Onderzoek Ondersteunende Software Verkiezingen: Uitslagvaststelling (OSV2020-U) (Tweede Kamer)

Rapportage voor de Kiesraad
Publicatieversie

Referentie: A2300029662 D5.2.2

—

22 september 2023

Inhoudsopgave

1. Management-samenvatting

Managementsamenvatting (1/4)

Inleiding

KPMG heeft in de maanden augustus en september van 2023 een op feiten gebaseerd onderzoek uitgevoerd naar de mate waarin de applicatie Ondersteunende Software Verkiezingen 2020: Uitslagvaststelling (hierna: OSV2020-U), versie 1.9.1 voldoet aan de wettelijke kaders.

Object van onderzoek

De OSV2020-U-applicatie wordt ontwikkeld door een externe leverancier in opdracht van de Kiesraad. Leverancier maakt daarvoor gebruik van een zelfontwikkeld platform genaamd ‘Elect’ dat onder andere ook in Duitsland voor verkiezingen wordt gebruikt. Het Elect-platform beschikt over een generieke set aan functionaliteiten; voor functionaliteiten die specifiek voor de Kiesraad zijn ontwikkeld is separaat maatwerk geleverd dat enkel in de Kiesraad-versie aanwezig is. Het platform is ontwikkeld met behulp van Java- en HTML-technologie en dient te worden geïnstalleerd op een computer van het centraal stembureau die niet verbonden is met het internet (air-gapped).

Opdracht en scope

Op verzoek van de Kiesraad is OSV2020-U versie 1.9.1 getoetst op de mate waarin de applicatie voldoet aan het wettelijk toetsingskader uit artikel P 1a van de Kieswet en de verdere uitwerking daarvan in het Kiesbesluit en de Kiesregeling. Dit toetsingskader bestaat uit een set van dertien eisen, vastgelegd in bijlage 2 bij artikel 2a van de Kiesregeling, waaraan het product van Leverancier dient te voldoen en waarop de Kiesraad periodiek toetst.

Versie 1.9.1 van OSV2020-U is thans voorzien als de versie waarmee de Kiesraad de Tweede Kamerverkiezingen in november 2023 wil ondersteunen. De toetsing is daarmee uitgevoerd met nadruk op de ondersteuning van Tweede Kamerverkiezingen. Toetsing van de applicatie met betrekking tot andere verkiezingstypen, zoals Europese Parlementsverkiezingen of Waterschapsverkiezingen, valt buiten scope van dit onderzoek.

Uitgevoerde activiteiten

Het onderzoek is uitgevoerd op basis van handmatige en geautomatiseerde analyse van de beschikbaar gestelde broncode, een documentatiestudie, interviews en het uitvoeren van functionele testen. De bevindingen zijn afgestemd met Leverancier van de applicatie in het kader van hoor en wederhoor en gedocumenteerd in deze rapportage.

Het onderzoek is uitgevoerd op versie 1.9.1 van OSV2020-U. In bijlage IV is een volledig overzicht opgenomen van de bestanden die voor dit onderzoek zijn gedeeld.

Algemeen beeld

Voor de meeste eisen die vervat zijn in de wettelijke kaders voldoet de applicatie aan de gestelde eisen. Wel is er een bevinding ten aanzien van de mate waarin de applicatie als open source is ontwikkeld (onderdeel G van het wettelijk toetsingskader) en zijn er een aantal aanbevelingen om de software verder te verbeteren.

Daarnaast geldt voor vrijwel alle onderdelen van het toetsingskader dat er geen eenduidig toetsbare specificatie bestaat en deze tot op zekere hoogte aan interpretatie onderhevig zijn. Redenerend vanuit de geest van het toetsingskader staan de bevindingen de toepassing van OSV2020-U echter niet in de weg.

Een nadere toelichting per eis is weergegeven in de tabel op de volgende pagina’s en een uitgebreid overzicht van de bevindingen en observaties per wettelijke eis is terug te vinden in hoofdstuk 3 ‘Wettelijke kaders’.

Naast het voldoen aan het wettelijk toetsingskader valt op dat er weinig systeemdocumentatie voorhanden is. Zo was meer documentatie verwacht rond de structuur van de applicatie en de wijze waarop aan Security- en Privacy-by-Design-principes invulling is gegeven.

Managementsamenvatting (2/4)

Geen substantiële bevindingen | Bevindingen ter overweging | Niet voldaan aan wettelijk toetsingskader

Onderdeel wettelijk kader	Resultaat	Toelichting
A. De programmatuur bevat de functionaliteiten die overeenkomstig de specificatie, bedoeld in artikel P 1, tweede lid, van het Kiesbesluit nodig zijn voor de berekening van de uitslag van de verkiezingen en de zetelverdeling		De functionaliteit van de programmatuur is getest gericht op de Tweede Kamerverkiezingen. Uit de testen blijkt dat de programmatuur voldoet aan de gestelde eis en alle functionaliteiten bevat die nodig zijn voor de berekening van de uitslag van de verkiezingen en de zetelverdeling, zoals bedoeld in artikel P 1, tweede lid, van het Kiesbesluit.
B. De programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn		De broncode is voldoende gestructureerd en past op verscheidene lagen maatregelen toe om modulaire aanpassingen door te kunnen voeren. Zo zijn de specifieke Nederlandse rekenregels vervat in een separate module binnen het Elect-platform. Wel is het aan te raden om te investeren in documentatie, gezien de omvang en complexiteit van de applicatie.
C. De kritische functies voor de berekening van de uitslag van de verkiezingen en de zetelverdeling zijn in de programmatuur herkenbaar en van elkaar gescheiden		Uit handmatige analyse en analyse met behulp van een gegenereerde dependency-matrix, blijkt dat de kritische functies, zoals gedefinieerd in de toelichting bij artikel P 1 van de Kiesregeling gepubliceerd in de *Staatscourant* (29577, 2014), over het algemeen goed te herkennen zijn en voldoende van elkaar gescheiden zijn.
D. De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen		Er is geverifieerd dat de applicatie, door middel van een aantal configuratie bestanden, ingezet kan worden voor verschillende verkiezingstypen zonder dat hiervoor aanpassingen aan de programmatuur nodig zijn. Andere verkiezingstypen zijn echter niet getest in het kader van dit onderzoek.
E. Toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen		Er zijn verschillende maatregelen getroffen om (toevallig of opzettelijk) foutief gebruik van de applicatie te voorkomen. Er is echter ruimte voor verbetering. De wijze waarop de applicatie controleert dat er geen internetverbinding is, is niet aangepast sinds het vorige onderzoek en nog altijd relatief eenvoudig te omzeilen. Hierbij moet opgemerkt worden dat een deel van de technische maatregelen enkel werkt bij het volgen van bijbehorende procedures. Deze procedures waren geen onderdeel van dit onderzoek.
F. 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		Er is tijdens het uitvoeren van de functionele testen geverifieerd dat de vereiste diakritische tekens in de applicatie ondersteund worden.

Managementsamenvatting (3/4)

Geen substantiële bevindingen | Bevindingen ter overweging | Niet voldaan aan wettelijk toetsingskader

Onderdeel wettelijk kader	Resultaat	Toelichting
G. De programmatuur wordt als open source ontwikkeld en maakt gebruik van open standaarden. Indien dit aantoonbaar niet mogelijk is, wordt technologie toegepast waarvan de doeltreffendheid in de praktijk is aangetoond en die direct toepasbaar is. Voor verkiezingsgegevens zoals kandidatenlijsten en zetelverdeling wordt de EML_NL standaard toegepast		De applicatie maakt enkel gebruik van open standaarden, maar is zelf niet volledig open source: het Elect-platform waar OSV2020-U op gebaseerd is, is een propriëtaire applicatie waarvan de broncode niet publiekelijk beschikbaar is, en voldoet daarmee niet aan de criteria voor open source richtlijnen zoals door OSI (de Open Source Initiative) vastgesteld en waaraan ook onder andere door overheid-community Pleio wordt gerefereerd. De Kiesraad geeft aan dat het, door het stopzetten van een recente aanbesteding in april 2023, op korte termijn niet kan voldoen aan deze vereiste en derhalve kiest voor 'proven technology'.
H. De standaardprogrammatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar		Hoewel het Elect-platform zelf geen vrij verkrijgbare programmatuur is, maakt de Kiesraad de specifieke broncode voor Nederlandse verkiezingstypen openbaar waardoor dit deel van de broncode door eenieder gecontroleerd kan worden. Daarnaast is de Kiesraad voornemens om alle onderdelen van de applicatie die benodigd zijn voor het maken van een testopstelling (op aanvraag) beschikbaar te stellen, waarmee aan het doel van het wettelijk kader voldaan wordt.
I. Het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau		De Kiesraad beschikt over het intellectueel eigendom van de op maat gemaakte software. Voor de rest van de applicatie, dat wil zeggen het Elect-platform, berust het eigendom bij Leverancier. Omdat het maatwerkdeel van de software niet opzichzelfstaand is, heeft de Kiesraad een onherroepelijk gebruiksrecht voor het Elect-platform.
J. De programmatuur is geschreven in een programmeertaal waarvoor een door een actieve gemeenschap onderhouden open source *compiler*, onderscheidenlijk *interpreter* beschikbaar is		De applicatie is geschreven in Java, dat een populaire en actief onderhouden programmeertaal is. Wel gebruikt de applicatie een versie van Java die binnenkort een deel van de ondersteuning zal verliezen, en wordt aangeraden over te stappen naar een recentere versie.
K. De programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem		De programmatuur is ontwikkeld voor verschillende besturingssystemen, waaronder Windows, Linux (Ubuntu) en macOS. Door middel van handmatige testen is geverifieerd dat de applicatie werkt op Windows 10 en Ubuntu, en daarmee voldoet aan de gestelde eis.

Managementsamenvatting (4/4)

Geen substantiële bevindingen | Bevindingen ter overweging | Niet voldaan aan wettelijk toetsingskader

Onderdeel wettelijk kader	Resultaat	Toelichting
L. Het is mogelijk de authenticiteit van de programmatuur vast te stellen		De authenticiteit van de programmatuur kan voorafgaand aan de installatie worden vastgesteld door een hash-waarde te berekenen over het installatiebestand en deze te vergelijken met een door de Kiesraad gepubliceerde waarde. Slechts bij een ongewijzigd installatiebestand zullen de waarden overeenkomen. De mogelijkheden om de authenticiteit van de applicatie te toetsen nadat deze geïnstalleerd is, zijn echter beperkt. In een dergelijk geval is de enige mogelijkheid om de (geverifieerde) applicatie op een ander platform nogmaals te installeren en de resulterende bestanden te vergelijken.
M. Bij het inlezen van verkiezingsgegevens in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening		Bij het inlezen van de gegevens in de applicatie wordt gebruikgemaakt van technische controles om de authenticiteit van de gebruikte gegevens vast te stellen, waaronder controles hash-waarden en een elektronische handtekening. Het verschilt per gegevensbestand welk type controle er gedaan moet worden.

2.

Inleiding en gevolgd proces

Inleiding en gevolgd proces

Aanleiding van de opdracht

De applicatie Ondersteunende Software Verkiezingen (OSV) wordt gebruikt voor de vaststelling van de uitslag en de zetelverdeling voor onder andere gemeenten en het centraal stembureau. Een eerdere versie van OSV is in 2009 ontwikkeld in opdracht van de Kiesraad, en is na 2019 vervangen door de opvolger OSV2020 die op een aantal aspecten vernieuwd en verbeterd is. Deze applicatie is onderverdeeld in drie onderwerpen, namelijk:

- kandidaatstellingssoftware voor politieke partijen;
- kandidaatstellingssoftware voor centrale stembureaus;
- software voor de vaststelling van de uitslag en zetelverdeling voor onder andere gemeenten en het centraal stembureau.

De Kiesraad laat deze software periodiek toetsen om te controleren of deze voldoet aan de wettelijke kaders (te weten het wettelijk toetsingskader uit artikel P 1a van de Kieswet en de verdere uitwerking daarvan in het Kiesbesluit en de Kiesregeling) en om de kwaliteit van de software te beoordelen. Dit onderzoek is daar onderdeel van, en richt zich specifiek op de ondersteuning voor de geplande Tweede Kamerverkiezingen in november 2023.

Doel

Het doel van de opdracht is het uitvoeren van een onafhankelijk onderzoek naar de mate waarin de applicatie voldoet aan het wettelijk toetsingskader uit artikel P 1a van de Kieswet en de verdere uitwerking daarvan in het Kiesbesluit en de Kiesregeling. Dit toetsingskader bestaat uit een set van dertien eisen waaraan het product van Leverancier dient te voldoen en waarop de Kiesraad periodiek toetst.

Uit het onderzoek moest duidelijk worden of de applicatie voldoet aan deze wettelijke kaders en ingezet kan worden bij verkiezingen, in dit geval specifiek de Tweede Kamerverkiezingen van november 2023.

Specifieker gesteld is gekeken of de applicatie voldoet aan de volgende eisen:

A. 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.
B. De programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn.
C. De kritische functies voor de berekening van de uitslag van de verkiezingen en de zetelverdeling zijn in de programmatuur herkenbaar en van elkaar gescheiden.
D. De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen.
E. Toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen.
F. 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.
G. 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.
H. De standaardprogrammatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar;
I. Het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau.
J. De programmatuur is geschreven in een programmeertaal waarvoor een door een actieve gemeenschap onderhouden open source *compiler*, onderscheidenlijk *interpreter* beschikbaar is.
K. De programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem.
L. Het is mogelijk de authenticiteit van de programmatuur vast te stellen.
M. Bij het inlezen van verkiezingsgegevens in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening.

Gevolgd proces

Het onderzoek is uitgevoerd in de periode augustus - september 2023 aan de hand van een analyse van de broncode van OSV2020-U (versie 1.9.1) en de beschikbaar gestelde documentatie (bijlage IV). Andere aspecten zoals organisatie en processen zijn buiten beschouwing gebleven. De bevindingen volgend uit het onderzoek zijn in het kader van hoor en wederhoor afgestemd met Leverancier.

3.
Toetsingsresultaten

A. Functioneel testen

Introductie

Om te bepalen of de programmatuur alle functionaliteiten bevat voor de berekening van de uitslag van de verkiezingen en de bijbehorende zetelverdeling zijn er functionele testen uitgevoerd aan de hand van de testscenario's die de Kiesraad heeft opgesteld. De software telt stemtellingen per stembureau op en berekent de zetelverdeling. Drie 'installers' zijn geleverd waarbij er een verschil is gemaakt tussen de verschillende niveaus (GSB, NBSB, HSB, HSB-C, NBSB-C en CSB). Op elk niveau zijn testen uitgevoerd.

Testaanpak

Voor het testen van de Tweede Kamerverkiezingen is er een onderscheid gemaakt tussen organisatieniveau, en daarvoor ook de installers, omdat de uiteindelijke telling van alle door de GSB en HSB verzamelde stemmen wordt uitgevoerd door de CSB. Als vervolg op de vorige reeks testen worden ook andere functionaliteiten en 'edge cases' getest om inzicht te krijgen in de functionaliteiten rondom het gebruik van de applicatie. Voor de berekening van de zetelverdeling zijn testscenario's opgesteld, weergegeven in de tabel die hiernaast is afgebeeld.

In totaal zijn dertien testscenario's opgesteld om de zetelverdeling en de aanwijzing van de kandidaten te toetsen. Deze scenario's worden 'TKx' genoemd om aan te geven dat ze de Tweede Kamerverkiezingen testen. Testen voor andere soorten verkiezingen zijn niet in scope van dit onderzoek.

Voor sommige scenario's zijn meerdere testgevallen opgesteld om een grotere dekking van alle mogelijkheden te hebben en meer vertrouwen te krijgen in de werking van de software. Zo worden testen met betrekking tot de toewijzing van restzetels meerdere malen en met verschillende configuraties uitgevoerd om te verifiëren dat de restzetel steeds aan de correcte kandidaat wordt toegewezen.

Bevindingen

In bijlage I is een samenvatting van de testresultaten opgenomen. Alle testgevallen zijn succesvol uitgevoerd. Er zijn geen bevindingen gedaan ten aanzien van de functionaliteit.

Testscenario's

Nr.	Scenario	Omschrijving
TK1	Zonder restzetels	Test om de basisfunctionaliteit van de software te analyseren zonder extra distributie van restzetels
TK2	Met restzetels	Test om de basisfunctionaliteit te analyseren, vergelijkbaar met TK1, maar de verdeling van restzetels is vereist
TK3	Meerdere restzetels	Test waarbij meerdere restzetels moeten worden verdeeld
TK4	Meerdere restzetels naar één partij	Test waarbij meerdere restzetels aan één partij moeten worden verdeeld
TK5	Volstrekte meerderheid	Test waarbij een partij de volstrekte meerderheid behaalt
TK6	Volstrekte meerderheid met loting	Test waarbij een partij de absolute meerderheid heeft en loting bepaalt van welke partij het zetelaantal wordt verminderd
TK7	Toewijzing restzetel na één loting	Test waarbij een loterij vereist is om de laatst overgebleven zetel toe te wijzen
TK8	Toewijzing restzetels na meerdere lotingen	Test waarbij een loterij vereist is om meerdere zetels toe te wijzen
TK9	Uitputting van lijsten	Test om uitputting van de lijst te testen
TK10	Toekenning van zetels bij lijstengroepen	Test waarbij zetels worden toegekend aan lijstengroepen
TK11	Uitputting bij lijstengroepen	Test waarbij paren van lijsten binnen lijstgroepen meer zetels krijgen dan vervuld worden
TK12	Voorkeurstemmen	Test waarbij zetels worden verdeeld op basis van voorkeurstemmen
TK13	Aanwijzing overige kandidaten	Test waarbij zetels worden verdeeld na de verdeling via voorkeursstemmen

Eis	Resultaat	Conclusie
Functioneel testen (A) De programmatuur bevat de functionaliteiten die overeenkomstig de specificatie als bedoeld in artikel P1, tweede lid, van het Kiesbesluit nodig zijn voor de berekening van de uitslag van de verkiezingen en de zetelverdeling	Geen bevindingen	Voldaan

B. Modulaire broncode

Introductie

Deze analyse is gebaseerd op de, in de programmeertaal Java geschreven en als JAR-bestand verpakte, broncode die is aangeleverd door de Kiesraad. Deze broncode betreft niet de afslag van de repository waarin de broncode wordt onderhouden, maar een combinatie van zowel de broncode, de gecompileerde componenten als externe packages (bibliotheken). Om te bepalen of de programmatuur gestructureerd opgezet is, is een handmatige analyse van de broncode uitgevoerd. Daarbij is gekeken naar de folderstructuur en de naamgeving. Daarnaast heeft steekproefsgewijs een visuele inspectie van de broncode plaatsgevonden.

Bevindingen

De programmatuur voldoet aan de gestelde eis. De broncode is gestructureerd opgebouwd in verschillende Java-packages die duidelijk gedefinieerd zijn en hun eigen functionaliteit huizen. Ditzelfde geldt voor de verschillende subfolders en classes die, waar toepasbaar, volgens een terugkerend patroon zijn opgebouwd. De folderstructuur is soms wat complex, en door de grote gelaagdheid van de folders is de leesbaarheid niet overal optimaal. Er zijn echter zeker een structuur en logica te herkennen in de opzet van de applicatie.

Binnen de broncode zelf wordt gebruikgemaakt van technieken en principes die modulariteit bevorderen. Zo wordt het Model-View-Controller (MVC-architectuurpatroon toegepast. Dit patroon verdeelt de applicatie in drie componenten: Model (de ‘entity’ packages), View (de ‘boundary’ packages) en Controller (de ‘control’ packages). Door MVC te gebruiken, ontstaat een meer modulaire codebase die beter onderhoudbaar en schaalbaar is, door een zorgvuldige scheiding van verantwoordelijkheden. Daarnaast wordt veelvuldig gebruikgemaakt van abstractie, en lijkt het concept ‘programming to an interface’ consequent gevolgd te worden. Het grote aantal kleine classes is een indicatie dat het Single Responsibility Principle goed gevolgd wordt, wat zeer belangrijk is voor het maken van modulaire aanpassingen.

Hierbij moet wel opgemerkt worden dat de code zeer complex is en dat de code nauwelijks documentatie bevat, zoals JavaDoc en/of inline commentaar. Dit, gecombineerd met het feit dat naamgeving zowel in het Duits als het Engels is, draagt bij aan een lagere onderhoudbaarheid van de broncode.

Missende documentatie en moeilijk te begrijpen naamgeving hebben een negatieve impact op de mogelijkheid om gericht aanpassingen te doen.

Ondanks het feit dat er verbetermogelijkheden zijn in zowel de structuur als de mogelijkheid tot het maken van modulaire aanpassingen, wordt de applicatie beoordeeld als voldoende gestructureerd en aanpasbaar.

Aanbevelingen

- Zorg voor goede documentatie, zowel binnen als buiten de applicatie. Dit vergroot de onderhoudbaarheid van de applicatie; het is dan eenvoudiger voor ontwikkelaars om aanpassingen te doen.
- Zorg voor consistente naamgeving, ook in de gebruikte taal. Java is een Engelstalige programmeertaal, het advies is daarbij aan te sluiten.

Conclusie

Eis	Resultaat	Conclusie
Modulaire broncode (B) De programmatuur, waaronder de broncode, is gestructureerd opgebouwd, zodanig dat modulaire aanpassingen mogelijk zijn	Geen bevindingen	Voldaan

C. Scheiding kritische functies voor verkiezingen

Introductie

Kritische functies voor de berekening van de uitslag van de verkiezingen en de zetelverdeling dienen in de programmatuur herkenbaar en van elkaar gescheiden te zijn. De mate waarin deze herkenbaar en van elkaar gescheiden zijn is beoordeeld door te kijken naar de mate van scheiding in de broncode zelf, op het niveau van folder- en bestandsstructuur. Daarnaast is ook gekeken naar de interactie tussen de functies door middel van een analyse van de dependency matrix.

Bevindingen

In de toelichting bij artikel P 1 van de Kiesregeling, gepubliceerd in de *Staatscourant* (29577, 2014), worden de kritische functies als volgt omschreven "*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".*

Deze functies zijn ondergebracht in verschillende Java-packages en daarmee van elkaar gescheiden. De specifiekere logica is vervolgens binnen de packages weer van elkaar gescheiden in verschillende bestanden ('classes').

In de dependency matrix (bijlage III) valt te zien dat er tussen de kritische functies voor het invoeren van de stemaantallen en de functies voor het vaststellen van de uitslag zeer weinig afhankelijkheid is. Binnen deze functies zelf, bijvoorbeeld tussen de vaststelling van de uitslag en het verdelen van de zetels, bestaat een grotere afhankelijkheid. Omdat de hiervoor benodigde functionaliteiten vanuit logisch oogpunt sterk van elkaar afhankelijk zijn, ligt het in de lijn der verwachting dat er meer interactie is tussen deze aspecten. De directe afhankelijkheden zijn daarnaast dusdanig klein dat ze niet als belemmerend worden aangemerkt. Een architectuuromschrijving van de applicatie ontbreekt, waardoor deze analyse niet getoetst kan worden tegen een gedocumenteerde applicatieomschrijving.

Over het algemeen zijn de kritische functies herkenbaar vanuit de naamgeving. Hierbij moet wel als kanttekening worden geplaatst dat de object- en functienamen soms in het Engels en soms in het Duits zijn, wat het zoeken naar specifieke functies lastig maakt en de leesbaarheid niet bevordert. In sommige gevallen komt de verklarende naamsaanduiding pas een aantal niveaus diep.

Aanbevelingen

- Zorg voor consistent gebruik van Duits of Engels (of Nederlands) bij de naamgeving van packages, objecten, methodes en variabelen om verwarring te voorkomen en zorg ervoor dat aan de packagenaam zelf herkenbaar is waar dit deel van de broncode voor wordt gebruikt.
- Zorg voor heldere (architectuur)documentatie zodat de structuur van de software ook begrijpelijk is zonder de code te moeten analyseren.

Conclusie

Eis	Resultaat	Conclusie
Scheiding kritische functies voor verkiezingen (C) De kritische functies voor de berekening van de uitslag van de verkiezingen en de zetelverdeling zijn in de programmatuur herkenbaar en van elkaar gescheiden	Geen bevindingen	Voldaan

D. Verschillende soorten verkiezingen

Introductie

De software OSV2020-U kan ingezet worden voor verschillende soorten verkiezingen (bijv. voor verkiezingen voor de Tweede Kamer, maar ook voor verkiezingen voor de gemeenteraad), maar is voor elke verkiezing wel anders ingericht. Voor deze vereiste is gekeken of de applicatie voor verschillende verkiezingen te gebruiken is, zonder dat daarvoor code-aanpassingen nodig zijn. Hierbij worden aanpassingen in configuratiebestanden niet beschouwd als zijnde code-aanpassingen.

Bevindingen

Het verkiezingstype is aan te passen door de vapp.properties (een platte-tekstbestand) te wijzigen; de stemgebiedstructuur, partijnamen en woonplaatsen zijn door de beheerder aan te passen middels het bestand vapp-metadata.zip.

Tijdens het eerste gebruik van een nieuwe OSV2020-U-installatie wordt gevraagd om de verkiezingsdefinitie in te lezen met daarin de basisgegevens van de verkiezing. Om de verkiezing verder in te richten, moeten de kandidatenlijsten, en eventueel de stembureaus, ingelezen worden.

Hiermee wordt voldaan aan de vereiste dat er geen codewijzigingen in de programmatuur nodig zijn om de applicatie te gebruiken voor verschillende soorten verkiezingen. Het wijzigen naar een ander verkiezingstype is getest.

Conclusie

Eis	Resultaat	Conclusie
Verschillende soorten verkiezingen (D) De programmatuur is, zonder dat hiervoor aanpassingen nodig zijn, te gebruiken voor verschillende soorten verkiezingen	Geen bevindingen	Voldaan

E. Preventie van toevallig of opzettelijk misbruik

Introductie

Het toevallig of opzettelijk foutief gebruik van de programmatuur moet, voor zover dit redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen worden. De OSV2020-U-applicatie wordt gebruikt om de verkiezingsuitslag te bepalen. Het is daarom van cruciaal belang dat de gegevens die ingevoerd en gebruikt worden om de uitslag te bepalen, correct en zonder fouten zijn. Voor dit onderzoek is gekeken naar de verschillende punten in de applicatie waarop belangrijke gegevens uitgewisseld worden of uitgewisseld kunnen worden.

Bevindingen

Toevallig of opzettelijk foutief gebruik van de programmatuur wordt tot op zekere hoogte voorkomen. Er is echter geen ontwerp of bijvoorbeeld een Security-by-Design-document aanwezig waarin alle eisen en maatregelen zijn beschreven.

In de applicatie zijn controles opgenomen om te voorkomen dat de applicatie met het internet verbonden is. Hierdoor wordt voorkomen dat kwaadwillenden van buiten het netwerk aanpassingen aan de applicaties kunnen aanbrengen, of gegevens uit de applicatie kunnen stelen of wijzigen. De gebruikte methode om een internetverbinding te voorkomen is voor iemand met kennis van de broncode wel eenvoudig te omzeilen.

Ook wordt de verbinding tussen de server en de clients beveiligd via een beveiligde verbinding ter voorkoming van misbruik door kwaadwillenden. Dit geldt ook voor de verbinding met de browser waar eigen certificaten worden gebruikt om de authenticiteit van de applicatie aan te geven. Vanuit de installatiehandleiding wordt de gebruiker geïnstrueerd om dit eigen certificaat als ‘vertrouwd’ op te nemen in de browser.

Er zijn verschillende maatregelen geïmplementeerd om de authenticiteit van bestanden te verifiëren. Deze variëren van een controle van de hash (een unieke code per bestand) tot meervoudige authenticiteitscontroles. Deze maatregelen zijn veelal verplichte controles tijdens het gebruik van de software.

Op gebruikersniveau is gezorgd voor een scheiding in rollen en bijbehorende rechten, zodat gebruikers alleen geautoriseerd zijn voor de acties die bij hun rol passen. Voor sommige acties wordt een vierogenprincipe afgedwongen door de applicatie.

Daarnaast worden de handelingen van gebruikers en beheerders vastgelegd in een logbestand.

Misbruik van gebruikersaccounts door derden wordt zo veel mogelijk voorkomen door een minimale wachtwoordsterkte, een maximaal aantal inlogpogingen en het feit dat gebruikers automatisch worden uitgelogd na 15 minuten zonder activiteit. Wachtwoorden van gebruikers moeten aan minimale vereisten voldoen en worden aanvankelijk door de beheerder geleverd. Gebruikers zijn verplicht na de eerste inlog hun wachtwoord te wijzigen. In het geval van een blokkade van een gebruikersaccount kan alleen de beheerder deze vrijgeven.

Bovenstaande maatregelen zijn in bijna alle gevallen afhankelijk van de mate waarin beheerders en gebruikers protocollen en veiligheidsvoorschriften naleven. Deze zijn niet getoetst in het kader van dit onderzoek.

Aanbevelingen

- De controle of de applicatie verbonden is met een netwerk kan omzeild worden door toegang tot de specifieke adressen waarop gecontroleerd wordt te beperken. Een andere methode past mogelijk beter, al blijft deze maatregel lastig te implementeren bij software die draait op systemen die niet volledig onder controle van de Kiesraad staan.
- Het is aanbevolen om tweefactorauthenticatie toe te passen op gebruikersaccounts, bijvoorbeeld door de ‘TOTP’-standaard toe te passen.
- Het opstellen van een Security-by-Design-document zorgt voor meer en beter inzicht in de beveiligingsrisico’s en bevordert actieve reflectie op nieuwe ontwikkelingen en risico’s.
- Maak zo mogelijk gebruik van publiekelijk controleerbare certificaten voor de communicatie tussen server en clients.

Conclusie

Eis	Resultaat	Conclusie
Preventie van toevallig of opzettelijk misbruik (E) Toevallig of opzettelijk foutief gebruik van de programmatuur wordt, voor zover redelijkerwijs technisch mogelijk is, door het ontwerp voorkomen	Geen significante bevindingen	Voldaan

F. Diakritische tekens en speciale karakters

Introductie

Om te bepalen of de programmatuur de Teletex-tekenset (van het Logisch Ontwerp GBA 3.14) ondersteunt voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten, zijn er functionele testen uitgevoerd.

Testaanpak

Om de tekenset te testen zijn specifieke testgevallen gecreëerd met verschillende partijen en kandidaten, waarbij verschillende diakritische tekens in de naamgeving voorkomen. Zie bijlage II voor een overzicht van de tekenset. Elk teken in deze tekenset is gebruikt in de naam van verschillende kandidaten en/of politieke groeperingen. Vervolgens is dit configuratiebestand in de software geïmporteerd en de weergave van de tekens handmatig gevalideerd. Deze toets is uitgevoerd op een Windows-besturingssysteem.

Bevindingen

Tijdens het testen zijn er geen afwijkingen geconstateerd. De Teletex-tekenset wordt ondersteund voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten.

Conclusie

Eis	Resultaat	Conclusie
Diakritische tekens en speciale karakters (F) 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	Geen bevindingen	Voldaan

G. Open source en open standaarden

Introductie

De vereiste dat de programmatuur als open source ontwikkeld dient te worden en gebruik dient te maken van open standaarden past in het actieplan Open Overheid. Voor de beoordeling 'open source' wordt gebruikgemaakt van de definitie zoals gevonden op rijksoverheid.nl, namelijk 'Open source betekent dat de broncode van bijvoorbeeld een website, programma of app, vrij beschikbaar is. Iedereen kan de broncode lezen, aanpassen en verspreiden.' Daarnaast is de industrie-standaarddefinitie van open source, zoals vastgelegd in en onderhouden door het Open Source Initiative, toegepast.

Bevindingen

De enige standaard waar de programmatuur gebruik van maakt is de open Election Markup Language (EML)-standaard. Binnen de applicatie wordt de variant EML_NL voor specifiek Nederlandse verkiezingen gebruikt; dit betreft een open standaard. Deze standaard wordt gebruikt om informatie te importeren en te exporteren.

De broncode van de softwareapplicatie wordt openlijk gepubliceerd op de website van de Kiesraad. In het bijbehorende licentiebestand wordt aangegeven dat de Creative Commons Zero (CC0)-verklaring niet van toepassing is op de broncode van OSV2020-U. In de voorgaande versies van OSV2020-U is een licentiebestand bijgevoegd met de volgende tekst: "*De gebruiker van de broncode mag deze bestuderen en analyseren, het distribueren van de broncode of de daarvan afgeleide werken aan derden is niet toegestaan."* Dit is echter niet in lijn met de opensourcedefinitie zoals bijgehouden door het Open Source Initiative, dat een globaal erkende definitie van 'open source' bijhoudt waarin specifiek aangegeven wordt dat de software onder andere vrijelijk verder gedistribueerd moet kunnen worden om als open source te kunnen worden beschouwd. Er wordt derhalve niet voldaan aan de richtlijnen.

De auteursrechten van het platformgedeelte van OSV2020-U liggen bij Leverancier, en niet bij de Kiesraad; dit gedeelte is niet open source.

Verder valt op dat een aantal externe bibliotheken die Leverancier gebruikt niet open source zijn, maar slechts onder specifieke licentievoorwaarden gebruikt kunnen worden.

Vanuit de Kiesraad wordt verwezen naar de nadere toelichting op de Kiesregeling: "*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."* De krappe tijdslijnen zorgen er in dit geval voor dat het niet mogelijk lijkt om een opensource-applicatie in te zetten voor de komende Tweede Kamerverkiezingen. Gezien de historie met de OSV-applicatie – deze is al vele jaren gebruikt bij Nederlandse verkiezingen – is de doeltreffendheid van deze oplossing aangetoond waarop het besluit is gevolgd om de OSV-applicatie wederom in te zetten.

Voor wat betreft de mogelijkheid om in de praktijk aangetoonde technologie in te zetten, valt te betwijfelen of het inderdaad niet mogelijk was om de software als open source te ontwikkelen. Daar OSV2020-U en eerdere versies al sinds 2009 worden ingezet, is er voldoende tijd geweest om een opensource-alternatief te ontwikkelen. De conclusie is dan ook dat de applicatie zelf niet als open source is ontwikkeld. Daar dit bekend is bij de Kiesraad, zijn er stappen genomen om een nieuwe, opensource-applicatie te ontwikkelen. Dit project is echter recentelijk stilgelegd.

Verder moet dergelijke technologie direct toepasbaar zijn. Doordat er voor het Elect-platform Kiesraad-specifiek maatwerk is opgeleverd, blijkt dit echter niet het geval te zijn.

Aanbevelingen

- Heroverweeg het ontwikkelen van een nieuwe (opensource)-applicatie ter ondersteuning van de berekening van de uitslag van de verkiezingen en de berekening van de zetelverdeling

Conclusie

Eis	Resultaat	Conclusie
Open source en open standaarden (G) 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	Significante bevindingen	Niet voldaan

H. Standaardprogrammatuur is vrij verkrijgbaar

Introductie

Standaardprogrammatuur, of standaardsoftware, zal in deze analyse worden gedefinieerd als ‘software die voor de markt is ontwikkeld in tegenstelling tot maatwerksoftware die op aanvraag op maat wordt gemaakt’.

Bevindingen

De programmatuur is een opzichzelfstaand geheel waarvoor verder geen randprogrammatuur vereist is, standaard of niet standaard. Binnen de applicatie wordt gebruikgemaakt van de formaten zip en pdf die software vereisen om te gebruiken. Hiervoor zijn echter meerdere vrij verkrijgbare standaardprogramma’s beschikbaar; vaak zijn deze zelfs meegeleverd met een besturingssysteem.

De programmatuur in de maatwerkbroncode is vrij verkrijgbaar en maakt geen gebruik van niet-standaard software anders dan het Elect-platform. Dit Elect-platform is echter een betaald product en derhalve niet vrij verkrijgbaar. Slechts een deel van de totale applicatie wordt hierdoor op de website van de Kiesraad gepubliceerd in de vorm van broncode.

De bedoeling van dit wettelijk kader, zoals beschreven in de aanvullende verklaring (*Staatscourant* 29577, 2014), dat *“een ieder die dat wil zelf een testopstelling [kan] maken en nagaan of het geheel onder alle omstandigheden goed functioneert”*, wordt – in tegenstelling tot het voorgaande onderzoek – in dit geval vervuld door het vanuit de Kiesraad (op aanvraag) beschikbaar stellen van de installatieprogrammatuur waarmee gebruikers een eigen testopstelling kunnen maken.

Conclusie

Eis	Resultaat	Conclusie
Standaardprogrammatuur is vrij verkrijgbaar (H) De standaardprogrammatuur waarvan gebruik wordt gemaakt is vrij verkrijgbaar	Geen bevindingen	Voldaan

I. Intellectueel eigendom

Introductie

Voor het beantwoorden van de vraag of het intellectueel eigendom berust bij een centraal stembureau, in dit geval de Kiesraad, is gekeken naar gemaakte overeenkomsten tussen de Kiesraad en zijn Leverancier. Daarnaast is ook naar licentieverwijzingen in de broncode gezocht.

Bevindingen

Vanuit de overeenkomst geldt dat de Kiesraad alleen het intellectueel eigendom bezit over het maatwerk (programma 4 en 5). Dit maatwerk bevindt zich in de NL-packages binnen de broncode, deze code wordt bij de leverancier in een separate opzichzelfstaande repository ontwikkeld en beheerd. Opvallend is dat er in de code binnen deze NL-packages op een aantal plekken expliciete copyright statements te vinden zijn, waarin aangegeven wordt dat het copyright toekomt aan Leverancier. Dit zou kunnen betekenen dat deze statements in conflict zijn met de eerdergenoemde overeenkomst. Hier wordt het copyright van de Kiesraad verwacht.

Vanuit de overeenkomst geldt dat voor het grootste deel van OSV2020-U, namelijk voor het Elect-platform, het intellectueel eigendom bij Leverancier ligt. De maatwerksoftware voor onderdelen 4 en 5 maakt echter volledig gebruik van dit platform. Het is dus niet mogelijk om die broncode elders in te zetten zonder dat het volledige platform toegankelijk is. De Kiesraad heeft wel een onherroepelijk recht om gebruik te maken van het Elect-platform.

Aanbevelingen

- Zorg ervoor dat de correcte licentie wordt opgenomen in de broncode. Dit kan bijvoorbeeld in de header of door een licentiebestand mee te leveren.

Conclusie

Eis	Resultaat	Conclusie
Intellectueel eigendom (I) Het intellectueel eigendom van de maatwerkprogrammatuur berust bij een centraal stembureau	Geen bevindingen	Voldaan

Overeenkomst

In de initiële overeenkomst tussen de Kiesraad en Leverancier is een onderscheid gemaakt in een vijftal te ontwikkelen applicaties:

- programma 1: kandidaatstelling politieke partijen;
- programma 2: onderzoek kandidatenlijsten;
- programma 3: vaststellen kandidatenlijsten;
- programma 4: samenvoegen stemtotalen;
- programma 5: zetelverdeling en vaststellen uitslag.

Hierbij is voor programma's 4 en 5, waar de OSV2020-U onder valt, het volgende overeengekomen:

- 7.3 De Intellectuele Eigendomsrechten met betrekking tot de deelprogramma's 4 en 5 van de Programmatuur (met uitzondering van de Nederlandse lokalisaties) (blijven) berusten bij Opdrachtnemer of diens licentiegevers. Opdrachtnemer verleent Opdrachtgever een niet-exclusieve, doorlopende, onherroepelijke licentie (met recht tot sublicentiëring) om de deelprogramma's 4 en 5 van de Programmatuur te gebruiken voor enig doel betrekking hebbend op de activiteiten van Opdrachtgever

Bij de vernieuwing van de OSV-applicatie verwijst het contract naar de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2014 (ARBIT-2014) waar in artikel 8 het volgende is vastgelegd:

- 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.
  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.

J. Opensourceprogrammeertaal

Introductie

De programmatuur dient te zijn geschreven in een programmeertaal waarvoor een actief onderhouden ‘open source compiler’ beschikbaar is. Om dit te onderzoeken is een handmatige analyse van de broncode en documentatie uitgevoerd.

Bevindingen

De applicatie is geschreven in Java. De meest recente compiler die kan worden gebruikt om de applicatie te bouwen is Java versie 11 (Java 11). Hoewel Java 11 een Long Term Support (LTS)-versie is van Java, verloopt 30 september 2023 het actieve onderhoud op deze versie. Wel wordt er nog tot 30 september 2026 security-ondersteuning aangeboden voor Java 11. De thans courante LTS-versie voor Java is versie 17; aangeraden wordt dan ook om de applicatie te upgraden naar deze versie van Java.

Java geldt als een van de populairste programmeertalen voor de realisatie van opensourcecomponenten en wordt nog actief onderhouden. Verschillende leveranciers leveren een versie 17 compiler; er is met OpenJDK ook een opensourcevariant.

Aanbevelingen

- Werk de afhankelijkheid van Java 11 weg en zorg ervoor dat het systeem werkt met een courante Java-versie.

Eis	Resultaat	Conclusie
Opensourceprogrammeertaal (J) De programmatuur is geschreven in een programmeertaal waarvoor een door een actieve gemeenschap onderhouden open source *compiler*, onderscheidenlijk i*nterpreter* beschikbaar is	Geen significante bevindingen	Voldaan

K. Besturingssystemen

Introductie

De applicatie dient te functioneren op ten minste twee verschillende besturingssystemen, waaronder in ieder geval een opensourcebesturingssysteem. Deze vereiste is gevalideerd middels verscheidene functionele testen.

Testaanpak

Om te valideren dat de applicatie werkt op meerdere besturingssystemen inclusief een opensourcebesturingssysteem, is de applicatie geïnstalleerd op zowel een Ubuntu (Linux - versie 22.04 LTS)- en Windows 10 (versie Pro 20H2)-besturingssysteem. Naast het opstarten van de applicatie zijn enkele testscenario's (TK1, TK2, TK6 en TK12) uit onderzoeksvraag 1 uitgevoerd om te valideren dat de applicatie goed functioneert.

Bevindingen

De gebruikte technologie – Java – werkt in principe onafhankelijk van het besturingssysteem. De gebruikte externe bibliotheken zijn ook niet afhankelijk van een specifiek besturingssysteem of een versie daarvan.

Het installeren, opstarten en testen van de software leidde niet tot functionele bevindingen; de applicatie werkt op zowel het Windows- als het Linux-besturingssysteem zonder dat aanpassingen of additionele software noodzakelijk waren.

Conclusie

Eis	Resultaat	Conclusie
Besturingssystemen (K) De programmatuur wordt ontwikkeld voor verschillende besturingssystemen, waaronder in ieder geval een open source besturingssysteem	Geen bevindingen	Voldaan

L. Vaststellen van de authenticiteit van de programmatuur

Introductie

Het moet mogelijk zijn om de authenticiteit van OSV2020-U te kunnen bepalen zodat kan worden voorkomen dat er gebruikgemaakt wordt van een aangepaste versie. Om deze vraag te onderzoeken is er gebruikgemaakt van de bijgeleverde handleiding en zijn de beschreven controlemethodes uitgevoerd. Hier werd de verificatie-hash bijgeleverd in plaats van dat deze gepubliceerd werd op de website van de Kiesraad.

Bevindingen

Het is mogelijk om de authenticiteit van de programmatuur vast te stellen. De applicatie wordt bij de gebruiker geleverd als een zip-bestand, waar de installatiebestanden in verpakt zitten. De gebruiker wordt geïnstrueerd om over dit zip-bestand een hash-waarde te berekenen. Op de website van de Kiesraad wordt een hash-waarde gedeeld die overeen moet komen met de berekende hash-waarde. Een verschil tussen deze waardes geeft aan dat de gebruiker niet de originele applicatie heeft. Het is dus mogelijk om te controleren of de aangeleverde applicatie dezelfde is als die welke door de Kiesraad is gedeeld. Hierbij moet wel vermeld worden dat deze controle niet afgedwongen wordt en makkelijk door de gebruiker (per ongeluk) overgeslagen kan worden.

Er is geen mogelijkheid aanwezig om de authenticiteit van een reeds geïnstalleerde applicatie te bepalen. Wel is het mogelijk om het gecontroleerde zip-bestand op een andere computer te installeren en de twee geïnstalleerde programma's te vergelijken. Dit is echter een zeer intensieve en omslachtige methode.

Op dit moment is het ook niet mogelijk om te bepalen of de gedeelde broncode gelijk is aan die van de programmatuur in het meegeleverde zip-bestand. Er is geen methode of applicatie gedeeld waarmee vanuit de broncode een installeerbare applicatie gemaakt kan worden.

Aanbevelingen

- Zorg ervoor dat ook de geïnstalleerde applicatie gecontroleerd kan worden, zodat tussentijds de authenticiteit van de programmatuur vastgesteld kan worden, bijvoorbeeld door de hash-waarde van verschillende JAR-bestanden (en hoe deze wordt berekend) te publiceren.
- Maak inzichtelijk hoe geverifieerd kan worden dat de gepubliceerde broncode past bij de installatiebestanden én de geïnstalleerde applicatie.

Conclusie

Eis	Resultaat	Conclusie
Vaststellen van de authenticiteit van de programmatuur (L) Het is mogelijk de authenticiteit van de programmatuur vast te stellen	Geen significante bevindingen	Voldaan

M. Vaststellen van de authenticiteit van de gegevens

Introductie

Bij het inlezen van verkiezingsgegevens in de programmatuur dient de authenticiteit van de gegevens bij voorkeur door middel van een gekwalificeerde elektronische handtekening vastgesteld te worden. Het is belangrijk om de authenticiteit van de verscheidene bestanden met verkiezingsgegevens vast te stellen, omdat ongeoorloofde aanpassingen aan deze bestanden verstrekkende gevolgen kunnen hebben voor de verkiezingsuitslag. Voor deze analyse is gekeken naar de beveiliging zoals gedocumenteerd in de bijgeleverde handleidingen; waar mogelijk is deze ook gecontroleerd.

Bevindingen

De applicatie controleert de authenticiteit van de bestanden met verkiezingsgegevens door middel van een aantal verschillende methodes. Deze vallen grofweg in drie categorieën:

1. Er wordt een hash-waarde berekend over een gegenereerd bestand. De gebruiker wordt bij het invoeren van een dergelijk bestand gevraagd om de ontbrekende acht karakters van de hash-waarde aan te vullen om zo de authenticiteit vast te stellen.
2. Er wordt een hash-waarde berekend over een gegenereerd bestand en de gebruiker wordt, op eenzelfde manier als hierboven beschreven, gevraagd om deze aan te vullen. Hiernaast is het bestand ook beveiligd met een elektronische handtekening.
3. Er wordt een hash-waarde berekend over een gegenereerd bestand, waarbij de gebruiker wordt gevraagd deze in zijn geheel te controleren.

Niet aangetroffen is een beschrijving van waarom sommige bestanden zwaarder beveiligd moeten worden dan andere. Vermoedelijk heeft dit te maken met de gevoeligheid van de informatie. Zo zijn er ook bestanden met verkiezingsgegevens die geen controle op authenticiteit hebben; in deze gevallen gaat het om informatie die ook handmatig in de applicatie ingevoerd kan worden of die via een vierogenprincipe gecontroleerd wordt.

Aanbevelingen

- Neem in een Security-by-Design-document op welk niveau van beveiliging voor de diverse bestanden met verkiezingsgegevens noodzakelijk is.

Conclusie

Eis	Resultaat	Conclusie
Vaststellen van de authenticiteit van de gegevens (M) Bij het inlezen van verkiezingsgegevens in de programmatuur wordt de authenticiteit van de gegevens vastgesteld, bij voorkeur door middel van een gekwalificeerde elektronische handtekening	Geen significante bevindingen	Voldaan

4.
Appendices

I - Functionele testgevallen en testdekking

Functionele testgevallen en testdekking

Resultaten

In de onderstaande tabel staan de resultaten van het testen van de verkiezingen voor de Tweede Kamer. De functionele testdekking is in overeenstemming met het zetelverdelingsdocument [1].

Tweede Kamer														
		TK1	TK2	TK3	TK4	TK5	TK6	TK7	TK8	TK9	TK10	TK11	TK12	TK13
A	**Zetelverdeling**													
1	Vaststelling stemtotalen	v	v	v	v	v	v	v	v	v	v	v	v	v
2	Directe toedeling van restzetels	v	v	v	v	v	v	v	v	v	v	v	v	v
3	Toedeling van restzetels		v	v	v	v	v	v	v	v				v
4	Wijziging bij volsterkte meerderheid						v							
5	Wijziging bij uitputting lijsten									v		v		
6	Verdeling binnen lijstengroepen										v	v	v	v
B	**Aanwijzing van de gekozen kandidaten**													
1	Aanwijzing met voorkeurstemmen											v	v	v
2	Aanwijzing overige kandidaten											v	v	v
3	Rangschikking kandidaten											v	v	v
Resultaat		v	v	v	v	v	v	v	v	v	v	v	v	v

[1]: Formele beschrijving van de berekening van de zetelverdeling, 05-02-2018,zie:
https://www.kiesraad.nl/verkiezingen/adviezen-en-publicaties/formulieren/2016/osv/osv-bestanden/formele-beschrijving-berekening-zetelverdeling

II - Tekenset basisregistratie personen

Teletex-karakteroverzicht (1/7)

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
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

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
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
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

Teletex-karakteroverzicht (2/7)

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
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
67	67	g	Small g

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
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

Teletex-karakteroverzicht (3/7)

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
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
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

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
E0	E2 84 A6	Ω	Ohm sign
E1	C3 86	Æ	Capital AE diphtong
E2	C4 90	Đ	Capital D with stroke
E3	C2 AA	ª	Ordinal indicator, feminine
E4	C4 A6	Ħ	Capital H with stroke
E7	C4 BF	Ŀ	Capital L with middle dot
E8	C5 81	Ł	Capital L with stroke
E9	C3 98	Ø	Capital O with slash
EA	C5 92	OE	Capital OE ligature
EB	C2 BA	º	Ordinal indicator, masculine
EC	C3 9E	Þ	Capital thorn, Icelandic
ED	C5 A6	Ŧ	Capital T with stroke
EE	C5 8A	Ŋ	Capital eng, Lapp
EF	C5 89	ŉ	Small n with apostrophe
F0	C4 B8	ĸ	Small k, Greenlandic
F1	C3 A6	æ	Small ae, diphtong
F2	C4 91	đ	Small d with stroke
F3	C3 B0	ð	Small eth, Icelandic
F4	C4 A7	ħ	Small h with stroke
F5	C4 B1	ı	Small i without dot
F7	C5 80	ŀ	Small l with middle dot
F8	C5 82	ł	Small l with stroke
F9	C3 B8	ø	Small o with slash

Teletex-karakteroverzicht (4/7)

Overzicht van de in GBA te gebruiken Teletex-karakters			
T.61 code	**UTF-8 code**	**Char**	**Omschrijving/Naam**
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	ŧ	Small t with stroke
FE	C5 8B	ŋ	Small eng, Lapp

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

Teletex-karakteroverzicht (5/7)

Overzicht van de in GBA te gebruiken gecombineerde Teletex-karakters						
T.61 code	**UTF-8 code**	**Char**	**T.61 code**	**UTF-8 code**	**Char**	**Omschrijving/Naam**
			C2 67	C4 A3	ģ	G cedilla (vroeger G acute)
C3 47	C4 9C	Ĝ	C3 67	C4 9D	ĝ	G circumflex
C6 47	C4 9E	Ğ	C6 67	C4 9F	ğ	G breve
C7 47	C4 A0	Ġ	C7 67	C4 A1	ġ	G dot
CB 47	C4 A2	Ģ				G cedilla
C3 48	C4 A4	Ĥ	C3 68	C4 A5	ĥ	H circumflex
C1 49	C3 8C	Ì	C1 69	C3 AC	ì	I grave
C2 49	C3 8D	Í	C2 69	C3 AD	í	I acute
C3 49	C3 8E	Î	C3 69	C3 AE	î	I circumflex
C4 49	C4 A8	Ĩ	C4 69	C4 A9	ĩ	I tilde
C5 49	C4 AA	Ī	C5 69	C4 AB	ī	I macron
C7 49	C4 B0	İ				I dot
C8 49	C3 8F	Ï	C8 69	C3 AF	ï	I diaeresis
CE 49	C4 AE	Į	CE 69	C4 AF	į	I ogonek
C3 4A	C4 B4	Ĵ	C3 6A	C4 B5	ĵ	J circumflex
CB 4B	C4 B6	Ķ	CB 6B	C4 B7	ķ	K cedilla
C2 4C	C4 B9	Ĺ	C2 6C	C4 BA	ĺ	L acute
CB 4C	C4 BB	Ļ	CB 6C	C4 BC	ļ	L cedilla
CF 4C	C4 BD	Ľ	CF 6C	C4 BE	ľ	L caron
C2 4E	C5 83	Ń	C2 6E	C5 84	ń	N acute
C4 4E	C3 91	Ñ	C4 6E	C3 B1	ñ	N tilde
CB 4E	C5 85	Ņ	CB 6E	C5 86	ņ	N cedilla
CF 4E	C5 87	Ň	CF 6E	C5 88	ň	N caron

Teletex-karakteroverzicht (6/7)

Overzicht van de in GBA te gebruiken gecombineerde Teletex-karakters						
T.61 code	**UTF-8 code**	**Char**	**T.61 code**	**UTF-8 code**	**Char**	**Omschrijving/Naam**
C1 4F	C3 92	Ò	C1 6F	C3 B2	ò	O grave
C2 4F	C3 93	Ó	C2 6F	C3 B3	ó	O acute
C3 4F	C3 94	Ô	C3 6F	C3 B4	ô	O circumflex
C4 4F	C3 95	Õ	C4 6F	C3 B5	õ	O tilde
C5 4F	C5 8C	Ō	C5 6F	C5 8D	ō	O macron
C8 4F	C3 96	Ö	C8 6F	C3 B6	ö	O diaeresis
CD 4F	C5 90	Ő	CD 6F	C5 91	ő	O double acute
C2 52	C5 94	Ŕ	C2 72	C5 95	ŕ	R acute
CB 52	C5 96	Ŗ	CB 72	C5 97	ŗ	R cedilla
CF 52	C5 98	Ř	CF 72	C5 99	ř	R caron
C2 53	C5 9A	Ś	C2 73	C5 9B	ś	S acute
C3 53	C5 9C	Ŝ	C3 73	C5 9D	ŝ	S circumflex
CB 53	C5 9E	Ş	CB 73	C5 9F	ş	S cedilla
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

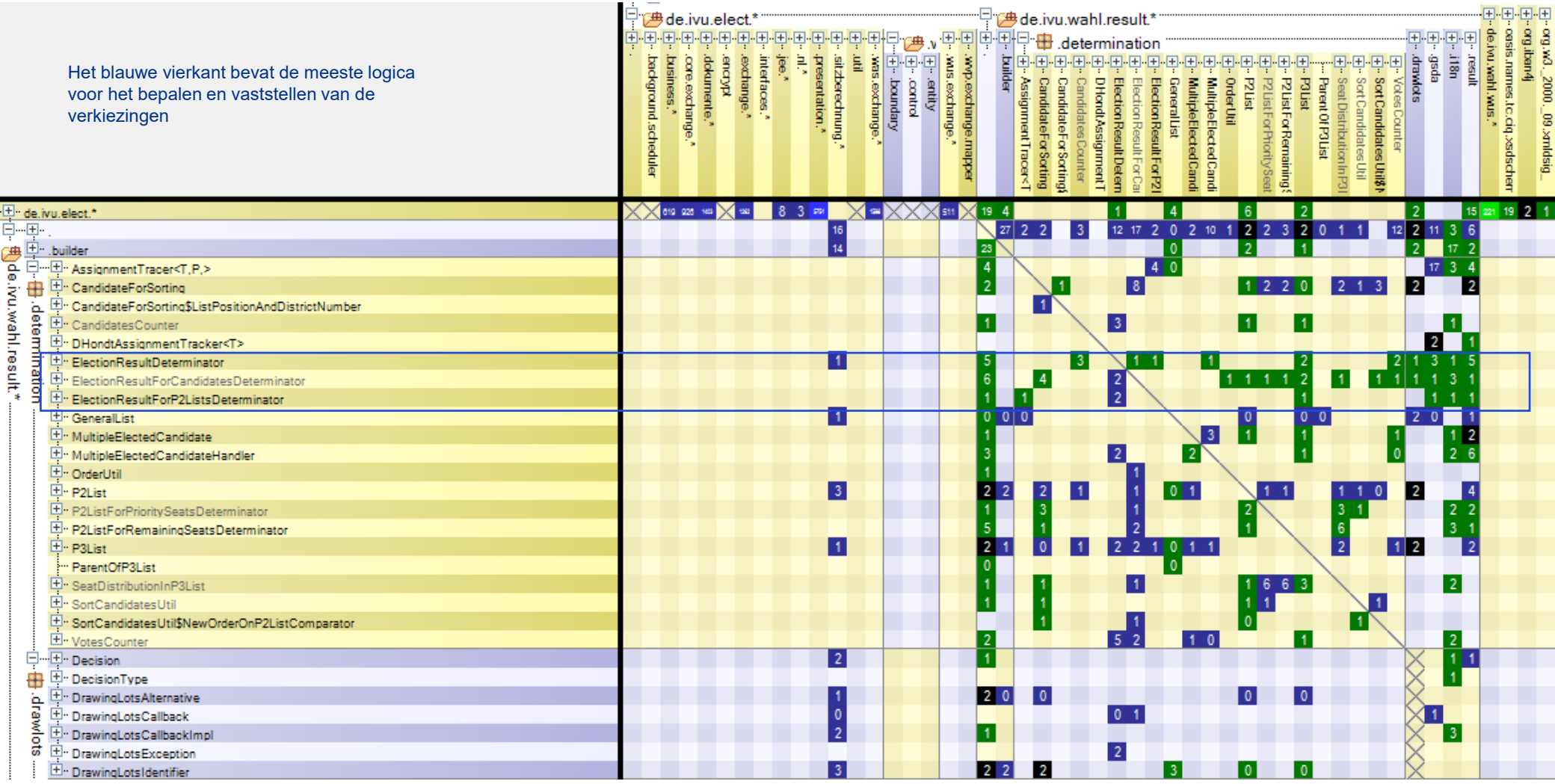
Teletex-karakteroverzicht (7/7)

Overzicht van de in GBA te gebruiken gecombineerde Teletex-karakters						
T.61 code	**UTF-8 code**	**Char**	**T.61 code**	**UTF-8 code**	**Char**	**Omschrijving/Naam**
CA 55	C5 AE	Ů	CA 75	C5 AF	ů	U ring
CD 55	C5 B0	Ű	CD 75	C5 B1	ű	U double acute
CE 55	C5 B2	Ų	CE 75	C5 B3	ų	U ogonek
C3 57	C5 B4	Ŵ	C3 77	C5 B5	ŵ	W circumflex
C2 59	C3 9D	Ý	C2 79	C3 BD	ý	Y acute
C3 59	C5 B6	Ŷ	C3 79	C5 B7	ŷ	Y circumflex
C8 59	C5 B8	Ÿ	C8 79	C3 BF	ÿ	Y diaeresis
C2 5A	C5 B9	Ź	C2 7A	C5 BA	ź	Z acute
C7 5A	C5 BB	Ż	C7 7A	C5 BC	ż	Z dot
CF 5A	C5 BD	Ž	CF 7A	C5 BE	ž	Z caron

III - Dependency matrix analyse

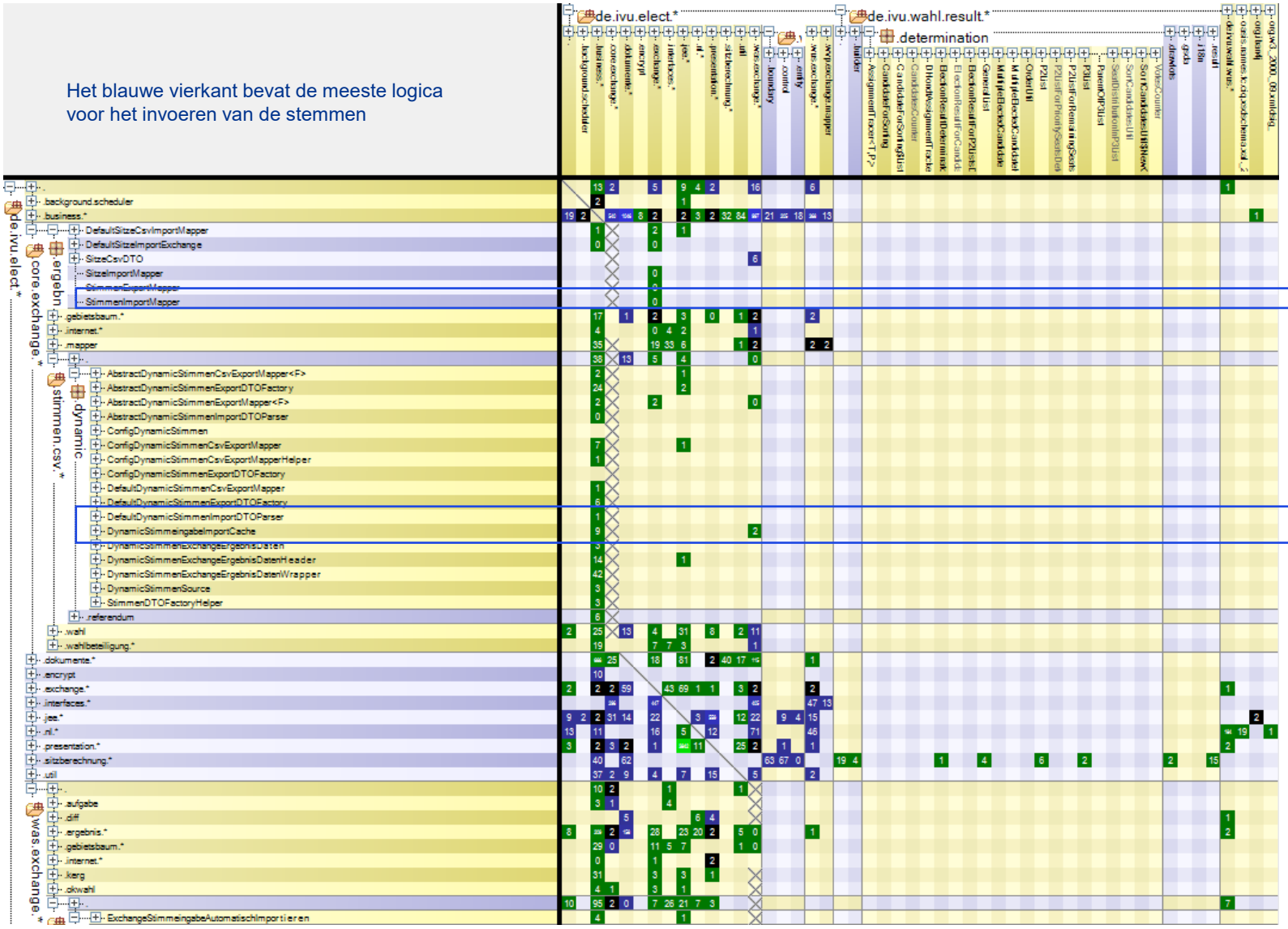
Wahl.Result map

Het blauwe vierkant bevat de meeste logica voor het bepalen en vaststellen van de verkiezingen



Stimmeingabe map

Het blauwe vierkant bevat de meeste logica voor het invoeren van de stemmen



IV - Gedeelde documenten

Gedeelde documenten

Bestandsnaam
Sonar-Report-for-OSV2020-U-1.9.0.pdf
2023-08-24_osv2020-u-installer-a10-tk-1.9.1_signed.zip
2023-08-24_osv2020-u-installer-a4-tk-1.9.1_signed.zip
2023-08-24_osv2020-u-installer-a9-tk-1.9.1_signed.zip
Nieuw tekstdocument.txt
ReleaseNotes-WAS-1.9.1.pdf
elect-model-db-h2-sql.zip
elect-model-db-mysql5-sql.zip
nl-rebuild-package.zip
nl-was-war-1.9.1-sources-all.zip
nl-was-war-1.9.1-sources-test.zip
nl-was-war-1.9.1-thirdparty.zip
20230824_TK (Map met testdata)
20231122_TK (Map met testdata)

Bestandsnaam
OSV2020-U-handleiding-AB-1.9.0.pdf
OSV2020-U-handleiding-BC-1.9.0.pdf
OSV2020-U-handleiding-EK-1.9.0.pdf
OSV2020-U-handleiding-EP-1.9.0.pdf
OSV2020-U-handleiding-GR-1.9.0.pdf
OSV2020-U-handleiding-PS-1.9.0.pdf
OSV2020-U-handleiding-TK-1.9.0.pdf
OSV2020-U-handleiding_installer-1.9.0.pdf
OSV2020-U-korte_handleiding-AB-1.9.0.pdf
OSV2020-U-korte_handleiding-BC-1.9.0.pdf
OSV2020-U-korte_handleiding-EK-1.9.0.pdf
OSV2020-U-korte_handleiding-EP-1.9.0.pdf
OSV2020-U-korte_handleiding-GR-1.9.0.pdf
OSV2020-U-korte_handleiding-PS-1.9.0.pdf
OSV2020-U-korte_handleiding-TK-1.9.0.pdf

Dit document is opgesteld voor de Kiesraad om inzicht te verschaffen in de uitkomsten van de toetsing van Ondersteunende Software Verkiezingen: Uitslagvaststelling(OSV2020-U). KPMG Advisory aanvaardt geen aansprakelijkheid voor gebruik van dit document voor enig ander doel en ten opzichte van andere partijen dan de Kiesraad.

kpmg.com/socialmedia