



Toetsing Verkiezingssoftware OSV2020 aan het Wettelijk Kader

Eindrapportage

Auteurs: Paul Hendriks / Rob Hendrix / Tania Klemenova
Expleo Netherlands
Van Deventerlaan 31 – 51
3528 AG Utrecht
T +31 (0)88 655 88 80
M +31 (0)6 51 21 72 55
E paul.hendriks@expleogroup.com

Datum: 30 januari 2023
Versie: 1.0
Status: definitief

Managementsamenvatting

Op verzoek van de Kiesraad is de Ondersteunende Software Verkiezingen (OSV2020) 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 Kiesregeling.

De toetsing is uitgevoerd voor de ondersteuning van

- Provinciale statenverkiezingen en
- Waterschapsverkiezingen.

Beoordeling

Op hoofdlijnen voldoet het programma OSV2020-U aan de daaraan in de Kieswet gestelde eisen.

Wat betreft de functionaliteit die nodig is voor de berekening van de uitslag van de verkiezingen en de zetelverdeling constateren we:

- Er zijn geen functionele onvolkomenheden geconstateerd ten opzichte van wat van de software verwacht wordt.
- Uit analyse van de formele beschrijving blijkt dat deze consequenties heeft die niet in lijn zijn met de Kieswet en het kiesstelsel. Dit betreft de behandeling van lijstgroepen en stellen gelijklopende lijsten. Een interpretatie van de formele beschrijving is nodig om vast te stellen dat OSV2020 conform specificatie werkt.

Bij twee van de overige twaalf gestelde niet-functionele eisen zien we verbetermogelijkheden:

- *Modulaire aanpassingen*: Een geactualiseerde architectuurbeschrijving ontbreekt. Een gelaagde structuur en de heldere componentindeling zijn onvoldoende terug te vinden in de structuur van de software. Voor het gebruik van OSV2020 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)*: De kritische functies zijn onvoldoende herkenbaar omdat niet gedocumenteerd is welke methodes deze functies implementeren. De implementaties zijn nauwelijks van elkaar gescheiden. De call graphs laten zien dat het niet eenvoudig is om de kritische functies zelfstandig door de programmatuur te volgen.

Aanbevelingen

Bij het testen van de functionaliteit van OSV2020-U voor de berekening van de uitslag van de verkiezingen en de zetelverdeling constateren we dat een heldere interpretatie van de formele beschrijving nodig is om testcases voor de behandeling van lijstgroepen en stellen gelijklopende lijsten te kunnen bepalen. We adviseren om die interpretatie vast te leggen in een aanpassing van de formele beschrijving.

Verder adviseren we de volgende verbetermaatregelen door te voeren voor de niet-functionele eisen die aan de software in het wettelijk kader worden gesteld:

- *Modulaire aanpassingen:* Actualiseer de architectuurbeschrijving van OSV2020 zodat deze aansluit bij de gerealiseerde software. Maak daarbij helder onderscheid tussen het maatwerk dat voor de Nederlandse situatie is gerealiseerd en de overige componenten. Verbeter de modulaire structuur van OSV2020 zodat deze beter aansluit bij de dan beschreven architectuur. Documenteer eventuele afwijkingen in de relatie tussen de beschreven softwarearchitectuur en de modulaire structuur van de software. Onderzoek de metingen met risicovolle scores en verbeter geconstateerde issues. Met deze maatregelen kan beheer en onderhoud van OSV2020 efficiënter worden doorgevoerd.
- *Kritische functies:* Documenteer de kritische functies en waar in de source code de implementatie van de kritische functies te vinden is. Verbeter de traceerbaarheid van de code van kritische functies door in het codecommentaar helderder te beschrijven wat de betreffende methode doet, welke resultaten worden opgeleverd (post condities), wat de voorwaarden zijn waaraan de methode moet voldoen (pre condities), en hoe de berekeningen worden uitgevoerd.

Inhoudsopgave

| | |
|---|-----------|
| Managementsamenvatting | 2 |
| Beoordeling | 2 |
| Aanbevelingen | 2 |
| 1. Achtergrond Toets OSV2020 | 6 |
| 1.1 Achtergrond en vraagstelling..... | 6 |
| 1.2 Toetskader..... | 7 |
| 1.3 Toetsuitvoering | 8 |
| 1.4 Leeswijzer | 12 |
| 2. Samenvattend resultaat en aanbevelingen | 13 |
| 2.1 Samenvattend oordeel | 13 |
| 2.2 Aanbevelingen..... | 14 |
| 2.3 Samenvattend testresultaat | 15 |
| 2.4 Samenvattende beoordeling eisen..... | 17 |
| 3. Functionele test OSV2020..... | 21 |
| 3.1 Testbasis voor de testen | 21 |
| 3.2 Testaanpak | 21 |
| 3.2.1 Logische testcases zonder lijstgroepen en gelijkkluidende lijsten | 22 |
| 3.2.2 Logische testcases met lijstgroepen en gelijkkluidende lijsten | 23 |
| 3.3 Testresultaten zonder lijstgroepen en gelijkkluidende lijsten | 25 |
| 3.3.1 Provinciale Staten met één kieskring..... | 26 |
| 3.3.2 Provinciale Staten met meerdere kieskringen | 27 |
| 3.3.3 Waterschappen minder dan 19 zetels..... | 28 |
| 3.3.4 Waterschappen met 19 of meer zetels | 29 |
| 3.4 Testresultaten met lijstgroepen en gelijkkluidende lijsten | 30 |
| 4. Oordeel per eis | 31 |
| 4.1 Functionaliteit | 31 |
| 4.2 Modulaire aanpassingen | 31 |
| 4.3 Kritische functies | 34 |
| 4.4 Soorten verkiezingen | 39 |
| 4.5 Voorkomen foutief gebruik | 41 |
| 4.6 Diakritische tekens..... | 43 |
| 4.7 Open source en standaarden | 44 |
| 4.8 Vrij verkrijgbare standaard programmatuur | 46 |

| | | |
|----------------|---|-----------|
| 4.9 | Intellectueel eigendom | 47 |
| 4.10 | Open source compiler..... | 48 |
| 4.11 | Vershillende besturingssystemen..... | 49 |
| 4.12 | Authenticiteit programmatuur | 50 |
| 4.13 | Authenticiteit aangeleverde gegevens..... | 51 |
| Annex A | Bronmateriaal..... | 56 |
| A.1 | Wet- en regelgeving..... | 56 |
| A.2 | Documenten | 56 |
| A.3 | Programmatuur | 58 |
| Annex B | Testen met lijstgroepen en gelijklopende lijsten | 59 |
| B.1 | Test met één partij met identieke lijst in twee kieskringen | 59 |
| B.2 | Test met twee stellen identieke lijsten in twee kieskringen..... | 61 |
| B.3 | Test met één partij met identieke kandidatenlijst met verschillende partijnaam..... | 63 |
| B.4 | Test met varianten van lijstgroepen en stellen gelijklopende lijsten | 64 |
| Annex C | Inzet van CAST tools..... | 70 |
| C.1 | CAST AIP | 70 |
| C.2 | Omvang OSV2020-U | 71 |
| C.3 | Scores voor Wijzigbaarheid | 73 |
| C.4 | Scores voor Beveiliging | 76 |
| C.5 | Applicatiestructuurvisualisaties | 88 |
| Annex D | Tekenset basisregistratie personen | 91 |
| D.1 | Overzicht van de te gebruiken Teletex-tekens | 91 |
| D.2 | Overzicht van de te gebruiken gecombineerde Teletex-tekens..... | 94 |

1. Achtergrond Toets OSV2020

1.1 Achtergrond en vraagstelling

Ter ondersteuning van verkiezingen wordt gebruik gemaakt van software die moet voldoen aan de eisen die in de Kieswet daaraan worden gesteld. Dit betreft met name de software die gebruikt wordt voor het vaststellen van de officiële verkiezingsuitslag en de zetelverdeling. Om het vertrouwen in het verkiezingsresultaat en het proces dat heeft geleid tot dat resultaat te waarborgen wordt een onafhankelijke partij gevraagd de software te toetsen aan het wettelijk kader. Het resulterend toetsrapport wordt tijdig voor verkiezingen openbaar gepubliceerd op de website van de Kiesraad om transparantie te bevorderen.

Dit rapport vormt het resultaat van de toetsing die in oktober 2022 tot en met januari 2023 is uitgevoerd voor de verkiezingssoftware OSV2020 (Ondersteunende Software Verkiezingen). Deze toetsing is specifiek uitgevoerd voor:

- de Provinciale statenverkiezingen die georganiseerd worden op 15 maart 2023,
- de Waterschapsverkiezingen die tegelijkertijd plaatsvinden.

De eerste versie van de Ondersteunende Software Verkiezingen (hierna OSV) is in 2009 in opdracht van de Kiesraad ontwikkeld. In 2020 is de bestaande versie vervangen door vernieuwde software. De te toetsen verkiezingssoftware betreft de delen van deze vernieuwde versie die gebruikt worden bij de vaststelling van de verkiezingsuitslag en de zetelverdeling. Voor het huidige OSV (verder: OSV2020) betreft dit de module OSV2020-U.

Op grond van het Kiesbesluit¹ [2] en bijbehorende regelingen dient de toetsing van verkiezingssoftware 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 de eisen die aan de software worden gesteld volgens de bijlage bij art. 2a van de Kiesregeling.

Dit onderzoek continueert de eerdere samenwerking van Expleo en haar voorganger SQS met de Kiesraad. Eerder heeft SQS in opdracht van de Kiesraad toetsen van OSV aan het wettelijk kader uitgevoerd.

- Eind 2014 / begin 2015 hebben we voor het eerst een toetsing van OSV uitgevoerd (zie [12]) 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 [13].
- 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 van OSV daarvoor uit te voeren (zie [16]).
- Expleo heeft in augustus/september 2020 de toetsing van OSV2020-U eerst uitgevoerd voor de ondersteuning van Gemeenteraadsverkiezingen. Aanvullend is in januari 2021 specifiek de ondersteuning voor Tweede Kamerverkiezingen getoetst [20].

¹. Zie: wetten.overheid.nl/BWBR0004632/2022-10-01/0#AfdelingII_HoofdstukP.

De software is op een aantal punten aangepast. De belangrijkste zijn:

- Beveiligingsaspecten van OSV2020-U zijn verbeterd.
- OSV2020-U is aangepast aan veranderingen in de wetgeving die ondertussen in werking zijn getreden. Het betreft met name wijzigingen die voortkomen uit de wetswijziging Nieuwe Procedure Vaststellen Verkiezingsuitslag (NPVV) [8].

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:

4. 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:

- *Formele beschrijving van de berekening van de zetelverdeling*, 20-11-2017 [15].

Deze specificatie is in detail uitgewerkt in mathematische notaties in:

- *Determination of the Election Result*, Joachim Nottebaum, versie 7.3, 01-10-2020 [19].

In de Kiesregeling [3] zijn in Bijlage 2² 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:

1. *Functionaliteit*: 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;
2. *Modulaire aanpassingen*: de programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn;
3. *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;
4. *Soorten verkiezingen*: de programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen;
5. *Voorkomen foutief gebruik*: toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen;

². Zie: wetten.overheid.nl/BWBR0034180/2022-10-01#Bijlage2.

6. *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;
7. *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 verkiezingsgegevens zoals kandidatenlijsten en zetelverdeling wordt de EML_NL standaard toegepast;
8. *Vrij verkrijgbare standaard programmatuur*: de standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar;
9. *Intellectueel eigendom*: het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau;
10. *Open source compiler*: de programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is;
11. *Verskillende besturingssystemen*: de programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem;
12. *Authenticiteit programmatuur*: het is mogelijk de authenticiteit van de programmatuur vast te stellen; en
13. *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 een ministeriële regeling [7] is in 2014 een toelichting gegeven op de geformuleerde wettelijke eisen. Deze toelichting wordt als uitgangspunt genomen bij nadere interpretatie van de eisen.

1.3 Toetsuitvoering

Dit rapport is het resultaat van de toetsing van OSV2020 die in oktober 2022 tot en met januari 2023 is uitgevoerd voor

- de Provinciale statenverkiezingen,
- de Waterschapsverkiezingen.

Omdat gedurende de toetsperiode aanpassingen in OSV2020-U zijn doorgevoerd is gestart met uitvoering van de toets voor de op 30 september 2022 aangeleverde versie (zie 'A.3 Programmatuur', [31]). De rapportage is gebaseerd op de toets van versie 1.8.2.3 die op 7 december 2022 is aangeleverd [33].

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 verificatie aangeboden aan de opdrachtgever. Opmerkingen daaruit zijn door ons beoordeeld en indien van toepassing in deze definitieve versie van het toetsingsrapport verwerkt.

OSV is oorspronkelijk ontwikkeld door IVU (IVU Traffic Technologies AG, zie: www.ivu.com) op basis van een bestaand softwarepakket voor verkiezingen. IVU.elect is in 2020 overgenomen door elect iT³ (onderdeel van vote iT, zie www.elect-it.com). Zij zorgen voor beheer en onderhoud (correctief en adaptief) van OSV2020. De

³. Zie: www.itcs-info.de/index.php/news/567-ivu-verkauf-der-tochter-fuer-wahlsoftware.

Nederlandse vertegenwoordiging van elect iT treedt op als contactpersoon namens de leverancier voor dit onderzoek.

OSV2020 bestaat uit meerdere modules. Figuur 1 en Figuur 2 zijn overgenomen uit de handleiding van OSV2020-U [26] en bevatten een overzicht van de modules van OSV2020 met bestands- en documentstromen tussen de diverse modules. De modules van OSV2020 die gebruikt worden door politieke partijen voor het samenstellen van de kandidatenlijsten (OSV2020-PP) en door het centraal stembureau voor het vaststellen van de kandidaatstelling (OSV2020-KS) vallen buiten de scope van deze toetsing. Deze toetsing betreft de software voor vaststelling van de officiële uitslag en zetelverdeling die wordt ondersteund door OSV2020-U.

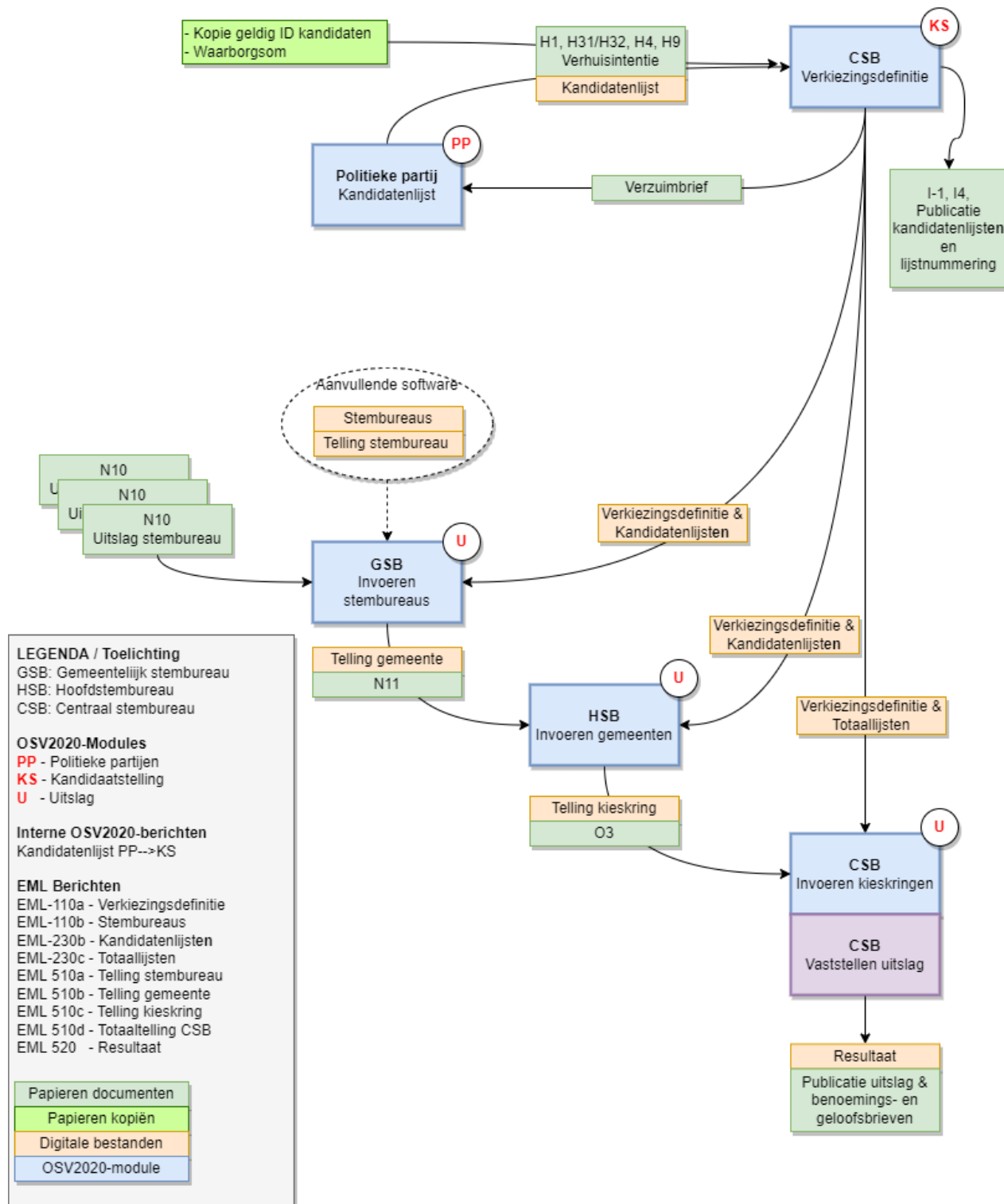
De uitvoering van de toets bestaat uit twee delen:

- *Toetsen specificaties:* Voor OSV2020-U 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 dekkinggraad van de uitgevoerde testen is geregistreerd.
- *Toetsen eisen:* We hebben beoordeeld in hoeverre OSV2020-U voldoet aan de eisen die in de bijlage van de Kiesregeling 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'.

Bij het toetsen van de eisen is gebruikgemaakt van de statische code-analyse tools CAST Highlight, CAST Application Intelligence Platform en CAST Imaging (zie: www.castsoftware.com).

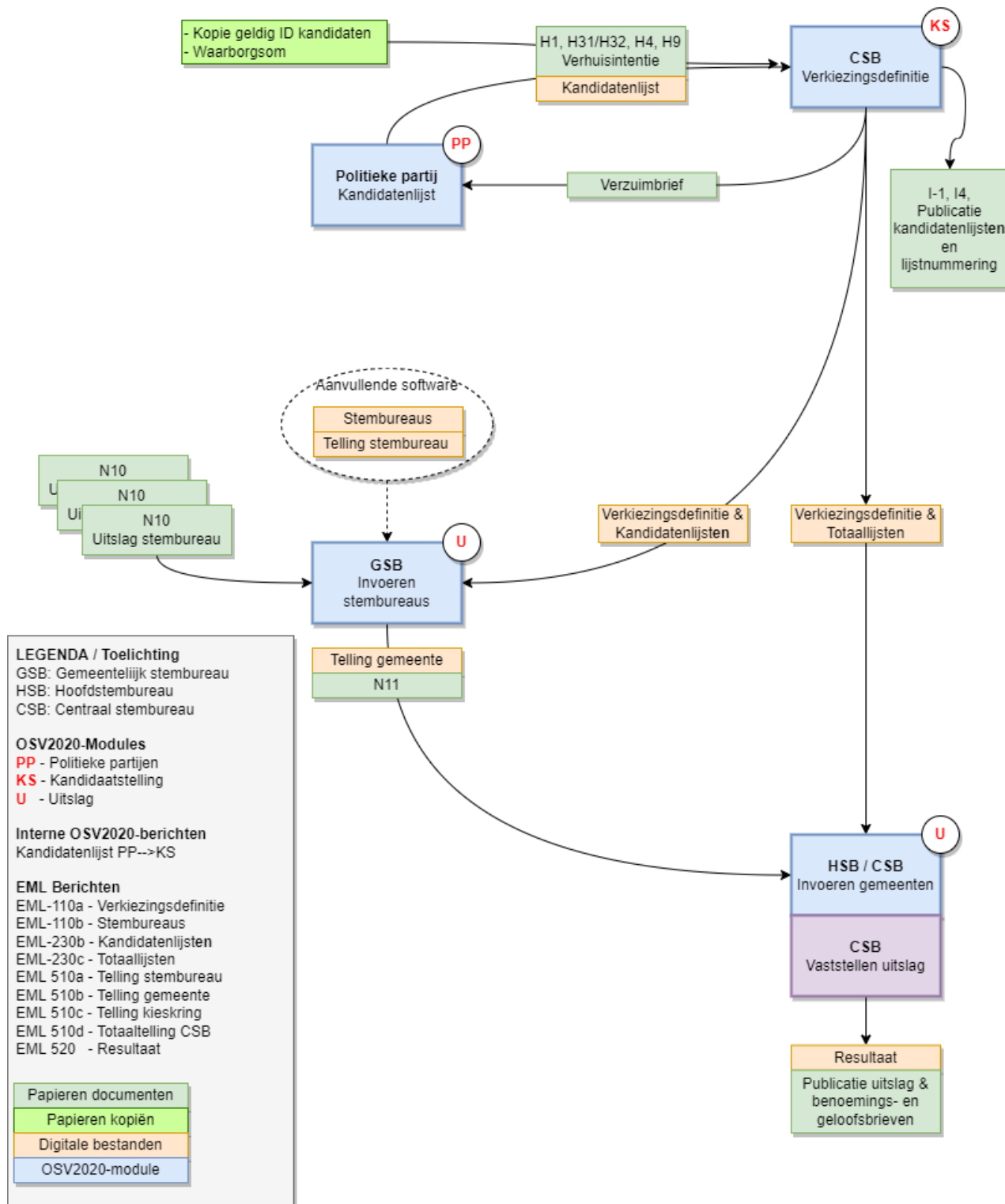


OSV2020 Bestands- en documentstromen



Figuur 1: Berichtenschema OSV2020-U voor verkiezingen met meerdere kieskringen zoals voor Provinciale Staten (bron: [26, pagina 5]).

OSV2020 Bestands- en documentstromen bij verkiezingen voor PS1 en AB



Figuur 2: Berichtenschema OSV2020-U bij verkiezingen voor Provinciale Staten met één kieskring of het algemeen bestuur van een waterschap (bron: [26, pagina 6]).

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 Kiesregeling moet voldoen. Tevens doen we aanbevelingen voor verbetering.
- *Hoofdstuk 3, Functionele test OSV2020:* In dit hoofdstuk worden de testen beschreven die zijn uitgevoerd om te verifiëren of OSV2020-U de berekeningen conform specificaties uitvoert.
- *Hoofdstuk 3.4, Oordeel per eis:* Voor elke eis uit de bijlage van de Kiesregeling wordt in dit hoofdstuk beschreven wat onze bevindingen zijn die hebben geleid tot ons oordeel over de mate waarin OSV2020-U voldoet aan de betreffende eis.
- *Bijlages:* Hier vindt u
 - een lijst van het gebruikte bronmateriaal (Annex A);
 - uitgewerkte voorbeelden van testen met lijstgroepen en gelijkkluidende lijsten (Annex B);
 - een beschrijving van de inzet van CAST en de resultaten daarvan (Annex C);
 - de getoetste karakterset voor het gebruik van diakritische tekens in OSV2020-U (Annex D).

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 Kiesregeling moet voldoen (2.4).

2.1 Samenvattend oordeel

Wat betreft de functionaliteit die nodig is voor de berekening van de uitslag van de verkiezingen en de zetelverdeling constateren we:

- Er zijn geen functionele onvolkomenheden geconstateerd ten opzichte van wat van de software verwacht wordt.
- Uit analyse van de formele beschrijving [15] blijkt dat deze consequenties heeft die niet in lijn zijn met de Kieswet en het kiesstelsel. Dit betreft de behandeling van lijstgroepen en stellen gelijkkluidende lijsten. Een interpretatie van de formele beschrijving is nodig om vast te stellen dat OSV2020 conform specificatie werkt. Door de Kiesraad is daartoe een toelichting gegeven. Daarmee blijkt dat het resultaat van OSV2020-U conform de interpretatie is die daaraan gegeven moet worden.

Bij twee van de overige twaalf gestelde niet-functionele eisen zien we verbetermogelijkheden:

- *Modulaire aanpassingen (eis 2, zie 4.2)*: Een geactualiseerde architectuurbeschrijving ontbreekt. Een gelaagde structuur en de heldere componentindeling zijn onvoldoende terug te vinden in de structuur van de software. Voor het gebruik van OSV2020 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)*: De kritische functies zijn onvoldoende herkenbaar omdat niet gedocumenteerd is welke methodes deze functies implementeren. De implementaties zijn nauwelijks van elkaar gescheiden. De call graphs laten zien dat het niet eenvoudig is om de kritische functies zelfstandig door de programmatuur te volgen.

Samenvattend is de mate waarin OSV2020-U voldoet aan de eisen uit de Kiesregeling door ons als volgt beoordeeld.

| Nr. | Onderwerp | Oordeel |
|-----|----------------------------|---------|
| 1. | Functionaliteit | <KG> |
| 2. | Modulaire aanpassingen | <KG> |
| 3. | Kritische functies | <KG> |
| 4. | Soorten verkiezingen | <OK> |
| 5. | Voorkomen foutief gebruik | <OK> |
| 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 OSV2020 voldoet aan de eisen uit de bijlage bij art. 2a van de Kiesregeling.

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: OSV2020 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 OSV2020. |
| <GG> | Groot gebrek: voor de betreffende eis zijn één of meerdere grote gebreken geconstateerd, die merkbaar impact hebben bij gebruik, onderhoud of beheer van OSV2020. |

Tabel 2: Kleuren en codering toetsresultaat.

2.2 Aanbevelingen

Bij het testen van de functionaliteit van OSV2020-U voor de berekening van de uitslag van de verkiezingen en de zetelverdeling constateren we dat een heldere interpretatie van de formele beschrijving nodig is om testcases voor de behandeling van lijstgroepen en stellen gelijklopende lijsten te kunnen bepalen. We adviseren om die interpretatie vast te leggen in een aanpassing van de formele beschrijving.

Verder adviseren we de volgende verbetermaatregelen door te voeren voor de niet-functionele eisen die aan de software in het wettelijk kader worden gesteld:

- *Modulaire aanpassingen (eis 2, zie 4.2)*: Actualiseer de architectuurbeschrijving van OSV2020 zodat deze aansluit bij de gerealiseerde software. Maak daarbij helder onderscheid tussen het maatwerk dat voor de Nederlandse situatie is gerealiseerd en de overige componenten. Verbeter de modulaire structuur van OSV2020 zodat deze beter aansluit bij de dan beschreven architectuur. Documenteer eventuele afwijkingen in de relatie tussen de beschreven softwarearchitectuur en de modulaire structuur van de software. Onderzoek de metingen met risicovolle scores en verbeter geconstateerde issues. Met deze maatregelen kan beheer en onderhoud van OSV2020 efficiënter worden doorgevoerd.
- *Kritische functies (eis 3, zie 4.3)*: Documenteer de kritische functies en waar in de source code de implementatie van de kritische functies te vinden is. Verbeter de traceerbaarheid van de code van kritische functies door in het codecommentaar helderder te beschrijven wat de betreffende methode doet, welke resultaten worden opgeleverd (post condities), wat de voorwaarden zijn waaraan de methode moet voldoen (pre condities), en hoe de berekeningen worden uitgevoerd.

2.3 Samenvattend testresultaat

Wat betreft de functionaliteit die nodig is voor de berekening van de uitslag van de verkiezingen en de zetelverdeling constateren we dat er geen functionele onvolkomenheden geconstateerd zijn ten opzichte van wat van de software verwacht wordt.

Er zijn geen bevindingen geconstateerd bij de uitgevoerde testen voor verkiezingen waarin de groepering van kieslijsten niet voorgeschreven is. Dit betreft de verkiezingen voor:

- Provinciale staten in provincies met één kieskring
- Algemeen Bestuur (in waterschappen met minder dan 19 zetels in het (gekozen deel van het) algemeen bestuur)
- Algemeen Bestuur (in waterschappen met 19 of meer zetels in het (gekozen deel van het) algemeen bestuur)

Ook voor de verkiezingen van Provinciale staten met meerdere kieskringen constateren we dat er geen functionele onvolkomenheden zijn ten opzichte van wat van de software verwacht wordt.

In sectie 3.4 laten we verschillen zien tussen het door OSV2020-U geleverde verkiezingsresultaat en het verwachte resultaat als we de formele beschrijving [15, pagina 10] letterlijk volgen. Dit betreft de behandeling van lijstgroepen en stellen gelijklopende lijsten.

Uit analyse van de formele beschrijving [15] blijkt dat deze consequenties heeft die niet in lijn zijn met de Kieswet en het kiesstelsel. Dit betreft de behandeling van lijstgroepen en stellen gelijklopende lijsten. Een interpretatie van de formele beschrijving is nodig om vast te stellen dat OSV2020 conform specificatie werkt. Door de Kiesraad is daartoe een toelichting gegeven. Daarmee blijkt dat het resultaat van OSV2020-U conform de interpretatie is die daaraan gegeven moet worden.

We constateren dat een heldere interpretatie van de formele beschrijving nodig is om testcases voor de behandeling van lijstgroepen en stellen gelijklopende lijsten te kunnen bepalen (zie sectie 3.2.2). We adviseren om die interpretatie vast te leggen in een aanpassing van de formele beschrijving.

Het testresultaat is samengevat in de volgende tabel. Deze bevat voor elke stap uit de berekening van de zetelverdeling [15]:

- *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 | Verkiezingen zonder kiesdistricten (PS1, AB1, AB2) | | Verkiezingen met kiesdistricten (PS2) | |
|--|---|--|---------------|---------------------------------------|---------------|
| | | Oordeel | Dekkingsgraad | Oordeel | Dekkingsgraad |
| A. Zetelverdeling | | | | | |
| 1. | Vaststelling van de stemtotalen per partij en het totale aantal uitgebrachte stemmen; berekening van de kiesdeler | <OK> | 100% | <KG> | |
| 2. | Toedeling van zetels op basis van het behalen van de kiesdeler | <OK> | 100% | <KG> | |
| 3. | Toedeling van restzetels | <OK> | 100% | <KG> | |
| 4. | Wijziging van de zetelverdeling indien een lijst de volstrekte meerderheid van stemmen behaalt | <OK> | 100% | <KG> | |
| 5. | Wijziging van de zetelverdeling in geval van uitputting van lijsten | <OK> | 100% | <KG> | |
| 6. | Verdeling van zetels binnen lijstengroepen | | | <KG> | |
| B. Aanwijzing van de gekozen kandidaten | | | | | |
| 1. | Aanwijzing van met voorkeurstemmen gekozen kandidaten | <OK> | 100% | <KG> | |
| 2. | Aanwijzing van de overige gekozen kandidaten | <OK> | 100% | <KG> | |
| 3. | Rangschikking van de kandidaten op de kandidatenlijsten | <OK> | 100% | <KG> | |

Tabel 3: Mate waarin OSV2020 voldoet aan specificaties voor berekening van de uitslag.

Om te bepalen of OSV2020-U voldoet aan de specificaties hebben we testen opgezet en uitgevoerd. Buiten de afhandeling van lijstgroepen en stellen gelijklopende lijsten zijn een zestiental logische testgevallen opgesteld die de berekening van de verkiezingsuitslag en de zetelverdeling afdoende afdekt. In de uitvoering zijn fysieke testgevallen gemaakt met daarin het aantal te verdelen zetels, waardoor de uitkomst van de zetelverdeling specifiek wordt voor de verkiezingstypes van Provinciale Staten en Waterschappen.

Het uitvoeren van testen voor OSV2020-U is een arbeidsintensief en foutgevoelig proces. De inrichting van een testomgeving die air-gapped is, bleek arbeidsintensief en de nodige doorlooptijd te vergen. Instructies voor inrichting van een testomgeving en installatie van de software in die testomgeving ontbreken. Met hulp van de Kiesraad is voor deze problematiek een oplossing uitgewerkt.

Doordat we niet beschikken over OSV2020-KS (zie Figuur 1 en Figuur 2) kon relevante invoer voor OSV2020-U (de Totaallijsten in format EML-230c) niet gegenereerd worden vanuit OSV2020-KS. Een beschrijving van het format met uitleg over het gebruik daarvan ontbreekt. Op basis van voorbeelden en met hulp van de leverancier zijn Totaallijsten gemaakt.

Onze aanbeveling is om de interface van OSV2020-U uit te breiden met testfunctionaliteit zodat het testen efficiënter kan worden uitgevoerd. Bijvoorbeeld het versneld invoeren van stemgegevens zou kunnen helpen bij testen. De controles op hash-codes zouden in testomstandigheden uitgeschakeld moeten kunnen worden.

Dergelijke testfunctionaliteit zou geautomatiseerd kunnen worden, maar deze mag nooit in een operationele omgeving beschikbaar komen voor gebruikers.

2.4 Samenvattende beoordeling eisen

De volgende tabel bevat een samenvatting van onze motivatie voor de mate waarin OSV2020-U voldoet aan de eisen uit de Kiesregeling. 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. | <KG> | <ul style="list-style-type: none"> • Er zijn geen bevindingen geconstateerd bij de uitgevoerde testen voor verkiezingen waarin de groepering van kieslijsten niet voorgeschreven is. • Ook voor de verkiezingen van Provinciale staten met meerdere kieskringen constateren we dat er geen functionele onvolkomenheden zijn ten opzichte van wat van de software verwacht wordt. • Uit analyse van de formele beschrijving blijkt dat deze consequenties heeft die niet in lijn zijn met de Kieswet en het kiesstelsel. Dit betreft de behandeling van lijstgroepen en stellen gelijkkluidende lijsten. • Een interpretatie van de formele beschrijving is nodig om vast te stellen dat OSV2020 conform specificatie werkt. Het blijkt dat het resultaat van OSV2020-U conform de interpretatie is die daaraan gegeven moet worden. | 31 |
| 2. | De programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn. | <KG> | <ul style="list-style-type: none"> • Een architectuurbeschrijving is niet voorhanden. • Voor de geboden functionaliteit hebben de risico's in applicatiestructurering 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. | 31 |

| Nr. | Eis | Oordeel | Motivatie | Pagina |
|-----|--|---------|---|--------|
| 3. | De kritische functies voor de berekening van de uitslag van <i>de</i> verkiezingen en de zetelverdeling zijn in de programmatuur herkenbaar en gescheiden. | <KG> | <ul style="list-style-type: none"> De kritische functies zijn onvoldoende herkenbaar omdat niet gedocumenteerd is welke methodes deze functies implementeren. De implementaties zijn nauwelijks van elkaar gescheiden. Gezien de omvang van de call graphs is het niet eenvoudig om de kritische functies zelfstandig door de programmatuur te volgen. Ontwikkelaars beschikken tegenwoordig over hulpmiddelen om algoritmes te visualiseren en de complexiteit te onderzoeken. Dergelijke hulpmiddelen ondersteunen (impact)analyses en transparantie. | 34 |
| 4. | De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen. | <OK> | <ul style="list-style-type: none"> OSV2020-U kan zonder aanpassingen aan de broncode gebruikt worden bij verschillende verkiezingstypen. Dit gebeurt met parameterinstellingen tijdens installatie en de verkiezingsdefinitie die de beheerder inleest en kan aanpassen. | 39 |
| 5. | Toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen. | <OK> | <ul style="list-style-type: none"> In de software en ten aanzien van de infrastructurele omgeving zijn voldoende maatregelen genomen om foutief gebruik te voorkomen. Bij een statische codeanalyse zijn enkele potentiële kwetsbaarheden voor beveiliging aangetroffen. We adviseren om deze te analyseren ter verdere verbetering van de beveiliging. | 41 |
| 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. | <OK> | <ul style="list-style-type: none"> Diakritische tekens van de GBA-tekenset worden door de programmatuur correct verwerkt. | 43 |
| 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. | <OK> | <ul style="list-style-type: none"> Voor de gegevensuitwisseling wordt gebruikgemaakt van de EML_NL standaard. Voor uitvoer wordt gebruikgemaakt van PDF, ODT (open standaard) en EML_NL (open). De gebruikte versie van PDF is versie 1.5. Deze wordt niet aangemerkt als open standaard. | 44 |

| Nr. | Eis | Oordeel | Motivatie | Pagina |
|-----|--|---------|--|--------|
| 8. | De standaard programmatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar. | <OK> | <ul style="list-style-type: none">• Voor iedereen die een testopstelling van OSV2020-U wil maken wordt een mogelijkheid beschikbaar gesteld om een kopie van het systeem aan te vragen voor eigen gebruik en analyse.• De sources van OSV2020-U worden op de website van de Kiesraad publiekelijk beschikbaar gesteld.• Er is een bestand met informatie over gebruikte externe softwareproducten en hun bijbehorende licentiering.• Het merendeel van de externe softwareproducten is publiek beschikbaar met publieke licentie. | 46 |
| 9. | Het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau. | <OK> | <ul style="list-style-type: none">• Intellectueel eigendom is vastgelegd op basis van ARBIT-2014 en ARBIT 2018.• Met de actuele overeenkomsten zijn deze afspraken nog steeds rechtsgeldig. | 47 |
| 10. | De programmatuur is geschreven in een programmeertaal, waarvoor een door een actieve gemeenschap onderhouden open source compiler, onderscheidenlijk interpreter beschikbaar is. | <OK> | <ul style="list-style-type: none">• Voor Java zijn diverse open source compilers beschikbaar. | 48 |
| 11. | De programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem. | <OK> | <ul style="list-style-type: none">• OSV2020 is ontwikkeld voor verschillende besturingssystemen: Windows/Linux en Mac OS.• Linux is een open source besturingssysteem. | 49 |
| 12. | Het is mogelijk de authenticiteit van de programmatuur vast te stellen. | <OK> | <ul style="list-style-type: none">• De authenticiteit van de programmatuur kan voorafgaand aan de installatie worden vastgesteld met op de website van de Kiesraad gepubliceerde informatie. | 50 |

| 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. | <OK> | <ul style="list-style-type: none">• OSV2020-U gebruikt verschillende manieren waarop bij het importeren van een bestand al dan niet controle ten aanzien van de authenticiteit wordt afgedwongen.• De Kiesraad en de leverancier geven aan dat gebruiksvriendelijkheid van OSV2020 belangrijk is geweest in de afweging van de gekozen beveiligingsniveaus en hun implementatie.• Voor tellingen stembureau (EML-510a) wordt de authenticiteit bij inlezen niet gecontroleerd. De tweede invoer moet zorgen voor controle van de bij de eerste invoer ingelezen informatie. We adviseren te overwegen een controle van hash-code en publieke sleutel aan te brengen. | 51 |

Tabel 4: Motivering van de mate waarin OSV2020 voldoet aan de eisen uit de bijlage bij art. 2a van de Kiesregeling.

3. Functionele test OSV2020

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's |
|--|--|-----------|
| Provinciale staten in provincies met één kieskring | Formele beschrijving van de berekening van de zetelverdeling [15]. | 18 t/m 21 |
| Provinciale staten in provincies met meer dan één kieskring | | 10 t/m 17 |
| Algemeen Bestuur (in waterschappen met minder dan 19 zetels in het (gekozen deel van het) algemeen bestuur) | | 22 t/m 25 |
| Algemeen Bestuur (in waterschappen met 19 of meer zetels in het (gekozen deel van het) algemeen bestuur) | | 18 t/m 21 |

Tabel 5: Voor de testen gehanteerde testbasis.

3.2 Testaanpak

Eerst hebben we testen uitgevoerd voor Provinciale Staten met één kieskring (zie Figuur 2). Daartoe zijn de versies van OSV2020-U voor gemeentelijk stembureau (GSB) en voor de combinatie van hoofdstembureau en centraal stembureau (CSB_HSB) geïnstalleerd. Op gemeentelijk niveau (GSB) is de invoer vanuit meerdere stembureaus verwerkt tot definitief gemaakte tellingen van de gemeente. Daarmee wordt het verwerken van resultaten over meerdere stembureaus afdoende getest.

Voor het testen van Provinciale Staten met meerdere kieskringen (zie Figuur 1) zijn vervolgens de drie afzonderlijke niveaus voor gemeentelijk stembureau (GSB), hoofdstembureau (HSB) en centraal stembureau (CSB) geïnstalleerd. Ook hiervoor zijn de drie niveaus in testen doorlopen zodat het verwerken van tellingen van GSB naar HSB en van HSB naar CSB afdoende is gedekt.

In de verdere testgevallen is daarom geen onderscheid aangebracht voor de verschillende organisatieniveaus. Daarbij ligt de nadruk op de bepaling van het definitieve verkiezingsresultaat inclusief de zetelverdeling. Dit is functionaliteit voor centrale stembureaus (CSB).

3.2.1 Logische testcases zonder lijstgroepen en gelijklopende lijsten

Voor het testen van het bepalen van het verkiezingsresultaat en het vaststellen van de zetelverdeling is een testbasis opgesteld van zestien logische testgevallen waarmee het berekenen van de juiste uitslag en de weergave hiervan op de processen-verbaal afdoende worden afgedekt. In de uitvoering zijn fysieke testgevallen gemaakt waarin rekening is gehouden met de verschillen in berekeningswijze afhankelijk van het verkiezingstype.

In deze testbasis is geen rekening gehouden met gelijklopende lijsten en lijstgroepen. In de testbasis worden stellen van gelijklopende lijsten en lijstgroepen als separate lijsten behandeld. In sectie 3.2.2 gaan we dieper in op de benodigde testgevallen specifiek voor lijstgroepen en stellen van gelijklopende lijsten.

| Nr. | Titel | Omschrijving |
|---------------|--|---|
| PSx.1 | Basistest zonder restzetels | Eenvoudige test waarmee de basiswerking van de software zonder verdeling van restzetels wordt aangetoond. |
| PSx.2 | Basistest met één restzetel | Eenvoudige test waarbij één restzetel moet worden verdeeld. |
| PSx.3 | Basistest met meerdere restzetels | Eenvoudige test, waarbij meerdere restzetels moeten worden verdeeld. |
| PSx.4 | Restzetel naar partij zonder zetel bij eerste toedeling | Eenvoudige test, waarbij een restzetel gaat naar een partij die bij de eerste toedeling geen zetel heeft behaald. |
| PSx.5 | Restzetel na loting | Testgeval waarbij loting nodig is voor het toewijzen van de laatste restzetel. |
| PSx.6 | Restzetel na loting in tweede stap | Testgeval met loting in tweede stap. |
| PSx.7 | Restzetel na loting met drie partijen | Testgeval met loting tussen drie partijen. |
| PSx.8 | Controle volstreekte meerderheid | Testgeval met een partij die de volstreekte meerderheid haalt en meteen de volstreekte meerderheid van het aantal te verdelen zetels heeft. |
| PSx.9 | Controle volstreekte meerderheid & correctie | Testgeval met een partij die de volstreekte meerderheid haalt maar in eerste instantie niet de volstreekte meerderheid van het aantal te verdelen zetels. Een andere partij moet een zetel inleveren voor de partij die de volstreekte meerderheid heeft. |
| PSx.10 | Volstreekte meerderheid waarbij door loting een restzetel ingeleverd moet worden | Testgeval met een partij die de volstreekte meerderheid haalt maar niet de volstreekte meerderheid van het aantal te verdelen zetels. Door loting moet bepaald worden welke partij een zetel moet inleveren. |
| PSx.11 | Uitputting van lijsten voor een lijst | Testgeval met uitputting van één van de lijsten. Deze krijgt in eerste instantie één zetel meer toegewezen dan het aantal beschikbare kandidaten op de lijst. De zetel wordt toegekend aan een andere partij. |
| PSx.12 | Uitputting van lijsten voor meerdere lijsten | Testgeval met uitputting van meerdere lijsten. Bij twee lijsten moet een zetel worden toebedeeld aan andere partijen. |
| PSx.13 | Voorkeursstemmen | Testgeval voor het toewijzen van zetels aan kandidaten met voldoende voorkeursstemmen. |
| PSx.14 | Controle afronding voorkeursdrempel | In deze testcase controleren we of de kiesdeler niet wordt afgerond. |

| Nr. | Titel | Omschrijving |
|---------------|--|---|
| PSx.15 | 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. |
| PSx.16 | Testgeval met overleden kandidaat en uitputting van de lijst | Testgeval met een overleden persoon waardoor de betreffende lijst wordt uitgeput en een zetel moet worden overgedragen aan een andere lijst. |

Tabel 6: Testbasis met logische testgevallen voor verkiezingen.

In de tabel zijn de testgevallen aangeduid met PSx. In de verdere rapportage worden de testen voor Provinciale Staten met één kieskring aangeduid met PS1 en die voor Provinciale Staten met meerdere kieskringen met PS2. Voor de verkiezingen van algemeen bestuur in waterschappen met minder dan 19 zetels in het (gekozen deel van het) algemeen bestuur gebruiken we AB1 en bij 19 of meer zetels AB2.

In de Formele beschrijving van de berekening van de zetelverdeling [15] is beschreven hoe in de algoritmes rekening moet worden gehouden met overleden kandidaten als onderdeel van hoofdonderdeel B (Aanwijzing van de gekozen kandidaten):

Een kandidaat van wie bekend is dat hij is overleden, wordt buiten beschouwing gelaten (art. P 19a Kieswet).

Het is mogelijk dat het overlijden van een kandidaat resulteert in uitputting van de lijst waarop de betreffende kandidaat was opgenomen. De specificatie geeft geen uitsluitsel wat dan moet gebeuren. In dat geval zal hoogstwaarschijnlijk de zetelverdeling (specifiek onderdeel A.5) toegepast moeten worden. Dit hebben we als uitgangspunt genomen voor testgeval PSx.16.

3.2.2 Logische testcases met lijstgroepen en gelijkkluidende lijsten

Voor Provinciale Staten met meerdere kieskringen (PS2) zijn extra testcases nodig voor de behandeling van lijstgroepen en stellen gelijkkluidende lijsten.

In de Formele beschrijving van de berekening van de zetelverdeling [15, pagina 10] zijn definities opgenomen van de begrippen "lijstengroepen" en "stellen gelijkkluidende lijsten":

Wettelijke bepalingen: art. P 2, P 3 en P 5 Kieswet

- In verschillende kieskringen ingediende kandidatenlijsten waarop dezelfde kandidaten in dezelfde volgorde voorkomen en die dus geheel identiek zijn, vormen samen een stel gelijkkluidende lijsten.
- In verschillende kieskringen ingediende kandidatenlijsten waarboven dezelfde partij-aanduiding staat of waarvan de eerste kandidaat dezelfde is, vormen samen een lijstengroep.
- Kandidatenlijsten die niet tot een stel gelijkkluidende lijsten behoren, zijn op zichzelf staande lijsten.

In stap 2 van onderdeel A.1 [15, pagina 10] wordt beschreven hoe het totaal aantal uitgebrachte stemmen bepaald moet worden:

- 2 De stemtotalen van de stellen gelijkkluidende lijsten, de lijstengroepen en de op zichzelf staande lijsten worden bij elkaar opgeteld.
Het resultaat van deze optelling is het totale aantal uitgebrachte stemmen.

Als we bovenstaande definities en specificaties letterlijk nemen heeft dit consequenties die niet in lijn zijn met de Kieswet en het kiesstelsel. Ter illustratie verwijzen we naar Tabel 7 waarin voorbeelden zijn opgenomen.

- *Grootst mogelijke verzamelingen:* In de definities van lijstgroepen en stellen van gelijkkluidende lijsten wordt niet aangegeven dat het de grootst mogelijke verzamelingen betreft. Een stel van drie gelijkkluidende lijsten bevat drie tweetallen van gelijkkluidende lijsten: Green in kieskring 1 (Green-KK1) met Green in KK 2 (Green-KK2), Green-KK2 met Green-KK3 en Green-KK1 met Green-KK3. Bij het bepalen van het totaal aantal uitgebrachte stemmen zouden stemmen die uitgebracht zijn op één lijst in een van deze kieskringen meermaals geteld worden.
- *Geheel identiek:* Voor stellen van gelijkkluidende lijsten is in de formele beschrijving niet beschreven dat ook de naam van de lijst gelijk moet zijn als de kandidaten in dezelfde volgorde voorkomen (zie Yellow-KK1 en Yellow'-KK2).
- *Gelijkkluidend ook lijstengroep:* per definitie is een stel gelijkkluidende lijsten meteen ook een lijstengroep of onderdeel daarvan. Het stel heeft namelijk dezelfde eerste kandidaat (zie Blue, Green). Ook dit leidt tot dubbel telling want zowel de stemtotalen van stellen gelijkkluidende lijsten als van lijstengroepen moeten worden opgeteld bij het bepalen van het totale aantal.
- *Overlappende lijstengroepen:* het is mogelijk dat twee verschillende lijstengroepen elkaar overlappen. Het is duidelijk dat White-KK1 en White-KK2 tot dezelfde lijstengroep behoren want ze hebben dezelfde partijnaam (White). Tevens behoren White-KK2 en White'-KK3 tot dezelfde lijstengroep omdat ze dezelfde lijsttrekker hebben (de eerste kandidaat op de kandidaten lijst: white2). Echter behoren White-KK1 en White'-KK3 niet tot dezelfde lijstengroep. Bij de bepaling van het totaal aantal uitgebrachte stemmen worden de stemmen van White-KK2 dubbel geteld.
- *Lijstengroepen ook opzichzelfstaand:* In de definitie van op zichzelf staande lijsten worden alleen de gelijkkluidende lijsten uitgesloten. Cyan-KK1, Cyan'-KK2 en Cyan'-KK3 behoren tot dezelfde lijstengroep want ze hebben dezelfde lijsttrekker. Daarnaast vormen Cyan'-KK2 en Cyan'-KK3 een stel gelijkkluidende lijsten. Volgens de definitie is Cyan-KK1 een op zichzelf staande lijst die ook onderdeel is van een lijstengroep. Moeten stemmen voor deze lijst tweemaal geteld worden?
- *Blanco-lijsten:* In bespreking met de Kiesraad is vastgesteld dat blanco-lijsten mogelijk zijn. Deze hebben geen partijnaam. Het onderscheid tussen verschillende blanco-lijsten wordt bepaald door de lijsttrekker van de blanco-lijst. In de software zijn blanco-lijsten toegestaan en worden deze behandeld. In de formele beschrijving worden blanco-lijsten echter niet behandeld. Als we de definitie van lijstengroepen toepassen op blanco-lijsten zouden alle blanco-lijsten in één lijstengroep bij elkaar gegroepeerd worden.

| kieskring | partijnaam | kandidatenlijst |
|-----------|------------|------------------------------------|
| 1 | Blue | blue1, blue2, blue3, blue4 |
| 2 | Blue | blue1, blue2, blue3, blue4 |
| 1 | Green | green1, green2, green3, green4 |
| 2 | Green | green1, green2, green3, green4 |
| 3 | Green | green1, green2, green3, green4 |
| 1 | Yellow | yellow1, yellow2, yellow3, yellow4 |
| 2 | Yellow' | yellow1, yellow2, yellow3, yellow4 |

| kieskring | partijnaam | kandidatenlijst |
|-----------|------------|--------------------------------|
| 1 | Cyan | cyan1, cyan2, cyan3, cyan4 |
| 2 | Cyan' | cyan1, cyan5, cyan6, cyan7 |
| 3 | Cyan' | cyan1, cyan5, cyan6, cyan7 |
| 1 | White | white1, white2, white3, white4 |
| 2 | White | white2, white3, white4, white5 |
| 3 | White' | white2, white3, white4, white6 |

| kieskring | partijnaam | kandidatenlijst |
|-----------|------------|--|
| 1 | Black | black1, black2, black3, black4 |
| 2 | Black | black1, black2, black3, black4 |
| 3 | Black | black1, black2, black3, black4, black5 |
| 4 | Black | black1, black2, black3, black4, black5 |

| kieskring | partijnaam | kandidatenlijst |
|-----------|------------|--------------------------------------|
| 1 | | blanco1, blanco2, blanco3, blanco4 |
| 2 | | blanco1, blanco5, blanco6, blanco7 |
| 3 | | blanco8, blanco9, blanco10, blanco11 |

Tabel 7: Voorbeelden van kieslijsten in meerdere kieskringen.

In de kern worden de problemen veroorzaakt door twee (mathematische) basisprincipes die worden geschonden:

Geen correcte indeling: De indeling in lijstgroepen vormt geen correcte indeling in de zin dat alle lijsten worden ingedeeld en er geen overlap ontstaat in de groepsindeling (zie bijvoorbeeld White en White' in Tabel 7). Een correcte indeling is alleen mogelijk als de relatie die voor paren van lijsten beschrijft dat ze tot dezelfde groep behoren voldoet aan drie eisen⁴:

- o *reflexief:* (x,x) is een element van de relatie voor elk element x van de verzameling waarin de relatie wordt gedefinieerd;
- o *symmetrisch:* (y,x) is een element van de relatie als (x,y) dat ook is;
- o *transitief:* als (x,y) en (y,z) tot de relatie behoren, dan ook (x,z) .

De definitie van lijstgroepen in de Formele beschrijving voldoet niet aan de eis voor transitiviteit.

- *Functies voor gecombineerde indelingen:* In de algoritmes worden functies gedefinieerd met als invoer zowel de indeling in lijstgroepen als in stellen van gelijkkluidende lijsten. Zie bijvoorbeeld de berekening van het totale aantal uitgebrachte stemmen voor de berekening van de kiesdeler (stap 2 van onderdeel A.1 [15, pagina 10]). Daardoor ontstaan dubbeltellingen (zie als uitgewerkt voorbeeld Annex B.1: Test met één partij met identieke lijst in twee kieskringen).

Daarnaast ontbreekt de formele beschrijving van de behandeling van blanco-lijsten.

We constateren dat een heldere interpretatie van de formele beschrijving nodig is om testcases voor de behandeling van lijstgroepen en stellen gelijkkluidende lijsten te kunnen bepalen. We adviseren om die interpretatie vast te leggen in een aanpassing van de formele beschrijving.

3.3 Testresultaten zonder lijstgroepen en gelijkkluidende lijsten

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.

⁴. Zie: [nl.wikipedia.org/wiki/Gelijkheid_\(wiskunde\)](https://nl.wikipedia.org/wiki/Gelijkheid_(wiskunde)).

3.3.1 Provinciale Staten met één kieskring

In de volgende tabel is de dekking van de eisen en de testresultaten per testgeval weergegeven voor Provinciale Staten met één kieskring.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|--|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| A Zetelverdeling | | | | | | | | | | | | | | | | |
| 1 Vaststelling stemtotalen en kiesdeler | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 Directe toedeling van zetels | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3 Toedeling van restzetels | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | ✓ | | | | | ✓ |
| 4 Wijziging bij volstreekte meerderheid | | | | | | | | ✓ | ✓ | ✓ | | | | | | |
| 5 Wijziging bij uitputting lijsten | | | | | | | | | | | ✓ | | | | | ✓ |
| 6 Verdeling binnen lijstengroepen ⁵ | | | | | | | | | | | | | | | | |
| B Aanwijzing van de gekozen kandidaten | | | | | | | | | | | | | | | | |
| 1 Aanwijzing met voorkeurstemmen | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 Aanwijzing overige kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | |
| 3 Rangschikking kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resultaat | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Tabel 8: Afdekking van de eisen en testresultaten voor Provinciale Staten met één kieskring.

In deze testen zijn geen bevindingen gedaan.

⁵. Provinciale Staten met één kieskring kennen geen lijstengroepen waardoor deze stap in de zetelverdeling niet voorkomt.

3.3.2 Provinciale Staten met meerdere kieskringen

In de volgende tabel is de dekking van de eisen en de testresultaten per testgeval weergegeven voor Provinciale Staten met meerdere kieskringen.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|--|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| 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 ⁶ | | | | | | | | | | | | | | | | |
| B Aanwijzing van de gekozen kandidaten | | | | | | | | | | | | | | | | |
| 1 Aanwijzing met voorkeurstemmen | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 Aanwijzing overige kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | |
| 3 Rangschikking kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resultaat | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Tabel 9: Afdekking van de eisen en testresultaten voor Provinciale Staten met meerdere kieskringen.

Er zijn aanvullende testen nodig voor de behandeling van lijstgroepen en stellen gelijklopende lijsten. Deze hebben invloed op alle stappen in de berekening van het verkiezingsresultaat en worden separaat behandeld in 3.2.2.

⁶ Provinciale Staten met meerdere kieskringen kennen lijstengroepen waardoor deze stap in de zetelverdeling afgedekt moet worden.

3.3.3 Waterschappen minder dan 19 zetels

In de volgende tabel is de dekking van de eisen en de testresultaten per testgeval weergegeven voor Waterschappen minder dan 19 zetels.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|--|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| 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 ⁷ | | | | | | | | | | | | | | | | |
| B Aanwijzing van de gekozen kandidaten | | | | | | | | | | | | | | | | |
| 1 Aanwijzing met voorkeurstemmen | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 Aanwijzing overige kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | |
| 3 Rangschikking kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resultaat | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Tabel 10: Afdekking van de eisen en testresultaten van Waterschappen minder dan 19 zetels.

In deze testen zijn geen bevindingen gedaan.

⁷. Waterschappen minder dan 19 zetels kennen geen lijstengroepen waardoor deze stap in de zetelverdeling niet voorkomt.

3.3.4 Waterschappen met 19 of meer zetels

In de volgende tabel is de dekking van de eisen en de testresultaten per testgeval weergegeven voor Waterschappen met 19 of meer zetels.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|--|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| 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 ⁸ | | | | | | | | | | | | | | | | |
| B Aanwijzing van de gekozen kandidaten | | | | | | | | | | | | | | | | |
| 1 Aanwijzing met voorkeurstemmen | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 Aanwijzing overige kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | |
| 3 Rangschikking kandidaten | | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Resultaat | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Tabel 11: Afdekking van de eisen en testresultaten van Waterschappen met 19 of meer zetels.

In deze testen zijn geen bevindingen gedaan.

⁸. Waterschappen met 19 of meer zetels kennen geen lijstengroepen waardoor deze stap in de zetelverdeling niet voorkomt.

3.4 Testresultaten met lijstgroepen en gelijkkluidende lijsten

Op basis van de formele beschrijving van de berekening van de zetelverdeling [14] hebben we een aantal testen uitgevoerd die laten zien hoe OSV2020-U omgaat met lijstgroepen en stellen gelijkkluidende lijsten. Voorbeelden van deze testen zijn beschreven in Annex B waarbij we het door OSV2020-U geleverde verkiezingsresultaat vergelijken met het verwachte resultaat als we de formele beschrijving [15, pagina 10] letterlijk volgen.

Op basis van de uitgevoerde testen komen we tot het volgende oordeel:

- We constateren verschillen tussen het door OSV2020-U geleverde verkiezingsresultaat en het verwachte resultaat als we de formele beschrijving [15, pagina 10] letterlijk volgen. Uit overleg met de Kiesraad blijkt dat het resultaat van OSV2020-U conform de interpretatie is die daaraan gegeven moet worden.
- In enkele testgevallen voor meerdere kieskringen is de uitvoering van de testcase in OSV2020-U niet mogelijk omdat het situaties betreft die in de praktijk ongewenst zijn en niet blijken voor te komen. In de formele beschrijving wordt (nog) niet expliciet aangegeven welke situaties moeten worden uitgesloten.

4. Oordeel per eis

In dit hoofdstuk wordt voor elk van de eisen die in de Kiesregeling [3] gesteld worden, besproken in hoeverre de programmatuur voldoet aan de betreffende eis en wat ons oordeel is.

Elke paragraaf begint met de formele tekst van de gestelde eis. Daarna volgt de nadere toelichting op de eis zoals deze is geformuleerd in de ministeriële regeling uit 2014 [7]. Vervolgens behandelen we de wijze van toetsing en het resulterende toetsoordeel.

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.*

Toelichting

Deze eis is bedoeld om vast te leggen dat de programmatuur de functionaliteiten bevat die nodig zijn om tot een correcte berekening van de uitslag en van de zetelverdeling te komen. In de eisen zoals die in 2008 zijn geformuleerd, wordt gesproken over deze functionaliteiten, met inbegrip van tussenstappen en tussenresultaten. Voorbeelden van tussenstappen en tussenresultaten zijn cijfers zoals lijsttotalen of de kiesdeler. In het Kiesbesluit (artikel P 1, zesde lid, onder a) is vastgelegd dat het centraal stembureau een specificatie moet opstellen van de wijze waarop de uitslag en de zetelverdeling moet worden berekend. Deze specificatie bepaalt hoe de geldende wet- en regelgeving voor de uitslagberekening moet worden toegepast. Door in de eerste eis te verwijzen naar de specificatie wordt gewaarborgd dat deze specificatie de basis vormt voor de (functionaliteiten van de) programmatuur en dat de relevante wet- en regelgeving correct wordt toegepast.

Toetsing & toetsoordeel

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.*

Toelichting

Deze eis bepaalt dat de programmatuur gestructureerd is opgebouwd. De programmatuur dient gestructureerd te zijn om het gemakkelijker te maken later veranderingen aan te brengen. Dit vereiste draagt daarmee bij aan de kwaliteit van de programmatuur.

Toetsing

Voor verificatie van deze eis bekijken we de structuur van de opgeleverde code in relatie tot de architectuurbeschrijving. Helaas is een geactualiseerde architectuurbeschrijving (nog) niet voorhanden. Daarmee is toetsing tegen een architectuurbeschrijving niet uitvoerbaar.

Vervolgens hebben we een statische code-analyse uitgevoerd met behulp van CAST tools (zie: www.castsoftware.com). Op basis van de sources van OSV2020-U berekent het CAST Application Intelligence Platform (CAST AIP⁹) voor diverse kwaliteitseigenschappen in hoeverre het softwaresysteem aan de betreffende kwaliteitseigenschap voldoet. Voor deze eis is de score voor 'Changeability' (Wijzigbaarheid) relevant. Een nadere beschrijving van de berekeningswijze is opgenomen in Annex C.1.



De score die CAST AIP aangeeft voor de wijzigbaarheid (changeability) van OSV2020-U is 3,37. Dit betreft een goede score die ruimte voor verdere verbetering laat zien. Tabel 12 geeft de scores voor wijzigbaarheid per technisch criterium die lager dan 3 scoren. Een score van 3 geeft aan dat op dat gebied een (erg) hoog risico is gedetecteerd (zie voor nadere uitleg Figuur 11). Tabel 13 geeft de scores voor metingen voor wijzigbaarheid die lager dan 3 scoren. De complete tabellen voor wijzigbaarheid zijn opgenomen in Annex C.3.

| Technical Criterium | NL | ELECT | DB | Total |
|---|------|-------|------|-------|
| Documentation – Volume of Comments | 1,15 | 1,00 | | 1,00 |
| Dead code (static) | 3,00 | 2,28 | 4,00 | 2,61 |
| Architecture – Object-level Dependencies | 3,21 | 2,56 | | 2,63 |
| Architecture – Reuse | 3,06 | 2,99 | | 2,98 |

Tabel 12: Technische criteria met (hoog) risico voor wijzigbaarheid van OSV2020-U.

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Avoid defining singleton or factory when using Spring | 1,00 | 1,00 | | 1,00 |
| Avoid undocumented Methods | 1,00 | 1,00 | | 1,00 |
| Avoid Functions having a very low Comment/Code ratio (Javascript) | | 1,00 | | 1,00 |
| Avoid undocumented Functions (Javascript) | | 1,00 | | 1,00 |
| Avoid Methods with a very low comment/code ratio | 1,01 | 1,00 | | 1,00 |
| Avoid Classes with a very low comment/code ratio | 1,25 | 1,00 | | 1,00 |
| Avoid long Table or View names | | | 1,00 | 1,00 |
| Avoid undocumented Interfaces | 1,00 | 1,00 | | 1,00 |
| Avoid Classes with a High Lack of Cohesion | 1,01 | 1,00 | | 1,00 |
| Avoid undocumented Classes | 1,48 | 1,00 | | 1,00 |
| Constant naming convention – case control (JEE) | 1,00 | 1,90 | | 1,00 |

⁹. Zie: doc.castsoftware.com/display/DOC83/Overview+of+CAST+Application+Intelligence+Platform.

| Measurement | NL | ELECT | DB | Total |
|---|------|-------|----|-------|
| Use ANSI standard operators in SQL WHERE clauses | | 1,00 | | 1,00 |
| Avoid Classes with a High Lack of Cohesion – variant | 1,20 | 1,05 | | 1,07 |
| Avoid Classes with High Coupling Between Objects | 1,39 | 1,05 | | 1,09 |
| Avoid unreferenced JSPs and web client files | 1,67 | 1,47 | | 1,49 |
| Avoid Too Many Copy Pasted Artifacts | 2,80 | 1,70 | | 1,73 |
| Avoid unreferenced Functions (Javascript/HTML5) | | 1,87 | | 1,87 |
| Avoid many-to-many association | | 1,95 | | 1,95 |
| Avoid Artifacts with High Fan-Out | 2,39 | 2,07 | | 2,11 |
| Avoid unreferenced Data Members | 3,79 | 2,12 | | 2,28 |
| Avoid unreferenced Methods | 2,53 | 2,27 | | 2,30 |
| Class Fan-In Distribution | 3,69 | 2,14 | | 2,32 |
| Avoid Artifacts with High Fan-In | 3,25 | 2,39 | | 2,49 |
| Class Fan-Out Distribution | 3,28 | 2,38 | | 2,49 |
| Copy Pasted Code (% of LOC) | 3,65 | 2,50 | | 2,50 |
| Reuse by Call Distribution | 1,80 | 2,77 | | 2,66 |
| Avoid Packages with High Efferent Coupling (CE) | 2,98 | 2,68 | | 2,72 |

Tabel 13: Metingen met (hoog) risico voor wijzigbaarheid van OSV2020-U.

Tenslotte hebben we CAST Imaging¹⁰ gebruikt om de applicatiestructuur van OSV2020-U te onderzoeken. In dit tool worden visualisaties van OSV2020-U geleverd op basis van de broncode. Figuren daarvan zijn opgenomen in Annex C.5.

Toetsoordeel

Een geactualiseerde architectuurbeschrijving ontbreekt. De score die CAST AIP aangeeft voor de wijzigbaarheid (changeability) van OSV2020-U is 3,37. Dit betreft een goede score die ruimte voor verdere verbetering laat zien. Diverse metingen laten een risicovolle score (lager dan 3) zien. Op basis van visualisaties van de applicatiestructuur zijn we van mening dat de structuur van de code onvoldoende helder is voor efficiënte doorvoering van aanpassingen.

Voor de geboden functionaliteit hebben de risico's in applicatiestructurering 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.

¹⁰. Zie: learn.castsoftware.com/imaging.

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.*

Toelichting

Deze eis 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.

Toetsing

Bij de leverancier hebben we nagevraagd welke methodes de in de toelichting genoemde functies implementeren. Dit resulteert in de volgende informatie:

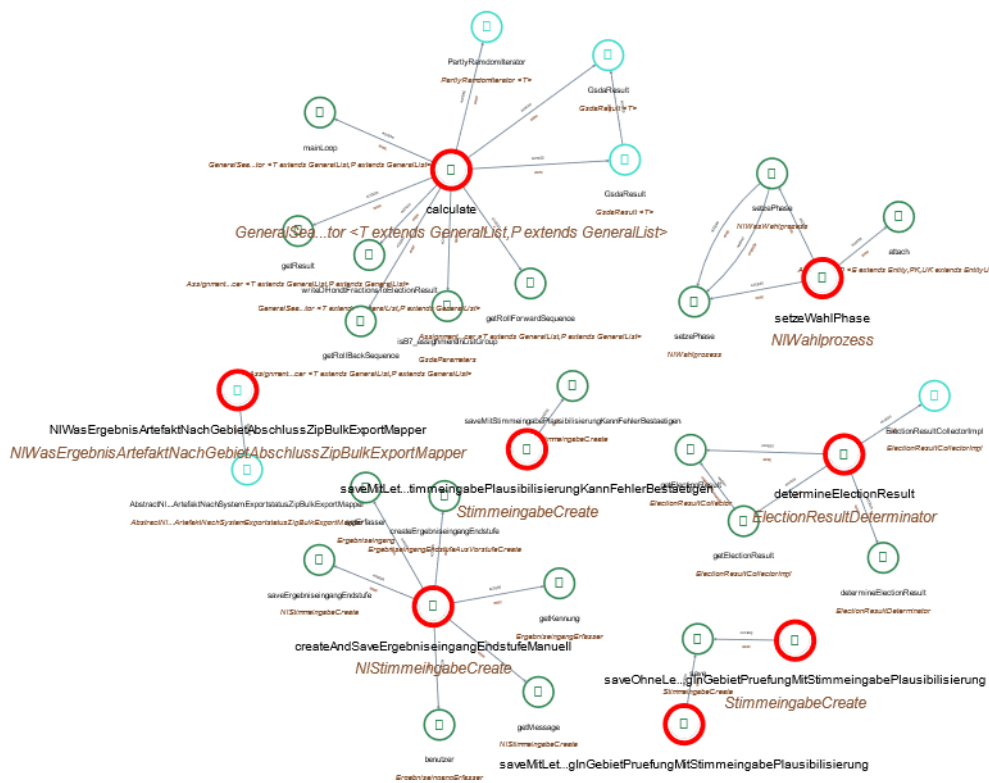
| Kritische functie | Opmerking | Method | Class | File |
|--|--|---|--|--|
| Invoeren van de vastgestelde aantallen stemmen (tellingen) die door de stembureaus zijn verricht | De methode die wordt aangeroepen als iemand zijn invoer van tellingen bevestigd; bij opslaan van de eerste of tweede invoer van de telling | saveMitLetzterErgebniseingang InGebietPruefungMitStimmeingabe Plausibilisierung (public void) | de.ivu.elect.business.stimmeingabe. control.StimmeingabeCreate | /elect-was-jar-5.23.0-sources/ de/ivu/elect/business/stimmeingabe/ control/StimmeingabeCreate.java |
| | Bij opslaan van de eerste of tweede invoer waarbij expliciet bevestigd wordt dat waarschuwingen genegeerd worden | saveMitLetzterErgebniseingang InGebietPruefungMitStimmeingabe PlausibilisierungKannFehlerBestaetigen (public void) | | |
| | Bij inlezen van tellingsgegevens (510a) | saveOhneLetzterErgebniseingang InGebietPruefungMitStimmeingabe Plausibilisierung (public void) | | |
| Vaststellen aantallen stemmen op het niveau van de gemeenten en hoofdstembureaus | De methode die wordt aangeroepen door de verkiezingsleider om na dubbele invoer de telling te bevestigen | createAndSaveErgebniseingang EndstufeManuell (public void) | de.ivu.elect.business.stimmeingabe. control.NIStimmeingabeCreate | /nl-was-jar-1.8.2.3-sources/ de/ivu/elect/business/stimmeingabe/ control/NIStimmeingabeCreate.java |
| Vaststellen aantallen stemmen op het niveau van de centrale stembureaus | Voor alle verkiezingen is dit hetzelfde als bovenstaande methode | | | |
| Vaststelling van de uitslag | De methode die wordt aangeroepen als de uitslag definitief wordt gemaakt | setzeWahlPhase (public void) | de.ivu.elect.business.wahl. boundary.NIWahlprozess | /nl-core-jar-1.8.2.3-sources/ de/ivu/elect/business/wahl/ boundary/NIWahlprozess.java |
| | De methode voor generatie van de bijbehorende documenten | NIWasErgebnisArtefaktNach GebietAbschlussZipBulkExportMapper (public) | de.ivu.elect.was.exchange.ergebnis. NIWasErgebnisArtefaktNach GebietAbschlussZipBulkExportMapper | /nl-was-exchange-1.8.2.3-sources/ de/ivu/elect/was/exchange/ergebnis/ NIWasErgebnisArtefaktNachGebietAbschlussZipBulkExportMapper.java |

| Kritische functie | Opmerking | Method | Class | File |
|---|--|---|---|--|
| De zetelverdeling | De methode voor bepaling van de zetelverdeling | determineElectionResult (public static ElectionResult) | de.ivu.wahl.result.determination. ElectionResultDeterminator | /nl-sitzberechnung-osv-legacy-1.0.3-sources/ de/ivu/wahl/result/determination/ ElectionResultDeterminator.java |
| De toewijzing van de zetels aan de kandidaten | De methode waarmee de toewijzing van zetels aan kandidaten wordt bepaald | calculate (public GsdaResult<T>) | de.ivu.wahl.result.gsda. GeneralSeatDistributor | /nl-sitzberechnung-osv-legacy-1.0.3-sources/ de/ivu/wahl/result/gsda/ GeneralSeatDistributor.java |

Tabel 14: Kritische functies van OSV2020-U met hun bijbehorende implementatie in de source code.

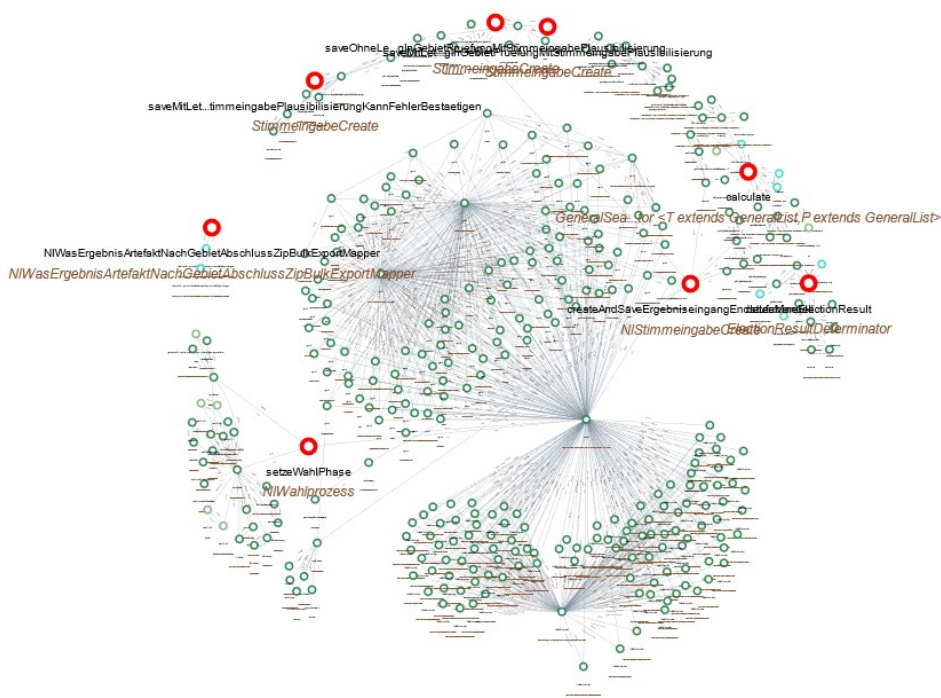
De in Tabel 14 genoemde informatie is essentieel om de kritische functies in de sourcecode te kunnen vinden. Omdat de doelstelling van deze eis is dat transparant is waar in de code de kritische functies zich bevinden is het raadzaam deze informatie te documenteren of anderszins (publiek) beschikbaar te stellen.

Met behulp van CAST tools hebben we de call graphs van de kritische functies bestudeerd om te toetsen in hoeverre de algoritmes gescheiden zijn van elkaar. Zo'n call graph visualiseert welke methodes in een methode gebruikt worden. Figuur 3 laat het eerste niveau van methodes zien die door de kritische functies (aangegeven met roodgekleurde cirkels) worden gebruikt. Op dit niveau is te zien dat twee van de kritische functies afhankelijk van elkaar zijn.



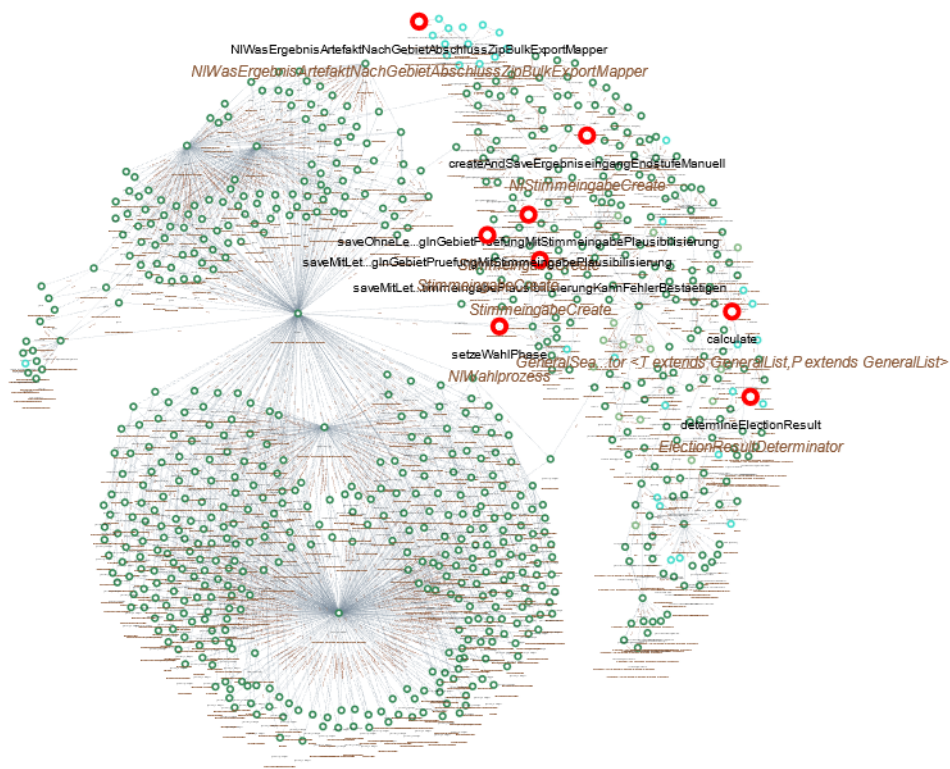
Figuur 3: Call graph van de kritische functies; niveau 1.

Als we de call graph voor de kritische functies verder uitwerken door van de onderliggende methodes de daarin gebruikte methodes toe te voegen wordt al op niveau 2 duidelijk dat de acht kritische functies samenklonteren tot drie verzamelingen (zie Figuur 4). Het aantal methodes neemt fors toe waardoor het moeilijk is om het overzicht over de algoritmes te behouden.



Figuur 4: Call graph van de kritische functies; niveau 2.

Bij een extra niveau resteren nog slechts twee samenhangende verzamelingen van methodes voor de kritische functies (Figuur 5). De complexiteit is niet meer te overzien.



Figuur 5: Call graph van de kritische functies; niveau 3.

Toetsoordeel

De kritische functies zijn onvoldoende herkenbaar omdat niet gedocumenteerd is welke methodes deze functies implementeren. De implementaties zijn nauwelijks van elkaar gescheiden. Gezien de omvang van de call graphs is het niet eenvoudig om de kritische functies zelfstandig door de programmatuur te volgen.

We achten dit een klein gebrek omdat hergebruik van methodes voor de hand liggend is met name daar waar het generieke functies betreft bijvoorbeeld voor de opslag van gegevens in de database. Ontwikkelaars beschikken tegenwoordig over hulpmiddelen om algoritmes te visualiseren en de complexiteit te onderzoeken. Dergelijke hulpmiddelen ondersteunen (impact)analyses en transparantie.

4.4 Soorten verkiezingen

4. De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen.

Toelichting

Deze eis bepaalt dat de programmatuur gebruikt kan worden bij verschillende typen verkiezingen (bijvoorbeeld voor zowel gemeenteraadsverkiezingen als Tweede Kamerverkiezingen) zonder dat deze daarvoor moet worden aangepast.

Toetskader

Afhankelijk van het type verkiezing zijn er verschillen op de volgende punten:

- *Organisatieniveaus*: Het type verkiezing bepaalt welke organisatorische niveaus voor gemeentelijk stembureau (GSB), hoofdstembureau (HSB) en centraal stembureau (CSB) aanwezig zijn (zie Figuur 2 en Tabel 15) en hoe deze worden ingevuld. Dit heeft gevolgen voor de noodzaak om tussen deze niveaus informatie uit te wisselen.
- *Berekeningen*: De berekening voor de zetelverdeling bij verkiezingen is afhankelijk van het verkiezingstype. De verschillen zijn uitgewerkt in de formele specificatie van de berekeningen (zie [19], tabel pag. 22).

| | Niveau 1 | Niveau 2 | Niveau 3 |
|--|-----------|------------------|-----------|
| Europees Parlement (EP) | Gemeente | Kieskring | Nederland |
| Eerste Kamer (EK) | Provincie | Nederland | |
| Tweede Kamer (TK) | Gemeente | Kieskring | Nederland |
| Provinciale Staten (PS); Aantal kieskringen >1 | Gemeente | Kieskring | Provincie |
| Provinciale Staten (PS); Aantal kieskringen =1 | Gemeente | Provincie | |
| Algemeen Bestuur Waterschap (ABW) | Gemeente | Algemeen Bestuur | |
| Gemeenteraad (GR) | Gemeente | | |

Tabel 15: Overzicht van gebiedsniveaus per verkiezingstype (bron: [26, §1.2]).

Toetsing

Bij de installatie van OSV2020-U is het noodzakelijk aan te geven om welk type verkiezingen het handelt en voor welke organisatieniveau(s) deze zijn. In de huidige versie van de software worden de parameters daartoe vastgelegd in de 'vapp.properties' file die in de folder 'installatiebestanden' aanwezig moet zijn. Zonder dit bestand is installatie niet mogelijk.

Als voorbeeld volgt hierna de betreffende file voor de verkiezingen voor Provinciale Staten met meer dan één kieskring. Daarbij wordt het verkiezingstype vastgelegd in de parameter 'ELECTION_CATEGORY', de mogelijke organisatieniveaus in 'ELECTION_LEVEL' en de verkiezingsdatum in 'ELECTION_DATE'. Op basis van deze parameters wordt tijdens de installatie de juiste versie van de software geïnstalleerd. Tijdens de installatie wordt – indien van toepassing – gevraagd om het niveau (GSB, HSB of CSB) waarvoor de software gebruikt gaat worden. Een installatie van OSV2020-U is dus specifiek voor het type verkiezing en indien van toepassing specifiek voor het niveau. Zo wordt bijvoorbeeld voor de Provinciale Verkiezingen met meer dan één kieskring voor het CSB-niveau de applicatie 'OSV2020-U (PS-CSB)' geïnstalleerd.

```
#
# vapp.properties
#

# set election category
# set election category BC|EK|ER|GR|AB|EP|PS|TK
ELECTION_CATEGORY=PS

# set election level (only election category with election level and not in PP)
ELECTION_LEVEL=A5

# set election date (date format YYYYMMDD)
ELECTION_DATE=20230315

#|-----|
#| Election Category      |
#| (without election level) |
#|-----|
#| BC (Bestuurscommissie) |
#| EK (Eerste Kamer)     |
#| ER (Eilandsraad)      |
#| GR (Gemeenteraad)      |
#|-----|

#|-----|-----|-----|
#| Election Category      |         |         |         |         |         |
#| (with election level)  | PSB | HSB | CSB | PSB,HSB | PSB,HSB,CSB | PSB, CSB_HSB | CSB_HSB |
#|-----|-----|-----|
#| AB (Waterschap)       | A1 |   |   |   |   |   | A7 | A6 |
#| EP (Europees Parlement) | A1 | A2 | A3 | A4 |   | A5 |   |   |
#| PS (Provinciale Staten, 1 Kieskring) | A1 |   |   |   |   |   | A7 | A6 |
#| PS (Provinciale Staten, >1 Kieskring) | A1 | A2 | A3 | A4 |   | A5 | A7 |   |
#| TK (Tweede Kamer)     | A1 | A2 | A3 | A4 |   | A5 |   |   |
#|-----|-----|-----|
```

Bij gecombineerde verkiezingen worden meerdere instanties van OSV2020-U (met elk een eigen database instantie) aangemaakt. Indien dus sprake is van gecombineerde verkiezingen zoals bij de Provinciale Statenverkiezingen en de verkiezingen voor het algemeen bestuur van een waterschap (of meerdere

waterschappen waarvan een gemeente deel kan uitmaken) worden beide verkiezingen door OSV2020-U gefaciliteerd. Deze combinatievariant hebben we kunnen testen.

Na installatie is het noodzakelijk dat de verkiezingsdefinitie wordt ingelezen, anders functioneert het programma niet. Bij het eerste gebruik van het programma moet daarom eerst door de beheerder de verkiezingsdefinitie worden ingelezen. Daarbij worden extra gegevens uitgevraagd die de beheerder eventueel kan aanpassen.

Met de informatie uit de verkiezingsdefinitie en de eventueel aanvullend uitgevraagde gegevens beschikt OSV2020-U over alle informatie om de juiste ondersteuning te bieden voor het betreffende type verkiezing. Zo is bijvoorbeeld bij verkiezingen voor algemene bestuur van Waterschappen met het aantal beschikbare zetels bekend wat het juiste algoritme is voor de telling en het bepalen van de zetelverdeling. De broncode van het zetelberekeningsalgoritme zelf blijft gelijk in elke installatie voor ieder verkiezingstype en wordt, bij het vaststellen van de uitslag, aangeroepen met de parameters die in 'vapp.properties' en het verkiezingsdefinitiebestand staan.

Eenmaal geïnstalleerd kan het programma niet meer voor een ander verkiezing gebruikt worden dan waarvoor het installatieprogramma gebouwd was. Bij een eenmaal geïnstalleerd programma kunnen verkiezingsdefinitie en kandidatenlijst eventueel gewijzigd worden door de 'ingerichte verkiezing' te verwijderen en beide bestanden opnieuw in te lezen.

Toetsoordeel

Het is mogelijk om de programmatuur te gebruiken voor verschillende typen verkiezingen. OSV2020-U kan zonder aanpassingen aan de broncode gebruikt worden bij verschillende verkiezingstypen. Dit gebeurt met parameterinstellingen tijdens installatie en de verkiezingsdefinitie die de beheerder inleest en kan aanpassen.

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.*

Toelichting

De eis waarborgt dat de programmatuur zo wordt ontwikkeld dat foutief gebruik ervan, voor zover mogelijk, wordt voorkomen. Dit houdt bijvoorbeeld in dat invoer van gegevens wordt gecontroleerd op consistentie.

Toetsing

Beveiliging van een softwaresysteem in operationeel gebruik vergt een combinatie van maatregelen in de software zelf, in de infrastructuur waarop deze executeert en de organisatorische context waarin het softwaresysteem gebruikt wordt. Voor deze eis kijken we naar maatregelen die redelijkerwijs technisch mogelijk zijn in de software en de infrastructuur. Bij de beoordeling van deze eis worden relevante maatregelen ten aanzien van de organisatorische context door ons meegewogen.

Ten aanzien van de software geeft de Kiesraad regelmatig opdracht tot uitvoering van pentesten. De bijdrage van de pentesten en de opvolging van aanbevelingen die daaruit voortkomen vallen buitende scope van deze

toets. Het meest recente resultaat van een beveiligingsonderzoek van OSV2020 [29] is via de website van de Kiesraad te raadplegen.

In de software zijn maatregelen genomen voor authenticatie en autorisatie van gebruikers van OSV2020-U. Dit blijkt uit de gebruikershandleiding van OSV2020-U [26, 27]. De beheerder (rol 'admin') en de verkiezingsleider beschikken beide over functionaliteit die niet bij dezelfde persoon terecht mag komen. Voor de implementatie van het 4-ogenprincipe bij invoer van stemresultaten zijn rollen met bijbehorende functionaliteit aanwezig.

CAST AIP (zie Annex C.1.) levert op basis van de sources van OSV2020-U een score voor de beveiliging (security) van 2,73. Dit betreft een redelijke score die ruimte voor verdere verbetering laat zien. Het tool constateert op basis van de sourcecode dat er potentiële beveiligingskwetsbaarheden voorkomen. Een aantal metingen beschouwt CAST als kritisch. Dit is het geval als aangetroffen potentiële kwetsbaarheden een groot effect kunnen hebben als deze zich daadwerkelijk manifesteren. De door CAST als kritisch aangemerkte potentiële kwetsbaarheden zijn opgenomen in Annex C.4 Tabel 33. Daarnaast zijn er kwetsbaarheden tegen CWE (Common Weakness Enumeration; zie: cwe.mitre.org/). Deze zijn opgenomen in Annex C.4 Tabel 34. Ons oordeel is dat deze potentiële kwetsbaarheden onderzocht moeten worden ter verdere verbetering van de beveiliging.



Wat betreft infrastructurele maatregelen voor beveiliging van OSV2020-U geeft de handleiding [26] de volgende informatie:

Air-gapped netwerk [26, §2.1]: Het netwerk waarop de verkiezingssoftware wordt geïnstalleerd mag onder geen enkel beding met internet verbonden zijn. Het netwerk moet een zogenaamd 'air-gapped' netwerk zijn, een netwerk dat geen enkele bedrade en niet bedrade verbinding naar de buitenwereld kent. Zodra het programma een verbinding met het internet vindt, tijdens of na de installatie, sluit het zichzelf af omdat dit wordt gezien als een onveilige installatie en/of situatie.

Beveiligde verbinding naar OSV2020-U-server [26, §2.1]: Er wordt gebruikt gemaakt van versleutelde verbinding tussen server en de erop aangesloten client-pc's, zodat geen gegevens vanaf een ander systeem afgeluisterd kunnen worden.

Beveiligingscertificaat [26, §2.3]: OSV2020-U maakt gebruik van een zelf ondertekend beveiligingscertificaat (self-signed certificate) ter beveiliging / encryptie van de communicatie tussen browser en applicatieserver.

Wachtwoordbeveiliging [26, §7.1]: In OSV2020 wordt afgedwongen dat het wachtwoord minimaal bestaat uit negen karakters met daarin minimaal opgenomen: één hoofdletter, één kleine letter, één cijfer en één bijzonder teken.

Bij een foutieve aanmeldpoging [26, §2.4, pagina 13] wordt een waarschuwing getoond. Er zijn in totaal zes aanmeldpogingen voor ieder gebruikerstype, en kan alleen iemand met rechten van een beheerder het account deblokkeren.

Aanmelden doet de beheerder [26, §2.4, pagina 13] door als gebruiker de naam 'admin' in kleine letters in te geven, en daarna het wachtwoord dat zij ingegeven heeft tijdens de installatie van het programma. Nadat de beheerder 'admin' zich voor het eerst heeft aangemeld moet zij tweemaal een nieuw wachtwoord ingeven. Daarbij dient minimaal één hoofdletter, één kleine letter, één cijfer en één

bijzonder teken in het wachtwoord te zijn opgenomen. Aanmeldnaam en wachtwoord zijn hoofdlettergevoelig. Als per ongeluk de toets CAPS LOCK is aangezet, dan komt er een waarschuwing bij het invoeren van het wachtwoord. Nadat tweemaal het nieuwe wachtwoord is ingevoerd en het wachtwoord aan de voorwaarden voldoet, worden met de knop Aanmelden de nieuwe aanmeldgegevens naar de OSV2020-server verzonden. Vanaf dat moment is het nieuwe wachtwoord van de beheerder actief en het programma vraagt de beheerder zich nogmaals aan te melden met de zojuist ingevoerde gegevens. Daarna opent zich het programma en kan de beheerder nieuwe gebruikers gaan aanmaken.

In de installatiehandleiding [28, pagina 5] wordt aangegeven:

De computers dienen in een gesloten netwerk op elkaar aangesloten te worden, een zogenaamd 'air gapped' netwerk. Het 'fysiek gescheiden netwerk' mag:

- geen koppeling hebben met het internet;
- geen koppeling hebben met de reguliere IT-infrastructuur van de gemeente.

Wordt OSV2020 gebruikt op een laptop of pc met een draadloze netwerkaansluiting (WiFi of Bluetooth), dan dient deze uitgezet te worden om te voorkomen dat de computer (draadloos) van buitenaf benaderd kan worden.

Toetsoordeel

Naar ons oordeel zijn in de software en ten aanzien van de infrastructurele omgeving voldoende maatregelen genomen om foutief gebruik te voorkomen. In de software zijn bij een statische codeanalyse enkele potentiële kwetsbaarheden voor beveiliging aangetroffen. We adviseren om deze te analyseren ter verdere verbetering van de beveiliging.

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.*

Toelichting

In deze eis is vastgelegd dat de programmatuur voor de vermelding van aanduidingen van politieke groeperingen en namen van kandidaten in ieder geval de diakritische tekens ondersteunt die ook in de Basisregistratie Personen voorkomen. Dit betreft een minimumvereiste. Ook letters of symbolen die niet in de Basisregistratie voorkomen mogen in de programmatuur worden ingebouwd. De Kiesraad heeft opgemerkt dat, aangezien de Kieswet bij de registratie van een aanduiding geen enkele beperking aan de letters of tekens stelt die deel uitmaken van de aanduiding, het de voorkeur verdient dit vereiste te schrappen. Anders zou het volgens de Kiesraad kunnen gebeuren dat een aanduiding wel bij het centraal stembureau kan worden geregistreerd, maar vervolgens niet correct kan worden weergegeven. Het is inderdaad zo dat er een verschil zou kunnen ontstaan tussen de bij het centraal stembureau geregistreerde aanduiding en de naamgeving in de programmatuur. Dit zou evenwel geen noemenswaardige problemen moeten opleveren, aangezien de verkiezingssoftware de uitslag niet vaststelt, maar deze alleen berekent. Het is vervolgens aan het centraal stembureau erop toe te zien dat de aanduiding in de officiële stukken eenvormig en correct wordt weergegeven.

De tekenset van de Basisregistratie Personen betreft een minimumeis. Uitgebreidere tekensets, zoals Unicode, zijn uiteraard ook toegestaan.

Toetskader

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 [4] luidt: "Onze Minister stelt een systeembeschrijving vast".
- 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 [5] wordt de systeembeschrijving gevormd door "de niet als toelichting gemarkeerde delen van het Logisch Ontwerp BRP, versie 4.0.0, bedoeld in artikel 3".
- In artikel 3 van de regeling wordt voor Logisch Ontwerp BRP, versie 4.0.0 verwezen naar bijlage 1 bij de regeling. Daarin is beschreven dat: "Deze bijlage wordt bekendgemaakt op www.rvig.nl". De genoemde versie 4.0.0 is niet meer beschikbaar.
- Op 22-10-2022 is versie 4.1 van het Logisch Ontwerp BRP [6] in werking getreden. Daarin wordt in paragraaf 5.1.1 voorgeschreven welke tekens, gebaseerd op de Teletex-standaard, binnen het BRP-systeem gebruikt mogen worden en hoe deze te coderen.

Toetsing

Om het gebruik van diakritische tekens te testen hebben we de volgende stappen uitgevoerd:

- Eerst hebben we de tekenset uit het Logisch Ontwerp GBA [6], paragrafen 5.1.1.2, 5.1.1.2 en 5.1.1.3 overgenomen in dit document (zie D.1 en D.2).
- Vervolgens hebben we in OSV2020-U een kandidatenlijst geladen waarbij in de achternaam van kandidaten en in de partijnamen diakritische tekens vanuit Word zijn gekopieerd. Visueel is gecontroleerd of de betreffende karakters op het scherm verschijnen.
- Daarna zijn alle documenten met OSV2020-U aangemaakt. Zowel in de gegenereerde odt- als 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 'Annex D Tekenset basisregistratie personen'. In het eml-bestand wordt er terecht voor gezorgd dat tekens die een bijzondere betekenis hebben in EML zoals '&' en '<' worden vervangen door & en < respectievelijk.
- 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.

Toetsoordeel

We constateren dat de programmatuur diakritische tekens van de GBA-tekenset correct verwerkt.

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.

Toelichting

In deze eis wordt het gebruik van open standaarden en open source voorgeschreven. Specifiek voor wat betreft verkiezingsgegevens (zoals de kandidatenlijst en de uitslaggegevens) wordt het gebruik van de EML_NL standaard verplicht gesteld.

Open standaarden bevorderen dat keuzevrijheid is geborgd, doordat zij naar hun aard niet leverancier-specifiek zijn en door iedere ICT-leverancier kunnen worden gehanteerd. Dit leidt tot kwalitatief hoogwaardige en kostenefficiënte informatie-uitwisseling door de overheid. Daarnaast leidt het gebruik van open standaarden tot een open en transparante ontwikkeling van de programmatuur en een open en transparant beheer van de programmatuur. Dat geldt ook voor de toepassing van open source. De Kiesraad is van mening dat het vereiste te algemeen is geformuleerd, waardoor het ook op alle uitvoer van de programmatuur betrekking heeft en in de praktijk niet hanteerbaar zou zijn. Om tegemoet te komen aan het commentaar van de Kiesraad is aan het vereiste toegevoegd dat waar het centraal stembureau kan aantonen dat het gebruik van open standaarden en of open source niet mogelijk is daarvan kan worden afgezien. In zulke gevallen zal wel technologie moeten worden toegepast waarvan de doeltreffendheid in de praktijk is aangetoond, zogenaamde 'proven technology', en die direct toepasbaar is.

Voor de verkiezingsgegevens (waaronder kandidatenlijsten en zetelverdeling) wordt de open standaard EML_NL gebruikt (zie: [9]). EML_NL komt voort uit de EML versie 5.0 van OASIS en is aangepast aan het Nederlandse kiesrecht. EML_NL heeft tot doel de gegevensuitwisseling (de interoperabiliteit) tussen verschillende programmatuur te waarborgen. De verkiezingssoftware wordt gebruikt door politieke partijen, gemeenten, hoofd- en centrale stembureaus. De Kiesraad beheert de open standaard EML_NL en de doorontwikkeling ervan. Het meest actuele specificatiedocument van EML_NL kan gevonden worden op de website van de Kiesraad.

Toetsing

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 verspreiden¹¹.
- *Open standaarden:* ICT-standaarden zijn afspraken over de manier om gegevens uit te wisselen. Overheden en bedrijven kunnen met open standaarden makkelijker met elkaar communiceren. Bijvoorbeeld als zij facturen sturen. De overheid zelf hanteert voor open standaarden het 'pas toe, of leg uit'-principe:
 - *Pas toe:* bij een ICT-dienst of -product kiest een overheidsorganisatie een open standaard van de 'pas toe, of leg uit'-lijst.
 - *Leg uit:* een overheidsorganisatie mag alleen voor een andere standaard kiezen als een open standaard tot problemen leidt. De organisatie moet dit wel uitleggen in het jaarverslag.

¹¹. Zie: www.rijksoverheid.nl/onderwerpen/digitale-overheid/open-overheid.

Door het Forum Standaardisatie wordt de lijst van standaarden bijgehouden¹² waarvan wordt aangegeven in hoeverre deze verplicht zijn. Voor deze standaarden geldt het 'Pas toe of leg uit'-beleid.

Toetsoordeel

De enige standaard die bij digitale informatie-uitwisseling binnen OSV2020-U gebruikt wordt, is de EML_NL-standaard¹³ [9]. Versie 1.0 daarvan is opgenomen in de lijst met verplichte open standaarden¹⁴ van Forum Standaardisatie en voldoet aan de gestelde eis¹⁵.

Bij het genereren van uitvoer bestanden maakt OSV2020 gebruik van de volgende formaten.

- *PDF, Portable Document Format*: Het blijkt dat OSV2020 pdf-documenten in versie 1.6 levert. In de verplichte 'pas toe of leg uit'-lijst is PDF opgenomen met versies PDF 1.7, PDF/A-1 en PDF/A-2. Daarbij is het uitdrukkelijke advies opgenomen om naar een van deze formaten te migreren. Er wordt opgemerkt dat vaak nog oudere versies van PDF worden gebruikt die niet door ISO worden ondersteund, bijvoorbeeld PDF 1.4, 1.5 en 1.6. Deze versies worden door een leverancier onderhouden, kwalificeren niet als open standaarden en kunnen beter niet worden gebruikt.
- *ODT, Open Document Text*: Dit formaat is onder ODF – Open Document Format opgenomen in de verplichte 'pas toe of leg uit'-lijst. In OSV2020-U heeft de gebruiker veelal de keuze om te kiezen tussen output in PDF- of ODT-formaat of beide.
- *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.*

Toelichting

In de eis is bepaald dat de standaard programmatuur waar voor het berekenen van de uitslag en de zetelverdeling gebruik van wordt gemaakt vrij verkrijgbaar moet zijn. In artikel P 1, vijfde lid, van het Kiesbesluit is vastgelegd dat de broncode van de programmatuur openbaar wordt gemaakt. Door alle maatwerkprogrammatuur te publiceren en te vermelden welke standaard programmatuur met welke instellingen wordt gebruikt, kan eenieder die dat wil zelf een testopstelling maken en nagaan of het geheel onder alle omstandigheden goed functioneert. Er mogen dan geen belemmeringen zijn zoals het gebruik van maatwerkprogrammatuur die van de leverancier niet gepubliceerd mag worden of standaard programmatuur die niet vrij verkrijgbaar is. In die gevallen zou namelijk een 'zwart gat' in de programmatuur ontstaan waarvan de werking niet kan worden nagegaan.

Toetsing

Uitgangspunt is dat de broncode van OSV2020-U door de Kiesraad via haar website vrij beschikbaar wordt gesteld. Dit is momenteel nog niet gebeurd. Dit gebeurt standaard op de dag van de kandidaatstelling. Voor de verkiezingen van Provinciale Staten en Waterschappen in 2023 is dit op 30 januari 2023. Met de sources is het

¹². Zie: www.forumstandaardisatie.nl/open-standaarden.

¹³. Zie: www.kiesraad.nl/verkiezingen/osv-en-eml/eml-standaard.

¹⁴. Zie: www.forumstandaardisatie.nl/open-standaarden/verplicht.

¹⁵. Zie: www.forumstandaardisatie.nl/open-standaarden/emlnl.

mogelijk om inzage te verkrijgen in de manier waarop de algoritmes in de sources zijn uitgewerkt die nodig zijn voor de vaststelling van het verkiezingsresultaat en de zetelverdeling. De laatste keer dat de software van OSV2020-U beschikbaar is gesteld¹⁶ betrof dit versie 1.4.3 voor de Gemeenteraadsverkiezingen van 2022.

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.

Bij de sources van OSV2020-U is door de leverancier één tekstbestand aangeleverd (THIRD-PARTY.txt) met informatie over de gebruikte softwareproducten van externe partijen inclusief licentie van het softwareproduct en de website waar het product gevonden kan worden. Daarin worden 98 externe producten benoemd.

Op basis van alleen de sources is het niet mogelijk om een operationele versie van OSV2020-U te creëren. Er ontbreken onder andere gebruikte externe softwareproducten en scripts en handleidingen voor installatie van de software. Daardoor is het niet mogelijk dat iedereen een testopstelling kan maken zoals wordt vereist in de toelichting bij deze eis.

De Kiesraad heeft toegezegd dat bij de publicatie van de sources een mogelijkheid voor gebruikers wordt gecreëerd om een operationele versie van het systeem te verkrijgen. De kopie van de OSV2020-U software is uitsluitend bestemd voor eigen gebruik en analyse. Na invulling van een formulier wordt de software via secure transfer verzonden. De ontvanger krijgt een link voor het downloaden van de software per e-mail en een sms-code op de mobiel. De downloadlink heeft een beperkte geldigheidsduur.

Toetsoordeel

Voor iedereen die een testopstelling van OSV2020-U wil maken wordt een mogelijkheid beschikbaar gesteld om een kopie van het systeem aan te vragen voor eigen gebruik en analyse. De sources van OSV2020-U worden op de website van de Kiesraad publiekelijk beschikbaar gesteld. Van de leverancier hebben we een tekstbestand ontvangen met informatie over gebruikte externe softwareproducten en hun bijbehorende licentiering. Op basis van analyse en inspectie van de geleverde sources blijkt het merendeel publiek beschikbaar met publieke licentie.

4.9 Intellectueel eigendom

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

Toelichting

Indien de programmatuur voor een centraal stembureau wordt ontwikkeld, moeten de intellectuele eigendomsrechten van deze programmatuur bij een centraal stembureau berusten. Deze verplichting is in deze eis verankerd. Indien het centraal stembureau niet over het intellectueel eigendomsrecht van de gehele programmatuur kan beschikken, omdat bijvoorbeeld onderdelen ervan als open source zijn ontwikkeld, betekent dit evenwel niet dat daarmee niet aan de eis is voldaan. Het centraal stembureau moet in ieder geval

¹⁶. Zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2022/1/31/broncode-osv2020-u-gemeenteraadsverkiezing-2022.

het intellectueel eigendomsrecht bezitten op maatwerkprogrammatuur die in opdracht van het centraal stembureau is ontwikkeld.

Toetsing

De ontwikkeling van OSV2020-U is onderdeel van de werkzaamheden voor beheer en onderhoud van Ondersteunende Software Verkiezingen (OSV).

In juli 2015 is een overeenkomst [11] 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.

In oktober 2019 zijn overeenkomsten [17, 18] getekend tussen de Staat der Nederlanden en IVU.elect GmbH. De overeengekomen nadere overeenkomst heeft een looptijd van 9 oktober 2019 en deze eindigt op 13 juli 2022. De overeengekomen aanpassingen in de overeenkomsten hebben geen betrekking op afspraken over intellectueel eigendom zodat de eerdere afspraken daarover nog steeds rechtsgeldig zijn.

Door een wijzigingsovereenkomst tussen de Staat der Nederlanden en Elect IT [30] wordt de looptijd van de nadere overeenkomst voortgezet tot en met 13 juli 2025. In deze overeenkomst wordt verwezen naar ARBIT 2018 [24]. De intellectuele eigendomsrechten zijn geregeld in artikel 24:

- 24.1 Tenzij anders overeengekomen komen alle auteursrechten die kunnen worden uitgeoefend – waar en wanneer dan ook – ten aanzien van de resultaten van de verrichte Diensten toe aan Opdrachtgever. Deze intellectuele eigendomsrechten worden op grond van de Overeenkomst door Opdrachtnemer op het moment van het ontstaan daarvan aan Opdrachtgever overgedragen, welke overdracht door Opdrachtgever reeds nu voor alsdan wordt aanvaard.

Toetsoordeel

Met de in ARBIT-2014 en ARBIT 2018 beschreven interpretatie van het intellectueel eigendomsrecht voldoet OSV2020-U 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.*

Toelichting

De eis ziet erop dat niet alleen de broncode openbaar is maar dat ook de manier waarop de broncode door de computer wordt uitgevoerd transparant is. De broncode wordt namelijk niet direct door een computer verwerkt. Daarvoor is nog programmatuur nodig (een zogenaamde compiler of interpreter) die ervoor zorgt dat de broncode door de computer verwerkt kan worden. Op grond van deze eis dient ook die programmatuur als open source beschikbaar te zijn.

Toetsing & toetsoordeel

De programmatuur voor OSV2020 is geschreven in Java. De leverancier geeft aan gebruik te maken van de compiler: Amazon Corretto 11¹⁷.

Voor Java zijn meerdere compilers beschikbaar¹⁸ waarvan diverse als open source. Open source compilers zijn onderdeel van de veelgebruikte, geïntegreerde ontwikkelomgeving (IDE – Integrated Development Environment) van bijvoorbeeld IntelliJ IDEA, Eclipse IDE, NetBeans en JDeveloper.

4.11 Verschillende besturingssystemen

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

Toelichting

De eis ziet erop toe dat de programmatuur voor meer dan één besturingssysteem wordt ontwikkeld. Zo wordt verzekerd dat de programmatuur ook op een open source besturingssysteem is te gebruiken. De achtergrond van dit vereiste is het beperken van de afhankelijkheid van één leverancier.

Toetsing

In de installatiehandleiding [28, pagina 4 en 5] worden de volgende eisen aan de besturingssystemen gesteld.

| Serververeisten en gecombineerde client-serververeisten voor OSV2020 | |
|--|---|
| Besturingssysteem | Windows: <ul style="list-style-type: none">• Windows 10, Windows Server 2016 (of nieuwer) Linux: <ul style="list-style-type: none">• Ubuntu 20.04 LTS of nieuwer Mac OS X: <ul style="list-style-type: none">• 10.15 of nieuwer |
| Client PC vereisten | |
| Besturingssysteem | Windows 10 compatible besturingssysteem |

Tabel 16: Systeemvereisten voor het te gebruiken besturingssysteem voor OSV2020-U.

¹⁷. Zie: aws.amazon.com/corretto.

¹⁸. Zie bijvoorbeeld: www.softwaretestinghelp.com/best-java-ide-and-online-compilers.

Bij de systeemvereisten OSV2020-U die de Kiesraad op de website publiceert [25], worden de volgende eisen gesteld.

Minimale systeemconfiguratie voor OSV2020-U

| | |
|--------------------------|--|
| Besturingssysteem | Gebruik een recente en ondersteunde versie van: <ul style="list-style-type: none">• <i>Windows</i>: Windows 10 (64-bit), Windows Server 2016 (64-bit) of nieuwer met beheerdersrechten gebruiker.• <i>Linux</i>: 64bit versie, bijvoorbeeld Ubuntu 20.04 (minimaal kernel 4.19)• <i>MacOS</i>: Versie 10.15 of nieuwer (64-bit compatible of Rosetta 2 bij de M1 processorarchitectuur). Maak uitsluitend gebruik van een besturingssysteem waarvoor (beveiligings)updates beschikbaar zijn. |
|--------------------------|--|

Tabel 17: Systeemvereisten voor het te gebruiken besturingssysteem voor OSV2020-U.

Uit eigen ervaring blijkt dat het systeem draait op een Windows 10.0 besturingssysteem en een Linux besturingssysteem (Ubuntu LTS 22.04). Bij de installatie op Linux bleken twee extra packages noodzakelijk te zijn. Het betreft de packages net-tools¹⁹ en libnss3-tools²⁰ die geen standaard onderdeel zijn van de Ubuntu installatie. Van net-tools wordt het commando netstat gebruikt en van libnss3 het commando setutil. De installatiehandleiding [28] is vooral gericht op de Windows-installatie. Deze bevat slechts summiere informatie voor de Linux installatie. Zonder diepgaande kennis van Linux (en Ubuntu) is installatie problematisch.

Toetsoordeel

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 OSV2020-U voor tenminste één open source besturingssysteem is ontwikkeld.

4.12 Authenticiteit programmatuur

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

Toelichting

Zie de nadere toelichting bij de volgende eis (in 4.13).

Toetsing

In de installatiehandleiding [28, pagina 5] wordt aangegeven:

OSV2020-U wordt geleverd als ZIP-bestand op DVD. Voordat dit ZIP-bestand uitgepakt kan worden, dient eerst de authenticiteit hiervan vastgesteld te worden. Op de website van de Kiesraad (kiesraad.nl) wordt dit nader uitgelegd. Na het vaststellen van de authenticiteit wordt het ZIP-bestand van DVD (of andere gegevensdrager) naar het PC-systeem gekopieerd waarop de OSV2020 software geïnstalleerd

¹⁹. Zie: sourceforge.net/projects/net-tools.

²⁰. Zie: pkgs.org/download/libnss3-tools.

gaat worden. Vanaf het PC-systeem wordt het ZIP-bestand nu uitgepakt, dit gaat dan uitpakken terwijl het ZIP-bestand nog op DVD staat.

Bij leveringen van OSV2020-U worden de installatiebestanden als één gecomprimeerd bestand (in zip-formaat) uitgeleverd. In de levering die we hebben ontvangen [33] bevat het zip-bestand een aantal tekstbestanden:

- nl-installer-was-1.8.2.3-OSV2020-U-installer.zip.sha256
- nl-installer-was-1.8.2.3-OSV2020-U-installer.zip.sha512
- nl-installer-was-1.8.2.3-tools.zip.sha256
- nl-installer-was-1.8.2.3-tools.zip.sha512
- nl-installer-was-1.8.2.3-utils.zip.sha256
- nl-installer-was-1.8.2.3-utils.zip.sha512

Deze bevatten respectievelijk de SHA-256 hash-codes²¹ en de SHA-512 hash-codes. Beide hash-codes zijn over de complete installatie (2022-12-02_WAS_1.8.2.3.zip) aangemaakt.

Zoals in de installatiehandleiding [28] is aangegeven is het de bedoeling dat vóór installatie de authenticiteit wordt vastgesteld volgens de informatie op de website van de Kiesraad. De nadere uitleg voor deze authenticiteitscontrole [22] zal te vinden zijn op die website. Daar is beschreven dat de hash-code van geleverde OSV2020 zip-bestand moet worden vergeleken met de hash-code die op die website staat. De werkwijze om de hash-code te bepalen is afhankelijk van het besturingssysteem dat wordt gebruikt.

De authenticiteitscontrole van de installatiebestanden wordt niet afgedwongen. Als 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. Aangezien OSV2020 air-gapped werkt, is de kans dat iemand dit voor elkaar krijgt uitermate klein.

Toetsoordeel

De nadere toelichting voor uitvoering van de authenticiteitscontrole bij installatie en de hash-codes wordt gepubliceerd op de website van de Kiesraad.

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.*

Toelichting

Met deze eis in combinatie met de eis voor authenticiteit van de programmatuur (4.12) is vastgelegd dat alle elektronische communicatie van of naar andere programmatuur, hetzij via een netwerk, via opslagmedia of

²¹. Een hash-code is een berekende waarde. In dit geval bestaat deze uit een aantal hexadecimale cijfers. Een voorbeeld hash-code is: cd09 2c5f 5340 80ce 3337 920e 9979 e875 1e53 6e01 486c 6d77 d3a6 a9d6 e329 dd51.

anderszins, is voorzien van een mogelijkheid om de authenticiteit van de gegevens vast te stellen, bij voorkeur door middel van een gekwalificeerde elektronische handtekening. Een gekwalificeerde elektronische handtekening is een handtekening waarbij een gekwalificeerd certificaat is gebruikt. Een gekwalificeerd certificaat is een digitaal bestand dat aan het oorspronkelijke document is toegevoegd. Er zijn speciale instanties die certificaten uitgeven, de zogeheten certificatieinstanties. De Nederlandse overheid maakt gebruik van een certificaat dat wordt uitgegeven door Public Key Infrastructure (PKI)-overheid.

Toetsing

Bij het aanmaken van een elektronisch bestand voor berichtuitwisseling (EML-bestand) berekent OSV2020 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 bestand aangemaakt met de hash-code.

Er is een zevental verschillende bestandstypen die door OSV2020-U worden ingelezen. De mogelijkheden voor inlezen van deze bestanden zijn afhankelijk van het organisatieniveau waarvoor de applicatie wordt gebruikt: gemeentelijk stembureau (GSB), hoofdstembureau (HSB) of centraal stembureau (CSB) (zie Figuur 1 en Figuur 2). Het betreft:

- *Verkiezingsdefinitie EML-110a (GSB, HSB, CSB)*: Dit bestand bevat een aantal basisgegevens van de verkiezing en wordt aangemaakt met OSV2020-KS. Na installatie van OSV2020-U kan de beheerder dit EML-bestand inlezen van cd-rom of USB-stick. Daarbij wordt gevraagd de gepresenteerde hash-code van het bestand te controleren met de hash-code in het meegeleverde tekstbestand dat tegelijk met de verkiezingsdefinitie is gegenereerd door OSV2020-KS (zie [26, pag.40]). De beheerder moet bevestigend doorklikken zonder daadwerkelijk een controle uit te voeren omdat er geen andere opties zijn.
- *Kandidatenlijsten EML-230b (GSB, HSB)*: Dit bestand bevat de kandidatenlijsten. Ook dit bestand wordt aangemaakt met behulp van OSV2020-KS en wordt door de beheerder ingelezen in OSV2020-U waarbij gevraagd wordt de hash-code te completeren (zie Figuur 7). De hash-code wordt gepresenteerd waarbij willekeurig twee maal vier cijfers onleesbaar zijn gemaakt. De ontbrekende cijfers moeten ter controle door de gebruiker worden ingevuld (zie [26, pag.43]).
- *Totaallijsten EML-230c (CSB)*: Dit bestand bevat kandidatenlijsten met uitgebreidere informatie en wordt eveneens aangemaakt met OSV2020-KS en ingelezen door de beheerder. Daarbij wordt dezelfde controle uitgevoerd als bij de Kandidatenlijsten.
- *Stembureaus EML-110b (GSB)*: Als een GSB een EML-bestand met informatie over stembureaus voorhanden heeft bijvoorbeeld van de vorige verkiezing, kan dit bestand in OSV2020-U ingelezen worden en aangepast door de beheerder. Bij inlezen van het bestand in OSV2020-U wordt niet gevraagd de authenticiteit van dit bestand te controleren.
- *Telling stembureau EML-510a (GSB)*: Een enkele gemeente beschikt over een applicatie waarmee tellingen van individuele stembureaus ondersteund worden. Het resultaat van de telling kan ingelezen worden in OSV2020-U. Volgens de Kiesraad is deze werkwijze formeel niet toegestaan. Het betreffende bestand kan ook gegenereerd zijn als back-up uit het eigen systeem. De verkiezingsleider kan in plaats van de eerste handmatige invoer het tellingbestand inlezen. Er moet altijd een tweede handmatige invoer door een andere gebruiker worden uitgevoerd waarvan de gegevens overeen moeten komen met de eerste invoer. Bij eventuele verschillen bepaalt de verkiezingsleider expliciet welke invoer de definitieve wordt op basis van expliciet aangegeven fouten en waarschuwingen met betrekking tot de verschillen tussen beide invoeren.
- *Telling gemeente EML-510b (HSB)*: Dit EML-bestand bevat de tellingen van een gemeente en is afkomstig uit GSB. Vanuit OSV2020-U GSB wordt een zip-file gegenereerd die het EML-bestand bevat en de

persoonlijke sleutel. Net als bij Telling stembureau kan de verkiezingsleider dit bestand inlezen als eerste invoer voordat sprake is van handmatige invoer. Voordat een tellingbestand kan worden ingelezen, wordt eerst de elektronische handtekening gecontroleerd. De elektronische handtekening kan alleen herkend worden met de publieke sleutel die door de beheerder is ingevoerd bij de gemeente waarvoor het bestand wordt ingelezen. Vervolgens vraagt de software om de ontbrekende delen van de hash-code aan te vullen. De gevraagde hash-code staat in de voettekst van het begeleidende proces-verbaal bij het elektronische tellingbestand.

- *Telling kieskring EML-510c (CSB)*: Dit bestand bevat de tellingen van de kieskring en is afkomstig uit HSB. Bij inlezen op CSB-niveau worden dezelfde controles op basis van de publieke sleutel en de hash-code uitgevoerd als bij het inlezen van de Telling gemeente op HSB-niveau.

Op basis van voorbeelden hebben we een Verkiezingsdefinitie, Kandidatenlijsten en Totaallijsten aangemaakt en deze vervolgens ingelezen in OSV2020-U. Als we het EML-bestand van de Verkiezingsdefinitie aanpassen kunnen we de aangepaste versie zonder problemen inlezen in OSV2020-U. De gevraagde controle van de hash-code is eenvoudig te omzeilen. De enige optie om verder te komen is de selectie van 'Hash-code is correct'.





Figuur 6: Importeren verkiezingsdefinitie met hash-code controle.

Bij het inlezen van de Kandidatenlijsten en Totaallijsten moet de hash-code worden aangevuld (zie Figuur 7). Het is mogelijk om de betreffende bestanden aan te passen. Vervolgens moet een correcte hash-code voor het aangepaste bestand geproduceerd worden. Dat vereist een geïnstalleerd programma om hash-codes te berekenen of internet-toegang. Een programma zoals Notepad++ levert deze functionaliteit.

TK_2021 17 mrt. 2021 [Instellen verkiezingsgegevens] [GSB] 0158 - Haaksbergen 2 Administratie

Importeren kandidatenlijsten

Oorspronkelijke bestandsnaam: Kandidatenlijsten_TK2021_Zwolle.eml.xml
Documenttype: EML 230b (Kandidatenlijsten) (XML)
Hash-code (SHA256): 4BC0 ▲▲▲▲ 9BA8 5E48 A049 ▼▼▼▼ 9F84 5BDA 903D 6659 4768 FCF3 1962 5D8E E3B4 4059

▲▲▲▲ * 
▼▼▼▼ * 

IMPORT-PREVIEW

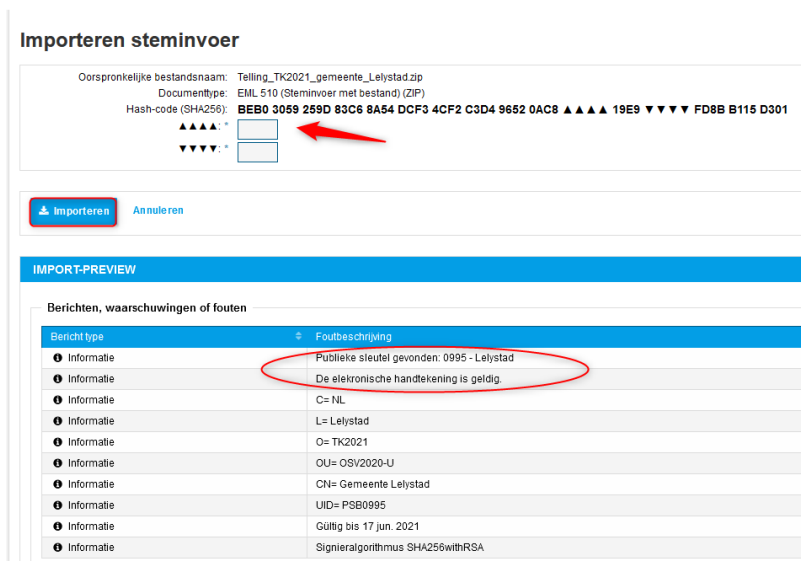
Berichten, waarschuwingen of fouten

| Bericht type | Foutbeschrijving |
|--------------|--|
| ● Informatie | Partij met ID Groen wordt aangemaakt |
| ● Informatie | Partij met ID CDA wordt aangemaakt |
| ● Informatie | Partij met ID VVD wordt aangemaakt |
| ● Informatie | Partij met ID Partij van de Arbeid (P.v.d.A.) wordt aangemaakt |
| ● Informatie | Partij met ID CU /SGP wordt aangemaakt |

Figuur 7: Importeren kandidatenlijsten met hash-code controle.

In OSV2020-U GSB hebben we Stembureaus en Telling Stembureau ingelezen waarbij handmatig aangebrachte veranderingen in deze bestanden geen probleem opleveren bij inlezen. De software controleert of het bestandsformaat correct is. De gebruiker hoeft geen daadwerkelijk controle op authenticiteit uit te voeren.

De Tellingen-bestanden (stembureau 510a, gemeente 510b, kieskring 510c) kunnen alleen als eerste invoer worden ingelezen door de verkiezingsleider (zie Figuur 8). Er vindt dus altijd een controle van de invoer plaats met handmatige invoer van de tellingsgegevens die als tweede invoer is vereist. Elke handmatige invoer moet worden uitgevoerd door een gebruiker die daartoe geautoriseerd is door de beheerder van OSV2020-U. Bij een conflict tussen de eerste en tweede invoer, kan alleen de verkiezingsleider dit conflict oplossen. Daarbij heeft hij/zij de mogelijkheid om een van beide invoeren te selecteren en deze definitief te maken. Daarmee wordt het 4-ogenprincipe deels ontkracht.



Figuur 8: Importeren steminvoer met controle van publieke sleutel en hash code controle.

Om succesvol Telling gemeente (EML-510b) in te lezen in OSV2020-U HSB en Telling Kieskring in OSV20202-U CSB (EML-510c) wordt eerst de publieke sleutel gecontroleerd. Deze sleutel is meegeleverd bij het tellingbestand en wordt herkend met behulp van de publieke sleutel die door de beheerder is ingevoerd bij de gemeente / kieskring waarvoor het bestand wordt ingelezen. Indien de publieke sleutel ontbreekt heeft dat geen gevolgen.

Toetsoordeel

OSV2020-U gebruikt verschillende manieren waarop bij het importeren van een bestand al dan niet controle ten aanzien van de authenticiteit wordt afgedwongen:

- *Geen controle:* Bij Stembureaus (EML-110b) en Telling stembureau (EML-510a).
- *Check gehele hash-code:* Bij Verkiezingsdefinitie (EML-110a).
- *Controle door aanvullen hash-code:* Bij Kandidatenlijsten (EML230-b) en Totaallijsten (EML230-c)
- *Controle door aanvullen hash-code en met publieke sleutel:* Telling gemeente (EML-510b) en kieskring (EML-510c).

De Kiesraad en de leverancier geven aan dat gebruiksvriendelijkheid van OSV2020 belangrijk is geweest in de afweging van de gekozen beveiligingsniveaus en hun implementatie. 'Geen controle' is noodzakelijk als het gaat om het importeren van bestanden die binnen de eigen organisatie zijn aangemaakt. Omdat bij installatie de parameters voor de verkiezingsdefinitie al zijn vastgelegd heeft de import van de Verkiezingsdefinitie alleen een verifiërende taak en is visuele inspectie van de gehele hash-code voldoende waarborg. De controle door aanvullen van de hash-code, bij tellingen aangevuld met controle van de publieke sleutel, vormen barrières tegen import van niet-geauthentiseerde bestanden.

Voor tellingen stembureau (EML-510a) wordt de authenticiteit bij inlezen niet gecontroleerd. De tweede invoer moet hierbij zorgen voor controle van de bij de eerste invoer ingelezen informatie. Technisch gezien zijn er mogelijkheden ook deze bestanden te voorzien van hash-code en elektronische handtekening. Met de leverancier van een externe app die tellingen levert moeten dan afspraken gemaakt worden over uitwisseling van zo'n handtekening. We adviseren om te overwegen een dergelijke beveiliging aan te brengen.

Annex A Bronmateriaal

A.1 Wet- en regelgeving

1. *Kieswet*, Geldend van 01-01-2023 t/m heden, Wet van 28 september 1989, houdende nieuwe bepalingen inzake het kiesrecht en de verkiezingen, zie: wetten.overheid.nl/BWBR0004627/2023-01-01.
2. *Kiesbesluit*, Geldend van 01-01-2023 t/m heden, Besluit van 19 oktober 1989, houdende vaststelling van nieuwe voorschriften ter uitvoering van de Kieswet, zie: wetten.overheid.nl/BWBR0004632/2023-01-01.
3. *Kiesregeling*, Geldend van 01-01-2023 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/BWBR0034180/2023-01-01.
4. *Besluit basisregistratie personen*, Geldend van 22-10-2022 t/m heden, Besluit van 28 november 2013, houdende regels ter uitvoering van de Wet basisregistratie personen (Besluit basisregistratie personen), zie: wetten.overheid.nl/BWBR0034306/2022-10-22.
5. *Regeling basisregistratie personen*, Geldend van 01-01-2023 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/BWBR0034327/2023-01-01.
6. *Logisch Ontwerp BRP, versie 4.1*, 21-10-2022, zie: www.rvig.nl/documenten/publicaties/2022/10/21/logisch-ontwerp-brp-4.1.
7. *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. 29577, 22-10-2014, zie: zoek.officielebekendmakingen.nl/stcrt-2014-29577.html.
8. *Wet nieuwe procedure vaststelling verkiezingsuitslagen*, Geldend van 01-01-2023 t/m heden, Wet van 15 juni 2022 tot wijziging van de Kieswet in verband met de aanpassing van de procedure voor de vaststelling van verkiezingsuitslagen alsmede regeling van enkele andere onderwerpen in die wet, de Waterschapswet, de Mediawet 2008 en de Mediawet BES (Wet nieuwe procedure vaststelling verkiezingsuitslagen), zie: wetten.overheid.nl/BWBR0047041/2023-01-01.

A.2 Documenten

9. *EML_NL 1.0, Het Nederlandse profiel van de EML 5.0; EML_NL – Het bestandsformaat voor de uitwisseling van gegevens voor de vaststelling van de uitslag van verkiezingen (inclusief de zetelverdeling)*, 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.
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. *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.
12. *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.
13. *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.
14. *Gedetailleerde specificatie Ondersteunende Software Verkiezingen (OSV); Kiesraad, IVU*, versie: 1.5.2, status: gecontroleerd, aangemaakt: 13-10-2008, laatste wijziging volgens titelblad: 28-04-2017, laatste wijziging volgens wijzigingshistorie: 01-02-2018, zie: www.kiesraad.nl/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-gedetailleerde-specificaties.
15. *Formele beschrijving van de berekening van de zetelverdeling*, 20-11-2017, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/formele-beschrijving-berekening-zetelverdeling.
16. *Toetsing Ondersteunende Software Verkiezingen (OSV), Definitieve rapportage*, SQS Nederland, versie 1.0, status: definitief, datum: 26-01-2018, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/osv-toetsingsrapport-sqs-osv-programma-4-en-5-26-1-2018.
17. *Nadere overeenkomst Beheer/Onderhoud OSV bij de Raamovereenkomst ARBIT inzake Ondersteunende Software Verkiezingen (OSV)*, Contractnummer: 201850024.154.001, ondertekend: 23-10-2019.
18. *Wijzigingsovereenkomst ARBIT-2014 inzake de Ondersteunende Software Verkiezingen (OSV)*, Contractnummer: 201400114.166.002_2, ondertekend: 23-10-2019.
19. *Determination of the Election Result*, auteur: Joachim Nottebaum, versie 7.3, 01-10-2020, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/determination-of-the-election-result.
20. *Toetsing Verkiezingssoftware OSV2020, Eindrapportage*, Expleo Netherlands, versie 2.0, status: definitief, datum: 27-01-2021, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2021/02/01/expleo-toetsingsrapport-osv2020.
21. *Information technology — Software measurement — Software quality measurement — Automated source code quality measures*. ISO/IEC. referentienummer: ISO/IEC 5055:2021(E). publicatiedatum: 01-04-2021.
22. *Vaststellen van de authenticiteit van de OSV2020 software*, Kiesraad, notitie, versie: 10-09-2021, zie: www.kiesraad.nl/adviezen-en-publicaties/formulieren/2020/10/5/vaststellen-van-de-authenticiteit-van-de-osv2020-software.
23. *Onderzoek Ondersteunende Software Verkiezingen (OSV2020-U), Rapportage voor de Kiesraad*, KPMG, status: Publicatieversie, referentie: A21.00024769 D5.1, 28-01-2022, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/rapporten/2022/1/31/toetsingsrapport-osv2020-u.
24. *Besluit vaststelling Algemene Rijksvoorwaarden voor inkoop (ARBIT-2018, ARIV-2018 en ARVODI-2018), Geldend van 10-09-2022 t/m heden*, Besluit van de Minister-President, Minister van Algemene Zaken van 3 mei 2018, nr. 3219106 houdende vaststelling van de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2018 (ARBIT-2018), de Algemene Rijksinkoopvoorwaarden 2018 (ARIV-2018) en de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten 2018 (ARVODI-2018), zie: wetten.overheid.nl/BWBR0040889/2022-09-10.

25. *Bijlage 3 Systeemvereisten OSV2020 U (uitslagvaststellingsoftware)*, Kiesraad, versie: 13 09 2022, zie: www.kiesraad.nl/adviezen-en-publicaties/formulieren/2020/10/5/systeemvereisten-osv2020-u.
26. *Handleiding Ondersteunende Software Verkiezingen (OSV2020)*, OSV2020-U: *Uitslagvaststelling, Invoeren en samenvoegen stemtotalen & vaststellen uitslag*, elect iT, versie 1.8.2.3, 01-12-2022.
27. *Handleiding Ondersteunende Software Verkiezingen (OSV2020)*, OSV2020-U: *Korte gebruikershandleiding, Handleiding voor gebruik van OSV2020-U, Invoeren en samenvoegen stemtotalen & vaststellen uitslag*, elect iT, versie 1.8.2.3, status: in bewerking, 01-12-2022.
28. *Handleiding Ondersteunende Software Verkiezingen (OSV2020)*, OSV2020-U: *Installatiehandleiding, Handleiding voor installatie van OSV2020-U m.b.v. het installatieprogramma*, elect iT, versie 1.8.2.3, status: in bewerking, 01-12-2022.
29. *Kiesraad; Resultaten Penetratietest OSV2020-U*, PricewaterhouseCoopers Advisory (PWC), status: definitief, referentie: 2022-0669, datum: 02-12-2022, zie: www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/rapporten/2023/1/18/beveiligingsrapport-osv2020-u.
30. *Wijzigingsovereenkomst overeenkomst Beheer/Onderhoud OSV2020 bij de Raamovereenkomst ARBIT 2014 inzake Ondersteunende Software Verkiezingen (OSV)*, Contractnummer: 201850024.154.003_1, niet gedateerd, niet ondertekend.

A.3 Programmatuur

31. *Sources van OSV2020-U*, versie 1.8.0, aangeleverd: 30-09-2022.
32. *Installatieprogramma OSV2020-U*, file: nl-installer-was-1.8.0-OSV2020-U-installer.
33. *Sources van OSV2020-U*, versie 1.8.2.3, aangeleverd: 07-12-2022.
34. *Installatieprogramma OSV2020-U*, file: nl-installer-was-1.8.2.3-OSV2020-U-installer.

Annex B Testen met lijstgroepen en gelijklopende lijsten

In deze annex laten we voorbeelden zien van uitgevoerde testen die laten zien dat er verschillen zijn tussen het door OSV2020-U geleverde verkiezingsresultaat en het verwachte resultaat als we de formele beschrijving [15, pagina 10] letterlijk volgen. Het blijkt dat het resultaat van OSV2020-U in overeenstemming is met de interpretatie die de Kiesraad aan de resultaatberekening geeft.

In enkele testgevallen is de uitvoering van de testcase in OSV2020-U niet mogelijk omdat het situaties betreft die ongewenst zijn en in de praktijk niet blijken voor te komen. In de formele beschrijving wordt (nog) niet expliciet aangegeven welke situaties moeten worden uitgesloten.

B.1 Test met één partij met identieke lijst in twee kieskringen

In deze test testen we de berekening van de zetelverdeling voor één partij die in twee kieskringen met dezelfde kieslijst uitkomt. We gaan bij deze test uit van een verkiezing met twee kiesdistricten waarbij 20 zetels te verdelen zijn. Er is één partij (Blue) die met dezelfde kieslijst in twee kiesdistricten aan de verkiezingen deelneemt.

| kieskring | partijnaam | kandidatenlijst | # Stemmen |
|---------------|------------|--------------------------------|---------------|
| 1 – Noord | Black | black1, black2, black3, black4 | 3.000 |
| | Blue | blue1, blue2, blue3, blue4 | 5.000 |
| 2 – Zuid | Blue | blue1, blue2, blue3, blue4 | 7.000 |
| | Cyan | cyan1, cyan5, cyan6, cyan7 | 2.000 |
| Totaal | | | 17.000 |

Tabel 18: Test met één partij met identieke lijst in twee kieskringen.

Verwacht testresultaat

Volgens de definitie van “stellen gelijklopende lijsten” in de Formele beschrijving [15, pagina 10]:

- In verschillende kieskringen ingediende kandidatenlijsten waarop dezelfde kandidaten in dezelfde volgorde voorkomen en die dus geheel identiek zijn, vormen samen een stel gelijklopende lijsten.

zijn de beide lijsten van Blue een stel gelijklopende lijsten want de kandidatenlijsten in beide kiesdistricten (blue1, blue2, blue3, blue4) zijn volledig identiek.

Tevens vormen beide lijsten van Blue een lijstengroep gezien de definitie in de formele beschrijving:

- In verschillende kieskringen ingediende kandidatenlijsten waarboven dezelfde partij-aanduiding staat of waarvan de eerste kandidaat dezelfde is, vormen samen een lijstengroep.

De partij-aanduiding (Blue) is hetzelfde en de lijsttrekker (de eerste kandidaat) is dezelfde (blue1).

De lijsten van Black in kieskring Noord en van Cyan in kieskring Zuid zijn voorbeelden van op zichzelf staande lijsten:

- Kandidatenlijsten die niet tot een stel gelijklopende lijsten behoren, zijn op zichzelf staande lijsten.

Vervolgens bepalen we het totale aantal uitgebrachte stemmen met stap 2 van onderdeel A.1 [15]:

- 2 De stemtotalen van de stellen gelijkkluidende lijsten, de lijstengroepen en de op zichzelf staande lijsten worden bij elkaar opgeteld.
Het resultaat van deze optelling is het totale aantal uitgebrachte stemmen.

| Categorie | totalen stemmen |
|---|-----------------|
| stel gelijkkluidende lijsten | |
| Blue – Noord, Blue – Zuid | 12.000 |
| Totaal stellen gelijkkluidende lijsten | 12.000 |
| lijstengroep | |
| Blue | 12.000 |
| Totaal lijstengroepen | 12.000 |
| op zichzelf staande lijsten | |
| Black – Noord | 3.000 |
| Cyan – Zuid | 2.000 |
| Totaal op zichzelf staande lijsten | 5.000 |
| Totaal | 29.000 |

Tabel 19: Berekening totaal aantal uitgebrachte stemmen.

Met dit totaal aantal uitgebrachte stemmen wordt de kiesdeler: $29.000 / 10 = 2.900$.

Testresultaat

Na het inlezen van de Verkiezingsdefinitie en Totaalijsten in OSV2020-U laat het programma de interpretatie zien. Vervolgens is de steminvoer in OSV2020-U gedaan volgens de informatie in Tabel 18. Na vaststelling van de uitslag levert het proces-verbaal de volgende informatie over de kandidatenlijsten en kiesdeler.

3. Ingeleverde kandidatenlijsten

De volgende politieke groeperingen hebben deelgenomen aan de verkiezing (in de volgende kieskringen):

| Lijstnr. | Lijstnaam | Ingeleverd | | | Kieskring | |
|----------|-----------|--|---|---------------------------|-----------|---|
| | | Lijstengroep (gelijkkluidende lijsten) | Lijstengroep (niet gelijkkluidende lijsten) | Op zichzelf staande lijst | 1 | 2 |
| 1 | Black | | | * | * | |
| 2 | Blue | * | | | * | * |
| 3 | Cyan | | | * | * | |

4. Aantal stemmen per lijst

| Lijstnr. | Kieskring | | Totaal |
|---------------|-------------|-------------|--------------|
| | 1 | 2 | |
| 1 | 3000 | . | 3000 |
| 2 | 5000 | 7000 | 12000 |
| 3 | . | 2000 | 2000 |
| Totaal | 8000 | 9000 | 17000 |

7. Kiesdeler

$$\begin{array}{l}
 \text{totaal aantal geldige stemmen op} \\
 \text{kandidaten}
 \end{array}
 :
 \begin{array}{l}
 \text{aantal zetels} \\
 10
 \end{array}
 =
 \begin{array}{l}
 \text{kiesdeler} \\
 1700
 \end{array}$$

Testconclusie

De kiesdeler die het programma (1.700) berekent komt niet overeen met de kiesdeler die in de formele beschrijving is vereist (2.900). Dit heeft gevolgen voor de bepaling van het verkiezingsresultaat en de zetelverdeling. De door het programma geleverde resultaten komen niet overeen met de geëiste specificatie als we de formele specificatie letterlijk nemen.

Het is duidelijk dat de stemmen voor Blue niet twee keer moeten worden meegeteld bij de bepaling van het totaal aantal stemmen. De kiesdeler die OSV2020-U berekent levert de juiste interpretatie.

B.2 Test met twee stellen identieke lijsten in twee kieskringen

Als een partij een kandidatenlijst in twee verschillende kiesdistricten indient en een aangepaste versie daarvan met dezelfde partijaanduiding in twee andere kieskringen hebben we te maken met twee stellen van identieke lijsten die alle vier samen tot een lijstengroep behoren. Voor deze test gaan we uit van een verkiezing met 10 beschikbare zetels.

| kieskring | partijnaam | kandidatenlijst | # Stemmen |
|-----------|------------|---|-----------|
| 1 – Noord | Black | black1, black2, black3, black4 | 2.500 |
| | Yellow | yellow1, yellow2, yellow3, yellow4 | 1.700 |
| 2 – Oost | Yellow | yellow1, yellow2, yellow3, yellow4 | 1.900 |
| | Cyan | cyan1, cyan5, cyan6, cyan7 | 5.000 |
| 3 – Zuid | Yellow | yellow1, yellow2, yellow3, yellow4, yellow5 | 2.300 |
| | Red | red1, red3, red2, red4, red5 | 3.500 |

| kieskring | partijnaam | kandidatenlijst | # Stemmen |
|---------------|------------|---|---------------|
| 4 – West | Yellow | yellow1, yellow2, yellow3, yellow4, yellow5 | 3.100 |
| Totaal | | | 20.000 |

Tabel 20: Test met één partij met twee stellen identieke lijsten in twee kieskringen.

Verwacht testresultaat

| categorie | totalen stemmen |
|---|-----------------|
| stel gelijklopende lijsten | |
| Yellow – Noord, Yellow – Oost | 3.600 |
| Yellow – Zuid, Yellow – West | 5.400 |
| Totaal stellen gelijklopende lijsten | 9.000 |
| lijstengroep | |
| Yellow | 9.000 |
| Totaal lijstengroepen | 9.000 |
| op zichzelf staande lijsten | |
| Black – Noord | 2.500 |
| Cyan – Oost | 5.000 |
| Red – Zuid | 3.500 |
| Totaal op zichzelf staande lijsten | 11.000 |
| Totaal | 29.000 |

Tabel 21: Berekening totaal aantal uitgebrachte stemmen.

Met dit totaal aantal uitgebrachte stemmen wordt de kiesdeler: $29.000 / 10 = 2.900$.

Testresultaat

3. Ingeleverde kandidatenlijsten

De volgende politieke groeperingen hebben deelgenomen aan de verkiezing (in de volgende kieskringen):

| Lijstnr. | Lijstnaam | Ingeleverd | | | Kieskring | | | |
|----------|-----------|--------------------------------------|---|---------------------------|-----------|---|---|---|
| | | Lijstengroep (gelijklopende lijsten) | Lijstengroep (niet gelijklopende lijsten) | Op zichzelf staande lijst | 1 | 2 | 3 | 4 |
| 1 | Black | | * | * | | | | |
| 2 | Yellow | * | | | * | * | * | * |

| | | | |
|---|------|---|---|
| 3 | Cyan | * | * |
| 4 | Red | * | * |

Merk op dat Yellow wordt gerepresenteerd als een lijstengroep (niet gelijklopende lijsten) terwijl deze lijst weldegelijk gelijklopende lijsten bevat. In de vorige testcase (Annex B.1) werd Blue weergegeven als lijstengroep (gelijklopende lijsten). Het onderscheid is dat Blue volledig bestaat uit één stel gelijklopende lijsten en Yellow uit meerdere stellen gelijklopende lijsten.

7. Kiesdeler

$$\begin{array}{l} \text{totaal aantal geldige stemmen op} \\ \text{kandidaten} \end{array} : \begin{array}{l} \text{aantal zetels} \\ 10 \end{array} = \begin{array}{l} \text{kiesdeler} \\ 2000 \end{array}$$

Net als bij de vorige test is er een verschil tussen de kiesdeler die het programma oplevert en de verwachte kiesdeler op basis van dubbeltelling van de stellen gelijklopende lijsten of lijstengroepen.

B.3 Test met één partij met identieke kandidatenlijst met verschillende partijnaam

Als een partij dezelfde kandidatenlijst in twee kiesdistricten heeft met een verschillende partijnaam, dan betreft dit volgens de formele beschrijving [15, pagina 10] een stel gelijklopende lijsten.

| kieskring | partijnaam | kandidatenlijst | # Stemmen |
|---------------|------------|--------------------------------|---------------|
| 1 – Noord | Black | black1, black2, black3, black4 | 3.000 |
| | Blue1 | blue1, blue2, blue3, blue4 | 5.000 |
| 2 – Zuid | Blue2 | blue1, blue2, blue3, blue4 | 7.000 |
| | Cyan | cyan1, cyan5, cyan6, cyan7 | 2.000 |
| Totaal | | | 17.000 |

Tabel 22: Test met één partij identieke kandidatenlijst met verschillende partijnaam.

Testresultaat

Als we deze situatie in OSV2020-U testen, ziet het programma Blue1 en Blue2 als onafhankelijke lijsten.

3. Ingeleverde kandidatenlijsten

De volgende politieke groeperingen hebben deelgenomen aan de verkiezing (in de volgende kieskringen):

| Lijstnr. | Lijstnaam | Ingeleverd | | | Kieskring | |
|----------|-----------|---------------------------------------|--|---------------------------|-----------|---|
| | | Lijstengroep (gelijkluidende lijsten) | Lijstengroep (niet gelijkluidende lijsten) | Op zichzelf staande lijst | 1 | 2 |
| 1 | Black | | | * | * | |
| 2 | Blue1 | | | * | * | |
| 2 | Blue2 | | | * | * | |
| 3 | Cyan | | | * | * | |

Testoordeel

Volgens de formele beschrijving is het voor een stel gelijkluidende lijsten voldoende dat de kandidatenlijsten volledig identiek zijn en wordt er geen uitspraak gedaan over de partijnaam bij de kandidatenlijst in de verschillende kiesdistricten. We achten het een correcte interpretatie van OSV2020-U dat identieke kandidatenlijsten met verschillende partijnamen in verschillende kiesdistricten niet als stel gelijkluidende lijsten worden herkend.

B.4 Test met varianten van lijstgroepen en stellen gelijkluidende lijsten

In deze testcase zijn allerlei combinaties van lijstgroepen en stellen gelijkluidende lijsten getoetst. Tabel 23 en Tabel 24 geven aan welke partijen met welke kandidaten in de diverse kieskringen zijn getest.

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|-----------|------------|------------------------------------|----------|
| 1 – Noord | Black | black1, black2, black3, black4 | 200 |
| | Blue | blue1, blue2, blue3, blue4 | 300 |
| | Green | green1, green2, green3, green4 | 700 |
| | Yellow | yellow1, yellow2, yellow3, yellow4 | 1.700 |
| | Cyan | cyan1, cyan2, cyan3, cyan4 | 3.100 |
| | Mauve | mauve5, mauve6, mauve7, mauve8 | 4.300 |

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|-----------|------------|------------------------------------|----------|
| | Orange | orange1, orange2, orange3, orange4 | 5.900 |
| | Red | red1, red2, red3, red4 | 6.700 |
| | **blanco** | purple1, purple2, purple3, purple4 | 7.900 |
| | **blanco** | white1, white2, white3, white4 | 8.900 |
| 2 – Oost | Blue | blue1, blue2, blue3, blue4 | 500 |
| | Green | green1, green2, green3, green4 | 1.100 |

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|-----------|------------|------------------------------------|----------|
| | Yellow | yellow1, yellow2, yellow3, yellow4 | 1.900 |
| | Cyan | cyan1, cyan5, cyan6, cyan7 | 3.700 |
| | Mauve | mauve5, mauve6, mauve7, mauve8 | 4.700 |
| | Orange | orange2, orange3, orange5, orange6 | 6.100 |
| | Red | red1, red2, red3, red4, red5 | 7.100 |
| | **blanco** | purple1, purple2, purple5, purple6 | 8.300 |
| | **blanco** | white1, white2, white3, white4 | 9.700 |
| 3 – Zuid | Green | green1, green2, green3, green4 | 1.300 |

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|---------------|------------|---|----------------|
| | Yellow | yellow1, yellow2, yellow3, yellow4, yellow5 | 2.300 |
| | Cyan | cyan1, cyan5, cyan6, cyan7 | 4.100 |
| | **blanco** | mauve5, mauve6, mauve7, mauve8 | 5.300 |
| | Red | red1, red3, red2, red4, red5 | 7.300 |
| | **blanco** | white1, white3, white2, white4 | 10.100 |
| 4 – West | Yellow | yellow1, yellow2, yellow3, yellow4, yellow5 | 2.900 |
| Totaal | | | 116.100 |

Tabel 23: Test met varianten van lijstgroepen en stellen gelijklopende lijsten (gesorteerd naar kieskring).

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|-----------|------------|---|----------|
| 1 – Noord | Black | black1, black2, black3, black4 | 200 |
| 1 – Noord | Blue | blue1, blue2, blue3, blue4 | 300 |
| 2 – Oost | | blue1, blue2, blue3, blue4 | 500 |
| 1 – Noord | Green | green1, green2, green3, green4 | 700 |
| 2 – Oost | | green1, green2, green3, green4 | 1.100 |
| 3 – Zuid | | green1, green2, green3, green4 | 1.300 |
| 1 – Noord | Yellow | yellow1, yellow2, yellow3, yellow4 | 1.700 |
| 2 – Oost | | yellow1, yellow2, yellow3, yellow4 | 1.900 |
| 3 – Zuid | | yellow1, yellow2, yellow3, yellow4, yellow5 | 2.300 |
| 4 – West | | yellow1, yellow2, yellow3, yellow4, yellow5 | 2.900 |
| 1 – Noord | Cyan | cyan1, cyan2, cyan3, cyan4 | 3.100 |

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|-----------|------------|------------------------------------|----------|
| 2 – Oost | | cyan1, cyan5, cyan6, cyan7 | 3.700 |
| 3 – Zuid | | cyan1, cyan5, cyan6, cyan7 | 4.100 |
| 1 – Noord | Mauve | mauve5, mauve6, mauve7, mauve8 | 4.300 |
| 2 – Oost | | mauve5, mauve6, mauve7, mauve8 | 4.700 |
| 3 – Zuid | **blanco** | mauve5, mauve6, mauve7, mauve8 | 5.300 |
| 1 – Noord | Orange | orange1, orange2, orange3, orange4 | 5.900 |
| 2 – Oost | | orange2, orange3, orange5, orange6 | 6.100 |
| 1 – Noord | Red | red1, red2, red3, red4 | 6.700 |
| 2 – Oost | | red1, red2, red3, red4, red5 | 7.100 |
| 3 – Zuid | | red1, red3, red2, red4, red5 | 7.300 |
| 1 – Noord | **blanco** | purple1, purple2, purple3, purple4 | 7.900 |
| 2 – Oost | | purple1, purple2, purple5, purple6 | 8.300 |

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|-----------|------------|-----------------------------------|----------|
| 1 – Noord | **blanco** | white1, white2, white3, white4 | 8.900 |
| 2 – Oost | | white1, white2, white3, white4 | 9.700 |

| kieskring | partijnaam | kandidatenlijst | #Stemmen |
|---------------|------------|-----------------------------------|----------------|
| 3 – Zuid | | white1, white3, white2, white4 | 10.100 |
| Totaal | | | 116.100 |

Tabel 24: Test met varianten van lijstgroepen en stellen gelijklopende lijsten (gesorteerd naar partij).

Testresultaat

De verkiezingsleider krijgt in OSV2020-U een overzicht te zien van de manier waarop het programma de kieslijsten typeert. Onderstaande tabel bevat de informatie daarover uit dat overzicht.

| Lijstpositie | Partijnaam | Type kandidatenlijst | Kieskring |
|--------------|----------------------|------------------------------------|---|
| 1 | Black | Onafhankelijke lijst | <input checked="" type="checkbox"/> 1 – Noord |
| 2 | Blue | Identieke lijst (2 kieskringen) | <input checked="" type="checkbox"/> 1 – Noord, <input checked="" type="checkbox"/> 2 – Oost |
| 3 | Green | Identieke lijst (3 kieskringen) | <input checked="" type="checkbox"/> 1 – Noord, <input checked="" type="checkbox"/> 2 – Oost, <input checked="" type="checkbox"/> 3 – Zuid |
| 4 | Yellow | Lijstengroep (4 kieskringen) | Stel 1: <input checked="" type="checkbox"/> 1 – Noord, <input checked="" type="checkbox"/> 2 – Oost Stel 2: <input checked="" type="checkbox"/> 3 – Zuid, <input checked="" type="checkbox"/> 4 – West |
| 5 | Cyan | Lijstengroep (3 kieskringen) | Individuele lijst: <input checked="" type="checkbox"/> 1 – Noord Stel 1: <input checked="" type="checkbox"/> 2 – Oost, <input checked="" type="checkbox"/> 3 – Zuid |
| 6 | Mauve | Identieke lijst (3 kieskringen) | <input checked="" type="checkbox"/> 1 – Noord, <input checked="" type="checkbox"/> 2 – Oost, <input checked="" type="checkbox"/> 3 – Zuid |
| 7 | Orange | Lijstengroep (2 kieskringen) | Individuele lijst: <input checked="" type="checkbox"/> 1 – Noord Individuele lijst: <input checked="" type="checkbox"/> 2 – Oost |
| 8 | Red | Lijstengroep (3 kieskringen) | Individuele lijst: <input checked="" type="checkbox"/> 1 – Noord Individuele lijst: <input checked="" type="checkbox"/> 2 – Oost Individuele lijst: <input checked="" type="checkbox"/> 3 – Zuid |
| 9 | Blanco (Purple1, A.) | Lijstengroep (2 kieskringen) | Individuele lijst: <input checked="" type="checkbox"/> 1 – Noord Individuele lijst: <input checked="" type="checkbox"/> 2 – Oost |
| 10 | Blanco (White1, H.) | Lijstengroep (3 kieskringen) | Stel 1: <input checked="" type="checkbox"/> 1 – Noord, <input checked="" type="checkbox"/> 2 – Oost Individuele lijst: <input checked="" type="checkbox"/> 3 – Zuid |

Tabel 25: Informatie uit OSV2020-U voor test met varianten van lijstgroepen en stellen gelijklopende lijsten.

Opmerkelijk is dat uit bovenstaande tabel blijkt dat de blanco-lijst bij Mauve uit kieskring Zuid is toegevoegd aan het tweetal gelijklopende lijsten dat expliciet de partijnaam Mauve voert. Daarmee wordt terecht een drietal van gelijklopende lijsten onderkend.

In het proces-verbaal van de uitslag van de verkiezing van de provinciale staten herkent OSV2020-U de volgende indeling van lijstgroepen en stellen gelijklopende lijsten.

3. Ingeleverde kandidatenlijsten

De volgende politieke groeperingen hebben deelgenomen aan de verkiezing (in de volgende kieskringen):

| Lijstnr. | Lijstnaam | Ingeleverd | | | Kieskring | | | |
|----------|----------------------|---------------------------------------|--|---------------------------|-----------|---|---|---|
| | | Lijstengroep (gelijkluidende lijsten) | Lijstengroep (niet gelijkluidende lijsten) | Op zichzelf staande lijst | 1 | 2 | 3 | 4 |
| 1 | Black | | | * | * | | | |
| 2 | Blue | * | | | * | * | | |
| 3 | Green | * | | | * | * | * | |
| 4 | Yellow | | * | | * | * | * | * |
| 5 | Cyan | | * | | * | * | * | |
| 6 | Mauve | | * | | * | * | * | |
| 7 | Orange | | * | | * | * | | |
| 8 | Red | | * | | * | * | * | |
| 9 | Blanco (Purple1, A.) | | * | | * | * | | |
| 10 | Blanco (White1, H.) | | * | | * | * | * | |

4. Aantal stemmen per lijst

| Lijstnr. | Kieskring | Kieskring | | | | Totaal |
|--------------------------|-----------|-----------|-------|-------|------|--------|
| | | 1 | 2 | 3 | 4 | |
| 1 | | 200 | . | . | . | 200 |
| 2 | | 300 | 500 | . | . | 800 |
| 3 | | 700 | 1100 | 1300 | . | 3100 |
| 4 | | 1700 | 1900 | 2300 | 2900 | 8800 |
| 5 | | 3100 | 3700 | 4100 | . | 10900 |
| 6 | | 4300 | 4700 | 5300 | . | 14300 |
| 7 | | 5900 | 6100 | . | . | 12000 |
| 8 | | 6700 | 7100 | 7300 | . | 21100 |
| 9 | | 7900 | 8300 | . | . | 16200 |
| 10 | | 8900 | 9700 | 10100 | . | 28700 |
| Totaal | | 39700 | 43100 | 30400 | 2900 | 116100 |
| <i>Blanco stemmen</i> | | 0 | 0 | 0 | 0 | 0 |
| <i>Ongeldige stemmen</i> | | 0 | 0 | 0 | 0 | 0 |

7. Kiesdeler

totaal aantal geldige stemmen op kandidaten : *aantal zetels* = *kiesdeler*
 116100 : 20 = 5805

8. Verdeling van de volle zetels

| Lijstnummer | Aantal stemmen : | Kiesdeler | = | Aantal volle zetels |
|-------------|------------------|-----------|---|---------------------|
| 1 | 200 : | 5805 | = | 0 |
| 2 | 800 : | 5805 | = | 0 |
| 3 | 3100 : | 5805 | = | 0 |
| 4 | 8800 : | 5805 | = | 1 |
| 5 | 10900 : | 5805 | = | 1 |
| 6 | 14300 : | 5805 | = | 2 |
| 7 | 12000 : | 5805 | = | 2 |
| 8 | 21100 : | 5805 | = | 3 |
| 9 | 16200 : | 5805 | = | 2 |
| 10 | 28700 : | 5805 | = | 4 |

| | | |
|--------------------------------------|----------|------------|
| Totaalaantal zetels | A | 20 |
| Totaalaantal toegewezen volle zetels | B | 15 |
| | | Verschil- |
| <i>Restzetels (A - B = C)</i> | | C 5 |

9. Verdeling van de restzetels

| Lijstnummer | Restzetel | | | | | Aantal restzetels |
|-------------|-------------|-------------|-------------|-------------|-----------------|-------------------|
| | 1 | 2 | 3 | 4 | 5 | |
| 1 | 200 | 200 | 200 | 200 | 200 | 200 |
| 2 | 800 | 800 | 800 | 800 | 800 | 800 |
| 3 | 3100 | 3100 | 3100 | 3100 | 3100 | 3100 |
| 4 | 4400 | 4400 | 4400 | 4400 | 4400 | 4400 1 |
| 5 | 5450 | 5450 | 3633 1/3 | 3633 1/3 | 3633 1/3 | 3633 1/3 1 |
| 6 | 4766 2/3 | 4766 2/3 | 4766 2/3 | 4766 2/3 | 4766 2/3 | 4766 2/3 1 |
| 7 | 4000 | 4000 | 4000 | 4000 | 4000 | 4000 |
| 8 | 5275 | 5275 | 5275 | 5275 | 4220 | 4220 1 |
| 9 | 5400 | 5400 | 5400 | 4050 | 4050 | 4050 1 |
| 10 | 5740 | 4783 2/6 | 4783 2/6 | 4783 2/6 | 4783 2/6 | 2 |

| | | | | | | |
|-------------------------------|----|---|---|---|----|---|
| restzetel toegekend aan lijst | 10 | 5 | 9 | 8 | 10 | 6 |
|-------------------------------|----|---|---|---|----|---|

Overeenkomstig artikel P 10 of artikel P 13, eerste lid, van de Kieswet (lijstuitputting) vindt er een overgang plaats van 2 zetels van lijst 10 naar andere lijsten.

10. Verdeling van de volle zetels

| <i>Lijstnaam</i> | <i>Lijstnummer</i> | <i>Aantal zetels</i> |
|----------------------|--------------------|----------------------|
| Blanco (White1, H.) | 10 | 4 |
| Red | 8 | 4 |
| Blanco (Purple1, A.) | 9 | 3 |
| Mauve | 6 | 3 |
| Orange | 7 | 2 |
| Cyan | 5 | 2 |
| Yellow | 4 | 2 |
| Green | 3 | 0 |
| Blue | 2 | 0 |
| Black | 1 | 0 |

Testoordeel

Uit de resterende informatie van het proces-verbaal blijkt dat OSV2020-U met de onderkende indeling in lijstgroepen en stellen gelijklopende lijsten correct de verdere stappen van de berekening uitvoert.

Annex C Inzet van CAST tools

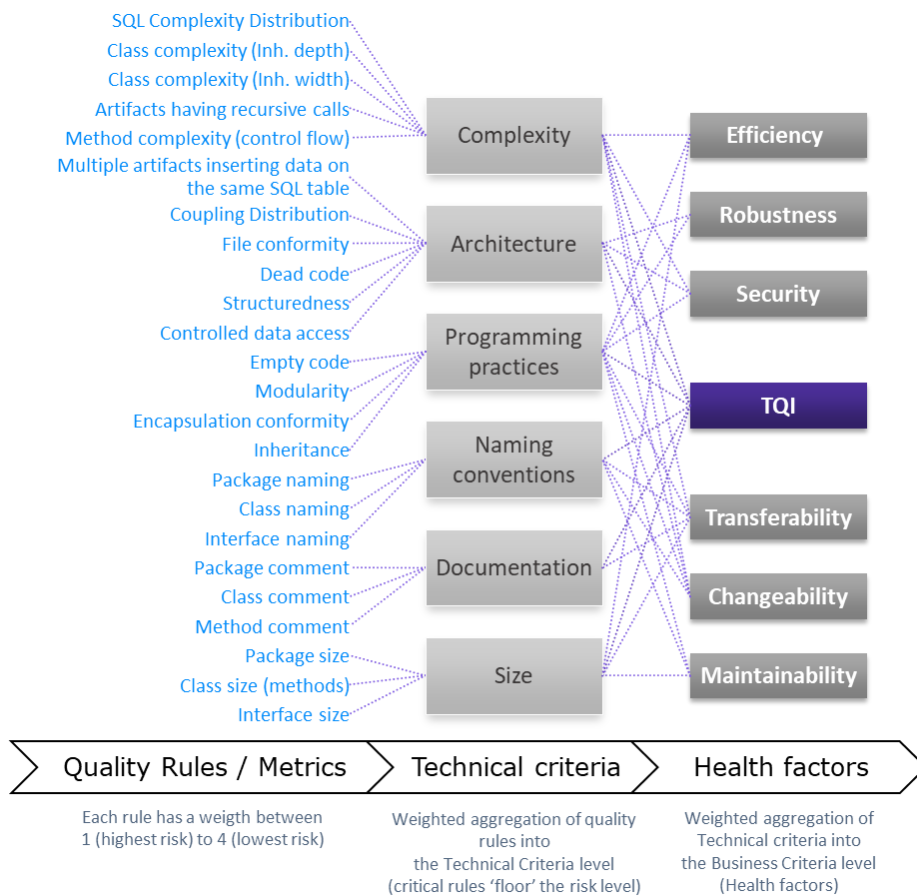
C.1 CAST AIP

CAST AIP voert een groot aantal metingen uit voor de aangeleverde sources (zie Figuur 9). Bij het merendeel van de metingen wordt het aantal gebreken bepaald en wordt het meetresultaat uitgedrukt als 'Compliance ratio':

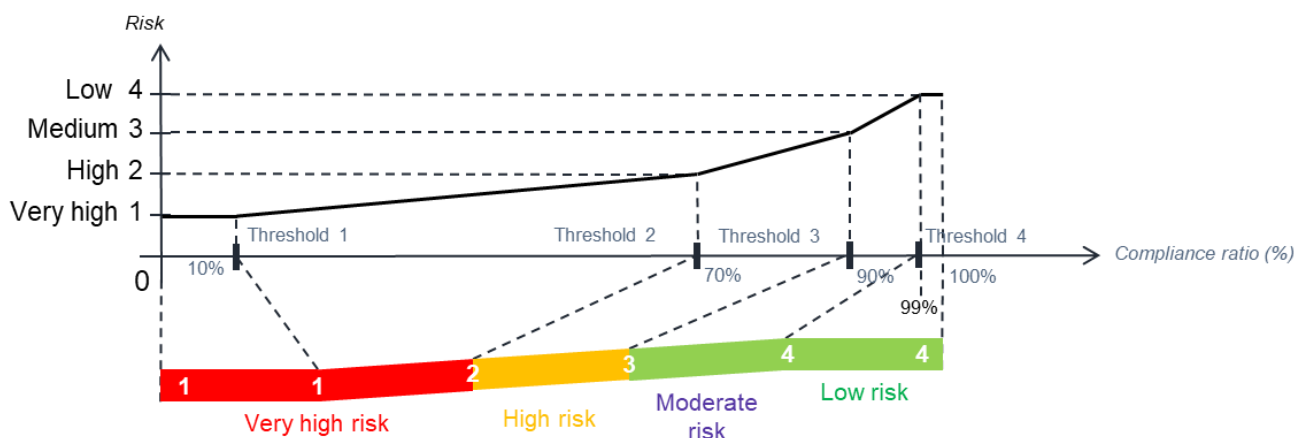
$$\text{Compliance ratio (\%)} = \frac{\# \text{ successful checks}}{\# \text{ successful checks} + \# \text{ failed checks}} \times 100$$

Elk meetresultaat wordt vervolgens uitgezet op een risicoschaal van 1 (hoog risico) tot 4 (laag risico), met drempelwaardes die zijn aangepast aan de ernst van de regel (zie Figuur 10 en Figuur 11).

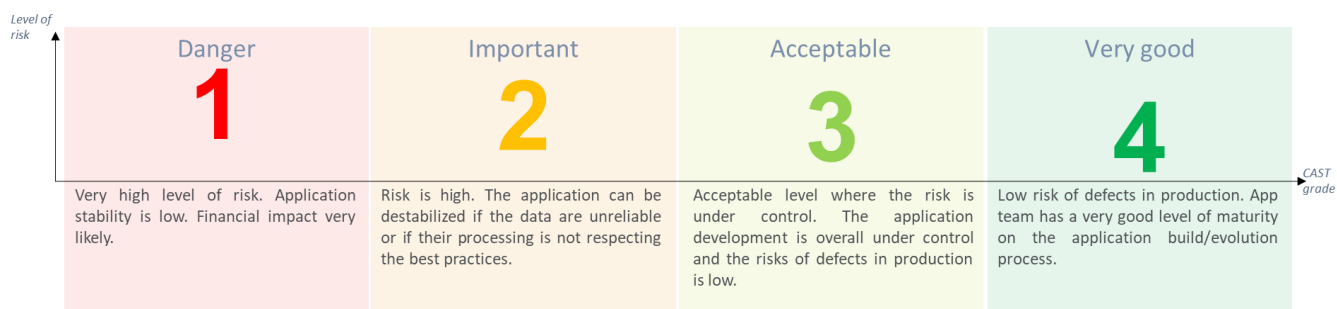
De meetresultaten worden geaggregeerd naar technische criteria op basis van gewogen middeling en deze worden weer samengevoegd tot een zestal kwaliteitskarakteristieken. Bij deze aggregaties zijn wegingsfactoren bepaald door experts van CAST op basis van praktijkervaring met architectuur en software best practices.



Figuur 9: Kwaliteitsmodel van CAST AIP.



Figuur 10: CAST AIP; omzetting van meetresultaten naar risico's.



Figuur 11: CAST AIP; beschrijving van risicocategorieën.

C.2 Omvang OSV2020-U

De aangeleverde sources van OSV2020-U bestaan grotendeels uit Java-code met daarnaast Html-code voor beschrijving van het gebruikersinterface en een sql-bestand voor beschrijving van de databasestructuur. Tabel 26 geeft een indruk van de omvang van de applicatie uitgedrukt in aantal coderegels (# LoC), aantal regels tekst met commentaar en aantal commentaarregels die uitgedcommentarieerde code bevatten.

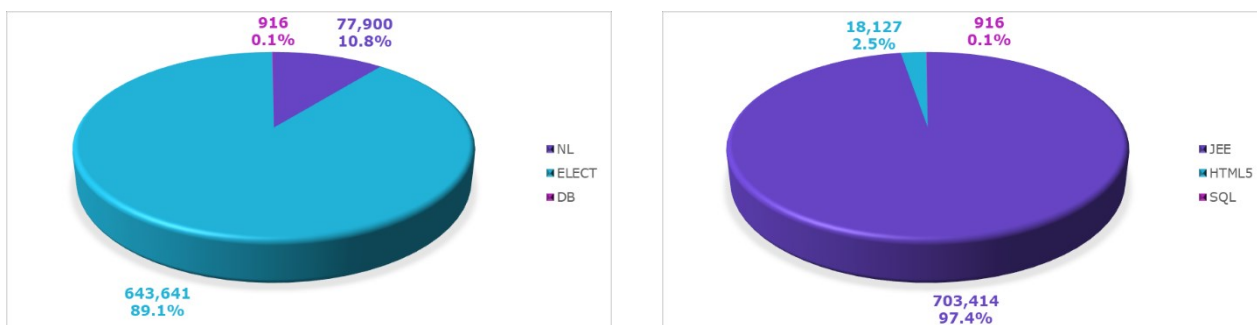
| Name | Size |
|----------------------------|---------|
| # Comment Lines | 111.537 |
| # Commented-out Code Lines | 1.475 |
| # LoC | 722.457 |

Tabel 26: Omvang van OSV2020-U.

De sources zijn verdeeld in drie modules op basis van de naamgeving van de folders. De 15 folders beginnend met 'nl' zijn ondergebracht in de module 'NL'; de overige 29 die beginnen met 'elect' in de module 'ELECT'. De beschrijving van de database is opgenomen in 'DB'. Tabel 27 geeft een beeld van de omvang van de diverse modules. Een visuele weergave is opgenomen in Figuur 12.

| Module Name | HTML5 | JEE | SQL | Totaal #LoC |
|---------------|---------------|----------------|------------|----------------|
| NL | 901 | 76.999 | | 77.900 |
| ELECT | 17.226 | 626.415 | | 643.641 |
| DB | | | 916 | 916 |
| Totaal | 18.127 | 703.414 | 916 | 722.457 |

Tabel 27: Omvang van OSV2020-U ingedeeld in modules uitgedrukt in aantallen coderegels (LoC = Lines of Code).



Figuur 12: Omvang van OSV2020-U ingedeeld naar modules (links) en toegepaste technologie (Rechts).

Tabel 28 geeft een overzicht van de door CAST AIP gedetecteerde artefacten waarvoor metingen worden uitgevoerd.

| Name | NL | ELECT | DB | #Artifacts |
|--|--------|--------|-----|------------|
| Number of Artifacts | 12.986 | 98.275 | | 111.261 |
| Number of Files | 1.383 | 10.431 | 1 | 11.815 |
| Number of Classes | 1.597 | 11.536 | | 13.133 |
| Number of WEB Pages | 112 | 1.321 | | 1.433 |
| Number of Interfaces | 107 | 863 | | 970 |
| Number of Methods | 12.826 | 96.241 | | 109.067 |
| Number of Functions | | 13 | | 13 |
| Number of Tables | | | 182 | 182 |
| Number of Template Classes | 20 | 487 | | 507 |
| Number of Template Class Instances | 38 | 2.907 | | 2.945 |
| Number of Template Interfaces | 1 | 67 | | 68 |
| Number of Template Interface Instances | 1 | 554 | | 555 |
| Number of Template Methods | 32 | 1.702 | | 1.734 |
| Number of Template Method Instances | 68 | 1.838 | | 1.906 |

Tabel 28: Aantal artefacten van OSV2020-U.

C.3 Scores voor Wijzigbaarheid

De score die CAST AIP aangeeft voor de wijzigbaarheid (changeability) van OSV2020-U is 3,37. Dit betreft een goede score die ruimte voor verdere verbetering laat zien. De score is gebaseerd op de naar onderwerp samengevoegde scores zoals die zijn weergegeven in Tabel 29. Tabel 30 bevat alle voor wijzigbaarheid relevante meetresultaten.

| Technical Criterium | NL | ELECT | DB | Total |
|---|------|-------|------|-------|
| Documentation – Volume of Comments | 1,15 | 1,00 | | 1,00 |
| Dead code (static) | 3,00 | 2,28 | 4,00 | 2,61 |
| Architecture – Object-level Dependencies | 3,21 | 2,56 | | 2,63 |
| Architecture – Reuse | 3,06 | 2,99 | | 2,98 |
| Documentation – Naming Convention Conformity | 3,35 | 3,60 | 2,50 | 3,21 |
| Programming Practices – Modularity and OO Encapsulation Conformity | 3,27 | 3,30 | | 3,30 |
| Architecture – OS and Platform Independence | 4,00 | 3,40 | | 3,40 |
| Complexity – OO Inheritance and Polymorphism | 3,69 | 3,68 | | 3,68 |
| Programming Practices – Structuredness | 4,00 | 3,97 | 3,29 | 3,81 |
| Architecture – Multi-Layers and Data Access | 4,00 | 3,86 | 3,89 | 3,87 |
| Complexity – Algorithmic and Control Structure Complexity | 3,95 | 3,93 | | 3,93 |
| Complexity – Dynamic Instantiation | 4,00 | 4,00 | | 4,00 |
| Complexity – SQL Queries | 3,70 | 4,00 | | 4,00 |

Tabel 29: Technische criteria met risicoscore voor wijzigbaarheid van OSV2020-U.

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Avoid defining singleton or factory when using Spring | 1,00 | 1,00 | | 1,00 |
| Avoid undocumented Methods | 1,00 | 1,00 | | 1,00 |
| Avoid Functions having a very low Comment/Code ratio (Javascript) | | 1,00 | | 1,00 |
| Avoid undocumented Functions (Javascript) | | 1,00 | | 1,00 |
| Avoid Methods with a very low comment/code ratio | 1,01 | 1,00 | | 1,00 |
| Avoid Classes with a very low comment/code ratio | 1,25 | 1,00 | | 1,00 |
| Avoid long Table or View names | | | 1,00 | 1,00 |
| Avoid undocumented Interfaces | 1,00 | 1,00 | | 1,00 |
| Avoid Classes with a High Lack of Cohesion | 1,01 | 1,00 | | 1,00 |

| Measurement | NL | ELECT | DB | Total |
|---|------|-------|------|-------|
| Avoid undocumented Classes | 1,48 | 1,00 | | 1,00 |
| Constant naming convention – case control (JEE) | 1,00 | 1,90 | | 1,00 |
| Use ANSI standard operators in SQL WHERE clauses | | 1,00 | | 1,00 |
| Avoid Classes with a High Lack of Cohesion – variant | 1,20 | 1,05 | | 1,07 |
| Avoid Classes with High Coupling Between Objects | 1,39 | 1,05 | | 1,09 |
| Avoid unreferenced JSPs and web client files | 1,67 | 1,47 | | 1,49 |
| Avoid Too Many Copy Pasted Artifacts | 2,80 | 1,70 | | 1,73 |
| Avoid unreferenced Functions (Javascript/HTML5) | | 1,87 | | 1,87 |
| Avoid many-to-many association | | 1,95 | | 1,95 |
| Avoid Artifacts with High Fan-Out | 2,39 | 2,07 | | 2,11 |
| Avoid unreferenced Data Members | 3,79 | 2,12 | | 2,28 |
| Avoid unreferenced Methods | 2,53 | 2,27 | | 2,30 |
| Class Fan-In Distribution | 3,69 | 2,14 | | 2,32 |
| Avoid Artifacts with High Fan-In | 3,25 | 2,39 | | 2,49 |
| Class Fan-Out Distribution | 3,28 | 2,38 | | 2,49 |
| Copy Pasted Code (% of LOC) | 3,65 | 2,50 | | 2,50 |
| Reuse by Call Distribution | 1,80 | 2,77 | | 2,66 |
| Avoid Packages with High Efferent Coupling (CE) | 2,98 | 2,68 | | 2,72 |
| Avoid Packages with High Afferent Coupling (CA) | 4,00 | 2,93 | | 3,05 |
| Avoid large Interfaces – too many Methods (JEE) | 4,00 | 3,03 | | 3,14 |
| Avoid Tables not using referential integrity | | | 3,29 | 3,29 |
| Avoid Classes with a High Depth of Inheritance Tree | 2,27 | 3,56 | | 3,38 |
| OO Complexity Distribution | 3,83 | 3,34 | | 3,40 |
| Class Complexity Distribution (WMC) | 3,69 | 3,36 | | 3,40 |
| Coupling Distribution | 3,92 | 3,38 | | 3,44 |
| Avoid declaring Instance Variables without defined access type | 4,00 | 3,36 | | 3,45 |
| Avoid using Fields (non static final) from other Classes | 3,42 | 3,49 | | 3,48 |
| Avoid having multiple artifacts deleting data on the same SQL table | | | 3,56 | 3,56 |
| Avoid Classes with a High Number Of Children | 3,73 | 3,63 | | 3,64 |
| Avoid Tables aliases ending with a numeric suffix | | 3,69 | | 3,69 |
| Avoid unreferenced Interfaces | 4,00 | 3,67 | | 3,73 |
| Add @Override on methods overriding or implementing a method declared in a super type | 4,00 | 3,94 | | 3,96 |
| Avoid Classes with High Weighted Methods per Class | 4,00 | 3,94 | | 3,96 |
| Avoid using break statement in FOR loops | 4,00 | 3,96 | | 3,97 |

| Measurement | NL | ELECT | DB | Total |
|---|------|-------|------|-------|
| Cyclomatic Complexity Distribution | 3,99 | 3,99 | | 3,99 |
| Avoid having multiple artifacts updating data on the same SQL Table | | | 4,00 | 4,00 |
| Avoid Classes with a High Public Data Ratio | 4,00 | 4,00 | | 4,00 |
| Avoid static Fields that are not final | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with High Integration Complexity | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with High Essential Complexity | 4,00 | 4,00 | | 4,00 |
| Avoid using Dynamic instantiation | 4,00 | 4,00 | | 4,00 |
| Avoid using anonymous Classes | 3,94 | 4,00 | | 4,00 |
| Avoid large Classes – too many Constructors (JEE) | 4,00 | 3,99 | | 4,00 |
| Avoid Classes implementing too many Interfaces (JEE) | 4,00 | 4,00 | | 4,00 |
| Field naming convention – case control | 3,77 | 4,00 | | 4,00 |
| Class naming convention – case control (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,io,File' | 4,00 | 4,00 | | 4,00 |
| Avoid using 'sun,*' Classes | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,lang,System,getenv()' | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with too many parameters | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with High Depth of Code | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with High Cyclomatic Complexity | 4,00 | 4,00 | | 4,00 |
| Avoid unreferenced Tables | | | 4,00 | 4,00 |
| Avoid using Web SQL databases | | 4,00 | | 4,00 |
| Avoid classes overriding only equals() or only hashCode() | 4,00 | 4,00 | | 4,00 |
| Avoid calls between JSP Pages | 4,00 | 4,00 | | 4,00 |
| Avoid database tables associated to more than one Entity | | 4,00 | | 4,00 |
| Avoid direct access to Database Tables | 4,00 | 4,00 | | 4,00 |
| Avoid direct access to Database Tables in Javascript | | 4,00 | | 4,00 |
| Avoid direct use of Database objects (JSP/ASP) | 4,00 | 4,00 | | 4,00 |
| Avoid having multiple artifacts inserting data on the same SQL Table | | | 4,00 | 4,00 |
| Avoid Tables without Primary Key (SQL) | | | 4,00 | 4,00 |
| Avoid usage of BannedAPI when using ESAPI library | 4,00 | 4,00 | | 4,00 |
| Collection must be the same between getter and setter | | 4,00 | | 4,00 |
| Avoid domain model depending on other Java API | | 4,00 | | 4,00 |
| Do not use auto-wiring | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with a Complex SELECT Clause | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with High RAW SQL Complexity | 4,00 | 4,00 | | 4,00 |
| Interface naming convention – case control | 4,00 | 4,00 | | 4,00 |

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Method naming convention – case control (JEE) | 4,00 | 4,00 | | 4,00 |
| Table naming convention – character set control (SQL) | | | 4,00 | 4,00 |
| Avoid table and column names that are too long (portability) | | 4,00 | | 4,00 |
| Avoid artifacts having recursive calls | 4,00 | 4,00 | | 4,00 |
| Avoid Artifacts with High Cyclomatic Complexity (HTML5/Javascript) | | 4,00 | | 4,00 |
| Avoid Artifacts with High Depth of Code (Javascript) | | 4,00 | | 4,00 |
| Avoid Artifacts with too many parameters (Javascript) | | 4,00 | | 4,00 |
| SQL Complexity Distribution | 3,09 | 4,00 | | 4,00 |

Tabel 30: Metingen met risicoscore voor wijzigbaarheid van OSV2020-U.

C.4 Scores voor Beveiliging

De score die CAST AIP aangeeft voor de beveiliging (security) van OSV2020-U is 2,73. Dit betreft een redelijke score die ruimte voor verdere verbetering laat zien. De score is gebaseerd op de naar onderwerp samengevoegde scores zoals die zijn weergegeven in Tabel 31. Tabel 32 bevat alle voor beveiliging relevante meetresultaten.



| Technical Criterium | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Efficiency – Memory, Network and Disk Space Management | 1,00 | 1,00 | | 1,00 |
| Secure Coding – API Abuse | 3,98 | 1,00 | | 1,00 |
| Programming Practices – Error and Exception Handling | 1,00 | 1,00 | | 1,00 |
| Programming Practices – Unexpected Behavior | 3,96 | 2,89 | | 2,89 |
| Secure Coding – Time and State | 4,00 | 2,94 | | 2,94 |
| Architecture – OS and Platform Independence | 4,00 | 3,40 | | 3,40 |
| Secure Coding – Weak Security Features | 3,81 | 3,98 | | 3,83 |
| Secure Coding – Input Validation | 4,00 | 3,86 | | 3,86 |
| Architecture – Multi-Layers and Data Access | 4,00 | 3,86 | 3,89 | 3,87 |
| Secure Coding – Encapsulation | 4,00 | 4,00 | | 4,00 |

Tabel 31: Technische criteria met risicoscore voor beveiliging van OSV2020-U.

| Measurement | NL | ELECT | DB | Total |
|---|----|-------|----|-------|
| Persistent class method's equals() and hashCode() must access its fields through getter methods | | 1,00 | | 1,00 |
| Review APIs not accessed by frontend functions | | 1,00 | | 1,00 |

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Avoid Stateful Beans not removed | | 1,00 | | 1,00 |
| Avoid using unnormalized input strings | | 1,00 | | 1,00 |
| Pages should use error handling page | 1,00 | 1,00 | | 1,00 |
| Avoid public/protected setter for the generated identifier field | | 1,00 | | 1,00 |
| Avoid using insufficient random generator | 1,00 | 1,00 | | 1,00 |
| Avoid direct definition of JavaScript Functions in a Web page (Javascript/HTML5) | | 1,00 | | 1,00 |
| Avoid static Field of type collection | 1,00 | | | 1,00 |
| Provide a private default Constructor for utility Classes (JEE) | 1,19 | 1,00 | | 1,00 |
| Favor PreparedStatement or CallableStatement over Statement | | 1,00 | | 1,00 |
| Avoid non thread safe singleton | | 1,00 | | 1,00 |
| Avoid use of a reversible one-way hash | 1,00 | | | 1,00 |
| Avoid using references to the id in the persistent class's method equals() | 4,00 | 1,00 | | 1,00 |
| Avoid Fields in Servlet Classes that are not final static | | 1,00 | | 1,00 |
| Avoid missing release of stream connection after an effective lifetime | 1,00 | 1,00 | | 1,00 |
| Avoid Unvalidated URL Redirect | | 1,00 | | 1,00 |
| Avoid testing floating point numbers for equality | | 1,00 | | 1,00 |
| Avoid file path manipulation | 4,00 | 1,00 | | 1,00 |
| Avoid reflected cross-site scripting (non persistent) | 4,00 | 1,00 | | 1,00 |
| Avoid URL redirection to untrusted site | 4,00 | 1,00 | | 1,00 |
| Use ANSI standard operators in SQL WHERE clauses | | 1,00 | | 1,00 |
| Avoid empty catch blocks for methods with high fan-in | 1,00 | 1,00 | | 1,00 |
| Avoid instanceof in Methods that override or implement Object,equals(), Comparable,compareTo() | 2,38 | 1,83 | | 1,85 |
| Avoid many-to-many association | | 1,95 | | 1,95 |
| Declare as Static all methods not using instance members (JEE) | 2,51 | 1,95 | | 1,96 |
| Avoid throwing an exception in a catch block without chaining it | 2,14 | 2,34 | | 2,30 |
| Avoid hidden form fields to prevent parameter tampering (Javascript/HTML5) | 4,00 | 2,79 | | 2,88 |
| Avoid empty catch blocks | 3,57 | 3,47 | | 3,48 |
| Avoid having multiple artifacts deleting data on the same SQL table | | | 3,56 | 3,56 |
| All types of a serializable Class must be serializable | 3,82 | 3,56 | | 3,57 |
| Avoid to use this within Constructor in multi-thread environment | 4,00 | 3,73 | | 3,75 |
| Avoid using deprecated method, constructor, field, type or package | 3,97 | 3,88 | | 3,90 |
| Avoid directly throwing instance of Exception class | 3,99 | 3,98 | | 3,98 |

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Avoid catching an exception of type Exception, RuntimeException, or Throwable | 4,00 | 3,99 | | 3,99 |
| Avoid hardcoded network resource names (JEE) | 3,89 | 4,00 | | 3,99 |
| Avoid using SAXParserFactory without restriction of XML External Entity Reference (XXE) | 4,00 | 4,00 | | 4,00 |
| CWE-681: Avoid numerical data corruption during incompatible mutation | 4,00 | 4,00 | | 4,00 |
| Check usage of '==' and '!=' on objects | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,System,exit()' | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,lang,Runtime,exec()' | 4,00 | 4,00 | | 4,00 |
| Avoid using predictable SecureRandom Seeds | 4,00 | 4,00 | | 4,00 |
| Avoid declaring throwing an exception and not throwing it | 4,00 | 4,00 | | 4,00 |
| Avoid missing default in switch statements | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,lang,Error' | 4,00 | 4,00 | | 4,00 |
| Use declarative transaction | 4,00 | 4,00 | | 4,00 |
| Avoid having multiple artifacts updating data on the same SQL Table | | | 4,00 | 4,00 |
| Avoid large number of String concatenation (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid using Vector | 4,00 | 4,00 | | 4,00 |
| Blocking synchronous calls should have associated timeouts | 4,00 | 4,00 | | 4,00 |
| Avoid Classes with a High Public Data Ratio | 4,00 | 4,00 | | 4,00 |
| Avoid declaring Non Final Class Variables with Public or Package access type | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,io,File' | 4,00 | 4,00 | | 4,00 |
| Avoid using 'sun,*' Classes | 4,00 | 4,00 | | 4,00 |
| Avoid using 'java,lang,System,getenv()' | 4,00 | 4,00 | | 4,00 |
| Avoid code injection | 4,00 | 4,00 | | 4,00 |
| Avoid deserialization injection | 4,00 | 4,00 | | 4,00 |
| Avoid deserialization injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid expression language injection | 4,00 | 4,00 | | 4,00 |
| Avoid expression language injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid hard-coded credentials | | 4,00 | | 4,00 |
| Avoid HTTP response splitting | 4,00 | 4,00 | | 4,00 |
| Avoid HTTP response splitting through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid LDAP injection | 4,00 | 4,00 | | 4,00 |
| Avoid NoSQL injection | 4,00 | 4,00 | | 4,00 |
| Avoid NoSQL injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid OS command injection | 4,00 | 4,00 | | 4,00 |

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|----|-------|
| Avoid process control | 4,00 | 4,00 | | 4,00 |
| Avoid reflection injection | 4,00 | 4,00 | | 4,00 |
| Avoid regular expression injection | 4,00 | 4,00 | | 4,00 |
| Avoid regular expression injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid resource injection | 4,00 | 4,00 | | 4,00 |
| Avoid resource injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid resource URL manipulation | 4,00 | 4,00 | | 4,00 |
| Avoid resource URL manipulation through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid second order deserialization injection | 4,00 | 4,00 | | 4,00 |
| Avoid second order expression language injection | 4,00 | 4,00 | | 4,00 |
| Avoid second order OS command injection | 4,00 | 4,00 | | 4,00 |
| Avoid second order regular expression injection | 4,00 | 4,00 | | 4,00 |
| Avoid second order SQL injection | 4,00 | 4,00 | | 4,00 |
| Avoid second order XPath injection | 4,00 | 4,00 | | 4,00 |
| Avoid SQL injection | 4,00 | 4,00 | | 4,00 |
| Avoid SQL injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid thread injection | 4,00 | 4,00 | | 4,00 |
| Avoid thread injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid uncontrolled format string | 4,00 | 4,00 | | 4,00 |
| Avoid uncontrolled format string through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid URL redirection to untrusted site through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid XPath injection | 4,00 | 4,00 | | 4,00 |
| Avoid XPath injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid code injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid cross-site scripting (persistent) | 4,00 | 4,00 | | 4,00 |
| Avoid cross-site scripting through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid dangerous file inclusion | 4,00 | 4,00 | | 4,00 |
| Avoid external control of system or configuration setting | 4,00 | 4,00 | | 4,00 |
| Avoid external control of system or configuration setting through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid file path manipulation through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid LDAP injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid mixing trusted and untrusted data in HTTP requests | 4,00 | 4,00 | | 4,00 |
| Avoid mixing trusted and untrusted data in HTTP requests through API requests | 4,00 | 4,00 | | 4,00 |

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|----|-------|
| Avoid MVC injection | 4,00 | 4,00 | | 4,00 |
| Avoid MVC injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid OS command injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid process control through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid reflection injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid second order LDAP injection | 4,00 | 4,00 | | 4,00 |
| Avoid second order server-side request forgery | 4,00 | 4,00 | | 4,00 |
| Avoid second order URL redirection to untrusted site | 4,00 | 4,00 | | 4,00 |
| Avoid second order XQuery injection | 4,00 | 4,00 | | 4,00 |
| Avoid server-side request forgery | 4,00 | 4,00 | | 4,00 |
| Avoid server-side request forgery through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid Struts 2 Action Fields without Validation | 4,00 | 4,00 | | 4,00 |
| Avoid using DocumentBuilder without restriction of XML External Entity Reference (XXE) | 4,00 | 4,00 | | 4,00 |
| Avoid using javascript or expression in the CSS file | | 4,00 | | 4,00 |
| Avoid using submitted markup containing "form" and "formaction" attributes | 4,00 | 4,00 | | 4,00 |
| Avoid using XMLReader without restriction of XML External Entity Reference (XXE) | 4,00 | 4,00 | | 4,00 |
| Avoid using XMLStreamReader without restriction of XML External Entity Reference (XXE) | 4,00 | 4,00 | | 4,00 |
| Avoid using XPathFactory without restriction of XML External Entity Reference (XXE) | 4,00 | 4,00 | | 4,00 |
| Avoid XQuery injection | 4,00 | 4,00 | | 4,00 |
| Avoid XQuery injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid Empty Finally Block When Calling Resource | 4,00 | 4,00 | | 4,00 |
| Avoid improper processing of the execution status of data handling operations | | 4,00 | | 4,00 |
| Avoid directly instantiating a Class used as a managed bean | 4,00 | 4,00 | | 4,00 |
| Persistent classes should Implement hashCode() and equals() | | 4,00 | | 4,00 |
| Avoid using Apache ActiveMQ 5,x before 5,13,0 | 4,00 | 4,00 | | 4,00 |
| Avoid using referer header field in HTTP request | 4,00 | 4,00 | | 4,00 |
| Avoid cookie injection | 4,00 | 4,00 | | 4,00 |
| Avoid data filter injection | 4,00 | 4,00 | | 4,00 |
| Avoid data filter injection through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid log forging | 4,00 | 4,00 | | 4,00 |
| Avoid log forging through API requests | 4,00 | 4,00 | | 4,00 |

| Measurement | NL | ELECT | DB | Total |
|---|------|-------|----|-------|
| Avoid return statement in finally block (Javascript) | | 4,00 | | 4,00 |
| Never exit a finally block with a return, break, continue, or throw | 4,00 | 4,00 | | 4,00 |
| Always enable authorization checks at function level for functions called on by APIs based with Spring Application | | 4,00 | | 4,00 |
| Avoid using RSA Cryptographic algorithms without OAEP (Optimal Asymmetric Encryption Padding) | 4,00 | 4,00 | | 4,00 |
| Avoid using Web SQL databases | | 4,00 | | 4,00 |
| Avoid using eval() (Javascript) | | 4,00 | | 4,00 |
| Avoid having iframe inside a tag | 4,00 | 4,00 | | 4,00 |
| Avoid hosting HTML code in iframe srcdoc | 4,00 | 4,00 | | 4,00 |
| Avoid using autofocus and onblur in submitted markup | 4,00 | 4,00 | | 4,00 |
| Avoid using autofocus and onfocus in submitted markup | 4,00 | 4,00 | | 4,00 |
| Avoid using import with external URI | 4,00 | 4,00 | | 4,00 |
| Avoid using oninput in body containing input autofocus | 4,00 | 4,00 | | 4,00 |
| Avoid using onscroll event with autofocus input | 4,00 | 4,00 | | 4,00 |
| Avoid using setData in ondragstart with attribute draggable set to true | 4,00 | 4,00 | | 4,00 |
| Avoid using setTimeout() (Javascript) | | 4,00 | | 4,00 |
| Avoid using source tag in video/audio with event handler | 4,00 | 4,00 | | 4,00 |
| Avoid using submit markup related to "form" with id attribute | 4,00 | 4,00 | | 4,00 |
| Avoid using video poster attributes in combination with javascript | 4,00 | 4,00 | | 4,00 |
| Avoid white-listing the "dirname" attribute in user generated content | 4,00 | 4,00 | | 4,00 |
| Always implement readObject() to prevent untrusted deserialization when loading from ObjectInputStream | 4,00 | 4,00 | | 4,00 |
| Avoid creating cookie without setting httpOnly option (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid plaintext storage of password | 4,00 | 4,00 | | 4,00 |
| Avoid using Cipher with no HMAC to ensure data integrity | 4,00 | 4,00 | | 4,00 |
| Avoid using cryptography hash with hard-coded salt | 4,00 | 4,00 | | 4,00 |
| Avoid using Insecure PBE Iteration Count | 4,00 | 4,00 | | 4,00 |
| Avoid using javax.crypto.NullCipher | 4,00 | 4,00 | | 4,00 |
| Avoid using unsecured cookie (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid hard-coded passwords (Javascript) | | 4,00 | | 4,00 |
| Avoid using generic methods such as 'ToJson' or 'ToString' to save sensitive or PII data | 4,00 | 4,00 | | 4,00 |
| Review APIs returning sensitive data fields | | 4,00 | | 4,00 |
| Avoid weak encryption providing not sufficient key size (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid Http Session without expiration | 4,00 | 4,00 | | 4,00 |

| Measurement | NL | ELECT | DB | Total |
|---|------|-------|----|-------|
| Avoid using HttpServletRequest,getRequestId() | 4,00 | 4,00 | | 4,00 |
| Avoid using risky cryptographic hash (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid creating cookie with an overly broad path (JEE) | | 4,00 | | 4,00 |
| Avoid generating key with insufficient random generator in cookies | 4,00 | 4,00 | | 4,00 |
| Avoid insecure use of YAML deserialization when using SnakeYaml (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid thrown Exceptions in servlet methods | | 4,00 | | 4,00 |
| Avoid using DefaultHttpClient constructor | 4,00 | 4,00 | | 4,00 |
| Avoid using deprecated SSL protocols to secure connection | 4,00 | 4,00 | | 4,00 |
| Avoid using jYAML to deserialize YAML (JEE) | 4,00 | 4,00 | | 4,00 |
| Avoid providing password in Web Service URL | 4,00 | 4,00 | | 4,00 |
| Avoid thread creation for application running on application server | 4,00 | 4,00 | | 4,00 |
| Avoid using 'System.gc' | 4,00 | 4,00 | | 4,00 |
| Close database resources ASAP | 4,00 | 4,00 | | 4,00 |
| CWE-672: Expired or Released Resource should not be used | 4,00 | 4,00 | | 4,00 |
| Avoid double checked locking | 4,00 | 4,00 | | 4,00 |
| Avoid having cookie with an overly broad domain (JEE) | | 4,00 | | 4,00 |
| Avoid using the Non-Serializable Object Stored in Session | | 4,00 | | 4,00 |
| Avoid debug forging | 4,00 | 4,00 | | 4,00 |
| Avoid debug forging through API requests | 4,00 | 4,00 | | 4,00 |
| Avoid enabling autocomplete "on" for inputs/forms | 4,00 | 4,00 | | 4,00 |
| Avoid catch blocks with assertion | 4,00 | 4,00 | | 4,00 |
| Avoid direct Class inheritance from java.lang.Throwable | 4,00 | 4,00 | | 4,00 |
| Avoid empty finally blocks | 4,00 | 4,00 | | 4,00 |
| Avoid using 'Throwable,printStackTrace()' outside a try catch block | 4,00 | 4,00 | | 4,00 |
| Always define column names when inserting values | | 4,00 | | 4,00 |
| Avoid EJBs using 'synchronized' qualifier, 'wait', 'notify' and 'notifyAll' Methods | 4,00 | 4,00 | | 4,00 |
| Avoid non serializable Entities | | 4,00 | | 4,00 |
| Avoid not aliased Tables | | 4,00 | | 4,00 |
| Avoid specifying column numbers instead of column names in ORDER BY clauses | | 4,00 | | 4,00 |
| Avoid unqualified column references | | 4,00 | | 4,00 |
| Avoid using delete on arrays | | 4,00 | | 4,00 |
| Avoid using delete with no object properties | 4,00 | 4,00 | | 4,00 |
| Avoid using Javascript Function constructor | | 4,00 | | 4,00 |

| Measurement | NL | ELECT | DB | Total |
|--|------|-------|------|-------|
| Avoid using native Methods (JNI) | 4,00 | 4,00 | | 4,00 |
| Collection-typed attributes getter must be defined with the correct interface | | 4,00 | | 4,00 |
| Avoid hard-coded network resource names (Javascript) | | 4,00 | | 4,00 |
| Avoid calls between JSP Pages | 4,00 | 4,00 | | 4,00 |
| Avoid database tables associated to more than one Entity | | 4,00 | | 4,00 |
| Avoid direct access to Database Tables | 4,00 | 4,00 | | 4,00 |
| Avoid direct access to Database Tables in Javascript | | 4,00 | | 4,00 |
| Avoid direct use of Database objects (JSP/ASP) | 4,00 | 4,00 | | 4,00 |
| Avoid having multiple artifacts inserting data on the same SQL Table | | | 4,00 | 4,00 |
| Avoid Tables without Primary Key (SQL) | | | 4,00 | 4,00 |
| Avoid blocking page loading with synchronous Javascript import | 4,00 | 4,00 | | 4,00 |
| Avoid instantiating Boolean | 4,00 | 4,00 | | 4,00 |
| Avoid String initialization with String object (created using the 'new' keyword) | 4,00 | 4,00 | | 4,00 |
| Avoid using DriverManager | | 4,00 | | 4,00 |
| Avoid using Hashtable | 4,00 | 4,00 | | 4,00 |
| Avoid using Javascript Document,all collection | | 4,00 | | 4,00 |
| Serialize session objects | 4,00 | 4,00 | | 4,00 |
| Avoid using console,log() (Javascript) | | 4,00 | | 4,00 |
| Avoid using URL,equals(Object obj) or URL,hashCode() | 4,00 | 4,00 | | 4,00 |
| Use version instead of timestamp | | 4,00 | | 4,00 |
| Avoid table and column names that are too long (portability) | | 4,00 | | 4,00 |

Tabel 32: Metingen met risicoscore voor beveiliging van OSV2020-U.

Het tool constateert voor drie kritische metingen dat er beveiligingskwetsbaarheden voorkomen. CAST beschouwt een meting als kritisch als aangetroffen potentiële kwetsbaarheden een groot effect kunnen hebben als deze zich daadwerkelijk manifesteren. De door CAST als kritisch aangemerkte potentiële kwetsbaarheden zijn opgenomen in Tabel 33. Daarnaast levert CAST specifiek voor beveiliging kwetsbaarheden op tegen CWE (Common Weakness Enumeration; zie: cwe.mitre.org/). Deze zijn opgenomen in Tabel 34. Ons oordeel is dat deze kwetsbaarheden onderzocht moeten worden en verbetering daarvan moet worden doorgevoerd ter verdere verbetering van de beveiliging.

| Technisch criterium | Meting | Artifact | Code-regel(s) |
|---|--|---|---------------|
| Programming Practices – Error and Exception Handling | Avoid empty catch blocks for methods with high fan-in | de.ivu.elect.util.ElectRandom.getRandom | 17 |
| | | de.ivu.elect.presentation.NISystemProperties.getDefaultElectionLevel | 44 |
| | | de.ivu.elect.business.benutzerverwaltung.entity.AbstractRolle.getRecht | 81 |
| | | de.ivu.elect.business.stimmeingabe.entity.AbstractStimmeingabe.hasAnzahlGroesserGleichNull | 123 |
| | | de.ivu.elect.presentation.gebietsbaum.NIGebietNummerFormatter.getDarstellung | 26 |
| | | de.ivu.elect.presentation.gebietsbaum.NIGebietNummerFormatter.getNummer | 47 |
| | | de.ivu.elect.dokumente.DokumentFormatter.formatNumber | 429 |
| | | de.ivu.elect.business.konfiguration.entity.AbstractKonfigurationLoader.getParameter | 190 |
| Efficiency – Memory, Network and Disk Space Management | Avoid missing release of stream connection after an effective lifetime | de.ivu.elect.exchange.zip.DelegateZipImportMapper.validateInputFormat | 49 |
| | | de.ivu.elect.core.exchange.wahl.AbstractNIExportArtefaktNachSystemExportstatusZipExportMapper.serialize | 187 |
| | | de.ivu.elect.was.exchange.okwahl.AbstractOkWahlZipExportMapper.serialize | 58 |
| | | de.ivu.elect.was.exchange.stimmeingabe.WasStimmeingabeXMLZIPEXportMapper.serialize | 31 |
| | | de.ivu.elect.wus.exchange.stimmzettel.AbstractStimmzettelZipExportMapper.serialize | 90 |
| | | de.ivu.elect.exchange.lokalisierung.properties.LokalisierungPropertiesExportMapper.schreibeProperties | 87 |
| | | de.ivu.elect.util.ThirdPartyReader.readThirdPartyInfos | 32 |
| | | | |

| Technisch criterium | Meting | Artifact | Code-regel(s) |
|----------------------------------|--|---|---------------|
| | | de.ivu.elect.was.exchange.stimmeingabe. WasErgebniseingangXMLZIPEXportMapper.serialize | 58 |
| Secure Coding – API Abuse | Review APIs not accessed by frontend functions | de.ivu.elect.presentation.ui.FaviconServlet.doGet/favicon/GET | 33-65 |

Tabel 33: Kwetsbaarheden voor kritische metingen zoals gedetecteerd door CAST AIP.

| CWE | Meting | Artifact | Coderegel(s) |
|--|--|---|---------------------------------------|
| CWE-477 – Use of Obsolete Function | Avoid using deprecated method, constructor, field, type or package | Komt voor in 1.569 objecten | |
| CWE-681 – Incorrect Conversion between Numeric Types | Avoid using incompatible mutation | Komt voor in 63 objecten | |
| CWE-543 – Use of Singleton Pattern Without Synchronization in a Multithreaded Context | Avoid defining singleton or factory classes when using Spring | Komt voor in 52 objecten | |
| | Avoid non thread safe singleton | de.ivu.elect.dokumente.wahlvorschlag. CoreWahlvorschlagsdatenDocument | Class CoreWahlvorschlagsdatenDocument |
| | | de.ivu.elect.sitzberechnung. math.Fraction | Class Fraction |
| CWE-778 – Insufficient Logging | Avoid throwing an exception in a catch block without chaining it | Komt voor in 17 objecten | |
| CWE-772 – Missing Release of Resource after Effective Lifetime | Avoid missing release of stream connection after an effective lifetime | Komt voor in 8 objecten | Zie Tabel 33. |
| CWE-567 – Unsynchronized Access to Shared Data in a Multithreaded Context | Avoid Fields in Servlet Classes that are not final static | de.ivu.elect.business.praesentation.control. PraesentationStaticResourceServlet.messages | Regels 52-53 |

| CWE | Meting | Artifact | Coderegel(s) |
|--|---|---|--------------|
| | | de.ivu.elect.business.praesentation.control.PraesentationStaticResourceServlet.praesentationServletPathFinder | Regels 49-50 |
| | | de.ivu.elect.business.praesentation.control.PraesentationStaticResourceServlet.praesentationStaticResourceServletSecurity | Regels 55-56 |
| | | de.ivu.elect.presentation.hilfe.HelpStaticResourceServlet.helpReader | Regels 27-28 |
| CWE-821 – Incorrect Synchronization | Blocking synchronous calls should have associated timeouts | de.ivu.elect.business.dokumente.boundary.AbstractDokumentGenerator.generiereDokumentSynchron | Regel 166 |
| | | de.ivu.elect.presentation.dokumente.AbstractDokumentErzeugenView.erzeugeDokumentInternalSynchron | Regel 448 |
| | | de.ivu.elect.presentation.dokumente.AbstractDokumentErzeugenView.poll | Regel 604 |
| CWE-611 – Improper Restriction of XML External Entity Reference | Avoid using SAXParserFactory without restriction of XML External Entity Reference (XXE) | de.ivu.elect.jee.exchange.JAXBUtil.unmarshal | Regel 120 |
| | | de.ivu.wahl.wus.xmlsecurity.SAXParserFactoryUtil.getSAXParserFactory | Regel 40 |
| CWE-22 – Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | Avoid file path manipulation | de.ivu.elect.util.ZipFileUtil.unzip | Regel 37 |
| CWE-23 – Relative Path Traversal | Avoid file path manipulation | de.ivu.elect.util.ZipFileUtil.unzip | Regel 37 |
| CWE-36 – Absolute Path Traversal | Avoid file path manipulation | | |

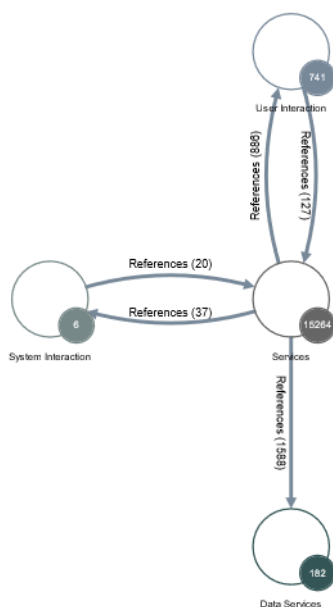
| CWE | Meting | Artifact | Coderegel(s) |
|--|---|---|-------------------|
| CWE-78 – Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | Avoid using 'java.lang.Runtime.exec()' | de.ivu.elect.business.system.control.KillProcess.run | Regels 74-87 |
| CWE-79 – Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | Avoid reflected cross-site scripting (non persistent) | de.ivu.elect.presentation.IvuCdataFilter.doFilter | Regels 40, 47, 50 |
| CWE-401 – Missing Release of Memory after Effective Lifetime | Avoid static Field of type collection | de.ivu.elect.business.security.control.NIElectExtendedUseCasePermissionFilter.DENYLIST_CACHE_KEINE_WAHL | Regel 51 |

Tabel 34: kwetsbaarheden voor CWE.

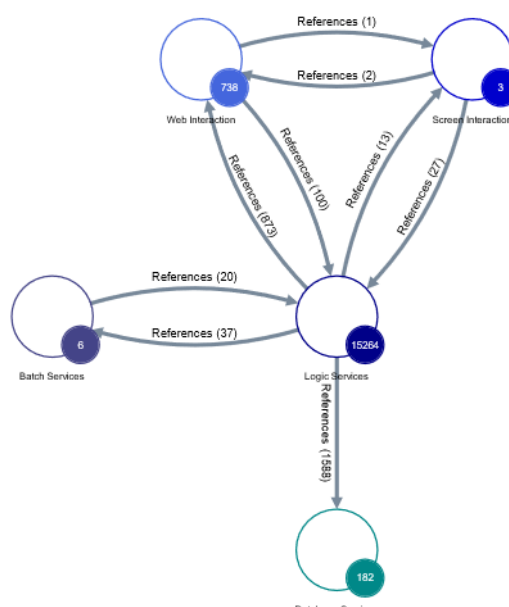
C.5 Applicatiestructuurvisualisaties

We hebben CAST Imaging²² gebruikt om de applicatiestructuur van OSV2020-U te onderzoeken. In dit tool worden visualisaties van OSV2020-U geleverd op basis van de broncode.

Een van de visualisaties die CAST Imaging biedt inzicht in de applicatiearchitectuur. Daartoe worden de sources ingedeeld naar de componenten waartoe deze behoren (op basis van hun extensies, naamgeving en functie binnen de applicatie). De statische code analyse met CAST AIP levert de relaties tussen de componenten. De hiernavolgende figuren zijn met CAST Imaging gegenereerd. Elke bol visualiseert de gegroepede sources. Het cijfer in de bol geeft aan hoeveel bestanden tot de betreffende component behoren. Bij de pijlen die de afhankelijkheden weergeven is het aantal referenties weergegeven zoals die in de sources zijn aangetroffen.

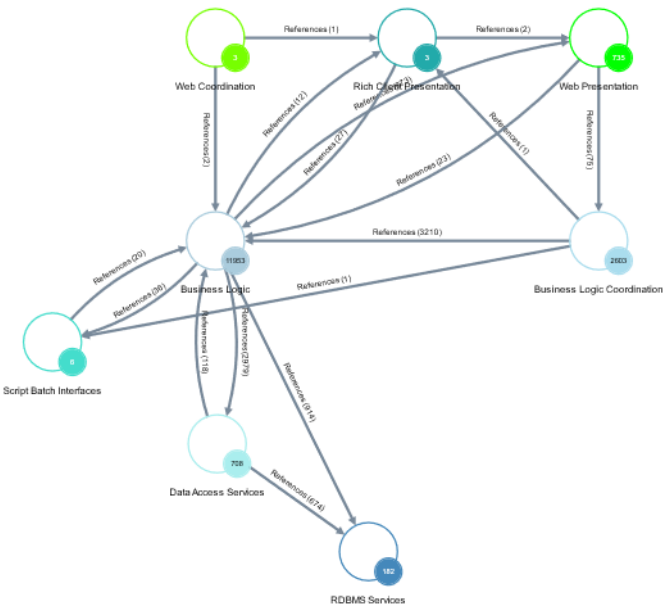


Level 1.

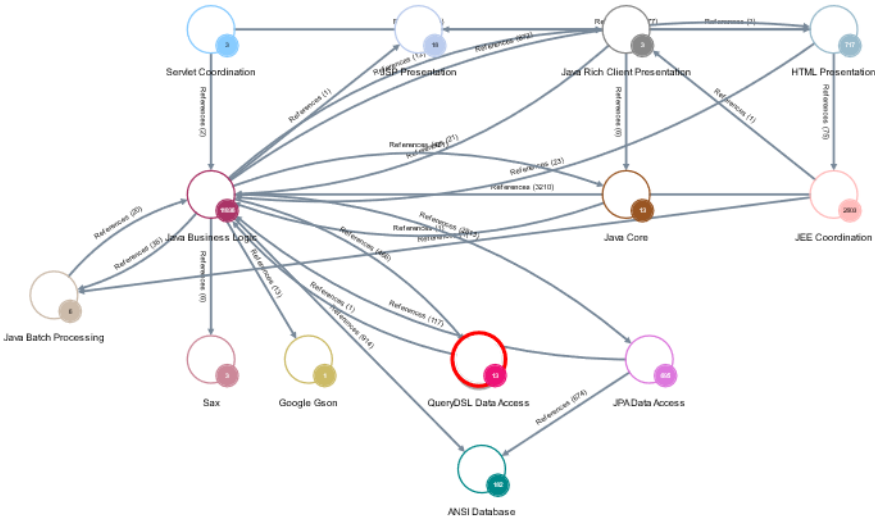


Level 2.

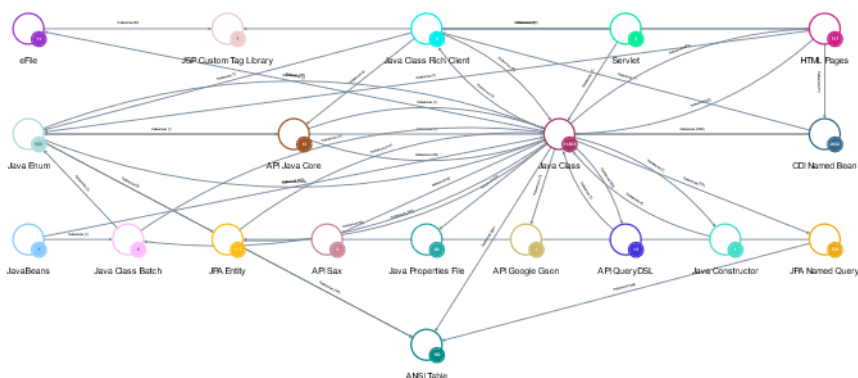
²². Zie: learn.castsoftware.com/imaging.



Level 3.



Level 4.



Level 5.

Figuur 13: Applicatiestructuur van OSV2020-U

Op basis van deze visualisaties van de applicatiestructuur zijn we van mening dat de structuur van de code onvoldoende helder is voor efficiënte doorvoering van aanpassingen. Dit is gebaseerd op de volgende observaties:

- We zien veel circulaire afhankelijkheden tussen de componenten.
- De naamgeving is zowel in Engels als Duits. Dit levert verwarring als een ontwikkelaar moet zoeken in welk van de componenten specifieke functionaliteit gerealiseerd is.

Annex D Tekenset basisregistratie personen

Volgens wet- en regelgeving dient OSV2020 de tekenset te ondersteunen die is beschreven in het Logisch Ontwerp BRP [6]. In paragraaf 5.1.1 van dit Logisch Ontwerp wordt voorgeschreven welke tekens, gebaseerd op de Teletex-standaard, binnen het BRP-systeem gebruikt mogen worden en hoe deze te coderen. Deze tekenset is opgenomen in deze Annex. Tevens is aangegeven in hoeverre de betreffende tekens voldoen aan de toets die we hebben uitgevoerd voor OSV2020-U.

D.1 Overzicht van de te gebruiken Teletex-tekens

De volgende tabel bevat een volledig overzicht van alle karakters die binnen Teletex voorkomen.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|----|---|---|---|---|---|---|---|----|---|---|---|---|----|----|
| 0 | | SP | 0 | @ | P | | p | | | | | ° | | | Ω | κ |
| 1 | | ! | 1 | A | Q | a | q | | | i | ± | ` | | | Æ | æ |
| 2 | | " | 2 | B | R | b | r | | | ¢ | 2 | ' | | | Ð | ð |
| 3 | | | 3 | C | S | c | s | | | £ | 3 | ^ | | | ª | ä |
| 4 | | | 4 | D | T | d | t | | | \$ | x | ~ | | | Ĥ | ĥ |
| 5 | | % | 5 | E | U | e | u | | | ¥ | μ | — | | | | ı |
| 6 | | & | 6 | F | V | f | v | | | # | ¶ | ˘ | | | IJ | ij |
| 7 | | ' | 7 | G | W | g | w | | | § | · | · | | | Ł | ł |
| 8 | | (| 8 | H | X | h | x | | | × | ÷ | ¨ | | | Ł | ł |
| 9 | |) | 9 | I | Y | i | y | | | | | | | | Ø | ø |
| A | | * | : | J | Z | j | z | | | | | | ° | | Œ | œ |
| B | | + | ; | K | [| k | | | | « | » | ¸ | | | º | ß |
| C | | , | < | L | | l | | | | | | ¼ | - | | Ɔ | ɔ |
| D | | - | = | M |] | m | | | | | | ½ | “ | | Ʀ | ƣ |
| E | | . | > | N | | n | | | | | | ¾ | ¸ | | Ŋ | ŋ |
| F | | / | ? | O | _ | o | | | | | | ¿ | ˘ | | ŋ | |

De volgende tabel bevat alle tekens uit de Teletex-tekenset die binnen het BRP-systeem gebruikt mogen worden (zie: 5.1.1.3 van het Logisch Ontwerp GBA [6]). Niet opgenomen tekens mogen niet gebruikt worden. Dat betreft onder andere de Hollandse IJ (codes E6 en F6). Voor de diakritische karakters (codes C0 t/m CF) geldt dat die slechts mogen voorkomen in combinatie met een ander karakter. In de laatste kolom is aangegeven of het betreffende karakter geslaagd is (✓) 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 | ✓ |
| 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 | ✓ |

| T.61 code | UTF-8 code | Char | Omschrijving | Check |
|-----------|------------|------|----------------------|-------|
| 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 | ✓ |
| 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 | ✓ |

| T.61 code | UTF-8 code | Char | Omschrijving | Check |
|-----------|------------|------|---------------------------|-------|
| 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 | ✓ |
| 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 | ✓ |

| T.61 code | UTF-8 code | Char | Omschrijving | Check |
|-----------|------------|------|------------------------------|-------|
| 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 diphthong | ✓ |
| E2 | C4 90 | Ð | Capital D with stroke | ✓ |
| E3 | C2 AA | ª | Ordinal indicator, feminine | ✓ |
| E4 | C4 A6 | ⱦ | Capital H with stroke | ✓ |
| E7 | C4 BF | Ł | 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 | Ʀ | Capital T with stroke | ✓ |

| T.61 code | UTF-8 code | Char | Omschrijving | Check |
|-----------|------------|------|-------------------------|-------|
| EE | C5 8A | Ŋ | Capital eng, Lapp | ✓ |
| EF | C5 89 | ñ | Small n with apostrophe | ✓ |
| F0 | C4 B8 | κ | Small k, Greenlandic | ✓ |
| F1 | C3 A6 | æ | Small ae, diphthong | ✓ |
| 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 | ✓ |

| T.61 code | UTF-8 code | Char | Omschrijving | Check |
|-----------|------------|------|-------------------------|-------|
| F7 | C5 80 | ı̇ | Small I with middle dot | ✓ |
| F8 | C5 82 | ı̈ | Small I with stroke | ✓ |
| F9 | C3 B8 | ø | Small o with slash | ✓ |
| FA | C5 93 | oe | Small oe ligature | ✓ |
| FB | C3 9F | ß | Small sharp s, German | ✓ |
| FC | C3 BE | þ | Small thorn, Icelandic | ✓ |
| FD | C5 A7 | ţ | Small t with stroke | ✓ |
| FE | C5 8B | ŋ | Small eng, Lapp | ✓ |

D.2 Overzicht van de te gebruiken gecombineerde Teletex-tekens

In de volgende tabel zijn alle gecombineerde tekens uit de Teletex-tekenset opgesomd die als teken binnen het BRP-systeem gebruikt mogen worden (zie: paragraaf 5.1.1.4 van het Logisch Ontwerp GBA [6]). 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 | ✓ ✓ |

| T.61 code | UTF-8 code | Char | T.61 code | UTF-8 code | Char | Naam | Check |
|-----------|------------|------|-----------|------------|------|--------------|-------|
| 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 | Ě | C7 65 | C4 97 | ě | E dot | ✓ ✓ |
| 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 | ğ | G cedilla | ✓ |
| 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 | Ï | C4 69 | C4 A9 | ï | 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 | ✓ ✓ |
| C2 4C | C4 B9 | Ĺ | C2 6C | C4 BA | ĺ | L acute | ✓ ✓ |
| CB 4C | C4 BB | Ľ | CB 6C | C4 BC | ľ | 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 | Ñ | 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 | ✓ ✓ |

| T.61 code | UTF-8 code | Char | T.61 code | UTF-8 code | Char | Naam | Check |
|-----------|------------|------|-----------|------------|------|----------------|-------|
| 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 | ř | 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 | ✓ ✓ |
| 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 | Û | CA 75 | C5 AF | ű | U ring | ✓ ✓ |
| aCD 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 | ÿ | 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 | ✓ ✓ |