Bijlage E - DHV basisarchitectuur

Uitgangspunten en beveiligingsconcept voor het Digitaal Hulpmiddel Verkiezingen (DHV) voor het vaststellen van verkiezingsuitslag en zetelverdeling

Versie 1.11

Managementsamenvatting

Aanleiding en doelstelling (Waarom)

Het vertrouwen in de Nederlandse verkiezingen is groot. De basis hiervoor ligt in een integer, transparant en controleerbaar verkiezingsproces. Ter ondersteuning van het verkiezingsproces en de vaststelling van de uitslag en zetelverdeling wordt al decennialang programmatuur ingezet voor het begeleiden van het proces en het uitvoeren van de benodigde validaties en berekeningen.

Nieuwe concept (Wat)

Bij het DHV is uitgegaan van een centrale oplossing, waardoor er gestuurd kan worden op wijze van inrichten van het systeem en centraal gemonitord kan worden op onregelmatigheden.

Mitigeren van cybersecurity dreigingen

Onder begeleiding van de NCSC en de AIVD is ingegaan op de mogelijke dreigingen, risico's en mitigerende maatregen ten aanzien van de inzet van software bij verkiezing. Ten aanzien van de programmatuur voor de vaststelling van de uitslag heeft dit geleid tot het definiëren van een reeks uitgangspunten. Deze uitgangspunten zijn:

- Geen vertrouwen (Zero trust): geen systeem, netwerk of persoon kan op zichzelf als geheel vertrouwd worden aangemerkt;
- Controleerbaarheid: eenieder moet kunnen vaststellen dat het digitale hulpmiddel tot de juiste uitslag en zetelverdeling is gekomen;
- Gelaagde beveiliging: voor een risico wordt niet slechts één maatregel toegepast, maar een gelaagde set aan maatregelen;
- Minimaliseer aanvalsoppervlakte: het digitale hulpmiddel dient een zo klein mogelijk aanvalsoppervlakte te hebben;
- Standaard beveiligd (Secure by default): het DHV dient standaard zo veilig mogelijk ontwikkeld, gebouwd en geconfigureerd te zijn;
- Ketenveiligheid: Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij hebben genomen om de aan hun opgelegde eisen te voldoen en ook hoe ze deze opgelegd hebben aan hun toeleveranciers en hoe ze dat controleren;
- Detectie indringers (Intrusion detection): Implementeer detectiemiddelen zodat kwetsbaarheden en potentiële aanvallen gedurende de verkiezingen kunnen worden waargenomen door een Security Operations Center (SOC);
- Incident respons: Een uitgangspunt is dat de basisarchitectuur rekening houdt met het feit dat het systeem gecompromitteerd is of kan worden (Ga-uit-van-een-inbraak/Assume breach principe). In dit kader is het uitgangspunt dat er een incident respons protocol ontwikkeld wordt dat in gang kan worden gezet, indien er onverhoopt een incident plaatsvindt. Zodoende kan tijdig actie worden ondernomen en schade beperkt blijven;
- Forensische paraatheid (Forensic readiness): Zorg ervoor dat de juiste loggegevens vastgelegd worden en goed beschermd zijn, zodat bij een forensisch onderzoek het bewijs ook juridisch houdbaar is en gebruikt kan worden voor juridische of strafrechtelijke procedures.

Om bovenstaande uitgangspunten concreet te maken is een set van maatregelen voorgesteld. Deze set is zowel in de hoofdtekst als in de managementsamenvatting uitgebreid beschreven. De betreffende tekst is in de managementsamenvatting te vinden onder 'Verkorte weergave van de hoofdonderwerpen uit de basisarchitectuur'.

Transparante en controleerbare werking

Om te voorkomen dat de uitslaggegevens die het DHV genereert ongemerkt gemanipuleerd kunnen worden, zoals het concept proces-verbaal met de uitslag, wordt deze voorzien van een digitale handtekening of digitaal waarmerk. De digitale handtekening of waarmerk zorgt ervoor dat iedere ongewenste aanpassing aan de verkiezingsuitslag gedetecteerd kan worden. Door de uitslaggegevens die voortkomen uit het DHV in herbruikbare vorm en uniform beschikbaar te stellen aan burgers kunnen deze de gegenereerde gegevens controleren.

Ketenpartners en verantwoordelijkheid

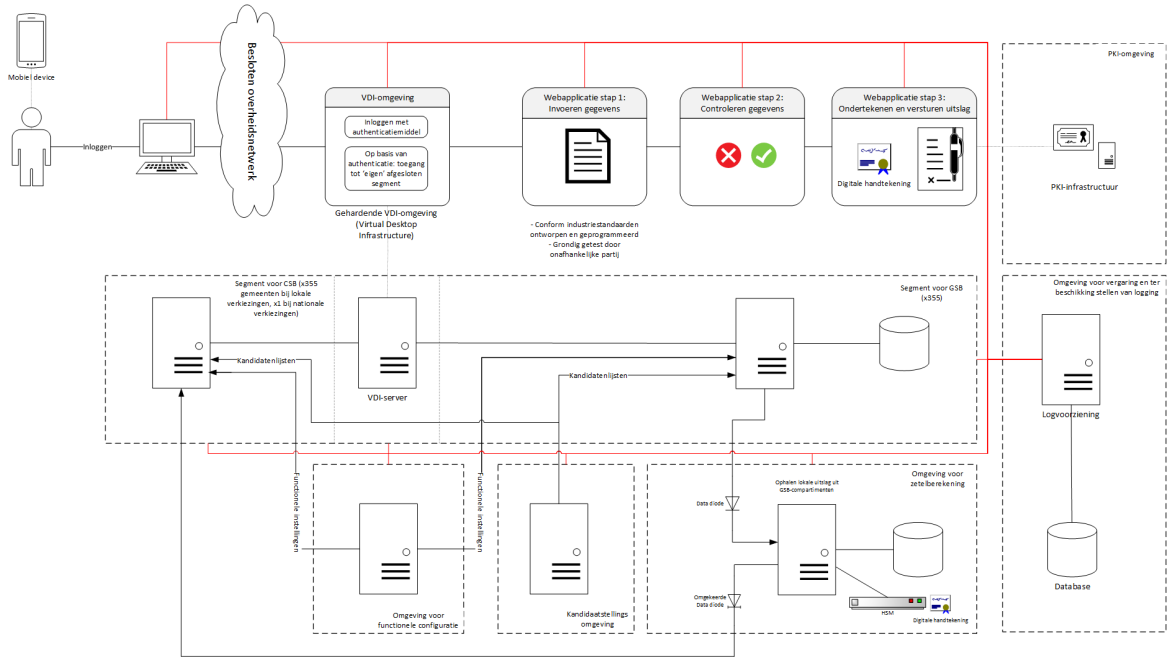
Bij de vaststelling van de uitslag zijn verschillende partijen betrokken. Deze partijen hebben elk een eigen verantwoordelijkheid binnen het proces. Het is mede daarom dat in nauwe samenwerking door Kiesraad, Ministerie van Binnenlandse Zaken, VNG, NVVB en IBD gewerkt is aan de voorliggende basisarchitectuur document voor het DHV. Deze samenwerking is belangrijk voor een breedgedragen en toekomstbestendige opzet van het DHV.

Verkorte weergave van de hoofdonderwerpen uit de basisarchitectuur

Basisarchitectuur

In figuur 1 is de basisarchitectuur op hoofdlijnen gevisualiseerd vanuit het perspectief van het proces voor de vaststelling van de uitslag.
Om het aanvalsoppervlak te verkleinen is het DHV uitsluitend beschikbaar voor werkstations van het GSB/CSB die zijn aangesloten op een besloten(semi)overheidsnetwerk. De gebruiker (GSB/CSB) dient dan ook allereerst in te loggen op een werkstation van het GSB/CSB.

Vervolgens wordt er een verbinding gemaakt met een (besloten) landelijk netwerk. Nadat er verbinding is gemaakt met het (besloten) landelijk netwerk, wordt er een sessie gestart in de Virtuele Desktop omgeving (VDI). Deze VDI-omgeving biedt de medewerkers van het GSB/CSB toegang tot een eigen afgescheiden compartiment. Vervolgens kan uitsluitend vanuit de VDI-sessie de webapplicatie worden benaderd die in een eigen (GSB/CSB) compartiment draait. In de webapplicatie kunnen gegevens worden ingevoerd, gecontroleerd, vastgesteld en digitaal ondertekend.



Figuur 1: Visualisatie technische opzet

In dit ontwerp zijn enkele belangrijke afwegingen ten aanzien van beveiliging integraal verwerkt. In de visualisatie is een logvoorziening opgenomen waarmee verschillende loggegevens (de rode lijn in de afbeelding) centraal worden verzameld en opgeslagen. De centrale logvoorziening maakt het mogelijk dat met behulp van een Security Operations Center (SOC) het DHV actief wordt gemonitord.

Het "Geen vertrouwen (Zero trust)" principe betekent dat geen systeem, netwerk, (markt)partij of persoon op zichzelf als geheel vertrouwd wordt. Daarom zijn er aanvullende maatregelen nodig. In het navolgende wordt ingegaan op aanvullende beveiligingsmaatregelen rond:

1. De werkstations;
2. Het netwerk;
3. De logging en het Security Operations Center (SOC);
4. Organisatorische maatregelen als functiescheiding en gebruiksrollen;
5. Naleving en controle;

6. Beheer en;
7. Hosting.

Ad 1) Maatregelen ten aanzien van de beveiliging van werkstation

Maatregel 1: toegang via gehardende Virtuele Desktop omgeving

De gebruiker dient eerst in te loggen (middels twee-factor-authenticatie) op de centrale VDI-omgeving van het DHV en heeft vandaaruit pas toegang tot de DHV-webapplicatie. De VDI-omgeving vormt hiermee een beveiligde tussenlaag tussen het werkstation van de gebruiker en de DHV-webapplicatie. De VDI-omgeving wordt centraal beheerd en gemonitord. Dit maakt het mogelijk eenduidige hardening toe te passen (zoals het centraal doorvoeren van beveiligingsupdates) waardoor de aanvalsmogelijkheden voor een kwaadwillende sterk worden beperkt.

Maatregel 2: gebruik gehardende image op de werkstations die centraal beschikbaar wordt gesteld

Werkstations die worden gebruikt om op de centrale VDI-omgeving te komen kunnen gecompromitteerd zijn. Om eventuele beveiligingsproblemen in de software van het werkstation van de gebruiker te ondervangen wordt technisch afgedwongen dat er een image wordt geïnstalleerd, gehardend en voorzien van beveiligingsinstellingen (bijvoorbeeld: dat met deze image in beginsel geen reguliere verbinding met internet mogelijk is, enkel de verbinding via besloten netwerk naar DHV is toegestaan). Er wordt een gemeente-specifiek certificaat opgenomen in de image. Dit certificaat is, in aanvulling op IP-whitelisting, een extra toegangscontrole voor toegang tot de VDI-omgeving.

Maatregel 3: alleen werkstations die conform een procedure worden beheerd en opgeslagen mogen worden gebruikt

Deze maatregel geeft een extra waarborg dat het werkstation, voordat dit wordt ingezet, overeenkomstig de gewenste procedures wordt beheerd. De werkstations worden hierbij overeenkomstig de voorschriften van de Kiesraad voorbereid. Aangezien gebruik wordt gemaakt van centraal gedistribueerde images, kan voor de hardening worden volstaan met een beperkte set aan aandachtspunten bij het inrichten van het werkstation (bijv. geen onveilige randapparatuur aansluiten) en instructies voor de opslag.

Ad 2) Maatregelen tegen aanvallen via het netwerk

Maatregel 4: DHV uitsluitend beschikbaar via besloten overheidsnetwerk (Diginetwerk)

Om het aanvalsoppervlak te verkleinen wordt het DHV ontsloten via een besloten (semi)overheidsnetwerk. Dit betekent dat uitsluitend de werkstations die in verbinding staan met het besloten netwerk, toegang hebben tot het DHV. Zodoende is het voor ongeautoriseerde aanvallers niet mogelijk om aanvallen via het internet uit te voeren op de omgeving (zoals DDoS-aanvallen). Het is alleen mogelijk om vanaf partijen die aangesloten zijn op het besloten netwerk dergelijke aanvallen uit te voeren. Via Diginetwerk is connectiviteit met alle aangesloten overheidsorganisaties via één koppeling mogelijk. Op termijn zal GGI-netwerk als besloten overheidsnetwerk worden gebruikt, maar gegeven de adoptiegraad van dit netwerk (februari 2020 33,5%) zal dit op de korte termijn Gemnet zijn waarop alle gemeenten zijn aangesloten.[1]

Maatregel 5: DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen

Deze technische maatregel zorgt ervoor dat uitsluitend vooraf aangemelde GSB/CSB IP-adressen een verbinding kunnen maken met het DHV (*IP-whitelisting*). Door IP-whitelisting is het voor

[1] Op een externe locatie zal veelal geen netwerkverbinding gemaakt kunnen worden met het Diginetwerk. Gemeenten zorgen in principe zelf - middels bijvoorbeeld bestaande thuiswerkvoorzieningen - voor toegang tot het gemeentelijk netwerk. Gemeenten kunnen ook (tegen een kostendekkend tarief) via de Kiesraad de benodigde VPN-hardware verkrijgen waarmee de verbinding naar het DHV kan worden gelegd.

aanvaller niet mogelijk om via een ander IP-adres, welke niet is aangemeld, het DHV te benaderen.

Maatregel 6: Gecompartimenteerde omgeving

Binnen het DHV wordt compartimentering toegepast, zodat aan ieder GSB en CSB een eigen afgescheiden omgeving toegekend wordt waarbinnen de gebruikersfunctionaliteiten en data zich bevinden. De impact van een eventuele succesvolle aanval op een GSB-compartiment blijft hierdoor beperkt tot het specifieke compartiment. Een extra maatregel die wordt toegepast om een compartiment af te schermen van de andere compartimenten is door het plaatsen van data diodes die ervoor zorgen dat gegevens enkel een bepaalde kant op kunnen gaan. Het toepassen van data diodes wordt voorzien bij het compartiment voor de zetelverdeling die tevens op een aparte server wordt ondergebracht.

Maatregel 7: Intrusion Prevention maatregelen

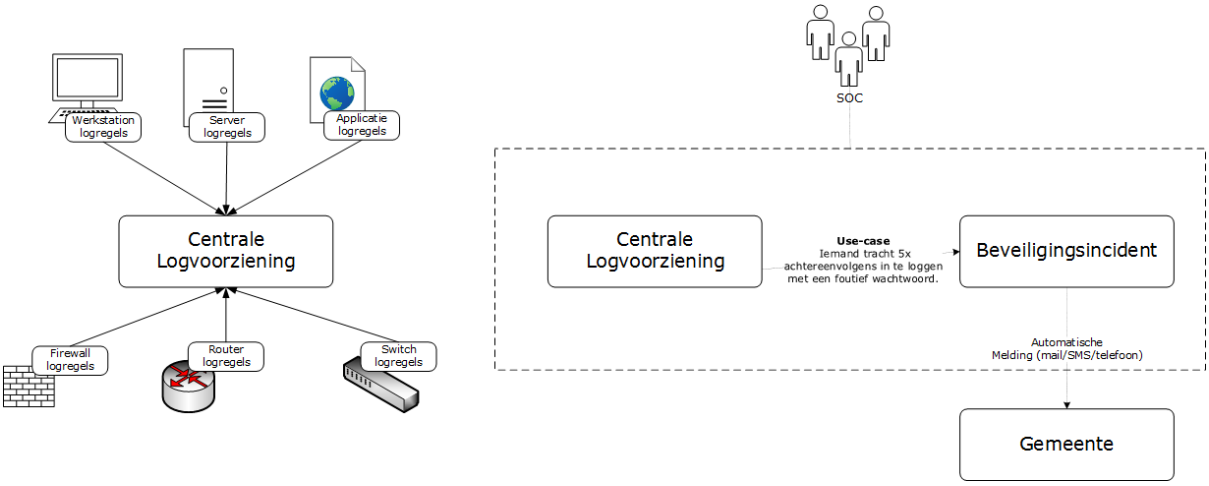
Aanvallers met netwerktoegang tot het DHV kunnen het systeem via het netwerk proberen aan te vallen. Aanvallen kunnen daarbij gericht zijn op de infrastructuur (zoals servers), maar ook op de webapplicatie zelf. Om dergelijke aanvallen te signaleren wordt voorzien in brede logging en monitoring van het DHV. Netwerk gebaseerde aanvallen worden met (next generation) firewall functionaliteiten afgevangen en door het IPS ondervangen met behulp van Web Application Firewall (WAF) functionaliteiten. De gebruikte IPS dient over al deze functionaliteiten te bezitten, zodat het DHV op verschillende niveaus kan worden beschermd.

Maatregel	**Belang**
Gehardende VDI (maatregel 1)	Vereist
Gehardende image bij gemeente (maatregel 2)	Toepassen indien haalbaar
Beheer werkstation conform richtlijnen Kiesraad (maatregel 3)	Dringend geadviseerd
DHV uitsluitend via besloten overheidsnetwerk (maatregel 4)	Vereist
Whitelist IP-adressen (maatregel 5)	Vereist
Gecompartimenteerde omgeving (maatregel 6)	Vereist
Intrusion Preventie maatregelen (maatregel 7)	Vereist

Ad 3) Maatregelen rond logging en Security Operations Center (SOC)

Om achteraf nog te kunnen vaststellen welke handelingen er door gebruikers zijn uitgevoerd in het DHV vindt logging plaats. De handelingen die worden vastgelegd zijn herleidbaar tot één persoon. De logging dient als input voor het in te stellen Security Operations Center (SOC). Dit SOC monitort de computer- en netwerkactiviteiten van het DHV. Log-informatie afkomstig van de verschillende componenten van het DHV, zoals de Virtuele Desktop omgeving, servers- en netwerkcomponenten en vanuit de standaard- en maatwerksoftware. De log-informatie wordt automatisch doorgestuurd naar het SOC, waar op basis van speciale software wordt gemonitord op verdachte situaties. Het SOC stelt onwenselijke situaties vast en informeert de Kiesraad en gebruikersorganisaties daarover zodat zij mitigerende maatregelen in werking kunnen stellen. Onderdeel van de afhandeling van incidenten is dat de gebruikersorganisaties en de Kiesraad zelf rapporteren naar aanleiding van de meldingen van het SOC en een terugkoppeling geven aan het SOC. Dit stelt het SOC in staat om een totaalbeeld te geven van de incidenten en hoe deze zijn afgehandeld.

Logging is ook nodig om achteraf te kunnen onderzoeken of er misbruik is gemaakt van het DHV en is input voor eventuele forensische onderzoeken. De logging dient dan ook beschikbaar te kunnen worden gesteld aan de veiligheidsdiensten. Het is een eis dat de inrichting van de datacentra en netwerken voldoet aan de benodigdheden van deze diensten;



Figuur 2: Centrale logvoorziening en melding naar gemeenten.

Het SOC is operationeel gedurende de periode dat het DHV operationeel is. Voorafgaand aan de invoer van de uitslagen is het DHV operationeel om de verkiezing te configureren en de stembureau- en kandidaatgegevens vast te leggen.

Ad 4) Organisatorische maatregelen als functiescheiding en gebruiksrollen

Bij de totstandkoming van de verkiezingsuitslag is het belangrijk dat de verantwoordelijkheden en bevoegdheden niet bij één persoon worden ondergebracht. Er zal sprake zijn van een vier-ogen principe en van functiescheiding. Deze functiescheiding geldt voor de functionele implementatie voor de gebruikers en geldt voor de implementatie ten aanzien van het technisch- en applicatiebeheer. Met de functionele scheiding wordt een scheidingslaag aangebracht in de programmatuur door het definiëren van bepaalde gebruikersrollen voor de verschillende functies binnen het DHV. De gebruiker krijgt enkel de functionaliteiten die voor de rol van de gebruiker relevant zijn. De gebruiker heeft geen toegang tot functionaliteiten die horen bij een andere rol. Voor alle gebruikers geldt dat zij alleen toegang krijgen tot het DHV middels twee-factor-authenticatie. De toepassing van twee-factor-authenticatie verschilt per gebruiker. Er worden drie typen (functionele)gebruikers onderscheiden:

- De beheerder(s) die zorgen voor de (verkiezings)configuratie en het gebruikersbeheer;
- De gebruikers die binnen GSB/CSB-bestanden en documenten voorzien van een digitale handtekening of waarmerk (de (vice-)voorzitter van het GSB/CSB);
- De gebruiker(s) die betrokken zijn bij de invoer van uitslaggegevens en het bepalen van de verkiezingsuitslag (Invoerder en Lid-GSB/CSB).

Gemeenten en de Kiesraad zorgen er middels het toepassen van een integriteitsverklaring of VOG zelf voor dat alle gebruikers aantoonbaar integer zijn. Strikte implementatie van functiescheiding houdt ook in dat één persoon niet meerdere rollen binnen het DHV kan vervullen. Gekoppeld aan het vier-ogen principe betekent dit dat voor het vaststellen van een verkiezingsuitslag, voor het GSB en CSB elk, minimaal vijf verschillende personen in het DHV geautoriseerd dienen te zijn. Het gaat hierbij om minimaal twee invoerders, één GSB/CSB lid, één (vice)voorzitter GSB en één beheerder.

Ad 5) Maatregelen rond naleving en controle

Het ontwerp van het DHV bevat diverse belangrijke beveiligingsnormenkaders, -voorschriften, -richtlijnen en eisen die van toepassing zijn op verschillende partijen. Indien een van de partijen niet voldoet aan een beveiligingseis, kan dit resulteren in beveiligingsrisico's. Het is bijvoorbeeld van belang dat de ontwikkelpartij conform *Secure Software Development* beveiligingsrichtlijnen werkt, om te voorkomen dat kwetsbaarheden worden geïntroduceerd in de software tijdens het ontwikkelproces. De Kiesraad controleert of de van toepassing zijnde beveiligingskaders door de verschillende partijen worden nageleefd. Hiertoe dient de Kiesraad een *right to audit* in de contracten met externe partijen op te nemen en afspraken vast te leggen met de overige partijen.

Ad 6) Maatregelen rond ontwikkeling en beheer

Voor het beheer wordt onderscheid gemaakt tussen; functioneel beheer, applicatiebeheer en technisch-beheer. Het functioneel beheer richt zich op het (blijvend) gebruik en gebruikersgemak van de applicatie.

Functioneel beheer zorgt ervoor dat de gebruikers de juiste informatie, mogelijkheden en bevoegdheden hebben om de applicatie te kunnen gebruiken. Daarnaast houdt functioneel beheer in de gaten of de applicatie nog alles doet wat de gebruikers nodig hebben om hun werkzaamheden uit te voeren. De Kiesraad is de functioneel beheerder van het DHV.

Het applicatiebeheer is erop gericht om de continuïteit van het DHV te waarborgen. Hierbij gaat het om werkzaamheden die betrekking hebben op het beheer van de ontwikkel en testomgeving, verschillende vormen van softwareonderhoud en het doorvoeren van de ontwikkelen van het DHV. Het applicatiebeheer wordt uitgevoerd onder de verantwoordelijkheid van de Kiesraad.

Onder technisch beheer wordt verstaan het inrichten van de infrastructuur, bijvoorbeeld met het oog op beveiliging, waar het DHV gebruik van maakt. Het technisch beheer kan worden verricht door de Kiesraad maar ook door de hosting partij. Voorgesteld wordt de rol van technisch beheer te leggen bij de hostingpartij. Dergelijke leveranciers hebben doorgaans zeer veel ervaring bij deze werkzaamheden. Dit verkleint de kans dat de infrastructuur onverhoopt onveilig wordt geconfigureerd. Bij de selectie- en gunningscriteria zal gekozen worden voor een hosting partij met een grote ervaring op dit gebied, worden alle afspraken en beveiligingseisen rondom de infrastructuur formeel vastgelegd in contractdocumentatie en zal de Kiesraad periodiek bij de hostingpartij onderzoeken of deze eisen worden nageleefd (bijvoorbeeld door middel van een audit).

Ad 7) Maatregelen rond hosting

De centrale software moet middels infrastructuur worden aangeboden aan de gebruikers: de hosting. Deze hosting vervult een belangrijke rol want zonder toegang tot de software is er geen uitslag. De infrastructuur en de hostingspartij moeten dan ook betrouwbaar en beschikbaar, integer en veilig zijn. De voorkeur gaat uit naar een hostingvariant waarbij de Kiesraad zoveel mogelijk controle heeft over de hosting en het fysieke datacenter. Dit kan ook infrastructuur van de kiesraad zijn. De hostingpartij moet de geschatte piekbelasting aan kunnen. Hierover dienen afspraken te worden opgenomen in de aanbesteding. De hostingpartij en de keten van toeleveranciers dienen aantoonbaar te voldoen aan algemene beveiligingseisen en –kaders zoals de Baseline Informatiebeveiliging Overheid en de AVG.

Om de beschikbaarheid van de infrastructuur te bevorderen, wordt redundantie aangebracht in het ontwerp. Voor datacentra geldt dat in de aanbestedingseisen wordt opgenomen dat een hostingpartij standaard gebruikmaakt van minimaal twee fysiek gescheiden datacentra. Als een datacentrum uitvalt, dan kan de dienstverlening worden voortgezet vanaf het andere datacentrum.

Functionele eisen

De functionele eisen beschrijven het DHV in termen van functionaliteit of 'specifiek gedrag' (Wat moet het systeem doen?). Het DHV faciliteert het invoeren van de uitslaggegevens op GSB- en CSB-niveau. Op basis van deze uitslaggegevens wordt de verkiezingsuitslag berekend en zetelverdeling bepaald. Daarnaast verzorgt het DHV de (digitale) uitvoer, welke op hoofdlijnen bestaat uit: de proces-verbalen, de benoemings- en geloofsbrieven en uitslaggegevens.

Niet-functionele eisen

Naast de functionele eisen zijn ook de niet-functionele eisen van essentieel belang bij de realisatie van het DHV. Niet-functionele eisen beschrijven een systeem of applicatie in termen van kwaliteit

in brede zin, met eisen aan betrouwbaarheid, beveiliging, beschikbaarheid, schaalbaarheid, bruikbaarheid en/of gebruikersgemak, onderhoudbaarheid, overdraagbaarheid, etc.

Het informatiesysteem moet voldoen aan de betrouwbaarheidseisen voor beschikbaarheid (het informatiesysteem moet in de week van de verkiezingen beschikbaar zijn om de uitslag te kunnen invoeren en verwerken), integriteit (de juistheid en volledigheid van de informatie is nodig om het vertrouwen, transparantie en controleerbaarheid van het verkiezingsproces te borgen) en vertrouwelijkheid.

Voor het DHV is door het incidentele gebruik van de applicatie geen vast servicewindow en beschikbaarheid te definiëren. Deze hangen samen met het verloop van de verkiezing. IJkpunt is hierbij de dag van stemming en de aansluitende week waar de beschikbaarheid 99% moet zijn. Op andere momenten rond de verkiezingen mag de beschikbaarheid lager liggen.

Verwerken persoonsgegevens

Met het DHV zullen persoonsgegevens worden verwerkt. De verwerking van persoonsgegevens dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG. De persoonsgegevens zullen in beginsel gepseudonimiseerd en versleuteld zijn zodat de persoonsgegevens niet herleidbaar zijn. De persoonsgegevens zijn enkel toegankelijk voor diegenen die daarvoor geautoriseerd zijn en worden niet langer dan noodzakelijk bewaard.
Er zal een DPIA (Data Protection Impact Assessment) worden uitgevoerd om eventuele aanvullende privacybeschermende maatregelen te bepalen. In de DPIA wordt ook aangegeven welke organisaties binnen het proces als verwerkersverantwoordelijken moet worden aangemerkt en tussen welke partijen een verwerkersovereenkomst dient te worden afgesloten.
Kandidaatgegevens zijn niet als vertrouwelijk aan te merken omdat deze actief openbaar worden gemaakt zodat de kiezer in staat wordt gesteld kennis te nemen op welke personen gestemd kan worden. Tevens vereist de controleerbaarheid en transparantie van het verkiezingsproces dat de gegevens van kandidaten beschikbaar zijn voor burgers. Gelet op het voorgaande wordt aan de verwerking van kandidaatsgegevens geen privacyrisico toegekend en worden er geen specifieke maatregelen voorzien ten aanzien van deze groep van persoonsgegevens.

Softwarekwaliteit (ISO-25010)

Voor de software kwaliteit wordt aangesloten bij ISO 25010. Deze biedt een structuur om bijvoorbeeld requirements, acceptatiecriteria, risico's en testdoelen op te stellen en een gevoel te krijgen voor hun volledigheid. Voor het DHV ligt de nadruk op de volgende kenmerken:

- Functionele geschiktheid: Hierbij gaat het erom in hoeverre de (opgeleverde) applicatie voldoet aan de gespecificeerde taken en gebruikersdoelen qua compleetheid, correctheid en toepasbaarheid;
- Betrouwbaarheid: Bij 'betrouwbaarheid' is het belangrijk dat een applicatie blijft functioneren zonder technische storingen. Hier spelen zaken als bedrijfszekerheid (beschikbaarheid), foutbestendigheid en de herstelbaarheid een grote rol;
- Beveiligbaarheid: Hieronder vallen zaken als vertrouwelijkheid, integriteit en verantwoording.

Product acceptatie plan

Het DHV gaat door meerdere ICT-leveranciers in opdracht van de Kiesraad gerealiseerd worden. Voordat de opdrachtgever tot acceptatie van het DHV kan besluiten, moet duidelijk zijn op welke criteria het DHV wordt geaccepteerd. Acceptatiecriteria hebben als doel ondubbelzinnig duidelijk te maken wat er van het product wordt verwacht en dienen derhalve vooraf te zijn vastgelegd.

Service Niveau Overeenkomst

Kwaliteit tijdens gebruik vindt zijn weerslag in een Service Niveau Overeenkomst (SNO). Er zal per (hoofd)leverancier een SNO afgesloten worden ten behoeve het gebruik van het DHV. In een SNO zijn de serviceniveaus beschreven die van toepassing zijn op de dienstverlening van de betreffende leverancier (opdrachtnemer) aan de Kiesraad (opdrachtgever). Dit betreft veelal beheerprocessen

als beschikbaarheid-, continuïteits- en capaciteitsbeheer, incidentbeheer, wijzigings- en releasebeheer (al dan niet ten behoeve van preventief, correctief of adaptief onderhoud), etc.

Gebruiksvriendelijkheid en toegankelijkheid

Bij de ontwikkeling van de gebruikersinterface dient de ontwikkelaar te voldoen aan de eisen voor gebruikersvriendelijkheid en toegankelijkheid. Ten aanzien van toegankelijkheid dient de webinterface te voldoet aan de eisen op niveau A en AA van de WCAG 2.0.

Back-up strategie

De Kiesraad beschikt te allen tijde over een oudere, geteste versie van de software zodat deze kan worden gedeployed indien er grootschalige beschikbaarheidsproblemen zijn bij de softwareontwikkelaar.

Open standaarden en zoveel mogelijk open source standaardsoftware

In lijn met het overheidsbeleid zal ook bij het DHV gebruik gemaakt worden van open standaarden. De lijst met open standaarden van het Forum Standaardisatie is ook voor het DHV richtinggevend. Qua standaard software zal het uitgangspunt zijn om open source software toe te passen waar dat mogelijk is. Ten aanzien van de broncode van de maatwerksoftware, die betrekking heeft op de berekening van de uitslag en zetelverdeling, zal deze openbaar gemaakt worden.

Transparantie en controleerbaarheid

Transparantie en controleerbaarheid bij de vaststelling van de verkiezingsuitslag zijn van essentieel belang om vertrouwen te kunnen hebben en houden in de vaststelling van de uitslag van de verkiezingen. Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is. Er zijn in het verkiezingsproces geen 'geheimen'. Alle vragen rondom het verkiezingsproces moeten beantwoord kunnen worden, en de antwoorden moeten voor iedereen controleerbaar en verifieerbaar zijn. Het verkiezingsproces moet verder objectief controleerbaar zijn. De controle-instrumenten kunnen, afhankelijk van de fase waarin een verkiezing zich bevindt, verschillen.

Exitstrategie

Een vroegtijdige beëindiging van een overeenkomst tussen opdrachtgever en opdrachtnemer (leverancier) is een onwenselijke situatie die bij voorkeur voorkomen moet worden. Een vroegtijdige beëindiging kan het gevolg zijn van verschillende oorzaken zoals een verschil van inzicht tussen opdrachtgever en opdrachtnemer, ondeugdelijke leveranties of een faillissement van de opdrachtnemer. In geval van de situatie waarin een overeenkomst vroegtijdig wordt beëindigd, is het van belang om de continuïteit zo goed mogelijk te waarborgen. De risico's zullen worden beperkt door het afsluiten van een Escrow-overeenkomst en zullen er afspraken worden gemaakt over het intellectueel eigendom, toe te passen software-componenten en software-licenties. Daarnaast is het van belang dat de Kiesraad beschikt over het Intellectueel Eigendom en de gebruiksrechten die nodig zijn om het beheer en onderhoud van het DHV uit te kunnen laten voeren door een derde partij.

Inhoud

Verklaringen van afkortingen

Afkorting	Betekenis
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AVG	Algemene verordening gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIT	Bureau ICT-toetsing
BSB	Briefstembureau
CSB	Centraal stembureau
DDoS	Distributed Denial-of-service
DHV	Digitaal Hulpmiddel Verkiezingen
DPIA	Data Protection Impact Assessment
EH	eHerkenning
EK	Eerste Kamerverkiezing
EML	Election Markup Language
EP	Europese Parlementsverkiezing
GGI	Gemeentelijke Gemeenschappelijke Infrastructuur
GR	Gemeenteraadsverkiezingen
GSB	Gemeentelijk stembureau
HSM	Hardware Security Module
IBD	Informatiebeveiligingsdienst gemeenten
IP	Internet Protocol
KC	Kiescollegeverkiezingen
KR	Kiesraad
NBSB	Nationaal briefstembureau
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NVVB	Nederlandse Vereniging voor Burgerzaken
OTAP	Ontwikkeling, Test, Acceptatie, Productie
OTP	One-time password
PKI	Public Key Infrastructure
PKIo	PKIoverheid
PS	Provinciale statenverkiezingen
PV	Proces-verbaal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SB	Stembureau
SNO	Service Niveau Overeenkomst
SBOL	Stembureau van het openbaar lichaam
SOC	Security operations center
TK	Tweede Kamerverkiezing
TLS	Transport Layer Security
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming
UVW	Unie van Waterschappen
VA	Verkiezingsautoriteit
VO	Vertegenwoordigend orgaan
VDI	Virtual Desktop Infrastructure
VNG	Vereniging van Nederlandse Gemeenten
VPN	Virtual Private Network / Virtueel Particulier Netwerk
WS	Waterschapsverkiezingen

Begrippenlijst

Begrip	Beschrijving
Authenticatie	De authenticatie is het proces waarin wordt nagegaan of een gebruiker, een andere computer of applicatie daadwerkelijk is wie wordt beweerd.
Autorisatie	De autorisatie is het proces waarin een subject (een persoon of een proces) rechten krijgt op het benaderen van een object (een bestand, een systeem).
Controleprotocol	Een door de Kiesraad opgestelde procedure die toeziet op het controleren van de uitslagresultaten die met het DHV zijn berekend.
eHerkenning	eHerkenning is een gestandaardiseerd inlogsysteem, waarmee organisaties hun diensten veilig online toegankelijk kunnen maken. In essentie regelt eHerkenning de digitale herkenning (authenticatie) en controleert het de digitale bevoegdheid (autorisatie) van iemand die online een dienst wil afnemen.
Escrow-overeenkomst	Overeenkomst tussen de softwareontwikkelaar, de opdrachtgever en een escrow-dienstverlener. De overeenkomst garandeert dat in een exit-scenario (bijv. faillissement van of conflict met de softwareontwikkelaar) de opdrachtgever altijd kan beschikken over de actuele versie van de broncode van het software en documentatie waarvoor de overeenkomst geldt.
Gebruikersorganisatie	De organisatie die gebruik maakt van het DHV. Hieronder valt in ieder geval het GSB en de CSB, maar ook de ondersteunde organisatie aan het GSB en CSB, zoals de gemeente die met het DHV werkt, wordt hiertoe gerekend.
Kiesraad	In dit document wordt onder Kiesraad mede begrepen de beheerorganisatie die verantwoordelijk is voor het DHV.
PKIoverheid	PKIoverheid is de public key infrastructure (PKI) van de Nederlandse overheid. Net als elke andere PKI is het een afsprakenstelsel om digitale certificaten uit te geven en te beheren. PKIoverheid wordt beheerd door Logius.
Plan P	Het plan dat kan worden toegepast in het geval van een calamiteit. Voor de vaststelling van de uitslag kan dan gebruik worden gemaakt van een papieren proces, bijvoorbeeld in gevallen waarin het DHV niet gebruikt kan worden.
Ondersteunende organisatie	De organisatie, zoals de gemeente, die het GSB en CSB ondersteund bij de uitvoering van diens werkzaamheden.

Begrip	Beschrijving
Open source software	Software waarvan de broncode gepubliceerd en vrij beschikbaar is. Iedereen kan deze software vrij kopiëren, aanpassen en verspreiden. De (door)ontwikkeling van open source software kan plaatsvinden door gemeenschappelijke samenwerking van zowel individuele programmeurs als grote bedrijven.
Open standaarden	Een open standaard is een standaard die voldoet aan 4 kenmerken zoals gespecificeerd door het Forum Standaardisatie: 1. De benodigde documentatie moet laagdrempelig beschikbaar zijn. 2. Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht. 3. Er moeten voldoende inspraakmogelijkheden zijn voor stakeholders tijdens de (door)ontwikkeling van de standaard. 4. De onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie moeten verzekerd zijn.
Spoofing (e-mail)	Het namaken van e-mailberichten met een vervalst afzenderadres.
Verificatieproces	Een separaat proces waarmee iedereen kan vaststellen dat de uitslag die is berekend in het DHV correct is.
Verkiezingsautoriteit	In dit document wordt onder Verkiezingsautoriteit mede begrepen de beheerorganisatie die verantwoordelijk is voor het DHV.

1. Inleiding

1.1. Doelstelling en reikwijdte

Het doel is om het nieuwe Digitaal Hulpmiddel Verkiezingen (DHV) te beschrijven. Bij de ontwikkeling van het DHV spelen de volgende doelstellingen een rol:

- Het DHV is een hulpmiddel voor de verkiezingen van de leden van de Tweede Kamer (TK), de Eerste Kamer (EK), van het Europees Parlement (EP), gemeenteraad (GR), Provinciale staten (PS), Waterschappen (WS), Eilandsraad (ER) en Kiescollege (KC);
- In het ontwerp en bij de ontwikkeling van het DHV zijn sterke maatregelen verwerkt die de weerbaarheid van het verkiezingsproces tegen cybersecurity-dreigingen vergroten.
- Het DHV is zo opgezet dat transparantie en controle door derden mogelijk zijn. Voortdurend moet duidelijk zijn waar data vandaan komt, hoe data wordt verwerkt en hoe het DHV tot resultaten komt;
- Het DHV ondersteunt een meer centraal georganiseerd verkiezingsproces door als digitaal hulpmiddel GSB en CSB te voorzien van een uniforme, veilige en eenvoudig te gebruiken oplossing. Hierdoor kan het vierkiezingsproces robuuster worden omdat variatie wordt geminimaliseerd en sneller mogelijke issues onderkend worden;
- De broncode van (de maatwerksoftware van) het DHV is openbaar.

1.2. Leeswijzer

Voor de betrouwbaarheid van digitale hulpmiddelen zijn meerdere aspecten bepalend. Deze betreffen onder andere de beveiliging van programmatuur, de computers (apparatuur en het besturingssysteem) waarop de programmatuur wordt geïnstalleerd, de infrastructuur om toegang te krijgen tot het digitaal hulpmiddel én de procedures/processen voor het beheer en gebruik hiervan.

De doelstelling van dit document is om de basis-architectuur van het DHV te beschrijven. De reikwijdte betreft uitsluitend het beschrijven van het DHV voor het vaststellen van de verkiezingsuitslag en zetelverdeling. De basis-architectuur van andere te ontwikkelen onderdelen voor het verkiezingsproces, zoals de kandidaatstelling, zal in een afzonderlijk document worden vastgelegd.

De reden voor het starten met het beschrijven van de architectuur voor het vaststellen van verkiezingsuitslag en zetelverdeling is dat deze beide onderdelen kritieke onderdelen vormen van het verkiezingsproces. Zij bieden namelijk de output, die grote consequenties voor het democratisch proces heeft. Een adequate beveiliging is daarom met name voor deze beide onderdelen belangrijk.

De basisarchitectuur zoals beschreven in dit document kent een aantal onderwerpen die invulling geven aan het DHV en die tegelijkertijd een antwoord geven op de tekortkomingen en gebreken in OSV. Verder bevat dit document uitgangspunten en randvoorwaarden in relatie tot het gebruik en inzet van het DHV. Bij de uitwerking hiervan is zoveel mogelijke rekening gehouden met de mogelijke afweging tussen: bruikbaarheid (kunnen mensen met een gemiddeld opleidingsniveau redelijk eenvoudig aan de slag met het DHV), veiligheid en financiële haalbaarheid. Waar deze drie uitgangpunten mogelijk (verregaand) kunnen gaan conflicteren.

In de basisarchitectuur wordt ervan uitgegaan dat het DHV wordt opgebouwd als een centraal informatiesysteem (webapplicatie), dat door middel van een besloten (overheids)netwerk wordt ontsloten naar de gebruikers bij GSB en CSB. Deze invulling loopt als een rode draad door dit document. Verdere onderwerpen die aan bod komen in de basisarchitectuur zijn het proces, de

beveiligingsinstrumenten, de vereiste functionaliteiten (zoals gebruikersrollen) en niet-functionele vereisten (zoals betrouwbaarheid), netwerkinrichting en beheer.

Ten slotte biedt dit document met de geschetste basisarchitectuur een leidraad voor het opstellen van toekomstige wetgeving.

2. Scope en ketenpartners Digitaal Hulpmiddel Verkiezingen

2.1. Scope DHV

In het document wordt uitgegaan van de procedure voor de vaststelling van de uitslag zoals deze is beschreven in het nog in voorbereiding zijnde wetvoorstel ten aanzien van aanpassing van de procedure voor de vaststelling van verkiezingsuitslagen. Het betreft de versie van het wetsvoorstel zoals dat ter advisering in september/oktober 2019 aan de Kiesraad is voorgelegd. Uitgaande van het wetvoorstel is het hoofdstembureau, dat thans nog in de Kieswet is opgenomen in de procedure voor de vaststelling van de uitslag, niet meegenomen in dit document. Het omgekeerde geldt voor het gemeentelijkstembureau welke wel is opgenomen in de nadere uitwerking van het DHV, maar nog niet als instantie is opgenomen in de Kieswet.

Voor het vaststellen van de verkiezingsuitslag voeren het gemeentelijk stembureau (GSB) en het centraal stembureau (CSB) berekeningen uit. Uit de Kieswet volgt welke uitslaggegevens het GSB en het CSB moeten berekenen en op welke wijze deze dienen te worden vastgesteld. Voor het uitvoeren van de berekeningen die nodig zijn om de voorgeschreven uitslaggegevens te bepalen, maakt het GSB en CSB gebruik van het Digitaal Hulpmiddel Verkiezingen (DHV).

Uitgangspunt voor dit document is dat het DHV een centraal ontsloten informatiesysteem is. Het DHV bestaat in deze opzet uit centrale server- en software-componenten. De software-componenten omvatten standaard- en maatwerkprogrammatuur. Onder de centrale computercomponenten en standaardsoftware vallen:

- Centrale (virtuele)hardwarecomponenten, zoals servers en netwerkcomponenten;
- Standaardsoftwarecomponenten, zoals besturingssystemen, serversoftware, databasesoftware;
- Standaardcomponenten voor PKI en authenticatie;
- Virtuele desktop omgevingen (VDI).

In de maatwerkprogrammatuur zijn de functionele onderdelen van het DHV ondergebracht. Hieronder vallen:

- Functie- en rolgebonden autorisaties en implementatie van de toe te passen authenticatiemiddelen;
- Invoeren, controleren en accepteren van uitslaggegevens;
- Totaliseren van uitslaggegevens;
- Berekenen van de zetelverdeling;
- Genereren van de voorgeschreven documenten (proces-verbaal, en aanverwante documenten);
- Genereren van digitale uitslagen bestand(en);
- Mogelijk maken om bestanden/documenten digitaal te tekenen;
- Faciliteren van digitale overdracht (tussen GSB en CSB);
- Beheren van gebruikers (registeren, (de)activeren gebruikers en (de)blokkeren) en instanties (toestaan/blokkeren netwerkverbinding);
- Configuratie van de verkiezingsinstellingen, lijst- en kandidaatgegevens, regiostructuur en modeldocumenten.

Het DHV wordt ontsloten via een (besloten) landelijk netwerk waarop de GSB's en CSB's zijn aangesloten. Het landelijk netwerk, de fysieke werkcomputer en de netwerkaansluiting van het GSB en CSB zijn geen onderdeel van het te realiseren DHV-informatiesysteem. Door middel van aansluitvoorschriften wordt voorzien in een (toetsbaar) normenkader dat de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van de fysieke werkcomputer en de netwerkaansluiting worden gewaarborgd.

Naast de computer- en software-componenten waaruit het DHV is opgebouwd, maakt het technisch-, applicatie- en functioneel beheer onderdeel uit van de scope van het DHV. Het beheer ziet mede op het beveiligen en hardenen van het informatiesysteem.

2.2. Buiten scope

De onderwerpen die buiten de scope vallen van het DHV zoals die in dit document worden beschreven, worden in deze paragraaf aangehaald.

2.2.1. Andere programmatuur en systemen die bij het verkiezingsproces worden gebruikt

Systemen en programmatuur met betrekking tot de registratie van kiezers, het registeren van ongeldige stempassen (ROS) en het ondersteunen van de stembureaus maken geen onderdeel uit van de in dit document beschreven basisarchitectuur DHV. De programmatuur voor de kandidaatstelling valt daarnaast buiten de scope van het DHV. Het digitaal kunnen overnemen van de kandidaatsgegevens uit de kandidaatstellingsprogrammatuur wordt echter wel voorzien in het DHV.

2.2.2. Aanvullende informatie beveiligingsmaatregelen die buiten scope van het DHV vallen

In deze basisarchitectuur zijn enkele belangrijke aanvullende informatiebeveiligings- en uitvoeringsvraagstukken niet expliciet behandeld. Dit document omvat de technische maatregelen die die direct samenhangen met het DHV. Daarnaast zijn er ook aanvullende, meer organisatorische vraagstukken. In de onderstaande paragrafen benoemen wij deze vraagstukken. Ieder van deze vraagstukken dient in een nader op te stellen document verder te worden uitgewerkt.

Maatregelen buiten DHV

Het DHV dient te zijn beveiligd tegen aanvallen die de beschikbaarheid, integriteit en vertrouwelijkheid van het verkiezingsproces kunnen schaden. Ondanks alle getroffen maatregelen bestaat de mogelijkheid dat het DHV wordt gecompromitteerd, waarbij de integriteit van de uitslag en zetelberekening kan worden aangetast. Er moeten andere maatregelen worden getroffen om een dergelijke integriteitsschending van het DHV te detecteren en op te volgen. Hieronder de maatregelen die in het kader van het vaststellen van een correcte uitslag en zetelverdeling van belang zijn, maar buiten scope van de basisarchitectuur vallen:

- Het controleprotocol: een door de Kiesraad opgestelde procedure die toeziet op het controleren van de uitslagresultaten die met het DHV zijn berekend.
- Het verificatieproces: een separaat proces waarmee iedereen kan vaststellen dat de uitslag die is berekend in het DHV correct is.
- Plan P (Papier): het plan dat kan worden toegepast in het geval van een calamiteit. Voor de vaststelling van de uitslag wordt gebruikgemaakt van het papieren proces, bijvoorbeeld in gevallen waarin het DHV niet gebruikt kan worden. Het papieren proces blijft leidend.

Opleiding & Awareness

Het is van belang dat zowel gebruikers als beheerders van het systeem worden opgeleid met betrekking tot correct en veilig gebruiken van het systeem. Dit kan worden vormgegeven door middel van procedures en instructies, zowel voor gebruikers als beheerders. Dergelijke procedures en instructies dienen te worden getest en gereviewd, onder meer door diezelfde gebruikers. Om medewerkers verder op te leiden en de informatiebeveiligingsbewustwording te verhogen, kan tevens gebruik worden gemaakt van klassikale- of online trainingen. Bewustwordingscampagnes kunnen zich hierbij specifiek richten op belangrijke aspecten voor gebruikers of beheerders, zoals het veilig omgaan met authenticatiemiddelen.

Detailinvulling SNO

Een Serviceniveau-overeenkomst (SNO) is van belang om vast te leggen aan welke kwaliteits- en beveiligingseisen en voorwaarden moet worden voldaan. Ook worden hierin belangrijke afspraken vastgelegd over de beschikbaarheid van netwerken en infrastructuur. De exacte eisen die worden gesteld in de SNO dienen nader te worden uitgewerkt.

Detailuitwerking interne processen en procedures
Om het DHV veilig te ontwikkelen en te houden is het van belang om diverse beheersingsprocessen en -procedures in te richten. Enkele voorbeelden hiervan zijn een detailuitwerking van het wijzigingenbeheerproces, vulnerabilitymanagementproces, disaster recovery procedures, continuïteitsplannen en logisch toegangsbeheer. Het uitgangspunt is dat deze processen en procedures nader worden uitgewerkt conform gangbare richtlijnen en standaarden en dat hierop periodiek wordt getoetst.

2.3. Ketenpartners

Als ketenpartners worden beschouwd alle interne/externe partners, die een positieve, dan wel negatieve, invloed hebben op de besluitvorming rondom en de uitvoering van de aanbesteding, de realisatie en het gebruik van het DHV.

In de volgende paragrafen zijn ketenpartners onderkend, waarbij een onderscheid gemaakt wordt tussen de volgende fasen:
- De aanbestedings-fase;
- De realisatie-fase (en ingebruikname-fase);
- De beheer-fase.

2.3.1. Aanbestedings-fase

De volgende ketenpartners worden ten behoeve van de aanbesteding van het DHV onderkend:

Ketenpartner	Doel/competentie
Ministerie van BZK	- Het formaliseren van de kaders die gesteld worden aan het DHV; - De politieke besluitvorming; - Borgen van de financiering; - Inbreng specifieke kennis verkiezingsproces (o.a. via deelname aan werkgroepen).
Kiesraad	- Inbreng specifieke kennis verkiezingsproces (o.a. via leiden van en deelname aan werkgroepen); - Borgen organisatorische uitvoerbaarheid; - Opdrachtgever, en dus eindverantwoordelijk, voor de aanbesteding van het DHV; - (primaire) Opsteller van de aanbestedingsdocumentatie.
VNG in afstemming met NVVB	- Inbreng specifieke kennis gemeentepraktijk (o.a. via deelname aan werkgroepen); - Beoordeling gemeentelijke uitvoerbaarheid; - Zorgdragen voor draagvlak bij gemeenten; - Creëren van bewustzijn bij gemeentelijke ambtenaren met betrekking tot (digitale) beveiliging; - Inbrengen informatiebeveiligingskennis en kennis van de BIO (VNG-IBD).
NCSC / AIVD	- Inbreng specifieke kennis cyberbedreigingen; - Review van het beveiligingsconcept; - Review op aanbestedingstraject.
UBR / HIS	- Inbreng specifieke kennis inkoop, aanbesteding en contractvorming; - Opstellen aanbestedingsstrategie;

Ketenpartner	Doel/competentie
	- Begeleiden aanbestedingstraject.
BIT	- Beoordeling (vooraf) van de projectaanpak en advies.

2.3.2. Realisatie-fase

De volgende ketenpartners worden ten behoeve van de realisatie van het DHV onderkend:

Ketenpartner	Doel/competentie
Ministerie van BZK	- Indien van toepassing, en aanvullend op hetgeen tijdens de aanbestedingsfase al is gerealiseerd: o Het formaliseren van de kaders die gesteld worden aan het DHV; o De politieke besluitvorming; o Borgen van de financiering; o Inbreng specifieke kennis verkiezingsproces.
Kiesraad	- Opdrachtgever, en dus eindverantwoordelijk, voor de realisatie van DHV; - Overall projectmanagement realisatie DHV; - Eerste aanspreekpunt (hoofd-)leverancier(s) DHV; - Deelname acceptatietesten realisatie DHV; - Indien van toepassing en aanvullend op hetgeen tijdens de aanbestedingsfase al is gerealiseerd: o Inbreng specifieke kennis verkiezingsproces; o Borgen organisatorische uitvoerbaarheid.
VNG in afstemming met NVVB	- Deelname gebruikerstesten realisatie DHV; - Indien van toepassing, en aanvullend op hetgeen tijdens de aanbestedingsfase al is gerealiseerd: o Inbreng specifieke kennis gemeentepraktijk; o Beoordeling gemeentelijke uitvoerbaarheid; o Zorgdragen voor draagvlak bij gemeenten. o Inbreng informatiebeveiligingskennis en kennis van de BIO (VNG-IBD)
Unie van Waterschappen (UVW)	- Deelname acceptatietesten realisatie DHV; - Inbreng specifieke kennis over de praktijk bij waterschappen; - Beoordeling uitvoerbaarheid voor waterschappen; - Zorgdragen voor draagvlak bij de waterschappen; - Creëren van bewustzijn bij ambtenaren van waterschappen met betrekking tot (digitale) beveiliging.
NCSC / AIVD	- Review op realisatietraject; - Indien van toepassing en aanvullend op hetgeen tijdens de aanbestedingsfase al is gerealiseerd: o Inbreng specifieke kennis cyberbedreigingen.
Eén of meer leveranciers DHV voor: - Realisatie DHV; - hosting; - netwerk; - authenticatie; - periodieke toetsing (pentesten, audits, ethisch hacking, etc.).	- Inbreng specifieke (technische) kennis en capaciteit; - Realisatie en tijdige oplevering onderdelen voor integratie met DHV.
Leverancier van het SOC (Security Operations Center)	- Inbreng specifieke (technische) kennis en capaciteit; - Realisatie en tijdige oplevering DHV.

Ketenpartner	Doel/competentie
Randvoorwaardelijke leveranciers voor producten en diensten, bijvoorbeeld: - SSC-ICT (Haagse Ring); - Logius (Diginetwerk); - VNG Realisatie (GGI-netwerk/ GGI-veilig); - KPN (Gemnet;) - eHerkenningsmakelaar.	- Inbreng specifieke (technische) kennis en capaciteit; - Realisatie/implementatie randvoorwaardelijke producten en diensten, benodigd voor de realisatie van DHV.

2.3.3. Beheer-fase

In de beheer-fase zien we veelal dezelfde ketenpartners terug als bij de realisatie van het DHV, alleen nu met een ander of een beperkter doel. De gebruik-fase richt zich op de voorbereiding en het gebruik van het DHV tijdens verkiezingen en op het onderhoud en de doorontwikkeling (applicatiebeheer) van het DHV tussen de verkiezingen.

Ketenpartner	Doel/competentie
Ministerie van BZK	- Borgen van de financiering.
Kiesraad/Verkiezingsautoriteit	**Exploitatie** - Zorgdragen operationele beschikbaarheid tijdens verkiezingen (o.a. helpdesk); - Functioneel beheer DHV op CSB-niveau; **Onderhoud/doorontwikkeling** - Opdrachtgever en dus eindverantwoordelijk, voor onderhoud/doorontwikkeling DHV; - Overall projectmanagement onderhoud/doorontwikkeling DHV; - Eerste aanspreekpunt (hoofd-)leverancier(s) DHV; - Inbreng specifieke kennis verkiezingsproces; - Borgen organisatorische uitvoerbaarheid; - Uitvoeren acceptatietesten; - Onderhoud en doorontwikkeling DHV.
VNG in afstemming met NVVB	- (reguliere) Terugkoppeling gemeentelijke uitvoerbaarheid; - Inbreng specifieke kennis gemeentepraktijk bij onderhoud/doorontwikkeling DHV; - Deelname gebruikerstesten doorontwikkeling DHV; - Creëren van bewustzijn bij gemeenteambtenaren met betrekking tot (digitale) beveiliging. - Inbreng informatiebeveiligingskennis en kennis van de BIO (VNG-IBD).
Unie van Waterschappen (UVW)	- (reguliere) Terugkoppeling uitvoerbaarheid bij waterschappen; - Inbreng specifieke kennis over de praktijk bij waterschappen bij het onderhoud/doorontwikkeling DHV; - Aandragen eisen en wensen vanuit de betreffende waterschappen ten behoeve van onderhoud/doorontwikkeling DHV.
Gemeenten (gebruikersorganisatie)	- Beheer werkstations en netwerkaansluiting t.b.v. DHV op GSB-niveau; - Doorvoeren lokale verkiezingsgegevens en gebruikersbeheer in het DHV;

Ketenpartner	Doel/competentie
	- (reguliere) Terugkoppeling gemeentelijke uitvoerbaarheid aan de VNG; - Specifieke kennis gemeentepraktijk met betrekking gebruik van DHV doorgeven aan VNG.
NCSC / AIVD	- Inbreng specifieke kennis cyberbedreigingen bij onderhoud/doorontwikkeling DHV; - (periodieke) toetsing van onderhoud/doorontwikkeling DHV qua beveiligingsconcept.
Eén of meer leveranciers DHV voor: - Technisch en applicatiebeheer (en onderhoud); - hosting; - netwerk; - authenticatie; - periodieke toetsing (pentesten, audits, ethisch hacking, etc.)	- (indien van toepassing) Inbreng specifieke (technische) kennis en capaciteit; - Realisatie en tijdige oplevering onderhoud/doorontwikkeling DHV (applicatiebeheer); - Technisch beheer DHV.
Leverancier van het SOC (Security Operations Center)	- Inbreng specifieke (technische) kennis en capaciteit; - Realisatie en tijdige oplevering onderhoud/doorontwikkeling DHV (applicatiebeheer).
Ondersteunende leveranciers voor producten en diensten, bijvoorbeeld: - SSC-ICT (Haagse Ring); - Logius (Diginetwerk); - VNG Realisatie (GGI-netwerk/ GGI-veilig); - KPN (Gemnet); - eHerkenningsmakelaar.	(indien van toepassing) - Inbreng specifieke (technische) kennis en capaciteit; - Realisatie/implementatie randvoorwaardelijke producten en diensten en benodigd onderhoud/doorontwikkeling DHV.

Daarnaast is er ook een keten voor de vaststelling van de verkiezingsuitslag. Deze keten kent verschillende gebruikers en de samenstelling kan per verkiezingssoort verschillen. Voor de vaststelling van verkiezingsuitslagen worden de volgende gebruikers onderkend:

Orgaan	Verkiezing/taken
Kiesraad/Verkiezingsautoriteit (als beheerorganisatie)	- Functioneel beheer DHV; - Ondersteuning Kiesraad als CSB.
Kiesraad/Verkiezingsautoriteit (als CSB)	- Centraal stembureau bij nationale verkiezingen (EK, TK en EP).
CSB (Gemeenten)	- Centraal stembureau bij provinciale staten (gevestigd in de provinciehoofdstad gemeente); - Centraal stembureau bij gemeenteraadsverkiezingen.
CSB (Waterschappen)	- Centraal stembureau bij waterschapsverkiezingen.
CSB (Openbaar lichaam)	- Centraal stembureau bij eilandsraadverkiezingen.
CSB (Kiescollege)	- Centraal stembureau bij verkiezingen voor het kiescollege.

Orgaan	Verkiezing/taken
GSB	- Gemeentelijk stembureau bij nationale en regionale verkiezingen.
NBSB	- Nationaal briefstembureau bij TK- en EP-verkiezing.
SB	- Stembureau bij nationale en regionale verkiezingen.
Waterschappen	- Ondersteunde organisatie aan het CSB
Gemeenten	- Ondersteunde organisatie aan het GSB/CSB.
Gemeente Den Haag	- Ondersteunde organisatie aan het NBSB.
Openbaar lichaam	- Ondersteunde organisatie aan het SBOL bij eilandsraadverkiezingen.

2.4. Verkiezingstypen en structuur

2.4.1. Kieswet en verkiezingen

De Kieswet regelt de verkiezingen voor de leden van de Eerste Kamer en Tweede Kamer der Staten-Generaal, het Europees Parlement, de Provinciale Staten, de algemene besturen van waterschappen, de eilandsraden, de gemeenteraden en de kiescolleges. De meeste verkiezingen vinden om de vier jaar plaats, een uitzondering hierop is de verkiezing voor het Europees Parlement welke om de vijf jaar wordt gehouden.

Er zijn situaties mogelijk waarbij de verkiezing voor een vertegenwoordigend orgaan afwijkt van de reguliere periode. Voorbeeld hiervan is de ontbindingsverkiezing voor de Tweede Kamer, nadat de regering zijn ontslag heeft aangeboden. Op het niveau van gemeenten kan er sprake zijn van een herindelingsverkiezing in geval de indeling van de gemeente wordt herzien. In een dergelijke situatie wordt er een nieuwe gemeenteraad gekozen buiten de reguliere landelijke gemeenteraadsverkiezingen. Herindelingsverkiezingen kunnen zowel binnen als buiten de termijn van vier jaar plaatsvinden.

2.4.2. Bepalen verkiezingsuitslag

De verkiezingsuitslag wordt in Nederland op verschillende niveaus bepaald door een daartoe ingesteld orgaan. De organen die betrokken zijn bij het vaststellen van de verkiezingsuitslag zijn het stembureau (SB), het gemeentelijkstembureau (GSB) en het centraal stembureau (CSB). In hoofdstuk 3 wordt nader uiteengezet hoe het proces voor de vaststelling van de verkiezingsuitslag verloopt en welk orgaan op welk niveau de uitslag bepaald.

2.4.3. Verkiezingstypen

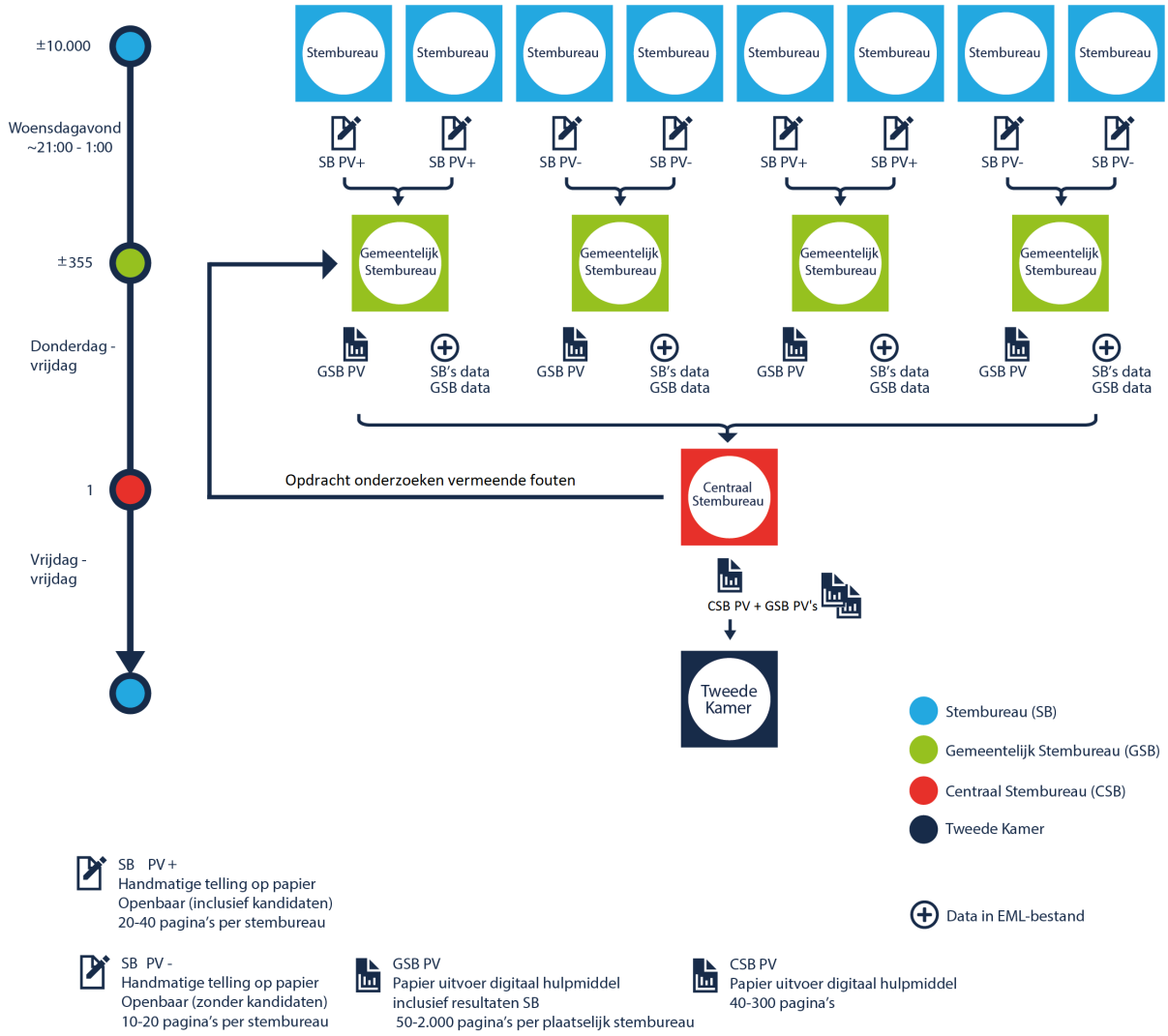
Voor elke verkiezing is er één CSB en zijn er één of meerdere GSB's. Welk orgaan als CSB optreedt en welke GSB's onderdeel zijn van de verkiezing is afhankelijk van het vertegenwoordigend orgaan waarvoor de verkiezing plaats vindt, ofwel het verkiezingstype. Afhankelijk van het verkiezingstype kunnen ook andere organen, dan het reeds aangehaalde stembureau, gemeentelijkstembureau en centraal stembureau, een rol hebben bij de vaststelling van de uitslag. Andere organen zijn: het briefstembureau (BSB), nationaal briefstembureau (NBSN), stembureau van het openbaar lichaam (SBOL) en kiescollege (KC). De onderstaande tabel geeft een overzicht van de verschillende verkiezingstypen en de acterende organen.

Verkiezingstype	Afkorting	Wie is CSB	Aantal CSB/GSB
Eerste Kamer	EK	Kiesraad	1/12+3 *
Tweede Kamer	TK	Kiesraad	1/355+1**
Europees Parlement	EP	Kiesraad	1/355+1**
Provinciale Staten	PS	Hoofdstad gemeente provincie	12/355
Algemeen bestuur Waterschappen	WS	Waterschap	22/443***
Eilandsraad	ER	Openbaar lichaam	3/3****
Gemeenteraad	GR	Gemeente	355/355
Kiescollege	KC	Openbaar lichaam	3/3****

* De Eerste Kamer wordt gekozen door de leden van de 12 provinciale staten en de 3 kiescolleges waarbij iedere provinciale staten en kiescollege een eigen stembureau is.
** Naast een GSB per gemeente is er bij TK en EP-verkiezing eveneens sprake van het nationaal briefstembureau (NBSB) dat de uitslag vaststelt van de kiezers in het buitenland.
*** Het aantal GSB's is bij waterschapsverkiezingen hoger doordat er gemeenten zijn die binnen de gemeentegrenzen meerdere waterschappen hebben, waardoor er binnen de gemeente voor elk waterschap een afzonderlijk GSB wordt ingesteld.
**** Bij de eilandsraad en kiescollege verkiezing is er sprake van "stembureau van het openbaar lichaam" in plaats van gemeentelijk stembureau (GSB)

Bij de uitwerking van het DHV wordt met name ingegaan op de uitwerking voor het GSB en CSB. Bij de verkiezingstypen waar het NBSN en SBOL onderdeel zijn van de vaststellingsketen, gelden voor deze organen in beginsel dezelfde uitgangpunten als voor het GSB.

Afhankelijk van het type verkiezing is er sprake van één of meerdere GSB's die de uitslag doorgeven aan het CSB. De volgende figuur geeft schematisch weer hoe de verkiezingsuitslag tot stand komt en op welke momenten binnen het vaststellingsproces een instantie zijn uitslag bepaald. In het volgende hoofdstuk 3 'Algemene procesbeschrijving vaststellen verkiezingsuitslag' is een nadere beschrijving opgenomen ten aanzien van het proces.



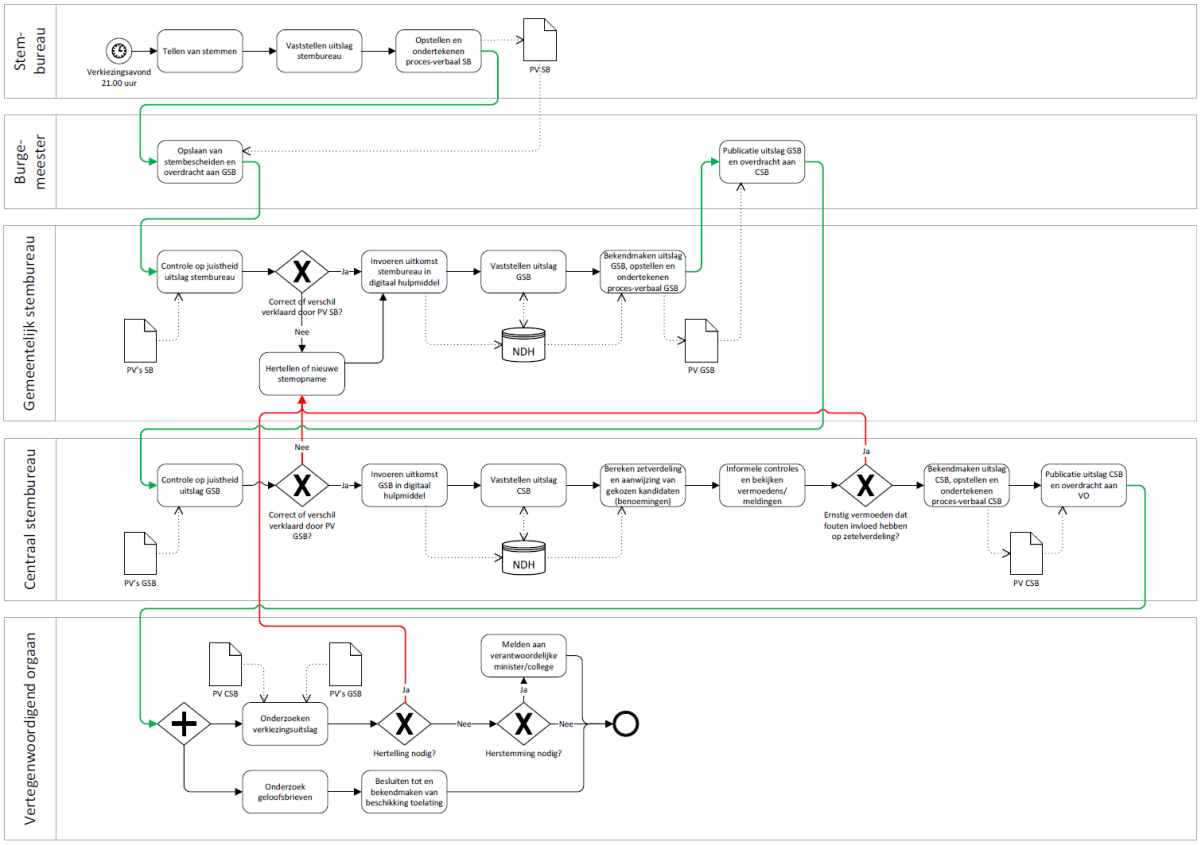
Figuur 3: Schematische weergave tot stand komen verkiezingsuitslag.

3. Algemene procesbeschrijving vaststellen verkiezingsuitslag

In dit hoofdstuk wordt het proces voor de vaststelling van de verkiezingsuitslag samengevat. Een uitgebreidere beschrijving van het proces is opgenomen in een separaat document "Procesbeschrijving Vaststellen verkiezingsuitslag".

Deze (verkorte) procesbeschrijving omvat het vaststellen van de verkiezingsuitslag. Het proces Vaststellen verkiezingsuitslag bestaat uit een keten van veelal sequentiële (sub)processen, uitgevoerd door verschillende actoren. Dit proces strekt zich uit van het tellen van de stemmen in het stembureau tot en met het bekendmaken van de uitslag en de toelatingen tot het vertegenwoordigend orgaan.
De procesbeschrijving is gebaseerd op de huidige Kieswet[2] (geldend op februari 2019), het beoogde Wetsvoorstel (tekst van oktober 2019) en de, bij het wetsvoorstel behorende, Memorie van Toelichting (tekst van oktober 2019).

De processen zijn gegroepeerd op actor (stembureau, burgemeester, gemeentelijk stembureau, centraal stembureau en vertegenwoordigend orgaan) en in sequentiële (en veelal chronologische) volgorde beschreven. Het proces Vaststellen verkiezingsuitslag ziet er op hoofdlijnen als volgt uit:



Figuur 4: Schematische weergave proces vaststelling uitslag.

Een vergrote weergave is opgenomen in de Bijlage D: Vergrote weergave afbeeldingen en tabellen.

In de wet en regelgeving zijn taken opgedragen aan bijvoorbeeld de burgemeester of de voorzitter van het GSB of de voorzitter van het CSB. In de praktijk worden deze werkzaamheden veelal uitgevoerd door daartoe aangewezen ambtenaren. Ten behoeve van de leesbaarheid wordt in dit document dan de (generieke) term burgemeester, GSB, CSB, etc. gebruikt.

[2] Met name de hoofdstukken N, O, P en V uit de Kieswet.

3.1. Stembureau

Het proces begint meteen na de sluiting van de stemming (verkiezingsavond om 21.00 uur). Het stembureau telt de stembiljetten en overige stembescheiden (stempassen, kiezerspassen en volmachtbewijzen) in het stemlokaal en stellen de uitkomsten daarvan in het openbaar vast. Eventuele bezwaren van aanwezigen worden genoteerd in het met de hand ingevulde papieren proces-verbaal (PV SB). De stembiljetten en overige stembescheiden worden elk afzonderlijk verpakt, verzegeld en vervolgens in één of meerdere transportboxen gestopt. Het proces-verbaal wordt samen met één of meerdere sleutels van de betreffende transportboxen in een envelop gestopt en verzegeld. De verzegelde envelop en transportbox(en) worden overgedragen aan de burgemeester.

3.2. Burgemeester

De burgemeester is verantwoordelijk voor het vervoer van het PV SB en de stembescheiden van het stembureau naar het gemeentelijk stembureau (GSB). Indien van toepassing behelst dit ook een (tijdelijke en) beveiligde opslag totdat het PV SB en de stembescheiden aan het GSB overgedragen kunnen worden.

3.3. Gemeentelijk stembureau (GSB)

Het proces begint de dag na de stemming bij de aanvang van de zitting van het gemeentelijk stembureau, en verloopt op hoofdlijnen als volgt. De wet kent twee sporen voor het bepalen van de uitslag van het stembureau, die van centraal of decentraal tellen. Bij decentraal tellen wordt op kandidaats-niveau de uitslag in het stembureau bepaald, bij centraal tellen wordt op lijst-niveau geteld en de uitslag daarvan in het PV SB vastgelegd. Het GSB stelt de volgende dag de uiteindelijke uitslag van het SB op lijst- en kandidaats-niveau vast. De uitslag van het stembureau op lijstniveau wordt door gemeenten gebruikt om op de verkiezingsavond de voorlopige uitslag door te geven.

Decentraal tellen
Bij een decentrale telling wordt de juistheid van de stembureau-uitslag gecontroleerd. Indien correct bevonden of de geconstateerde verschillen zijn verklaard in het PV SB, wordt de uitkomst van het stembureau ingevoerd in het digitale hulpmiddel. Indien niet correct of de geconstateerde verschillen niet zijn verklaard in het PV SB, besluit het GSB tot een nieuwe stemopname waarbij door het GSB de stembescheiden opnieuw geteld worden. De uitkomst van de hertelling wordt vastgelegd in een corrigendum als aanvulling op het PV SB. De (gewijzigde) uitkomst van het betreffende stembureau wordt in het digitale hulpmiddel ingevoerd.

Centraal tellen
Bij een centrale telling wordt de uitslag van het betreffende stembureau door het GSB vastgesteld en vervolgens vergeleken met de uitslag op lijstniveau, welke in het stembureau was vastgesteld. Indien correct bevonden of geconstateerde verschillen zijn verklaard, wordt de uitkomst van het betreffende stembureau ingevoerd in het digitale hulpmiddel. Indien niet correct of deze verschillen niet zijn verklaard, besluit het GSB tot het hertellen van het aantal toegelaten kiezers en wordt de uitkomst van het betreffende stembureau, aangevuld met eventuele geconstateerde verschillen, ingevoerd in het digitale hulpmiddel. De uitslag van het stembureau wordt bekend gemaakt aan de aanwezigen en eventuele bezwaren worden genoteerd in het proces-verbaal (PV GSB).

Nadat de uitslagen van alle stembureaus in het digitale hulpmiddel zijn ingevoerd worden deze uitslagen getotaliseerd tot een uitslag op GSB-niveau. Na het totaliseren controleert het GSB, aan de hand van het controleprotocol, of de uitslag die met het digitale hulpmiddel is berekend correct tot stand is gekomen. Vervolgens wordt de GSB-uitslag bekend gemaakt aan de aanwezigen en worden eventuele bezwaren genoteerd in het PV GSB. Na het officieel vaststellen en ondertekenen

van het PV GSB worden het PV GSB en de stembescheiden weer overgedragen aan de burgemeester.

3.4. Burgemeester

De burgemeester is verantwoordelijk voor de publicatie van de GSB-uitslag en de overdracht aan het centraal stembureau (CSB) van het PV GSB, het door het digitaal hulpmiddel gegenereerde digitale uitslaggegevens, en, indien decentraal geteld, de verzegelde enveloppen (met daarin per stembureau een PV SB en, indien van toepassing, een corrigendum).

3.5. Centraal stembureau (CSB)

Het proces bij het CSB begint als het papieren PV GSB ontvangen is, en verloopt op hoofdlijnen als volgt. Na ontvangst wordt de juistheid van de GSB-uitslag gecontroleerd. Als het CSB ervan overtuigd is dat een betrouwbare verkiezingsuitslag vast te stellen is, wordt de uitkomst van het GSB ingevoerd in het digitale hulpmiddel. Indien niet correct of de geconstateerde verschillen niet zijn verklaard in het PV GSB, verzoekt het CSB het GSB om een nieuwe stemopname. De uitkomst van deze hertelling (op basis van het nieuwe PV GSB) wordt vervolgens ingevoerd in het digitale hulpmiddel.

Nadat de uitslagen van alle GSB's in het digitale hulpmiddel zijn ingevoerd worden deze uitslagen getotaliseerd tot een uitslag op CSB-niveau. Na een aantal informele controles en het bekijken van de schriftelijke, onderbouwde meldingen wordt bepaald of er een ernstig vermoeden bestaat dat geconstateerde fouten invloed hebben op de zetelverdeling. Indien dit zo is, wordt het GSB verzocht een nieuwe stemopname uit te voeren, anders wordt de uitslag CSB bekend gemaakt aan de aanwezigen en eventuele bezwaren genoteerd in het PV CSB.

Na het officieel vaststellen en ondertekenen van het PV CSB wordt een afschrift van het PV CSB door het CSB gepubliceerd en ter inzage gelegd (en vervolgens bewaard tot het moment van vernietiging). Het PV CSB wordt overgedragen aan het vertegenwoordigend orgaan (VO).

3.6. Vertegenwoordigend orgaan (VO)

Het VO is de laatste instantie die oordeelt over het verloop van de verkiezing. Het VO onderzoekt hiertoe de verkiezingsuitslag en de geloofsbrieven van de benoemden.

De verkiezingsuitslag wordt onderzocht op basis van het PV CSB en de PV's GSB. Als er redenen zijn te twijfelen aan de geldigheid van de stemming of de juistheid van de uitslag, kan het VO besluiten om tot een hertelling over te gaan. Deze *hertelling* wordt uitgevoerd door het GSB waar het bewuste stemlokaal gevestigd was, onder verantwoordelijkheid van het VO. Daarnaast heeft het VO de bevoegdheid om tot een *herstemming* te besluiten. Dit moet gemeld worden aan de verantwoordelijke minister of college. Binnen dertig dagen vindt dan een nieuwe stemming plaats, met dezelfde partijen, kandidaten en kiezers.

Het VO onderzoekt de geloofsbrief en beslist of de benoemde als lid van dat orgaan wordt toegelaten. Daarbij gaat het VO na, of de benoemde aan de vereisten voor het lidmaatschap voldoet en geen met het lidmaatschap onverenigbare betrekking vervult. Het lidmaatschap van het vertegenwoordigend orgaan vangt aan zodra de beschikking omtrent de toelating aan de benoemde bekend is gemaakt. Als het VO besluit een benoemde niet toe te laten of een benoemde ziet af van diens lidmaatschap, wordt het CSB verzocht een nieuwe kandidaat te benoemen, waarna vervolgens de betreffende geloofsbrief door het VO wordt onderzocht.

4. Beveiligingsconcept

Het beveiligingsconcept voor het DHV bestaat uit verschillende elementen. In dit hoofdstuk worden de uitgangpunten en hoofdlijnen van het beveiligingsconcept geschetst. Nadere concretisering van de beveiligingsmaatregelen zijn in de vervolg hoofdstukken en in de bijlagen te vinden.

Het beveiligingsconcept voor het DHV is een onderdeel van een meer omvattende set aan maatregelen en procedures om de betrouwbaarheid en controleerbaarheid van de verkiezingsuitslag te vergroten. Andere maatregelen omvatten onder andere:

- Het verificatieproces op basis van de voorlopige uitslagen;
- Statistische controles op basis van stembureau- en gemeente-uitslagen;
- Toepassen van het door de Kiesraad opgestelde controle protocol;
- Het (gestructureerd en snel) online beschikbaar stellen van de uitslaggegevens.

Dit hoofdstuk richt zich primair op de uitgangspunten en maatregelen die direct betrekking hebben op het DHV. In Bijlage A: Overzicht dreigingsscenario's en maatregelen is een overzicht opgenomen waarin wordt aangegeven met welke maatregelen verschillende dreigingsscenario's worden ondervangen.

4.1. Uitgangpunten

Bij het opstellen van de basisarchitectuur en het bijbehorende ontwerp zijn verschillende uitgangspunten toegepast. Deze uitgangspunten zijn opgesteld aan de hand van aanbevelingen voortkomend uit de risicoanalyse die samen met het NCSC en de AIVD tussen oktober 2019 en maart 2020 is uitgevoerd. De onderstaande uitgangspunten zijn integraal toegepast op het ontwerp van het DHV. Aan de partijen die zich inschrijven op de aanbesteding zal worden gevraagd een nadere invulling te geven aan elk van deze uitgangspunten. De onderstaande uitgangspunten zijn in elk geval minimaal vereist.

- **Geen vertrouwen (Zero trust)**: geen systeem, netwerk of persoon kan op zichzelf als geheel vertrouwd worden aangemerkt;
- **Controleerbaarheid**: eenieder moet kunnen vaststellen dat het digitale hulpmiddel tot de juiste uitslag en zetelverdeling is gekomen;
- **Gelaagde beveiliging**: voor een risico wordt niet slechts één maatregel toegepast, maar een gelaagde set aan maatregelen;
- **Minimaliseer aanvalsoppervlakte**: het digitale hulpmiddel dient een zo klein mogelijk aanvalsoppervlakte te hebben;
- **Standaard beveiligd (Secure by default)**: het DHV dient standaard zo veilig mogelijk ontwikkeld, gebouwd en geconfigureerd te zijn;
- **Ketenveiligheid**: Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij hebben genomen om de aan hun opgelegde eisen te voldoen en ook hoe ze deze opgelegd hebben aan hun toeleveranciers en hoe ze dat controleren;
- **Detectie indringers (Intrusion detection)**: Implementeer detectiemiddelen zodat kwetsbaarheden en potentiële aanvallen gedurende de verkiezingen kunnen worden waargenomen door een Security Operations Center (SOC);
- **Incident respons**: Een uitgangspunt is dat de basisarchitectuur rekening houdt met het feit dat het systeem gecompromitteerd is of kan worden (Ga-uit-van-een-inbraak/Assume breach principe). In dit kader is het uitgangspunt dat er een incident respons protocol ontwikkeld wordt dat in gang kan worden gezet, indien er onverhoopt een incident plaatsvindt. Zodoende kan tijdig actie worden ondernomen en schade beperkt blijven;
- **Forensische paraatheid (Forensic readiness)**: Zorg ervoor dat de juiste loggegevens vastgelegd worden en goed beschermd zijn, zodat bij een forensisch onderzoek het bewijs ook juridisch houdbaar is en gebruikt kan worden voor juridische of strafrechtelijke procedures.

4.2. Randvoorwaarden

Naast de bovenstaande uitgangspunten zijn er enkele belangrijke randvoorwaarden van toepassing om op een veilige manier gebruik te kunnen maken van het DHV.

- Het DHV moet aantoonbaar voldoen aan relevante beveiligingsnormen en –kaders. De meest relevante beveiligingsnormen en -kaders zijn hieronder opgenomen. Deze normen en kaders zullen deels voor de aanbesteding (in het Programma van Eisen) en bij de realisatie (door de leveranciers) nadere concretisering krijgen. In paragraaf 4.7 Naleving en controle is daarnaast beschreven hoe wordt gecontroleerd of onderstaande beveiligingsnormen en -kaders daadwerkelijk worden toegepast door de verschillende partijen.
    - **Algemene beveiligingseisen:** Baseline Informatiebeveiliging Overheid (BIO), Voorschrift, Informatiebeveiliging Rijksdienst (VIR), CIS Top 20 Security Controls;
    - **Secure software development:** NCSC Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software, BIO Themadocument Applicatieontwikkeling, OWASP Application Security Verification Standard, Microsoft Security Development Lifecycle (alle uitgangspunten hieruit zijn integraal toegepast in het PvE);
    - **(web)applicaties**: NCSC ICT-beveiligingsrichtlijnen voor webapplicaties, BIO Themadocument Applicatieontwikkeling, OWASP Top 10 Web Application Security Risks, OWASP Application Security Verification Standard (ASVS);
    - **Hosting en infrastructuur**: BIO – Themadocument Huisvesting Informatievoorziening, NCSC Factsheet virtualiseer met verstand, BIO – Themadocument Serverplatform;
    - **Detectie**: NCSC Handreiking voor implementatie van detectie-oplossingen;
    - **Versleuteling & communicatie:** NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS), BIO – Themadocument Communicatievoorzieningen, NCSC Factsheet Veilig beheer van digitale certificaten;
    - **Toegangsbeveiliging**: BIO – Themadocument Toegangsbeveiliging, NCSC Factsheet gebruik tweefactorauthenticatie;
    - **Privacy**: Algemene Verordening Gegevensbescherming (AVG), Uitvoeringswet AVG;
    - **Inkoop**: CIP – Handleiding security proof inkopen, CIP – Wizard Security proof inkopen, CIP – Grip op beveiliging in inkoopcontracten;
    - **Detectie**: NCSC Handreiking voor implementatie van detectie-oplossingen.
- De GSB's/CSB's gebruiken het DHV en moeten voldoen aan een aantal vooraf gedefinieerde aansluitvoorschriften, tenzij het gebruik van het NHD in bepaalde situaties niet gewenst is. De aansluitvoorschriften zijn verwerkt in een set van voorwaarden en worden vastgesteld aan de hand van een verzameling van de belangrijkste beveiligingseisen die specifiek van toepassing zijn op de digitale risico's in het proces voor de vaststelling van de uitslag.

4.3. Actoren en verantwoordelijkheden

Verschillende actoren hebben een directe rol bij het ontwikkelen, beheren en gebruiken van het DHV. Deze actoren hebben ieder een eigen verantwoordelijkheid, zie in dit kader ook de verschillende ketenpartners zoals die zijn opgenomen in paragaaf 2.3. Het beveiligingsconcept van het DHV is erop gericht om een duidelijke verantwoordelijkheid verdeling aan te brengen, zowel in het systeem(ontwerp) als in de ontwikkel-, beheer- en gebruikersprocedures.

De volgende actoren worden onderscheiden met een korte beschrijving van de verantwoordelijkheden:

Gebruikersorganisatie (Gemeente/GSB/CSB)

- Verantwoordelijk voor het aanschaffen en veilig configureren van de werkstations op basis van een voorschrift van de Kiesraad;

- Verantwoordelijk voor het aansluiten van het werkstation op het (besloten) netwerk dat toegang biedt tot het DHV;
- Verantwoordelijk voor de fysieke- en logische toegangsbeveiliging tot het werkstation;
- Het opvolgen van beveiligingsincidenten die van toepassing zijn op de eigen GSB/CSB-omgeving. Hiertoe worden door het Security Operations Center (SOC) alerts verstuurd naar de GSB/CSB op basis van opgestelde monitoring use-cases;
- Verantwoordelijk voor het afhandelen van beveiligingsincidenten die zich hebben voorgedaan in de eigen omgeving;
- Het GSB/CSB neemt beveiligingsincidenten mee in het betrouwbaarheidsoordeel en doet daar, indien nodig, melding van in het PV;
- Kan wijzigingsverzoeken indienen bij de Kiesraad. Bijvoorbeeld: indien blijkt dat een onderdeel van het DHV niet gebruiksvriendelijk is, kan een gemeente een wijzigingsverzoek indienen.
- Dient aantoonbaar te voldoen aan de beveiligingsvoorschriften zoals opgesteld door de Kiesraad.

Kiesraad
- Is eigenaar van het DHV;
- Is verantwoordelijk voor de uitvoering van het functioneel beheer;
- Is verantwoordelijk voor acceptatie van het DHV (en beoordeeld of het aan de eisen is voldaan voor het gebruik);
- Stelt, in afstemming met het SOC, de use-cases en afhandelingsprocedure voor beveiligingsincidenten vast;
- Stelt het controleprotocol vast dat GSB/CSB toepassen bij gebruik van het DHV;
- Stelt het voorschrift op ten aanzien van gebruikersorganisatie, onder andere met betrekking tot het hardenen van werkstations;
- Stelt eisen aan de hostingpartij en softwareontwikkelaar ten aanzien van beveiliging;
- Stelt eisen aan de hostingpartij en softwareontwikkelaar ten aanzien van de OTAP-straat;
- Ziet toe of de hostingpartij en softwareontwikkelaar zich aan de eisen houden;
- Het opvolgen van beveiligingsincidenten die van toepassing zijn op de eigen omgeving én op de centrale infrastructurele componenten;
- Verantwoordelijk voor het afhandelen van beveiligingsincidenten die van toepassing zijn op de eigen omgeving én op de centrale infrastructurele componenten;
- Verantwoordelijk voor het ondersteunen van GSB's/CSB's bij het opvolgen van beveiligingsincidenten. Escaleert indien blijkt dat gebruikersorganisaties onvoldoende opvolging geeft aan beveiligingsincidenten;
- Rapporteert over beveiligingsincidenten die zich hebben voorgedaan in de eigen omgeving en de centrale infrastructurele componenten.

Security Operations Center (SOC)
- Verzorgt de technische infrastructuur, software en expertise die nodig is om de log-informatie te verwerken en daarbij de gewenste analyses uit te voeren;
- Monitort voortdurend op (technische) dreigingen die van toepassing zijn op de centrale infrastructurele componenten en rapporteert daarover aan de Kiesraad;
- Verantwoordelijk voor het onderhouden en beheren van het SOC;
- Verstuurt een melding naar de GSB/CSB bij het voordoen van een beveiligingsincident van toepassing op hun eigen omgeving;
- Verstuurt beveiligingsincidenten die als hoog-risico zijn aangemerkt naar de Kiesraad. De classificatie van de hoge-risico incidenten dient nader uitgewerkt te worden samen met het SOC;
- Verstuurt een melding naar de Kiesraad bij het voordoen van een beveiligingsincident van toepassing op haar eigen omgeving en centrale componenten.

Hostingpartij
- Verantwoordelijk voor het uitvoeren van het technisch beheer op de infrastructuur;
- Verantwoordelijk voor de fysieke beveiliging van de infrastructuur;

- Verantwoordelijk voor de logische beveiliging van de infrastructuur;
- Dient aantoonbaar te voldoen aan de beveiligingsvoorschriften zoals opgesteld door de Kiesraad.

Softwareontwikkelaar

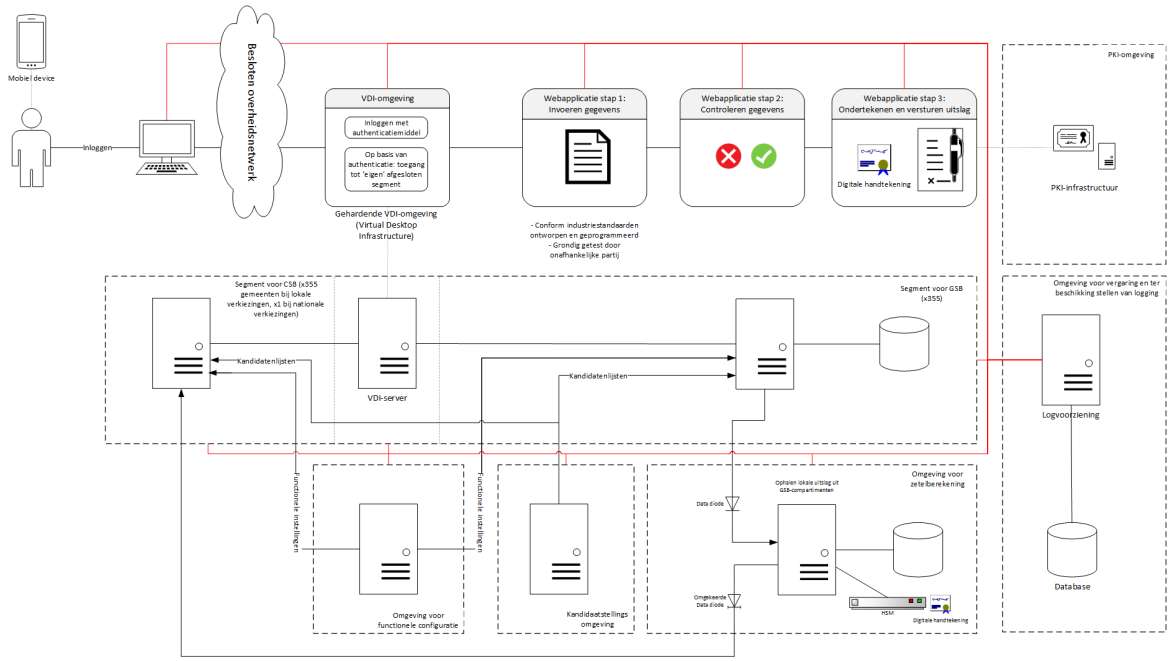
- Verantwoordelijk voor het veilig ontwikkelen van de software (security by design, privacy by design);
- Verantwoordelijk voor het veilig uitvoeren van het applicatiebeheer (waaronder doorontwikkelen) van de software;
- Dient aantoonbaar te voldoen aan de beveiligingsvoorschriften zoals opgelegd door de Kiesraad.
- Verantwoordelijk voor het uitvoeren van performance en stresstesten en het aantonen dat de software kwaliteitseisen.

Helpdesk

- Verantwoordelijk voor het bieden van ondersteunen aan gebruikersorganisaties ten behoeve van het gebruik en de implementatie van het DHV.

4.4. Basisarchitectuur

In de onderstaande figuur is de basisarchitectuur op hoofdlijnen gevisualiseerd vanuit het perspectief van het proces voor de vaststelling van de uitslag.



Figuur 5: Visualisatie technische opzet.

Een vergrote weergave is opgenomen in de Bijlage D: Vergrote weergave afbeeldingen en tabellen.

In de bovenstaande visualisatie zijn enkele belangrijke ontwerpbeslissingen uitgewerkt. In de bovenste rij zijn de stappen vanuit het perspectief van een gebruiker toegelicht. De gebruiker (GSB/CSB) logt allereerst in op een werkstation van het GSB/CSB. Vervolgens wordt er een verbinding gemaakt met een (besloten) landelijk netwerk. Nadat er verbinding is gemaakt met het (besloten) landelijk netwerk, wordt er een sessie gestart in de Virtuele Desktop omgeving (VDI). Deze VDI-omgeving biedt de medewerkers van het GSB/CSB toegang tot een eigen afgescheiden compartiment. Vervolgens kan uitsluitend vanuit de VDI-sessie de webapplicatie worden benaderd die in een eigen (GSB/CSB) compartiment draait. In de webapplicatie kunnen gegevens worden ingevoerd, gecontroleerd, vastgesteld en digitaal ondertekend. In dit ontwerp zijn enkele

belangrijke afwegingen ten aanzien van beveiliging integraal verwerkt. In de visualisatie is een logvoorziening opgenomen waarmee verschillende loggegevens (de rode lijn in de afbeelding) centraal worden verzameld en opgeslagen. De centrale logvoorziening maakt het mogelijk dat met behulp van een Security Operations Center (SOC) het DHV actief wordt gemonitord. In de volgende paragrafen worden twee belangrijke afwegingen nader toegelicht ten aanzien van de werkstations en de netwerkverbinding.

4.4.1. Maatregelen ten aanzien beveiliging werkstation

Om de mogelijkheden van een aanvaller via het werkstation van het GSB of CSB op het DHV te beperken wordt een combinatie van verschillende maatregelen voorzien in het ontwerp. Deze maatregelen helpen om de kans en impact op dergelijke aanvallen te beperken.

Maatregel 1: toegang via gehardende Virtuele Desktop omgeving
De centrale DHV-webapplicatie wordt niet direct ontsloten naar de gebruiker. De gebruiker verkrijgt via de centrale VDI-omgeving van het DHV toegang tot de DHV-webapplicatie. Authenticatie tot de DHV-omgeving en -applicatie vindt plaats middels twee-factor-authenticatie. De VDI-omgeving vormt hiermee een beveiligde tussenlaag tussen het werkstation van de gebruiker en de DHV-webapplicatie. Bij dergelijke VDI-oplossingen, logt een gebruiker doorgaans in met twee-factor-authenticatie op de VDI-omgeving, waarna de gebruiker automatisch wordt ingelogd op de webapplicatie (bijvoorbeeld door Single Sign-On technieken). De exacte implementatie is echter afhankelijk van de gekozen oplossing.

De VDI-omgeving wordt centraal beheerd en gemonitord (zie ten aanzien van monitoring tevens paragraaf 6.2). Dit maakt het mogelijk eenduidige hardening toe te passen (zoals het centraal doorvoeren van beveiligingsupdates) waardoor de aanvalsmogelijkheden voor een kwaadwillende sterk worden beperkt. Ten aanzien van de uitvoerbaarheid voor de gebruikers wordt een beperkte impact verwacht: de VDI-omgeving kan immers zo worden ingericht dat voor een eindgebruiker weinig tot geen verschil merkbaar is ten opzichte van alleen een webapplicatie. Voor de gebruiker is de beschikbaarheid van de VDI-omgeving wel van belang, aangezien de gebruiker zonder de VDI-omgeving niet kan werken in de DHV-applicatie. Voor het beheer van de VDI-omgeving zijn wel aanvullende handelingen en processen vereist voor de Kiesraad. Hierbij kan op hoofdlijnen worden gedacht aan het inrichten van functionele beheerprocessen en/of een servicedesk door de Kiesraad.

Maatregel 2: gebruik gehardende image op de werkstations die centraal beschikbaar wordt gesteld
Om eventuele beveiligingsproblemen in de software van het werkstation van de gebruiker te ondervangen wordt een besturingssysteem als een image beschikbaar gesteld aan de gebruikersorganisatie. De gebruikersorganisaties moeten deze image gebruiken op werkstations t.b.v. DHV. Deze image wordt, voordat deze beschikbaar wordt gesteld, gehardend en voorzien van beveiligingsinstellingen (bijvoorbeeld: dat met deze image in beginsel geen reguliere verbinding met internet mogelijk is, enkel de verbinding via besloten netwerk naar DHV is toegestaan). Het is daarnaast technisch mogelijk om een gemeente-specifiek certificaat op te nemen in de image. Dit certificaat is, in aanvulling op IP-whitelisting, een extra toegangscontrole voor toegang tot de VDI-omgeving.

Deze maatregel verkleint verder de kans dat onvoldoende gehardende werkstations worden gebruikt om het DHV te gebruiken. Daarnaast biedt deze maatregel het voordeel dat er geen data lokaal op de werkstations blijft staan.

Zowel voor de Kiesraad als voor de gebruikersorganisaties zitten aan deze maatregel consequenties qua kosten en uitvoerbaarheid verbonden. De Kiesraad moet de gehardende image verzorgen, testen en veilig ter beschikking stellen. Gebruikersorganisaties moeten ervoor zorgen dat zij de image (tijdig) op de beoogde werkstations werkend krijgen.

Maatregel 3: alleen werkstations die conform een procedure worden beheerd en opgeslagen mogen worden gebruikt
Deze maatregel geeft een extra waarborg dat het werkstation, voordat dit wordt ingezet, overeenkomstig de gewenste procedures wordt beheerd. De werkstations worden hierbij overeenkomstig de voorschriften van de Kiesraad voorbereid. Aangezien gebruik wordt gemaakt van centraal gedistribueerde images, kan voor de hardening worden volstaan met een beperkte set aan aandachtspunten bij het inrichten van het werkstation (bijv. geen onveilige randapparatuur aansluiten) en instructies voor de opslag.

Deze maatregel is procedureel van aard, waardoor de kans bestaat dat gebruikersorganisaties de voorschriften niet correct toepassen. Om de kans hierop te verkleinen, kan via controleprotocol en eventuele audit nagegaan worden of de voorschriften correct worden opgevolgd.

Conclusie/advies
Het verdient de voorkeur dat de drie beschreven maatregelen toegepast worden. De verwachting is echter dat dit wel uitvoeringstechnisch complex is.

De volledig gehardende VDI-omgeving is met afstand de belangrijkste maatregel van de drie beschreven maatregelen. 'Schone' werkstations bij de gemeente zijn daarnaast een goede en eenvoudig te realiseren maatregel.

De maatregelen dienen volgens onderstaande tabel te worden toegepast:

Maatregel	**Belang**
Gehardende VDI (maatregel 1)	Vereist
Gehardende image bij gemeente (maatregel 2)	Toepassen indien haalbaar
Beheer werkstation conform richtlijnen Kiesraad (maatregel 3)	Dringend geadviseerd

4.4.2. Maatregelen tegen aanvallen via het netwerk

Bij een centraal ontsloten systeem als het DHV moet rekening worden gehouden met een aanvallen via het netwerk. In de basisarchitectuur zijn reeds maatregelen verwerkt die helpen om de kans en impact op dergelijke aanvallen via het netwerk te beperken. De verschillende maatregelen die worden voorzien worden hieronder beschreven.

Maatregel 1: DHV uitsluitend beschikbaar via besloten overheidsnetwerk
Om het aanvalsoppervlak te verkleinen wordt het DHV ontsloten via een besloten (semi)overheidsnetwerk. Dit betekent dat uitsluitend de werkstations die in verbinding staan met het besloten netwerk, toegang hebben tot het DHV. Een nadere toelichting met betrekking tot het beoogde besloten netwerk en de bijbehorende aansluitmogelijkheden wordt in paragraaf 6.1 beschreven.

Het besloten overheidsnetwerk dient te worden aangesloten op het Diginetwerk, dit netwerk is niet direct vanaf het internet toegankelijk. Zodoende is het voor ongeautoriseerde aanvallers niet mogelijk om aanvallen via het internet uit te voeren op de omgeving (zoals DDoS-aanvallen). Het is alleen mogelijk om vanaf partijen die aangesloten zijn op het besloten netwerk dergelijke aanvallen uit te voeren.

Maatregel 2: DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen
Deze technische maatregel zorgt ervoor dat uitsluitend vooraf aangemelde GSB/CSB IP-adressen een verbinding kunnen maken met het DHV (*IP-whitelisting*). Praktisch kunnen dit de externe IP-adressen van gemeenten zijn binnen het gekozen besloten netwerk. Merk op dat dit niet de internet-facing externe IP-adressen betreffen, maar de externe IP-adressen binnen het domein van het besloten netwerk. Door IP-whitelisting is het voor aanvaller niet mogelijk om via een ander IP-adres, welke niet is aangemeld, het DHV te benaderen.

Het toepassen van IP-whitelisting brengt enkele aandachtspunten ten aanzien van uitvoerbaarheid met zich mee. De gebruikersorganisatie moeten ervoor zorgen dat er een actueel overzicht is van de gebruikte IP-adressen en deze IP-adressen dienen geregistreerd te worden om toegang te verkrijgen tot het DHV.

Maatregel 3: gecompartimenteerde omgeving
Binnen het DHV wordt compartimentering toegepast, zodat aan ieder GSB en CSB een eigen afgescheiden omgeving toegekend wordt waarbinnen de gebruikersfunctionaliteiten en data zich bevinden. De impact van een eventuele succesvolle aanval op een GSB-compartiment blijft hierdoor beperkt tot het specifieke compartiment.

In de ontwerpplaat (Figuur 5) zijn de compartimenten aangeduid met stippellijnen. Het uitgangspunt hierbij is dat personen met toegang tot een bepaalde GSB/CSB-omgeving geen toegang krijgen tot een andere GSB/CSB-omgeving. Tevens worden voor andere belangrijke functie in het DHV, zoals de zetelberekening en de omgeving voor functioneel beheer, een apart compartiment voorzien. Een extra maatregel die worden toegepast om een compartiment af te schermen van de andere compartimenten is door het plaatsen van data diodes die ervoor zorgen dat gegevens enkel een bepaalde kant op kunnen gaan. Het toepassen van data diodes wordt voorzien bij het compartiment voor de zetelverdeling die tevens op een aparte server wordt ondergebracht.

Maatregel 4: Intrusion Prevention maatregelen
Aanvallers met netwerktoegang tot het DHV kunnen het systeem via het netwerk proberen aan te vallen. Aanvallen kunnen daarbij gericht zijn op de infrastructuur (zoals servers), maar ook op de webapplicatie zelf. Hier worden ook DDoS-aanvallen onder gerekend. Om dergelijke aanvallen te signaleren wordt voorzien in brede logging en monitoring van het DHV. In paragraaf 6.2 wordt nader ingegaan op logging en monitoring. Om direct weerstand te beiden tegen netwerkaanvallen wordt een Intrusion Prevention Systeem (IPS) ingezet. Deze IPS heeft daarbij verschillende beschermende functies. Netwerk gebaseerde aanvallen worden met (next generation) firewall functionaliteiten afgevangen en door het IPS worden ondervangen met behulp van Web Application Firewall (WAF) functionaliteiten. De gebruikte IPS dient over al deze functionaliteiten te bezitten, zodat het DHV op verschillende niveaus kan worden beschermd.

Met de implementatie van het IPS wordt tevens voorzien dat de loginformatie die met het IPS wordt gegenereerd beschikbaar komt voor het SOC, zodat netwerk gebaseerde aanvallen snel gedetecteerd kunnen worden. Met de implementatie van het IPS worden aanvullende kosten voorzien, onder meer licentie- en installatiekosten.

Conclusie/advies
Het uitgangspunt is dat alle vier voorgenomen maatregelen worden geïmplementeerd bij de realisatie van het DHV. Anders dan bij de maatregelen ten aanzien van het werkstation dienen deze maatregelen integraal te worden doorgevoerd om aan de gewenste beveiligingsuitgangspunten van het DHV te voldoen.

4.5. Functiescheiding en gebruikersrollen

Bij functiescheiding worden de verantwoordelijkheden en bevoegdheden binnen de organisatie over verschillende functionarissen verdeeld. Door functiescheiding wordt de afhankelijkheid van individuele functionarissen geminimaliseerd en wordt vermenging van bevoegdheden voorkomen. Ook bij de totstandkoming van de verkiezingsuitslag is het belangrijk dat de verantwoordelijkheden en bevoegdheden niet bij één persoon worden ondergebracht. In relatie tot het verkiezingsproces wordt hierbij ook gesproken over het vier-ogen principe.

De implementatie van functiescheiding komt in het DHV op verschillende onderdelen terug. Daarbij kan onderscheid gemaakt worden tussen de functionele implementatie voor de gebruikers en de implementatie ten aanzien van het technisch- en applicatiebeheer. De in deze paragraaf

beschreven gebruikersrollen hebben betrekking op de functionele implementatie en komen terug in hoofdstuk 5 ten aanzien van de functionele-opzet. De functiescheiding ten aanzien van technisch- en applicatiebeheer is nader beschreven in hoofdstuk 7 Beheer.

In paragraaf 4.4 is bij de basisarchitectuur ingegaan op de compartimentering van het DHV, zodat elke instantie GSB, CSB en de Kiesraad (als functioneel beheerorganisatie) over een eigen omgeving beschikt. Met de functionele scheiding wordt een scheidingslaag aangebracht in de programmatuur door het definiëren van bepaalde gebruikersrollen voor de verschillende functies binnen het DHV. De gebruiker krijgt enkel de functionaliteiten die voor de rol van de gebruiker relevant zijn. De gebruiker heeft geen toegang tot functionaliteiten die horen bij een andere rol.

4.5.1. Functiegroepen en authenticatiemiddel

Binnen het DHV worden meerdere typen (functionele)gebruikers onderscheiden:

- De beheerder(s) die zorgen dat de (verkiezings)configuratie en het gebruikersbeheer zijn doorgevoerd;
- De gebruikers die binnen GSB/CSB-bestanden en documenten voorzien van een digitale handtekening of waarmerk;
- De gebruiker(s) die betrokken zijn bij de invoer van uitslaggegevens en het bepalen van de verkiezingsuitslag.

Voor het GSB, CSB en de Kiesraad worden binnen deze groepen afzonderlijke gebruikersrollen gedefinieerd met daaraan gekoppeld de functionele mogelijkheden die bij die rol horen.

Afhankelijk van onder welke gebruikersgroep een gebruiker valt wordt een bepaalde authenticatiemiddel toegepast bij het inloggen bij het DHV. Voor het DHV wordt twee-factor-authenticatie toegepast waarbij als eerste factor een persoonsgebonden gebruikersnaam/wachtwoord wordt toegepast en een eenmalige code (oftewel 'one-time password' (OTP)) dan wel een certificaat als tweede factor wordt gebruikt.

Er is gekozen om voor de beheerder(s) en ondertekenaar(s) een zwaarder authenticatiemiddel in te zetten dan voor de invoerders. Hiervoor zijn een aantal argumenten:

- De gevolgen van de handelingen van beheerder(s) en ondertekenaar(s) hebben potentieel veel meer rechtsgevolgen. Dit rechtvaardigt de inzet van een zwaar middel als eHerkenning (EH) betrouwbaarheidsniveau 3 of 4. Daarnaast zijn de gebruikers van deze typen langer van tevoren bekend. Dit maakt het organiseren van toegang via EH mogelijk. In paragraaf 4.6 wordt nader ingegaan op het toepassen van eHerkenning;
- De invoerder(s) vergen een hoge mate van flexibiliteit qua accounts. Deze kunnen op het laatste moment nog worden toegevoegd of verwijderd worden. Dit is niet mogelijk met EH.

4.5.2. Gebruikersrollen

De volgende gebruikersrollen met bijbehorende functiemogelijkheden worden in het DHV onderscheiden binnen het GSB-compartiment:

- Invoerder GSB;
- Lid GSB;
- Voorzitter en vicevoorzitter GSB;
- Beheerder GSB.

De volgende gebruikersrollen met bijbehorende functiemogelijkheden worden in het DHV onderscheiden binnen het CSB-compartiment:

- Invoerder CSB;
- Lid CSB;
- Voorzitter en vicevoorzitter CSB;
- Beheerder CSB.

De volgende gebruikersrol met bijbehorende functiemogelijkheden wordt in het DHV onderscheiden binnen het VA-compartiment:

- Functioneel beheerder.

In paragraaf 5.1 wordt de nadere functionele invulling van de verschillende rollen beschreven.

Strikte implementatie van functiescheiding houdt ook in dat één persoon niet meerdere rollen binnen het DHV kan vervullen. Het is van belang zich te realiseren dat voor het vaststellen van een verkiezingsuitslag, voor het GSB en CSB elk, minimaal vijf verschillende personen in het DHV geautoriseerd dienen te zijn. Het gaat hierbij om minimaal twee invoerders, één GSB/CSB lid, één (vice)voorzitter GSB en één beheerder.

4.5.3. Functie in mandaat

Het is voorstelbaar dat de handelingen in het DHV niet door de formele GSB/CSB-functionaris wordt uitgevoerd, maar dat deze GSB/CSB-functionaris dit heeft gemandateerd aan een ander persoon, bijvoorbeeld aan ondersteunende medewerkers van het GSB of CSB. Het DHV sluit niet uit dat autorisaties kunnen worden ingesteld op andere personen dan de formele GSB/CSB-functionaris. Als dit formeel juridisch een vereiste gaat worden, dan zal bij de keuze van het authenticatiemiddel en de bijbehorende registratieprocedure hier rekening mee gehouden moeten worden.

4.5.4. Loggen gebruikershandelingen

Om achteraf nog te kunnen vaststellen welke handelingen er door gebruikers zijn uitgevoerd in het DHV vindt logging plaats. Het loggen van handelingen van gebruikers is een van de verschillende logging-onderwerpen die binnen het DHV zijn voorzien. In paragraaf 6.2 wordt nader ingegaan op de verschillende vormen van logging en de wijze van monitoring.

De handelingen die worden vastgelegd in de logging zijn herleidbaar tot geregistreerde gebruikers en (als de wijze van registratie overeenkomstig de voorschriften is uitgevoerd) tot één persoon. Dit betekent evenwel dat er in het kader van monitoring en (mogelijk) onderzoek persoonsgegevens van gebruikers worden verwerkt. De verwerking van persoonsgegevens dient binnen de kaders van de AVG en de uitvoeringswet AVG plaats te vinden en waar dat nodig is dient in het DHV privacy beschermende maatregelen te worden geïmplementeerd. In paragraaf 8.2 wordt nadere stilgestaan bij de verwerking van persoonsgegevens in het DHV.

4.5.5. Integriteitsverklaring of VOG gebruikers

Het uitgangspunt is dat gemeenten en de Kiesraad zelf zorgen dat de GSB- en CSB-gebruikers van het DHV integer zijn. Hierbij kan worden gedacht aan het toepassen van verklaringen zoals een integriteitsverklaring of VOG.

4.6. eHerkenning

Afhankelijk van de rol die een persoon heeft toegekend gekregen binnen het DHV is een bepaalde (hogere of lagere) mate van zekerheid over de identiteit van die persoon vereist alvorens die persoon bepaalde taken kan uitvoeren. Voor de rollen met taken waarvoor een hoge mate van zekerheid over de identiteit van de persoon vereist is (het aanmaken van gebruikers en het digitaal ondertekenen van bestanden), zal gebruik worden gemaakt van het authenticatiemiddel eHerkenning.

In essentie regelt eHerkenning de digitale herkenning (authenticatie) en controleert het de digitale bevoegdheid (autorisatie) van personen. Concreet: Is de persoon wie hij zegt dat hij is? En mag hij doen wat hij doet? eHerkenning controleert en bevestigt dit. eHerkenning kent vijf betrouwbaarheidsniveaus, elk met een verschillend niveau van identificatie en authenticatie.

Niveau	Identificatie gebruiker	Authenticatie gebruiker
EH1	De relatie tussen de aanvrager en gebruikersorganisatie wordt alleen gecontroleerd aan de hand van de Kamer van Koophandel-registratie.	Gebruikersnaam en wachtwoord
EH2	De relatie tussen de aanvrager en gebruikersorganisatie wordt gecontroleerd aan de hand van de Kamer van Koophandel-registratie.	Gebruikersnaam en (sterk) wachtwoord
EH2+	De relatie tussen de aanvrager en gebruikersorganisatie wordt gecontroleerd aan de hand van de Kamer van Koophandel-registratie.	Gebruikersnaam en wachtwoord, aangevuld met een sms-code of een pincode (via token)
EH3	De relatie tussen de aanvrager en gebruikersorganisatie wordt gecontroleerd aan de hand van de Kamer van Koophandel-registratie. De persoon voor wie het middel is dient zich fysiek te legitimeren met een origineel identiteitsbewijs[3].	Gebruikersnaam en wachtwoord, aangevuld met een sms-code of een pincode (via token)
EH4	De relatie tussen de aanvrager en gebruikersorganisatie wordt gecontroleerd aan de hand van de Kamer van Koophandel-registratie. Persoonsgegevens worden gecontroleerd door op locatie het originele identiteitsbewijs te tonen. Zowel de wettelijk vertegenwoordiger, dan wel de machtigingenbeheerder en de betreffende persoon voor wie het middel is moeten zich fysiek legitimeren met een origineel identiteitsbewijs[4].	PKI-certificaat

Uit bovenstaande tabel blijkt dat alleen op de betrouwbaarheidsniveaus EH3 en EH4 zekerheid is over de identiteit van de gebruiker.

4.6.1. Huidig gebruik eHerkenning door gemeenten

Vrijwel alle gemeenten beschikken over eHerkenningsaccounts, met name voor het gebruik in het sociale domein (de SUWI-keten). Deze eHerkenningsaccounts hebben naar verwachting geen nut voor het gebruik binnen het DHV, omdat deze accounts maximaal het betrouwbaarheidsniveau EH2+ zullen hebben en persoonsgebonden zijn. De houders van deze accounts zijn overwegend andere personen dan de personen die bij de verkiezingen betrokken zijn.

4.6.2. Gewenst gebruik eHerkenning binnen het DHV

Met het DHV willen we een verbetering doorvoeren ten opzichte van de huidige applicatie voor het vaststellen van de verkiezingsuitslag (OSV), welke gebruik maakt van één-factor-authenticatie zonder vooraf gebruikers in persoon te identificeren. Dit komt overeen met een betrouwbaarheidsniveau van maximaal EH2+. eHerkenning zal binnen het DHV gebruikt gaan worden voor taken waarbij een hoge mate van zekerheid over de identiteit van de persoon (en dus een identificatie in persoon) vereist is. Dit betekent dus een betrouwbaarheidsniveau van EH3 of EH4.

Voor het vaststellen van de verkiezingsuitslag met behulp van het DHV zal eHerkenning gebruikt worden door:

- Beheerders GSB/CSB: voor het aanmaken van de gebruikers;
- (vice-)Voorzitter GSB/CSB: voor het digitaal ondertekenen van (digitale) bestanden.

Uitgangspunt hierbij is dat zowel het aanmaken van gebruikers of de ondertekening van bestanden terug te leiden moet zijn naar één unieke persoon, de beheerder GSB/CSB respectievelijk (vice-) voorzitter GSB/CSB.

Aanmaken gebruikers

[3] In de markt zijn op dit moment ontwikkelingen gaande waarbij het fysiek tonen van originele identiteitsbewijzen vervangen kan worden door een zogenaamde 'online onboarding'. Hierbij wordt door een combinatie van NFC (near field communication)-technologie en videostreaming een proces ingericht waarbij geen fysiek contact meer nodig is. Naar verwachting is in Q3/Q4 2020 dit proces goedgekeurd door het Agentschap Telecom.

[4] Idem.

Voor de beheerders GSB/CSB is eHerkenning vereist omdat zij de taak hebben gebruikersaccounts aan te maken voor de invoerders en leden van GSB/CSB die bijv. de stembureau-uitslag invoeren en uitslagen accorderen binnen het DHV.

Digitaal ondertekenen
Voor de (vice-)voorzitter GSB/CSB is eHerkenning vereist voor het digitaal ondertekenen van bestanden (bijv. concept proces-verbaal met de gemeente-uitslag). eHerkenning heeft geen eigen ondertekendienst, deze moet separaat geregeld worden. Verschillende leveranciers van ondertekendiensten gaan hier verschillend mee om:

- Via een smartcard met daarop een certificaat: Hiervoor moeten zowel in de (gehardende) werkplek als in de VDI bepaalde USB-poorten opengezet worden voor het koppelen van de cardreader. Dit is niet gewenst;
- Via een hardware security module (HSM): Deze HSM staat doorgaans fysiek bij een Certificaatautoriteit (CA) of een andere bevoegde instantie. De HSM is sterk beveiligd en slaat de certificaten van gebruikers op. Het unlocken van de eigen persoonsgebonden certificaten die in de HSM staan, gebeurt via de telefoon (smart-token met twee- of drie-factor-authenticatie).

Bij EH4 krijgt de betreffende gebruiker drie certificaten: voor authenticatie, voor ondertekening (signing) en encryptie. Voor signing-certificaten is de oplossing met een HSM al redelijk in gebruik. Voor authenticatie-certificaten is dit minder het geval. Hier wordt vaak de combinatie gemaakt met een toegangspas zoals de Rijkspas 3. Een authenticatie-certificaat in een HSM is echter wel mogelijk.[5]

Alternatief: waarmerken door middel van een PKIO-systeemcertificaat
In plaats van het digitaal ondertekenen van een bestand met een gekwalificeerde elektronische handtekening door de (vice-)voorzitter kan ook overwogen worden deze te vervangen door het plaatsen van een waarmerk. Een waarmerk is technisch gezien hetzelfde als een gekwalificeerde elektronische handtekening, maar dan op basis van een certificaat op organisatieniveau. Hierbij zijn twee alternatieven te onderkennen:

- Iedere gebruikersorganisatie heeft een *eigen systeemcertificaat*, hierbij zijn er dus 350-400 systeem-certificaten nodig. Dit alternatief geeft de zekerheid dat het bestand niet gemanipuleerd is én de zekerheid dat het bestand door de betreffende GSB/CSB is aangemaakt;
- Het hele DHV gebruikt *één systeemcertificaat* voor het waarmerken van documenten. Dit alternatief geeft de zekerheid het bestand niet gemanipuleerd is, maar het is niet meer duidelijk door welke GSB/CSB het bestand is aangemaakt.

4.6.3. Conclusie/advies

Voor de beheerder GSB/CSB volstaat betrouwbaarheidsniveau EH3, er is dan immers sprake van tot op de persoon herleidbare identificatie.

Voor de (vice-)voorzitter GSB/CSB zijn er twee voor de hand liggende alternatieven:

- Betrouwbaarheidsniveau EH3, en het gebruik van het PKIO-systeemcertificaat voor het digitaal waarmerk van de uitvoergegevens;
- Betrouwbaarheidsniveau EH4 (met een PKIO-persoonsgebonden certificaat), waarbij het signing-certificaat wordt gebruikt met een ondertekendienst.

Voor de opslag van certificaten is in alle situaties een HSM de methode die geprefereerd wordt boven het gebruik van een smartcard. Het gebruik van smartcards maakt het noodzakelijk om

[5] De ontwikkelingen op het gebied van digitale authenticatie en signing zijn sterk aan het ontwikkelen. De mogelijkheden om EH te gebruiken worden relatief snel laagdrempeliger en de verspreiding groter. Het herijken van de inzichten rondom authenticatie en signing dient dan ook met enige regelmaat plaats te vinden.

USB-devices aan de werkstations te koppelen en deze ook binnen de VDI-omgeving beschikbaar te maken. Dit vergroot het aanvalsoppervlak van het DHV en maakt de aansluiting complexer.

Gemeenten hebben geen ervaring met een betrouwbaarheidsniveau boven EH2+, dus meteen de stap maken naar EH4 betekent een hogere inspanning ten aanzien van de implementatie. Door ontwikkelingen als online onboarding is de stap naar EH4 op korte termijn veel kleiner dan wordt aangenomen. Voor de (vice)voorzitter is het gebruik van EH4 dan ook de voorkeursoplossing. Slechts indien dit voor onoverbrugbare uitvoeringsproblemen gaat leiden, dan is de stap naar EH3 aan de orde. Bij EH3 is de keuze om wel persoonsgebonden PKIO-certificaten voor signing in te zetten een onlogische keuze. Het gebruik van PKIO-systeemcertificaten ligt bij de keuze voor EH3 meer voor de hand.

4.7. Naleving en controle

Het ontwerp van het DHV bevat diverse belangrijke beveiligingsnormenkaders, -voorschriften, -richtlijnen en eisen die van toepassing zijn op verschillende partijen. Indien een van de partijen niet voldoet aan een beveiligingseis, kan dit resulteren in beveiligingsrisico's. Het is van belang om vast te stellen dat de voorgeschreven maatregelen daadwerkelijk door iedere partij worden toegepast. Het uitgangspunt is derhalve dat de Kiesraad controleert of de van toepassing zijnde beveiligingskaders door de verschillende partijen worden nageleefd. Hiertoe dient de Kiesraad een *right to audit* in de contracten met externe partijen op te nemen en afspraken vast te leggen met de overige partijen. De Kiesraad kan controleren of de beveiligingseisen worden nageleefd door zelf controles uit te voeren, controles te laten uitvoeren door derde partijen of burgers en door te steunen op assurancerapportages.

4.7.1. Controlematrix

In de onderstaande matrix is per partij aangegeven aan welke beveiligingskaders zij dienen te voldoen. Daarnaast is beschreven hoe wordt getoetst of de kaders daadwerkelijk worden nageleefd, op wiens initiatief wordt getoetst en aan wie wordt gerapporteerd over de toetsing.

Tabel 1: Controlematrix met een beschrijving van de wijze waarop de verschillende partijen aantoonbaar dienen te voldoen aan de beveiligingskaders en -eisen.

Partij	Moeten voldoen aan (een specificatie van) de volgende beveiligingskaders	Wordt getoetst d.m.v.	Op initiatief van	Gerapporteerd aan	Opmerking
Gebruikers-organisatie (primair Gemeenten)	BIO (Baseline Informatiebeveiliging Overheid)	Self-assessment in het kader van de ENSIA	Gemeenten/ VNG	College van B&W	Er kunnen eventueel vragen worden toegevoegd aan de ENSIA vragenlijst in het kader van het DHV.
				Gemeenteraad	
	Voorschrift/aansluitvoorwaarden Veilige Verkiezingen, dit bevat: - Voorschrift voorbereiden werkstations - Voorschrift veilige opslag werkstations - Voorschrift uitgifte autorisaties - Voorschrift hardenen werkstations (invulling afhankelijk van keuze voor vooraf gehardende images)	Self-assessment normenkader Veilige Verkiezingen	Kiesraad	Kiesraad	Kan eventueel worden toegevoegd aan de ENSIA-normatiek
		Optioneel: audit op aanvraag, uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	

Partij	Moeten voldoen aan (een specificatie van) de volgende beveiligingskaders	Wordt getoetst d.m.v.	Op initiatief van	Gerapporteerd aan	Opmerking
	AVG en UAVG	Controle door Autoriteit Persoonsgegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	
Verkiezings-autoriteit / Kiesraad	BIO (Baseline Informatiebeveiliging Overheid)	Self-assessment in het kader van de jaarlijkse In-Control Verklaring	Kiesraad / BZK	Kiesraad / BZK	
	Voorschrift/normenkader Veilige Verkiezingen, bevat o.a.: - Voorschrift voorbereiden werkstations - Voorschrift veilige opslag werkstations - Voorschrift uitgifte autorisaties - Voorschrift hardenen werkstations (invulling afhankelijk van keuze voor vooraf gehardende images)	Audit uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	
Software-ontwikkelaar	Programma van Eisen (PvE) softwareontwikkelaar. In dit PvE zitten o.a. eisen over: - Voldoen aan de BIO d.m.v. statement of compliance - Secure Software Development - Wijzigingenbeheer - Vierogenprincipe - Patchmanagement - Hardening - Toegangsbeheer - Logging Het PvE is gebaseerd op de volgende kaders en best practices: 1) BIO Themadocument Applicatieontwikkeling 2) OWASP Top 10 Web Application Security Risks 3) OWASP Application Security Verification Standard (ASVS) 4) NCSC Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software 5) NCSC ICT-beveiligingsrichtlijnen voor webapplicaties	Audit uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	Een auditor kan worden ingeschakeld om te controleren of de softwareontwikkelaar voldoet aan de eisen uit het PvE.
		Pentesten, secure code reviews, configuratiereviews, redteaming en andere beveiligingstesten uitgevoerd door een gekwalificeerde marktpartij	Kiesraad	Kiesraad	Deze testen worden op reguliere basis uitgevoerd en ten minste voorafgaand aan iedere verkiezing.
		Pentesten, secure code reviews, configuratiereviews en andere beveiligingstesten uitgevoerd door burgers	Kiesraad	Kiesraad	Dit kan worden vormgegeven d.m.v. een zogenaamde hackwedstrijd/ hackathon/ hackmarathon.
		Responsible Disclosure procedure	Burgers	Kiesraad	Via deze procedure kunnen burgers zelf kwetsbaarheden melden op een gecontroleerde manier.
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	

Partij	Moeten voldoen aan (een specificatie van) de volgende beveiligingskaders	Wordt getoetst d.m.v.	Op initiatief van	Gerapporteerd aan	Opmerking
Hostingpartij (aanname: tevens beheerder datacenter)	Programma van Eisen (PvE) hostingpartij. In dit PvE zitten o.a. eisen over: - Voldoen aan de BIO d.m.v. statement of compliance - Veilige inrichting datacenter - Wijzigingenbeheer infrastructuur - Netwerkbeveiliging - Encryptie - Hardening infrastructuur - Vierogenprincipe - Patchmanagement - Toegangsbeheer - Logging Het PvE is gebaseerd op de volgende kaders en best practices: 1) BIO – Themadocument Huisvesting Informatievoorziening 2) BIO – Themadocument Communicatievoorzieningen 3) BIO – Themadocument Toegangsbeveiliging 4) NCSC Factsheet virtualiseer met verstand 5) NCSC Factsheet gebruik tweefactorauthenticatie 6) NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) 7) NCSC Factsheet Veilig beheer van digitale certificaten	Audit uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij). Eventueel in de vorm van een ISAE-3402 Type 2 verklaring.	Kiesraad	Kiesraad	In de ideale situatie geeft de hostingpartij zelf al jaarlijks een ISAE3402-verklaring af met een dekkend normenkader en dekkende scope. Zo niet, dan moet dit worden afgedwongen in de eisen.
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	
SOC (uitgaande van overheidspartij)	BIO	Self-assessment in het kader van de jaarlijkse In-Control Verklaring	SOC	Kiesraad	
	Nader op te stellen programma van eisen voor logging en monitoring, gebaseerd op o.a.: 1) NCSC Handreiking voor implementatie van detectie-oplossingen. 2) Use-cases monitoring zoals opgesteld door de Verkiezingsautoriteit / Kiesraad	Optioneel: audit op aanvraag, uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	

Een vergrote weergave is opgenomen in de Bijlage D: Vergrote weergave afbeeldingen.

4.7.2. Transparantie en toetsing

Naast de beveiligingskaders die in de voorgaande paragraaf zijn beschreven kent de Kieswet ook kaders ten aanzien van controleerbaarheid. Het verkiezingsproces kent een wettelijk verankerde mate van transparantie en controleerbaarheid als het gaat om het vaststellen van de verkiezingsuitslag. Deze transparantie maakt het, onder meer voor burgers en media, mogelijk om toe te zien op het verloop van het proces. In paragraaf 8.7 wordt nader stilgestaan bij transparantie en controleerbaarheid rondom de vaststelling van de uitslag.

Met betrekking tot het gebruik van DHV stelt de Kieswet enkele normen, onder andere met betrekking tot de implementatie van de zetelverdeling in de software. Deze normen, zie voor thans geldende wettelijke bepalingen 'Bijlagen C: Huidig wettelijk eisen kader (art P1a)', zien onder andere toe op de toetsing van de specificatie en correcte werking van het DHV door een onafhankelijke partij. De Kieswet voorziet daarnaast een controle protocol, aan de hand waarvan het GSB en het CSB de door het DHV gegenereerde uitslag gegevens controleert op juistheid. Met het controle protocol wordt beoogd dat buiten het DHV om wordt geverifieerd of de gegenereerde resultaten correct zijn.

5. Functionele-opzet

In dit hoofdstuk wordt ingegaan op de functionele opzet van het DHV en de verschillende (functionele) gebruikers die in het DHV worden onderscheiden.

5.1. Gebruikersrollen en functionaliteiten

In paragraaf 4.5 zijn in het kader van functiescheiding verschillende gebruikersrollen benoemd. In deze paragraaf wordt nader ingegaan op de functionaliteiten die vallen onder de verschillende rollen.

5.1.1. Gemeentelijk stembureau (GSB)

De volgende gebruikersrollen met bijbehorende functionaliteiten worden in het DHV onderscheiden binnen het GSB-compartiment:

- Invoerder GSB
    - Invoeren (handmatig) van de stembureau-uitslaggegevens;
    - Inzicht in de status van de stembureaus binnen de gemeente;
    - Kunnen wijzigen van het eigen wachtwoord en profiel instellingen;
    - Invoeren bezwaren en onregelmatigheden die door het stembureau zijn opgetekend.
- Lid GSB
    - Opgeven vervolgactie bij niet overeenkomende ingevoerde stembureau-uitslag;
    - Herroepen ingevoerd stembureauresultaat en op nieuw laten invoeren (mogelijk zolang het gemeenteresultaat niet is geaccordeerd);
    - Accorderen van de gemeentelijke optelling voordat de Voorzitter GSB deze ondertekent. Het accorderen is pas mogelijk nadat alle stembureau-resultaten volledig zijn ingevoerd. Na het accorderen is het niet meer mogelijk om stembureau uitslagen aan te passen;
    - Inzicht in de status van de stembureaus binnen de gemeente;
    - Overzicht van alle bezwaren en onregelmatigheden die door de stembureaus zijn opgetekend en door de Invoerder GSB zijn ingevoerd. Het overzicht geeft inzicht in alle bezwaren en die van de afzonderlijke stembureaus;
    - Overzicht (voorlopig) gemeente resultaat;
    - Overzicht met resultaten uit plausibiliteit controles;
    - Overzicht van ingelogde (alle) gebruikers en voortgang van de uitslagverwerking binnen het eigen compartiment;
    - Mogelijkheid om, na ondertekening door de Voorzitter GSB, het concept proces-verbaal te downloaden/printen;
    - Kunnen wijzigen van het eigen wachtwoord en profiel instellingen.
- Voorzitter en vicevoorzitter GSB
    - Terugdraaien van een eerder door het Lid GSB geaccordeerd gemeenteresultaat;
    - Bevestigen dat uitkomst controleprotocol geen aanleiding geeft tot herzien van de uitslag, zo niet terugdraaien van het door Lid GSB geaccordeerde gemeenteresultaat;
    - (Digitaal) ondertekenen van het gemeenteresultaat (nadat Lid GSB het resultaat heeft geaccordeerd en de Voorzitter GSB de controle heeft bevestigd) en de gegenereerde uitslag bestanden (waaronder het concept proces-verbaal voor schriftelijke ondertekening door het GSB);
    - Akkoord geven voor het doorzetten van de digitale gemeenteresultaten naar het CSB;
    - Herroepen van digitaal ondertekende gegevens en de doorgestuurde gegevens naar het CSB. Deze mogelijkheid is beschikbaar gedurende de periode dat herziening van de uitslag mogelijk is. Het is hierna mogelijk om het gemeenteresultaat opnieuw vast te stellen;
    - Inzicht in de status van de stembureaus binnen de gemeente;

    - Overzicht van alle bezwaren en onregelmatigheden die door de stembureaus zijn opgetekend en door de Invoerder GSB zijn ingevoerd. Het overzicht geeft inzicht in alle bezwaren en die van de afzonderlijke stembureaus;
    - Overzicht (voorlopig) gemeenteresultaat;
    - Overzicht met resultaten uit plausibiliteit controles;
    - Overzicht van ingelogde (alle) gebruikers en voortgang van de uitslagverwerking binnen het eigen compartiment;
    - Mogelijkheid om, na ondertekening door de Voorzitter GSB, het (concept) proces-verbaal te downloaden/printen;
    - Kunnen wijzigen van het eigen wachtwoord en profiel instellingen.
- Beheerder GSB
    - Instellen van lokale verkiezingsgegevens, stembureau gegevens, kandidatenlijsten, contact gegevens (voor de VA), etc.;
    - Inzicht in de status van de stembureaus binnen de gemeente;
    - Registeren van de (lokale) Invoerder GSB en Lid GSB gebruikers (aanmaken voorzitter GSB en Beheerder GSB verloopt via de Functioneel beheerder van de KR);
    - Koppelen 2FA middel aan Invoerder GSB en Lid GSB gebruikers;
    - Beheer van Invoerder GSB en Lid GSB gebruikers ((de)activeren gebruikers, wachtwoord resetten, etc.);
    - Overzicht van gelogde gebruikershandelingen eigen compartiment;
    - Wijzingen van het eigen wachtwoord en profiel instellingen.

5.1.2. Centraal stembureau

De volgende gebruikersrollen met bijbehorende functionaliteiten worden in het DHV onderscheiden binnen het CSB-compartiment:

- Invoerder CSB
    - Vergelijkbare functiemogelijkheden als Invoerder GSB, maar dan voor CSB.
- Lid CSB
    - Vergelijkbare functiemogelijkheden als Lid GSB, maar dan voor CSB;
    - Opgegeven vervolgactie indien ontvangen digitaal gemeenteresultaat niet aan vereisten voldoet.
- Voorzitter en vicevoorzitter CSB
    - Vergelijkbare functiemogelijkheden als voorzitter GSB, maar dan voor CSB.
- Beheerder CSB
    - Vergelijkbare functiemogelijkheden als Beheerder GSB, maar dan voor CSB.

5.1.3. Kiesraad

De volgende gebruikersrol met bijbehorende functionaliteiten worden in het DHV onderscheiden binnen het KR-compartiment:

- Functioneel beheerder KR
    - Instellen van globale verkiezingsgegevens, zoals configuratie van de verkiezingentypen en regiostructuur;
    - Beheren van de document-templates voor de verschillende uitvoer documenten, waaronder die voor de wettelijke model documenten;
    - Registeren van (vice)Voorzitter GSB/CSB-gebruikers en Beheerders GBS/CSB voor de verschillende GSB's en CSB's en koppelen eHerkenning middel aan (vice)Voorzitter en Beheerders GBS/CSB;
    - Beheer van (vice)Voorzitter en Beheerders GBS/CSB, ((de)activeren gebruikers, wachtwoord resetten, etc.);
    - Overzicht van gelogde gebruikershandelingen van de verschillende GSB- en CSB-compartimenten;
    - Beheer toegang instellingen tot de verschillende GSB- en CSB-compartimenten, instellen IP-whitelisting, (de)activeren gebruikers toegang tot een bepaald GSB/CSB-compartiment;

- Kunnen wijzigen van het eigen wachtwoord en profiel instellingen.

5.2. Specifieke gebruikerspaden

In deze paragaaf worden enkele specifieke gebruikerspaden nader beschreven. Met de beschrijving wordt mede aangegeven welke gebruikers handelingen in het DHV plaatsvinden. De gebruikerspaden die nader worden toegelicht hebben betrekking op registratie GSB/CSB-gebruikers en het invoeren, accorderen en digitaal ondertekenen van de uitslaggegevens en zijn essentieel voor (een goed begrip) van het beveiligingsconcept.

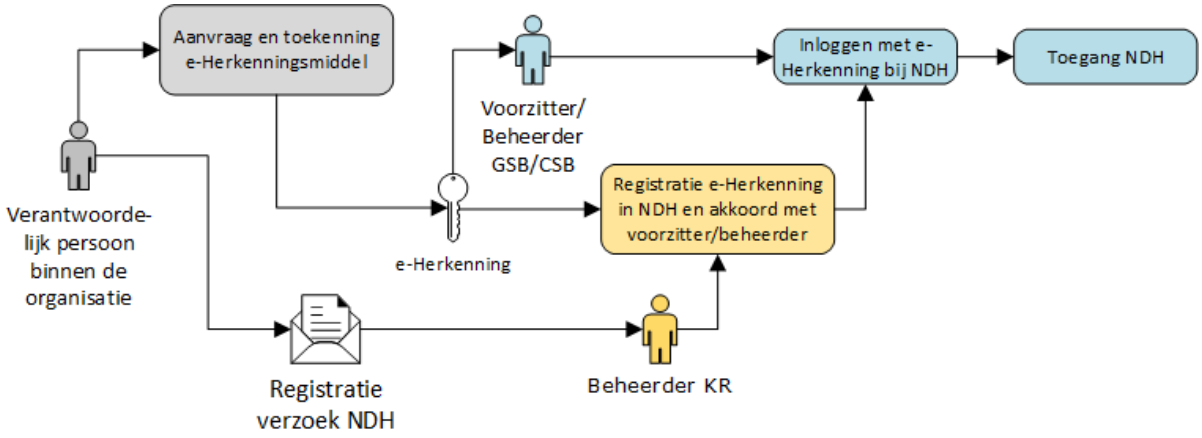
5.2.1. Registratie en toegang gebruikers

In hoofdstuk 4 Beveiligingsconcept zijn de uitgangpunten met betrekking tot functiescheiding en de authenticatiemiddelen beschreven. Deze uitgangspunten vinden weerslag in de wijze waarop gebruikers worden geregistreerd en toegang verkrijgen tot de functionaliteit in het DHV. Zoals in hoofdstuk 4 is beschreven worden, afhankelijk van de gebruikersrol, in verschillende authenticatiemiddelen voorzien. Het is belangrijk dat de registratie van de verschillende gebruikers tijdig in het DHV plaatsvindt. De Kiesraad kan in het DHV het registratie verloop monitoren en kan indien nodig richting de gebruikersorganisatie aanwijzingen geven.

Voor de **Beheerder GSB/CSB** en de **(vice)Voorzitter GSB/CSB** geldt dezelfde registratie-procedure en wordt hetzelfde authenticatiemiddel toegepast: eHerkenning.

De volgende stappen worden hierbij voorzien:

1. Indien de betreffende Beheerder of (vice)Voorzitter GSB/CSB nog niet beschikt over het vereiste eHerkenningsmiddel wordt dit door de verantwoordelijke organisatie (dit is de rechtspersoon waaronder de functionaris is aangesteld) aangevraagd (overeenkomstig de daarvoor geldende aanvraagprocedure);
2. Nadat de betreffende Beheerder of (vice)Voorzitter GSB/CSB beschikt over het vereiste eHerkenningsmiddel wordt bij de KR het registratieverzoek ingediend;
    - Het verzoek omvat de vereiste persoons- en contactgegevens, evenals de identificerende eigenschappen van het eHerkenningsmiddel.
3. De Functioneel beheerder KR registreert, nadat is vastgesteld dat het verzoek en de daarop vermelde gegevens correct zijn, de Beheerder of (vice)Voorzitter GSB/CSB in het DHV;
    - De betreffende gebruiker wordt hiermee geautoriseerd voor een bepaald GSB/CSB-compartiment;
    - Met de registratie van de gebruiker wordt eveneens het persoonsgebonden eHerkenningsmiddel gekoppeld in het DHV;
    - De betreffende gebruiker ontvangt bericht als de registratie door de Functioneel beheerder KR is afgerond.
4. De betreffende Beheerder of (vice)Voorzitter GSB/CSB kan vervolgens met zijn eHerkenningsmiddel inloggen in het DHV.

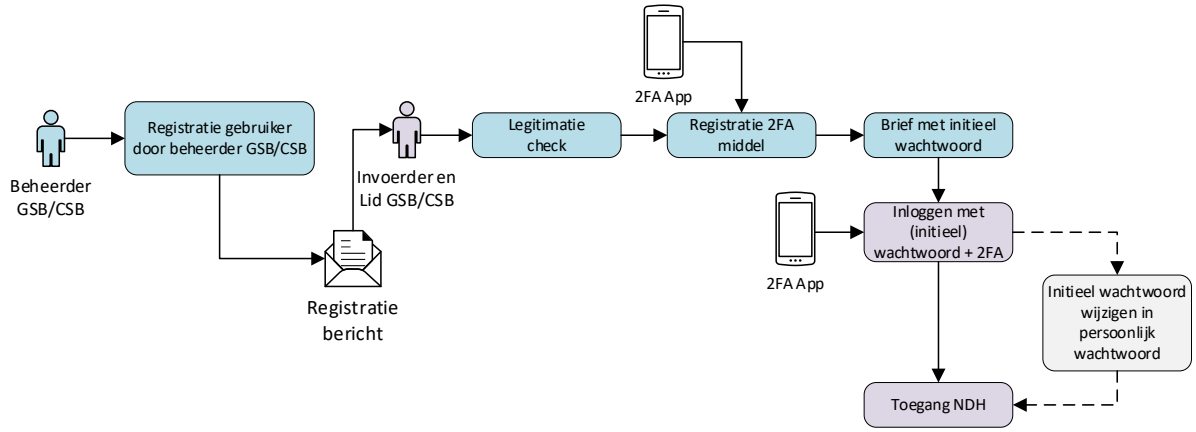


Figuur 6: Schematische weergave registratie Beheerder en (vice)Voorzitter GSB/CSB.

Voor de **Invoerder GSB/CSB en het Lid GSB/CSB** wordt een andere registratie procedure gevolgd die meer flexibiliteit biedt aan het GSB/CSB om de beschikbare personen op te geven en te wijzigen in het DHV, zoals beschreven in paragraaf 4.5. Voor deze gebruikers wordt de registratie uitgevoerd door de Beheerder GSB/CSB. Om deze gebruikers te registeren is vereist dat eerst een Beheerder voor het betreffende GSB/CSB-compartiment is geautoriseerd. Bij de Invoerder GSB/CSB en het Lid GSB/CSB wordt gebruik gemaakt van een generiek 2FA authenticatiemiddelen (dit kan een hardware token of token app zijn) dat door de betreffende organisatie, zijnde de gemeente dan wel het GSB of CSB, zelf wordt uitgegeven aan de gebruiker.

Stapsgewijs kan deze als volgt worden beschreven:

1. De verantwoordelijke organisatie bepaalt welke personen als Invoerder GSB/CSB of Lid GSB/CSB dienen te worden geregisterd in het DHV;
2. Nadat de Beheerder GSB/CSB de betreffende persoons- en contactgegevens heeft ontvangen, registreert de Beheerder GSB/CSB de personen in het betreffende GSB/CSB-compartiment van het DHV;
    - De betreffende gebruiker ontvangt bericht als de registratie door de Beheerder GSB/CSB is afgerond.
3. Voordat de betreffende gebruikers inlogt in het DHV meldt de persoon zich bij de Beheerder om zich te legitimeren;
4. Nadat is vastgesteld dat de identiteit correct is, wordt het generieke 2FA-middel gekoppeld aan het gebruikersaccount en wordt deze geactiveerd;
    - Met het activeren van het account wordt een initieel wachtwoord bepaald dat een beperkte geldigheidsduur kent. Binnen de geldigheidsduur dient de gebruiker in te loggen in het DHV.
5. De eerste keer logt de gebruiker in met een initieel wachtwoord, welke aansluitend dient te worden gewijzigd door een door de gebruiker zelf gekozen wachtwoord;
    - Bij het inloggen is tevens de verificatiecode vereist die uit het generieke 2FA-middel komt.
6. De betreffende Invoerder GSB/CSB of Lid GSB/CSB kan vervolgens met zijn eigen wachtwoord en 2FA inloggen in het DHV.



Figuur 7: Schematische weergave registratie Invoerder en Lid GSB/CSB.

De Beheerder GSB/CSB en de Functioneel beheerder KR kunnen nagaan welke gebruikers zijn ingelogd, dan wel ingelogd zijn geweest. Het is voor de Beheerder GSB/CSB mogelijk om het account van een Invoerder GSB/CSB of Lid GSB/CSB te deactiveren of om het wachtwoord te resetten, bijvoorbeeld als de gebruiker het wachtwoord niet meer weet. De Functioneel beheerder KR kan het gebruikersaccount van de Beheerder en (vice)Voorzitter GSB/CSB deactiveren.

5.2.2. Invoeren, accorderen en digitaal ondertekenen van de uitslaggegevens

Bij het beoogde invoeren, accorderen en digitaal ondertekenen van de uitslaggegevens in het DHV hebben verschillende gebruikers een rol.
Bij dit proces wordt ook meegenomen dat het DHV tegenstrijdigheden in de invoer zichtbaar maakt en afdwingt dat de correcte gegevens worden verwerkt, bijvoorbeeld wanneer de optelsom van het aantal stemmen op kandidaten van een lijst niet overeenkomt met het lijsttotaal.

Nadat een gebruiker is ingelogd in het DHV kunnen de volgende gebruikerspaden zich voordoen.

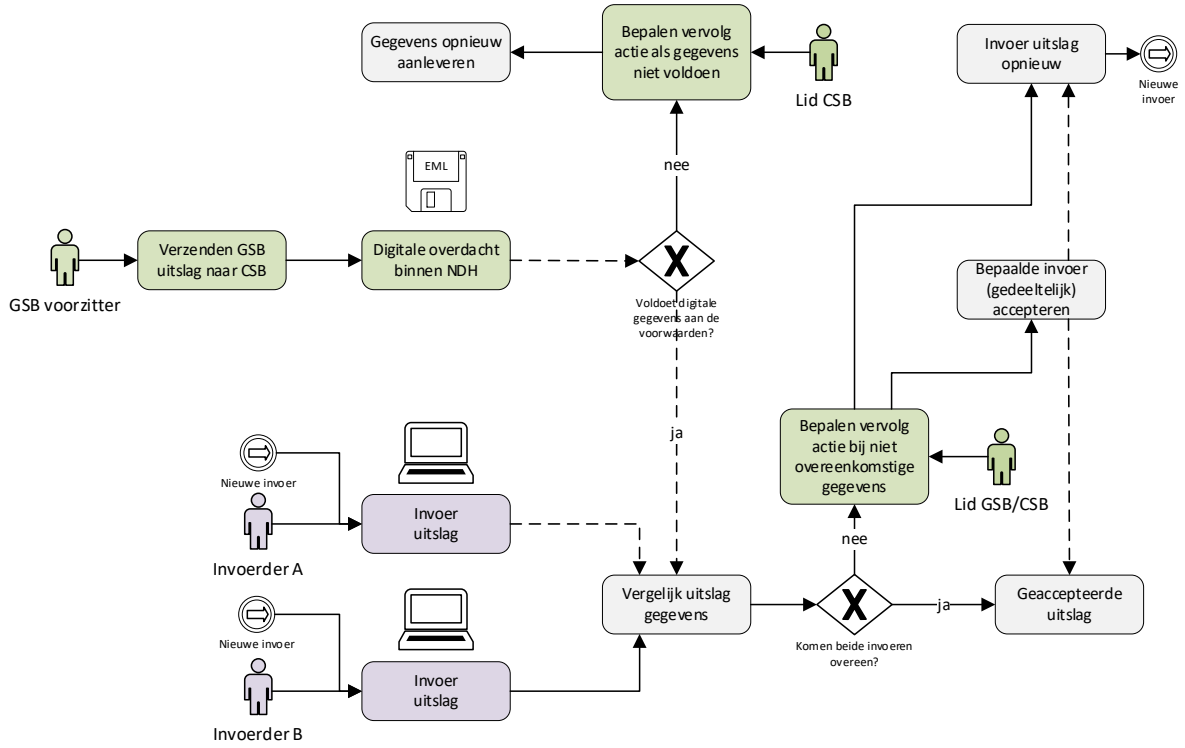
De **invoer van de uitslag door een Invoerder GSB/CSB** gebeurt aan de hand van het papieren uitslagresultaten van het stembureau in geval van GSB en die van het GSB in geval van CSB. Het papieren uitslagresultaat kan het proces-verbaal zijn van het stembureau of van het GSB, dan wel de opgave van het stembureau indien er centraal wordt geteld.

1. Nadat de Invoerder GSB/CSB een papieren uitslagresultaat heeft ontvangen, voert deze de uitslaggegevens in het DHV;
2. Zodra de Invoerder GSB/CSB van mening is dat alle uitslaggegevens zijn overgenomen in het DHV geeft die de opdracht de gegevens op te slaan. Als de ingevoerde gegevens niet voldoen, wordt dit aan de Invoerder GSB/CSB gemeld en dient deze de ingevoerde gegevens te corrigeren;
3. Voordat de gegevens worden opgeslagen vindt er een automatische validatie en verificatie plaats op de ingevoerde gegevens;
    - Bij de verificatie wordt gecontroleerd of alle vereiste gegevens aanwezig zijn, of de ingevoerde waarden voldoen aan de criteria. Tevens wordt gekeken of de ingevoerde getallen correct optellen. Voldoen de ingevoerde gegevens niet dan wordt hiervan een foutmelding gegeven aan de Invoerder GSB/CSB. De ingevoerde gegevens worden als een valide of niet-valide invoer bewaard, zodat de (reeds ingevoerde) gegevens later hersteld kunnen worden. Het is mogelijk dat dit herstel pas kan plaatsvinden nadat het GSB/CSB een nieuwe stemopneming heeft uitgevoerd en tot een correcte uitslag is gekomen waarna de invoer in het DHV kan worden afgerond;
    - Bij de validatie wordt ook gecontroleerd op onwaarschijnlijkheden. Van een onwaarschijnlijkheid is sprake als de invoer abnormale waarden bevat. Dit is bijvoorbeeld het geval als het aantal blanco of ongeldige stemmen boven een

bepaald (hoog) percentage uitkomt. Ook als de ingevoerde uitslag precies overeenkomt met een reeds eerder ingevoerd stembureau/gemeente wordt dit als onwaarschijnlijk aangemerkt. Bij onwaarschijnlijkheden krijgt de Invoerder GSB/CSB een waarschuwing en het verzoek om de ingevoerde gegevens te controleren. Mocht de waarschuwing onterecht zijn kan de Invoerder GSB/CSB de gegevens alsnog opslaan;
    - Foutmeldingen en waarschuwingen worden door het DHV vastgelegd en het Lid GSB/CSB en de (vice)Voorzitter GSB/CSB mogelijkheid de voorgedane meldingen in een overzicht op te vragen.
4. Nadat de eerste invoer volledig is afgerond en er een gevalideerd resultaat is opgeslagen, kan de tweede invoer plaatsvinden. Nadat een andere Invoerder GSB/CSB het proces-verbaal heeft ontvangen voert deze gebruiker de uitslaggegevens in;
    - Voor de tweede invoer geldt dezelfde validatie en verificatie van de ingevoerde gegevens als bij de eerste invoer.
5. Op het moment dat er twee valide invoerresultaten zijn, vindt er een automatische vergelijking plaats tussen beide ingevoerde uitslagen. Als beide ingevoerde uitslagen overeenkomen wordt de uitslag als definitief resultaat opgeslagen. Als beide uitslagen niet overeenkomen wordt de vergelijking van beide uitslagen voorgelegd aan een Lid GSB/CSB;
6. Bij niet overeenkomende uitslagen dient een Lid GSB/CSB te bepalen wat er vervolgens met de uitslagen gebeurt. Het Lid kan in een dergelijk situatie bepalen dat:
    - Een van beide ingevoerde uitslagen correct is en als definitief resultaat wordt opgeslagen;
    - Dat de ingevoerde uitslag van één van de twee invoeren, bijvoorbeeld doordat er bij tweede invoer de aantallen stemmen bij twee kandidaten binnen een lijst zijn omgedraaid, gedeeltelijk incorrect is en dat een bepaald deel van de invoer opnieuw dient te worden ingevoerd;
    - Dat de uitslag in zijn geheel, tweemaal, opnieuw dient te worden ingevoerd.
7. Afhankelijk van hetgeen het Lid GSB/CSB opgeeft in het DHV wordt de uitslag als geaccepteerd opgeslagen of vindt er een (gedeeltelijk) nieuwe invoer plaats.

In de situatie dat de **uitslaggegevens (tevens) digitaal worden doorgezet** vindt er een aangepast invoerproces plaats.

1. Nadat de (vice)Voorzitter GSB akkoord heeft gegeven voor het (digitaal) doorzetten van het gemeente resultaat, wordt de GSB uitslag vrijgeven voor het CSB. Het CSB kan vervolgens de uitslag in het CSB-compartiment raadplegen;
2. Zodra de gegevens in het CSB-compartiment beschikbaar komen vindt er een automatische validatie plaats op de uitslaggegevens. Indien de validatie daar aanleiding toe geeft, dient een Lid CSB het gemeente resultaat te beoordelen. Het Lid CSB kan daarbij bepalen dat:
    - De uitslaggegevens van het GSB voldoen en kunnen worden gebruikt bij de verdere invoer van de GSB uitslag;
    - De uitslaggegevens van het GSB voldoen niet en worden niet gebruikt bij de invoer. Het GSB wordt hierbij verzocht om alsnog de correcte uitslaggegevens aan te leveren. In een dergelijk situatie gaat een melding naar het betreffende GSB-compartiment, zodat het GSB hierop actie kan ondernemen in het DHV.
3. Voldoet het doorgezette gemeenteresultaat, dan wordt deze als een gevalideerde eerste invoer aangemerkt en kan gelijk de tweede invoer uitgevoerd worden door een Invoerder CSB;
4. De vervolgstappen komen overeen met die reeds zijn beschreven vanaf de tweede invoer door een Invoerder GSB/CSB.

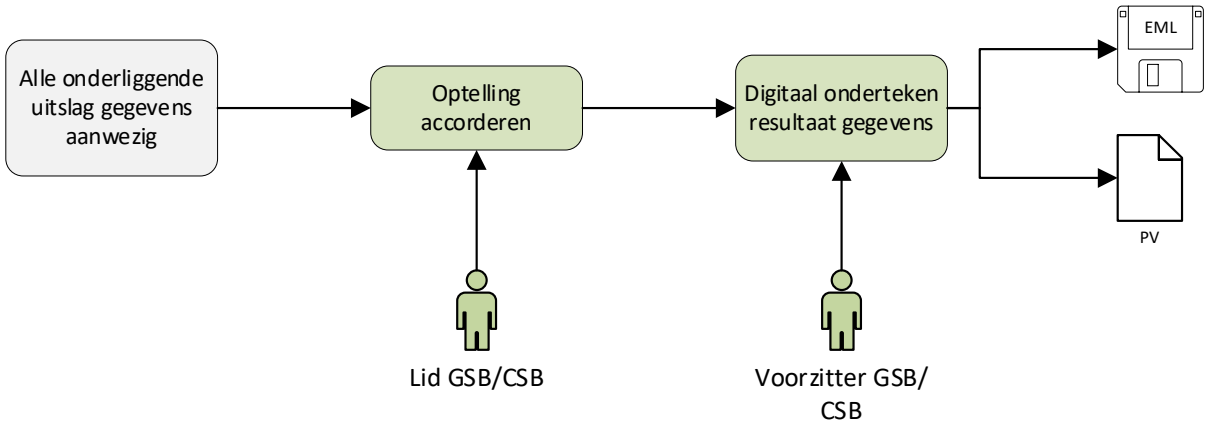


Figuur 8: Schematische weergave van het invoer proces

Nadat alle onderliggende stembureau/gemeente resultaten zijn ingevoerd en geaccepteerd zijn wordt de totaaltelling uitgevoerd. De totaaltelling vormt de basis voor het **accorderen en digitaal onderteken van de uitslaggegevens**. De volgende stappen worden door Lid GSB/CSB en (vice)Voorzitter GSB/CSB uitgevoerd.

1. De optelling, die het DHV berekend heeft, wordt door een Lid GSB/CSB geaccordeerd. Nadat de optelling door het Lid GSB/CSB is geaccordeerd kan er geen wijziging meer plaatsvinden in de onderliggende stembureau/gemeente-uitslagen (invoer is niet meer mogelijk);
    - Voordat het Lid GSB/CSB akkoord gaat met de door het DHV berekende optelling vindt er verificatie plaats aan de hand van het controleprotocol;
    - Als blijkt dat de optelling niet correct is en dit komt door een onjuiste invoer van een stembureau/gemeente-uitslag, wordt het akkoord opgeschort en vindt er correctie plaats van de ingevoerde uitslag. Lid GSB/CSB kan hiertoe de invoer van een bepaald stembureau/gemeente vrijgeven voor een nieuwe invoer;
    - Is de optelling niet correct en ligt dit niet aan een onjuist ingevoerde uitslag, dan komt dit doordat het DHV niet correct heeft opgeteld. In een dergelijke situatie dient de optelling buiten het DHV om plaats te vinden.
2. In geval van het CSB vindt, nadat de optelling is geaccordeerd, de zetelverdeling plaats. De berekening van de zetelverdeling vindt in een separaat compartiment plaats, dat los staat van de GSB en CSB-compartimenten. Nadat de zetelverdeling is berekend binnen het DHV, wordt deze beschikbaar in het CSB-compartiment;
3. De optelling en indien van toepassing de berekening van de zetelverdeling komen vervolgens beschikbaar voor de (vice)Voorzitter GSB/CSB. De (vice)Voorzitter GSB/CSB bevestigt dat de controles zijn uitgevoerd en geen aanleiding hebben gegeven om de uitslag te herzien;
    - Indien de (vice)Voorzitter GSB/CSB de bevestiging niet kan geven, kan deze het akkoord van Lid GSB/CSB intrekken en daarmee mogelijk maken dat de ingevoerde uitslag wordt aangepast.

4. Als er geen reden is om de uitslag te herzien en de (vice)Voorzitter GSB/CSB de controles heeft bevestigd kan er overgegaan worden tot het digitaal ondertekenen van het GSB/CSB-resultaat;
    - Met de ondertekening wordt eveneens het concept proces-verbaal van een digitale handtekening voorzien, als ook het uitslagbestand.
5. Met de ondertekening wordt het concept proces-verbaal beschikbaar voor het Lid GSB/CSB en de (vice)Voorzitter GSB/CSB zodat deze het document kunnen printen, om het vervolgens in de openbare zitting door de leden (schriftelijk) te ondertekenen;
    - Nadat het proces-verbaal binnen het DHV digitaal is ondertekend, wordt het doorgezet naar een separaat portaal van waaruit het Lid GSB/CSB en de (vice)Voorzitter GSB/CSB het document kunnen downloaden om het te kunnen printen binnen de kantoor omgeving. Toegang tot de download-portal verloopt via twee-factor-authenticatie.
6. Indien tijdens de openbare zitting geen redenen naar voren komen om de uitslag te herzien wordt deze aldaar vastgesteld;
    - Blijkt in de zitting dat de uitslag nader onderzoek vergt en mogelijke herziening in aanmerking komt, beschikt de (vice)Voorzitter GSB/CSB over de mogelijkheid om het eerder digitaal ondertekende resultaat in te trekken. Hiermee ontstaat de mogelijkheid om de ingevoerde uitslag te herzien.
7. Geeft de zitting van het GSB/CSB geen aanleiding tot het herzien van de reeds digitaal ondertekende uitslag dan kan de (vice)Voorzitter GSB/GSB akkoord geven om de uitslag door te zetten. In geval van het GSB wordt vervolgens de uitslag beschikbaar in het CSB compartiment.
    - Voordat de (vice)Voorzitter GSB/CSB akkoord geeft om de uitslag door te zetten, dient de (vice)Voorzitter GSB/CSB de in de zitting ingebrachte bezwaren en de hierop gedane reactie van het GSB/CSB over te nemen in het DHV. Deze invoer wordt vervolgens als aanvulling gehecht aan het eerdere gegeneerde (concept) proces-verbaal. De aanvulling is beschikbaar voor Lid en (vice)Voorzitter GSB/CSB om geprint te kunnen worden.



Figuur 9: Schematische weergave accorderen en digitaal ondertekenen GSB/CSB-resultaat.

In het DHV wordt de mogelijkheid voor het GSB/CSB voorzien dat de reeds ingevoerde en (digitaal)ondertekende uitslag herzien dient te worden. Aanleiding om de uitslag te herzien kan zijn dat er een nieuwe stemopname heeft plaatsgevonden of dat er een hertelling of herstemming heeft plaatsgevonden. In een dergelijke situatie kan de (vice)Voorzitter GSB/GSB een eerder vastgestelde uitslag intrekken en daarmee ontstaat de mogelijkheid om de invoer van stembureau of gemeente resultaten te herzien.

6. Netwerk, logging en monitoring

6.1. Netwerk

In het kader van het principe "Gelaagde beveiliging" en "Minimaliseer aanvalsoppervlakte" is het verstandig om de kans op een aanval via het netwerk zo veel mogelijk te beperken voor zover dit uitvoeringstechnisch mogelijk is.

Het "Geen vertrouwen (Zero trust)" principe veronderstelt echter dat geen systeem, netwerk, (markt)partij of persoon op zichzelf als geheel vertrouwd kan worden aangemerkt. Derhalve dienen er, ongeacht in welke mate het netwerk wordt vertrouwd, maatregelen te worden getroffen die desalniettemin het risico beperken dat het DHV wordt gecompromitteerd via het netwerk. Maatregelen 1 en 3, zoals beschreven in het Ontwerp basisarchitectuur (paragraaf 4.4), gaan reeds uit van dit principe.

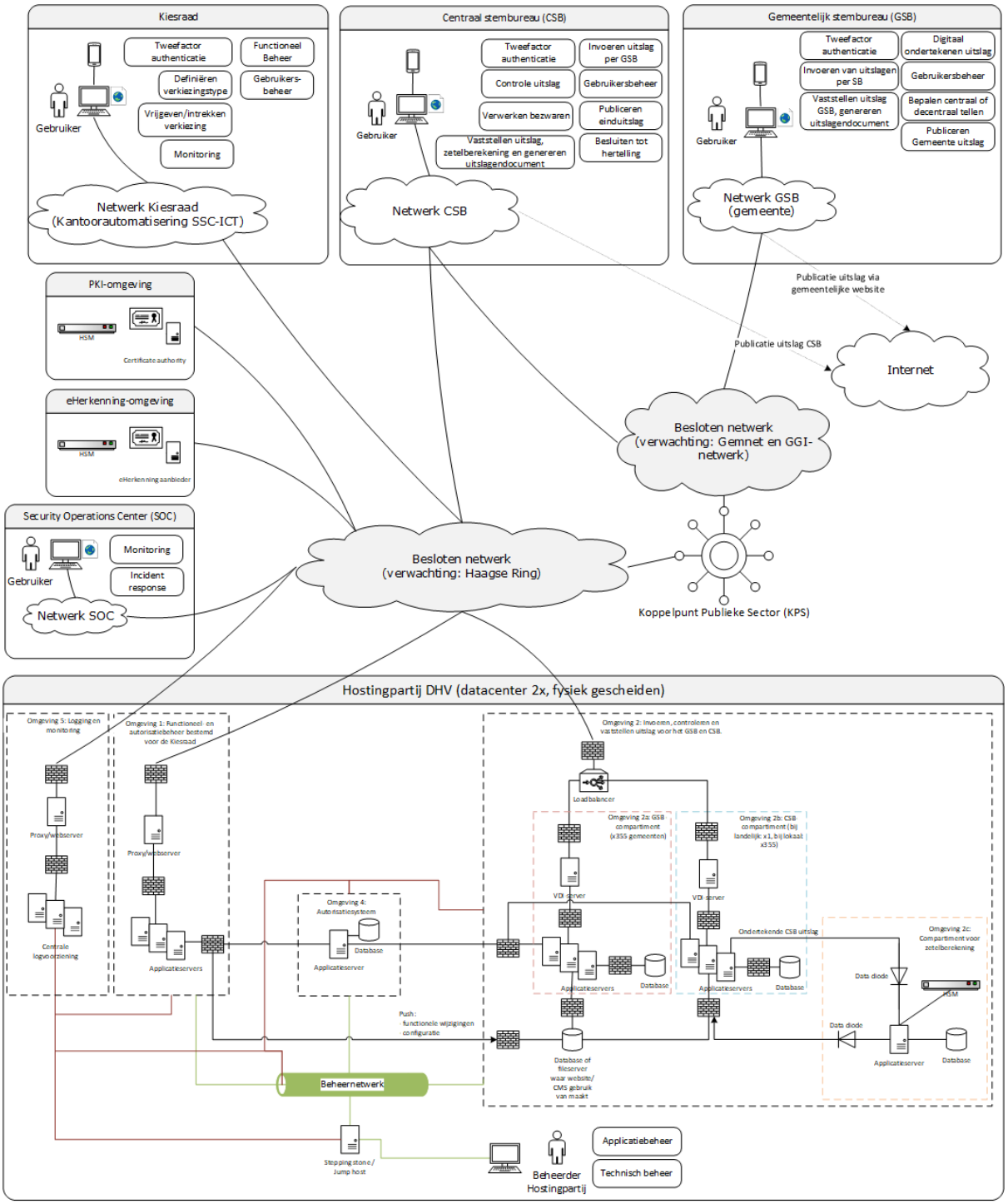
Om de aanvalsoppervlakte te verkleinen, is er in de basisarchitectuur een ontwerpkeuze gemaakt om het DHV uitsluitend beschikbaar te maken voor werkstations van het GSB/CSB die zijn aangesloten op een besloten(semi)overheidsnetwerk. De landelijke (semi)overheidsnetwerken als Gemnet en GGI-Netwerk hebben, mede gelet op het besloten karakter en de gerichtheid op het veilig verbinden van gemeentelijke systemen, een voorkeur bij het ontsluiten van het DHV. In dit hoofdstuk worden de consequenties van deze ontwerpkeuze ten aanzien van de haalbaarheid voor het GSB/CSB nader besproken.

6.1.1. Diginetwerk

Diginetwerk is een afsprakenstelsel voor het koppelen van besloten netwerken van de overheid. Via deze gekoppelde netwerken kunnen overheidsorganisaties onderling gegevens uitwisselen.[6] Door het besloten karakter is Diginetwerk een veiliger alternatief dan het open internet voor het uitwisselen van gegevens tussen overheidsorganisaties. Via Diginetwerk is connectiviteit met alle aangesloten overheidsorganisaties via één koppeling mogelijk.

Onder andere de Haagse Ring, GGI-netwerk[7] en Gemnet[8] maken onderdeel uit van het Diginetwerk. In de volgende visualisatie worden de verschillende netwerkverbindingen naar de verschillende partijen geschetst.

[6] Op de website van Logius is nadere informatie over het Diginetwerk beschikbaar.
[7] Informatie over GGI-Netwerk is beschikbaar op de website van VNG Realisatie, hier is onder andere het Architectuur GGI-Netwerk: high level design te vinden.
[8] KPN is de exploitant van Gemnet.



Legenda	
Symbool	Beschrijving
	(Virtuele) server
	(Virtuele) firewall
	Gebruiker
	Werkstation (desktop, laptop, tablet, etc.)
	Diginetwerk
	Database
	Certificate server
	Load balancer
	Modem
	Smart phone

Figuur 10: Conceptuele visualisatie koppelingen Diginetwerk en infrastructuur DHV.

Een vergrote weergave is opgenomen in de Bijlage D: Vergrote weergave afbeeldingen en tabellen.

Onder de hosting zijn verschillende componenten opgenomen die de technische infrastructuur vormen van het DHV. Onder infrastructuur wordt in het kader van het DHV elk geval de onderstaande componenten verstaan die worden gebruikt om het DHV te hosten en beschikbaar te stellen aan de GSB's/CSB's:

- **Netwerkcomponenten, zoals:** routers, switches, modems, etc.;
- **Servers:** applicatieservers, webservers, proxyservers, opstapservers, databaseservers, etc.;
- **Beveiligingscomponenten:** Intrusion Detection Systemen, Intrusion Prevention Systemen, firewalls, Next Generation Firewalls, etc.;
- **Beheercomponenten**: alle componenten die benodigd zijn voor het beheren van de bovengenoemde infrastructuur. Hierbij kan worden gedacht aan: Identity & Access Management (IAM) toepassingen, VPN-oplossingen, werkstations van de technisch beheerders, etc.

De dataverbindingen over de verschillende netwerken, zowel binnen het DHV als met de werkstations bij de gebruikersorganisatie, zijn beveiligd doormiddel van erkende versleutelingsmethoden, zoals Transport Layer Security (TLS). De versleutelingsmethoden zorgt voor de encryptie van data die over het netwerk wordt uitgewisseld. Op de verschillende servers zal encryptie van data plaatsvinden, daarbij gaat het onder andere om de gebruikersgegevens die in de database versleuteld worden opgeslagen en het digitaal ondertekenen van uitslaggegevens. Voor het digitaal ondertekenen wordt aangesloten bij erkende ondertekendiensten, die samenvallen met aanbieders van eHerkenningsmiddelen en PKI-overheidscertificaten.

6.1.2. Diginetwerk naar GSB en CSB

De gemeentelijke stembureaus en de centrale stembureaus dienen toegang te hebben tot het DHV. Voor de toegang is van belang dat het GSB en CSB aangesloten zijn op het Diginetwerk. De aansluiting van het GSB en het CSB zal in de praktijk lopen via de ondersteunende organisatie van het GSB dan wel CSB. De volgende ondersteunde organisaties kunnen worden onderscheiden:

- Gemeente, ten aanzien van GSB bij de lokale en nationale verkiezingen en tevens CSB bij GR- en PS-verkiezingen;
- Waterschap, ten aanzien van het CSB bij WS-verkiezingen;
- Openbaar lichaam, ten aanzien van SBLO bij de lokale en nationale verkiezingen en CSB bij KC- en ER-verkiezingen en SB bij EK-verkiezing in relatie tot het Kiescollege;
- Gemeente Den Haag, ten aanzien van het NBSB bij TK- en EP-verkiezing;
- Provincie, ten aanzien van SB bij EK-verkiezing;
- Kiesraad, ten aanzien van CSB bij EK-, TK- en EP-verkiezing.

Gemeenten

De organisaties met de meeste aansluitingen naar het DHV zijn de gemeenten. Bestaande gemeentelijke netwerken die onderdeel uitmaken van Diginetwerk zijn het GGI-Netwerk en het Gemnet. De voorkeur gaat uit naar GGI-netwerk. Een verschil op dit moment tussen beide netwerken is de adoptiegraad. Het GGI-Netwerk heeft op basis van cijfers van VNG[9] van februari 2020 een adoptie percentage van 33,5%. Bij Gemnet, dat onder meer wordt gebruikt voor het BRP-berichten verkeer, is sprake van 100% adoptie. Gezien de huidige adoptiegraad zal Gemnet voor de meeste gemeenten de aansluiting zijn op het Diginetwerk. Indien de gemeente is aangesloten op het GGI-Netwerk, dan heeft dit netwerken de voorkeur als primaire aansluiting naar het Diginetwerk. Gemeenten die aangesloten zijn op beide netwerken hebben de mogelijkheid om beide netwerken te gebruiken om verbinding te leggen met het DHV. Bij

[9] Beschikbaar via 'Waar staat je gemeente': https://www.waarstaatjegemeente.nl/dashboard/Dienstverlening-en-digitalisering

eventuele uitval van een netwerk kan een gemeente in een dergelijke situatie overschakelen op het andere netwerk (bijvoorbeeld: GGI-Netwerk indien Gemnet niet beschikbaar is of vice versa).

De opzet van het DHV is erop gericht dat gebruikers via het gemeentelijke kantoor-netwerk toegang krijgen. Om dit mogelijk te maken is het vereist dat de verbinding tot Diginetwerk (dan wel via Gemnet of GGI-Netwerk) ontsloten wordt tot de werkstations die worden ingezet voor het DHV door de gemeenten. Het kan zijn dat een degelijke verbinding, tot de werkstations, niet in alle gemeenten is gerealiseerd. Bij de uitrol van het DHV wordt een aansluitingsprocedure voorzien, waarbij gemeenten geholpen worden met een tijdig inregelen en testen.

Waterschappen
De waterschappen zijn de ondersteunde organisatie voor het CSB bij WS-verkiezingen. Net als gemeenten kunnen Waterschappen via Gemnet aangesloten worden op het Diginetwerk en daarmee tot het DHV. Voor waterschappen geldt dezelfde aansluitprocedure als voor gemeenten. In welke mate de 21 waterschappen reeds zijn aangesloten op het Diginetwerk zal nader moeten worden onderzocht.

Kiesraad
De Kiesraad maakt voor de werkplekken gebruik van de diensten van SSC-ICT. Via het netwerk van SSC-ICT is het mogelijk om verbonden te worden met de Haagse Ring en daarmee tot het Diginetwerk en daarmee tot het DHV.

Openbaar lichaam en Provincie
Of en in welke vorm het DHV wordt ontsloten naar de openbare lichamen en de provincies is nog niet duidelijk. Voor de openbare lichamen speelt daarbij mee dat onderzocht moet worden of de beschikbare netwerkmogelijkheden in het Caribische deel van Nederland aansluiten bij de gewenste betrouwbaarheid en veiligheid. Voor de uitrol van het DHV naar de openbare lichamen is, mede gelet op de relatief beperkte omvang van de ondersteunende organisatie, niet uit te sluiten dat er aanvullende (specifieke) begeleiding nodig is bij het aansluiten en het gebruik.

De provincies die bij de EK-verkiezing optreden als stembureau kunnen eveneens via Gemnet verbonden worden met Diginetwerk en daarmee toegang krijgen tot het DHV.

6.1.3. Gebruik DHV op een externe locatie

In de voorgaande paragaaf is ervan uit gegaan dat gebruikers via de werkstations binnen het organisatienetwerk toegang krijgen tot het DHV. Nu kan de situatie zich voordoen, met name in de situatie dat er sprake is van centrale stemopname door het GSB, dat buiten het organisatienetwerk-verbinding tot het DHV is vereist. Op een externe locatie zal naar verwachting geen netwerkaansluiting aanwezig zijn die gebruikt kan worden om verbinding te maken met het Diginetwerk. Ten aanzien van de externe locatie zijn de volgende opties mogelijk:

- De gemeente dient zelf zorg te dragen voor een geschikte netwerkverbinding tot Diginetwerk. Hiertoe kan de gemeente eventueel gebruik maken van bestaande thuiswerk voorzieningen waarmee toegang kan worden verkregen tot het gemeentelijknetwerk;
- Gemeenten die een externe locatie gebruiken kunnen door middel van centraal beschikbaar gestelde hardware een beveiligde VPN-verbinding opzetten naar het DHV;
- Gemeenten die een externe locatie gebruiken kunnen op werkstations VPN-client software installeren die de beveiligde VPN-verbinding tot stand brengt naar het DHV.

Op dit moment wordt ervan uit gegaan dat optie 1, waarbij de gemeente zelf de vereiste verbinding tot het DHV zorgt, het uitgangspunt is. In de situatie waarbij het voor de gemeente niet mogelijk is om tijdig de vereiste verbinding te realiseren, is het echter mogelijk dat de gemeente (tegen een kostendekkend tarief) de benodigde VPN-hardware kan verkrijgen waarmee de verbinding naar het DHV kan worden gerealiseerd.

6.2. Logging en monitoring

Logging en monitoring is een set van maatregelen waarbij de systeemcomponenten gebeurtenissen worden vastgelegd (loggen) en geanalyseerd (monitoring).

6.2.1. Logging

Onder logging wordt in het kader van het DHV in elk geval verstaan:

- Het verzamelen van evenementen (*events*) die plaatsvinden in elk van de componenten zoals beschreven onder hoofdstuk 2 Reikwijdte. Dit houdt onder andere in dat het netwerkverkeer van en naar het DHV wordt gelogd, maar ook dat alle events op alle infrastructurele componenten en de applicaties worden gelogd;
- Logging wordt op een zodanige wijze verzameld opgeslagen dat de integriteit niet kan worden aangetast;
- Logging dient (real time) beschikbaar te kunnen worden gesteld aan de veiligheidsdiensten. Het is een eis dat de inrichting van de datacentra en netwerken voldoet aan de benodigdheden van deze diensten;
- Logging heeft verschillende doelen:
    - Het achteraf kunnen onderzoeken of er misbruik is gemaakt van het DHV. In het verlengde hiervan is het tevens input voor forensische onderzoeken;
    - Het dient als input voor het SOC. Logevents worden automatisch doorgestuurd naar het SOC, waar op basis van speciale software wordt gemonitord op verdachte situaties.

6.2.2. Monitoring

Het aantal gebeurtenissen dat kan worden vastgelegd is vrijwel ongelimiteerd. Door speciale standaard software te gebruiken wordt de logging continu gemonitord op gebeurtenissen die kunnen duiden op onwenselijke situaties.

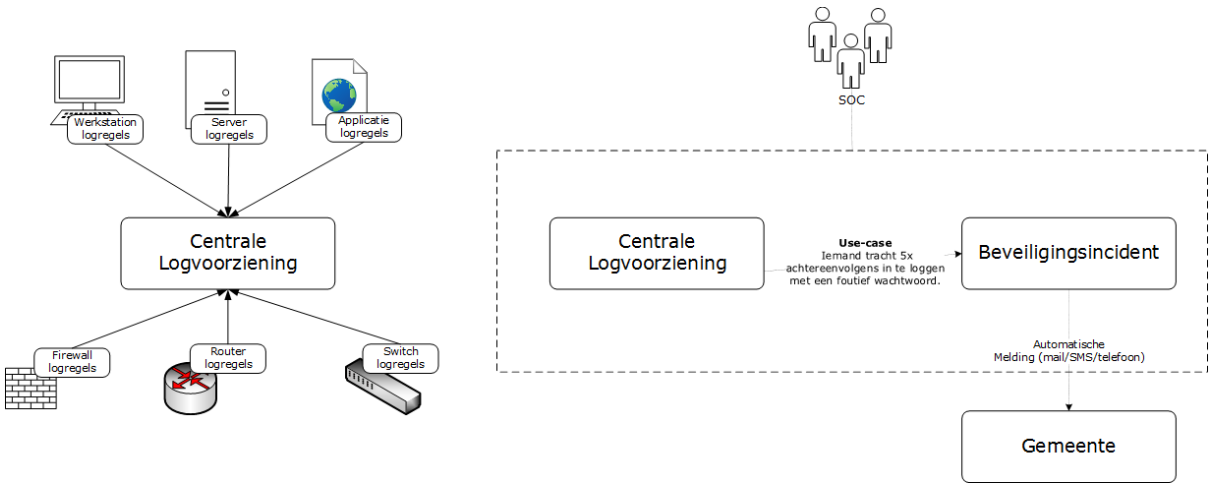
In onderstaande tabel zijn enkele voorbeelden opgenomen die als onwenselijk bestempeld kunnen worden (monitoring use cases):

Prioriteit	Titel melding / event	Datum	Tijd	Gebruiker	IP-adres	Activiteit	Details	Bronsysteem
Midden	Foutieve inlogpogingen	27-02-2020	10:00	Pietje Puk	192.168.1.1	Gebruiker heeft binnen 30 seconden meer dan 5 maal achtereenvolgens getracht in te loggen met een foutief wachtwoord.	<technische details>	Systeemnaam en IP-adres
Hoog	Benadering vanuit onbekend IP-nummer	24-02-2020	11:58	Foeke Ritsel	111.1.0.1	Het DHV wordt benaderd vanuit een locatie met een IP-nummer dat niet op de whitelist staat	<technische details>	IP-adres
Hoog	Invoer van uitslagen wordt heel frequent aangepast	23-02-2020	14:02	Jeroen de Klaas	191.117.1.1	Vanuit een specifieke gemeente worden de uitslagen veel vaker aangepast dan gemiddeld.	<technische details>	Systeemnaam en IP-adres
Middel	Hoge invoersnelheid gegevens	23-02-2020	12:01	Jan de Martin	191.118.1.1	Vanaf een werkstation worden continu 300 aanslagen per minuut gemeten. Deze snelheid is	<technische details>	Systeemnaam en IP-adres

Prioriteit	Titel melding / event	Datum	Tijd	Gebruiker	IP-adres	Activiteit	Details	Bronsysteem
						zo hoog dat aannemelijk is dat er een niet menselijke invoerder aan het werk is		

Er wordt een Security Operations Center (SOC) ingesteld dat centraal de computer- en netwerkactiviteiten van het DHV monitort. De log-informatie is afkomstig van de verschillende componenten van het DHV, zoals de Virtuele Desktop omgeving, servers- en netwerkcomponenten en vanuit de standaard- en maatwerksoftware. Het SOC monitort de log-informatie en kan daarbij, mede gebaseerd op use-cases (geautomatiseerd), onwenselijke situaties vaststellen en partijen daarover informeren of een mitigerende maatregelen in werking stellen. Het SOC kan tevens op basis van de beschikbare log-informatie zelfstandig onderzoeken of er sprake is van een mogelijk beveiligingsincident, bijvoorbeeld door netwerklogging te analyseren op afwijkende activiteiten.

Het SOC is operationeel gedurende de periode dat het DHV operationeel is. Voorafgaand aan de invoer van de uitslagen is het DHV operationeel om de verkiezing te configureren en de stembureau- en kandidaatgegevens vast te leggen. Na afloop van de vaststelling van de verkiezingsuitslag dienen gegevens van het DHV nog beschikbaar te zijn voor eventueel (strafrechtelijk) onderzoek.



Figuur 11: Vereenvoudigde visualisatie van de centrale logvoorziening en een melding naar gemeenten.

6.2.3. Gebruikerspad SOC

Het SOC monitort het DHV en rapporteert over mogelijke ongewenste situaties (incident). Voor de beoordeling en de afhandeling van een incident wordt een beroep gedaan op de gebruikersorganisatie (zoals het GSB/CSB, dan wel de gemeente) en de beheer organisatie (Kiesraad). Het is voor de afhandeling van incidenten van belang dat gebruikersorganisatie en de beheerorganisatie over medewerkers beschikken die meldingen van het SOC kunnen beoordelen en afhandelen. Voor de beoordeling en afhandeling wordt onderscheid gemaakt tussen functionele incidenten en infrastructurele incidenten.

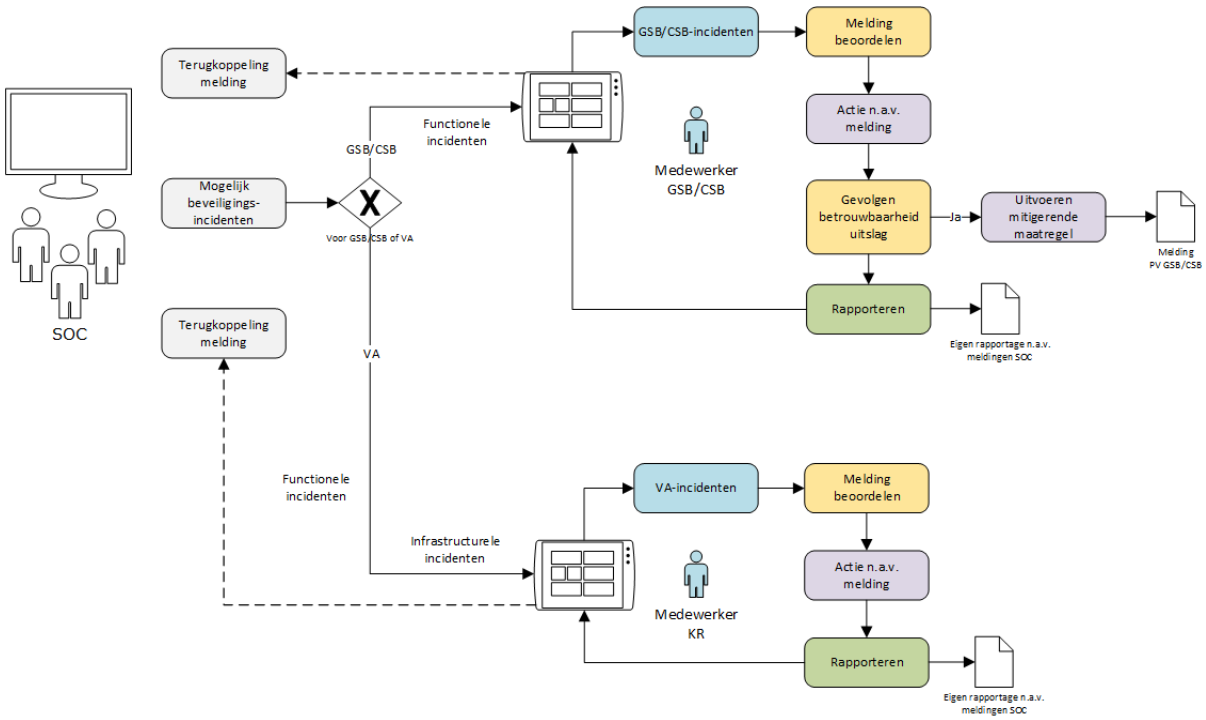
Functionele incidenten
De functionele incidenten hebben betrekking op gebruikers handelingen binnen een bepaalde GSB/CSB-compartiment. Een voorbeeld hiervan is dat een persoon van het GSB vijf keer probeert in te loggen met een verkeerd wachtwoord. In een dergelijke situatie moet een medewerker van de betreffende gebruikersorganisatie nagaan of het om een onschuldig voorval gaat of dat er

iemand is die ongeautoriseerd probeert in te loggen op het DHV. Functionele incidenten meldt het SOC aan de gebruikersorganisatie en worden niet gemeld aan de beheerorganisatie.

Infrastructurele incidenten

Bij infrastructurele incidenten gaat om incidenten die gericht zijn op de infrastructuur van het DHV of die van dusdanige aard zijn dat die buiten het functionele situatie vallen. Bij het laatste kan het bijvoorbeeld gaan om de situatie waarbij door het SOC wordt gedetecteerd dat er netwerk-gebaseerde aanvallen of hackpogingen met betrekking tot de webapplicatie worden uitgevoerd vanaf een of meerdere systemen. Ook indien zich een situatie voordoet dat meer dan 5 inlogpingen binnen een minuut gelijktijdig worden uitgevoerd op meerdere GSB/CSB-compartimenten, is het aannemelijk dat het niet gaat om enkele gebruikers die proberen in te loggen, maar dat er geautomatiseerde middelen worden ingezet om toegang te verkrijgen tot het DHV. Infrastructurele incidenten worden aan de Kiesraad gemeld en worden zo nodig in afstemming met andere (beheer)partijen, zoals de technische beheerder, afgehandeld. In bepaalde voorgediende situaties kan het SOC een mitigerende maatregel activeren, zoals het blokkeren van bepaalde IP-adressen voor toegang tot het DHV. Uitgangspunt is dat er snel wordt ingegrepen als de werking en/of betrouwbaarheid van het DHV in het geding is.

In de volgende afbeelding wordt schematisch weergegeven hoe incidenten die door het SOC zijn gesignaleerd worden afgehandeld door de gebruikersorganisatie of de beheerorganisatie.



Figuur 12: Schematische weergave van SOC incidenten en de afhandeling ervan.

Voor het GSB en CSB geldt dat zij bij de afhandeling van een incident moeten beoordelen of het incident gevolgen heeft voor de betrouwbaarheid van de uitslag. Van een situatie waarbij het GSB of CSB aanvullende maatregelen dient te nemen, is sprake als blijkt dat een bepaalde invoerder structureel afwijkende uitslaggegevens heeft ingevoerd en dat daarvoor geen goede verklaring voor is. Doet zoiets zich voor, dan kan het GSB/CSB alle ingevoerde uitslagen waar de desbetreffende invoerder bij betrokken was, aanvullend controleren om zich ervan te gewisse dat de (ingevoerde)uitslag de juiste is.

Onderdeel van de afhandeling van incidenten is dat de gebruikersorganisaties en de Kiesraad rapporteren naar aanleiding van de meldingen van het SOC. Naast een eigen rapportage over de

voorgedane incidenten wordt beoogd dat er een terugkoppeling plaatsvindt naar het SOC over de afhandeling van het incident. De terugkoppeling staat het SOC in staat om een totaalbeeld te geven van de incidenten en hoe deze zijn afgehandeld.

7. Beheer

Voor het beheer wordt onderscheid gemaakt tussen; functioneel beheer, applicatiebeheer en technisch-beheer. In dit hoofdstuk wordt nader ingegaan op de reikwijdte en relevante kaders bij de verschillende vormen van beheer.

7.1. Functioneel beheer

Daar waar het applicatiebeheer zich richt op het onderhoud en de doorontwikkeling van de applicatie(-software), en het technisch beheer op het onderhoud van de onderliggende hardware en infrastructuur, richt het functioneel beheer zich op het (blijvend) gebruik en gebruikersgemak van de applicatie. Functioneel beheer zorgt ervoor dat de gebruikers de juiste informatie, mogelijkheden en bevoegdheden hebben om de applicatie te kunnen gebruiken. Daarnaast houdt functioneel beheer in de gaten houden of de applicatie nog alles doet wat de gebruikers nodig hebben om hun werkzaamheden uit te voeren.

Functioneel beheer is hiermee de 'linking pin' tussen het verkiezingsproces en het DHV. De Kiesraad is de functioneel beheerder van het DHV en hanteert daarbij het BiSL framework (Business information Services Library) als raamwerk. BiSL is een best-practice voor functioneel beheer en informatiemanagement, dat zich richt op de vraagzijde van de informatievoorziening en de aansluiting borgt tussen de primaire processen enerzijds en de ondersteunende ICT anderzijds.

In de werkzaamheden voor functioneel beheer wordt onderscheidt gemaakt tussen de periode tijdens de vaststelling van de verkiezingsuitslag, en de perioden tussen de verkiezingen in.

7.1.1. Functioneel beheer tijdens de vaststelling van de verkiezingsuitslag

De werkzaamheden van functioneel beheer tijdens een verkiezingsperiode bestaan onder andere uit het:

- Configureren van het DHV ten behoeve van de betreffende verkiezing;
- Beveiligingsbeheer op het gebied van toegang, rollen en autorisatie;
- Aanmaken van gebruikers DHV ten behoeve van de betreffende verkiezing (bijv. voorzitter GSB en Beheerder GSB);
- Zijn van het eerste aanspreekpunt en gesprekspartner voor GSB/CSB en ketenpartners (gebruikers), leverancier(s) en applicatie- en technisch beheer van het DHV;
- (mede)Prioriteren en coördineren van spoedwijzigingen;
- Informeren en adviseren van gebruikers over het gebruik, incidenten en calamiteiten, etc. van het DHV (in de verkiezingsperiode).

7.1.2. Functioneel beheer in de periode tussen de verkiezingen in

De werkzaamheden van functioneel beheer in de periode tussen de verkiezingen in, bestaan onder andere uit het:

- Inrichten van een gebruikersoverleg;
- Inventariseren eisen en wensen aan het DHV van de gebruikers van het DHV;
- Opstellen impactanalyses naar aanleiding van beoogde aanpassingen/doorontwikkeling aan het DHV;
- Opstellen en bewaken van eisen voor aanpassingen/doorontwikkeling aan het DHV (vertaling van gebruikerseisen en wensen naar eisen voor de leverancier(s));
- Testen van de nieuwe en/of aangepaste functionaliteit, en regressietesten van de huidige functionaliteit, van het DHV;
- Organiseren en begeleiden van (gebruikers)acceptatietesten voor nieuwe en/of aangepaste functionaliteit van het DHV;
- Begeleiden implementatie van een nieuwe release van het DHV;
- Ondersteunen van gebruikers bij het gebruik van het DHV, uitvoering zal met name door leverancier plaatsvinden (training, helpdesk, etc.);
- Informeren en adviseren van gebruikers over het gebruik, wijzigingen, toekomstige ontwikkelingen, etc. van het DHV;

- Zijn van het eerste aanspreekpunt en gesprekspartner voor gebruikers en ketenpartners, leverancier(s) en applicatie- en technisch beheer van het DHV;
- Beheren van de documentatie rondom het DHV, uitvoering zal met name door de leverancier plaatsvinden (inrichtingsdocumentatie, gebruikershandleidingen, opleidingsdocumentatie, etc.).

7.2. Applicatiebeheer

Het applicatiebeheer is erop gericht om de continuïteit van het DHV te waarborgen. Onder het applicatiebeheer vallen verschillende (beheer, onderhoud en doorontwikkeling) werkzaamheden en processen. Het applicatiebeheer dient op efficiënte en betrouwbare wijze plaats te vinden op basis van bestendigde processen zoals opgenomen in de Application Services Library (ASL). Het applicatiebeheer omvat:

- Correctief onderhoud: Het oplossen van fouten en incidenten;
- Adaptief onderhoud: Het aanpassen van de applicatie n.a.v. het optimaliseren en/of verbeteren van de prestatie van de applicatie;
- Preventief onderhoud: het onderhouden van de applicatie om eventueel optredende incidenten en ongewenste situaties te voorkomen;
- Doorontwikkeling: Het aanpassen van de applicatie naar aanleiding van nieuwe of gewijzigde technische en functionele wensen en eisen.

Heden ten dage zijn er verschillende tools die worden toegepast bij de invulling van het applicatiebeheer en die een belangrijke rol spelen bij de communicatie tussen partijen. Het is belangrijk dat deze tools ook voor de verschillende partijen efficiënt werken en een meerwaarde hebben, zoals:

- Gemakkelijk en overzichtelijk indienen van verzoeken (zoals change/service requests);
- Inzicht verschaffen in de actuele status van verzoeken en de voortgang ervan;
- Inzicht verschaffen in oudere (afgehandelde) verzoeken en de afhandeling ervan;
- Attenderen als er sprake is van een te ondernemen actie naar aanleiding van een verzoek.

In hoofdstuk 8 Niet-functionele eisen staan verschillende normen en kaders die (mede)bepalend zijn voor de nadere invulling van het applicatiebeheer.

7.3. Technisch beheer

Onder technisch beheer verstaan wij in het kader van het DHV op hoofdlijnen het volgende:

- Het inrichten van de infrastructuur waar het DHV gebruik van maakt. Dit houdt onder meer in:
  - Installeren van de componenten;
  - Inrichten van wijzigingenbeheer;
  - Inrichten en bijhouden van alle componenten in een Configuration Management Database (CMDB);
  - Configureren van de componenten.
- Het beveiligen van de infrastructuur waar het DHV gebruik van maakt conform de eisen die de Kiesraad aan de beveiliging stelt. Dit houdt onder meer de volgende aspecten in:
  - Inrichten van fysiek- en logisch toegangsbeheer tot de componenten;
  - Inrichten van een hardeningsproces voor alle componenten;
  - Inrichten van een patchmanagementproces voor alle componenten;
  - Inrichten van netwerksegmentatie;
  - Inrichten van beschikbaarheidsbeheer;
  - Inrichten van vulnerabilitymanagementprocessen;
  - Inrichten van logging op alle componenten;
  - Aansluiten van de componenten op Intrusion Detection en Intrusion Prevention Systemen van het SOC.

7.3.1. Buiten reikwijdte technisch beheer infrastructuur

De infrastructuur van gemeenten, het Diginetwerk, GGI-Netwerk en Gemnet vallen buiten de reikwijdte van het technisch beheer van het DHV.

7.3.2. Afweging technisch beheerpartij

Er zijn verschillende modellen mogelijk voor het beheren van de infrastructuur. Een belangrijke afweging betreft de keuze in hoeverre de hostingpartij het technisch beheer op de infrastructuur mag uitvoeren. Hieronder zijn een tweetal opties verder beschreven.

7.3.2.1. *Kiesraad voert technisch beheer uit*

In deze optie voert de Kiesraad zelf het technisch beheer van de infrastructuur uit. Dit heeft als gevolg dat de hostingpartij uitsluitend het datacenter en de fysieke systemen (zoals servers en switches) levert. Praktisch zal de Kiesraad een beheerteam moeten opzetten met de kennis en kunde om het technisch beheer uit te kunnen voeren. In de onderstaande paragrafen zijn de consequenties ten aanzien van de beveiliging van het DHV en de uitvoerbaarheid beschreven.

Beveiliging
Het voordeel van deze optie is dat de Kiesraad volledig *in control* is van de infrastructuur (behalve de fysieke hosting van apparatuur). Het kan de beveiligingseisen zelf naleven en handhaven. Een ander voordeel is dat de Kiesraad de medewerkers die de infrastructuur beheren zelf kan screenen, waardoor er een sterker gevoel van controle ontstaat. Het is echter de vraag of de sterkere mate van controle of het technisch beheer zich vertaalt in een sterkere mate van feitelijke beveiliging van de infrastructuur.

Uitvoerbaarheid
Deze optie kent echter ook uitdagingen ten aanzien van de uitvoerbaarheid:

- Naast de functioneel beheer werkzaamheden, heeft de Kiesraad eveneens de beheerfunctie voor het technisch beheer en de daarbij behorende operationele taken;
- De Kiesraad dient een technisch beheerteam samen te stellen of aan te nemen, aangezien het deze rol tot op heden niet heeft gehad. Dit brengt organisatorische wijzigingen en kosten met zich mee.

7.3.2.2. *Hostingpartij voert technisch beheer uit*

Een alternatieve optie is het technisch beheer uit laten voeren door dezelfde partij als waar de hosting wordt afgenomen.

Beveiliging
Een voordeel van het beleggen van het technisch beheer bij de hostingpartij is dat dergelijke leveranciers doorgaans zeer veel ervaring hebben bij deze werkzaamheden. Indien een ervaren en volwassen organisatie het technisch beheer doet, kan dit de kans verkleinen dat de infrastructuur onverhoopt onveilig wordt geconfigureerd.
Bij deze optie is de Kiesraad in mindere mate *in control* van de infrastructuur. Waar bij optie 1 de Kiesraad de volledige controle heeft over de infrastructuur en de mensen die de infrastructuur beheren, is het bij deze optie afhankelijk van de vastgelegde afspraken en eisen met de hostingpartij. De Kiesraad kan, naast de vastgelegde afspraken en eisen, aanvullende controle uitoefenen bij de hostingpartij, bijvoorbeeld door periodiek door middel van een audit te onderzoeken in hoeverre de afspraken worden nageleefd.

Uitvoerbaarheid
Deze optie kent echter de volgende uitdagingen ten aanzien van de uitvoerbaarheid:

- Deze optie vereist een sterke regierol van de Kiesraad. Het goed inrichten van leveranciersmanagement bij de Kiesraad is essentieel.
- Voor leveranciersmanagement dient een team te worden samengesteld, wat organisatorische wijzigingen en kosten met zich mee brengt.

7.3.2.3. *Advies*

Gezien de uitdagingen ten aanzien van de uitvoerbaarheid van optie 1, is het advies om het technisch beheer van infrastructurele componenten bij de hostingpartij te beleggen. Het is hierbij randvoorwaardelijk dat:

- De Kiesraad een betrouwbare hostingpartij te kiezen met sterke ervaring op dit gebied (opstellen selectie- en gunningscriteria);
- Alle afspraken en beveiligingseisen rondom de infrastructuur formeel zijn vastgelegd in contractdocumentatie tussen de Kiesraad;
- De Kiesraad periodiek bij de hostingpartij onderzoekt of deze eisen worden nageleefd (bijvoorbeeld door middel van een audit).

7.3.3. Hosting

Er bestaan verschillende risico's bij het hosten van het informatiesysteem door een interne of externe hostingpartij. Onder hosting verstaan wij in deze context een dienst die de Kiesraad afneemt van een partij voor het aanbieden van de centrale software op infrastructuur (zoals servers en netwerkcomponenten). Onderstaand zijn enkele in het oog springende risico's beschreven, waarna de maatregelen om deze risico's te mitigeren zijn toegelicht.

7.3.3.1. *In het oog springende risico's*

De onderstaande risico's beschrijven op hoofdlijnen de scenario's waarmee rekening gehouden moet worden bij het hosten van het informatiesysteem:

- De hostingpartij maakt fouten, manipuleert de infrastructuur of is gehackt, waardoor de integriteit of beschikbaarheid van de uitslagberekening niet kan worden gegarandeerd;
- De keten van toeleveranciers van de hostingpartij maakt fouten, manipuleert de infrastructuur (zoals de hardware) of is gehackt, waardoor de integriteit of beschikbaarheid van de uitslagberekening niet kan worden gegarandeerd;
- De hostingpartij en/of keten van toeleveranciers is kwetsbaar voor manipulatie door andere staten, waardoor de integriteit van de infrastructuur en hardware niet kan worden geborgd;
- Medewerkers van de hostingpartij verkrijgen via de infrastructuur oneigenlijke toegang tot de verkiezingsdata en manipuleren de uitslagen moedwillig;
- Er zitten kwetsbaarheden in de infrastructuur van de hostingpartij, waardoor ongeautoriseerden toegang kunnen verkrijgen tot het systeem of het systeem onbeschikbaar kunnen maken;
- De fysieke beveiliging van het datacenter is ontoereikend, waardoor onbevoegden toegang verkrijgen tot de infrastructuur;
- Door een incident of ramp (zoals brand of overstroming) raakt het datacenter onbeschikbaar of gaat de hardware onderliggend aan de hostingdienst kapot.

7.3.3.2. *Eisen hosting*

Voor de hosting van de centrale oplossing worden op hoofdlijnen de volgende eisen gesteld:

- De Kiesraad voert controle en toezicht uit op de hosting. De gebruikte datacenters bevinden zich bij voorkeur op Nederlands grondgebied en in ieder geval binnen de EER. De Kiesraad is eigenaar van de (virtuele)compartimenten en de daarbinnen gebruikte programmatuur. Specifieke fysieke componenten (zoals data diodes) om compartimenten/systemen af te scheiden, zijn tevens eigendoem van de Kiesraad;
- De hosting wordt uitsluitend beheerd door personen met een Verklaring van Geen Bezwaar (VGB) of vergelijkbare screening;
- De leverancier (het bedrijf/de organisatie) wordt onderworpen aan een screening om vast te stellen dat er geen gevaar bestaat voor de veiligheid conform de regeling omtrent de naslag op verzoek naar personen en organisaties. Deze eis geldt niet indien gebruik wordt gemaakt van insourcing, bijvoorbeeld indien SSC-ICT de hosting zal verzorgen in een Rijksdatacenter;

- De hostingpartij moet de geschatte piekbelasting aan kunnen. Deze piekbelasting dient te worden berekend in samenwerking met de Kiesraad, hostingpartij en softwareontwikkelaar. Hierover dienen afspraken te worden opgenomen in de aanbesteding;
- De hostingpartij moet capaciteit kunnen bijschakelen bij onverhoopt beperkte beschikbaarheid van het systeem;
- Alle afspraken rondom de dienstverlening (o.a. ten aanzien van de beschikbaarheid van de infrastructuur) dienen te worden vastgelegd in een Dienstenniveau-overeenkomst (DNO)/Service Niveau Overeenkomst (SNO);
- Voor het hosten van het informatiesysteem worden de best practices omtrent hosting toegepast. Onderstaande richtlijnen specifiek gericht op hosting worden in elk geval toegepast:
    - Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Huisvesting Informatievoorziening;
    - NCSC Factsheet virtualiseer met verstand;
    - Op basis van de gekozen infrastructurele componenten worden daarnaast passende hardeningsrichtlijnen per component toegepast. Bijvoorbeeld: een Microsoft server dient conform best practices op het gebied van Microsoft server hardening te worden geconfigureerd, een Cisco router wordt conform best practices voor Cisco routers gehardend, etc.
- De hostingpartij en de keten van toeleveranciers dienen daarnaast aantoonbaar te voldoen aan algemene beveiligingseisen en -kaders:
    - BIO;
    - AVG.
- De Kiesraad zal door middel van een onafhankelijke auditor beoordelen of de softwareontwikkelaar voldoet aan de hierboven gestelde richtlijnen en kaders;
- Het vierogenprincipe wordt ook bij het beheer van de infrastructuur toegepast. Wijzigingen in de infrastructuur kunnen uitsluitend door twee geautoriseerde beheerders worden doorgevoerd;
- Er dient redundantie te worden aangebracht in de hosting;
- Er dient gebruik te worden gemaakt van minimaal twee fysiek gescheiden datacenters;
- De hosting dient te voldoen aan de eisen rondom beschikbaarheid en disaster recovery zoals in detail beschreven in paragraaf 8.1.

Voor een volledige uitwerking van alle eisen voor de hostingpartij kan het Programma van Eisen worden geraadpleegd.

7.3.4. Meerdere hostingpartijen

Om de integriteit en beschikbaarheid van het DHV te verhogen, kunnen maatregelen worden getroffen met betrekking tot de inzet van meerdere hostingpartijen. Er bestaan verschillende varianten van dergelijke maatregelen, allen met een impact op het beveiligingsniveau en de uitvoerbaarheid. In deze paragraaf worden de keuzes ten aanzien van het gebruik van meerdere hostingpartijen met betrekking tot het DHV beschreven.

Er zijn de volgende keuzes gemaakt in de basisarchitectuur:
- Er wordt gebruikgemaakt van een hostingpartij die dient te voldoen aan de eisen zoals tevens beschreven in paragraaf 4.7 'Naleving en controle' en paragraaf 7.3.3.2 'Eisen hosting';
- Om de beschikbaarheid van de infrastructuur te bevorderen, wordt redundantie aangebracht in het ontwerp. Voor datacentra geldt dat in de aanbestedingseisen wordt opgenomen dat een hostingpartij standaard gebruikmaakt van minimaal twee fysiek gescheiden datacentra. Als een datacentrum uitvalt, dan kan de dienstverlening worden voortgezet vanaf het andere datacentrum. Daarnaast is de aanname dat ook andersoortige high-availability maatregelen dienen te worden ingezet (denk aan: gebruik van clusters,

loadbalancers, master-slave nodes en andere technieken). Aanvullend dient een sterk back-up en continuïteitsplan te worden opgesteld, waarin wordt beschreven hoe in het geval van onbeschikbaarheid van een hostingpartij kan worden overgeschakeld naar een ander datacentrum;
- Er wordt geen gebruikgemaakt van twee hostingpartijen om maatregelen in te voeren om de integriteit van de uitslagvaststelling verder te verhogen. In het ontwerp zitten verschillende sterke maatregelen (digitaal ondertekenen bestanden, compartimentering, afgeschermde omgeving voor zetelberekening, etc.) die de integriteit van de verwerkte gegevens bevorderen. Daarnaast worden buiten het DHV om ook maatregelen getroffen om te detecteren of het DHV integer heeft gewerkt (zie ook paragraaf 2.2.2 'Aanvullende informatie beveiligingsmaatregelen die buiten scope van het DHV vallen'). Een separate tweede hostingpartij bieden beperkte meerwaarde, maar brengen zeer hoge kosten en impact in de uitvoerbaarheid met zich mee. Derhalve is de keuze gemaakt om geen gebruik te maken van twee hostingpartijen.

7.4. Softwareontwikkeling

Er bestaan verschillende risico's bij het ontwikkelen van software door een leverancier. Onderstaand zijn enkele in het oog springende risico's beschreven, waarna de maatregelen om deze risico's te mitigeren zijn toegelicht.

7.4.1. In het oog springende risico's

De onderstaande risico's beschrijven op hoofdlijnen de scenario's waarmee rekening gehouden moet worden bij het ontwikkelen van de software:
- De softwareontwikkelaar maakt fouten, manipuleert de software of is gehackt, waardoor de integriteit of beschikbaarheid van de uitslagberekening niet kan worden gegarandeerd;
- De keten van toeleveranciers van de softwareontwikkelaars maakt fouten, manipuleert de software of is gehackt, waardoor de integriteit of beschikbaarheid van de uitslagberekening niet kan worden gegarandeerd;
- De softwareontwikkelaar en/of keten van toeleveranciers is kwetsbaar voor manipulatie door andere staten, waardoor de integriteit van de software niet kan worden geborgd;
- De softwareontwikkelaar ontwikkelt de broncode op een wijze dat de Kiesraad niet eenvoudig kan overstappen naar een andere leverancier;
- Er zitten kwetsbaarheden in de ontwikkelde software, waardoor ongeautoriseerden toegang kunnen verkrijgen tot het systeem of het systeem onbeschikbaar kunnen maken.

7.4.2. Eisen ontwikkelen software

Voor het ontwikkelen van de software worden de volgende eisen gesteld:
- De Kiesraad is eigenaar van de software en is in control van de systeemacceptatie;
- De ontwikkelde software voldoet aan de kaders die uit de Kieswet volgen, waaronder die op grond van artikel P 1a Kieswet, zoals opgenomen in 'Bijlagen C: Huidig wettelijk eisen kader (art P1a)'. Onderdeel hiervan is dat de broncode openbaar wordt gemaakt;
- De softwareleverancier (het bedrijf/de organisatie) wordt onderworpen aan een screening om vast te stellen dat er geen gevaar bestaat voor de veiligheid conform de regeling omtrent de naslag op verzoek naar personen en organisaties[10]. Uitsluitend in het geval dat er geen negatief advies wordt gegeven, zal de leverancier de software ontwikkelen;
- De software wordt uitsluitend ontwikkeld door personen met een Verklaring van Geen Bezwaar (VGB) of vergelijkbare screening;
- De Kiesraad stelt eisen aan de ontwikkelmethode. De leverancier kan de ontwikkelmethode nader uitwerken in de aanbesteding, binnen de kaders die door de Kiesraad zijn gesteld in het daarvoor opgestelde Programma van Eisen;

[10] "Regeling omtrent de naslag op verzoek van anderen naar personen en organisaties" is gepubliceerd in de Staatscourant en beschikbaar op de website van de AIVD.

- De Kiesraad bepaalt de functionele en non-functionele eisen en kan deze te allen tijde wijzigen;
- Indien kwetsbaarheden worden aangetroffen, dient de softwareontwikkelaar deze tijdig en adequaat te verhelpen. Dergelijke afspraken dienen in contractdocumentatie te worden opgenomen;
- De Kiesraad maakt afspraken met de softwareontwikkelaar ten aanzien van responsible disclosure, zodat burgers en andere betrokkenen kwetsbaarheden in de software op een gecontroleerde manier kunnen melden;
- De softwareontwikkelaar dient reproducible builds van de software te maken, zodat kan worden geverifieerd dat de gecompileerde software overeenkomt met de open source code;
- De softwareontwikkelaar dient te worden verplicht om maatregelen te treffen om ongeoorloofde wijzigingen aan de software te detecteren;
- Voor het ontwikkelen van het informatiesysteem worden de best practices omtrent Secure Software Development toegepast. Onderstaande richtlijnen specifiek gericht op Secure Software Development worden in elk geval toegepast en gespecificeerd in het Programma van Eisen:
    - Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Applicatieontwikkeling;
    - NCSC Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software;
    - NCSC ICT-beveiligingsrichtlijnen voor Webapplicaties
    - OWASP Application Security Verification Standard.
- De softwareleverancier en de keten van toeleveranciers dienen daarnaast aantoonbaar te voldoen aan algemene beveiligingseisen en -kaders:
    - BIO;
    - AVG.

De Kiesraad zal door middel van een onafhankelijke auditor beoordelen of de softwareontwikkelaar voldoet aan de hierboven gestelde richtlijnen en kaders. Zie hierover ook paragraaf 4.7 Naleving en controle.

Voor een volledige uitwerking van alle eisen voor de softwareontwikkelaar kan het Programma van Eisen worden geraadpleegd.

7.5. Introductie OTAP-straat

Bij het ontwikkelen van software wordt vaak gebruikgemaakt van een zogenoemde OTAP (Ontwikkeling, Test, Acceptatie, Productie)-straat. Deze methodiek wordt gebruikt om verschillende fasen tijdens softwareontwikkeling gestructureerd te doorlopen. Onderstaand is een korte beschrijving van deze stappen en de bijbehorende omgevingen opgenomen.

- **Ontwikkeling**: de software wordt ontwikkeld in een aparte ontwikkelomgeving. Deze omgeving is toegankelijk voor de softwareontwikkelaars en is niet aangesloten op de productieomgeving;
- **Test**: nadat software in de ontwikkelomgeving is ontwikkeld, wordt de code doorgaans overgezet naar de testomgeving. In deze omgeving wordt de software automatisch of manueel getest, zowel technisch als functioneel. In deze omgeving wordt de software tevens vaak getest op kwetsbaarheden door middel van een penetratietest;
- **Acceptatie**: nadat de software is goedgekeurd, wordt deze overgebracht naar de acceptatieomgeving. In deze omgeving is de hardware en de infrastructuur (nagenoeg) gelijk aan de productieomgeving. In deze omgeving kan de software derhalve getest worden zoals het in productie zou draaien. Ook de acceptatieomgeving wordt veelal gebruikt om de software te testen op kwetsbaarheden via een penetratietest;
- **Productie**: Nadat de software alle testen succesvol heeft doorlopen, wordt deze naar de productieomgeving gebracht. Dit is de omgeving die daadwerkelijk wordt gebruikt door de eindgebruikers.

Het uitgangspunt hierbij is dat de verschillende OTAP-omgevingen sterk van elkaar zijn gescheiden. Dit betreffen aparte omgevingen die los van elkaar functioneren.

7.5.1. Beveiliging

Voor het DHV is het wenselijk om gebruik te maken van een dergelijke OTAP-straat. Dit heeft verschillende voordelen ten aanzien van de beveiliging van het DHV:

- Het verkleint de kans dat een softwareontwikkelaar onverhoopt een aanpassing aan het DHV in productie brengt met nadelige gevolgen heeft voor de beschikbaarheid, integriteit of vertrouwelijkheid van het systeem. Alle wijzigingen worden immers uitvoerig getest in verschillende omgevingen voordat deze in productie worden gebracht;
- Het verkleint de kans dat een kwaadwillende softwareontwikkelaar ongezien ongeautoriseerde wijzigingen aanbrengt in het DHV. Indien een ongeautoriseerde wijziging wordt aangezien de software na het aanbrengen van de wijziging nog functioneel, technisch en op beveiliging wordt getest door andere personen en instanties;
- Indien een van de ontwikkelomgevingen is gecompromitteerd door een aanvaller, verkleint een sterk afgescheiden OTAP-straat de kans dat de productieomgeving van het DHV ook wordt gecompromitteerd;
- Een OTAP-straat biedt de Kiesraad de mogelijkheid om de ontwikkelpartij de toegang tot de productieomgeving te ontnemen. Het is mogelijk om de ontwikkelpartij slechts autorisaties toe te kennen om de test, ontwikkel en acceptatieomgeving te benaderen. De Kiesraad kan vervolgens de ontwikkelde code in productie brengen.

7.5.2. Uitvoerbaarheid

Een OTAP-straat brengt daarnaast enkele aandachtspunten ten aanzien van de uitvoerbaarheid met zich mee. Onderstaand zijn enkele in het oog springende aandachtspunten beschreven:

- Het proces voor het ontwikkelen en in productie brengen van het DHV dient te worden vastgelegd in procesbeschrijvingen;
- Het proces voor het doorvoeren van wijzigingen in de software kan mogelijk een te lange doorlooptijd hebben voor spoedwijzigingen. Indien er bijvoorbeeld bij uitzondering een belangrijke wijziging moet worden aangebracht in de software op de dag van te telling, dient hiertoe een noodprocedure te worden opgesteld. Dit is van belang om de gebruikers van het DHV tijdig te kunnen voorzien van een geüpdatet DHV.

8. Niet-functionele eisen

Naast de functionele eisen, zoals beschreven in hoofdstuk 5 'Functionele-opzet', zijn ook de niet-functionele eisen van essentieel belang bij de realisatie van het DHV. De functionele eisen beschrijven een systeem of applicatie in termen van functionaliteit of 'specifiek gedrag' (Wat moet het systeem doen?). Niet-functionele eisen beschrijven een systeem of applicatie in termen van kwaliteit in brede zin, met eisen aan betrouwbaarheid, beveiliging, beschikbaarheid, schaalbaarheid, bruikbaarheid en/of gebruikersgemak, onderhoudbaarheid, overdraagbaarheid, etc.

In onderstaande paragrafen zijn de essentiële niet-functionele eisen voor het DHV benoemd en op hoofdlijnen uitgewerkt.

8.1. Betrouwbaarheidseisen

Het informatiesysteem moet voldoen aan de betrouwbaarheidseisen voor beschikbaarheid, integriteit en vertrouwelijkheid. Onderstaand zijn de belangrijkste uitgangspunten ten aanzien van deze betrouwbaarheidseisen beschreven.

Betrouwbaarheidseis	Waardering	Beschrijving
Beschikbaarheid	Hoog	Het informatiesysteem moet in de week van de verkiezingen beschikbaar zijn om de uitslag te kunnen invoeren en verwerken. Binnen twee dagen na de verkiezingen dient de uitslag vastgesteld te worden. Het digitale hulpmiddel dient in ieder geval daarom de twee dagen na de dag van de stemming maximaal beschikbaar te zijn. Welke beschikbaarheidseisen worden verwacht, is na deze tabel nader beschreven. Uitval van het systeem in deze periode kan leiden tot grootschalige publieke verontwaardiging, negatieve publiciteit, vertraging en het verlies van vertrouwen in het verkiezingsproces.
Integriteit	Hoog	De juistheid en volledigheid van de informatie verwerkt in het informatiesysteem is van groot belang om de integriteit van het verkiezingsproces te waarborgen. Zonder juistheid en volledigheid van de informatie, kan het vertrouwen, transparantie en controleerbaarheid van het verkiezingsproces niet worden geborgd.
Vertrouwelijkheid	Midden	Het informatiesysteem verwerkt verschillende gegevens, waaronder het aantal toegelaten kiezers, het aantal stemmen per lijst, het aantal blanco stemmen, het aantal ongeldige stemmen en (persoons)gegevens van politici. De vertrouwelijkheid van het aantal stemmen is laag: deze informatie is openbaar. Kennisname van (persoons)gegevens van o.a. de politici en eventueel gebruikers van het systeem door onbevoegden is ongewenst en kan een afwijking vormen ten opzichte van de AVG.

Beschikbaarheid

De mogelijkheden om een informatiesysteem te gebruiken hangen samen met twee parameters:

- Servicewindow: dit is de periode op een dag dat het systeem gebruikt kan worden met ondersteuning van de leverancier. In deze periode kan gepland onderhoud plaatsvinden zonder dat dit invloed heeft op afgesproken beschikbaarheidsniveau;
- Beschikbaarheid: dit is het percentage van het servicewindow dat het systeem daadwerkelijk beschikbaar dient te zijn. Hierbij is het ongeplande onbeschikbaarheid de factor die bepalend is. De periode waarover de beschikbaarheid wordt gemeten is een kalenderweek (van zondag t/m zaterdag).

Voor het DHV is door het incidentele karakter van de applicatie geen vast servicewindow en beschikbaarheid te definiëren. Deze hangen samen met het verloop van de verkiezing. IJkpunt is hierbij de dag van stemming. Het systeem dient drie weken, voor de dag van stemming beschikbaar te zijn voor gebruikers van gemeenten, GSB en CSB. Dit is een indicatie en kan eventueel wijzigen of per verkiezing verschillen. Het systeem dient eveneens (bij benadering) drie weken na de dag van stemming beschikbaar te zijn voor gebruikers van gemeenten, GSB en CSB. In de periode van ongeveer zes weken dat het DHV wordt ingezet voor de vaststelling van de verkiezingsuitslag is een hoge beschikbaarheid vereist, welke als volgt is opgebouwd (merk op: dit betreft de productieomgeving):

Periode	**Sevicewindow van / tot**	**Beschikbaarheid**
3 weken tot de dag van stemming	7:30 - 18:30 uur	90% het systeem mag binnen deze periode tussen de genoemde uren dus maximaal 66 min/dag niet beschikbaar zijn
	18.30 - 7.30 uur	70%
dag van stemming en de aansluitende week (datum stemming +0 t/m +7 dagen)	0.00 - 24.00 uur	99% het systeem mag binnen deze periode dus gemiddeld 14,4 min/dag niet beschikbaar zijn met maximum van 30 min/dag)
2 weken na de eerste week na de dag van stemming (datum stemming +8 t/m +22 dagen) NB. Binnen deze periode bestaat de mogelijk om, in geval van een nieuwe stemopname, de beschikbaarheid te verhogen	7:30 - 18:30 uur	90% het systeem mag binnen deze periode tussen de genoemde uren dus maximaal 66 min/dag niet beschikbaar zijn
	18.30 - 7.30 uur	70%
Buiten de verkiezingsperiode van 6 weken	Op afspraak.	Voor gebruikers: niet beschikbaar Voor ontwikkelen, testen en functioneel beheer is de beschikbaarheid van het systeem +/- 70%.

8.2. Verwerken persoonsgegevens

Met het DHV zullen persoonsgegevens worden verwerkt. De verwerking van persoonsgegevens dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG. Dit betekent dat er passende technische en organisatorische maatregelen genomen dienen te worden om de persoonsgegevens te beschermen. De opgenomen maatregelen zijn ook van toepassing op partijen die in opdracht verwerkingen uitvoeren op de persoonsgegevens.

Op de verwerking van persoonsgegevens zijn de volgende algemene uitgangspunten van toepassing:

- Pas in beginsel pseudonimisering en versleuteling van persoonsgegevens toe zodat deze in beginsel niet herleidbaar zijn;
- De persoonsgegevens zijn enkel toegankelijk voor diegenen die daarvoor geautoriseerd zijn;
- Bewaar persoonsgegevens niet langer dan noodzakelijk;
- Bepaal hoe er gehandeld dient te worden als gegevens onrechtmatig worden verwerkt.

Deze uitgangspunten dienen te worden omgezet naar passende technische en organisatorische maatregelen. Hiervoor is het van belang vast te stellen ten aanzien van welke (persoons)gegevens privacybeschermende maatregelen genomen dienen te worden en in welke mate er sprake kan zijn van een privacyschending. De persoonsgegevens die in het digitaal hulpmiddel worden verwerkt zijn in twee groepen onder te verdelen:

1. Kandidaatsgegevens: gegevens van personen die voorkomen op de kandidatenlijst;
2. Gebruikersgegevens: gegevens van personen die geautoriseerd zijn om gebruik te maken van het digitale hulpmiddel.

Kandidaatsgegevens
Kandidaatsgegevens zijn onder te verdelen in twee categorieën: de gegevens van personen die op grond van de Kieswet verwerkt worden en de (aanvullende) persoonsgegevens die niet op grond van de Kieswet worden verwerkt. Op de persoonsgegevens die op grond van de Kieswet worden verwerkt is de Uitvoeringswet AVG niet van toepassing.[11] Op grond van de Kieswet worden de volgende persoonsgegevens verwerkt:

- Naam;
- Initialen;
- Roepnaam;
- Geslachtsaanduiding;
- Geboortedatum;
- Woonplaats;
- Correspondentieadres;
- Politieke gezindheid.

Op grond van de Kieswet zijn de kandidaatsgegevens niet als vertrouwelijk aan te merken. De kandidaatsgegevens worden actief openbaar gemaakt zodat de kiezer in staat wordt gesteld kennis te nemen op welke personen gestemd kan worden. Tevens vereist de controleerbaarheid en transparantie van het verkiezingsproces dat de gegevens van kandidaten beschikbaar zijn voor burgers. Gelet op het voorgaande wordt aan de verwerking van kandidaatsgegevens geen privacyrisico toegekend en worden er geen specifieke maatregelen voorzien ten aanzien van deze groep van persoonsgegevens.

Naast de in de Kieswet opgenomen kandidaatsgegevens, kan er sprake zijn van de verwerking van aanvullende persoonsgegevens van kandidaten. Op dit moment wordt niet voorzien dat aanvullende kandidaatsgegevens in het digitaal hulpmiddel worden verwerkt.

Gebruikersgegevens
In het digitale hulpmiddel worden persoonsgegevens van gebruikers verwerkt ten behoeve van de authenticatie en autorisatie van gebruikers en voor het monitoren en controleren van de handelingen die in het digitale hulpmiddel worden verricht door gebruikers. De volgende persoonsgegevens worden hierbij onderscheiden:

- Naam, Initialen, Voornaam;
- Gebruikersnaam;
- E-mailadres;

[11] Artikel 2 lid 2 Uitvoeringswet AVG.

- Mobiel telefoonnummer;
- Adresgegevens;
- Gebruik rol.

Op grond van de richtlijnen van de Autoriteit persoonsgegevens is een Data Protection Impact Assessment (DPIA) vereist als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor betrokken. Een waarschijnlijk hoog privacyrisico wordt in beginsel verondersteld als de verwerking is opgenomen in de DPIA-lijst.[12] Aangezien in het digitaal hulpmiddel logging en monitoring wordt voorzien die het mogelijk maakt om grootschalig handelingen van gebruikers te controleren, wat kan worden aangemerkt als controle van werknemers zoals opgenomen in de PIA-lijst, wordt derhalve voorzien in een DPIA ten aanzien van de verwerking van gebruikersgegevens.

Op basis van de uit te voeren uitgevoerde DPIA zullen de privacybeschermende maatregelen worden bepaalde die worden voorzien in het DHV. In de DPIA zal antwoorde worden gegeven op de vraag welke organisaties binnen het proces als verwerkersverantwoordelijken moet worden aangemerkt en tussen welke partijen een verwerkersovereenkomst dient te worden afgesloten.

8.3. Softwarekwaliteit (ISO-25010)

Iedereen wil altijd kwalitatief goede systemen en applicaties, maar wat wordt er dan precies bedoeld met '(software)kwaliteit'? Hoe wordt de kwaliteit van software getoetst? Is software van goede kwaliteit als het bedrijfsprocessen ondersteunt? Of wanneer gegevens op een veilige en betrouwbare wijze zijn verwerkt? Is de software voor de eindgebruiker makkelijk te gebruiken? Met behulp van de kenmerken zoals gedefinieerd in de kwaliteitsstandaard voor software (ISO 25010) kan hieraan handen en voeten gegeven worden. Deze kenmerken bieden een structuur om bijvoorbeeld requirements, acceptatiecriteria, risico's en testdoelen op te stellen en een gevoel te krijgen voor hun volledigheid.

8.3.1. ISO 25010

Voor softwarekwaliteit onderscheidt ISO 25010 de volgende kenmerken: Functionele geschiktheid, Prestatie-efficiëntie, Uitwisselbaarheid, Bruikbaarheid, Betrouwbaarheid, Beveiligbaarheid, Onderhoudbaarheid en Overdraagbaarheid.

[12] Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (GEB / DPIA) verplicht is, Autoriteit Persoonsgegevens. Stcrt. nr 64418, 27 november 2019.

Figuur 13: Visualisatie onderdelen ISO-25010.

Net als voor de meeste standaarden geldt ook hier dat voor een individueel systeem niet alle kenmerken even belangrijk zijn. Voor het DHV ligt de nadruk op de volgende kenmerken:

- **Functionele geschiktheid**: Hierbij gaat het erom in hoeverre de (opgeleverde) applicatie voldoet aan de gespecificeerde taken en gebruikersdoelen qua compleetheid, correctheid en toepasbaarheid;
- **Betrouwbaarheid**: Bij 'betrouwbaarheid' is het belangrijk dat een applicatie blijft functioneren zonder technische storingen. Hier spelen zaken als bedrijfszekerheid (beschikbaarheid), foutbestendigheid en de herstelbaarheid een grote rol;
- **Beveiligbaarheid**: Hieronder vallen zaken als vertrouwelijkheid, integriteit en verantwoording. (zie paragraaf 8.1 voor een verdere uitwerking).

8.3.2. Product Acceptatie Plan

Het DHV gaat door meerdere ICT-leveranciers in opdracht van de Kiesraad gerealiseerd worden. Voordat de opdrachtgever tot acceptatie van het DHV kan besluiten, moet duidelijk zijn op welke criteria het DHV wordt geaccepteerd. Acceptatiecriteria hebben als doel ondubbelzinnig duidelijk te maken wat er van het product wordt verwacht en dienen derhalve vooraf te zijn vastgelegd.

Van een leverancier wordt verwacht dat hij ten behoeve van de op te leveren software een Product Acceptatie Plan (PAP) opstelt. Een PAP bevat concrete acceptatiecriteria waarmee de werkproducten (en daarmee uiteindelijk het DHV in zijn totaal) eenduidig te beoordelen zijn, zodat een objectieve acceptatie van het product (DHV) mogelijk is. De werkproducten voor het DHV omvatten in ieder geval:

- **Software**: De software die de leverancier voor het DHV ontwikkelt en oplevert aan de Kiesraad;
- **Documentatie**: Software Architecture Document (SAD), handleidingen, (interne) kwaliteits- en toetsingsrapportages, etc.

In het PAP moeten in ieder geval de volgende acceptatiecriteria terugkomen:
- Tooling (en methodiek) waarmee de leverancier zelf de kwaliteit van haar software monitort gedurende de realisatie;
- Tooling (en methodiek) waarmee de leverancier zelf haar software (geautomatiseerd) test gedurende de realisatie;
- De opgeleverde software behaalt een score van minimaal 4 sterren bij de TÜV/SIG-toetsing (of een vergelijkbare score bij een vergelijkbare toetsing).

8.3.3. Service Niveau Overeenkomst

Kwaliteit tijdens gebruik vindt zijn weerslag in een Service Niveau Overeenkomst (SNO). Er zal per (hoofd)leverancier een SNO afgesloten worden ten behoeve het gebruik van het DHV. In een SNO zijn de serviceniveaus beschreven die van toepassing zijn op de dienstverlening van de betreffende leverancier (opdrachtnemer) aan de Kiesraad (opdrachtgever). Dit betreft veelal beheerprocessen als beschikbaarheid-, continuïteits- en capaciteitsbeheer, incidentbeheer, wijzigings- en releasebeheer (al dan niet ten behoeve van preventief, correctief of adaptief onderhoud), etc.

Teneinde om tot een werkbare SNO te komen, moeten de leveranciers (en de Kiesraad) een duidelijke en overeenkomende visie hebben op zaken zo divers als:
- Het (ad hoc) kunnen op- en afschalen van benodigde capaciteit;
- Het (ad hoc) kunnen toevoegen of verwijderen van gebruikers;
- Een back-up strategie voor calamiteiten tijdens de verkiezingen;
- Aangepaste tijdlijnen tijdens de verkiezingen en buiten de verkiezingen voor de MTTR (mean time to repair), de MTBF (mean time between failures), etc.

De serviceniveaus worden beschreven in termen van prestatie-indicatoren en de leveranciers zijn verantwoordelijk voor het realiseren van en het periodiek rapporteren over de gerealiseerde prestatie-indicatoren. Indien het afgesproken niveau van dienstverlening niet gehaald wordt, kan besloten worden tot het opstellen en uitvoeren van verbeterplannen door de leverancier, escalaties en zelfs het leveren van compensaties (boetes). Ook dit is vastgelegd in de SNO.

8.4. Gebruiksvriendelijkheid en toegankelijkheid

Bij de ontwikkeling van de gebruikersinterface dient de ontwikkelaar te voldoen aan de eisen voor gebruikersvriendelijkheid en toegankelijkheid. Ten aanzien van toegankelijkheid dient de webinterface te voldoen aan de eisen op niveau A en AA van de WCAG 2.0 (https://www.digitoegankelijk.nl/onderwerpen/niveaus-van-wcag-2.0/).

Bij gebruiksvriendelijkheid is een essentieel dat de gebruiker ervaring wordt meegenomen in het ontwerp (User experience design). Aangezien dit een specifieke expertise vereist dient dit in het ontwikkel team te worden voorzien. Net als voor de realisatie van de back-end van het DHV, geldt voor de implementatie van de gebruikersinterface dat de (front-end) expertise aanwezig is in het ontwikkel en onderhoud team.

8.5. Back-up strategie

De Kiesraad beschikt te allen tijde over een oudere, geteste versie van de software zodat deze kan worden gedeployed indien er grootschalige beschikbaarheidsproblemen zijn bij de softwareontwikkelaar.

Tijdens het gebruik bij de vaststelling van de uitslag dient dataverlies, door een incident, zoveel mogelijk beperkt te blijven. Gedurende deze periode wordt uitgegaan van een werkbare herstel-punt-doelstelling (Recovery Point Objective, afgekort RPO) van maximaal 1 uur. Na het optreden van een incident dient het DHV binnen een bepaalde tijd naar behoren te functioneren, inclusief het eventueel herstel naar het laatste datapunt binnen de RPO. Als herstel-tijd-doelstelling (Recovery Time Objective, afgekort RTO) wordt maximaal 4 uur als uitgangspunt genomen bij het DHV.

8.6. Open standaarden en zoveel mogelijk open source standaardsoftware

In lijn met het overheidsbeleid[13] zal ook bij het DHV gebruik gemaakt worden van open standaarden. De lijst met open standaarden van het Forum Standaardisatie is ook voor het DHV richtinggevend.

Qua standaard software zal het uitgangspunt zijn om open source software toe te passen waar dat mogelijk is. Ten aanzien van de broncode van de maatwerksoftware, die betrekking heeft op de berekening van de uitslag en zetelverdeling, zal deze openbaar gemaakt worden. Derden kunnen op deze wijze kennisnemen van de berekeningen die in de maatwerk software is opgenomen. Waar mogelijk zal de maatwerk software onder een open source licentie beschikbaar komen, zodat anderen de broncode kunnen gebruiken om zelf verbeteringen en varianten van de software te ontwikkelen.

8.7. Transparantie en controleerbaarheid

Transparantie en controleerbaarheid bij de vaststelling van de verkiezingsuitslag zijn van essentieel belang om vertrouwen te kunnen hebben en houden in de vaststelling van de uitslag van de verkiezingen. Transparantie en controleerbaarheid zijn daarmee essentiële waarborgen binnen het gehele verkiezingsproces en op deze manier wordt eenieder ook in de gelegenheid gesteld om het proces van uitslagvaststelling (inclusief de werking van de digitale hulpmiddelen) te controleren.

Transparantie
Het verkiezingsproces moet zo zijn ingericht, dat het helder van structuur en opzet is. Er zijn in het verkiezingsproces geen 'geheimen'. Alle vragen rondom het verkiezingsproces moeten beantwoord kunnen worden, en de antwoorden moeten voor iedereen controleerbaar en verifieerbaar zijn.

Controleerbaarheid
Het verkiezingsproces moet objectief controleerbaar zijn. De controle-instrumenten kunnen, afhankelijk van de fase waarin een verkiezing zich bevindt, verschillen.

Die transparantie en controleerbaarheid geldt vanzelfsprekend ook voor de werking en het gebruik van de digitale hulpmiddelen (programmatuur en apparatuur) tijdens de vaststelling van de verkiezingsuitslag, en de perioden tussen de verkiezingen in.

8.7.1. Tijdens de vaststelling van de verkiezingsuitslag

Maatregelen ten behoeve van de transparantie en controleerbaarheid tijdens de vaststelling van de verkiezingsuitslag zijn onder andere:

- *In het openbaar bepalen en vaststellen van het aantal stemmen en uitslag op stembureau-, gemeentelijk stembureau- en centraal stembureau-niveau*
  Het stembureau en het gemeentelijk stembureau bepalen in het openbaar het aantal stemmen en respectievelijk de SB- en de GSB-uitslag. Het centraal stembureau stelt in het openbaar het aantal stemmen en de CSB-uitslag vast;
- *Publiceren uitslaggegevens op stembureau-, gemeentelijk stembureau- en centraal stembureau-niveau*
  Dit betreft het op een toegankelijke wijze publiceren van de volledige papieren en digitale gegevensstromen:
    - Het zo snel mogelijk publiceren van de voorlopige stembureau-uitslag, onder andere ten behoeve van een nog in te richten verificatieproces;

[13] Informatie over het overheidsbeleid on onderliggende regelgeving en afspraken is beschikbaar op de website van het Forum Standaardisatie.

    - Het publiceren van de processen-verbaal op SB-, GSB- en CSB-niveau, op het internet en ter inzage gelegd op het gemeentehuis (alleen PV SB en PV GSB);
    - Het publiceren (op het internet) van de digitale bestanden met de gegevens van de uitslag op kandidaatsniveau per GSB, en de uitslag GSB- en CSB-niveau (en wellicht in de toekomst ook op SB-niveau);
- *De Kiesraad rapporteert over de betrouwbaarheid van de verkiezingen aan de hand van meldingen, bezwaren, (beveiligings)incidenten, etc.*
  Dit betreft:
    - Tijdens de bekendmakingen van de uitslagen op SB-, GSB- en CSB-niveau kan iedereen mondeling bezwaren inbrengen. De bezwaren, en reactie daarop van het SB, GSB of CSB, worden opgenomen in het betreffende proces-verbaal. Daarnaast kunnen onderbouwde vermoedens door iedereen schriftelijk ingediend worden bij het CSB, inclusief de ambtshalve vermoedens door CSB-medewerkers zelf. Deze vermoedens worden opgenomen in het proces-verbaal van het CSB;
    - De processen-verbaal bevatten ook de meldingen van bijvoorbeeld onregelmatigheden in het stembureau;
    - Het GSB en CSB geven (zelf) een oordeel over de betrouwbaarheid van respectievelijk de GSB-uitslag en de CSB-uitslag, bijvoorbeeld door de publicatie van de uitkomsten van de door de Kiesraad opgestelde controle-protocollen;
    - Meldingen van (internationale) waarnemers, politieke partijen en media worden door de Kiesraad beschouwd en gerapporteerd;
    - Rapportage door de Kiesraad (mede op basis van gegevens van het Security Operations Center (SOC)) over de betrouwbaarheid van de verkiezingen op basis van de, door het SOC gedetecteerde (en hoog geclassificeerde), beveiligingsincidenten bij GSB's en/of CSB tijdens de verkiezing.

8.7.2. Periode tussen de verkiezingen in

Maatregelen ten behoeve van de transparantie en controleerbaarheid in de periode tussen de verkiezingen zijn onder andere:

- *Publiceren van broncode*
  Uiterlijk op de dag van de kandidaatstelling wordt de broncode van de programmatuur (en bijbehorende documentatie), die bij de daaropvolgende verkiezingen gebruikt wordt, openbaar gemaakt. In 'Bijlagen C: Huidig wettelijk eisen kader (art P1a)' is de thans van toepassing zijnde regelgeving opgenomen. De ontwikkelde broncode maakt gebruik van open standaarden en zoveel mogelijk 'open source (standaard)software';
- *Publicatie uitkomsten van periodieke toetsingen*
  Dit betreft:
    - Periodieke toetsing van de opgeleverde software als gevolg van met name applicatiebeheer (onderhoud/doorontwikkeling van de software) door het (laten) uitvoeren van code-reviews, pentesten, etc. door onafhankelijke instanties;
    - Periodieke toetsing van de (onder)leveranciers door een onafhankelijke instanties audits te laten uitvoeren, of door het opvragen van de resultaten van hun self-assessments, om te onderzoeken in hoeverre de (onder)leveranciers de gemaakte afspraken binnen de gestelde richtlijnen en kaders naleven.

8.8. Exitstrategie

Een vroegtijdige beëindiging van een overeenkomst tussen opdrachtgever en opdrachtnemer (leverancier) is een onwenselijke situatie die bij voorkeur voorkomen moet worden. Een vroegtijdige beëindiging kan het gevolg zijn van verschillende oorzaken zoals een verschil van inzicht tussen opdrachtgever en opdrachtnemer, ondeugdelijke leveranties of een faillissement van de opdrachtnemer. In geval van de situatie waarin een overeenkomst vroegtijdig wordt beëindigd, is het van belang om de continuïteit zo goed mogelijk te waarborgen.

Ten aanzien van de ontwikkeling van het DHV worden de volgende exit-scenario's onderkend:

- Vroegtijdige beëindiging tijdens de aanbesteding. De aanbesteding van het DHV wordt beëindigd door bijvoorbeeld nieuwe inzichten of gewijzigde omstandigheden. Daarnaast spelen bij de aanbesteding onderwerpen een rol die van invloed zijn op de andere exit-scenario's;
- Vroegtijdige beëindiging tijdens de realisatie. De overeenkomst wordt beëindigd gedurende de realisatie van het DHV. Dit kan het gevolg zijn van een faillissement of van een wanprestatie;
- Vroegtijdige beëindiging tijdens het beheer. De overeenkomst wordt beëindigd als het DHV in gebruik is bij de Kiesraad. Ook dit kan het gevolg zijn van een faillissement of van een wanprestatie;
- Beëindiging door afloop van de contractduur. De overeenkomst loopt af en de overeenkomst met de leverancier wordt niet verlengd.

In elk van de exit scenario's zal de beëindiging risico's voor de Kiesraad opleveren die zoveel mogelijk moeten worden weggenomen door het nemen van maatregelen. Van de leverancier zal worden verwacht dat hij bij beëindiging van de overeenkomst datgene doet dat noodzakelijk is om zorg te dragen dat een nieuwe leverancier aansluitend en zonder onderbreking de werkzaamheden voor het DHV kan voortzetten. Deze zogenaamde Exit procedure dient in de praktijk bewezen te zijn, uit te voeren te zijn met minimale inspanning van de Kiesraad en tegen marktconforme kosten.

Bij het beperken van de risico's kan een Escrow-overeenkomst een rol spelen. Een Escrow overeenkomst is een overeenkomst tussen de ontwikkelaar van de software, de opdrachtgever en een Escrow-dienstverlener. De overeenkomst garandeert dat een opdrachtgever kan beschikken over de actuele versie van de broncode van het softwarepakket en van technische en functionele documentatie waarvoor de overeenkomst geldt. Kopieën van de broncode en de documentatie worden bij de Escrow-dienstverlener gestald. De Escrow dienstverlener voert vervolgens het beheer en controle uit op de beschikbaarheid van de broncode en de documentatie, maar ziet er ook op toe dat volgens een afgesproken schema bovenstaande informatie wordt vernieuwd. Als een exit-scenario realiteit wordt, levert de Escrow-dienstverlener de meest actuele broncode en documentatie aan de opdrachtgever.

De voordelen van een Escrow overeenkomst voor de Kiesraad zijn:
- Controle over het intellectueel eigendom;
- Continuïteit van het verkiezingsproces;
- Veilige stellen van de investering in de software;
- Verzekering tegen gevolgschade bij een exit situatie.

Een Escrow overeenkomst is verder belangrijk omdat de Kiesraad vermoedelijk afhankelijk zal blijven van een softwareleverancier voor onderhoud, updates en aanpassingen. Zo zal in de overeenkomst met de softwareleverancier opgenomen moeten worden dat als de softwaremaker de SNO niet kan nakomen (bijvoorbeeld ten gevolge van een faillissement), de Escrow regeling ingeroepen kan worden.

8.8.1. Vroegtijdige beëindiging tijdens de aanbesteding

Bij een aanbesteding komen onderwerpen ter sprake die van belang zijn in een mogelijk exit scenario. Deze onderwerpen kunnen als vereisten in de overeenkomst tussen opdrachtgever en opdrachtnemer worden vastgelegd. Zo zullen er afspraken worden gemaakt over het intellectueel eigendom, toe te passen software-componenten en software-licenties.

In onderstaande opsomming zijn aandachtspunten die een rol spelen binnen de exit scenario's realisatie, beheer en beëindiging na aflopen contractduur en die relevant zijn om onderdeel uit te maken van de aanbesteding:
- Adequate documentatie, niet alleen technisch maar ook functioneel. Een nieuwe leverancier kan zich zo snel een beeld vormen van het DHV;

- Transparantie in de gekozen opzet en inrichting van het DHV. Een nieuwe leverancier wordt zo min mogelijk verrast door verborgen eigenschappen of inrichtingsonderdelen;
- Vermijden van exotische programmatuur en een keuze voor generieke en algemeen toegankelijke programmeertalen. Het voordeel hiervan is dat uit meerdere nieuwe leveranciers kan worden gekozen wat bijdraagt aan concurrentie, een adequate kwaliteit en een marktconforme prijs;
- Vermijden van onnodige complexiteit en een keuze voor zoveel mogelijk eenvoud. Hierdoor wordt het voor een nieuwe leverancier gemakkelijker om zich in te werken;
- Inrichten van een OTAP-straat. De Kiesraad heeft door middel van OTAP een goed gestructureerd proces waarin ook een nieuwe leverancier kan participeren;
- Een marktconforme en courante aanpak. Dit maakt de overstap naar een nieuwe leverancier voor de Kiesraad gemakkelijker. Er zijn aanbieders die de rol van de oude leverancier kunnen overnemen;
- Overdraagbaarheid (niet-functionele eisen) van het DHV naar een andere leverancier. Door op voorhand afspraken te maken is zowel voor de Kiesraad als voor de leverancier duidelijk wat wordt verwacht bij een overdracht van het DHV naar een nieuwe leverancier;
- Faillissement van de leverancier, beëindiging van bedrijfsactiviteiten, overlijden of vertrek van belangrijke werknemers, overname of samengaan van de leverancier met een concurrent of onredelijke prijsverhogingen;
- Een efficiënte geschilbeslechting zorgt ervoor dat zo min mogelijk tijd en geld verloren gaat bij een geschil met een leverancier. Zodat snel kan worden overgestapt op een andere leverancier;
- Escrow (zie boven).

8.8.2. Vroegtijdige beëindiging tijdens de realisatie

Beëindiging van de overeenkomst tijdens de realisatie van het DHV zal tot gevolg hebben dat OSV langer in stand gehouden moet worden en het DHV later gereed zal zijn. Gezien de operationele risico's hiervan voor de Kiesraad dient deze periode tot een minimum te worden beperkt.

In de situatie dat de overeenkomst wordt beëindigd tijdens de realisatie zijn er twee mogelijke scenario's:

- De verdere realisatie van het DHV wordt voortgezet door een andere leverancier;
- De realisatie van het DHV wordt gestaakt en er wordt een nieuwe leverancier gezocht die een eigen oplossing realiseert.

Welk scenario gezien de omstandigheden het meest gunstig is kan op voorhand niet worden bepaald en is sterk afhankelijk van de specifieke situatie die tot de beëindiging leidde. In beide gevallen dient de Kiesraad zorg te dragen dat alle zaken die tot het moment van beëindiging zijn gerealiseerd beschikbaar blijven voor eventuele overdracht naar een nieuwe leverancier.

Bij vroegtijdige beëindiging van de overeenkomst zal de Kiesraad daarom zonder beperkingen over alle rechten die nodig zijn om het DHV verder te ontwikkelen moeten beschikken. Dit om reeds opgebouwde kennis en software beschikbaar te stellen aan een andere leverancier.

8.8.3. Vroegtijdige beëindiging tijdens het beheer

Wanneer sprake is van een vroegtijdige beëindiging van de overeenkomst nadat het DHV door de Kiesraad in gebruik is genomen, dient de continuïteit te worden gewaarborgd door voortzetting van het beheer (onderhoud, updates en aanpassingen) van het DHV door een andere leverancier of door de Kiesraad zelf.

Hierbij kan een onderverdeling worden gemaakt naar:

- Continuïteit van het DHV in de productieomgeving;
- Continuïteit in het beheer van het DHV in de ontwikkel, test en acceptatie omgeving.

8.8.4. Beëindiging door afloop van de contractduur

Van de leverancier wordt verwacht dat hij het DHV zodanig heeft ontworpen en gerealiseerd dat de werkzaamheden zonder obstructies kunnen worden overgenomen door een andere leverancier. Zaken die minimaal door de leverancier geleverd dienen te worden bij het einde van de overeenkomst zijn:

- De meest recente versie van de broncode van de beheerde software, zodat voortzetting van het beheer mogelijk is;
- Het volledige datamodel van het DHV met technische en functionele beschrijving;
- Volledige ondersteuning die nodig is voor het onderbrengen van het beheer bij een andere leverancier;
- Alle documentatie, rapporten en overige producten die de leverancier beschikbaar heeft.

Daarnaast is het van belang dat de Kiesraad beschikt over het Intellectueel Eigendom en de gebruiksrechten die nodig zijn om het beheer en onderhoud van het DHV uit te kunnen laten voeren door een derde partij. Het belang om te beschikken over het intellectueel eigendom geldt zowel voor het realisatie-, het beheer- als het beëindigingsscenario na afloop van de contractduur.

Bijlage A: Overzicht dreigingsscenario's en maatregelen

In het onderstaande overzicht worden verschillende dreigingsscenario's benoemt en daarbij aangegeven welke voorgenomen maatregelen in het DHV worden genomen en welke maatregen buiten het DHV om worden voorzien.

Legenda

Maatregelsoort	**Beschrijving betekenis**
Preventief (reduceert kans)	De maatregel verkleint de kans dat de betreffende dreiging via een kwetsbaarheid tot een concreet risico leidt.
Preventief (reduceert impact)	De maatregel reduceert de impact van een succesvolle aanval.
Detectief	De maatregel vergroot de kans dat een aanval te wordt gedetecteerd.
Correctief	De maatregel herstelt de negatieve consequenties van een aanval of risico.

Dreigingsscenario		**Werkstation van GSB of CSB waarmee de portal wordt gebruikt is gecompromitteerd, waardoor de ingevoerde en getoonde gegevens worden gemanipuleerd**
Maatregelen DHV		
1	*Omschrijving*	Toegang via gehardende Virtuele Desktop omgeving
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Gebruik centraal beschikbaar gestelde gehardende image
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Alleen werkstations die conform een procedure worden beheerd en opgeslagen mogen worden gebruikt
	Soort	Preventief (verkleint kans)
4	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint impact)
5	*Omschrijving*	Logging en monitoring
	Soort	Detectief
6	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Detectief en Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Werkstations GSB en CSB functioneren niet**
Maatregelen DHV		
1	*Omschrijving*	Gebruik centraal beschikbaar gestelde gehardende image
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Alleen werkstations die conform een procedure worden beheerd en opgeslagen mogen worden gebruikt
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Opleiding en awareness (nader uit te werken)
	Soort	Preventief (verkleint kans)
4	*Omschrijving*	Logging en monitoring
	Soort	Detectief
5	*Omschrijving*	Mogelijkheid om vooraf geconfigureerde hardware te verkrijgen van de Kiesraad als terugvaloptie
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Portal onbereikbaar door DDoS-aanval**
Maatregelen DHV		
1	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans) en Correctief
2	*Omschrijving*	DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint impact)
4	*Omschrijving*	Intrusion Prevention maatregelen
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Eisen hosting
	Soort	Preventief (verkleint kans)
6	*Omschrijving*	Logging en monitoring
	Soort	Detectief
7	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Een actor weet via het datacenter of hostingprovider de gegevens in de portal te manipuleren**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen hosting
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint kans en impact)
4	*Omschrijving*	Gebruik van digitale handtekeningen
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Logging en monitoring
	Soort	Detectief
6	*Omschrijving*	Back-up strategie
	Soort	Correctief
7	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Detectief en Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**De beheerder(s) van de portal veranderen oneigenlijk gegevens in de portal**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen hosting
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint kans en impact)
4	*Omschrijving*	Gebruik van digitale handtekeningen
	Soort	Preventief (verkleint kans)
	Omschrijving	Logging en monitoring

5	*Soort*	Detectief
6	*Omschrijving*	Back-up strategie
	Soort	Correctief
7	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Detectief en Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Portal functioneert niet meer goed door onbeschikbaarheid van derde partij**
Maatregelen DHV		
1	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Logging en monitoring
	Soort	Detectief
3	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
4	*Omschrijving*	Mogelijkheid om vooraf geconfigureerde hardware te verkrijgen van de Kiesraad als terugvaloptie
	Soort	Correctief
5	*Omschrijving*	Back-up strategie
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Gebruiker van het webportaal kan zich niet authentiseren, omdat er geen account(s) voor de betreffende gebruikers beschikbaar is/zijn**
Maatregelen DHV		
1	*Omschrijving*	Sterke persoonsgebonden tweefactorauthenticatie (E-herkenning)
	Soort	Preventief (verkleint kans)
	Omschrijving	Inrichten fysiek- en logisch toegangsbeheer (nader uit te werken)

2	*Soort*	Preventief (verkleint kans)
3	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Webportal kan een piekbelasting niet aan**
Maatregelen DHV		
1	*Omschrijving*	Eisen hosting
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint kans en impact)
3	*Omschrijving*	Logging en monitoring
	Soort	Detectief
4	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Ongeautoriseerde personen krijgen een authenticatiemiddel in handen**
Maatregelen DHV		
1	*Omschrijving*	Sterke persoonsgebonden tweefactorauthenticatie (E-herkenning)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Inrichten fysiek- en logisch toegangsbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Functiescheiding
	Soort	Preventief (verkleint impact)
4	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen
	Soort	Preventief (verkleint kans)
6	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint impact)
	Omschrijving	Logging en monitoring

7	*Soort*	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario	**Het besloten netwerk functioneert niet, waardoor het GSB en CSB geen gebruik kan maken van het digitale hulpmiddel**	
Maatregelen DHV		
1	*Omschrijving*	Eisen hosting
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans) en Correctief
3	*Omschrijving*	Logging en monitoring
	Soort	Detectief
4	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
5	*Omschrijving*	Mogelijkheid om vooraf geconfigureerde hardware te verkrijgen van de Kiesraad als terugvaloptie
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario	**Portal wordt aangevallen vanaf een (gecompromitteerd) systeem dat ook op het besloten netwerk is aangesloten en de portal kan bereiken**	
Maatregelen DHV		
1	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans) en Correctief
2	*Omschrijving*	DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint impact)

4	*Omschrijving*	Intrusion Prevention maatregelen
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Eisen hosting
	Soort	Preventief (verkleint kans)
6	*Omschrijving*	Logging en monitoring
	Soort	Detectief
7	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Detectief en Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Portal functioneert niet door hardware- of softwarefouten**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen ontwikkelen software
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Wijzigingenbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
4	*Omschrijving*	Gebruik van een OTAP-straat
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Softwarekwaliteit
	Soort	Preventief (verkleint kans)
6	*Omschrijving*	Mogelijkheid om vooraf geconfigureerde hardware te verkrijgen van de Kiesraad als terugvaloptie
	Soort	Correctief
7	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Detectief en Correctief
8	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief

Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Gegevens via het besloten netwerk worden gemanipuleerd**
Maatregelen DHV		
1	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint impact)
4	*Omschrijving*	Intrusion Prevention maatregelen
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Toepassen encryptie voor dataverkeer
	Soort	Preventief (verkleint kans)
6	*Omschrijving*	Gebruik van digitale handtekeningen
	Soort	Preventief (verkleint kans)
7	*Omschrijving*	Logging en monitoring
	Soort	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Kwetsbaarheden in software komen aan het licht**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen ontwikkelen software
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Wijzigingenbeheer (nader uit te werken)
	Soort	Preventief (verkleint impact)

4	*Omschrijving*	Gebruik van een OTAP-straat
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario	**Leverancier kan niet tijdig de software leveren, bijvoorbeeld omdat het bedrijf is platgelegd door ransomware**
Maatregelen DHV	
1 *Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
Soort	Preventief (verkleint kans)
2 *Omschrijving*	Eisen ontwikkelen software
Soort	Preventief (verkleint kans)
3 *Omschrijving*	Wijzigingenbeheer (nader uit te werken)
Soort	Preventief (verkleint impact)
4 *Omschrijving*	Gebruik van een OTAP-straat
Soort	Preventief (verkleint kans)
5 *Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
Soort	Preventief, Detectief en Correctief
6 *Omschrijving*	Back-up strategie
Soort	Correctief
7 *Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
Soort	Correctief
Terugval (maatregelen buiten het DHV om)	
1 *Omschrijving*	Plan P
Soort	Correctief

Dreigingsscenario	**Leverancier van de software wordt gecompromitteerd, waardoor de software mogelijk gemanipuleerd is. Bij het testen van de software en dus voor ingebruikname komt dit niet aan het licht**
Maatregelen DHV	

1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen ontwikkelen software
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Wijzigingenbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
4	*Omschrijving*	Gebruik van een OTAP-straat
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
6	*Omschrijving*	Intrusion Prevention maatregelen
	Soort	Preventief (verkleint kans)
7	*Omschrijving*	Logging en monitoring
	Soort	Detectief
8	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Leverancier van de software wordt gecompromitteerd, waardoor de software mogelijk gemanipuleerd is. Dit komt na ingebruikname van de software aan het licht**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen ontwikkelen software
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Wijzigingenbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
4	*Omschrijving*	Gebruik van een OTAP-straat
	Soort	Preventief (verkleint kans)

5	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
6	*Omschrijving*	Intrusion Prevention maatregelen
	Soort	Preventief (verkleint kans)
7	*Omschrijving*	Logging en monitoring
	Soort	Detectief
8	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Gebruikers van de software maken invoerfouten die de software had kunnen detecteren, zoals controleren of de optellingen van deeltotalen overeenkomen met het eindtotaal**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen ontwikkelen software
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Software controleert op invoerfouten (functionele eis)
	Soort	Preventief (verkleint kans), Detectief en Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Digitaal hulpmiddel blijkt bij gebruik nog een (verstorende) fout te bevatten**
Maatregelen DHV		
1	*Omschrijving*	Leveranciers worden zorgvuldig geselecteerd en gescreend
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Eisen ontwikkelen software
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Wijzigingenbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
4	*Omschrijving*	Gebruik van een OTAP-straat
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
6	*Omschrijving*	Back-up strategie
	Soort	Correctief
7	*Omschrijving*	Continuïteitsplannen en disaster recovery procedures (nader uit te werken)
	Soort	Correctief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Plan P
	Soort	Correctief

Dreigingsscenario		**Een interne medewerker van het GSB of CSB wijzigt bewust of onbewust oneigenlijk de uitslag**
Maatregelen DHV		
1	*Omschrijving*	Sterke persoonsgebonden tweefactorauthenticatie (E-herkenning)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Inrichten fysiek- en logisch toegangsbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Functiescheiding
	Soort	Preventief (verkleint impact)
4	*Omschrijving*	Software controleert op invoerfouten (functionele eis)
	Soort	Preventief (verkleint kans), Detectief en Correctief
5	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
6	*Omschrijving*	Logging en monitoring
	Soort	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief

2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario	**GSB of CSB handelen niet conform informatiebeveiligingsinstructies**	
Maatregelen DHV		
1	*Omschrijving*	Inrichten instructies en procedures voor gebruik DHV (nader uit te werken)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
3	*Omschrijving*	Logging en monitoring
	Soort	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario	**Fouten of onvolkomenheden in de gebruikersinstructies of het proces dat gevolgd moet worden**	
Maatregelen DHV		
1	*Omschrijving*	Inrichten instructies en procedures voor gebruik DHV (nader uit te werken)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Controleren naleving beveiligingskaders, -eisen en voorschriften
	Soort	Preventief, Detectief en Correctief
3	*Omschrijving*	Logging en monitoring
	Soort	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief

3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Misbruik van het digitale hulpmiddel, bijvoorbeeld dat deze is gecompromitteerd of bewuste dan wel onbewuste handelingen van een persoon, is niet herleidbaar tot datum, tijd en bron**
Maatregelen DHV		
1	*Omschrijving*	Sterke persoonsgebonden tweefactorauthenticatie (E-herkenning)
	Soort	Preventief (verkleint kans)
2	*Omschrijving*	Logging en monitoring
	Soort	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Website van gemeente wordt gehackt en online geplaatste PV's (N10 en N11) worden aangepast**
Maatregelen DHV		
1	*Omschrijving*	Niet in scope DHV basisarchitectuur
	Soort	
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Dreigingsscenario		**Misbruik van inloggegevens voor het digitale hulpmiddel**
Maatregelen DHV		
1	*Omschrijving*	Sterke persoonsgebonden tweefactorauthenticatie (E-herkenning)
	Soort	Preventief (verkleint kans)

2	*Omschrijving*	Inrichten fysiek- en logisch toegangsbeheer (nader uit te werken)
	Soort	Preventief (verkleint kans)
3	*Omschrijving*	Functiescheiding
	Soort	Preventief (verkleint impact)
4	*Omschrijving*	DHV uitsluitend beschikbaar via besloten overheidsnetwerk (twee besloten netwerken voor redundantie)
	Soort	Preventief (verkleint kans)
5	*Omschrijving*	DHV uitsluitend beschikbaar vanaf gewhiteliste IP-adressen
	Soort	Preventief (verkleint kans)
6	*Omschrijving*	Gecompartimenteerde omgeving
	Soort	Preventief (verkleint impact)
7	*Omschrijving*	Logging en monitoring
	Soort	Detectief
Terugval (maatregelen buiten het DHV om)		
1	*Omschrijving*	Controleprotocol
	Soort	Detectief en Correctief
2	*Omschrijving*	Verificatieproces
	Soort	Detectief en Correctief
3	*Omschrijving*	Plan P
	Soort	Correctief
4	*Omschrijving*	Transparantie geborgd in het verkiezingsproces
	Soort	Preventief, Detectief en Correctief

Bijlage B: Verwijzingen en bronnen

Titel	Bron
Regeling omtrent naslag naar personen en organisaties door de AIVD	https://www.aivd.nl/documenten/kamerstukken/2018/04/26/regeling-omtrent-naslag-naar-personen-en-organisaties-door-de-aivd
Voorschrift Informatiebeveiliging Rijksdienst (VIR)	https://wetten.overheid.nl/BWBR0022141/2007-07-01
Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie (VIR-BI)	https://wetten.overheid.nl/BWBR0033507/2013-06-01
Baseline Informatiebeveiliging Overheid (BIO)	https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/ https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/ https://www.bio-overheid.nl/
Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Huisvesting Informatievoorziening	https://cip.stage.remotion.nl/media/1271/bio-thema-2-huisvesting-iv-concept-10.pdf
Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Communicatievoorzieningen	https://cip.stage.remotion.nl/media/1269/bio-thema-5-communicatievoorzieningen-concept-v10.pdf
Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Toegangsbeveiliging	https://cip.stage.remotion.nl/media/1267/bio-thema-3-toegangsbeveiliging-concept-10.pdf
Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Applicatieontwikkeling	https://cip.stage.remotion.nl/media/1268/bio-thema-4-applicatieontwikkeling-concept-v10.pdf
Baseline Informatiebeveiliging Overheid (BIO) – Themadocument Serverplatform	https://cip.stage.remotion.nl/media/1270/bio-thema-6-serverplatform-concept-v10.pdf
CIP – Handleiding security proof inkopen	https://www.cip-overheid.nl/media/1127/20180415-security-proof-inkopen-2pager-1.pdf https://www.cip-overheid.nl/media/1129/20180415-security-proof-inkopen-handleiding-vsp-vse-werkwijze-1.pdf
CIP – Wizard Security proof inkopen	https://www.cip-overheid.nl/media/1128/20180415-security-proof-inkopen-wizard.xlsx
CIP – Grip op beveiliging in inkoopcontracten	https://www.cip-overheid.nl/media/1130/20141007_grip-op-beveiliging-in-inkoopcontracten-een-prestatiegerichte-aanpak_v1_0.pdf

Titel	Bron
NCSC ICT-beveiligingsrichtlijnen voor webapplicaties	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
NCSC Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beleids--en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software
NCSC Factsheet Veilig beheer van digitale certificaten	https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten
NCSC Factsheet gebruik tweefactorauthenticatie	https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie
NCSC Factsheet virtualiseer met verstand	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/virtualiseer-met-verstand
NCSC Handreiking voor implementatie van detectie-oplossingen	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/handreiking-voor-implementatie-van-detectie-oplossingen
NCSC beveiligingsrichtlijnen voor mobiele apparaten	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten
NCSC ICT-beveiligingsrichtlijnen voor mobiele apps	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-mobiele-apps
CIP - Grip op Secure Software Development (SSD) – Beveiligingseisen voor (web)applicaties	https://www.cip-overheid.nl/media/1101/grip-op-ssd-het-proces-v20.pdf
CIP - Grip op Secure Software Development (SSD) Het testen van de (versie 2.0) Beveiligingseisen voor (web)applicaties	https://www.cip-overheid.nl/media/1102/grip-op-ssd-beveiligingseisen-v2_0.pdf
OWASP Top 10 Web Application Security Risks	https://owasp.org/www-project-top-ten/
OWASP Application Security Verification Standard (ASVS)	https://owasp.org/www-project-application-security-verification-standard/
Algemene Verordening Gegevensbescherming (AVG)	https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg
Uitvoeringswet AVG	https://wetten.overheid.nl/BWBR0040940/2018-05-25

Titel	Bron
Kieswet	https://wetten.overheid.nl/BWBR0004627
Kiesbesluit	https://wetten.overheid.nl/BWBR0004632
Kiesregeling	https://wetten.overheid.nl/BWBR0034180

Bijlage C: Huidig wettelijk eisen kader (art P1a)

Artikel P 1a Kieswet
1. Indien het centraal stembureau programmatuur gebruikt ten behoeve van de berekening van de uitslag van de verkiezing of de berekening van de zetelverdeling, maakt het centraal stembureau elektronisch op een algemeen toegankelijke wijze openbaar welke programmatuur het gebruikt.
2. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld omtrent de openbaarmaking van de programmatuur en wordt bepaald onder welke voorwaarden het centraal stembureau programmatuur kan gebruiken ten behoeve van de berekening van de uitslag van de verkiezing of de berekening van de zetelverdeling en aan welke eisen deze programmatuur moet voldoen.

Artikel P 1 Kiesbesluit
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.

3. Het centraal stembureau laat de specificatie, bedoeld in het tweede lid, door een onafhankelijke instantie toetsen en maakt de specificatie en de uitkomst van de toets openbaar.

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.

5. Het centraal stembureau maakt uiterlijk op de dag van kandidaatstelling ten minste de documentatie en de broncode met betrekking tot de programmatuur die bij de daaropvolgende verkiezingen wordt gebruikt, openbaar.

Artikel P 2 Kiesbesluit
1. Het centraal stembureau maakt de aantallen stemmen, zoals deze aantallen door het centraal stembureau zijn ingevoerd in de programmatuur, gelijktijdig met het vaststellen van de uitslag openbaar.

Bijlage 2. bij artikel 2a van de Kiesregeling
Eisen aan de programmatuur die door de centrale stembureaus wordt gebruikt ten behoeve van de vaststelling van de uitslag van verkiezingen of de berekening van de zetelverdeling

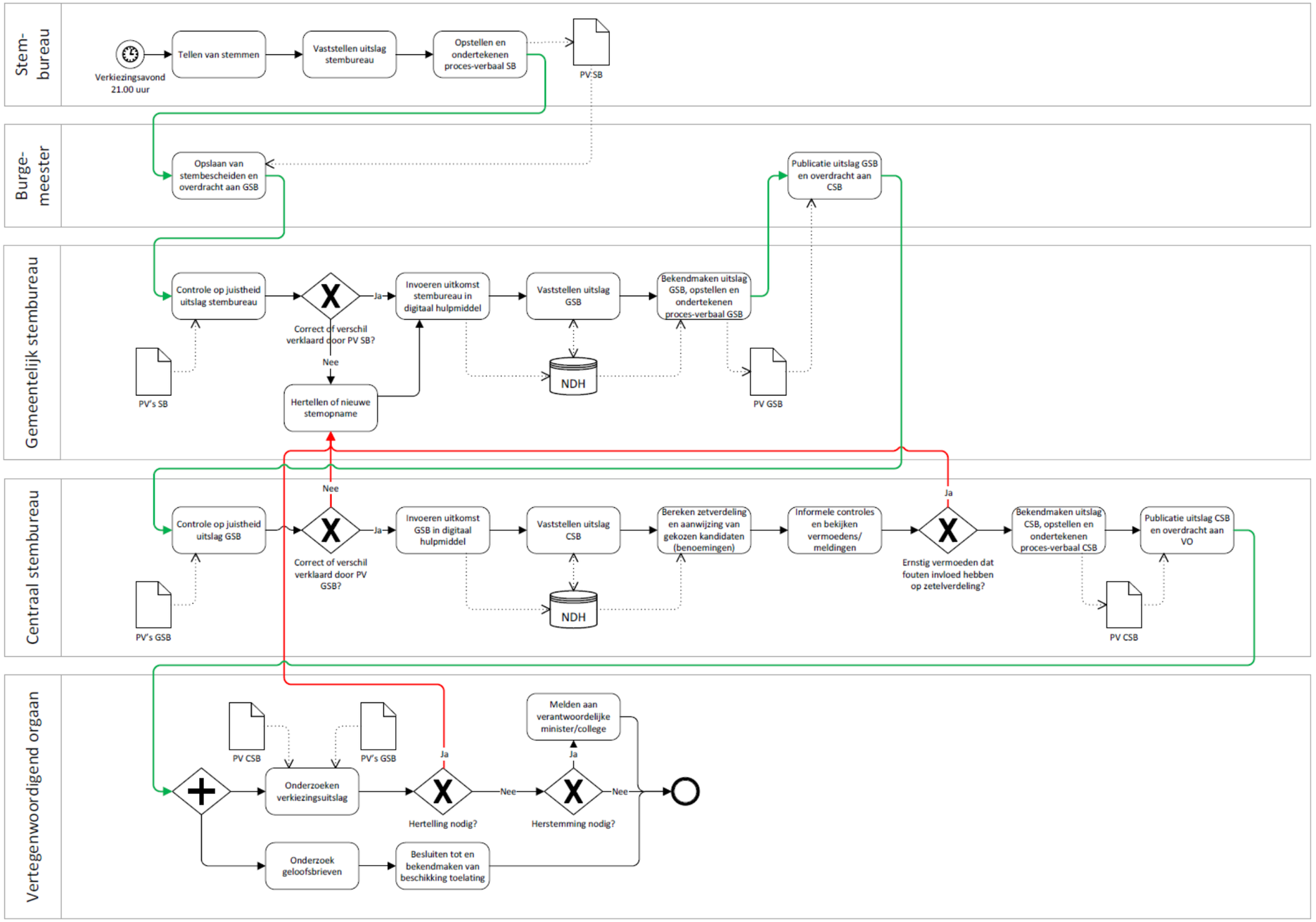
De programmatuur, bedoeld in artikel P 1, eerste lid, van het Kiesbesluit, ten behoeve van de berekening van de uitslag van de verkiezingen of de berekening van de zetelverdeling, voldoet aan de volgende eisen:

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;

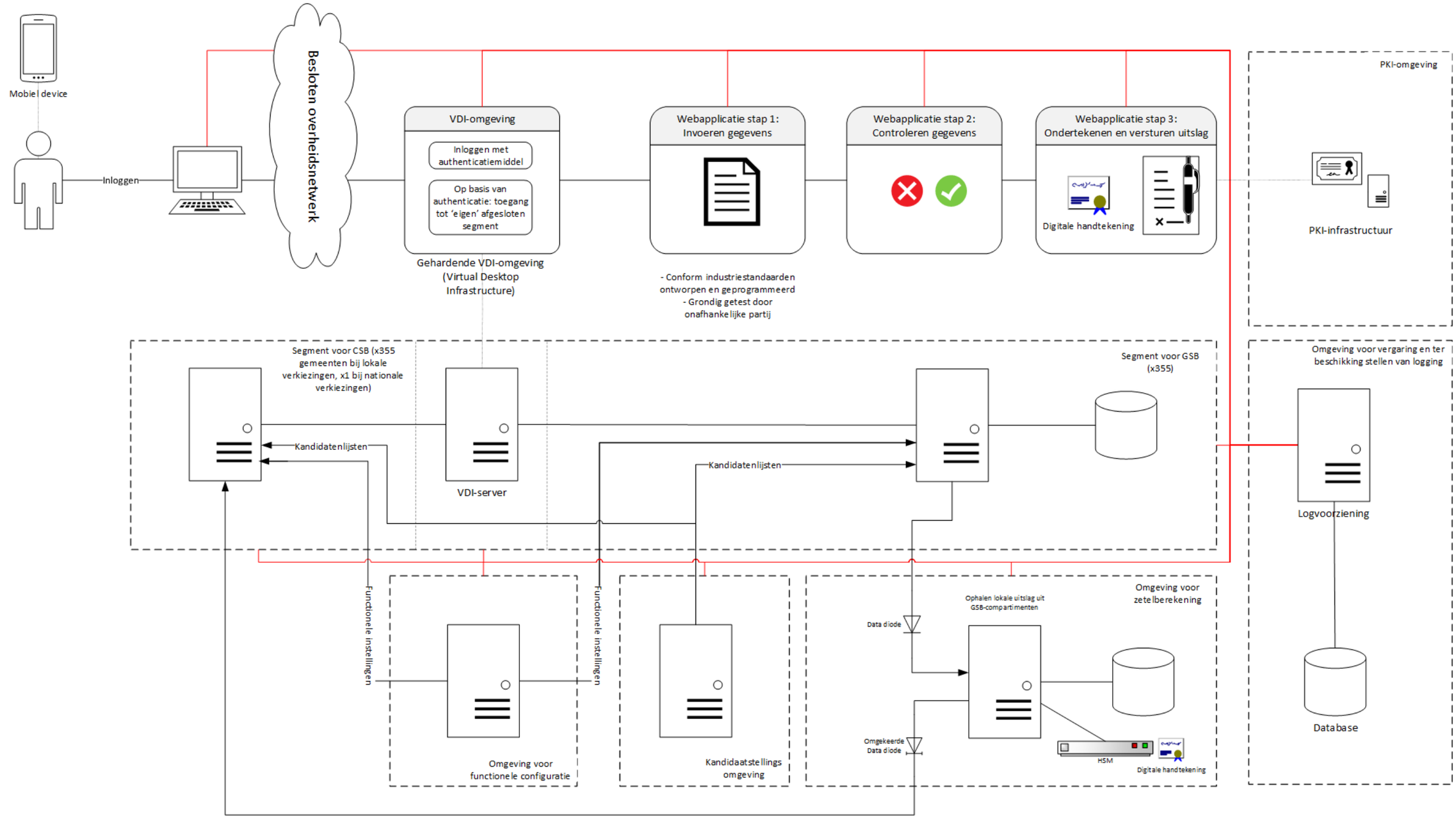
f. de programmatuur ondersteunt voor de vermelding van de aanduidingen van de politieke groeperingen en de namen van de kandidaten in ieder geval de diakritische tekens van de tekenset die op grond van artikel 3, eerste lid, van het Besluit basisregistratie personen voor de basisregistratie personen 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 standaard programmatuur 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; en
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.

Bijlage D: Vergrote weergave afbeeldingen en tabellen

Figuur 4: Schematische weergave proces vaststelling uitslag.



Figuur 5: Visualisatie technische opzet.

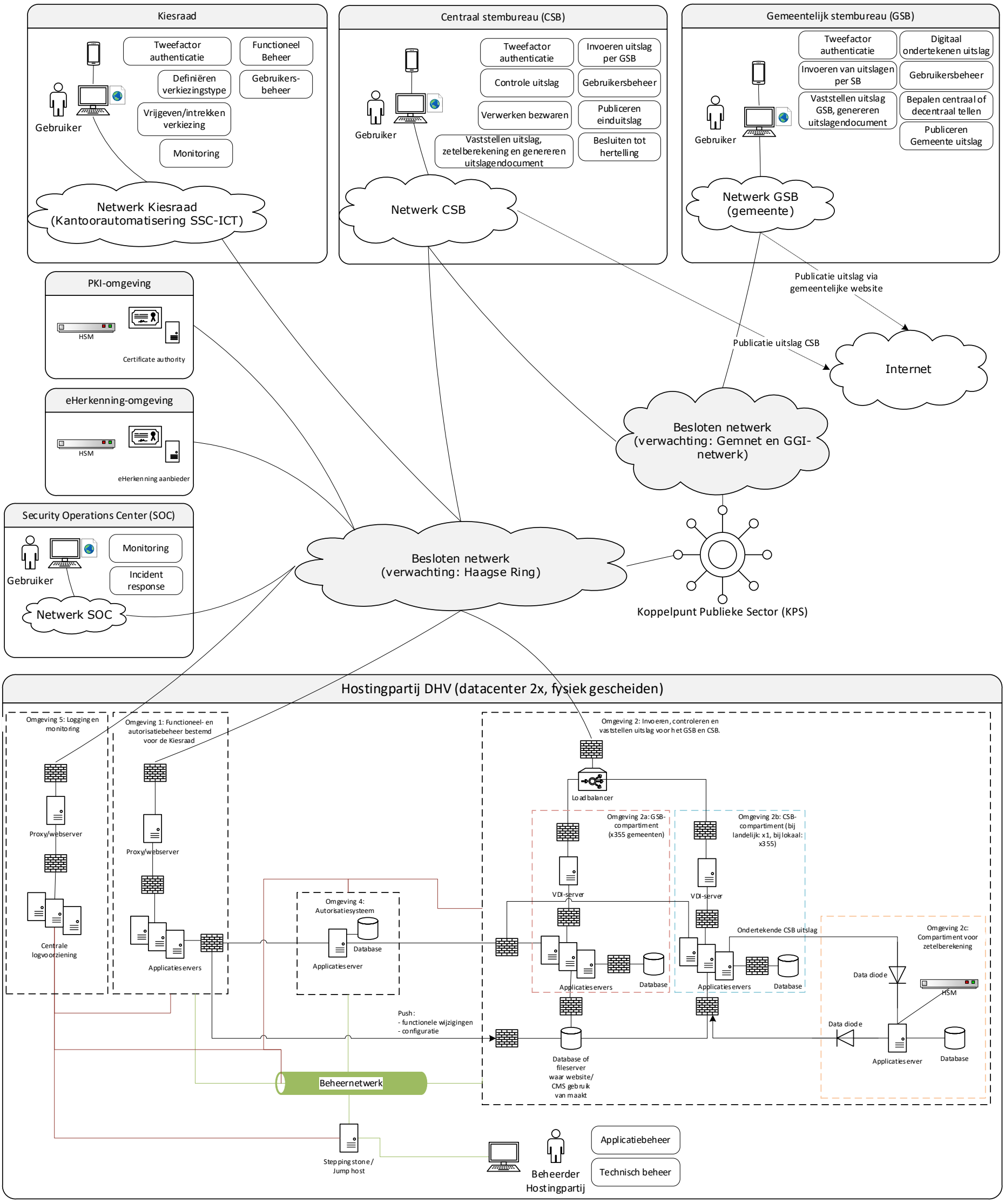


Tabel 2: Controlematrix met beschrijving op welke wijze verschillende partijen voldoen aan de beveiligingskaders.

Partij	Moeten voldoen aan (een specificatie van) de volgende beveiligingskaders	Wordt getoetst d.m.v.	Op initiatief van	Gerapporteerd aan	Opmerking
Gebuikers-organisatie (primair Gemeenten)	BIO (Baseline Informatiebeveiliging Overheid)	Self-assessment in het kader van de ENSIA	Gemeenten / VNG	College van B&W	Er kunnen eventueel vragen worden toegevoegd aan de ENSIA vragenlijst in het kader van het DHV.
				Gemeenteraad	
	Voorschrift/aansluitvoorwaarden Veilige Verkiezingen, dit bevat: - Voorschrift voorbereiden werkstations - Voorschrift veilige opslag werkstations - Voorschrift uitgifte autorisaties - Voorschrift hardenen werkstations (invulling afhankelijk van keuze voor vooraf gehardende images)	Self-assessment normenkader Veilige Verkiezingen	Kiesraad	Kiesraad	Kan eventueel worden toegevoegd aan de ENSIA-normatiek
		Optioneel: audit op aanvraag, uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	
Verkiezings-autoriteit/ Kiesraad	BIO (Baseline Informatiebeveiliging Overheid)	Self-assessment in het kader van de jaarlijkse In-Control Verklaring	Kiesraad / BZK	Kiesraad / BZK	
	Voorschrift/normenkader Veilige Verkiezingen, bevat o.a.: - Voorschrift voorbereiden werkstations - Voorschrift veilige opslag werkstations - Voorschrift uitgifte autorisaties - Voorschrift hardenen werkstations (invulling afhankelijk van keuze voor vooraf gehardende images)	Audit uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	
Software-ontwikkelaar	Programma van Eisen (PvE) softwareontwikkelaar. In dit PvE zitten o.a. eisen over: - Voldoen aan de BIO d.m.v. statement of compliance - Secure Software Development - Wijzigingenbeheer - Vierogenprincipe - Patchmanagement - Hardening - Toegangsbeheer - Logging Het PvE is gebaseerd op de volgende kaders en best practices: 1) BIO Themadocument Applicatieontwikkeling 2) OWASP Top 10 Web Application Security Risks 3) OWASP Application Security Verification Standard (ASVS) 4) NCSC Beleids- en beheersingsrichtlijnen voor de ontwikkeling van veilige software 5) NCSC ICT-beveiligingsrichtlijnen voor webapplicaties	Audit uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	Een auditor kan worden ingeschakeld om te controleren of de softwareontwikkelaar voldoet aan de eisen uit het PvE.
		Pentesten, secure code reviews, configuratiereviews, redteaming en andere beveiligingstesten uitgevoerd door een gekwalificeerde marktpartij	Kiesraad	Kiesraad	Deze testen worden op reguliere basis uitgevoerd en ten minste voorafgaand aan iedere verkiezing.
		Pentesten, secure code reviews, configuratiereviews en andere beveiligingstesten uitgevoerd door burgers	Kiesraad	Kiesraad	Dit kan worden vormgegeven d.m.v. een zogenaamde hackwedstrijd/ hackathon/ hackmarathon.
		Responsible Disclosure procedure	Burgers	Kiesraad	Via deze procedure kunnen burgers zelf kwetsbaarheden melden op een gecontroleerde manier.
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	

Partij	Moeten voldoen aan (een specificatie van) de volgende beveiligingskaders	Wordt getoetst d.m.v.	Op initiatief van	Gerapporteerd aan	Opmerking
Hostingpartij (aanname: tevens beheerder datacenter)	Programma van Eisen (PvE) hostingpartij. In dit PvE zitten o.a. eisen over: - Voldoen aan de BIO d.m.v. statement of compliance - Veilige inrichting datacenter - Wijzigingenbeheer infrastructuur - Netwerkbeveiliging - Encryptie - Hardening infrastructuur - Vierogenprincipe - Patchmanagement - Toegangsbeheer - Logging Het PvE is gebaseerd op de volgende kaders en best practices: 1) BIO– Themadocument Huisvesting Informatievoorziening 2) BIO – Themadocument Communicatievoorzieningen 3) BIO – Themadocument Toegangsbeveiliging 4) NCSC Factsheet virtualiseer met verstand 5) NCSC Factsheet gebruik tweefactorauthenticatie 6) NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) 7) NCSC Factsheet Veilig beheer van digitale certificaten	Audit uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij). Eventueel in de vorm van een ISAE-3402 Type 2 verklaring.	Kiesraad	Kiesraad	In de ideale situatie geeft de hostingpartij zelf al jaarlijks een ISAE3402-verklaring af met een dekkend normenkader en dekkende scope. Zo niet, dan moet dit worden afgedwongen in de eisen.
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	
SOC (uitgaande van overheidspartij)	BIO	Self-assessment in het kader van de jaarlijkse In-Control Verklaring	SOC	Kiesraad	
	Nader op te stellen programma van eisen voor logging en monitoring, gebaseerd op o.a.: 1) NCSC Handreiking voor implementatie van detectie-oplossingen. 2) Use-cases monitoring zoals opgesteld door de Verkiezingsautoriteit / Kiesraad	Optioneel: audit op aanvraag, uitgevoerd door een onafhankelijke auditor (zoals de ADR of een marktpartij)	Kiesraad	Kiesraad	
	AVG en UAVG	Controle door Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	Autoriteit Persoons-gegevens	

Figuur 10: Visualisatie koppelingen Diginetwerk en infrastructuur DHV.



Legenda	
Symbool	Beschrijving
	(Virtuele) server
	(Virtuele) firewall
	Gebruiker
	Werkstation (desktop, laptop, tablet, etc.)
	Diginetwerk
	Database
	Certificate server
	Load balancer
	Modem
	Smart phone