Toetsing Ondersteunende Software Verkiezingen (OSV)

sqs.com

Definitieve rapportage



De Ondersteunende Software Verkiezingen is beoordeeld op de volgende twee aspecten:

- de mate waarin de software voldoet aan de opgestelde specificatie voor de berekening van de uitslag en zetelverdeling;
- de mate waarin de software voldoet aan de eisen die aan de software worden gesteld volgens de bijlage bij art. 2a van de Kies- en referendumregeling.

Dit rapport beschrijft het resultaat van de toetsing, die is uitgevoerd in de periode van december 2017 tot en met januari 2018.

SQS Nederland

Orteliuslaan 889, 3528 BE Utrecht

Telefoon: +31 88 655 88 80
Fax: +31 88 655 88 89
E-mail: info-nl@sqs.com
Website: www.sqs.com/nl

Managementsamenvatting

Op verzoek van de Kiesraad is de Ondersteunende Software Verkiezingen (OSV) beoordeeld op de volgende twee aspecten:

- de mate waarin de software voldoet aan de opgestelde specificatie voor de berekening van de uitslag en zetelverdeling;
- de mate waarin de software voldoet aan de eisen die aan de software worden gesteld volgens de bijlage bij art. 2a van de Kies- en referendumregeling.

Beoordeling

Op hoofdlijnen voldoen de programma's P4 en P5 van OSV aan de daaraan gestelde eisen. Bij het testen van de functionaliteit voor de berekening van de verkiezingsuitslag en de bijbehorende zetelverdeling zijn we geen onvolkomenheden tegengekomen.

Bij drie van de dertien gestelde eisen zien we verbetermogelijkheden:

- *Eis 5, de mate waarin technische mogelijkheden ter voorkoming van foutief gebruik worden uitgenut:* OSV gebruikt verouderde en/of niet meer ondersteunde softwarecomponenten zoals de gebruikte versies van Java en Jboss. Dit levert een beveiligingsrisico. De Kiesraad heeft organisatorische maatregelen genomen om dit technisch risico te mitigeren.
- *Eis 2, de mate waarin modulaire aanpassingen kunnen worden doorgevoerd:* De gelaagde structuur en de heldere componentindeling die beschreven worden in de architectuurbeschrijving, zijn onvoldoende terug te vinden in de structuur van de software.
- *Eis 3, de mate waarin kritische functies traceerbaar zijn in de code:* Voor de percentageberekeningen bij de referendumuitslag is in de code niet te volgen hoe het resultaat tot stand komt. Dit komt doordat het documenterend commentaar daartoe ontoereikend is.

Aanbevelingen

Als belangrijkste technische maatregel om verder foutief gebruik van OSV te voorkomen adviseren we om te onderzoeken of en hoe versies van gebruikte softwarecomponenten geactualiseerd kunnen worden. Dit verkleint de kans op misbruik van beveiligingslekken in deze componenten.

Pas de modulaire structuur van OSV aan zodat deze beter aansluit bij de gelaagde architectuur zoals beschreven in de architectuurbeschrijving. Documenteer de afwijkingen in de relatie tussen de beschreven softwarearchitectuur en de modulaire structuur van de software. Met deze maatregelen kan beheer en onderhoud van OSV efficiënter worden doorgevoerd.

We adviseren de traceerbaarheid van de code van kritische functies (zie 4.3) te verbeteren door in het codecommentaar helderder te beschrijven wat de betreffende methode doet, welke resultaten worden opgeleverd (post condities), wat de voorwaardes zijn waaraan de methode moet voldoen (pre condities), en hoe de berekeningen worden uitgevoerd.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond en vraagstelling

Bij het gebruik van software bij verkiezingen wordt een hoge mate van transparantie betracht. Met name waar het gaat om software die wordt gebruikt bij de vaststelling van de officiële uitslag en zetelverdeling. Het centraal stembureau dient de software door een onafhankelijke instantie te laten toetsen. Dit rapport vormt het resultaat van de toetsing die in december 2017 / januari 2018 is uitgevoerd.

Bij verkiezingen wordt gebruikgemaakt van Ondersteunende Software Verkiezingen — OSV. Specifiek voor het vaststellen van de uitslag en de zetelverdeling zijn respectievelijk programma's P4 en P5 van toepassing.

Op grond van het Kiesbesluit [2] en bijbehorende regelingen dient de toetsing van OSV op twee aspecten te worden uitgevoerd:

- de mate waarin de software voldoet aan de opgestelde specificatie voor de berekening van de uitslag en zetelverdeling;
- de mate waarin de software voldoet aan eisen die wet en regelgeving daaraan stelt.

Eind 2014 / begin 2015 hebben we voor het eerst een toetsing van OSV uitgevoerd (zie [19][1]) waarbij op dat moment nog geen mogelijkheid aanwezig was voor ondersteuning van een referendum. Begin 2016 is de toetsing van OSV specifiek voor de referendumsoftware uitgevoerd [20].

In voorbereiding van de gemeenteraadsverkiezingen van maart 2018 in combinatie met het referendum over de vernieuwde Wet op de inlichtingen- en veiligheidsdiensten, ook wel 'sleepwet', heeft de Kiesraad gevraagd om de toetsing opnieuw uit te voeren. De software is ondertussen op een aantal punten aangepast. De belangrijkste zijn:

- Aanbevelingen uit een beveiligingsonderzoek dat Fox-IT [22] heeft uitgevoerd zijn in de software geïmplementeerd. Onder andere is een algoritme dat gebruikt wordt voor hashing verbeterd van SHA-1 naar SHA-256.
- Lijstencombinaties worden niet meer toegestaan en daarmee is de ondersteuning daarvoor onmogelijk gemaakt.
- De huidige versie van OSV verplicht de gebruiker om gegevens twee keer in te voeren ter ondersteuning van het vierogen-principe.

De toetsing is uitgevoerd voor alle soorten verkiezingen inclusief het referendum, die op grond van de Kieswet worden gehouden. De scope van de toetsing is beperkt tot de programma's 4 en 5 van OSV, die worden gebruikt bij de vaststelling van de uitslag en zetelverdeling.

---

1. In 'Bijlage A: Bronmateriaal' is een lijst van documentatiemateriaal opgenomen. In de tekst wordt hiernaar verwezen met het nummer van de betreffende referentie tussen vierkante haken.

1.2 Toetskader

In het Kiesbesluit [2] is in artikel P 1 lid 4 en lid 6 over de software ter ondersteuning van verkiezingen opgenomen:

1. Het centraal stembureau laat de programmatuur, bedoeld in het eerste lid, door een onafhankelijke instantie toetsen en maakt de uitkomst van de toets uiterlijk op de dag van de kandidaatstelling openbaar.
6. De onafhankelijke instantie, bedoeld in het vierde lid, toetst of de programmatuur:
   a. voldoet aan de specificatie, bedoeld in het tweede lid;
   b. voldoet aan de eisen, die bij ministeriële regeling aan de programmatuur zijn gesteld.

In lid 2 van hetzelfde artikel is over de specificatie opgenomen:

2. Het centraal stembureau stelt voor de programmatuur een specificatie op van de voor de berekening van de uitslag van de verkiezingen of de berekening van de zetelverdeling geldende wet- en regelgeving. De specificatie maakt duidelijk op welke wijze in de programmatuur de wet- en regelgeving moet worden toegepast bij de berekening van de uitslag van de verkiezingen of de berekening van de zetelverdeling.

Als specificatiedocumenten heeft de Kiesraad voor deze toetsing de volgende documenten geleverd:

- *Determination of the Election Result*, Joachim Nottebaum, versie 6.1, 28-01-2014 [17].
- *Formele beschrijving van de berekening van de zetelverdeling*, 20-11-2017 [27].
- *Gedetailleerde Specificatie Ondersteunende Software Verkiezingen (OSV) Kiesraad*, versie 1.5.1, status: gecontroleerd, aangemaakt: 13-10-2008, laatste wijziging: 28-04-2017 [25].

In de Kies- en referendumregeling [5] zijn in Bijlage 2 de eisen opgenomen waaraan de programmatuur moet voldoen die door de centrale stembureaus wordt gebruikt voor de vaststelling van de uitslag van verkiezingen of de berekening van de zetelverdeling:

- *Functionaliteit*[2]*:* de programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit nodig zijn voor de berekening van de uitslag van de verkiezingen en de zetelverdeling;
- *Modulaire aanpassingen:* de programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn;
- *Kritische functies:* de kritische functies voor de berekening van de uitslag van de verkiezingen en de zetelverdeling zijn in de programmatuur herkenbaar en van elkaar gescheiden;
- *Soorten verkiezingen:* de programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen;
- *Voorkomen foutief gebruik:* toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen;
- *Diakritische tekens:* de programmatuur ondersteunt voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten in ieder geval de diakritische tekens van de tekenset die op grond van artikel 3, eerste lid, van het Besluit basisregistratie personen voor de basisregistratie personen is vastgesteld;
- *Open source en standaarden:* de programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de

[2]. We hebben labels aan de eisen toegevoegd zodat we aan de betreffende eis kunnen refereren.

doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor verkiezingsgegevens zoals kandidatenlijsten en zetelverdeling wordt de EML_NL standaard toegepast;
- *Vrij verkrijgbare standaard programmatuur:* de standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar;
- *Intellectueel eigendom:* het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau;
- *Open source compiler:* de programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is;
- *Verschillende besturingssystemen:* de programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem;
- *Authenticiteit programmatuur:* het is mogelijk de authenticiteit van de programmatuur vast te stellen; en
- *Authenticiteit aangeleverde gegevens:* bij het inlezen van verkiezingsgegevens in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.

In Bijlage 3 van de Kies- en referendumregeling [5] zijn in de eisen opgenomen waaraan de referendumprogrammatuur moet voldoen:
- *Functionaliteit:* de programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit juncto artikel 16 van het Besluit raadgevend referendum, nodig zijn voor de berekening van de uitslag van het referendum;
- *Modulaire aanpassingen:* de programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn;
- *Kritische functies:* de kritische functies voor de berekening van de uitslag van het referendum zijn in de programmatuur herkenbaar en van elkaar gescheiden;
- *Voorkomen foutief gebruik:* toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen;
- *Open source en standaarden:* de programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor referendumgegevens wordt de EML_NL standaard toegepast;
- *Vrij verkrijgbare standaard programmatuur:* de standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar;
- *Intellectueel eigendom:* het intellectueel eigendom van de maatwerkprogrammatuur berust bij het centraal stembureau;
- *Open source compiler:* de programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is;
- *Verschillende besturingssystemen:* de programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem;
- *Authenticiteit programmatuur:* het is mogelijk de authenticiteit van de programmatuur vast te stellen; en
- *Authenticiteit aangeleverde gegevens:* bij het inlezen van referendumgegevens in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.

Merk op dat bij de eisen voor het referendum geen eisen zijn opgenomen voor ‘Soorten verkiezingen’ en ‘Diakritische tekens’. De eisen voor ‘Functionaliteit’, ‘Kritische functies’, ‘Open source en standaarden’ en ‘Authenticiteit aangeleverde gegevens’ zijn toegesneden naar de specifieke omstandigheden van het referendum. De overige eisen zijn identiek geformuleerd.

1.3 Toetsuitvoering

Dit rapport is het resultaat van de toetsing van OSV, die is uitgevoerd in de periode van december 2017 tot en met januari 2018. De toets is uitgevoerd voor versie 2.21.1 die op 12 december 2017 is aangeleverd (zie ‘A.3 Programmatuur’).

Het onderzoek is uitgevoerd in opdracht van de Kiesraad. Ze heeft ons voorzien van de benodigde software en informatie om het onderzoek te kunnen uitvoeren. Een conceptversie van dit rapport is ter review aangeboden aan de opdrachtgever en tegelijkertijd aan de leverancier van de software. Reviewopmerkingen zijn in deze definitieve versie van het toetsingsrapport verwerkt.

OSV is ontwikkeld door IVU (IVU Traffic Technologies AG, zie: www.ivu.com) op basis van een reeds bestaand softwarepakket voor verkiezingen[3]. Onderhoud (correctief en adaptief) wordt door IVU uitgevoerd. De Nederlandse vertegenwoordiging van IVU treedt op als contactpersoon namens de leverancier voor dit onderzoek.

Voor programma 4 en 5 van OSV zijn de volgende modules beschouwd:

- `de.ivu.wahl.wus.electioncategory`
- `de.ivu.wahl.wus.loggerinterface`
- `de.ivu.wahl.wus.reportgenerator`
- `de.ivu.wahl.wus.util`
- `de.ivu.wahl.wus.xmlsecurity`
- `osv_alg`
- `osv45`

De uitvoering van de toets bestaat uit twee delen:

- *Toetsen specificaties:* Voor programma 5 van OSV zijn testgevallen ontwikkeld op basis van de specificatie-documenten voor elke stap uit de berekening van de zetelverdeling. Deze zijn zodanig vastgelegd dat deze herhaald uit te voeren zijn. De beschreven testen zijn uitgevoerd waarbij de resultaten in deze rapportage zijn vastgelegd. De dekkingsgraad van de uitgevoerde testen is geregistreerd.
- *Toetsen eisen:* We hebben beoordeeld in hoeverre programma’s 4 en 5 van OSV voldoen aan de eisen die in de bijlage van de Kies- en referendumregeling gesteld zijn. Bij eis 1 hebben de experts gebruikgemaakt van de resultaten van de testen die zijn uitgevoerd bij de hiervoor genoemde stap ‘Toetsen specificaties’.

[3]. Zie: www.ivu.com/products-solutions/ivuelect.html voor specifieke informatie van IVU over haar oplossing voor verkiezingssoftware.

1.4 Leeswijzer

Dit document is als volgt opgebouwd:

- *Hoofdstuk 2, Samenvattend resultaat en aanbevelingen:* Dit hoofdstuk bevat de samenvatting van ons oordeel op basis van de uitgevoerde testen aan de hand van de specificaties en het expertoordeel met betrekking tot de eisen waaraan de software volgens de Kies- en referendumregeling moet voldoen. Tevens doen we aanbevelingen voor verbetering.
- *Hoofdstuk 3, Functionele test OSV:* In dit hoofdstuk worden de testen beschreven die zijn uitgevoerd om te verifiëren of programma 5 van OSV de berekeningen conform specificaties uitvoert.
- *Hoofdstuk 4, Oordeel per eis:* Voor elke eis uit de bijlage van de Kies- en referendumregeling wordt in dit hoofdstuk beschreven wat onze bevindingen zijn die hebben geleid tot ons oordeel over de mate waarin OSV voldoet aan de betreffende eis.
- *Bijlages:* Hier vindt u een lijst van het gebruikte bronmateriaal (bijlage A) en de getoetste karakterset bij eis 6 (bijlage B). Bijlage C bevat informatie over de percentageberekeningen, die gebruikt is voor de beoordeling van de traceerbaarheid van deze kritische functies.

2 Samenvattend resultaat en aanbevelingen

Dit hoofdstuk bevat de samenvatting van ons oordeel en de daarop gebaseerde aanbevelingen voor verbetering. We beginnen met een samenvatting van het toetsoordeel in 2.1. De aanbevelingen worden beschreven in 2.2. Het oordeel is gebaseerd op de uitvoering van functionaliteitstesten voor de berekening van de verkiezingsuitslag (zie 2.3) en ons expertoordeel met betrekking tot de eisen waaraan de software volgens de Kies- en referendumregeling moet voldoen (2.4).

2.1 Samenvattend oordeel

Op hoofdlijnen voldoen de programma's P4 en P5 van OSV aan de daaraan gestelde eisen. Bij het testen van de functionaliteit voor de berekening van de verkiezingsuitslag en de bijbehorende zetelverdeling zijn we geen onvolkomenheden tegengekomen.

Bij drie van de dertien gestelde eisen zien we verbetermogelijkheden:

- *Voorkomen foutief gebruik (eis 5, zie 4.5):* Aanbevelingen uit het rapport van Fox-IT hebben geleid tot organisatorische en technische maatregelen die het risico op foutief gebruik verminderen. OSV gebruikt echter verouderde en/of niet meer ondersteunde softwarecomponenten zoals de gebruikte versies van Java en Jboss. Dit levert een beveiligingsrisico. De Kiesraad heeft organisatorische maatregelen genomen om dit technisch risico te mitigeren.
- *Modulaire aanpassingen (eis 2, zie 4.2):* De gelaagde structuur en de heldere componentindeling die beschreven worden in de architectuurbeschrijving, zijn onvoldoende terug te vinden in de structuur van de software. Voor het gebruik van OSV heeft dit geen directe gevolgen. Beheer en onderhoud worden daardoor negatief beïnvloed. Ontwikkelaars die de programmatuur niet goed kennen, zullen moeite hebben aanpassingen door te voeren.
- *Kritische functies (eis 3, zie 4.3):* Met de informatie van de leverancier zijn de methodes te vinden die de berekeningen voor de kritische functies realiseren. De methodes voor de verkiezingen en de zetelverdeling zijn te onderscheiden. Voor de percentageberekeningen bij de referendumuitslag is in de code niet te volgen hoe het resultaat tot stand komt.

Samenvattend is de mate waarin programma's 4 en 5 voldoen aan de eisen uit de Kies- en referendumregeling door ons als volgt beoordeeld.

Nr.	Onderwerp	Oordeel
1.	Functionaliteit	<OK>
2.	Modulaire aanpassingen	<KG>
3.	Kritische functies	<KG>
4.	Soorten verkiezingen	<OK>
5.	Voorkomen foutief gebruik	<KG>
6.	Diakritische tekens	<OK>
7.	Open source en standaarden	<OK>

Nr.	Onderwerp	Oordeel
8.	Vrij verkrijgbare standaard programmatuur	<OK>
9.	Intellectueel eigendom	<OK>
10.	Open source compiler	<OK>
11.	Verschillende besturingssystemen	<OK>
12.	Authenticiteit programmatuur	<OK>
13.	Authenticiteit aangeleverde gegevens	<OK>

Tabel 1: Mate waarin OSV voldoet aan de eisen uit de bijlage bij art. 2a van de Kies- en referendumregeling.

Bij de presentatie van het toetsresultaat maken we gebruik van codering en kleuren om aan te geven of aan een eis al dan niet wordt voldaan. Bij constatering van een gebrek geven we aan of het daarbij naar onze mening om een klein dan wel groot gebrek handelt. De betekenis van de codering en kleuren is als volgt:

Code	Omschrijving
<OK>	*Geen gebrek:* OSV voldoet aan de betreffende eis.
<KG>	*Klein gebrek:* alleen kleine gebreken zijn voor de betreffende eis geconstateerd; deze hebben nauwelijks effect bij gebruik, onderhoud en beheer van OSV.
<GG>	*Groot gebrek:* voor de betreffende eis zijn één of meerdere grote gebreken geconstateerd, die merkbaar impact hebben bij gebruik, onderhoud of beheer van OSV.

Tabel 2: Kleuren en codering toetsresultaat.

2.2 Aanbevelingen

Als belangrijkste technische maatregel om verder foutief gebruik van OSV (zie 4.5) te voorkomen adviseren we om te onderzoeken of en hoe versies van gebruikte softwarecomponenten geactualiseerd kunnen worden. Dit verkleint de kans op misbruik van beveiligingslekken in deze componenten. Met name Java en Jboss moeten bijgewerkt worden naar actuele versies. Voer daarom een scenarioanalyse uit. In die analyse moet de huidige status van OSV (het verwachte gebruik en de levensduur van de software) en de impact op de architectuur als belangrijke aspecten worden gewogen.

Pas de modulaire structuur van OSV aan (zie 4.2) zodat deze beter aansluit bij de gelaagde architectuur zoals beschreven in de architectuurbeschrijving [25]. Documenteer de afwijkingen in de relatie tussen de beschreven softwarearchitectuur en de modulaire structuur van de software. Met deze maatregelen moeten ontwikkelaars sneller kunnen vinden waar en hoe aanpassingen in de software te realiseren. Beheer en onderhoud van OSV kan dan efficiënter worden doorgevoerd.

We adviseren de traceerbaarheid van de code van kritische functies (zie 4.3) te verbeteren door in het codecommentaar helderder te beschrijven wat de betreffende methode doet, welke resultaten worden opgeleverd (post condities), wat de voorwaardes zijn waaraan de methode moet voldoen (pre condities), en hoe de berekeningen worden uitgevoerd.

2.3 Samenvattend testresultaat

Op basis van de door ons uitgevoerde testen (zie hoofdstuk 3) zijn geen onvolkomenheden gedetecteerd.

Het testresultaat is samengevat in de volgende tabel. Deze bevat voor elke stap uit de berekening van de zetelverdeling [27]:

- *Oordeel:* het eindresultaat van toetsing van de software voor de betreffende stap (met kleuren en codering),
- *Dekkingsgraad:* de mate waarin de uitgevoerde toetsen de functionaliteit van de betreffende stap afdekken.

Nr.	Stap	Oordeel	Dekkingsgraad
A.	**Zetelverdeling**		
1.	Vaststelling van de stemtotalen per partij en het totale aantal uitgebrachte stemmen; berekening van de kiesdeler	<OK>	100%
2.	Toedeling van zetels op basis van het behalen van de kiesdeler	<OK>	100%
3.	Toedeling van restzetels	<OK>	100%
4.	Wijziging van de zetelverdeling indien een lijst de volstrekte meerderheid van stemmen behaalt	<OK>	95%
5.	Wijziging van de zetelverdeling in geval van uitputting van lijsten	<OK>	100%
6.	Verdeling van zetels binnen lijstengroepen	<OK>	100%
B.	**Aanwijzing van de gekozen kandidaten**		
1.	Aanwijzing van met voorkeurstemmen gekozen kandidaten	<OK>	100%
2.	Aanwijzing van de overige gekozen kandidaten	<OK>	100%
3.	Rangschikking van de kandidaten op de kandidatenlijsten	<OK>	100%

Tabel 3: Mate waarin OSV software voldoet aan specificaties voor berekening van de uitslag.

Het testen van de functionaliteit van het referendum is gebaseerd op de formele beschrijving voor het berekenen van de uitslag voor het referendum [21]. Op basis van die beschrijving is een achttal testgevallen opgezet, die het invoeren van de referendumverkiezing en de berekening en weergave van de referendumuitslag afdekken.

Om te bepalen of OSV (P4 en P5) voldoet aan de specificaties hebben we testen opgezet en uitgevoerd. Voor de gemeenteraadsverkiezingen is een tiental logische testgevallen opgesteld die de berekening van de verkiezingsuitslag en de zetelverdeling afdoende afdekt. Voor de regressietesten op de overige verkiezingssoorten zijn twee relevante testgevallen geselecteerd, die de basisfunctionaliteit van OSV afdekken.

De dekkingsgraad van stap A.4 is niet volledig. Een zeer uitzonderlijke situatie wordt niet door een van de testgevallen behandeld. Het betreft een zeer uitzonderlijke situatie waarbij een partij de absolute meerderheid behaalt en een eerder toegekende restzetel aan een andere partij op basis van loting teruggehaald moet worden.

Het uitvoeren van testen voor P4 en P5 van OSV is een arbeidsintensief en foutgevoelig proces. Het testen van verschillende verkiezingssoorten blijkt bijzonder lastig te zijn. OSV moet opnieuw geïnstalleerd worden en alle stappen voor het vastleggen van verkiezingsdefinitie en kieslijsten moeten opnieuw uitgevoerd worden. Het testen met anders samengestelde kieslijsten en te verdelen zetels is moeizaam doordat de verkiezingsdatabase opgeschoond of verwijderd moet worden. De aanwezige functionaliteit voor het schonen van de verkiezingsdatabases blijkt niet correct te werken.

Onze aanbeveling is om de interface van P4 en P5 uit te breiden zodat het testen efficiënter kan worden uitgevoerd.

2.4 Samenvattende beoordeling eisen

De volgende tabel bevat een samenvatting van onze motivatie voor de mate waarin programma 4 en 5 voldoet aan de eisen uit de Kies- en referendumregeling. Voor een uitwerking wordt verwezen naar de betreffende pagina van dit rapport.

Nr.	Eis	Oordeel	Motivatie	Pagina
1.	De programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit nodig zijn voor de berekening van de uitslag van *de verkiezingen en de zetelverdeling*. De programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit *juncto artikel 16 van het Besluit raadgevend referendum,* nodig zijn voor de berekening van de uitslag van *het referendum*.	<OK>	• We hebben geen onvolkomenheden gedetecteerd. • Dit oordeel is gebaseerd op het resultaat van de uitgevoerde testen zoals weergegeven in Tabel 3. Het testresultaat voor de referendumsoftware wordt behandeld in § 3.3.3.	23
2.	De programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn.	<KG>	• De architectuurbeschrijving belooft een gelaagde structuur en heldere componentindeling die grotendeels, maar niet volledig is terug te vinden in de broncode. • Voor de geboden functionaliteit heeft onvolledige structurering geen directe gevolgen zodat we dit als een klein gebrek waarderen. • Voor onderhoud heeft de onvolledige structurering negatieve gevolgen. Ontwikkelaars zullen moeite hebben te vinden waar welke functionaliteit gerealiseerd is.	23
3.	De kritische functies voor de berekening van de uitslag van *de verkiezingen en de zetelverdeling* zijn in de programmatuur herkenbaar en gescheiden. De kritische functies voor de berekening van de uitslag van *het referendum* zijn in de programmatuur herkenbaar en van elkaar gescheiden.	<KG>	• Met de informatie van de leverancier zijn de methodes te vinden die de berekeningen voor de kritische functies realiseren. • De callgraph van de methodes voor de verkiezingen en de zetelverdeling laat zien dat er geen afhankelijkheden zijn tussen beide berekeningen. • Voor de percentageberekeningen bij de referendumuitslag is in de code niet te volgen hoe het resultaat tot stand komt.	28
4.	De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen. *Deze eis is niet van toepassing op de referendumsoftware.*	<OK>	• Als een nieuwe verkiezingssoort vergelijkbaar is met bestaande soorten, kan door invulling van de parameters en hergebruik van de bestaande algoritmes snel de benodigde programmatuur gerealiseerd worden. • Als de bestaande algoritmes ontoereikend zijn, is onoverkoombaar dat aanpassingen meer werk kosten.	30

Nr.	Eis	Oordeel	Motivatie	Pagina
5.	Toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen.	<KG>	• Aanbevelingen uit het rapport van Fox-IT hebben geleid tot organisatorische en technische maatregelen die het risico op foutief gebruik verminderen. • OSV gebruikt verouderde en/of niet meer ondersteunde softwarecomponenten zoals de gebruikte versies van Java en Jboss. Dit levert een beveiligingsrisico. • De Kiesraad heeft organisatorische maatregelen genomen om dit technisch risico te mitigeren.	30
6.	De programmatuur ondersteunt voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten in ieder geval de diakritische tekens van de tekenset die op grond van artikel 3, eerste lid, van het Besluit basisregistratie personen voor de basisregistratie personen is vastgesteld. *Deze eis is niet van toepassing op de referendumsoftware.*	<OK>	• Diakritische tekens van de GBA-tekenset worden door de programmatuur correct verwerkt.	31
7.	De programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor *verkiezingsgegevens zoals kandidatenlijsten en zetelverdeling* wordt de EML_NL standaard toegepast. De programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor *referendumgegevens* wordt de EML_NL standaard toegepast	<OK>	• De broncode van OSV wordt door de Kiesraad via haar website vrij beschikbaar gesteld en is daarmee ‘open source’. • Voor de gegevensuitwisseling wordt gebruikgemaakt van de EML_NL standaard. • Voor uitvoer wordt gebruikgemaakt van PDF (open standaard), RTF (de facto), CSV (de facto) en EML-NL (open).	32
8.	De standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar.	<OK>	• Het merendeel van de tools, die worden toegepast bij de ontwikkeling van OSV (Eclipse, JBoss Application Server, Apache en XOM), zijn vrij verkrijgbaar. • Alleen voor Altova Stylevision moet betaald worden. Dit tool is niet bedrijfskritisch voor realisatie van OSV.	34
9.	Het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau.	<OK>	• In juli 2015 is een overeenkomst afgesloten waarbij intellectueel eigendom is vastgelegd op basis van ARBIT-2014.	35
10.	De programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is.	<OK>	• Voor Java zijn diverse open source compilers beschikbaar. • De leverancier maakt gebruik van de incrementele ontwikkelomgeving (IDE) van Eclipse, die beschikbaar is vanaf de website: www.eclipse.org.	35
11.	De programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem.	<OK>	• OSV is ontwikkeld voor verschillende besturingssystemen: Windows/Linux en Mac OS. • Linux is een open source besturingssysteem.	36
12.	Het is mogelijk de authenticiteit van de programmatuur vast te stellen.	<OK>	• De authenticiteit van de programmatuur kan voorafgaand aan de installatie worden vastgesteld. • De controle op authenticiteit van de programmatuur wordt geadviseerd, maar niet afgedwongen. • Run-time wordt de authenticiteit niet geverifieerd.	36

Nr.	Eis	Oordeel	Motivatie	Pagina
13.	Bij het inlezen van *verkiezingsgegevens* in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening. Bij het inlezen van *referendumgegevens* in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.	<OK>	• Maatregelen zijn genomen om de authenticiteit van uitgewisselde gegevens beter vast te stellen. • Twee van de drie gebruikte beveiligingsniveaus laten de mogelijkheid toe dat de authenticiteit van ingelezen gegevens niet altijd wordt vastgesteld. • Door organisatorische maatregelen en technische verbeteringen is het risico op misbruik uitermate klein geworden.	37

Tabel 4: Motivering van de mate waarin OSV voldoet aan de eisen uit de bijlage bij art. 2a van de Kies- en referendumregeling.

3 Functionele test OSV

In dit hoofdstuk wordt eerst de testbasis van de uitgevoerde testen vastgelegd in 3.1. Daarna volgt de testaanpak in 3.2. Het resultaat van de testen is in 3.3 weergegeven.

3.1 Testbasis voor de testen

Voor de uitgevoerde testen is de volgende testbasis gehanteerd:

Testdoel	Document	Pagina
Referendum	De formele beschrijving voor het berekenen van de uitslag voor het referendum [21].	gehele document
Gemeenteraden met minder dan 19 zetels	Formele beschrijving van de berekening van de zetelverdeling [27].	22 t/m 25
Gemeenteraden met 19 of meer zetels	Formele beschrijving van de berekening van de zetelverdeling [27].	18 t/m 21
Regressietest op overige verkiezingssoorten	Formele beschrijving van de berekening van de zetelverdeling [27]. Mathematische uitwerking van de algoritmes voor bepaling van het kiesresultaat [17].	gehele document 22

Tabel 5: Voor de testen gehanteerde testbasis.

3.2 Testaanpak

Voor alle testen geldt, dat voor het testen gebruik is gemaakt van de invoer op twee stembureaus in één gemeente. Daarmee wordt het verwerken van resultaten over meerdere bureaus afdoende getest. Omdat er geen wijzigingen zijn geweest in de software voor het gebruik op hoofdstembureaus (HSB) en het centraal stembureau (CSB), is het niet noodzakelijk over meerdere HSB's invoer te gebruiken.

3.2.1 Gemeenteraden

Voor het testen van de software voor de verkiezing van zowel de gemeenteraden met minder dan 19 zetels (GR1) als gemeenteraden met 19 of meer zetels (GR2) zijn op basis van de testbasis tien logische testgevallen opgesteld, waarmee het berekenen van de juiste uitslag en de weergave hiervan op de processen-verbaal afdoende wordt afgedekt. In de uitvoering worden fysieke testgevallen gemaakt met daarin het aantal te verdelen zetels, waardoor de uitkomst van de zetelverdeling specifiek wordt voor GR1 en GR2.

De testgevallen zijn als volgt opgezet:

Nr.	Titel	Omschrijving
GRx.1	Basistest zonder restzetels	Eenvoudige test waarmee de basiswerking van de software zonder verdeling van restzetels wordt aangetoond.
GRx.2	Basistest met restzetels	Eenvoudige test, waarbij aanvullend op GRx.1 ook een restzetel moet worden verdeeld.
GRx.3	Controle volstrekte meerderheid	Testgeval met een partij die de volstrekte meerderheid haalt.
GRx.4	Restzetel na loting	1. Testgeval waarbij loting nodig is voor het toewijzen van de laatste restzetel. 2. Testgeval waarbij twee restzetels verdeeld moeten worden en loting nodig is voor het toewijzen van de laatste restzetel.
GRx.5	Uitputting van lijsten	Testgeval in geval van uitputting van een lijst.
GRx.6	Voorkeursstemmen	Testgeval voor het toewijzen van zetels aan kandidaten met voldoende voorkeursstemmen.
GRx.7	Controle afronding voorkeurdrempel	In deze testcase controleren we of de kiesdeler niet wordt afgerond.
GRx.8	Voorkeurskandidaat middels loting	In deze testcase beschrijven we het geval dat een tweetal kandidaten van eenzelfde partij hetzelfde aantal voorkeursstemmen behaalt. Daarna volgt toedeling middels loting.
GRx.9	Complexe test	Complex testgeval om consequentie- en stapelingsfouten in de software uit te sluiten

Tabel 6: Logische testgevallen Gemeenteraden met minder dan 19 zetels.

In de tabel zijn de testgevallen aangeduid met GRx. In de verdere rapportage worden de testen voor gemeenteraden met minder dan 19 zetels aangeduid met GR1, en die voor gemeenteraden met 19 of meer zetels met GR2.

3.2.2 Referendum

Voor het testen van de referendumsoftware is op basis van de testbasis een achttal testgevallen opgesteld waarmee het berekenen van de juiste uitslag en de weergave hiervan op de processen-verbaal afdoende wordt afgedekt.

De testgevallen zijn als volgt opgezet:

Nr.	Titel	Omschrijving
Ref.1	Alleen voorstemmers	Testgeval waarbij er alleen voorstemmers voor de referendumvraag zijn.
Ref.2	Alleen tegenstemmers	Testgeval waarbij er alleen tegenstemmers voor de referendumvraag zijn.
Ref.3	Alleen blanco-stemmers	Testgeval waarbij er alleen blanco-stemmers voor de referendumvraag zijn.
Ref.4	Gelijk aantal voor en tegen	Testgeval met een exact gelijk aantal voor- en tegenstemmers.
Ref.5	Geen ongeldig en volmacht	Testgeval zonder ongeldige en volmachtstemmers, maar wel voor-, tegen- en blanco-stemmers.

Nr.	Titel	Omschrijving
Ref.6	Wel ongeldig en volmacht	Testgeval met voor-, tegen- en blanco-stemmers, inclusief ongeldige en volmachtstemmers. Dit testgeval bevat lage aantallen.
Ref.7	Grens 30%	Testgeval waarmee de weergave van de percentages voor het voorkomen van afrondingsproblemen wordt getest. In deze test is gekozen voor het weergeven van een percentage net onder de 30%.
Ref.8	Reële getallen	Testgeval met reële, grote getallen.

Tabel 7: Logische testgevallen Referendum.

3.2.3 Regressietesten

De berekening voor de zetelverdeling bij verkiezingen is afhankelijk van de verkiezingssoort [27]. De volgende soorten zijn van toepassing:

- Tweede Kamer
- Provinciale staten in provincies met meer dan één kieskring
- Provinciale staten in provincies met één kieskring, algemeen besturen en gemeenteraden met 19 of meer raadszetels
- Gemeenteraden, algemeen besturen en eilandsraden met minder dan 19 raadszetels
- Europees Parlement
- Eerste Kamer

De berekeningen voor

- Provinciale staten in provincies met één kieskring, algemeen besturen met 19 of meer raadszetels
- Algemeen besturen en eilandsraden met minder dan 19 raadszetels

worden afgedekt door de testgevallen voor gemeenteraden (zie § 3.2.1)

Voor de verkiezingssoorten Tweede Kamer (TK), Provinciale staten in provincies met meer dan één kieskring (PS2), Europees Parlement (EP) en Eerste Kamer (EK), zijn regressietesten uitgevoerd. Voor deze test zijn op basis van de tabel op pagina 22 van de testbasis (zie Figuur 1) passende testgevallen uit de beschikbare testen gebruikt. Er is vastgesteld dat de testgevallen GRx.4(2) en GRx.6 voldoende zijn om de belangrijkste basisfunctionaliteit af te dekken. Zie daarvoor ook de weergegeven afdekking van de eisen in § 3.3.1 of 3.3.2.

Criteria ε :=	EP	EK	TK	PS2	PS1/ GR2	GR1/ ER
	1	6	2	3	4	5
Multiple electoral districts	yes	yes	yes	yes	no	no
Different nomination in different electoral districts	no	yes	yes	yes	no	no
Method for distribution of residual seats amongst combined lists etc. (LA = largest average, LR = largest remainder)	LA	LA	LA	LA	LA	1. LR 2. LA
Minimum for taking part in residual seat distribution (KT = electoral quota)	KT		KT			
Minimum for taking part in residual seat distribution by largest remainder						75% of KT
Fictitious seat distribution for checking validity of combined lists needed	no	no	no	yes	yes	yes
Restriction to one seat by largest average						yes
Preferential barrier (*) For EK elections, the number of votes must **reach**, while for all other elections the number of votes must **exceed** the given percentage of the electoral quota for a candidate to receive a priority seat.	10%	100% (*)	25%	25%	25%	50%
Absolute majority regulation in seat distribution amongst P42-lists	yes	no	yes	yes	yes	yes
Vote values		yes				

Figuur 1: Basis van de algoritmes voor de overige verkiezingssoorten, overgenomen uit [17].

3.3 Testresultaten

In de onderstaande paragrafen zijn de resultaten na testuitvoering per testgeval weergegeven. Daarbij zijn voor de weergegeven logische testgevallen in sommige situaties meerdere fysieke testgevallen gemaakt en uitgevoerd. Daarmee wordt de zekerheid over de juiste functionele werking verhoogd. Deze extra testgevallen zijn niet in de tabellen weergegeven, omdat ze geen toegevoegde waarde hebben op de gevraagde testdekking.

3.3.1 Gemeenteraden met minder dan 19 zetels

In onderstaande tabel is de dekking van de eisen en de testresultaten per testgeval weergegeven voor gemeenteraadsverkiezingen in gemeentes met minder dan 19 raadszetels.

		GR1.1	GR1.2	GR1.3	GR1.4(1)	GR1.4(2)	GR1.5	GR1.6	GR1.7	GR1.8	GR1.9
A	**Zetelverdeling**										
1	Vaststelling stemtotalen en kiesdeler	√	√	√	√	√	√	√	√	√	√
2	Directe toedeling van zetels	√	√	√	√	√	√				√
3	Toedeling van restzetels		√	√	√	√	√				√
4	Wijziging bij volstrekte meerderheid			√							
5	Wijziging bij uitputting lijsten						√				√
6	Verdeling binnen lijstengroepen										√

		GR1.1	GR1.2	GR1.3	GR1.4(1)	GR1.4(2)	GR1.5	GR1.6	GR1.7	GR1.8	GR1.9
B	**Aanwijzing van de gekozen kandidaten**										
1	Aanwijzing met voorkeurstemmen							√	√	√	√
2	Aanwijzing overige kandidaten							√	√		√
3	Rangschikking kandidaten							√	√		√
Resultaat		<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>

Tabel 8: Afdekking van de eisen en testresultaten Gemeenteraden met minder dan 19 zetels.

De dekkingsgraad van stap A.4 is niet volledig. De omschrijving voor A.4 [27] stelt in stap 4: “Waren er meer lijsten waaraan voor hetzelfde gemiddelde of overschot als van de in stap 3 bedoelde lijst een restzetel is toegewezen, dan wordt bij loting in de zitting van het centraal stembureau bepaald van welke lijst het zetelaantal met 1 wordt verminderd.” Dit geval treedt alleen op als er een partij is met de volstrekte meerderheid van stemmen waaraan niet de volstrekte meerderheid van zetels is toegewezen. De laatste restzetel die is toegewezen aan een andere lijst moet nu alsnog worden toegewezen aan de lijst die de volstrekte meerderheid heeft behaald. Loting wordt toegepast als er meerdere partijen waren waaraan onder dezelfde omstandigheden een zetel was toegewezen. Omdat de kans dat dit optreedt uitermate miniem is, is voor deze zeer uitzonderlijke situatie geen separaat testgeval gemaakt.

In de testen zijn geen bevindingen gedaan.

3.3.2 Gemeenteraden met 19 of meer zetels

In onderstaande tabel is de dekking van de eisen en de testresultaten per testgeval weergegeven voor gemeenteraadsverkiezingen waarbij 19 of meer zetels verdeeld worden.

		GR2.1	GR2.2	GR2.3	GR2.4(1)	GR2.4(2)	GR2.5	GR2.6	GR2.7	GR2.8	GR2.9
A	**Zetelverdeling**										
1	Vaststelling stemtotalen en kiesdeler	√	√	√	√	√	√	√	√	√	√
2	Directe toedeling van zetels	√	√	√	√	√	√				√
3	Toedeling van restzetels		√	√	√	√	√				√
4	Wijziging bij volstrekte meerderheid			√							
5	Wijziging bij uitputting lijsten						√				√
6	Verdeling binnen lijstengroepen										√
B	**Aanwijzing van de gekozen kandidaten**										
1	Aanwijzing met voorkeurstemmen							√	√	√	√
2	Aanwijzing overige kandidaten							√	√		√

	GR2.1	GR2.2	GR2.3	GR2.4(1)	GR2.4(2)	GR2.5	GR2.6	GR2.7	GR2.8	GR2.9
3 Rangschikking kandidaten							√	√		√
Resultaat	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>	<OK>

Tabel 9: Afdekking van de eisen en testresultaten Gemeenteraden met minder dan 19 zetels.

In de testen zijn geen bevindingen gedaan.

3.3.3 Referendum

Nr.	Titel	Resultaat
Ref.1	Alleen voorstemmers	<OK>
Ref.2	Alleen tegenstemmers	<OK>
Ref.3	Alleen blanco-stemmers	<OK>
Ref.4	Gelijk aantal voor en tegen	<OK>
Ref.5	Geen ongeldig en volmacht	<OK>
Ref.6	Wel ongeldig en volmacht	<OK>
Ref.7	Grens 30%	<OK>
Ref.8	Reële getallen	<OK>

Tabel 10: Testresultaten Referendum.

Er zijn geen bevindingen gedaan in de testen. De testen dekken de volledige beschrijving in de testbasis (zie § 3.1) af.

3.3.4 Regressietesten

In onderstaande tabel zijn testresultaten voor de overige vier verkiezingssoorten weergegeven.

Verkiezingssoort	Nr.	Testgeval	Resultaat
Tweede Kamer	TK.4(2)	Restzetel na loting, waarbij twee restzetels verdeeld moeten worden en loting nodig is voor het toewijzen van de laatste restzetel.	<OK>
	TK.6	Voorkeursstemmen	<OK>
Provinciale staten in provincies met meer dan één kieskring	PS2.4(2)	Restzetel na loting, waarbij twee restzetels verdeeld moeten worden en loting nodig is voor het toewijzen van de laatste restzetel.	<OK>
	PS2.6	Voorkeursstemmen	<OK>
Europees Parlement	EP.4(2)	Restzetel na loting, waarbij twee restzetels verdeeld moeten worden en loting nodig is voor het toewijzen van de laatste restzetel.	<OK>
	PS2.6	Voorkeursstemmen	<OK>

Verkiezingssoort	Nr.	Testgeval	Resultaat
Eerste Kamer	EK.4(2)	Restzetel na loting, waarbij twee restzetels verdeeld moeten worden en loting nodig is voor het toewijzen van de laatste restzetel.	<OK>
	EK.6	Voorkeursstemmen	<OK>

Tabel 11: Testresultaten regressietesten TK, PS2, EP en EK.

In de testen zijn geen bevindingen gedaan.

4 Oordeel per eis

In dit hoofdstuk wordt voor elk van de eisen die in de Kies- en referendumregeling [5] gesteld worden, besproken in hoeverre de programmatuur voldoet aan de betreffende eis en wat ons oordeel is.

We hanteren de indeling en volgorde van de dertien eisen zoals die geformuleerd zijn voor de berekening van de verkiezingsuitslag en de zetelverdeling. De elf eisen voor de referendumsoftware worden bij de overeenkomstige eis voor verkiezingssoftware behandeld. Bij de twee eisen (nummers 4 en 6) die niet van toepassing zijn op de referendumsoftware is dat expliciet aangegeven. Bevindingen zijn van toepassing op verkiezingssoftware en referendumsoftware. Daar waar dit niet het geval is, wordt dit specifiek aangegeven.

Elke paragraaf begint met de formele tekst van de gestelde eis. Daar waar van toepassing zijn beide eisen (zowel voor de verkiezingen als voor referenda) opgenomen waarbij tekstuele verschillen dik gedrukt zijn.

4.1 Functionaliteit

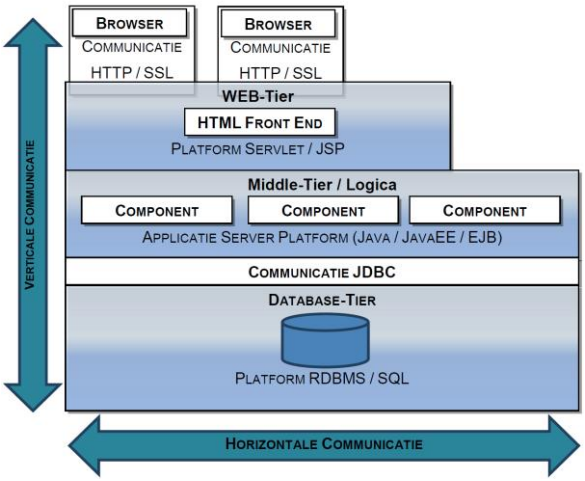
1. *De programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit nodig zijn voor de berekening van de uitslag van **de verkiezingen en de zetelverdeling**.*
1. *De programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit **juncto artikel 16 van het Besluit raadgevend referendum,** nodig zijn voor de berekening van de uitslag van **het referendum**.*

Deze eis is getoetst door het opstellen van testcases op basis van specificaties en uitvoering van testen met behulp van de programmatuur. De testen, hun uitvoering en het resultaat zijn beschreven in hoofdstuk 3.

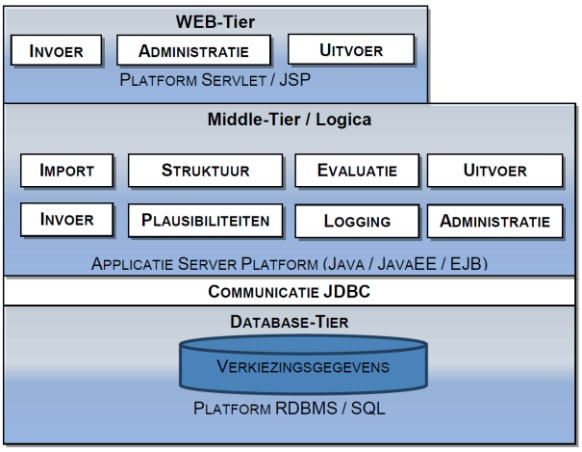
4.2 Modulaire aanpassingen

2. *De programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn.*

Voor verificatie van deze eis bekijken we de structuur van de opgeleverde code in relatie tot de architectuur zoals die beschreven is in de gedetailleerde specificatie [25]. Volgens de architectuurbeschrijving is de programmatuur opgebouwd volgens het meerlagenmodel (zie Figuur 2). Specifiek voor programma's 4 en 5 wordt deze nader ingevuld zoals weergegeven in Figuur 3.

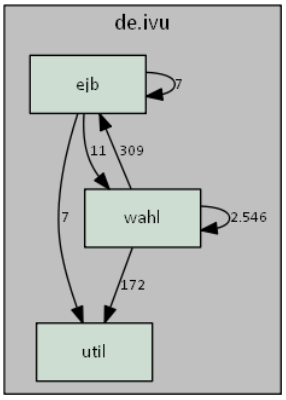


Figuur 2. N-tier model (volgens [25, pagina 93]).



Figuur 3. Componenten van het verkiezingssysteem (volgens [25, pagina 96]).

Bij analyse van de code van programma's 4 en 5 blijkt de decompositie volgens de package-indeling als volgt.



Figuur 4. OSV programma 4 en 5; levels 1 en 2.

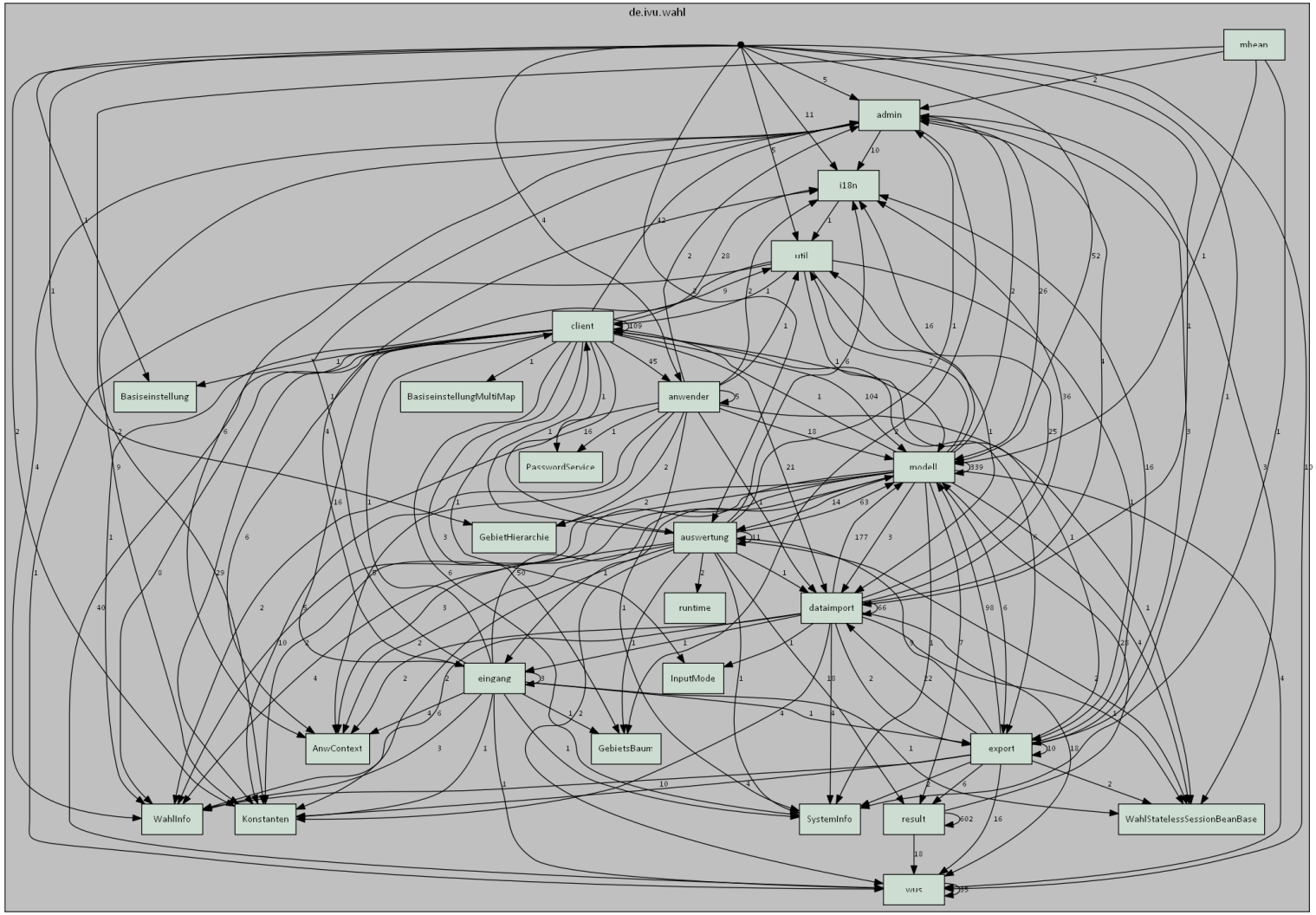
Op het hoogste niveau wordt de programmatuur ingedeeld in drie packages `de.ivu.wahl`, `de.ivu.ejb` en `de.ivu.util` (zie Figuur 4). In de figuur is met pijlen aangegeven hoe vaak een klasse uit het ene package gebruikmaakt van een andere component.

Als we ervan uitgaan dat `wahl` de inhoudelijke verkiezingssoftware bevat, is het logisch dat vanuit dat package aanroepen plaatsvinden naar packages met de Enterprise JavaBeans `ejb` en de generieke voorzieningen `util`.

In het algemeen zijn circulaire afhankelijkheden slecht voor de modulaire opbouw van programmatuur en druisen in tegen de principes van een gelaagde architectuur zoals voorgesteld in Figuur 2. De circulaire afhankelijkheid met `ejb` is verdedigbaar gegeven de rol van Enterprise JavaBeans om de business logica van de applicatie te bevatten[4].

Kijken we één niveau dieper in de structuur van de package `de.ivu.wahl`, dan ontstaat het beeld dat is weergegeven in Figuur 5.

4. Zie bijvoorbeeld: nl.wikipedia.org/wiki/Enterprise_JavaBeans.



Figuur 5. OSV programma 4 en 5; uitwerking level 3 ‘de.ivu.wahl’.

We hebben de leverancier gevraagd om de componenten van het package `de.ivu.wahl` in te delen naar de modulaire structuur uit de architectuurbeschrijving. Dat levert de volgende informatie.

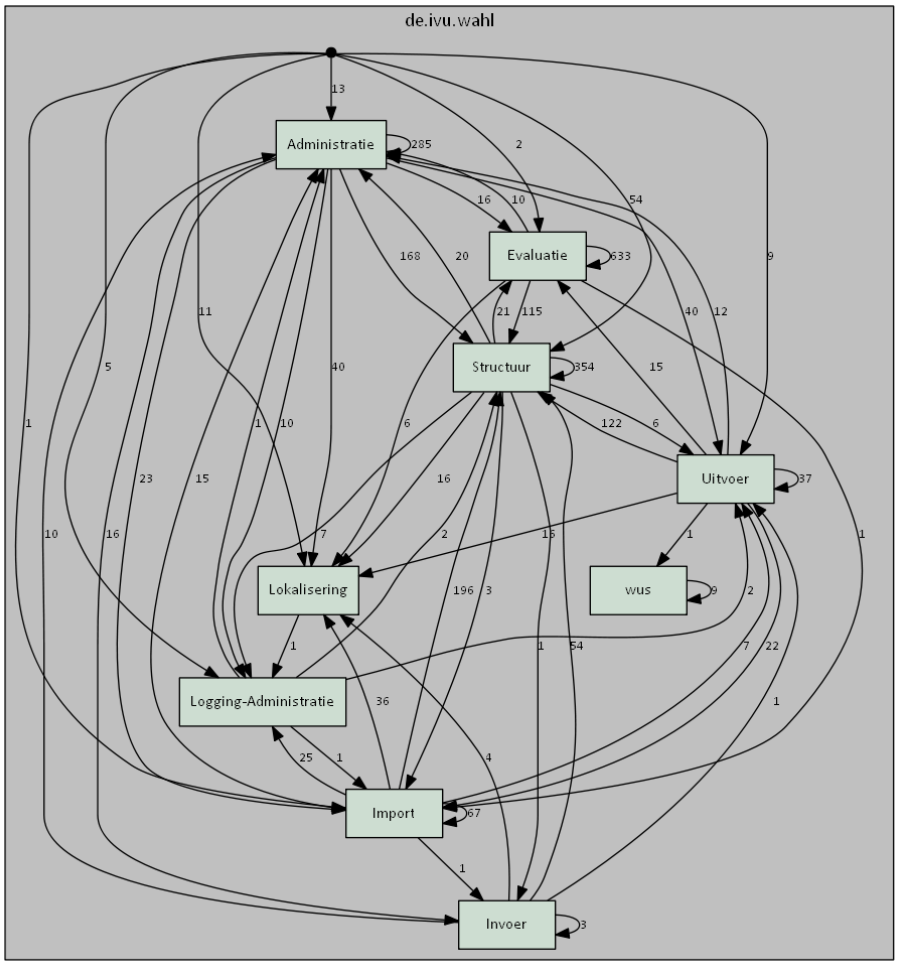
Package	Logische component
Admin	Administratie
AnwContext	Administratie
Anwender	Administratie
Auswertung	Evaluatie
Basiseinstellung	Administratie
BasiseinstellungMultiMap	Administratie
Client	Administratie
Dataimport	Import
Eingang	Invoer
Export	Uitvoer
GebietHierarchie	Administratie
GebietsBaum	Administratie
i18n	Lokalisering
InputMode	Import
Konstanten	Administratie
Mbean	Structuur
Modell	Structuur
PasswordService	Administratie
Result	Evaluatie
Runtime	Evaluatie
SystemInfo	Administratie
Util	Logging-Administratie
WahlInfo	Structuur
WahlStatelessSessionBeanBase	Administratie
wus.electioncategory	Structuur
wus.reportgen	Uitvoer
wus.xmlsecurity	Uitvoer

Tabel 12: Logische indeling van componenten uit 'de.ivu.wahl'.

Met deze logische indeling worden de afhankelijkheden tussen de logische componenten weergegeven in Figuur 6.

Op basis van deze analyse zijn we van mening dat de componentindeling zoals die is aangegeven in de architectuurbeschrijving onvoldoende is terug te vinden in de structuur van de code zoals die blijkt op basis van de packagenamen en het onderling gebruik van packages. Dit is gebaseerd op de volgende observaties:

- We zien veel circulaire afhankelijkheden tussen de componenten.
- Van het package `util` verwachten we dat dit eerder zou thuishoren in `de.ivu.util`.
- Afgaand op hun naamgeving bevatten `mbean` en `runtime` eveneens generieke functionaliteit die beter zou thuishoren in `de.ivu.util`.
- Binnen `wahl` zijn twee packages aangetroffen die zich bezighouden met gebruiksinformatie `anwender` en `client`.
- Voor de zetelverdeling zijn zowel `auswertung` als `result` verantwoordelijk.
- De naamgeving van packages is zowel in Engels als Duits. Dit levert verwarring als een ontwikkelaar moet zoeken in welk van de twee packages specifieke functionaliteit gerealiseerd is.



Figuur 6. OSV programma 4 en 5; indeling 'de.ivu.wahl' naar architectuurcomponenten.

Onze conclusie is dat de broncode onvoldoende gestructureerd is om op eenvoudige wijze aanpassingen door te voeren. De architectuurbeschrijving belooft een gelaagde structuur en heldere componentindeling die grotendeels, maar niet volledig is terug te vinden in de broncode. Het gevolg is dat aanpassingen van de software meer tijd in beslag zullen nemen dan bij een nog striktere doorvoering van architectuurprincipes in de codeopbouw.

Voor de geboden functionaliteit heeft onvolledige structurering geen directe gevolgen zodat we dit als een klein gebrek waarderen. Voor onderhoud heeft de onvolledige structurering negatieve gevolgen. Ontwikkelaars zullen moeite hebben te vinden waar welke functionaliteit gerealiseerd is. Onderhoud (adaptief en correctief) zal daardoor meer tijd vergen. Zo lang onderhoud wordt uitgevoerd door de ontwikkelaars van de software, mag ervan worden uitgegaan dat zij de software 'kennen'. Bij overgang naar een andere leverancier of bij aanpassingen in het ontwikkel- en beheerteam zal de onvolledige structurering nadelige gevolgen hebben.

4.3 Kritische functies

3. *De kritische functies voor de berekening van de uitslag van **de verkiezingen en de zetelverdeling** zijn in de programmatuur herkenbaar en gescheiden.*
3. *De kritische functies voor de berekening van de uitslag van **het referendum** zijn in de programmatuur herkenbaar en van elkaar gescheiden.*

Voor de interpretatie van deze eis gaan we uit van de toelichting die op deze eis is gegeven in de ministeriële regeling [12]:

> Onderdeel c legt vast dat de kritische functies in de programmatuur duidelijk herkenbaar en van elkaar gescheiden zijn. Het gaat hierbij om de functies die voor het berekenen van de uitslag en de zetelverdeling noodzakelijk zijn, zoals de invoer van de vastgestelde aantallen stemmen (tellingen) die door de stembureaus zijn verricht, de vastgestelde aantallen stemmen op het niveau van de gemeenten en hoofdstembureaus, en, op het niveau van de centrale stembureaus, de vastgestelde aantallen stemmen, de vaststelling van de uitslag, de zetelverdeling en de toewijzing van de zetels aan de kandidaten. Het is van belang dat deze functies herkenbaar en van elkaar gescheiden zijn, omdat daarmee transparant is waar in de code de kritische functies zich bevinden en zo de werking van deze functies zelfstandig te volgen is door de programmatuur heen. Zowel onderdeel b als onderdeel c zijn naar aanleiding van het advies van de Kiesraad verduidelijkt.

Met de eis wordt dus beoogd dat de kritische functies vindbaar zijn in de code en dat de werking zelfstandig te volgen is door de programmatuur.

Bij de leverancier hebben we nagevraagd welke methodes de uitslag van de verkiezingen en de zetelverdeling realiseren:

- *uitslag verkiezingen:* De berekende of geïmporteerde stemresultaten worden per stemgebied in de database opgeslagen. Het vaststellen van het totaalresultaat is een optelling waarvoor:
  - twee methodes `addGruppenstimmen` en `addKandidatenstimmen` aanwezig zijn uit de class `de.ivu.wahl.modell.GesamtstimmenImpl` en
  - de methode `addGruppeMitKandidaten` uit `de.ivu.wahl.auswertung.erg.ResultSummary`.
- *zetelverdeling:* Deze is geïmplementeerd in de class `de.ivu.wahl.result.determination.ElectionResultDeterminator` in de methode `determineElectionResult`.

Voor het bepalen van de referendumuitslag worden door de Kiesraad de volgende functies als kritisch beschouwd:

- de optellingen van het totaal aantal stemmen door het centraal stembureau (dat is de Kiesraad),
- de berekeningen van het opkomstpercentage en de percentages voor- en tegenstemmen.

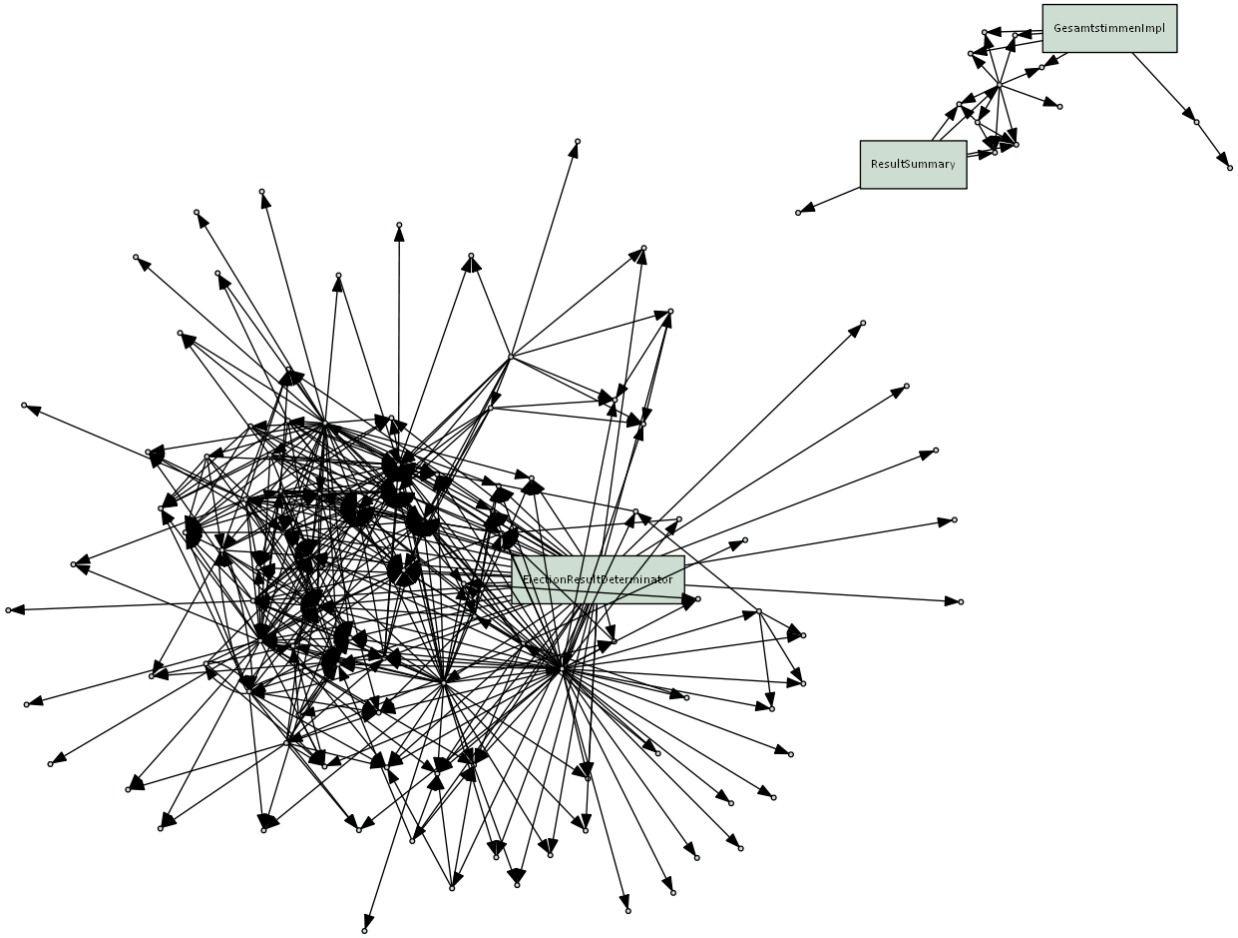
Bij de leverancier hebben we nagevraagd welke methodes voor deze functies gebruikt worden. Deze zijn:

- *optellingen:* Hiervoor worden dezelfde methodes gebruikt als voor verkiezingen (zie hierboven). Daarbij worden politieke partijen gebruikt in de rol van de antwoordmogelijkheden bij het referendum. Bij elke politieke partij wordt één kandidaat voor die partij aangemaakt om de stemmen voor het referendum te kunnen tellen als kandidaatstemmen.

- *percentageberekeningen:* De percentages worden berekend in de documentgenerator. De gegevens hiervoor komen uit het gegenereerde XML-bestand. De percentages worden weergegeven als breuk (zodat geen afronding plaatsvindt).

Met de informatie van de leverancier zijn de genoemde kritische functies vindbaar in de programmatuur.

De callgraph van de methodes voor de uitslag van de verkiezingen en de zetelverdeling (gevisualiseerd in Figuur 7) laat zien dat er geen afhankelijkheden zijn tussen beide berekeningen. De callgraph laat voor elke methode zien welke (publieke) methodes daarin gebruikt worden. In de figuur is te zien dat er geen afhankelijkheden zijn tussen de berekeningen van de totaaluitslag (de kleine callgraph rechtsboven in de figuur) en die van de zetelverdeling (linksonder).



Figuur 7. Callgraph voor berekening van de totaaltelling (rechtsboven) en zetelverdeling (linksonder).

Voor de percentageberekeningen van de referendumsoftware hebben we (zie ‘Bijlage C: Kritische functies; percentageberekeningen’) geconstateerd, dat in de code niet te volgen is hoe het betreffende resultaat tot stand komt. Door verbeterde documentatie van de sources is dit te verbeteren.

4.4 Soorten verkiezingen

4. *De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen.*
   Deze eis is niet van toepassing op de referendumsoftware.

De leverancier geeft aan dat het toevoegen van een nieuw type verkiezing relatief eenvoudig is als het te doorlopen proces veel lijkt op een al bestaande verkiezing. Dit wordt bevestigd door de formele specificatie van de berekeningen [17]. In § 1.5 van dat document worden de verschillende verkiezingssoorten behandeld en worden deze uitgewerkt in variaties van de algoritmes (in § 2.1).

Naar onze mening is hiermee in voldoende mate invulling gegeven aan de eis dat de programmatuur, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken is voor verschillende soorten verkiezingen. Als een nieuwe verkiezingssoort vergelijkbaar is met bestaande soorten, kan door invulling van de parameters en hergebruik van de bestaande algoritmes snel de benodigde programmatuur gerealiseerd worden. Als de bestaande algoritmes ontoereikend zijn, is onoverkoombaar dat aanpassingen meer werk kosten.

4.5 Voorkomen foutief gebruik

5. *Toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen.*

Begin 2017 heeft Fox-IT in opdracht van de Kiesraad een onderzoek uitgevoerd naar de beveiliging van (het gebruik van) OSV [22]. Aanbevelingen uit dit rapport hebben geleid tot aanpassingen in de software [28] en de formulering van voorwaarden voor gebruik van OSV [26]. De combinatie van deze organisatorische en technische maatregelen vermindert het risico op foutief gebruik van de software.

De belangrijkste doorgevoerde verbeteringen in de software zijn:

- *Vier-ogen-principe wordt technisch afgedwongen:* Bij de invoer van kandidaat-uitslaggegevens moet dubbele invoer plaatsvinden. Er kan niet meer worden volstaan met enkele invoer. Voor de beheerder van OSV lijkt de keuzemogelijkheid voor enkelvoudige invoer nog mogelijk. We adviseren deze mogelijkheid onzichtbaar te maken.
- *Verbeterde verificatie van integriteit van EML-bestanden:* zie verder § 4.13 van dit rapport.
- *Aanscherping instelling wachtwoorden:* OSV toont bij de keuze voor een wachtwoord een sterkte-indicatie met behulp van kleuren. We verwachten daarnaast een tekstuele aanduiding al was het maar om slechtzienden/kleurenblinden ook te bedienen. Gebruik van een sterk wachtwoord wordt niet door OSV afgedwongen; wel geadviseerd aan beheerders en gebruikers (zie [26], respectievelijk in § 5 en § 7). Het wachtwoord wordt in OSV beter versleuteld opgeslagen. Er wordt daarbij een sterkere vorm van encryptie toegepast.
- *Versleutelde verbinding voor de webapplicatie*: Tijdens de installatie van OSV wordt een certificaat aangemaakt op de server. Met dit certificaat wordt de netwerkcommunicatie versleuteld (https).

Een van de belangrijkste kwetsbaarheden in software betreft het gebruik van verouderde en/of niet meer ondersteunde softwarecomponenten. Als deze niet (meer) worden bijgewerkt naar actuele versies, worden

beveiligingsupdates niet meer doorgevoerd en kunnen veiligheidsleks misbruikt worden. Bij OSV is dit in ieder geval van toepassing op softwarecomponenten zoals de gebruikte versies van Java en Jboss.

Terecht merkt Fox-IT in haar rapportage [22, pagina 68] het gebruik van niet-ondersteunde software aan als een bevinding met een hoog risico. De nuancering die Fox-IT daarbij aangeeft is:

> Gezien de wijze waarop OSV zou moeten worden gebruikt volgens de richtlijnen, namelijk op een 'stand-alone' systeem of in een 'afgeschermd' netwerk, kan de mogelijkheid om deze kwetsbaarheden feitelijk uit te buiten beperkt zijn. Wanneer de OSV-omgeving echter benaderbaar is, bijvoorbeeld doordat deze op enigerlei wijze gekoppeld is aan de reguliere kantooromgeving, dan is de impact van de tekortkomingen aanzienlijk groter.

De Kiesraad heeft organisatorische maatregelen genomen om het technisch risico van niet-ondersteunde software te mitigeren. In de voorwaarden voor het gebruik van OSV [26] worden daartoe de volgende richtlijnen gegeven:

- Maak gebruik van een fysiek gescheiden netwerk. Geen koppeling met de reguliere IT-infrastructuur van de gemeente.
- Zorg dat eventueel aanwezige draadloze communicatiemodules, zoals Wifi en Bluetooth uit zijn (doe dit doormiddel van de instellingen in de BIOS van de computer).
- Controleer dat er geen andere netwerkkabels zijn aangesloten dan die daadwerkelijk nodig zijn.

Aanvullend aan de reeds genomen maatregelen kan foutief gebruik van OSV op technisch niveau verder voorkomen worden door defensief programmeren[5]. Bijvoorbeeld moet de invoer van gegevens consequent gecontroleerd worden op juistheid zodat deze niet misbruikt kan worden. Daartoe moeten parameters van publieke methodes geverifieerd worden voordat ze worden gebruikt.

Onze conclusie is dat er technisch gezien nog verbetermogelijkheden zijn om foutief gebruik van de software te voorkomen.

4.6 Diakritische tekens

6. *De programmatuur ondersteunt voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten in ieder geval de diakritische tekens van de tekenset die op grond van artikel 3, eerste lid, van het Besluit basisregistratie personen voor de basisregistratie personen is vastgesteld.*
   Deze eis is niet van toepassing op de referendumsoftware.

We constateren dat de programmatuur diakritische tekens van de GBA-tekenset correct verwerkt. Deze conclusie is gebaseerd op de volgende test.

In het Besluit basisregistratie personen kunnen we de volgende informatie vinden over de te gebruiken tekenset:

- Artikel 3, lid 1 van het Besluit basisregistratie personen [6] luidt: "Onze Minister stelt een systeembeschrijving vast.".

---

5. Zie: en.wikipedia.org/wiki/Defensive_programming.

- In artikel 4 van het besluit staat: “De systeembeschrijving geeft een beschrijving van de aspecten die zijn aangeduid in de tabel die als bijlage 2 bij dit besluit is gevoegd.”. In de betreffende bijlage 2 is geen verwijzing naar de tekenset opgenomen.
- Volgens artikel 2 uit de Regeling basisregistratie personen [7] wordt de systeembeschrijving gevormd door:
  a. de in bijlage 1 bij deze regeling genoemde onderdelen van het Logisch Ontwerp GBA, versie 3.10, bedoeld in artikel 3, eerste lid;
  b. de in bijlage 2 bij deze regeling genoemde onderdelen van het Logisch Ontwerp RNI, versie 2.12, bedoeld in artikel 3, tweede lid;
  c. de hoofdstukken 3 en 4 van de in bijlage 3 bij deze regeling opgenomen beschrijving van de wijze waarop de in de bijlagen 1 en 2 bedoelde onderdelen worden toegepast.
- Volgens bijlage 4 uit de bijbehorende regeling is het “Logisch Ontwerp GBA, versie 3.8” van toepassing en volgens bijlage 5 eveneens het “Logisch Ontwerp RNI, versie 2.10.02”.
- In het Logisch Ontwerp GBA [8] wordt in bijlage II voorgeschreven welke tekens gebaseerd op de Teletex-standaard binnen het GBA-systeem gebruikt mogen worden en hoe deze te coderen.
- In het Logisch Ontwerp RNI [9] wordt in bijlage II direct verwezen naar het Logisch Ontwerp GBA [8] en worden de voorschriften daaruit van toepassing verklaard op RNI.

Om het gebruik van diakritische tekens te testen hebben we de volgende stappen uitgevoerd:
- Eerst hebben we de tekenset uit het Logisch Ontwerp GBA [8], bijlage II.3 en II.4 overgenomen in dit document (zie B.1 en B.2).
- Vervolgens hebben we in ‘P1 – Aanmaken kandidatenlijsten’ een kandidatenlijst aangemaakt waarbij in de achternaam van kandidaten de diakritische tekens vanuit Word zijn gekopieerd. Visueel is gecontroleerd of de betreffende karakters op het scherm verschijnen.
- Diakritische tekens kunnen ook worden ingevoerd door in een invoerveld met de combinatie ‘Ctrl – spatie’ een optie te kiezen uit een dropdown-lijst van in te voegen mogelijkheden. In de dropdown verschijnen niet alle mogelijkheden uit de GBA-tekenset. Enkele van de caron-tekens blijken problematisch.
- Daarna zijn alle documenten met P1 aangemaakt. Zowel in de gegenereerde pdf-bestanden als in het eml-bestand is gecontroleerd of diakritische tekens juist worden weergegeven. Waar dat correct gebeurt, is dit aangegeven in de tabellen in ‘Bijlage B: Tekenset basisregistratie personen‘.
- De namen van de aangemaakte bestanden bevatten geen diakritische tekens. Na controle blijkt dat het systeem dit oplost door extra volgnummers toe te voegen aan bestandsnamen indien dat noodzakelijk is.

4.7 Open source en standaarden

*7. De programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor **verkiezingsgegevens zoals kandidatenlijsten en zetelverdeling** wordt de EML_NL standaard toegepast.*

*7. De programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor **referendumgegevens** wordt de EML_NL standaard toegepast.*

Voor de definities van ‘open source’ en ‘open standaarden’ maken we gebruik van de overheidsinformatie op dit gebied:

- *Open source:* Open source betekent dat de broncode van bijvoorbeeld een website, programma of app, vrij beschikbaar is. Iedereen kan de broncode lezen, aanpassen en verspreiden[6].
- *Open standaarden:* Een standaard is een afspraak die is vastgelegd in een specificatiedocument. Om gegevens uit te wisselen moeten ICT-systemen dezelfde standaard hebben geïmplementeerd. Voorwaarde is dan wel dat het specificatiedocument vrij te verkrijgen is[7].
  Alle standaarden op de lijst van Forum Standaardisatie zijn ‘open’. Hiervoor hanteert het vier kenmerken waaraan een standaard moet voldoen om als 'open standaard' aangemerkt te worden.
  - De benodigde documentatie moet laagdrempelig beschikbaar zijn.
  - Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht.
  - Er moeten voldoende inspraakmogelijkheden zijn voor stakeholders tijdens de (door)ontwikkeling van de standaard.
  - De onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie moeten verzekerd zijn.

Gebruik van ‘open source’ is voor programma’s 4 en 5 geregeld. De broncode van deze programma’s wordt door de Kiesraad via haar website vrij beschikbaar gesteld[8] (gecontroleerd op 3 januari 2018). Omdat de broncode is geschreven in Java, is deze voor Java-kenners leesbaar, aanpasbaar en kan door iedereen verspreid worden. Kennis en ervaring met Java is op de Nederlandse markt ruimschoots beschikbaar.

De enige standaard die bij digitale informatie-uitwisseling binnen OSV gebruikt wordt, is de EML-NL standaard[9] [16]. Deze standaard is gebaseerd op de (internationale) EML-standaard, versie 5.0. De Nederlandse EML standaard, versie 1.0, is opgenomen in de lijst met open standaarden van Forum Standaardisatie en voldoet aan de gestelde eis[10].

De leverancier maakt bij de gebruikte EML standaard de volgende aantekening. Bij de ontwikkeling van OSV is uitgegaan van de internationale Election Markup Language standaard[11] (versie 5.0 die er op dat moment in 2008 was). De EML-standaard moet op onderdelen gelokaliseerd worden. Deze lokalisering is destijds voor Nederland (en OSV) toegepast in nauw overleg met de specialisten van de Kiesraad. In 2013 is een officiële Nederlandse EML_NL-standaard in het leven geroepen gebaseerd op de in gebruik zijnde EML-lokalisaties van OSV. In de praktijk kan het voorkomen dat de laatste OSV-versie gebruikmaakt van een nog niet officieel bevestigde nieuwe versie van EML_NL. Dit kan veroorzaakt worden door de korte tijdspanne die ligt tussen een officiële bekrachtiging van een aanpassing op de Kieswet en het beschikbaar moeten zijn van OSV voor een verkiezing. Als een kieswetwijziging effect heeft op de informatie-uitwisseling in de EML-bestanden zal deze zo snel mogelijk in OSV worden opgenomen vooruitlopend op bekrachtiging van de standaard.

---

6. Zie: www.rijksoverheid.nl/onderwerpen/digitale-overheid/open-overheid.
7. Zie: www.forumstandaardisatie.nl/thema/open-standaarden.
8. Zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-broncode-programma-4-en-5-versie-2.19.2.
9. Zie: www.kiesraad.nl/verkiezingen/osv-en-eml/eml-standaard.
10. Zie: www.forumstandaardisatie.nl/standaard/emlnl.
11. Zie: en.wikipedia.org/wiki/Election_Markup_Language.

Bij het genereren van uitvoer-bestanden maakt OSV gebruik van de volgende formaten.

- *PDF, Portable Document Format:* Het blijkt dat OSV pdf-documenten in versie 1.4 levert. In de 'pas toe of leg uit'-lijst zijn PDF 1.7, PDF/A-1 en PDF/A-2 opgenomen. Het is raadzaam naar een van deze formaten te migreren.
- *RTF, Rich Text Format:* Dit formaat is niet opgenomen in de 'pas toe of leg uit'-lijst, maar is dermate algemeen geaccepteerd dat het als een de facto standaard beschouwd kan worden. In OSV heeft de gebruiker veelal de keuze om te kiezen tussen output in PDF- of RTF-formaat.
- *CSV, Comma Separated Values:* Dit formaat is niet opgenomen in de 'pas toe of leg uit'-lijst en is eveneens een de facto standaard.
- *EML, Election Markup Language:* Zie de bovenstaande beschrijving van EML en EML-NL.

4.8 Vrij verkrijgbare standaard programmatuur

8. De standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar.

De leverancier heeft aangegeven dat de volgende tools worden toegepast bij de ontwikkeling van OSV:

- Eclipse *Java EE IDE for Web Developers, Version: Indigo Service Release 1:* Dit tool wordt gebruikt als ontwikkelomgeving (IDE = Integrated Development Environment). Deze omgeving is vrij beschikbaar vanaf de website van Eclipse: www.eclipse.org.
- *Altova StyleVision, version 2015 rel. 4:* Dit tool (zie: www.altova.com/stylevision.html) wordt gebruikt voor de generatie van de sjablonen voor documenten (in XSLT). Een 'trial'-versie is vrij verkrijgbaar.
- *JBoss Application Server, JBoss-4.2.3.GA:* Dit tool is vrij verkrijgbaar onder andere via SourceForge (sourceforge.net/projects/jboss/files/JBoss/JBoss-4.2.3.GA/).
- *Apache:* wordt gebruikt voor de generatie van documenten en rapporten. Deze software is vrij verkrijgbaar via: xmlgraphics.apache.org/. Voor OSV wordt gebruikgemaakt van de volgende tools:
  - Apache FOP 1.1, avalon-framework-4.2.0.jar, batik 1.7, Xalan-J 2.7.0, Xerces 2.7.1
  - Apache Derby inbedded database, versie 10.11.1.1
  - Apache POI 3.1
- *XOM 1.1 XML object model:* Dit tool wordt gebruikt voor object modellering. Het is als open source verkrijgbaar via: www.xom.nu.

Afgezien van Altova StyleVision zijn de tools vrij verkrijgbaar. Altova is een hulpmiddel bij de generatie van sjablonen. We achten dit tool niet bedrijfskritisch voor de realisatie van OSV.

4.9 Intellectueel eigendom

9. Het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau.

In juli 2015 is een overeenkomst [15] getekend tussen de Staat der Nederlanden en IVU met betrekking tot OSV. Deze overeenkomst is afgesloten op basis van ARBIT. Het intellectueel eigendom op de software is geregeld in artikel 8 van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2014 (ARBIT-2014) [10]:

8.1 Alle intellectuele eigendomsrechten die ten aanzien van de Prestatie waar en wanneer ook kunnen of zullen kunnen worden uitgeoefend, berusten bij:

a. Opdrachtgever voor zover het betreft een Prestatie die specifiek voor Opdrachtgever is of wordt ontworpen of vervaardigd en/of onder leiding of toezicht van Opdrachtgever dan wel aan de hand van diens instructies of ontwerpen is of wordt gerealiseerd. Voor zover nodig worden deze rechten op grond van de Overeenkomst door Wederpartij aan Opdrachtgever overgedragen welke overdracht reeds nu voor alsdan door Opdrachtgever wordt aanvaard;

b. Wederpartij of een derde in alle overige gevallen. Wederpartij verleent in dat geval aan Opdrachtgever een nader bij de Overeenkomst te bepalen niet exclusief recht tot gebruik van de Prestatie dat in ieder geval toereikend is voor nakoming van het in de Overeenkomst(en) bepaalde.

Met deze interpretatie van het intellectueel eigendomsrecht voldoet OSV aan de gestelde eis.

4.10 Open source compiler

10. De programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is.

De programmatuur voor OSV is geschreven in Java. Voor Java zijn meerdere compilers beschikbaar[12] waarvan diverse als open source. Een van de open source compilers is onderdeel van de incrementele ontwikkelomgeving (IDE) van Eclipse (zie ook 4.8).

[12]. Zie bijvoorbeeld: en.wikipedia.org/wiki/Java_compiler.

4.11 Verschillende besturingssystemen

11. De programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem.

In de beschrijving van de systeemvereisten voor programma's 4 en 5 [24] worden de volgende eisen aan de besturingssystemen gesteld.

Serververeisten (of gecombineerde client-serververeisten)	
Besturingssysteem	**Windows:** 2008 Server, Windows 7, Windows 8 en Windows 10 **Linux:** SuSE Linux Enterprise Server 11 of nieuwer Red Hat Enterprise Linux 4 of nieuwer CentOS 6 of nieuwer Ubuntu 12.04 LTE of nieuwer **Mac OS X:** 10.8 of nieuwer

Clientvereisten	
Besturingssysteem	Gebruik op de (client)computer een recent besturingssysteem dat ondersteund wordt.

Tabel 13: Systeemvereisten voor het te gebruiken besturingssysteem voor programma 4 en 5 van OSV.

Uit eigen ervaring blijkt dat het systeem draait op een Windows 10 besturingssysteem en een Mac.

Hieruit blijkt dat het systeem is ontwikkeld voor verschillende besturingssystemen (Windows/Linux en Mac OS). Aangezien Linux een open source besturingssysteem betreft, wordt voldaan aan de eis dat OSV voor tenminste één open source besturingssysteem is ontwikkeld.

4.12 Authenticiteit programmatuur

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

De authenticiteit van de programmatuur kan voorafgaand aan de installatie worden vastgesteld. Daartoe wordt niet meer gebruikgemaakt van separate software (met bijbehorende beveiligingsrisico's), maar van de programmatuur die onderdeel is van het gebruikte besturingssysteem. Bij Windows betreft dit het programma `certutil`, bij Linux of Mac `shasum`. Dit is een verbetering ten opzichte van de eerdere situatie waarbij een separaat programma `Cygwin` geïnstalleerd moest worden met bijbehorende beveiligingsrisico's (zie [22], Bevinding 10, pagina 84).

Met de genoemde programma's wordt een SHA-256 hash-code berekend over de aangeleverde installatiebestanden. Deze hash-code moet gelijk zijn aan de hash-code die de Kiesraad op haar website publiceert[13]. De handleiding voor deze authenticiteitscontrole is te vinden op de website [23].

In de voorwaarden voor het gebruik van OSV [26] wordt als richtlijn gegeven dat de procedure voor het vaststellen van de authenticiteit van de programmatuur moet worden uitgevoerd. Deze controle wordt niet afgedwongen.

Voor deze integriteitscontrole zijn tevens bevindingen 7 en 12 uit de rapportage van Fox-IT [22, pagina 65] van toepassing. Beide worden door Fox-IT geclassificeerd met een hoog risico.

- *Bevinding 7:* Integriteitscontrole OSV installatie-cd-rom kan omzeild worden
- *Bevinding 12:* Overeenkomst broncode en uitvoerbare bestanden niet mogelijk

Ten aanzien van bevinding 7 zijn mitigerende maatregelen genomen; voor bevinding 12 is dat nog niet gebeurd in de huidige versie van OSV. Bij nieuwe leveringen van OSV worden de installatiebestanden als één gecomprimeerd bestand (in zip-formaat) uitgeleverd. Daarbij wordt een hash-code over de complete installatie aangemaakt. In de gebruiksvoorwaarden [26] is als richtlijn opgenomen dat de hash-code moet worden gecontroleerd. Als nu individuele bestanden gemanipuleerd zouden worden, levert dit een andere hash-code voor de installatie die niet overeenkomt met de gepubliceerde hash-code.

Run-time wordt de authenticiteit van de programmatuur niet geverifieerd. Daardoor is het – in theorie – mogelijk dat een gebruiker een aangepaste versie van de software op een computer installeert en daarmee de verkiezingsuitslag en/of zetelverdeling beïnvloedt. Dit is te voorkomen door gebruik te maken van bijvoorbeeld een 'Challenge-handshake authentication protocol'[14] waarmee periodiek gecontroleerd wordt of de gebruikte software overeenkomt met de uitgegeven software.

De leverancier plaatst de volgende kanttekening: De gebruikersvriendelijkheid van OSV bij installatie en gebruik heeft een erg hoge prioriteit gehad bij de ontwikkeling destijds en heeft deze nog steeds. Uitgangspunt hierbij is dat een gebruiker met weinig IT-kennis de programmatuur zonder hulp van een IT-expert kan installeren en gebruiken. Bij instructies worden gebruikers geadviseerd de authenticiteit van OSV vast te stellen en waar uitleg voor deze procedure gevonden kan worden. Uit reacties van de deelnemers aan dergelijke instructies blijkt dat slechts 5 tot 10 procent (nog) daarvan gebruikmaakt en dat dit eigenlijk alleen gebeurt door de IT-expert van een gemeente en niet door de gebruiker(s) van de programmatuur.

4.13 Authenticiteit aangeleverde gegevens

13. *Bij het inlezen van **verkiezingsgegevens** in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.*
13. *Bij het inlezen van **referendumgegevens** in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.*

---

13. Zie: www.kiesraad.nl/verkiezingen/gemeenteraden/ondersteunende-software-verkiezingen-osv/osv-voor-gemeenten.
14. Zie: nl.wikipedia.org/wiki/Challenge-handshake_authentication_protocol.

De authenticiteit van gegevens wordt in de programmatuur vastgesteld door de hash-code van het ingelezen bestand te vergelijken met de hash-code afgedrukt in het bijbehorende document. Deze controle wordt niet in alle gevallen afgedwongen door OSV. De Kiesraad heeft organisatorische maatregelen genomen om het risico op misbruik te mitigeren. Door verbeteringen in de toegepaste technologie en verbeterde organisatorische maatregelen is het risico op misbruik uitermate klein geworden.

Volgens Bijlage E § 8.2 van de gedetailleerde specificatie [25] worden hash-codes van 64 hexadecimale tekens[15] gebruikt om de authenticiteit van uitgewisselde gegevens vast te stellen. Bij het aanmaken van de hash-code wordt gebruikgemaakt van een SHA-256 hashing algoritme[16]. In de documentatie is aangegeven dat rekening is gehouden met de mogelijkheid om naar een (betere) hash-berekening over te gaan, mocht dit nodig zijn.

De gebruikte hash-code en het gebruikte hashing algoritme zijn verbeterd[17] ten opzichte van de eerder uitgevoerde toetsingen van OSV en de referendumsoftware. De hash-code bestond eerder uit slechts 32 hexadecimale tekens en als algoritme werd toentertijd het ondertussen gekraakte SHA-1 algoritme toegepast.

Bij het aanmaken van een elektronisch bestand voor berichtuitwisseling (EML-bestand) berekent de software de hash-code behorend bij dat bestand. Als de wet gelijktijdig een papieren versie voorschrijft, wordt de hash-code onderaan het document afgedrukt. In andere gevallen wordt een apart document aangemaakt met de hash-code.

Er zijn twee mogelijkheden om de authenticiteit van ingelezen gegevens vast te stellen (volgens [25], § 8.3):
1. op het moment dat het elektronisch bestand wordt ingelezen in OSV en de hash-code wordt vergeleken met de hash-code op het papieren document, en;
2. nadat het elektronisch bestand is ingelezen, door middel van de in de log-bestanden vastgelegde hash-code en het tijdstip van het aangemaakte en ingelezen elektronisch bestand.

Bij het inlezen van het elektronisch bestand (optie 1 hierboven) zijn drie varianten van beveiligingsniveaus onderscheiden:
a. Op het laagste beveiligingsniveau wordt de hash-code alleen in een logbestand weggeschreven en hoeft de gebruiker deze niet te controleren;
b. Op het middelste beveiligingsniveau wordt de hash-code getoond en wordt de gebruiker gevraagd om deze te bevestigen middels een ‘ja/nee’ vraag;
c. Op het hoogste beveiligingsniveau is de gebruiker verplicht om acht tekens van de hash-code verdeeld in twee willekeurige groepen van vier tekens in te voeren. Er kan niet verder worden gegaan zonder het afgedrukte document.

De onderstaande tabel geeft een overzicht van de bestanden die in programma’s 4 en 5 van OSV kunnen worden ingelezen (volgens [25]) met het bijbehorende beveiligingsniveau.

15. Hexadecimale tekens worden gerepresenteerd door de cijfers 0 tot en met 9 en de letters A tot en met F.
16. Zie: nl.wikipedia.org/wiki/SHA-familie.
17. Zie en.wikipedia.org/wiki/Hash_function_security_summary voor een vergelijking van de kwaliteit van de diverse hashing algoritmes.

Bestand	EML	Van	Prog.	Naar	Prog.	Beveiligingsvariant	Opmerking
Verkiezingsdefinitie	110a	CSB	P0	div.	alle	a	
Referendumvraag	630	CSB	P0	div.	P4	a	
Kandidatenlijsten	230b	CSB	P2-3	PSB, HSB	P4	c/b	bij zelfde gemeente (PS)
Totaallijsten	230c	CSB	P2-3	CSB	P4, P5	b	
Stembureaus	110b	PSB (of extern programma)	P4	PSB	P4	a	
Telling stembureau	510a	PSB (of extern programma)	P4	PSB	P4	a	zelden gebruikt
Telling gemeente	510b	PSB	P4	HSB	P4	c/b	zelfde gemeente
Telling kieskring	510c	HSB	P4	CSB	P4	c/b	zelfde gemeente
Totaaltelling	510d	PSB, CSB	P4	CSB	P5	b	

Tabel 14: Mogelijke invoer voor P4 en P5 met bijbehorende variant van controle (volgens [25], pagina 120)

We achten de eerste twee beveiligingsniveaus (‘a’ en ‘b’) inadequaat om daadwerkelijk de authenticiteit van in te lezen verkiezingsgegevens vast te stellen:

- Bij ‘a’ kan na verloop van tijd door verificatie in het logbestand nog enigszins nagegaan worden of met de juiste gegevens is gewerkt. Dat kan echter te laat zijn.
- Bij ‘b’ heeft de gebruiker de mogelijkheid om – ongezien – met ‘ja’ door te klikken en verder te werken. Dit beveiligingsniveau is dan gelijkwaardig met ‘a’ (ervan uitgaand dat de hash-code in het logbestand wordt weggeschreven).

Voor cruciale tellingsbestanden (510b, 510c en 510d) zijn de afgedwongen beveiligingsniveaus verhoogd van ‘c/a’ (bij de vorige toets van OSV) naar ‘c/b’. Daarmee is het beveiligingsniveau verbeterd, maar wordt nog niet het hoogste beveiligingsniveau ‘c’ voor deze tellingsbestanden in alle situaties afgedwongen.

De Kiesraad en de leverancier geven beide aan dat gebruiksvriendelijkheid van OSV belangrijk is geweest in de afweging van de gekozen beveiligingsniveaus en hun implementatie. Besloten is dat in bepaalde situaties wordt afgezien van de controle van de hash-code bij het inlezen van een EML-bestand (volgens [25, Bijlage E]). In die situaties wordt de kans klein geacht dat ongemerkt wijzigingen in elektronische bestanden kunnen plaatsvinden. De controle op basis van de log-bestanden blijft mogelijk. Bij de afweging of situaties bestaan, waarbij de controle niet noodzakelijk is, hebben de volgende omstandigheden een rol gespeeld:

- de afstand tussen het aanmaken en het inlezen van het bestand;
- de tijd die verstrijkt tussen het aanmaken en het inlezen van het bestand;
- de fase in het verkiezingsproces.

Fox-IT geeft in haar rapport diverse oplossingen voor verbetering van de integriteit van EML-bestanden (zie [22], Bevinding 5, pagina 73 e.v.):

1. Voeg een digitale handtekening toe aan de EML-bestanden. De verificatie is hoofdzakelijk nodig om de integriteit van de EML-bestanden tijdens transport te waarborgen. Als OSV gecompromitteerd is, gelden andere mogelijke aanvallen en gevolgen. Een dergelijke digitale handtekening vereist een ingrijpende wijziging in OSV en een proces dat voorziet in de verspreiding van sleutelmateriaal en/of certificaten.
2. In de huidige werkwijze is het belangrijk dat meer karakters worden gevalideerd. Het invoeren van meer karakters van de hash-waarde heeft een bepaalde grens ten aanzien van gebruiksgemak. Gezien de

benodigde tijd voor het berekenen van een collision bij gebruik van geoptimaliseerde software en/of hardware zijn minimaal, en waarschijnlijk meer, dan twintig hexadecimale karakters benodigd. Dit is mogelijk voorbij de grens van gebruiksvriendelijkheid. Het aantal in te voeren karakters zou verminderd kunnen worden door gebruik te maken van een andere visuele representatie van de hash-waarde.

3. Laat OSV de gebruiker vragen om een aantal karakters (al dan niet aaneengesloten) in te vullen waarbij de plaats van de karakters steeds willekeurig bepaald wordt. Dit zorgt ervoor dat een aanvaller niet kan voorspellen op welke plaats de gedeeltelijke collision zich moet bevinden.
4. De minimale inspanning vereist dat de gebruikers de hash-waardes visueel verifiëren. In het kader van gebruiksvriendelijkheid wordt aangeraden om onderzoek te doen naar de mogelijkheden om de karakters op een visueel gebruiksvriendelijke wijze te tonen.

Van deze vier oplossingsrichtingen zijn ondertussen de volgende gerealiseerd (zie ook [28]).

- De instructietekst op het controlescherm is verduidelijkt. Er wordt nadrukkelijker gewezen op een visuele controle van de hash-code (oplossing 4).
- In plaats van de eerdere vier karakters moeten nu acht karakters worden ingevoerd (oplossing 2).
- De acht karakters worden uitgevraagd in twee groepjes van vier waarvoor willekeurige posities in de code worden genomen (oplossing 3).

De gekozen beveiligingsniveaus ‘a’ en ‘b’ blijven mogelijk en hun implementatie biedt daarmee de mogelijkheid dat de authenticiteit van ingelezen verkiezingsgegevens niet altijd wordt vastgesteld. Daarmee blijft een risico aanwezig dat een gebruiker veranderingen aanbrengt in verkiezingsgegevens die consequenties hebben voor de totaaltelling en/of de zetelverdeling.

De Kiesraad geeft aan dat ten aanzien van de kandidatenlijst en tellingbestanden het controleniveau ‘a’ of ‘b’ alleen mogelijk is als het een gegevensbestand van de eigen organisatie betreft. In dat geval is geen sprake van organisatie overstijgende overdracht. Men betwijfelt of niveau ‘c’ waarde toevoegt als het bestand wordt ingelezen door de persoon die het bestand heeft aangemaakt. In de overdacht van plaatselijk stembureau (PSB) naar hoofstembureau (HSB) en van PSB naar centraal stembureau (CSB) bij dezelfde gemeente kan het EML-bestand op de OSV computer blijven staan om vervolgens direct weer ingelezen te worden. De overdracht op bijvoorbeeld een USB-stick is dan niet aan de orde.

Naar onze mening is in de geschetste situaties en met deze omstandigheden de kans op fraude met ingelezen verkiezingsgegevens verkleind edoch niet volledig uitgebannen. In fraudegevallen moet niet alleen rekening gehouden worden met fraude door externen. Fraude door eigen medewerkers is een serieus te nemen mogelijkheid. Verdere mitigatie van het risico op fraude met aangeleverde gegevens is aan te bevelen door consequent af te dwingen dat de hash-codes worden ingevuld bij inlezen van het bestand.

Naar ons oordeel wordt de authenticiteit van gegevens nu beter vastgesteld in vergelijking tot de situatie bij onze eerdere toetsingen. Het risico is kleiner geworden door de doorgevoerde verbeteringen sinds de eerder door ons uitgevoerde toetsen.

Bijlage A: Bronmateriaal

A.1 Wet- en regelgeving

1. *Kieswet, Geldend van 01-12-2017 t/m heden*, Wet van 28 september 1989, houdende nieuwe bepalingen inzake het kiesrecht en de verkiezingen, zie: wetten.overheid.nl/BWBR0004627/2017-12-01.
2. *Kiesbesluit, Geldend van 01-12-2017 t/m heden,* Besluit van 19 oktober 1989, houdende vaststelling van nieuwe voorschriften ter uitvoering van de Kieswet, zie: wetten.overheid.nl/BWBR0004632/2017-12-01.
5. *Kies- en referendumregeling, Geldend van 16-12-2017 t/m heden*, Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 6 november 2013, nr. 2013-0000435969, houdende regels ter uitvoering van de Kieswet en het Kiesbesluit (Kiesregeling), zie: wetten.overheid.nl/BWBR0034180/2017-12-16.
6. *Besluit basisregistratie personen, Geldend van 01-01-2018 t/m heden*, Besluit van 28 november 2013, houdende regels ter uitvoering van de Wet basisregistratie personen (Besluit basisregistratie personen), zie: wetten.overheid.nl/BWBR0034306/2018-01-01.
7. *Regeling basisregistratie personen, Geldend van 01-01-2018 t/m heden*, Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 3 december 2013, nr. 2013-0000731182, DCB/CZW/S&B, houdende regels ter uitvoering van de Wet basisregistratie personen en het Besluit basisregistratie personen (Regeling basisregistratie personen), zie: wetten.overheid.nl/BWBR0034327/2018-01-01.
8. *Logisch Ontwerp GBA versie 3.10*, datum: 08-10-2016, zie: www.rvig.nl/documenten/richtlijnen/2016/10/14/logisch-ontwerp-gba-versie-3-10.
9. *Logisch Ontwerp RNI versie: 2.12.01*, datum: 08-10-2016, zie: www.rvig.nl/documenten/richtlijnen/2016/10/27/logisch-ontwerp-rni-versie-2-12.
10. *Besluit vaststelling Algemene Rijksvoorwaarden voor inkoop (ARBIT-2014, ARIV-2014 en ARVODI-2014), [Regeling vervallen per 04-10-2016.], Geldend van 05-04-2014 t/m 03-10-2016*, Besluit van de Minister-President, Minister van Algemene Zaken van 26 maart 2014, nr. 3132081, houdende vaststelling van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2014 (ARBIT-2014), de Algemene Rijksinkoopvoorwaarden 2014 (ARIV-2014) en de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten 2014 (ARVODI-2014), zie: wetten.overheid.nl/BWBR0035022/2014-04-05.
11. *Eisen voor de programmatuur die door de centrale stembureaus wordt gebruikt ten behoeve van de vaststelling van de uitslag van verkiezingen van de leden van de Tweede Kamer, de leden van het Europees parlement, de leden van Provinciale Staten en de gemeenteraden*, 15-04-2008, zie: zoek.officielebekendmakingen.nl/kst-31200-VII-55-b1.
12. *Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 7 oktober 2014, nr. 2014-0000529148, houdende wijziging van de Kiesregeling met het oog op het stellen van eisen aan de programmatuur voor de berekening van de verkiezingsuitslag*, Staatscourant, nr. 33828, 28-11-2014, zie: zoek.officielebekendmakingen.nl/stcrt-2014-33828.html.

A.2 Documenten

13. *Overeenkomst inzake Ondersteunende Software Verkiezingen tussen De Staat der Nederlanden: Kiesraad en IVU Traffic Technologies AG*, kenmerk: 2008:0000562428, ondertekend: 16-12-2008.
14. *Nutzung der Softwaremodule des WAS-Systems für die Wahlen in den Niederlanden*, brief van Destatis aan Kiesraad, kenmerk: IIC/2230-WB1, 26-03-2009.
15. *Raamovereenkomst ARBIT inzake de Ondersteunende Software Verkiezingen (OSV), afgesloten tussen De Staat der Nederlanden en IVU Traffic Technologies AG*, getekend door beide partijen op 13 07 2015 en 16 07 2015.
16. *EML_NL 1.0, Het Nederlandse profiel van de EML 5.0*, versie 1.0.a, Juli 2013, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/eml-bestanden/specificatiedocument-eml_nl-versie-1.0a.
17. *Determination of the Election Result*, Kiesraad, auteur: Joachim Nottebaum, versie 6.1, 28-01-2014, zie: www.kiesraad.nl/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-specificatie-determination-of-the-election-result.
18. *Toets specificatie berekening uitslag verkiezingen*, Universiteit Utrecht, R. Nehmelman, W. van der Woude, 02-10-2014, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-toetsingsrapport-specificatie-berekening-uitslag.
19. *Toetsing Ondersteunende Software Verkiezingen (OSV), Definitieve rapportage*, SQS Nederland, versie 1.0, status: definitief, datum: 26-01-2015, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-toetsingsrapport-sqs-26-februari-2015-programma-4-en-5.
20. *Toetsing Referendumsoftware van Ondersteunende Software Verkiezingen (OSV), Definitieve rapportage*, SQS Nederland, versie 1.0, status: definitief, datum: 19-02-2016, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-toetsingsrapport-sqs-referendumsoftware-19-2-2016.
21. *Formele beschrijving voor het berekenen van de uitslag referendum*, 07-06-2016, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/formele-beschrijving-berekening-uitslag-referendum.
22. *Onderzoek OSV en proces; Rapportage, Fox-IT, opdrachtgever: Kiesraad*, Paul Pols, Daniël Niggebrugge, Francisco Dominguez, versie: 1.0, status: definitief, referentie: PR-160624, classificatie: public, datum: 02-03-2017, zie: www.kiesraad.nl/adviezen-en-publicaties/rapporten/2017/3/fox-it/fox-it.
23. *Vaststellen van de authenticiteit van de OSV software,* versie: 6-3-2017, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/vaststellen-authenticiteit-osv-software.
24. *Systeemvereisten voor OSV Programma 4 en 5*, versie: 6-3-2017, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/systeemvereisten-voor-osv-programma-4-en-5.
25. *Gedetailleerde specificatie Ondersteunende Software Verkiezingen (OSV); Kiesraad*, versie: 1.5.1, status: gecontroleerd, aangemaakt: 13-10-2008, laatste wijziging: 28-04-2017, zie: www.kiesraad.nl/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-gedetailleerde-specificaties.

26. *Voorwaarden voor gebruik OSV*, versie 19-10-2017, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/voorwaarden-voor-gebruik-osv.
27. *Formele beschrijving van de berekening van de zetelverdeling*, 20-11-2017.
28. *Follow-up bevindingen Fox-IT en aanpassingen OSV gemeenteraadsverkiezingen 2018,* versie: 14-12-2017, zie: www.kiesraad.nl/adviezen-en-publicaties/rapporten/2017/12/15/follow-up-bevindingen-fox-it-en-aanpassingen-osv-gemeenteraadsverkiezingen-en-raadgevend-referendum2018.

A.3 Programmatuur

29. *Sources van OSV*, versie 2.21.1, aangeleverd: 12-12-2017, file: osv45_v2.21.1_source_for_review.
30. *Programma's P0, P1 en P2-3*, versie 2.21.1, aangeleverd: 12-12-2017, file: osv_suite_installer_v2.21.1.
31. *Programma's P4 en P5*, versie 2.21.1, aangeleverd: 12-12-2017, file: osv_programma4en5_installer_v2.21.1.

Bijlage B: Tekenset basisregistratie personen

Volgens wet- en regelgeving dient OSV de tekenset te ondersteunen die is beschreven in het Logisch Ontwerp GBA [8]. De betreffende tekenset is opgenomen in deze bijlage. Tevens is aangegeven in hoeverre de betreffende tekens voldoen aan de toets die we hebben uitgevoerd voor ondersteuning in programma 4 en 5 van OSV.

B.1 Overzicht van de in GBA te gebruiken karakters

In de volgende tabel zijn alle karakters opgesomd, die als teken binnen het GBA-systeem gebruikt mogen worden. In de laatste kolom is aangegeven of het betreffende karakter geslaagd is (V) voor de beschreven test.

T.61 code	UTF-8 code	Char	Omschrijving	Check
20	20	SP	Space	√
21	21	!	Exclamation mark	√
22	22	"	Quotation mark	√
25	25	%	Procent sign	√
26	26	&	Ampersand	√
27	27	'	Apostrophe	√
28	28	(	Left parenthesis	√
29	29	)	Right parenthesis	√
2A	2A	*	Asterisk	√
2B	2B	+	Plus sign	√
2C	2C	,	Comma	√
2D	2D	-	Hyphen or minus sign	√
2E	2E	.	Full stop, period	√
2F	2F	/	Solidus	√
30	30	0	Digit 0	√
31	31	1	Digit 1	√
32	32	2	Digit 2	√
33	33	3	Digit 3	√
34	34	4	Digit 4	√
35	35	5	Digit 5	√
36	36	6	Digit 6	√
37	37	7	Digit 7	√
38	38	8	Digit 8	√
39	39	9	Digit 9	√
3A	3A	:	Colon	√
3B	3B	;	Semicolon	√

T.61 code	UTF-8 code	Char	Omschrijving	Check
3C	3C	<	Less-than sign	√
3D	3D	=	Equals sign	√
3E	3E	>	Greater-than sign	√
3F	3F	?	Question mark	√
40	40	@	Commercial at	√
41	41	A	Capital A	√
42	42	B	Capital B	√
43	43	C	Capital C	√
44	44	D	Capital D	√
45	45	E	Capital E	√
46	46	F	Capital F	√
47	47	G	Capital G	√
48	48	H	Capital H	√
49	49	I	Capital I	√
4A	4A	J	Capital J	√
4B	4B	K	Capital K	√
4C	4C	L	Capital L	√
4D	4D	M	Capital M	√
4E	4E	N	Capital N	√
4F	4F	O	Capital O	√
50	50	P	Capital P	√
51	51	Q	Capital Q	√
52	52	R	Capital R	√
53	53	S	Capital S	√
54	54	T	Capital T	√
55	55	U	Capital U	√

T.61 code	UTF-8 code	Char	Omschrijving	Check
56	56	V	Capital V	√
57	57	W	Capital W	√
58	58	X	Capital X	√
59	59	Y	Capital Y	√
5A	5A	Z	Capital Z	√
5B	5B	[	Left square bracket	√
5D	5D	]	Right square bracket	√
5F	5F	_	Low line	√
61	61	a	Small a	√
62	62	b	Small b	√
63	63	c	Small c	√
64	64	d	Small d	√
65	65	e	Small e	√
66	66	f	Small f	√
67	67	g	Small g	√
68	68	h	Small h	√
69	69	i	Small i	√
6A	6A	j	Small j	√
6B	6B	k	Small k	√
6C	6C	l	Small l	√
6D	6D	m	Small m	√
6E	6E	n	Small n	√
6F	6F	o	Small o	√
70	70	p	Small p	√
71	71	q	Small q	√
72	72	r	Small r	√
73	73	s	Small s	√
74	74	t	Small t	√
75	75	u	Small u	√
76	76	v	Small v	√
77	77	w	Small w	√
78	78	x	Small x	√
79	79	y	Small y	√
7A	7A	z	Small z	√
7C	7C	|	Vertical Bar	√
A1	C2 A1	¡	Inverted exclamation mark	√

T.61 code	UTF-8 code	Char	Omschrijving	Check
A2	C2 A2	¢	Cent sign	√
A3	C2 A3	£	Pound sign	√
A4	24	$	Dollar sign	√
A5	C2 A5	¥	Yen sign	√
A6	23	#	Number sign	√
A7	C2 A7	§	Section sign	√
A8	C2 A4	¤	Currency symbol	√
AB	C2 AB	«	Angle quotation mark left	√
B0	C2 B0	°	Degree sign	√
B1	C2 B1	±	Plus/minus sign	√
B2	C2 B2	²	Superscript 2	√
B3	C2 B3	³	Superscript 3	√
B4	C3 97	×	Multiply sign	√
B5	C2 B5	µ	Micro sign	√
B6	C2 B6	¶	Paragraph sign	√
B7	C2 B7	·	Middle dot	√
B8	C3 B7	÷	Divide sign	√
BB	C2 BB	»	Angle quotation mark right	√
BC	C2 BC	¼	Fraction one quarter	√
BD	C2 BD	½	Fraction one half	√
BE	C2 BE	¾	Fraction three quarters	√
BF	C2 BF	¿	Inverted question mark	√
E0	E2 84 A6	Ω	Ohm sign	√
E1	C3 86	Æ	Capital AE diphtong	√
E2	C4 90	Đ	Capital D with stroke	√
E3	C2 AA	ª	Ordinal indicator, feminine	√
E4	C4 A6	Ħ	Capital H with stroke	√
E7	C4 BF	Ŀ	Capital L with middle dot	√
E8	C5 81	Ł	Capital L with stroke	√
E9	C3 98	Ø	Capital O with slash	√
EA	C5 92	Œ	Capital OE ligature	√
EB	C2 BA	º	Ordinal indicator, masculine	√
EC	C3 9E	Þ	Capital thorn, Icelandic	√
ED	C5 A6	Ŧ	Capital T with stroke	√
EE	C5 8A	Ŋ	Capital eng, Lapp	√
EF	C5 89	ŉ	Small n with apostrophe	√

T.61 code	UTF-8 code	Char	Omschrijving	Check
F0	C4 B8	ĸ	Small k, Greenlandic	√
F1	C3 A6	æ	Small ae, diphtong	√
F2	C4 91	đ	Small d with stroke	√
F3	C3 B0	ð	Small eth, Icelandic	√
F4	C4 A7	ħ	Small h with stroke	√
F5	C4 B1	ı	Small i without dot	√
F7	C5 80	l·	Small l with middle dot	√

T.61 code	UTF-8 code	Char	Omschrijving	Check
F8	C5 82	ł	Small l with stroke	√
F9	C3 B8	ø	Small o with slash	√
FA	C5 93	œ	Small oe ligature	√
FB	C3 9F	ß	Small sharp s, German	√
FC	C3 BE	þ	Small thorn, Icelandic	√
FD	C5 A7	ŧ	Small t with stroke	√
FE	C5 8B	ŋ	Small eng, Lapp	√

B.2 Overzicht van de te gebruiken gecombineerde karakters

De volgende tabel bevat alle gecombineerde karakters, die als teken binnen het GBA-systeem gebruikt mogen worden. In de laatste twee kolommen is aangegeven of de betreffende karakters zijn geslaagd voor de uitgevoerde test.

T.61 Code	UTF-8 code	Char	T.61 Code	UTF-8 code	Char	Naam	Check	
C1 41	C3 80	À	C1 61	C3 A0	à	A grave	√	√
C2 41	C3 81	Á	C2 61	C3 A1	á	A acute	√	√
C3 41	C3 82	Â	C3 61	C3 A2	â	A circumflex	√	√
C4 41	C3 83	Ã	C4 61	C3 A3	ã	A tilde	√	√
C5 41	C4 80	Ā	C5 61	C4 81	ā	A macron	√	√
C6 41	C4 82	Ă	C6 61	C4 83	ă	A breve	√	√
C8 41	C3 84	Ä	C8 61	C3 A4	ä	A diaeresis	√	√
CA 41	C3 85	Å	CA 61	C3 A5	å	A ring	√	√
CE 41	C4 84	Ą	CE 61	C4 85	ą	A ogonek	√	√
C2 43	C4 86	Ć	C2 63	C4 87	ć	C acute	√	√
C3 43	C4 88	Ĉ	C3 63	C4 89	ĉ	C circumflex	√	√
C7 43	C4 8A	Ċ	C7 63	C4 8B	ċ	C dot	√	√
CB 43	C3 87	Ç	CB 63	C3 A7	ç	C cedilla	√	√
CF 43	C4 8C	Č	CF 63	C4 8D	č	C caron	√	√
CF 44	C4 8E	Ď	CF 64	C4 8F	ď	D caron	√	√
C1 45	C3 88	È	C1 65	C3 A8	è	E grave	√	√
C2 45	C3 89	É	C2 65	C3 A9	é	E acute	√	√
C3 45	C3 8A	Ê	C3 65	C3 AA	ê	E circumflex	√	√
C5 45	C4 92	Ē	C5 65	C4 93	ē	E macron	√	√
C7 45	C4 96	Ė	C7 65	C4 97	ė	E dot	√	√

T.61 Code	UTF-8 code	Char	T.61 Code	UTF-8 code	Char	Naam	Check	
C8 45	C3 8B	Ë	C8 65	C3 AB	ë	E diaeresis	√	√
CE 45	C4 98	Ę	CE 65	C4 99	ę	E ogonek	√	√
CF 45	C4 9A	Ě	CF 65	C4 9B	ě	E caron	√	√
			C2 67	C4 A3	ģ	G cedilla (vroeger G acute)		√
C3 47	C4 9C	Ĝ	C3 67	C4 9D	ĝ	G circumflex	√	√
C6 47	C4 9E	Ğ	C6 67	C4 9F	ğ	G breve	√	√
C7 47	C4 A0	Ġ	C7 67	C4 A1	ġ	G dot	√	√
CB 47	C4 A2	Ģ				G cedilla	√	
C3 48	C4 A4	Ĥ	C3 68	C4 A5	ĥ	H circumflex	√	√
C1 49	C3 8C	Ì	C1 69	C3 AC	ì	I grave	√	√
C2 49	C3 8D	Í	C2 69	C3 AD	í	I acute	√	√
C3 49	C3 8E	Î	C3 69	C3 AE	î	I circumflex	√	√
C4 49	C4 A8	Ĩ	C4 69	C4 A9	ĩ	I tilde	√	√
C5 49	C4 AA	Ī	C5 69	C4 AB	ī	I macron	√	√
C7 49	C4 B0	İ				I dot	√	
C8 49	C3 8F	Ï	C8 69	C3 AF	ï	I diaeresis	√	√
CE 49	C4 AE	Į	CE 69	C4 AF	į	I ogonek	√	√
C3 4A	C4 B4	Ĵ	C3 6A	C4 B5	ĵ	J circumflex	√	√
CB 4B	C4 B6	Ķ	CB 6B	C4 B7	ķ	K cedilla	√	√

T.61 Code	UTF-8 code	Char	T.61 Code	UTF-8 code	Char	Naam	Check	
C2 4C	C4 B9	Ĺ	C2 6C	C4 BA	ĺ	L acute	√	√
CB 4C	C4 BB	Ļ	CB 6C	C4 BC	ļ	L cedilla	√	√
CF 4C	C4 BD	Ľ	CF 6C	C4 BE	ľ	L caron	√	√
C2 4E	C5 83	Ń	C2 6E	C5 84	ń	N acute	√	√
C4 4E	C3 91	Ñ	C4 6E	C3 B1	ñ	N tilde	√	√
CB 4E	C5 85	Ņ	CB 6E	C5 86	ņ	N cedilla	√	√
CF 4E	C5 87	Ň	CF 6E	C5 88	ň	N caron	√	√
C1 4F	C3 92	Ò	C1 6F	C3 B2	ò	O grave	√	√
C2 4F	C3 93	Ó	C2 6F	C3 B3	ó	O acute	√	√
C3 4F	C3 94	Ô	C3 6F	C3 B4	ô	O circumflex	√	√
C4 4F	C3 95	Õ	C4 6F	C3 B5	õ	O tilde	√	√
C5 4F	C5 8C	Ō	C5 6F	C5 8D	ō	O macron	√	√
C8 4F	C3 96	Ö	C8 6F	C3 B6	ö	O diaeresis	√	√
CD 4F	C5 90	Ő	CD 6F	C5 91	ő	O double acute	√	√
C2 52	C5 94	Ŕ	C2 72	C5 95	ŕ	R acute	√	√
CB 52	C5 96	Ŗ	CB 72	C5 97	ŗ	R cedilla	√	√
CF 52	C5 98	Ř	CF 72	C5 99	ř	R caron	√	√
C2 53	C5 9A	Ś	C2 73	C5 9B	ś	S acute	√	√
C3 53	C5 9C	Ŝ	C3 73	C5 9D	ŝ	S circumflex	√	√
CB 53	C5 9E	Ş	CB 73	C5 9F	ş	S cedilla	√	√

T.61 Code	UTF-8 code	Char	T.61 Code	UTF-8 code	Char	Naam	Check	
CF 53	C5 A0	Š	CF 73	C5 A1	š	S caron	√	√
CB 54	C5 A2	Ţ	CB 74	C5 A3	ţ	T cedilla	√	√
CF 54	C5 A4	Ť	CF 74	C5 A5	ť	T caron	√	√
C1 55	C3 99	Ù	C1 75	C3 B9	ù	U grave	√	√
C2 55	C3 9A	Ú	C2 75	C3 BA	ú	U acute	√	√
C3 55	C3 9B	Û	C3 75	C3 BB	û	U circumflex	√	√
C4 55	C5 A8	Ũ	C4 75	C5 A9	ũ	U tilde	√	√
C5 55	C5 AA	Ū	C5 75	C5 AB	ū	U macron	√	√
C6 55	C5 AC	Ŭ	C6 75	C5 AD	ŭ	U breve	√	√
C8 55	C3 9C	Ü	C8 75	C3 BC	ü	U diaeresis	√	√
CA 55	C5 AE	Ů	CA 75	C5 AF	ů	U ring	√	√
CD 55	C5 B0	Ű	CD 75	C5 B1	ű	U double acute	√	√
CE 55	C5 B2	Ų	CE 75	C5 B3	ų	U ogonek	√	√
C3 57	C5 B4	Ŵ	C3 77	C5 B5	ŵ	W circumflex	√	√
C2 59	C3 9D	Ý	C2 79	C3 BD	ý	Y acute	√	√
C3 59	C5 B6	Ŷ	C3 79	C5 B7	ŷ	Y circumflex	√	√
C8 59	C5 B8	Ÿ	C8 79	C3 BF	ÿ	Y diaeresis	√	√
C2 5A	C5 B9	Ź	C2 7A	C5 BA	ź	Z acute	√	√
C7 5A	C5 BB	Ż	C7 7A	C5 BC	ż	Z dot	√	√
CF 5A	C5 BD	Ž	CF 7A	C5 BE	ž	Z caron	√	√

Bijlage C: Kritische functies; percentageberekeningen

In deze bijlage volgen we in de code de berekeningen voor het opkomstpercentage en de percentages voor- en tegenstemmen bij een referendum.

De leverancier heeft aangegeven dat de percentages worden berekend in de documentgenerator. De gegevens komen uit het gegenereerde XML-bestand. De percentages worden weergegeven als breuk (zodat er geen afronding plaatsvindt). De omzetting van de procentuele waarde naar een breuk wordt via XSLT uitgevoerd. Voor PDF en RTF zijn dit twee verschillende bestanden, respectievelijk Wrr83-to-FO.xslt en Wrr83-to-RTF.xslt. In elk formateringsbestand is een template voor de breuk opgenomen, dat begint met `<xsl:template name="Fraction">`. De aanroepen van de template beginnen met `<xsl:call-template name="Fraction">`.

Het template voor formatering van de breuk is als volgt voor Wrr83-to-FO.xslt:

```
<xsl:template name="Fraction">
   <xsl:param name="x" select="&apos;&apos;"/>
   <xsl:param name="y" select="&apos;&apos;"/>
   <fo:inline font-family="Arial" font-size="9pt" font-weight="bold">
      <xsl:value-of select="floor( $x div $y )"/>
   </fo:inline>
   <xsl:if test="$x mod $y &gt; 0">
      <fo:inline font-family="Arial" font-size="9pt" font-weight="bold">
         <xsl:text> </xsl:text>
      </fo:inline>
      <fo:inline font-family="Arial" font-size="9pt" font-weight="bold">
         <xsl:value-of select="$x mod $y"/>
      </fo:inline>
      <fo:inline font-family="Arial" font-size="9pt" font-weight="bold">
         <xsl:text>/</xsl:text>
      </fo:inline>
      <fo:inline font-family="Arial" font-size="9pt" font-weight="bold">
         <xsl:value-of select="$y"/>
      </fo:inline>
   </xsl:if>
</xsl:template>
```

Voor Wrr83-to-RTF.xslt is de formatering van de breuk als volgt.

```
<xsl:template name="Fraction">
   <xsl:param name="altova:nMaxWidthIn" select="6.26389"/>
   <xsl:param name="templatetablelevel" select="0"/>
   <xsl:param name="x" select="&apos;&apos;"/>
   <xsl:param name="y" select="&apos;&apos;"/>
   <xsl:text>{\f1\fs18\b </xsl:text>
   <xsl:call-template name="write-text">
      <xsl:with-param name="text">
```

```
        <xsl:value-of select="floor( $x div $y )"/>
      </xsl:with-param>
    </xsl:call-template>
    <xsl:text>}</xsl:text>
    <xsl:if test="$x mod $y &gt; 0">
      <xsl:text>{\f1\fs18\b </xsl:text>
      <xsl:call-template name="write-text">
        <xsl:with-param name="text">
          <xsl:text> </xsl:text>
        </xsl:with-param>
      </xsl:call-template>
      <xsl:text>}</xsl:text>
      <xsl:text>{\f1\fs18\b </xsl:text>
      <xsl:call-template name="write-text">
        <xsl:with-param name="text">
          <xsl:value-of select="$x mod $y"/>
        </xsl:with-param>
      </xsl:call-template>
      <xsl:text>}</xsl:text>
      <xsl:text>{\f1\fs18\b </xsl:text>
      <xsl:call-template name="write-text">
        <xsl:with-param name="text">
          <xsl:text>/</xsl:text>
        </xsl:with-param>
      </xsl:call-template>
      <xsl:text>}</xsl:text>
      <xsl:text>{\f1\fs18\b </xsl:text>
      <xsl:call-template name="write-text">
        <xsl:with-param name="text">
          <xsl:value-of select="$y"/>
        </xsl:with-param>
      </xsl:call-template>
      <xsl:text>}</xsl:text>
    </xsl:if>
  </xsl:template>
```

Beide templates zijn duidelijk verschillend. Het merendeel van het template zorgt voor de formattering van de gegevens. Als we de formatteringscommando's verwijderen, houden we de volgende commando's over voor de berekening van de breuk. Deze commando's zijn voor beide templates identiek.

```
  <xsl:template name="Fraction">
    <xsl:param name="x" select="&apos;&apos;"/>
    <xsl:param name="y" select="&apos;&apos;"/>
      <xsl:value-of select="floor( $x div $y )"/>
    <xsl:if test="$x mod $y &gt; 0">
          <xsl:value-of select="$x mod $y"/>
          <xsl:text>/</xsl:tekst>
```

```
          <xsl:value-of select="$y"/>
```

Dit is een correct algoritme om het percentage als breuk weer te geven. De breuk wordt daarbij niet vereenvoudigd.

Voor berekening van het opkomstpercentage wordt dit template als volgt toegepast:

```
  <xsl:call-template name="Fraction">
     <xsl:with-param name="x" select="100 * (eml:TotalCounted +
        eml:RejectedVotes[@ReasonCode=&quot;blanco&quot;] +
        eml:RejectedVotes[@ReasonCode=&quot;ongeldig&quot;])"/>
     <xsl:with-param name="y" select="eml:Cast"/>
     …
  </xsl:call-template>
```

Voor berekening van de percentages voor- en tegenstemmen wordt het template als volgt toegepast.

```
  <xsl:call-template name="Fraction">
     <xsl:with-param name="x" select="100 * $validVotes"/>
     <xsl:with-param name="y" select="eml:TotalCounted +
        eml:RejectedVotes[@ReasonCode=&quot;blanco&quot;]"/>
     …
  </xsl:call-template>
```

Om te toetsen of de percentageberekening te volgen is door de code, hebben we gezocht naar de code die de `eml:RejectedVotes` oplevert. Dit gebeurt in het programma `EML510Helper` met de private methode `appendGeneralVotingResults`. Deze code is niet te begrijpen zonder nadere toelichting. Het toelichtend commentaar bij deze code is onvoldoende om de werking van de methode te kunnen begrijpen.

```
  // <Cast>13011</Cast>
  // <TotalCounted>6480</TotalCounted>
  // <RejectedVotes ReasonCode="blanco">0</RejectedVotes>
  // <RejectedVotes ReasonCode="ongeldig">13</RejectedVotes>

  private void appendGeneralVotingResults(Element result,
      Gebiet region,
      String id_Ergebniseingang,
      boolean emptyResults) {
    GruppeAllgemeinXmlAdapter adapter = new GruppeAllgemeinXmlAdapter();
    List<GruppeAllgemein> gruppenAllgemein = GruppeKonstanten.GruppeAllgemein
        .filterGruppenAllgemeinVisibleInRegionOrGueltige(region,
adapter.getGruppenAllgemein());

    if (emptyResults) {
      for (GruppeAllgemein gruppeAllgemein : gruppenAllgemein) {
        adapter.putEmlXml(result, gruppeAllgemein, 0);
```

```
      }
    } else {
      GeneralVotingResults generalVotingResults = bean.getVotesHandling()
          .getGeneralVotingResults(id_Ergebniseingang, region.getID_Gebiet());
      for (GruppeAllgemein gruppeAllgemein : gruppenAllgemein) {
        int value = generalVotingResults.getVotes(gruppeAllgemein);
        adapter.putEmlXml(result, gruppeAllgemein, value);
      }
    }
  }
```

Deze methode wordt slechts op één plek binnen de class `EML510Helper` gebruikt en wel binnen de private methode `appendCandidateResults`. Uit de naamgeving van deze methode blijkt dat methodes voor het optellen van het aantal stemmen per kandidaat zijn gebruikt voor de realisatie van de referendumsoftware. Bij een referendum is geen sprake van kandidaten. Daarmee wordt het algoritme om de totaalpercentages voor een referendum te berekenen niet meer te volgen door de code.

```
  /**
   * @param emptyResults true if all results should be zero
   */
  private void appendCandidateResults(String id_Ergebniseingang,
      Gebiet region,
      Element result,
      boolean emptyResults,
      EMLMessageType emlType) throws FinderException {
    Long start = new Date().getTime();

    String id_Gebiet = region.getID_Gebiet();
    // Find lists for that region
    Collection<Liste> listCol;
    if (region.getGebietsart() < WahlInfo.getWahlInfo().getGebietsartMitListen()) {
      // We are at root region without lists and have to use all lists in that case
      listCol = bean.getListeHome().findAll();
    } else {
      listCol = bean.getListeHome().findAllByGebiet(id_Gebiet);
    }
    List<Liste> lists = new ArrayList<Liste>(listCol);
    // Sort lists by Affiliation Id
    Collections.sort(lists, new Comparator<Liste>() {
      @Override
      public int compare(Liste x, Liste y) {
        return Integer.signum(x.getGruppe().getSchluessel() - y.getGruppe().getSchluessel());
      }
    });
    for (Liste list : lists) {
      appendCandidateVotingResults(result,
          list,
```

```
            id_Gebiet,
            id_Ergebniseingang,
            emptyResults,
            emlType);
    }
    appendGeneralVotingResults(result, region, id_Ergebniseingang, emptyResults);
    System.out.print("appendCandidateResults in ms: " + (new Date().getTime() - start));
//$NON-NLS-1$
  }
```