wahl.mbean	Extension to JBoss for creating data base structure, and for making exported files available via the web browser	mbean
Wahl.Modell	Persistence Functionality to store election data elements in the data base	Persistence
Wahl.result	Functionality of P5 to assign seats based on the voting data	P4, P5 specific code
Wahl.runtime	Caching mechanism to store computed results to improve performance. It is not clear whether this is currently used, but may be needed in future	Business layer
Wahl.util	Not used	Business layer
Reportgenerator	Functionality to create EML files and PDF/RTF output	Report generator
xmlsecurity	Code to determine how EML files are validated, including the choice for the SHA-1 hash function	Business layer

A.3 Eis 2: documentatie

In de onderstaande tabel is het resultaat weergegeven van de review van de gedetailleerde specificatie. Op de meeste punten heeft de SIG direct kunnen vaststellen dat dit overeenkomt. Op twee punten heeft de SIG nog niet kunnen vaststellen dat de onderzochte versie van de documentatie en broncode overeenkomen. Dit zal in het definitieve rapport opgehelderd worden.

© 2009 Software Improvement Group

Section (page)	Summary	OK?	Remarks SIG
2.5 (40)	P4 automates the adding of votes level by level. The number and kind of levels differs per type of election. Votes counts are transported using EML between levels, except for the first level.	Yes	Demonstrated and tested.
2.5.1 (41)	An administrator must prepare the application for use.	Yes	Demonstrated and tested.
2.5.2.1 (41)	Access restriction by ID/password. There are three kinds of use(r)s: administration, data entry and finalization of data.	Yes	All three uses were demonstrated and tested, but all with an administration user.
2.5.2.2 (42)	Description of what UI looks like, the available menu items.	Yes	Demonstrated and tested, not verified if each button is present in the right situation.
2.5.2.3 (45)	Relevant changes to the data are logged.	Yes	Demonstrated.
2.5.2.4 (45)	Process description of manual input of election results. • No concurrent input during manual entry. • Entered data is checked for plausibility. • After data is entered, edits are only stored if data passes plausibility check. • Manual data needs to be entered twice.	To be determined	Demonstrated and tested, except for the restriction that no concurrent input is possible during manual entry.
2.5.2.5 (50)	Process description of input of election results by EML file. • Validity of input file is verified by hash code. The user has to enter (part of) a hash code provided together with the EML file.	Yes	Demonstrated and tested.
2.5.2.6 (51)	A status bar shows the cur-	Yes	Observed during demonstra-

© 2009 Software Improvement Group

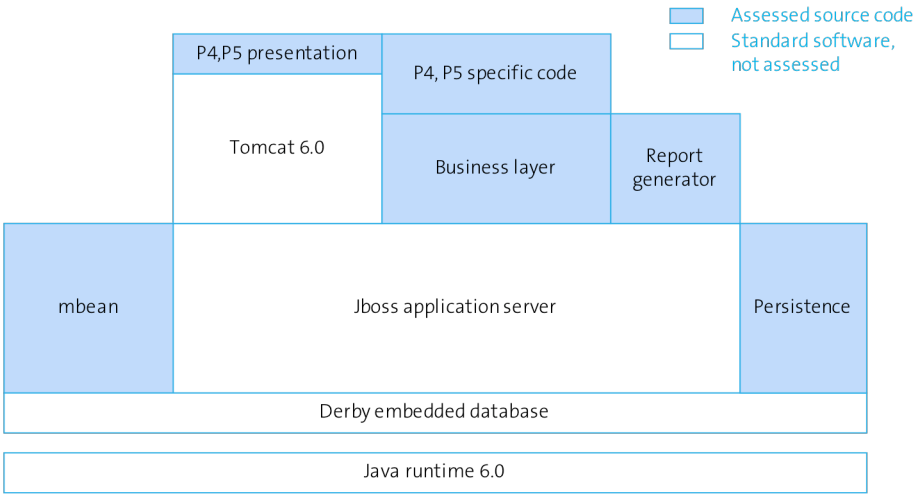
	rent state of data entry.		tion
2.5.2.7 (52)	Administrators can add, edit and delete polling stations for a municipality.	Yes	Demonstrated.
2.5.2.8 (52)	The file with voting lists and candidates can be uploaded by an administrator.	Yes	Demonstrated and tested.
2.5.2.9 (52)	Results can be exported (in EML, PDF and/or RTF). Detailed specifications of the various subtypes of EML exported and form names for the PDF/RTF documents.	Yes	Demonstrated and tested. Not checked if the documents are of the specified types.
2.5.3 (54)	Inline help functionality is present.	To be determined	Not observed during demonstration or testing.
2.6 (55)	An adapted version of the P4 for use in referenda. Use is similar to normal P4, P1 through P3 are not used because there is no list of candidates. Most relevant difference is that it is possible to create a referendum definition from the application.	To be determined for next report	Not demonstrated or tested. This functionality is only needed in the last version for other elections, and not for the European elections.

A.4 Eis 3: ontwerp

A.4.1 Architectuur

De architectuur van het programma is weergegeven in onderstaande figuur. Voor de blauw gearceerde modules in dit ontwerp is er broncode beschikbaar. De witte blokken zijn standaardpakketten die geen onderdeel uitmaken van de broncode van OSV 4 en 5.

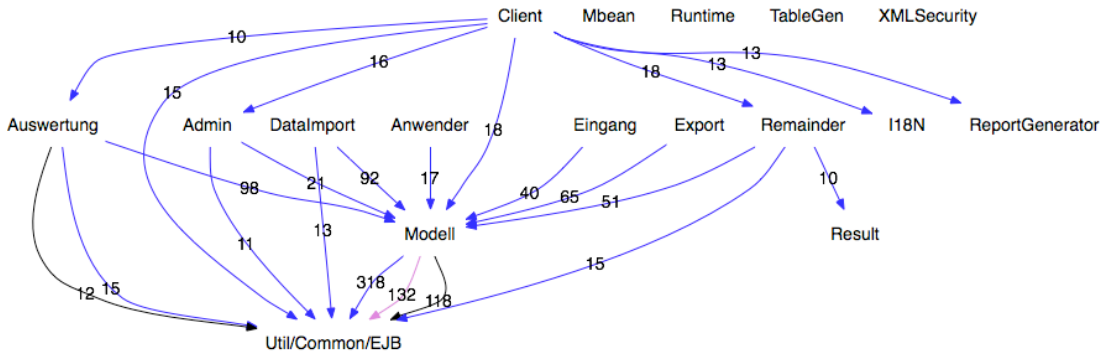
© 2009 Software Improvement Group



Figuur 2: Architectuur van OSV 4 en 5.

A.4.2 Afhankelijkheden tussen modules

Door middel van broncode-analyse is vastgesteld wat de afhankelijkheden tussen deze modules zijn. Hiervoor is bepaald hoe vaak de code in een bepaalde module een aanroep doet van een code-eenheid in een andere module. Dit is weergeven in Figuur 3.



Figuur 3: De module-structuur van OSV 4 en 5. De pijlen geven aanroepen vanuit de ene module naar de andere aan, met daarbij het aantal aanroepen. Pijlen met minder dan 8 aanroepen zijn weggelaten. Uit deze figuur blijkt dat er geen grote cyclische afhankelijkheden zijn.

In totaal is er op twaalf plaatsen in de code een afhankelijkheid vastgesteld die ingaat tegen de architectuur. Dit is een zeer klein aantal afhankelijkheden, en de broncode is daardoor bovengemiddeld op het gebied van modulestructuur.

A.4.3 Lijst van plausibility checks

Bijgevoegd is de lijst van testen die het programma doet om verkeerd gebruik van de programmatuur te voorkomen. In de technische sessie is gedemonstreerd hoe hiermee voorkomen wordt dat er verkeerde informatie ingevoerd wordt.

© 2009 Software Improvement Group

Topic	Error	Warning
In all fields: no negative value allowed	x	
In all fields: only numbers allowed (no characters)	x	
Amount of people entitled to vote may not be 0	x	
Amount of people entitled to vote may not be 9999999999 or larger.	x	
Sum of blanc, invalid and valid votes must be equal to the total number of votes, error when larger or smaller.	x	
Sum of blank votes may not be larger than the total number of votes.	x	
Amount of blank votes may not be too high (according to defined threshold value)		x
Amount of invalid votes may not be too high (according to defined threshold value)		x
Sum of all votes (distributed over political parties) must be equal to the total amount of valid votes (error when larger or smaller number)	x	
Sum of votes for one political party must be equal to the votes distributed over the candidates for this party (error when smaller or larger)	x	
Second input: whenever a value is entered, that differs from the first input, an error appears.	x	

A.5 Eis 5: verschillende besturingssystemen

In de in Figuur 2 weergegeven architectuur is te zien dat de programmatuur gebaseerd is op het JBoss-platform dat weer gebaseerd is op het Java-platform.

A.6 Eis 6: diakritische tekens

In het logisch ontwerp versie 3.6 van het GBA wordt ook gesproken over het mogelijke gebruik van Unicode voor het weergeven van de voor het GBA gebruikte diakritische tekens.

> *Bij de uitwisseling van gegevens gebruikt de LRD Unicode en niet de manier van coderen die is beschreven in Bijlage II Teletex. Unicode wordt gebruikt omdat de LRD met behulp van webtechnologie wordt bevraagd en het gebruik van Unicode in de webomgeving gebruikelijk (p.633).*

© 2009 Software Improvement Group

Tijdens de technische sessie heeft IVU de weergave van verschillende accenten gedemonstreerd.

A.7 Eis 7: authenticiteit programmatuur

Tijdens de technische sessie is de volgende procedure voor controle van authenticiteit van de programmatuur uitgelegd en deze is door de SIG uitgevoerd:

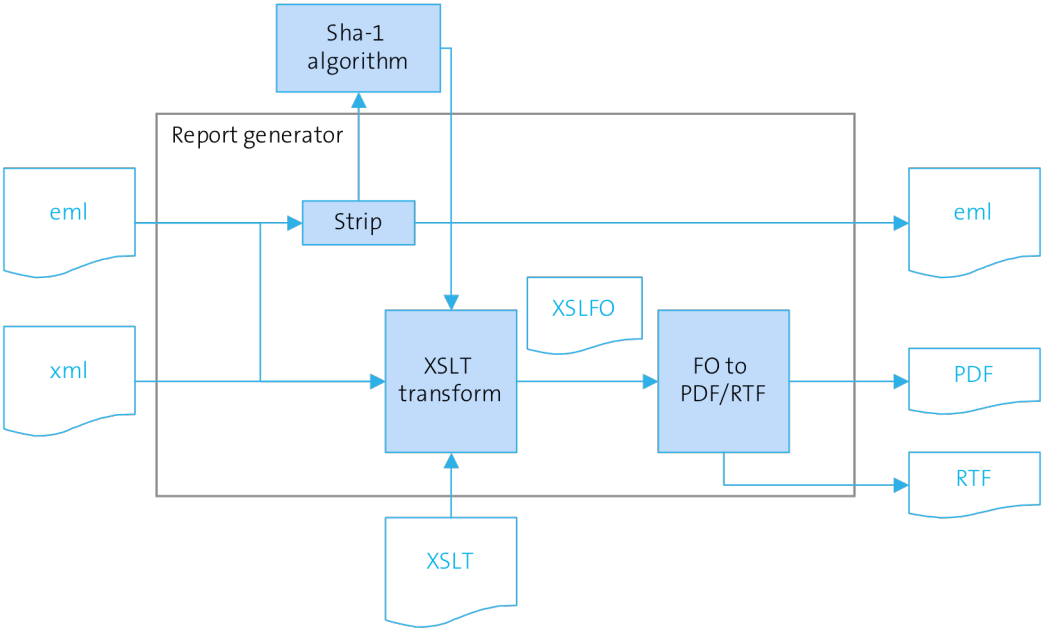
- De aanleverende partij berekent een hashcode (digitale vingerafdruk) en geeft deze door per brief aan de gebruiker van de programmatuur
- De gebruiker ontvangt de installatiebestanden elektronisch.
- De gebruiker berekent de hashcode over deze bestanden met behulp van reeds aanwezige programmatuur.
- De gebruiker vergelijkt deze hashcode met de in brief gegeven hashcode. Als deze gelijk is, zijn de installatiebestanden authentiek

A.8 Eis 8: authenticiteit gegevens

Om de authenticiteit van gegevens die de programmatuur produceert te kunnen controleren, is gekozen voor controle van authenticiteit door middel van een hashcode (digitale vingerafdruk) in een begeleidend afgedrukt document. De module die hiervoor verantwoordelijk is is de report generator. De werking hiervan is weergeven in Figuur 4. De stappen van de controle zijn de volgende:

- Vanuit de programmatuur wordt een EML bestand met stemgegevens aan de report generator gestuurd.
- De report generator verwijdert niet-essentiële informatie (‘strippen’) en slaat de gestripte EML op en stuurt deze bovendien naar het SHA-1 algoritme
- De XSLT transformator ontvangt ook het oorspronkelijke EML bestand, en maakt hier een afdrukbaar document van, dat bovendien de door het SHA-1 algoritme berekende hashcode bevat.
- Het afdrukbare document wordt opgeslagen in PDF of RTF
- De gebruiker zet het EML bestand op een informatiedrager (bijvoorbeeld cd of USB-stick) en drukt het afdrukbare document af
- Een andere gebruiker ontvangt zowel de informatiedrager als het afgedrukte document
- Deze gebruiker vraagt het programma om het EML bestand in te laden
- De programmatuur vraagt de gebruiker om de hashcode te controleren en aan te vullen. De gebruiker is verplicht om de eerste 4 tekens van de hashcode in te voeren, en kan dus niet verder zonder het afgedrukte document

© 2009 Software Improvement Group



Figuur 4: Werking van de report generator. Aan de linkerkant komt uit te voeren informatie vanuit de programmatuur binnen. Verkiezingsdata is hierbij weergegeven in EML. Deze wordt rechts uitgevoerd in gestripte vorm. Tegelijkertijd wordt een begeleidend afdrukbaar document (PDF of RTF) gemaakt dat de hashcode van dit bestand bevat.

© 2009 Software Improvement Group

B. Disclaimer

Alle conclusies in dit rapport zijn gebaseerd op een *best effort* analyse. De analyse is in een beperkte tijd uitgevoerd. De Software Improvement Group kan niet garanderen dat de interpretatie van de bevindingen in dit rapport foutloos is. Het is mogelijk dat verdere gesprekken met de onderhoudsmedewerkers van de systemen alsmede een verdere analyse van de broncode, tot een andere interpretatie van de bevindingen dan die in dit rapport is beschreven kunnen leiden.

© 2009 Software Improvement Group