

Enterprise Architecture Document

Stakeholders

Rol	Naam
Enterprise Data Architect	Jean-Michel COGNIAUX (JMC)
Security Architect	Sébastien BERNARD (SBE) Costas SIMATOS (CSI)
Business Analyst	Laureen MADEJ (LMA) Alexia WINANDY (AWI)
Functional Analyst	Philippe EVRARD (PHE) Maxime MICHEZ (MMI) Arnaud PIRLOT (API)
Technical Analyst	Amory SCHOONBROODT (ASC) Olivier BLANPAIN (OBL)
Project Manager	Aurélie HERKENNE (AHE)
Data Privacy Officer	Francis OUAAL (FOA)

Herziening van de inhoud

Elke nieuwe versie van het document moet worden opgenomen in de onderstaande tabel. Elke versie moet een status toegewezen krijgen: "Creation", "Update", "Final draft", "Review", "Approval", "Published".

Versie	Datum	Wie	Status	Wijzigingen
0.1	01/09/2023	LMA & AWI	Draft	Initiëring van het document
0.2	03/10/2023	JMC	Draft	
1.2	31/10/2023			Approved

Inhoud

1	Referenties.....	4
2	Context	4
3	Doelstellingen van het document	6
3.1	Verwijzing naar Archimate	6
3.2	Verwijzing naar TOGAF	7
3.3	Logische benadering.....	8
4	Omschrijving	9
5	Beperkingen.....	11
6	Werkhypothesen.....	11
7	Bedrijfsbehoeften	14
8	Evaluatie van de risico's	16
9	Vereisten.....	18
9.1	Bedrijfsvereisten	18
9.2	Functionele vereisten.....	21
9.3	Niet-functionele vereisten.....	24
9.4	Technische vereisten.....	28
9.5	Beveiligingsvereisten	33
9.6	Vereisten buiten het toepassingsgebied	39
10	Oplossing	40
10.1	Motivatiediagram	40
10.2	Bedrijfsarchitectuur (Business Layer)	46
10.3	Functionele toepassingsarchitectuur (Application Layer)	47
10.4	Technische architectuur (Technology Layer)	53
10.5	SWOT	54
10.5.1	SWOT Business.....	55
10.5.2	Technische SWOT	56
11	Bijlagen.....	59
11.1	Glossarium	59
11.2	Archimate-elementen	60
11.2.1	Business Architecture.....	60

11.2.2	Architecture Application	61
11.2.3	Architecture Technology	63

1 Referenties

	Documentnaam	Beschrijving	Auteur
REF01	Lijst van de use cases	Lijst van use cases per systeem, gebruikt als basis voor het analyseren van de risk assessments en het vaststellen van de verschillende requirements	NRB & Civadis
REF02	PROJECT NETVOTING_BE - Rapport deel 1	Studie over de mogelijkheid om online stemmen in België in te voeren Deel 1 (ver. 4 december 2020)	Hoofdpromotor: Prof. Jean-Benoit Pilet (Université libre de Bruxelles) Promotoren: Prof. Bart Preneel (KU Leuven), Prof. Silvia Erzeel (Vrije Universiteit Brussel), Prof. Olivier Pereira (UCLouvain)
REF03	Functioneel schema van het stemmen in hokjes		Civadis
REF04	CDC		Organiserend bestuur
REF05	Website https://elections.fgov.be/	Officiële Belgische website	fgov

2 Context

Dit document is een vervolg op de interuniversitaire studie NETVOTING-BE (J.-B. Pilet et al., Étude sur la possibilité d'introduire le vote Internet en Belgique, elections.fgov.be, 2020).

Het onderwerp van deze studie was elektronisch stemmen in België. Ze is opgebouwd rond vier dimensies van het online stemmen:

- de IT-dimensie en de beveiliging van het stelsysteem
- de aanvaarding door burgers en overheden (sociaal-politieke dimensie)
- de organisatorische dimensie
- de wettelijke en regelgevende dimensie

De doelstellingen van de studie luiden als volgt:

- Een gedetailleerde inventaris opmaken van de ervaringen met online stemmen in vijf landen: Australië, Estland, Frankrijk, Noorwegen en Zwitserland.
- Nagaan in welke mate deze ervaringen kunnen worden omgezet naar België.

De NETVOTING-BE studie concludeerde als volgt: "Gezien de moeilijkheden die nog steeds verbonden zijn aan het stemmen via internet en die moeilijk te overwinnen blijven in een context van overheidsverkiezingen, bestudeert een aantal onderzoekers steeds actiever de mogelijkheid om een aantrekkelijke tussenstap aan te bieden tussen het stemmen in een stembureau en het stemmen via internet. Bijvoorbeeld, in het geval van een stelsysteem per post met bepaalde online componenten, zou de kiezer toegang kunnen krijgen tot zijn of haar stembiljet via het internet, waardoor de vaak riskante logistiek van het verzenden van post naar de kiezer wordt vermeden, in het bijzonder voor kiezers die in het buitenland wonen. Het stembiljet (of een vereenvoudigde versie van het stembiljet met alleen de keuze van de kiezer als die via de computer wordt gemaakt) moet door de kiezer worden afgedrukt, ingevuld en naar een stembureau worden gestuurd. Deze strategie heeft het voordeel dat het probleem van de individuele controleerbaarheid de facto wordt opgelost: de kiezer kan er zeker van zijn dat zijn papieren stembiljet zijn stemintentie weergeeft".

3 Doelstellingen van het document

De doelstellingen van dit "Enterprise Architecture Document" zijn:

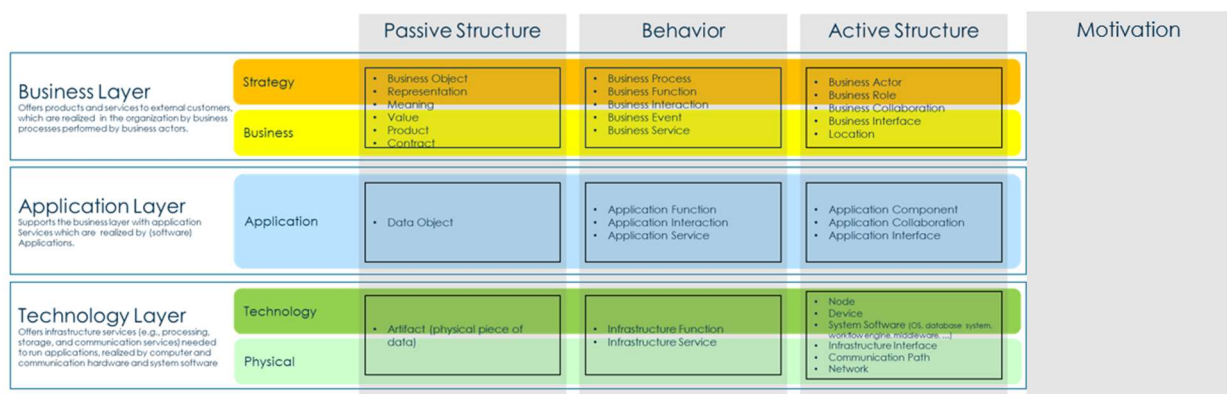
- De beslissing ondersteunen om de beste oplossing te implementeren, in lijn met de doelstellingen en naleving van de vereisten.
- De oplossing documenteren en beslissingen rationaliseren:
 - Als basis dienen voor het schatten van de kosten van de oplossing
 - Een overzicht op hoog niveau bieden van de oplossing in termen van bedrijfs-, toepassings- en technologische aspecten
 - Dienen als input voor:
 - Opstellen van de SWOT-matrix
 - Identificeren van mogelijkheden voor volledig of gedeeltelijk hergebruik tussen verschillende systemen
 - "Solution Architecture Blueprint"

Dit "Enterprise Architecture Document" beschrijft de behoeften en vereisten, evenals verschillende high-level architecturen die nuttig zijn voor het implementeren van de vraag.

Dit document behandelt bedrijfs-, toepassings- en technologische aspecten, inclusief context, risicoanalyse en informatiemodellen.

3.1 Verwijzing naar Archimate

Dit document verwijst naar de Archimate-modelleertaal en stelt architectuurartefacten voor in de volgende drie lagen: bedrijf, toepassing en technologie.



3.2 Verwijzing naar TOGAF

Dit document verwijst naar de concepten van Building Blocks: de ABB's.

Het "Open Group Architecture Framework", ook bekend onder het acroniem TOGAF, is een verzameling concepten en een industriestandaard op het gebied van IT-architecturen voor bedrijven.

Twee belangrijke elementen van het framework zijn de ABB's ("Architecture Building Blocks") en SBB's ("Solution Building Blocks").

Een "Building Block" is een verzameling functionaliteiten die zijn gedefinieerd om te voldoen aan de behoeften van de onderneming binnen een organisatie.

ABB à IN SCOPE van dit document "Enterprise Architecture Document"

- Definiëren welke functionaliteiten er geïmplementeerd zullen worden
- Bedrijfsmatige, functionele en technologische vereisten
- De ontwikkeling van de SBB's sturen en leiden
- De ABB-specificaties omvatten minstens de volgende elementen:
 - Fundamentele functionaliteiten en attributen, inclusief capaciteit, beveiliging en onderhoud, ...
 - Interfaces: API's, gegevensformaten, protocollen, hardware-interfaces, normen, ...
 - Bouwstenen afhankelijk van de vereiste functionaliteiten
 - Relatie met entiteiten en bedrijfs-/organisatiebeleid

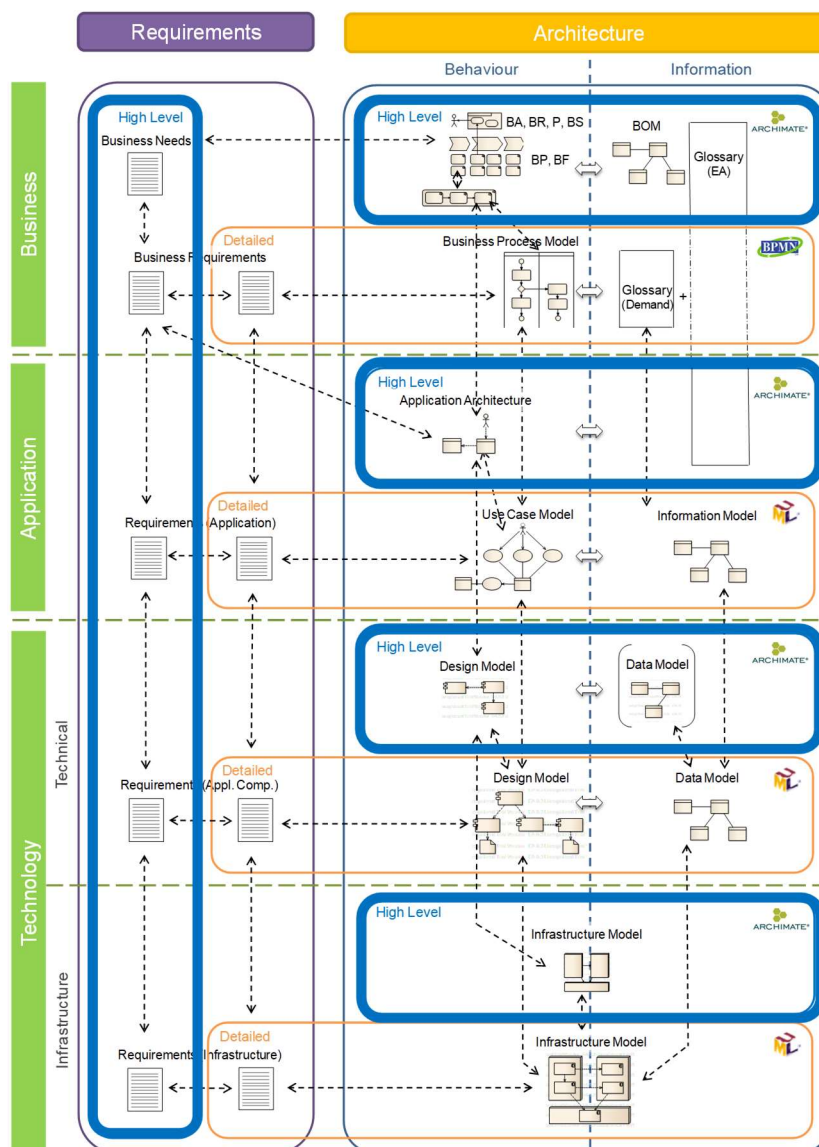
SBB à OUT of SCOPE van dit "Enterprise Architecture Document"

- Definiëren welke hardware, software, editors, enz. de functionaliteit zullen implementeren
- De implementatie definiëren
- Tegemoetkomen aan de beperkingen die zijn geïdentificeerd in ABB
- De SBB-specificaties omvatten ten minste de volgende elementen:
 - Specifieke functionaliteiten en eigenschappen
 - Interfaces
 - Integratie van SBB's in het IT-landschap en het operationele beleid
 - Specificatie van gedeelde kenmerken binnen de totale IT-omgeving: beveiliging, locatie, schaalbaarheid, prestaties, configuraties, enz.
 - Ontwerppilots en -beperkingen, inclusief fysieke architectuur

3.3 Logische benadering

Dit document respecteert ook de volgende logische benadering:

- Verzamelen van de bedrijfsbehoeften (Business Needs)
- Bepalen van de bedrijfsvereisten (BR sécuri- Business Requirements)
- Bepalen van de functionele vereisten (FR – Functional Requirements)
- Bepalen van de niet-functionele vereisten (NFR – Non Functional Requirements)
- Bepalen van de technische vereisten (TR – Technical Requirements)
- Bepalen van de veiligheidsvereisten (SEC – Security Requirements)
- Bepalen van de bedrijfsarchitecturen
- Bepalen van de logische architecturen
- Bepalen van de toepassingsarchitecturen
- Bepalen van de technologische architecturen



4 Omschrijving

Het project heeft betrekking op het uitvoeren van een studie over de functionele, budgettaire, technische en veiligheidsbeschrijving van de ontwikkeling van een online stemsysteem, evenals het onderhoud en de controle ervan, voor verkiezingen die in België door de federale overheid worden georganiseerd (d.w.z. voor Europese, federale en gewestelijke verkiezingen).

Het resultaat van dit werk belicht 3 verkiezingssystemen:

1. ~~Hybride online stemsysteem~~
2. ~~Volledig online stemsysteem~~
3. Kioskstemsysteem

Dit document behandelt alleen het kioskstemsysteem. De hybride en volledig online systemen worden behandeld in andere Enterprise Architecture Documents.

De klant wil een set specificaties voor het geval een van de oplossingen in de toekomst wordt geïmplementeerd:

1. De functionele vereisten
2. De vereisten op het vlak van beveiliging en cyberveiligheidselementen
3. De vereisten inzake integriteit, vertrouwelijkheid, verifieerbaarheid, transparantie en monitoring
4. ~~Een realistisch tijdschema voor de ontwikkeling van dit systeem~~
5. ~~Een raming van de globale kostprijs van de infrastructuur en de ontwikkeling, uitgesplitst per module (CAPEX + OPEX)~~
6. ~~Een capaciteitsplan inzake middelen voor de implementatie~~
7. ~~Een raming van de kosten voor onderhoud, audit en controle van de oplossingen (OPEX)~~

Alleen de punten 1, 2 en 3 zijn opgenomen in dit Enterprise Architecture Document. De andere punten worden in andere documenten behandeld.

In elk van de drie verkiezingssystemen wordt de status van de stem gecontroleerd en geeft een bevestigingsbericht aan of de stem al dan niet in aanmerking is genomen. In het geval van de kioskstemming krijgt de kiezer toegang tot de stemverificatie door in te loggen met behulp van zijn of haar identiteitskaart en rijksregisternummer¹. De authenticatie die nodig is om toegang te krijgen tot het systeem vereist een CSAM-verbinding (eID of ItsMe). Voor Belgen in het buitenland die geen geactiveerde identiteitskaart hebben, omvat de CSAM-authenticatie alternatieve authenticatiemethoden naast eID en ItsMe die van toepassing zijn. De implementatie van deze alternatieve authenticatiemethoden heeft geen impact op de software die zal worden gecreëerd en is enkel een kwestie van configuratie (bv. een tweede instantie voorzien voor dezelfde toepassing waardoor Belgen die geen gebruik kunnen maken van eID of ItsMe zich kunnen authenticeren).

¹ De CSAM-authenticatie omvat alternatieve authenticatiemethoden met hetzelfde zekerheidsniveau die onder andere van toepassing zijn voor Belgen in het buitenland.

Een dubbele verificatie van stemmen wordt vermeld in het interuniversitaire project Netvoting-be (J.-B. Pilet et al., Étude sur la possibilité d'introduire le vote Internet en Belgique, elections.fgov.be, 2020). Deze dubbele verificatie houdt rekening met het feit dat de stem is geregistreerd en voorziet ook in de mogelijkheid om de inhoud van de stem te verifiëren. De in de studie genoemde mogelijkheid om de inhoud van de stem te controleren, is in deze analyse niet overgenomen om praktische redenen die verband houden met de uitvoering, de haalbaarheid en het stemgeheim.

5 Beperkingen

De volgende tabel geeft een overzicht van de beperkingen die van invloed zouden kunnen zijn op de oplossing die in dit document wordt beschreven.

- Als er sprake is van een tijdsbeperking, geef dan specifiek aan: wanneer?
- Als de beperking van een externe speler komt, geef dan in de beschrijving aan van wie deze komt.
- Maak de beschrijving zo expliciet mogelijk:
 - o Welke impact heeft dit op het project?
 - o Waarom is het belangrijk om er rekening mee te houden?

	Datum	Wie	Beschrijving
CTR01	01/09/23	PHE	De implementatie van een oplossing vereist een wijziging van de huidige wetgeving. Dit vereist a priori een politiek akkoord.
CTR02	01/09/23	PHE	Naleving van de verkiezingsagenda.
CTR03	01/09/23	APE	Het systeem kan niet worden gehost in de publieke cloud: de bronnen en de applicatie, zowel in de ontwikkelings- als in de productiefase.

6 Werkhypothesen

De volgende tabel bevat de werkhypothesen die zijn gemaakt, d.w.z. de voorstellen die zijn gedaan als antwoord op de vragen die zijn gesteld tijdens de ontwikkeling van de oplossing.

	Datum	Wie	Beschrijving
HYP01	01/09/2023	JMC	<p>Het stelsysteem is bedoeld voor verkiezingen georganiseerd door de federale overheid. De betrokken niveaus zijn:</p> <ul style="list-style-type: none">• Europees (Europees Parlement)• Federaal (Kamer van Volksvertegenwoordigers)• Gewestelijk (Waals, Vlaams en Brussels Parlement en Raad van de Duitstalige Gemeenschap) <p>De provinciale en gemeentelijke verkiezingen vallen niet onder deze studie.</p>
HYP02	30/09/2023	JMC	De aanpak van het kiosksysteem is een elektronisch stelsysteem dat alle functies bevat die nodig zijn om te stemmen, met uitzondering van het versturen van uitnodigingen naar de kiezers.
HYP03	30/09/2023	JMC	<p>In het traditionele "papieren" stelsysteem heeft het stembiljet twee functies:</p> <ol style="list-style-type: none">1) Het presenteren van de kieslijsten van de partijen → In het kiosksysteem wordt de term "stembiljet" vervangen door "de kieslijsten van de partijen".2) Het dienen als fysieke drager voor het registreren van de keuze van de kiezer en voor het tellen van de stemmen → In het kiosksysteem zal de term "stembiljet" vervangen worden door "elektronisch stembiljet" en zal het bestaan als een elektronisch bericht in transit

			tussen de stemcomputer (aka de elektronische terminal die ter beschikking wordt gesteld van de kiezer) en de toepassing.
HYP04	30/09/2023	JMC	<p>In het traditionele "papieren" stelsysteem is de stembus een fysieke kluis die de erin gedeponeerde stembiljetten ontvangt en beschermt en het stemgeheim garandeert.</p> <p>In het kiosksysteem is het concept van de stembus nog steeds aanwezig. Het is een elektronische stembus met dezelfde functies, namelijk: elektronische stembiljetten ontvangen, ze beschermen en het stemgeheim garanderen.</p>
HYP05	30/09/2023	JMC	<p>Het kiosksysteem ondersteunt de volgende functies:</p> <ul style="list-style-type: none"> • Ontvangst van de partij- en kandidatenlijsten; • Ontvangst van de kiezerslijsten; • Presentatie van de verkiezingslijsten van de partijen via een interface; • Verificatie van de inaanmerkingneming van de stemmen van de kiezers; • Uitgifte van het stembewijs aan de kiezers; • Controle of kiezers hun stem hebben uitgebracht en opstellen van de presentielijst (lijst van kiezers die via het kiosksysteem een stem hebben uitgebracht); • Tellen van de stemmen; • Interface voor stemtoezicht (anoniem); • Opstellen van het rapport met de samengevoegde resultaten; • Afdrukken van het rapport met de samengevoegde resultaten.
HYP06	03/10/2023	JMC	<p>Presentie:</p> <ul style="list-style-type: none"> • Kiezers in België hoeven zich niet te registreren om te stemmen. Ze gaan naar het stemlokaal en gebruiken een computer om hun stem uit te brengen. De presentielijst wordt automatisch bijgewerkt (door informatiestromen in pseudo-realtime tussen de stemcomputer en het kiosksysteem). • Belgen die vanuit het buitenland stemmen, moeten zich registreren om te kunnen stemmen. De presentielijst wordt vóór de stemming opgesteld. Ze wordt niet bijgewerkt tijdens de stemming.
HYP07	14/09/2023	JMC	<p>De volgende begrippen verdwijnen:</p> <ul style="list-style-type: none"> • Stemopnemingsbureau • Ontvangstbureau • Proces-verbaal van samenstelling van de bureaus
HYP08	03/10/2023	JMC	<p>In de context van het kiosksysteem moeten er 2 types van bureaus voorzien worden:</p> <ul style="list-style-type: none"> - Het hoofdbureau Het enige echte. Het bestaat uit een voorzitter, bijzitters en getuigen. Zijn functie is toezicht houden op de stemverrichtingen, de stemming sluiten en de geldigheid van de stemming garanderen. - De kieskringbureaus Naar rato van één per kieskring zijn er evenveel kieskringbureaus als dat er kieskringen zijn. Elk kieskringbureau bestaat uit een voorzitter, bijzitters en getuigen. Zijn functie is

			toezicht houden op de stemverrichtingen, de stemming sluiten en de geldigheid van de stemming garanderen.
HYP09	04/10/2023	JMC	<p>In de context van het kiosksysteem zal het concept van het stembureau evolueren.</p> <p>In het buitenland zullen de kiosken de huidige stemhokjes (op de ambassade of het consulaat) vervangen.</p> <p>In België zullen de stemlokalen uitgerust worden met een of meer kiosken op openbare plaatsen (stations, administraties, enz.) → andere locaties dan de traditionele stembureaus.</p> <p>Stemmen in het buitenland: Stemlokaal = verzameling stemhokjes (kiosken) met stemcomputers. Dit bureau zal bemand worden door leden van het stembureau.</p> <p>Stemmen in België: Stemlokaal = plaats uitgerust met een of meer stemhokjes (kiosken). De stemlokalen staan onder toezicht van stewards die toezien op de veiligheid, ter voorkoming van diefstal, schade, enz., maar niet van een voorzitter, bijzitters en getuigen.</p>
HYP10	03/10/2023	JMC	<p>De lokalen zijn vier dagen voor de dag van de stemming geopend voor stemmingen in België, van woensdag tot zaterdag.</p> <p>De stembureaus zijn alleen open op de dag van de verkiezingen voor stemmen die in het buitenland worden uitgebracht.</p>
HYP11	15/10/2023	JMC	<p>Voor stemlokalen, in het geval van stemmen die in België worden uitgebracht, zijn de bewakers niet beëdigd. Dit betekent dat de bewakers alleen kunnen helpen met vragen over de stemcomputers en IT-kwesties. Ze kunnen geen vragen van kiezers beantwoorden over de stemming zelf.</p> <p>Voor stembureaus, in het geval van stemmen die in het buitenland worden uitgebracht, wordt de permanentie verzekerd door beëdigde personen. Zij kunnen vragen over de computer en vragen over het stemproces beantwoorden.</p>

7 Bedrijfsbehoeften

Business Needs [BN].

De bedrijfsbehoefte is de uitdrukking van een wens, verlangen, probleem of frustratie om gestelde doelen of doelstellingen te bereiken. De zakelijke behoefte is de reden "waarom" het project is gestart (algemene doelstelling). De bedrijfsbehoefte kan bijvoorbeeld zijn: "Voorkom stemmen op papier" of "Verbeter de efficiëntie van het stemmen door een IT-systeem te gebruiken".

BN001	Een zelfbedieningstoegang krijgen tot de kieslijsten van de partijen en een keuze kunnen maken De kiezer maakt verbinding met de stemcomputer, die op zijn beurt verbinding maakt met de server waarop de oplossing staat, via een beveiligd webnetwerk. De kiezer logt in op het systeem om toegang te krijgen tot de steminterface. Het systeem presenteert kiezers de kieslijsten van partijen die specifiek zijn voor hun context (bijvoorbeeld voor regionale verkiezingen). De kiezer stemt rechtstreeks.
BN002	Vooraf stemmen Kiezers stemmen met behulp van de stemcomputer en de ter beschikking gestelde interface: ze voeren hun keuze in (per selectie) en valideren deze. De periode van vervroegd stemmen duurt vier dagen voor stemmen uitgebracht in België, van woensdag tot zaterdag. Belgen in het buitenland kunnen niet vooraf stemmen. Na registratie stemmen ze op de dag van de stemming.
BN003	Tellen van de vooraf uitgebrachte stemmen op de dag van de stemming Het tellen van de kioskstemmen vindt plaats op de officiële dag van de stemming. Dit zorgt ervoor dat er geen voorresultaten worden gepubliceerd die de keuze van de kiezers zouden kunnen verstoren.
BN004	Controleren of er rekening is gehouden met de stem(men) Zodra de kiezer zijn keuze heeft gemaakt, wordt er onmiddellijk een bevestigingsbericht geproduceerd waarin de keuze van de kiezer wordt aangegeven en wordt bevestigd dat er rekening is gehouden met de stem.
BN005	Doorlichten van het stelsysteem De inrichtende macht moet in staat zijn om: <ul style="list-style-type: none">• Het systeem tijdens en buiten verkiezingsperioden aan een audit te onderwerpen;• De controlepunten en de tolerantiedrempel te bepalen;• De goede werking en de veiligheid van het systeem te garanderen;• Interne en externe audits uit te voeren.
BN006	Een meerwaarde bieden in vergelijking met de huidige 3 stelsystemen

Verwachtingen: flexibiliteit, eenvoud en grotere toegankelijkheid ten opzichte van de huidige systemen.

Namelijk:

- Stemmen op papier
- Elektronisch stemmen
- Stemmen per post

BN007 Moderniseren van het stemmen

Het systeem moet geheel of gedeeltelijk gebruik maken van moderne informatietechnologieën om:

- De huidige stelsystemen geheel of gedeeltelijk te dematerialiseren;
- Menselijke handelingen geheel of gedeeltelijk te automatiseren door geautomatiseerde processen;
- De snelheid te verhogen waarmee burgers kunnen stemmen, stemmen tellen en resultaten publiceren.

BN008 Beheersen van de kostprijs van de oplossing

De inrichtende macht moet zich bewust zijn van de jaarlijkse kosten voor het onderhouden en updaten van het systeem, om te garanderen dat het systeem altijd operationeel is vanuit functioneel en veiligheidsoogpunt. Bij deze kosten moet rekening worden gehouden met de "fulltime" interne middelen die nodig zijn tijdens niet-verkiezingsperioden.

8 Evaluatie van de risico's

Veiligheidsrisico's Impact- en waarschijnlijkheidsindicatoren volgens de volgende schaal:

- High: de impact of waarschijnlijkheid van het risico is hoog
- Medium: de impact of waarschijnlijkheid van het risico is middelgroot
- Low: de impact of waarschijnlijkheid van het risico is laag

RSK001	De oplossing staat bloot aan cyberaanvallen	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Het kiosksysteem is beschikbaar via het internet en staat daarom bloot aan cyberaanvallen, ook al is het een beveiligd niet-publiek netwerk.			
RSK002	De integriteit van de gegevens van de oplossing wordt bedreigd.	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Het kiosksysteem is beschikbaar via het internet en staat daarom bloot aan cyberaanvallen die de integriteit van de gegevens van de oplossing kunnen bedreigen. Gezien de elektronische stembus kunnen echter bijbehorende beschermingsmaatregelen worden overwogen.			
RSK003	De identiteit van de kiezer kan gestolen worden	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Het kiosksysteem is beschikbaar via een netwerk en een beveiligde webinterface, op gecontroleerde ter beschikking gestelde posten en geauthenticeerd door een bevoegde gebruiker.			
RSK004	De authenticiteit van de stem kan veranderd worden	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
Aangezien in België de stem niet wordt gevalideerd door een stemopnemer en de kiezer niet kan worden geïdentificeerd door een persoon die door de inrichtende macht werd beëdigd, kan de oprechtheid van de stem in twijfel worden getrokken/gewijzigd, aangezien het onmogelijk is om te garanderen dat de kiezer niet is beïnvloed en dat zijn identiteit niet is misbruikt. Dit ondanks de aanwezigheid van stewards in het stemlokaal, aangezien zij onder druk gezet en geïntimideerd kunnen worden. De organisatie van een massale stemming voor een bepaalde kandidaat of een bepaald voorstel kan niet worden uitgesloten.			
RSK005	Het stemgeheim kan in twijfel worden getrokken	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
In België is er geen garantie dat de kiezer en degene die de stem uitbrengt dezelfde persoon zijn, ondanks de aanwezigheid van stewards in het stemlokaal, aangezien zij onder druk gezet en geïntimideerd kunnen worden.			
RSK006	De architectuur van de oplossing kan veiligheidslekken vertonen.	Impact (High/Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
De architectuur van de oplossing kan beveiligingslekken bevatten die misbruikt kunnen worden. De architectuur bevat verschillende componenten waarvan de beheerdersrechten beveiligingslekken kunnen openen of softwareversies (toepassingen en OS - 'Operating System') die niet zijn bijgewerkt of verouderd zijn.			

RSK007	De ontwikkeling van de oplossing is gebrekkig	Impact (High Medium/Low)	Waarschijnlijkheid (High/Medium/Low)
--------	---	-----------------------------	---

De oplossing kan beveiligingsfouten in de code hebben (injectie van kwaadaardige code, gebruik van verouderde bibliotheken, enz.).

Conclusie:

We kunnen ervan uitgaan dat technische tekortkomingen met betrekking tot de architectuur, geprivilegieerde accounts en kwaadaardige code kunnen worden beperkt door controles op het niveau van de definitie van de architectuur, de ontwikkeling van de code, het beheer van de toegangen en de controle op wijzigingen die worden aangebracht in componenten (firewallregel, bijvoorbeeld).

Het voordeel van de Kioskoplossing is dat de klantenposten bekend en gecontroleerd zijn, wat betekent dat er meer geavanceerde firewallregels kunnen worden ingesteld, die zoveel mogelijk beperken wat er op de klantenpost kan worden gedaan.

Helaas is het met deze oplossing echter **vrijwel onmogelijk** om het volgende te garanderen:

- **De identiteit van de kiezer:** Aangezien de kiezer niet geïdentificeerd kan worden door een persoon die beëdigd is door de inrichtende macht, kan zijn identiteit in twijfel worden getrokken.
De identificatie via een systeem zoals CSAM en de aanwezigheid van een steward beperken het risico echter.
- **De oprechtheid van de stem:** het stemmen gebeurt op afstand. Het gebeurt niet in een stembokje en kan worden beïnvloed door een derde partij.
- **Het stemgeheim:** het stemgeheim kan niet worden gegarandeerd. Het stemmen gebeurt niet in een stembokje. Het is heel goed mogelijk om massale stemmingen te organiseren zonder dat dit ontdekt kan worden.
Het controleren van de klantenposten kan dit risico echter helpen beperken.

De risico's verbonden aan deze stemmethode hebben een grote impact op de hierboven beschreven pijlers. De huidige traditionele manier van stemmen, waarbij de kiezer fysiek aanwezig is in het stembokje en een stembiljet of stemmachine gebruikt, is al onderhevig aan internetbeïnvloedingscampagnes en ondermijnt het vertrouwen van de kiezer in de uitkomst van verkiezingen. Niet weten wie er daadwerkelijk heeft gestemd, of de stem de echte wens van de persoon is, en de mogelijkheid om massaal te stemmen zonder garantie van de anonimiteit van de stem, zou dit groeiende wantrouwen alleen maar versterken.

De kioskoplossing biedt echter het voordeel dat de klantenpost kan worden gecontroleerd. Dit maakt het mogelijk om deze risico's te beperken door de afschrikwekkende aanwezigheid van een steward, het beperken van de mogelijke acties die kunnen worden uitgevoerd op de klantenpost en de meer geavanceerde netwerkbeveiliging.

9 Vereisten

Bedrijfs-, functionele, niet-functionele, technische en beveiligingsvereisten. De oplossing zal absoluut aan de prioritaire vereisten moeten voldoen.

- **MUST** = De oplossing kan niet worden geïmplementeerd tenzij aan de eis wordt voldaan. MVP (Minimum Viable Product).
- **SHOULD** = De oplossing kan in een eerste versie worden geïmplementeerd zonder dat aan de eis wordt voldaan, op voorwaarde dat de eis in een toekomstige versie wordt opgenomen.
- **COULD** = Dit is een "Nice to have", het niet voldoen aan deze eis is geen blokkerend punt voor de aanvaarding.

9.1 Bedrijfsvereisten

Business Requirements [BR].

De bedrijfsvereisten zijn wat het systeem moet doen om aan de geuite bedrijfsbehoeften te voldoen. De bedrijfsvereisten beschrijven de karakteristieken van een systeem vanuit het oogpunt van de eindgebruiker van dat systeem. Het systeem is een middel om bedrijfsdoelstellingen te leveren, te vervullen of eraan te voldoen.

BR001	Globaal en uniek systeem	Prio (Must / Should / Could)
Het kiosksysteem moet gebruikt kunnen worden voor alle verkiezingen georganiseerd door de federale overheid (federale, gewestelijke en Europese verkiezingen) en voor alle soorten kiezers (stemmen uitgebracht door Belgen in België en stemmen uitgebracht door Belgen in het buitenland).		
BR002	Naleving van de Belgische grondwettelijke stemprincipes	Prio (Must / Should / Could)
De fundamentele elementen van het Belgische kiesstelsel zijn vastgelegd in de Grondwet:		
1. De verkiezingen vinden plaats volgens het algemeen stemrecht		
Het algemeen stemrecht geeft alle burgers de kans om hun mening te uiten zonder beperkingen wat betreft rijkdom of erfelijkheid.		
2. Het principe van evenredige vertegenwoordiging wordt toegepast		
Een evenredig systeem is een kiesstelsel dat aan elke lijst een aantal verkozenen toekent dat evenredig is met het aantal stemmen dat deze lijst heeft gekregen.		
3. Elke kiezer heeft één stem (behalve in het geval van een gevolmachtigde)		
De verschillende verkiezingen hebben drie voorwaarden gemeen om te mogen stemmen:		
<ul style="list-style-type: none">- Minstens 18 jaar oud zijn. Behalve voor de Europese verkiezingen (vanaf 2024), waar 16- en 17-jarigen kunnen kiezen om te stemmen als ze dat willen.- Ingeschreven zijn in het bevolkingsregister van een Belgische gemeente op de dag dat de kiezerslijst wordt afgesloten (de inschrijving in het vreemdelingenregister van de gemeente geldt voor de Europese en gemeenteraadsverkiezingen).		

- Niet het voorwerp uitmaken van een gerechtelijke beslissing die het kiesrecht schorst.

4. De stemming is geheim

Het is onmogelijk om te zeggen wie waarvoor heeft gestemd.

5. De stemming is verplicht

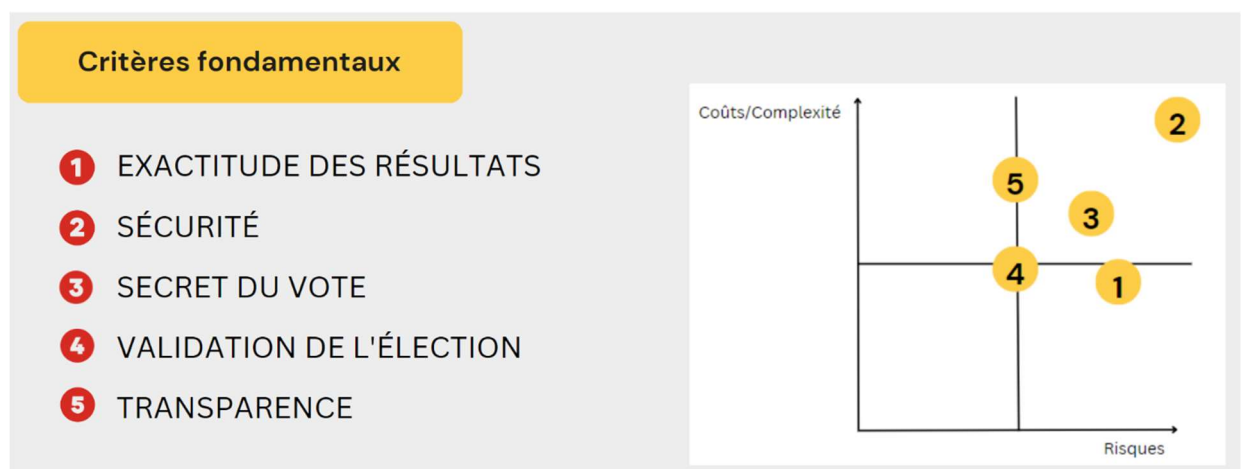
Elke Belgische burger die aan de bovenstaande voorwaarden voldoet, is verplicht om te stemmen. Het niet uitoefenen van dit recht stelt hem bloot aan sancties. Als het voor een burger onmogelijk is om persoonlijk te stemmen, kan hij zijn stem uitbrengen via een vertrouwenspersoon.

- Belgen in België hoeven vooraf geen bijzondere stappen te ondernemen. Als ze voldoen aan de vier hierboven vermelde voorwaarden om te stemmen, krijgen ze automatisch een oproeping.
- Europese buitenlanders die in België aan de Europese verkiezingen deelnemen, moeten zich laten registreren.
- Belgen in het buitenland zijn verplicht om te stemmen als ze op de consulaire lijsten staan en zich vooraf hebben geregistreerd voor deze stemmethode.

Tijdens een workshop met IBZ op 15 februari 2023 rangschikten de deelnemers de verschillende fundamentele criteria voor het uitvoeren van de studie in volgorde van belangrijkheid. Deze criteria werden gezamenlijk gerangschikt in de volgende volgorde:

- 1) Nauwkeurigheid van de resultaten
- 2) Veiligheid
- 3) Geheim van de stemming
- 4) Validatie van de verkiezingen
- 5) Transparantie

Vervolgens plaatsten we ze op een matrix in termen van de kosten/complexiteit van implementatie en de risico's van niet-implementatie.



Critères fondamentaux	Fundamentele criteria
EXACTITUDE DES RÉSULTATS	NAUWKEURIGHEID VAN DE RESULTATEN

SÉCURITÉ	VEILIGHEID
SECRET DU VOTE	GEHEIM VAN DE STEMMING
VALIDATION DE L'ÉLECTION	VALIDATIE VAN DE VERKIEZING
TRANSPARENCE	TRANSPARANTIE
Coûts/Complexité	Kosten/Complexiteit
Risques	Risico's

BR003 Evolutieve architectuur

Prio (Must / Should / Could)

De oplossing moet onafhankelijke, onderling verbonden componenten bevatten die hergebruikt kunnen worden naarmate de oplossing evolueert. Dit principe garandeert een zekere rationaliteit en efficiëntie in kostenbeheersing.

BR004 Beheer van wijzigingen

Prio (Must / Should / Could)

Dit nieuwe systeem moet uitgelegd en begrepen worden door de vertegenwoordigers van de inrichtende macht en door de leden van de onthaal-/tellingbureaus die het systeem zullen gebruiken.

BR005 Beheer van de faciliteitengemeenten

Prio (Must / Should / Could)

Dit zijn gemeenten die, in de zin van de toepassing van de wetten op het gebruik van talen in administratieve aangelegenheden, genieten van een systeem van taalkundige faciliteiten ten voordele van hun inwoners. De wet van 8 november 1962 voorzag in vijf categorieën gemeenten die konden afwijken van de regel van territoriale eentaligheid (met een minimum van 30% minderheden) zonder de status van tweetalige gemeente te verwerven (behalve in Brussel).

"Faciliteitengemeenten" worden gekenmerkt door eentalige interne diensten (de administratie werkt in één taal) en externe tweetaligheid (de administratie gebruikt twee talen in haar contacten met het publiek).

BR006 Procedure voor coördinatie met belanghebbenden

Prio (Must / Should / Could)

Opstellen van een coördinatieprocedure met de accreditatieorganisatie, het cybercriminaliteits- en defensiecentrum, het college van deskundigen (vertegenwoordigers van de verschillende vergaderingen) en de betrokken toezichthoudende organen.

9.2 Functionele vereisten

Functional Requirements [FR].

De functionele vereisten (FR- Functional Requirements) zijn een verklaring over hoe een systeem zich moet gedragen. Ze definiëren wat het systeem moet doen om aan de bedrijfsbehoeften te voldoen. De functionele vereisten kunnen worden gezien als kenmerken die de gebruiker detecteert.

FR001 Invoeren van gegevenslijsten (Data File Transfer) Prio (Must / Should / Could)

- Lijst van Belgische kiezers die in België wonen, invoer van de kiezerslijst uitgegeven door de gemeenten.
- Lijst van Belgische kiezers die in het buitenland wonen en zich hebben geregistreerd, invoer van de kiezerslijst uitgegeven door de beroepsconsulaire posten/diplomatieke posten.
- Lijst van politieke partijen, invoer van de officiële lijst van partijen en kandidaten verstrekt door de inrichtende macht, in een gestandaardiseerd formaat.

FR002 Opgeven van de samenstelling van de kieskring- en hoofdbureaus Prio (Must / Should / Could)

Het systeem moet het mogelijk maken om de leden van de kiesbureaus te coderen nadat ze beëdigd zijn:

- Datum van de verkiezingen;
- Kanton / kieskring / kiescollege (stemming Europees Parlement);
- Nummer van het kieskringbureau;
- Naam van de persoon;
- Rol (voorzitter, bijzitter of getuige).

Het systeem moet het mogelijk maken de redenen in te geven, waarvoor een bijzitter of voorzitter weigert zich aan te melden bij het bureau.

Het systeem moet het mogelijk maken verzoeken en beslissingen over het al dan niet ontheffen van bijzitters of voorzitters die daarom verzoeken, te coderen (beslissingslogboeken).

FR003 Unieke authenticatie

Prio (Must / Should / Could)

De unieke authenticatie is een methode die een gebruiker toegang geeft tot de functionaliteiten van het kiosksysteem door gebruik te maken van een unieke authenticatie om toegang te krijgen tot alle functionaliteiten.

FR004 "Gebruiksvriendelijke" interface Prio (Must / Should / Could)

Gebruiksvriendelijke, ergonomische en intuïtieve interface voor kiezers die toegang willen tot het kiosksysteem.

Het belangrijkste doel van een gebruiksvriendelijke interface is om een zo bevredigend mogelijke gebruikerservaring te bieden: grafische interface, gemakkelijk herkenbare invoerzones, grootte van de invoerzones, grootte van de tekens, natuurlijke gebruikerstaal, enz.

In overeenstemming met de norm EN 301 549 V3.2.1 (2022) moet het systeem een hoge mate van toegankelijkheid garanderen, met name voor ouderen, kleurenblinden, slechtzienden en mensen met een handicap.

Het World Wide Web Consortium (W3C) publiceert regelmatig een lijst met standaarden die moeten worden geïmplementeerd om een zo hoog mogelijk niveau van toegankelijkheid te garanderen.

FR005 Zelfbediening Prio (Must / Should / Could)

Na het inloggen en authenticeren biedt het systeem kiezers de optie om direct te stemmen via een interface en een bericht te ontvangen waarin wordt bevestigd dat hun stem in aanmerking is genomen.

FR006 Rapporten en dashboards Prio (Must / Should / Could)

Het kiosksysteem moet rapporten kunnen produceren op basis van verzoeken van belanghebbenden.

Deze rapporten moeten gemakkelijk toegankelijk zijn.

Deze rapporten en dashboards moeten ook automatisch worden bijgewerkt wanneer de gegevens worden bijgewerkt.

FR007 Beheer van meervoudig stemmen Prio (Must / Should / Could)

Het doel is niet om het meervoudig stemmen te verbieden, maar om de verschillende stemmen te beheren die de kiezer zou kunnen uitbrengen. Alleen de laatste stem wordt in aanmerking genomen.

Het toestaan van meervoudig stemmen garandeert de geheimhouding van de stemming. De kiezer zou immers beïnvloed kunnen worden door een derde partij bij een eerste stemming, en dan opnieuw kunnen stemmen door zijn eigen keuze te maken.

FR008 Consolidatie van de kiezerslijsten Prio (Must / Should / Could)

Het kiosksysteem voorziet in de integratie van de lijst van kiezers die in België stemmen en de lijsten van Belgische kiezers in het buitenland, op voorwaarde dat deze laatsten op voorhand geregistreerd zijn.

FR009 Data Anonymisation, Pseudonymisation Prio (Must / Should / Could)

Anonimisering en pseudonimisering van gegevens hebben tot doel private, gevoelige of vertrouwelijke informatie uit de ruwe gegevens te maskeren. Het resultaat zijn gegevens die met geen enkel individu in verband kunnen worden gebracht.

Anonimisering en pseudonimisering van gegevens is een manier om een valse maar realistische versie van organisatiegegevens te creëren. Het doel is om gevoelige gegevens te beschermen en tegelijkertijd een functioneel alternatief te bieden wanneer echte gegevens niet nodig zijn.

Bij anonimisering kan de broninformatie niet worden geregenereerd. Dit is wel het geval bij pseudonimisering. Er wordt gekozen voor anonimisering, pseudonimisering wordt afgewezen.

FR010 Toegangsbeheer Prio (Must / Should / Could)

Het betreft hier de planning, de ontwikkeling en de uitvoering van beveiligingsrichtlijnen, -processen en -procedures om een gepaste authenticatie, autorisatie, toegang en audit mogelijk te maken.

- De juiste toegangen activeren en ongepaste toegangen voorkomen.
- Alle relevante regels en beleidsrichtlijnen op het gebied van privacy, bescherming en vertrouwelijkheid begrijpen en naleven.
- Ervoor zorgen dat de privacy- en vertrouwelijkheidsbehoeften van alle belanghebbenden worden toegepast en gecontroleerd.

FR011 Stemhokje Prio (Must / Should / Could)

Het stembureau/-lokaal bestaat uit meerdere stemcomputers. Het stembureau/-lokaal staat onder toezicht.

FR012 Time out – Beheer van de activiteitsduur van de sessie Prio (Must / Should / Could)

Om het risico van binnendringen van de stemcomputer te beperken, is de duur van de sessieactiviteit beperkt:

- Onderbreking van de sessie bij inactiviteit. De sessie wordt onderbroken als de kiezer gedurende een nader te bepalen periode geen actie onderneemt op de stemcomputer. Bijvoorbeeld 30 seconden.
- Onderbreking van de sessie bij activiteit. De sessie wordt onderbroken als de kiezer verbonden is met de stemcomputer voor een periode langer dan een te definiëren tijdsinterval. Bijvoorbeeld 15 minuten.

FR013 Publicatie van de resultaten Prio (Must / Should / Could)

De stemmen van het kiosysteem (vooraf stemmen) worden gereserveerd en geteld op de officiële stemdag. Verder is het verboden om gedeeltelijke vervroegde resultaten vast te stellen.

9.3 Niet-functionele vereisten

Non Functional Requirements [NFR].

Een "niet-functionele vereiste" houdt een beperking in op de infrastructuur van de oplossing. Het gaat meestal om hoge prestaties, volume, beschikbaarheid, schaalbaarheid, enz.

NFR001	Beleid inzake het bewaren van gegevens	Prio (Must / Should / Could)
<p>De databewaringstermijn moet worden gedefinieerd, in overeenstemming met het dataretentiebeleid dat wordt toegepast op de verschillende stelsystemen. De gegevens worden verwijderd zodra de verkiezingsresultaten zijn gevalideerd.</p> <p>De ontvangen elektronische stembiljetten worden in de elektronische stembus bewaard totdat de resultaten zijn gevalideerd. Daarna worden ze vernietigd (gewist in overeenstemming met de procedures die in het kader van de stemming worden toegepast). Voor de ontwikkelings- en testperiode kan een specifiek beleid worden toegepast.</p> <p>Op basis van deze periode zal een geautomatiseerd proces verouderde gegevens uit de opslag van het systeem verwijderen.</p>		
NFR002	Performance	Prio (Must / Should / Could)
<p>Elke transactie heeft een maximale reactietijd van 2 seconden, zodat de gebruiker onmiddellijk feedback krijgt.</p>		
NFR003	Service Level Agreement	Prio (Must / Should / Could)
<p>De SLA moet worden gedefinieerd voor elk onderdeel van het systeem (backend, frontend, opslag, middleware, enz.).</p> <p>De Service Level Agreement (SLA) is een gedocumenteerde overeenkomst die de kwaliteit van de dienstverlening definieert, een voorgeschreven prestatie tussen de systeemontwikkelaar en de inrichtende macht.</p> <p>Het gaat om clausules op basis van een contract waarin de precieze doelstellingen worden gedefinieerd die worden verwacht en het serviceniveau dat wordt gewenst door de inrichtende macht, en waarin de verantwoordelijkheden worden vastgelegd. Dit dient als basis voor het monitoren van het systeem in productie.</p>		
NFR004	RTO – Recovery Time Objective	Prio (Must / Should / Could)
<p>De "Recovery Time Objective" (RTO) of hersteltijddoelstelling is de streefduur en het serviceniveau waarbinnen een bedrijfsproces moet worden hersteld na een onderbreking om een verstoring van de bedrijfscontinuïteit te voorkomen.</p> <p>De verwachte RTO is bijna 0 seconden op de onderdelen backend, opslag en frontend, voor de periode van vervroegd stemmen, d.w.z. (D-7) totdat de verkiezing is gevalideerd.</p> <p>SLA-niveau = 99.96%</p> <p>Downtime/onbeschikbaarheid per dag = 35 seconden</p> <p>Downtime/onbeschikbaarheid per week = 4 minuten 1,9 seconden</p>		

Downtime/onbeschikbaarheid per maand = 17 minuten 23 seconden

Downtime/onbeschikbaarheid per kwartaal = 52 minuten 9,8 seconden

Downtime/onbeschikbaarheid per jaar = 3 uur 28 minuten 39 seconden

De verwachte RTO kan langer zijn buiten de periode van vervroegd stemmen, d.w.z. (D-7) totdat de verkiezing is gevalideerd.

SLA-niveau = 99,900%

Downtime/onbeschikbaarheid per dag = 1 minuut 26 seconden

Downtime/onbeschikbaarheid per week = 10 minuten 5 seconden

Downtime/onbeschikbaarheid per maand = 43 minuten 28 seconden

Downtime/onbeschikbaarheid per kwartaal = 2 uur 10 minuten 24 seconden

Downtime/onbeschikbaarheid per jaar = 8 uur 41 minuten 38 seconden

NFR005 RPO – Recovery Point Objective

Prio (Must / Should / Could)

Een "Recovery Point Objective" (RPO) of herstelpuntdoelstelling is het maximaal aanvaardbare interval waarin transactionele gegevens van een IT-service verloren gaan.

De RPO wordt bepaald door de tijd tussen gegevensback-ups en de hoeveelheid gegevens die verloren zou kunnen gaan tussen back-ups te onderzoeken. De verwachte RPO is 0 seconden.

NFR006 Belasting in een multi-user context Prio (Must / Should / Could)

De oplossing moet bestand zijn tegen een aanzienlijke belasting. Kiezers zullen niet allemaal op hetzelfde moment verbinding maken, maar het aantal is aanzienlijk (basis = jaar 2019: stemmen in België + stemmen van Belgen in het buitenland = 8.167.709, en aantal stembiljetten = 7.218.036).

NFR007 Tests Prio (Must / Should / Could)

De types van tests, protocollen en resultaten worden gepubliceerd voordat het systeem in productie gaat.

Schaalbaarheidstest (basis = jaar 2019: stemmen in België + stemmen van Belgen in het buitenland = 8.167.709, en aantal stembiljetten = 7.218.036)

- Beveiligingstest gegevenstoegang, cfr OWASP-kwetsbaarheid, statisch en dynamisch
- DRtest – Disaster Recovery
- Unittests (minimum 80%)

-
- UAT
 - Geautomatiseerde functionele tests
 - Handmatige functionele tests
 - Penetratietests (interne en externe vijandige agenten)
 - Veiligheidstests
 - Non-regressietests
 - SCA - Software Composition Analysis

De testprotocollen worden vooraf ter validatie naar de accreditatieorganisatie gestuurd. De resultaten worden naar de accreditatieorganisatie gestuurd als input voor hun systeemvalidatieprocedures.

NFR008 Hoge beschikbaarheid Prio (Must / Should / Could)

24 uur per dag, 7 dagen per week gedurende de 7 dagen die aan de dag van de verkiezingen voorafgaan.

NFR009 IT-ondersteuning Prio (Must / Should / Could)

De IT-leverancier houdt toezicht op en biedt IT-ondersteuning voor het systeem aan de inrichtende macht.

De IT-leverancier biedt geen eerstelijns-ondersteuning aan burgers die willen stemmen.

De IT-leverancier produceert volledige documentatie, d.w.z. over de functionele en technische aspecten, onafhankelijk van de serviceovereenkomst.

De accreditatieorganisatie is betrokken bij het verkiezingsproces.

Het cybercriminaliteits- en defensiecentrum is betrokken bij het verkiezingsproces.

NFR010 Betrouwbaarheid - Fault Tolerant Process

Prio (Must / Should / Could)

De processen voor gegevensinvoer, -generatie, -transformatie en -restitutie moeten storingstolerant zijn.

Bij een storing moeten de processen correct herstarten waar ze gebleven waren.

Er moet minimaal automatisch een waarschuwing worden verstuurd en processen die zijn mislukt moeten handmatig opnieuw kunnen worden gestart.

NFR011 Naleving van het privacybeleid voor gegevens - AVG

Prio (Must / Should / Could)

Principes die moeten worden nageleefd in de context van de Belgische grondbeginselen.

Persoonsgegevens mogen alleen worden gebruikt met toestemming van de betrokkene voor het bekende doel, door de voorwaarden te accepteren.

Wanneer een betrokkene zich terugtrekt:

- Er mogen geen persoonlijke gegevens meer worden verzameld;
- Eerder verzamelde persoonsgegevens mogen niet worden gebruikt in de verwerking.

Wanneer een betrokkene zich aanmeldt:

- Persoonsgegevens worden verzameld en gebruikt door de verwerking met betrekking tot het doel waarvoor de betrokkene toestemming heeft gegeven door in te stemmen met de voorwaarden en alle beginselen van de AVG te volgen, bijv. "Minimalisatiebeginsel".
-

Wanneer een betrokkene zijn/haar recht om te worden gewist (recht om te worden vergeten - art. 17 van de AVG) uitoefent, moeten al zijn/haar persoonsgegevens worden gewist uit alle opslagmedia, maar ook uit toepassingen en rapporten waarin ze kunnen worden geïdentificeerd. In bepaalde gevallen kan pseudo-anonimisering (Art. 32°, Art. 25°, andere van de AVG) of anonimisering worden toegepast.

In de specifieke context van de Belgische verkiezingen zijn de principes en verschillende kiesreglementen die moeten worden nageleefd in het kader van de Belgische grondwettelijke principes:

- Alle gegevens, inclusief persoonsgegevens, worden onmiddellijk na de validering van de verkiezingen gewist.
- Het recht om te worden vergeten kan niet afwijken van deze beginselen en verkiezingsregels.
- Dit reglement is dus in overeenstemming met de AVG.

9.4 Technische vereisten

Technical Requirements [TR].

Een "Technische Vereiste" houdt een beperking in op het technische ontwerp van de applicatiecomponenten van de oplossing.

TR001	Web GUI – Graphical User Interface	Prio (Must / Should / Could)
<p>Ergonomische en intuïtieve grafische interface zodat kiezers toegang hebben tot het systeem.</p> <p>Naleving van de <i>look-and-feel</i> die door IBZ is voorgesteld en/of door de andere verkiezingsmodules en de softwarebibliotheek van manipuleerbare objecten (widgets) is vastgesteld. De <i>look-and-feel</i> is een verzameling regels voor de visuele presentatie en het gedrag van grafische interfaces. De presentatieregels hebben met name betrekking op het gebruik van kleuren, typografie, de presentatie en betekenis van logo's en pictogrammen, de presentatie van vensters (locatie, vorm en gedrag van widgets) en cursorvormen. Gedragsregels bepalen hoe visuele elementen reageren op gebruikersacties (muisbewegingen, indrukken van muis- en toetsenbordknoppen).</p> <p>De toepassing van deze regels is bedoeld om het leren te vergemakkelijken en de gebruikerstevredenheid te verbeteren.</p>		
TR002	Gegevensinvoer	Prio (Must / Should / Could)
<p>Het formaat van de gegevensbestanden moet voldoen aan het formaat dat is gedefinieerd en gevalideerd door de inrichtende macht.</p> <p>EML-formaat (Election Markup Language), definitie op Europees niveau van de XML-bestanden (Extensible Markup Language) die voor verkiezingen worden gebruikt.</p>		
TR003	Formaat kieslijsten partijen	Prio (Must / Should / Could)
<p>Het formaat van de lijsten moet zoveel mogelijk overeenkomen met het formaat dat is gedefinieerd en gevalideerd door de inrichtende macht, ter bevordering van de standaardisatie van de interface en de presentatie.</p>		
TR004	IAM – Identity & Access Management	Prio (Must / Should / Could)
<p>Sterk authenticatiesysteem: CSAM (eID en itsme).</p> <p>CSAM is een identiteits- en toegangsbeheersysteem voor e-government en binnen het Europese eIDAS-kader. Het systeem werd opgezet door de Belgische federale overheid. Het systeem maakt identificatie, authenticatie, autorisatie en beheer van mandaten mogelijk. CSAM is een samenwerking tussen de RSZ, het Directoraat-generaal Digitale Transformatie, de FOD Financiën, de Kruispuntbank, de FOD Economie, KMO, Middenstand en Energie en de FOD Binnenlandse Zaken. De eerste overeenkomsten werden ondertekend in 2011, maar het duurde tot 2013 vooraleer het systeem actief werd.</p> <p>Kiezers kunnen zich via CSAM aanmelden met een beveiligingscode, via een authenticatietoepassing, eID of via de itsme-toepassing.</p>		

Inloggen via een token, een beveiligingscode via e-mail of een ander alternatief systeem is ook mogelijk, op voorwaarde dat het beveiligingsniveau vergelijkbaar of hoger is.

Access Repository authenticatiesysteem gebaseerd op:

- De verkiezingslijsten van kiezers ontvangen van de gemeenten voor Belgische kiezers die in België stemmen, van beroepsconsulaire/diplomatieke posten
- De lijst van de andere tussenkomende partijen

Toegangscontrole: er moet een gedetailleerde beschrijving zijn van alle rollen (groepen, privileges, autorisaties) die in het systeem worden gebruikt en de exacte toegangsrechten (functionaliteiten en gegevens) voor elke rol. Een toegangscontrolematrix heeft de voorkeur voor deze regels.

TR005 Integriteit van het stelsysteem Prio (Must / Should / Could)

Alleen de systeemontwerpers, de accreditatieorganisatie, het college van deskundigen en de inrichtende macht hebben toegang tot de niet-gecompileerde en gecompileerde code.

Op verzoek van de verschillende belanghebbenden (die de bevoegdheid hebben om dit verzoek te doen) mag de code worden gepubliceerd, op voorwaarde dat de beveiligingscode wordt verwijderd.

TR006 Beheer van de meertaligheid Prio (Must / Should / Could)

Frans, Nederlands en Duits.

TR007 Audit Trail Prio (Must / Should / Could)

Het is belangrijk om de geladen gegevens te kunnen traceren. Een 'Audit Trail'-functie archiveert de historie van de stromen. Tijdens de uitvoering wordt relevante informatie met betrekking tot de toewijzing van resources en de status van uitgevoerde werkitens vastgelegd in Audit Trails.

TR008 Verwerken van grote datavolumes Prio (Must / Should / Could)

Het datavolume is niet gekoppeld aan de hoeveelheid informatie per kiezer, maar aan het aantal kiezers.

Er zijn Processing Engines van de juiste grootte nodig om parallelle verwerking mogelijk te maken.

TR009 Monitoring, Logging and Alerting Prio (Must / Should / Could)

Het systeem moet worden gemonitord en gebeurtenissen moeten worden gelogd (operationele en beveiligingslogs) in de verschillende onderdelen, van de invoer van gegevens tot de weergave en het gebruik van gegevens in rapporten en dashboards.

Er moet ook een waarschuwingsmechanisme zijn in geval van storingen, gebaseerd op de vooraf gedefinieerde SLA.

TR010 CI/CD – Release Management Prio (Must / Should / Could)

Het concept van CI/CD is een combinatie van de twee praktijken van continue integratie (CI) en continue levering of continue uitrol (CD).

Hoewel het vaak samen wordt gezien, impliceert het ene niet noodzakelijk het andere. CI houdt in dat bij elke wijziging van de code wordt gecontroleerd of er geen regressie is. Het doel is om integratieproblemen zo vroeg mogelijk in het ontwikkelproces te identificeren. Deze praktijk is wenselijk, maar governance in termen van Release Management moet aanwezig zijn.

CD houdt in dat het systeem in zeer korte cycli wordt geproduceerd. Het doel is om heel snel te bouwen, te testen en uit te rollen. Deze praktijk moet worden gecontroleerd in de context van:

- een systeem dat zo cruciaal is als het stelsysteem
- een 'Release Management (Fixed Release)'-logica
- een 'Code Review/Audit'-logica
- de accreditatielogica.

CI is een gewenste praktijk om automatisering tijdens de ontwikkelperiode mogelijk te maken.

Om een beheerst 'Release Management' te bereiken, moet een CI/CD-proces worden gedefinieerd en ondersteund door een set tools.

TR011	Scheduler	Prio (Must / Should / Could)
--------------	------------------	------------------------------

De geautomatiseerde processen moeten geprogrammeerd en gepland worden met behulp van een planner. Deze planner moet het ook mogelijk maken om waarschuwingsmechanismen te definiëren indien nodig.

Bijvoorbeeld: back-ups maken, testen, enz.

TR012	Disaster Recovery Plan (DRP)	Prio (Must / Should / Could)
--------------	-------------------------------------	------------------------------

In het geval van een ramp moet het systeem operationeel zijn in overeenstemming met de SLA, RTO's en RPO's.

Er moet een gedocumenteerd DRP worden opgesteld.

TR013	Back-up en archivering van gegevens	Prio (Must / Should / Could)
--------------	--	------------------------------

Er moet een gegevensback-up worden geïmplementeerd in overeenstemming met de gedefinieerde criteria (zie RTO's en RPO's).

TR014	Back-up van de code en de configuratieparameters	Prio (Must / Should / Could)
--------------	---	------------------------------

Een back-up van de ontwikkelingscodes en systeemconfiguratieparameters moet worden geïmplementeerd op basis van de SLA.

TR015	Code Versioning	Prio (Must / Should / Could)
--------------	------------------------	------------------------------

Er moet een krachtige tool voor het beheer van de codeversies worden geïmplementeerd om:

- De verschillende versies en patches van de code te identificeren
- Een geschiedenis bij te houden van de verschillende versies en patches

Dit systeem is een aanvulling op de tool die certificeert dat de gecompileerde code die in productie wordt genomen (gecertificeerd en goedgekeurd) identiek is aan de code die werd gegenereerd, voor dezelfde versie.

Deze tool garandeert ook dat de broncodecompilatieprocessen tot de verwachte gecompileerde resultaten leiden.

TR016 Gegevensopslag Prio (Must / Should / Could)

Er wordt een algemeen relationeel databasebeheersysteem gebruikt.

TR017 Broncode Prio (Must / Should / Could)

De software heeft een goed gestructureerde broncode en is opgedeeld in modules, zonder functionele overlap.

Elke module biedt een specifieke set functionaliteiten aan. Elke functionaliteit wordt gepresenteerd door slechts één module.

Elke module bevat de nodige uitleg over de werking ervan.

TR018 DTAP-omgevingen Prio (Must / Should / Could)

Er zijn strikt gescheiden omgevingen voor ontwikkeling (D), tests (T), aanvaarding (A), opleiding en productie (P) voorzien.

TR019 Gegevensversleuteling Prio (Must / Should / Could)

De gegevensversleuteling moet het type gegevens specificeren dat geanonimiseerd moet worden, de methode die gebruikt wordt en de tool die gebruikt wordt. Deze software moet recente en publiekelijk geteste algoritmen zonder bekende kwetsbaarheden gebruiken.

TR020 Accreditatie Prio (Must / Should / Could)

De accreditatieorganisatie moet de broncode, configuratieparameters en infrastructuur (App SRV en Storage) valideren.

De accreditatieorganisatie moet het gelijkvormigheidsattest verstrekken.

TR021 Stemcomputer Prio (Must / Should / Could)

De stemcomputer moet de volgende kenmerken hebben:

- De stemcomputer mag niet geheel of gedeeltelijk de broncode van de stemserver bevatten.
- De stemcomputer kan de stemgegevens voor de duur van het stemproces bewaren om een RPO van 0 seconden te garanderen. Zodra de gegevens met succes zijn overgezet naar de server en de kiezer zich heeft afgemeld, worden de gegevens verwijderd. De gegevens worden opgeslagen in het cashgeheugen, niet op de HDD.
- De stemcomputer moet de technische logboeken bijhouden voor de duur van het stemproces. De gegevens worden opgeslagen in een cashgeheugen, niet op de HDD.

Daarnaast moet de stemcomputer aan specifieke veiligheidscriteria voldoen om verbinding te kunnen maken met het stelsysteem.

Deze criteria omvatten:

- Installatie van een VPN dat alleen toegang geeft tot het stelsysteem als kiezer;

-
- Implementatie van een kioskmodus waarbij de kiezer de stemtoepassing niet mag kunnen verlaten;
 - De fysieke toegangen zullen geblokkeerd moeten worden, inclusief USB-poorten, ethernetpoorten, VGA-, DVI- en DisplayPort-poorten. & HDMI, boïtier ... ;
 - De harde schijf zal verplicht gecodeerd moeten zijn;
 - De toegangen vanop afstand tot de stemcomputer zullen geblokkeerd moeten worden;
 - De computer moet up-to-date worden gehouden (bot, browser, enz.) en voorzien zijn van antivirussoftware.

TR022 **Versleuteling van de overgedragen gegevens** Prio (Must / Should / Could)

- De gegevens die worden overgedragen tussen de stemcomputers en de server waarop de oplossing staat, moeten worden versleuteld.
 - De opgeslagen gegevens moeten versleuteld zijn.
-

9.5 Beveiligingsvereisten

Security Requirements [SEC].

Een "Beveiligingsvereiste" houdt een beperking in op het ontwerp van de oplossing die garandeert dat wordt voldaan aan beveiligingskenmerken zoals vertrouwelijkheid, integriteit en beschikbaarheid.

SEC001	Implementeren van een technische en organisatorische oplossing van hoge kwaliteit die geen grote kwetsbaarheden vertoont (kwetsbaarheden die door de uitgever zijn gepubliceerd en/of door derden openbaar zijn gemaakt).	Prio (Must / Should / Could)
<ul style="list-style-type: none">- Gebruikmaken van de laatste ondersteunde en bijgewerkte versies van de besturingssystemen, webserver, encryptieoplossingen en databases die in de oplossing worden gebruikt.- Zich ervan vergewissen dat de nieuwste beveiligingsupdates worden toegepast.- Controleren of de veiligheidslekken in componenten van derden ook zijn gedekt.- Gebruikmaken van openbare encryptieprotocollen en algoritmen die als "sterk" worden beschouwd.		
SEC002	Definiëren van de stem van een kiezer als een atomaire verrichting die bestaat uit de selectie, de validatie, de registratie van het elektronische stembiljet in de elektronische stembus, het tellen van de stemmen en de afgifte van een ontvangstbewijs.	Prio (Must / Should / Could)
<p>Zodra de kiezer zijn of haar stemkeuze definitief heeft gevalideerd, moeten alle bovenstaande verrichtingen zonder onderbreking worden uitgevoerd totdat de laatste verrichting is voltooid. Het mislukken van één actie resulteert in het mislukken van de hele keten en omgekeerd is het succes van de keten alleen mogelijk als elk van de unitaire acties correct wordt uitgevoerd.</p>		
SEC003	Authenticeren van de kiezers door ervoor te zorgen dat de belangrijkste risico's in verband met identiteitsdiefstal aanzienlijk worden verminderd.	Prio (Must / Should / Could)
<p>Kiezers authenticeren zich met behulp van oplossingen voor multifactorauthenticatie. In geval van verlies of diefstal van hun authenticatiemiddel, stelt een procedure de kiezer in staat om te stemmen en maakt deze het verloren of gestolen authenticatiemiddel onbruikbaar.</p>		
SEC004	Zorgen voor strikte vertrouwelijkheid van het elektronische stembiljet zodra dit is aangemaakt op de post van de kiezer.	Prio (Must / Should / Could)
<p>Versleutelen van het elektronische stembiljet op de computer van de kiezer, aan de kantzijde en voordat deze wordt verzonden, met behulp van een openbaar algoritme dat als "sterk" wordt beschouwd.</p>		
SEC005	Zorgen voor strikte vertrouwelijkheid en integriteit van het elektronische stembiljet tijdens het vervoer ervan.	Prio (Must / Should / Could)

Een beveiligd, versleuteld kanaal gebruiken om het elektronische stembiljet, dat zelf al versleuteld is, van de post van de kiezer naar de elektronische stembus te transporteren.

SEC006 Verzekeren van de scheiding van de subnetwerken in functie van de terminals die toegang geven tot de elektronische stembussen Prio (Must) / Should / Could

Zich ervan vergewissen dat het netwerkplan van de oplossing garandeert dat:

- de kiosken
- de controleterminals
- de administratieve terminals
- de stemopnemingsterminals

zich op voorbehouden subnetwerken bevinden.

SEC007 Zich vergewissen van de identificatie van alle terminals Prio (Must) / Should / Could

Zich ervan verzekeren dat het netwerkplan van de oplossing garandeert dat:

- de kiosken
- de controleterminals
- de administratieve terminals
- de stemopnemingsterminals

worden geïnventariseerd op naam, MAC-adres en vast IP-adres. Een dynamische adrestoewijzing (DHCP) is niet toegestaan.

SEC008 Ervoor zorgen dat de identiteit van de kiezer en de uiting van zijn stem volledig gescheiden blijven gedurende de gehele verwerkingsperiode. Prio (Must) / Should / Could

Over geen directe link beschikken tussen de kiezer en het gecodeerde elektronische stembiljet zodra de stem is uitgebracht. Het elektronische stembiljet heeft geen tijdstempel, in tegenstelling tot de presentielijst. Het elektronische stembiljet en de presentielijst worden in afzonderlijke versleutelde opslagruimtes bewaard.

SEC009 Versterken van de vertrouwelijkheid en de integriteit van de gegevens door de geheimhouding te verdelen, waardoor de stemmen opgenomen kunnen worden en de mogelijkheid van een stemopneming vanaf een bepaalde geheimhoudingsdrempel verzekerd wordt. Prio (Must) / Should / Could

Genereren van minimaal drie sleutels en eisen dat minstens twee van deze sleutels onontbeerlijk zijn om de stemopneming mogelijk te maken. Sleutels moeten op een openbare en bekende manier worden gegenereerd en op een veilig medium worden opgeslagen.

SEC010 Definiëren van de stemopneming als een atomaire functie die alleen kan worden gebruikt na het afsluiten van de stemming Prio (Must) / Should / Could

De stemopnemingsoptie mag pas geactiveerd kunnen worden als de stemming afgesloten werd en de digitale of fysieke stembus en de presentielijst verzegeld werden.

Eenmaal geactiveerd mag de stemopnemingsverrichting pas onderbroken worden na de volledige uitvoering en voltooiing ervan.

SEC011	Verzekeren van de integriteit van het systeem, de digitale stembus en de presentielijst	Prio (Must / Should / Could)
---------------	--	------------------------------

Zich ervan vergewissen dat het gebruikte systeem identiek is aan het systeem dat gecontroleerd werd door de onafhankelijke deskundige die de beoordeling heeft uitgevoerd in opdracht van de verwerkingsverantwoordelijke. Er moeten hashwaarden van de elementen door de expert worden berekend en deze moeten op het systeem herberekend kunnen worden om ze te kunnen vergelijken en verifiëren. De stembus en de presentielijst moeten worden verzegeld en er moet een hashwaarde worden berekend zodra deze zijn verzegeld.

SEC012	Zich ervan vergewissen dat de stemopneming van de elektronische stembussen achteraf kan worden geverifieerd.	Prio (Must / Should / Could)
---------------	---	------------------------------

Mogelijkheid om te bewijzen dat de stemopneming foutloos is verlopen. Hiervoor is het nodig om alle elementen te bewaren die nodig zijn om het cryptografische bewijs te verifiëren dat aantoonst dat de stemopneming van de elektronische stembus degene is die de stemmen bevat van de kiezers die hun stem hebben uitgebracht (de kiezers) en alleen deze laatste, en dat deze stemmen correct opgenomen werden.

SEC013	Verzekeren van een automatische controle van de integriteit van het systeem, de elektronische stembus en de kiezerslijst.	Prio (Must / Should / Could)
---------------	--	------------------------------

Met onregelmatige en onvoorspelbare tussenpozen berekenen van een hashwaarde van de bovengenoemde elementen en deze vergelijken met de vooraf berekende referentiewaarde.

SEC014	De transparantie van de elektronische stembus voor alle kiezers waarborgen	Prio (Must / Should / Could)
---------------	---	------------------------------

Kiezers zoveel mogelijk geruststellen dat ze geen toegang hebben tot de expertise van de stemoplossing, wat de goede werking van het systeem en de oprechtheid en integriteit van de stem als geheel garandeert. Het doel is om kiezers in staat te stellen zich ervan te vergewissen dat hun stembiljet in aanmerking is genomen in de elektronische stembus en dat de elektronische stembiljetten correct zijn samengesteld.

Daartoe dient het volgende te worden gedaan:

- Elk stembewijs bevat unieke informatie, volledig ongecorreleerd met de identiteit van de kiezer (digitale hashwaarde, willekeurig getal, "zero-knowledge-proof", enz.), die wordt berekend wanneer de kiezer zijn of haar stemkeuze valideert.
- Het elektronische stemplatform ontvangt de informatie en publiceert deze zodat deze toegankelijk is voor alle kiezers. Kiezers kunnen er dus zeker van zijn dat hun stembiljet daadwerkelijk in de stembus zit.

SEC015	Voorkomen dat het systeem wordt blootgesteld aan bedreigingen voor de cyberveiligheid	Prio (Must / Should / Could)
---------------	--	------------------------------

De architectuur moet de nodige verdedigingsmiddelen implementeren om cyberaanvallen (DDOS, Brute Force, enz.) te voorkomen. Voor WEB-toepassingen moet

ook rekening worden gehouden met de belangrijkste kwetsbaarheden die door OWASP zijn gepubliceerd.

SEC016	Gebruikmaken van een informatiesysteem dat de fysieke en logische beveiligingsmaatregelen implementeert die worden aanbevolen door uitgevers.	Prio (Must / Should / Could)
---------------	--	------------------------------

Toepassen van de best practices in de documentatie van de uitgevers, in het bijzonder de uitgevers van stemoplossingen, alsook de uitgevers van webserver, applicatieservers en database-uitgevers.

SEC017	Ervoor zorgen dat een interventieplan kan worden geactiveerd bij een veiligheidsincident	Prio (Must / Should / Could)
---------------	---	------------------------------

In het geval van een veiligheidsincident moet een interventieplan kunnen worden geïmplementeerd. Dit plan moet regelmatig worden herzien en volledig worden beheerst door alle betrokkenen.

SEC018	Verzekeren van een beheer van de toegangen tot het systeem	Prio (Must / Should / Could)
---------------	---	------------------------------

De toegang tot het systeem en de onderdelen ervan voor bevoorrechte accounts moet worden onderworpen aan:

- Toegangsbeheerproces met validatie door een goedgekeurde manager;
- Goede praktijken die het aantal van dergelijke accounts beperkt tot een maximum van 5 per component (serverbeheerders, databasebeheerders, enz.);
- Niet vrijgeven van wachtwoorden door het installeren van een PAM-component ("Privilege Access Management");
- 'Least Privilege'-principe voor alle geprivilegieerde accounts;
- Periodieke juridische controle;
- Respect voor de scheiding van de taken.

SEC019	Zorgen voor een opvolging van de kwetsbaarheden en patches	Prio (Must / Should / Could)
---------------	---	------------------------------

Er moet voor een opvolging van de kwetsbaarheden gezorgd worden, alsook voor de toepassing van de patches indien beschikbaar. Zo niet, moeten er tegenmaatregelen worden voorgesteld om de kwetsbaarheden te verhelpen.

SEC020	Verzekeren van de opvolging van de versies van het systeem	Prio (Must / Should / Could)
---------------	---	------------------------------

Elke update van het systeem, door ontwikkeling of door het updaten van een component, moet getraceerd worden samen met de gerelateerde wijzigingen. Om de oorsprong en integriteit van een nieuwe versie te garanderen, zal voor een hashing van de binaries worden gezorgd.

SEC021	Zich vergewissen van de dichtheid van de omgevingen	Prio (Must / Should / Could)
---------------	--	------------------------------

De omgevingen die nodig zijn voor ontwikkeling, testen, acceptatie of productie moeten volledig dicht zijn, zonder mogelijke afwijkingen.

SEC022	Controleren van de integriteit van de ontwikkeling	Prio (Must / Should / Could)
---------------	---	------------------------------

De aangeleverde code moet dagelijks gescand worden om de aanwezigheid van kwaadaardige code gedurende de gehele ontwikkelcyclus te voorkomen.

SEC023 Controleren van de integriteit van het systeem Prio (Must / Should / Could)

Het systeem zal regelmatig onderworpen worden aan veiligheidscontroles (Penetration Testing, Access Review, enz.).

SEC024 Definitie van een machtigingsmodel Prio (Must / Should / Could)

Er wordt een machtigingsmodel gedefinieerd waarin rollen en groepen worden gespecificeerd, evenals de bijbehorende rechten en toewijzings-/validatieprocessen, waarbij altijd het 'Least Privilege'-principe wordt gerespecteerd.

SEC025 Logboek van de veiligheidsgebeurtenissen Prio (Must / Should / Could)

De veiligheidsgebeurtenissen worden gecodeerd, opgeslagen en gecategoriseerd. Ze worden zodanig opgeslagen dat hun integriteit gegarandeerd is (alleen lezen). Ze bevatten ten minste:

- Het tijdstip (uitgedrukt in UTC en gebaseerd op een betrouwbare bron);
- Het IP-adres en/of de systeemnaam van de betrokken systemen;
- De identiteit van de gebruiker en/of het systeem;
- Het beveiligingsniveau;
- De details van de gebeurtenis.

De veiligheidslogboeken moeten onafhankelijk van het systeem worden bijgehouden.

SEC026 Scheiding van de taken Prio (Must / Should / Could)

Het machtigingsmodel moet een functiescheidingsmatrix ("Segregation of Duties") specificeren. Het toegangsbeheer moet ervoor zorgen dat deze functiescheidingsregels worden geïmplementeerd.

SEC027 Aanstellen van de verantwoordelijken voor de veiligheid Prio (Must / Should / Could)

Er moeten verantwoordelijken voor de veiligheid, inclusief voor gegevensbescherming, worden aangesteld en kenbaar worden gemaakt in een organigram.

SEC028 Verzekeren van de veiligheid van de hardware Prio (Must / Should / Could)

De apparatuur die door het systeem wordt gebruikt, moet beveiligd zijn en zich in een ruimte bevinden met bewaakte en gecontroleerde fysieke toegang.

SEC029 Verzekeren van de veiligheid van de ontwikkelingscyclus Prio (Must / Should / Could)

De ontwikkelingscyclus (Secure Development Life Cycle) wordt uitgevoerd binnen een veilig en aantoonbaar raamwerk in overeenstemming met modellen zoals het Software Assurance Maturity Model (SAMM) van OWASP.

SEC030 Beperken van de fysieke toegang tot het systeem Prio (Must / Should / Could)

De fysieke toegangen tot de servers moet worden beperkt qua personen en voor een bepaalde periode. Deze zullen goedgekeurd worden door de verantwoordelijke voor de veiligheid en getraceerd worden in een logboek.

9.6 Vereisten buiten het toepassingsgebied

Out of Scope Requirements [OUT].

Een "vereiste buiten het toepassingsgebied" is een zakelijke, functionele, niet-functionele of technische eis waarmee geen rekening wordt gehouden als beperking voor de oplossing. Deze vereisten worden in deze sectie gemeld om te garanderen dat ze werden overwogen en geanalyseerd. Aan deze vereisten moet wel worden voldaan, maar dan buiten de oplossing zelf.

OUT001 Communicatie over de opening van het vooraf stemmen

Het kiosksysteem zorgt niet voor de uitnodigingen, maar de communicatie wordt verzorgd door de inrichtende macht.

OUT002 Registratie voor Belgen die in het buitenland wonen

Belgen die in het buitenland wonen en die willen stemmen, moeten zich registreren voor het kiosksysteem. Ze moeten een PDF-formulier downloaden (dat niet gewijzigd kan worden) van de website van Buitenlandse Zaken en dit terugsturen. De burger ontvangt dan vervolgens per post of e-mail een uitnodiging met uitleg over deze nieuwe stemmethode (procedure).

OUT003 Online ondersteuning voor de kiezers

Het systeem voorziet niet in de creatie van een documentatiegids die toegankelijk is in het systeem, link naar een hotline, helpdesk, implementatie van een ChatBox, enz.

OUT004 Toegankelijkheid van stemlokalen en stembureaus

De organiserende autoriteit is verantwoordelijk voor de toegankelijkheid van de stemlokalen en stembureaus.

OUT005 Ergonomie van het stemhokje

De inrichtende macht is verantwoordelijk voor de ergonomische inrichting van de stemhokjes.

OUT006 Ergonomie van het kiosksysteem

Zoals uitgedrukt in vereiste TR001 "Web GUI – Graphical User Interface", voldoet het kiosksysteem aan de ergonomische behoeften van het grootste aantal kiezers.

Het kiosksysteem biedt geen ondersteuning voor het vervangen van de grafische interface door een steminterface. Het kiosksysteem bevat geen audiosysteem voor het uitwisselen van informatie van het kiosksysteem naar de kiezer en vice versa. Geen computerproces, geen koptelefoon, geen microfoon.

OUT007 Redundantie

- De inrichtende macht is verantwoordelijk voor de redundantie van het elektriciteitsnetwerk.
 - De organiserende autoriteit is verantwoordelijk voor de redundantie van het computernetwerk.
-

OUT008 **Beheer van het stemmen bij volmacht**

Het kiosksysteem voorziet niet in het beheer van het stemmen bij volmacht.

Kiezers kunnen hun stem uitbrengen door een volmacht te geven aan een andere kiezer (artikel 147bis van het Kieswetboek). Op deze manier kan de gevolmachtigde namens de volmachtgever stemmen.

Voortaan is het mogelijk om een volmacht te geven aan een andere kiezer. Een kiezer mag slechts één volmacht hebben. Volmachten kunnen worden gegeven tot de dag van de verkiezingen in de gevallen 1 tot 6 hieronder, en tot de dag voor de dag van de verkiezingen als je op vakantie bent in het buitenland (geval nr. 7).

10 Oplossing

Deze sectie beschrijft het architectuurontwerp van het kiosksysteem.

Ter herinnering, het TOGAF raamwerk en de Archimate-modelleertaal worden gebruikt:

1- De **businesslaag** betreft de bedrijfsprocessen, diensten, functies en gebeurtenissen van de bedrijfsentiteiten. Deze laag biedt producten en diensten aan klanten, die worden gerealiseerd door bedrijfsprocessen die worden uitgevoerd door de verschillende bedrijfsfactoren en -rollen.

2- De **toepassingslaag** betreft de softwaretoepassingen die de onderdelen van het bedrijf en de organisatie ondersteunen met applicatiediensten.

3- De **technologielaag** betreft de hardware- en communicatie-infrastructuur om de applicatielaag te ondersteunen. Deze laag levert de infrastructuurdiensten die nodig zijn om de applicaties uit te voeren, geïmplementeerd door de computer- en communicatiehardware en de systeemsoftware.

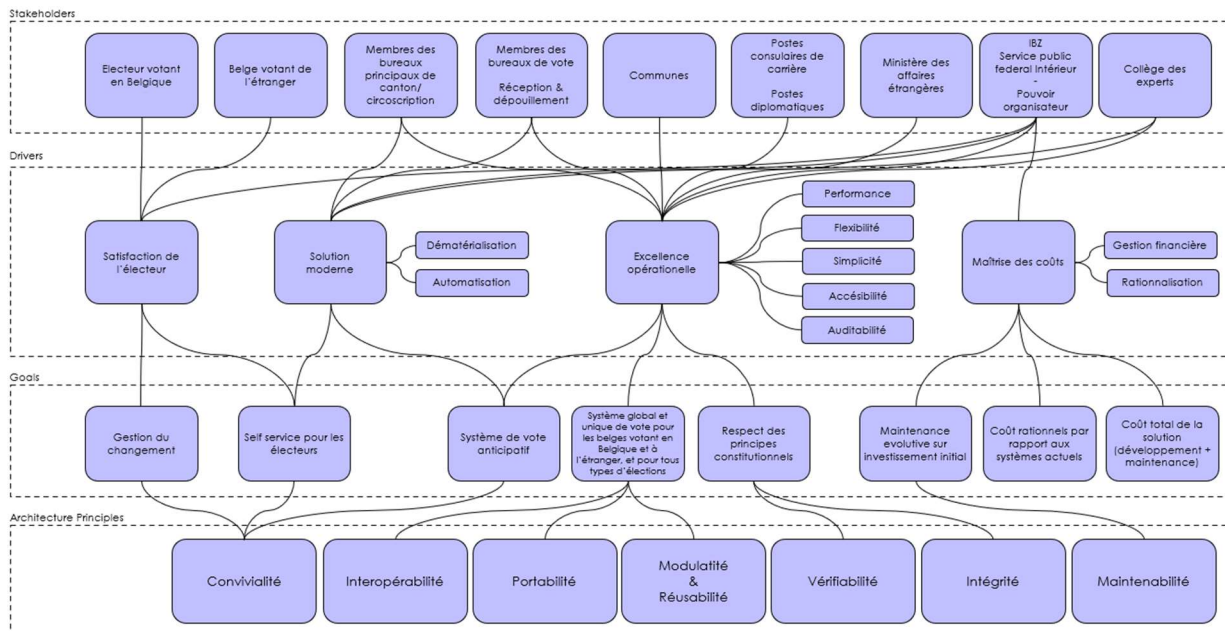
10.1 **Motivatiediagram**

De motivatie behandelt de manier waarop de bedrijfsarchitectuur is afgestemd op de context ten tijde van het ontwerp.

Het motivatiediagram wordt gebruikt om het waarom, de redenen en de motivaties te modelleren die het ontwerp van de bedrijfsarchitectuur hebben geleid en beperkt. Het presenteert alle motivationele elementen, d.w.z. de elementen die de context en de onderliggende motieven leveren. De motivationele elementen werpen licht op de gemaakte ontwerpkeuzes, waardoor we de gemaakte keuzes in een veranderende context kunnen begrijpen.

Het doel van dit diagram is om een volledig of gedeeltelijk overzicht te geven van het motivatieaspect door verschillende elementen met elkaar in verband te brengen:

- **STAKEHOLDERS:** De internationale norm met richtlijnen voor maatschappelijke verantwoordelijkheid, bekend als ISO 26000, definieert een stakeholder als "een individu of groep die een belang heeft bij een beslissing of activiteit van een organisatie".
- **DRIVERS:** Een driver is een externe of interne omstandigheid die een organisatie motiveert om haar doelstellingen te definiëren en de veranderingen door te voeren die nodig zijn om ze te bereiken.
- **GOAL:** Een "Goal" of doel vertegenwoordigt een intentieverklaring op hoog niveau, een gewenste richting of eindtoestand voor een organisatie en haar belanghebbenden.
- **ARCHITECTURE PRINCIPLE:** Een principe vertegenwoordigt een kwalitatieve intentieverklaring waaraan de architectuur moet voldoen.



Stakeholders	Stakeholders
Electeur votant en Belgique	Kiezer die in België stemt
Belge votant de l'étranger	Belg die vanuit het buitenland stemt
Membres des bureaux principaux de canton/circoscription	Leden van de hoofdbureaus van het kanton/de kieskring
Membres des bureaux de vote	Leden van de stembureaus
Réception & dépouillement	Ontvangst en stemopneming
Communes	Gemeenten
Postes consulaires de carrière	Beroepsconsulaire posten
Postes diplomatiques	Diplomatieke posten
Ministère des affaires étrangères	Ministerie van Buitenlandse Zaken
IBZ Service public fédéral Intérieur - Pouvoir organisateur	IBZ Federale Overheidsdienst Binnenlandse Zaken - Inrichtende macht
Collège des experts	College van Deskundigen
Drivers	Drivers

Satisfaction de l'électeur	Tevredenheid van de kiezer
Solution moderne	Moderne oplossing
Dématérialisation	Dematerialisering
Automatisation	Automatisering
Excellence opérationnelle	Operationele uitmuntendheid
Performance	Prestatie
Flexibilité	Flexibiliteit
Simplicité	Eenvoud
Accésibilité	Toegankelijkheid
Auditabilité	Controleerbaarheid
Maîtrise des coûts	Kostenbeheersing
Gestion financière	Financieel beheer
Rationalisation	Rationalisering
Goals	Doelen
Gestion du changement	Beheer van wijzigingen
Self service pour les électeurs	Zelfbediening voor kiezers
Système de vote anticipatif	Systeem om vooraf te stemmen
Système global et unique de vote pour les belges votant en Belgique et à l'étranger, et pour tous types d'élections	Globaal en uniek stelsysteem voor Belgen die stemmen in België en in het buitenland, en voor alle soorten verkiezingen
Respect des principes constitutionnels	Naleving van de Belgische grondwettelijke principes
Maintenance évolutive sur investissement initial	Evolutief onderhoud op initiële investering
Coût rationnels par rapport aux systèmes actuels	Rationele kosten in vergelijking met huidige systemen
Coût total de la solution (développement + maintenance)	Totale kostprijs van de oplossing (ontwikkeling + onderhoud)
Architecture Principes	Architectuurprincipes
Convivialité	Gebruiksvriendelijkheid
Interopérabilité	Interoperabiliteit
Portabilité	Overdraagbaarheid
Modularité & Réusabilité	Modulariteit en herbruikbaarheid
Vérifiabilité	Controleerbaarheid
Intégrité	Integriteit
Maintenabilité	Onderhoudbaarheid

Drivers:

- TEVREDENHEID van de kiezer: In een context waarin meerdere stelsystemen beschikbaar zijn voor de kiezer, moet het kiosksysteem een positieve gebruikerservaring bieden, anders zal de kiezer zich wenden tot de andere systemen.
- MODERNE OPLOSSING: In een context waarin het verbruik van natuurlijke hulpbronnen wordt gerationaliseerd en digitalisering zich uitbreidt naar alle activiteiten in onze

samenlevingen, is stemmen met een kiosk een oplossing voor deze uitdagingen. De automatisering van stemprocessen maakt deel uit van dit rationaliseringsproces en wordt mogelijk gemaakt door de digitalisering van stemmedia.

- OPERATIONELE UITMUNTENDHEID: De organiserende autoriteit heeft haar wens geuit om de stemoperaties te verbeteren: meer flexibiliteit, eenvoudigere processen, betere toegang tot stemapparatuur en meer controleerbaarheid om transparantie en democratische controle te garanderen.
- KOSTENBEHEERSING: Rationalisatie maakt het mogelijk om de beste oplossing te vinden, in overeenstemming met de vereisten, in verhouding tot de gedane investering, door het toepassen van de beste praktijken in financieel beheer en kostenbeheersing.

Goals:

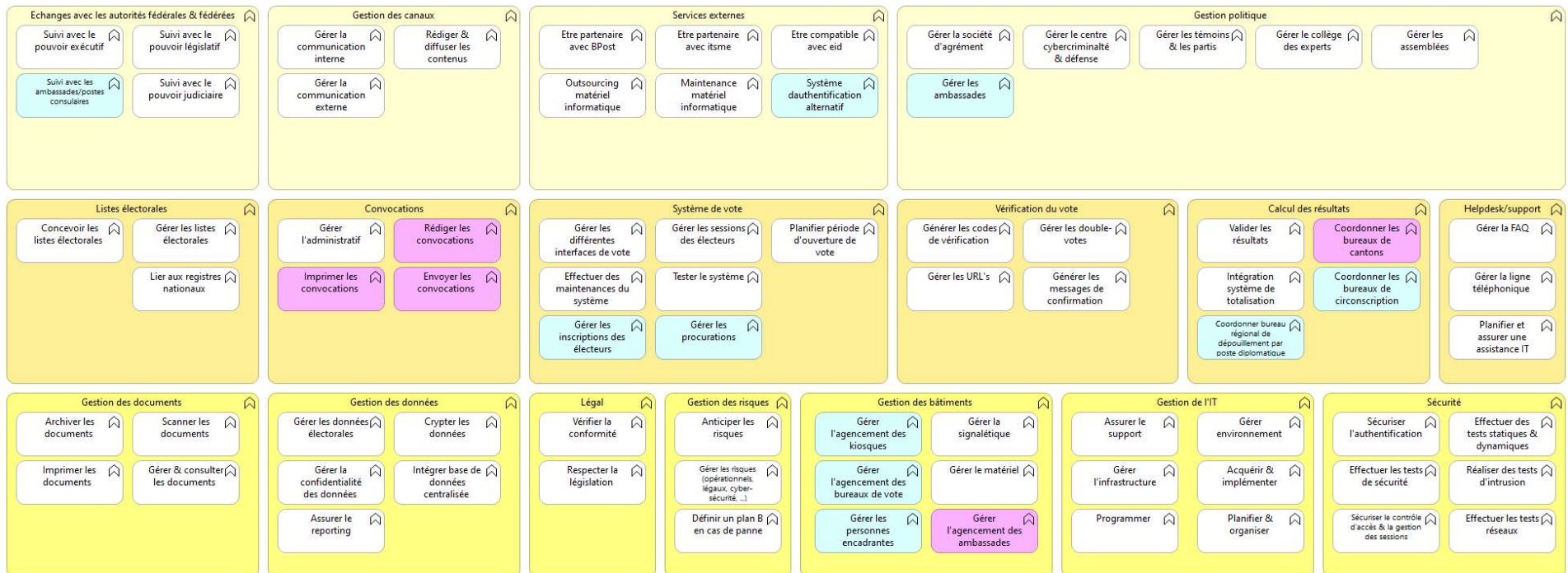
- VERANDERINGSBEHEER: Essentieel element voor het succes van de oplossing. Een perfecte oplossing is een mislukking als ze niet wordt gebruikt. Dit betekent niet alleen communiceren, inspireren en opleiden van burgers, maar ook van belanghebbenden zoals lokale autoriteiten, leden van het kiesbureau, enz.
- SELF-SERVICE voor kiezers: Ervoor zorgen dat kiezers meer betrokken zijn bij het democratische leven van hun samenleving en in een vroeger stadium deelnemen aan het stemproces. Dit vergroot het vertrouwen van de burgers in het stemmechanisme. Het ontlast ook de inrichtende macht van een aantal taken.
- ANTICIPATIEF STEMSYSTEEM: De stemperiode van het kiosksysteem voor het stemmen in België is niet beperkt tot de dag van de stemming. Dit stelt burgers in staat zich te organiseren om te kunnen stemmen en is een factor in de strijd tegen de dalende opkomst van burgers die gaan stemmen. Vooraf stemmen geldt niet voor Belgen die in het buitenland stemmen.
- GLOBAAL EN UNIEK SYSTEEM: Het kiosksysteem moet zowel kiezers in België als Belgen in het buitenland bereiken. Het kiosksysteem moet de Europese, federale en regionale verkiezingen dekken. Eén enkel systeem zal niet alleen zorgen voor meer consistentie en operationele controle, maar ook voor een betere gebruikerservaring en financiële controle.
- RESPECT VOOR CONSTITUTIONELE PRINCIPES: Dit zijn sine qua non voorwaarden, fundamentele beperkingen, zonder welke het kiosksysteem niet kan worden geïmplementeerd.
- EVOLUTIEF ONDERHOUD: De investering in het kiosksysteem wordt gerechtvaardigd door het feit dat het open is. Elke nieuwe functionaliteit moet worden geïmplementeerd op het kiosksysteem zonder de oplossing volledig te herzien. Dit garandeert het rationele karakter van de investering: initiële investering voor een operationeel systeem, en indien nodig, verdere investering voor bijkomende functionaliteiten.

- RATIONELE KOSTEN vergeleken met die van huidige systemen: Met het oog op het rationaliseren van de kosten moet het kiosksysteem een financieel voordeel bieden en een lagere Total Cost of Ownership (TCO) hebben dan de huidige systemen.
- TOTALE KOSTPRIJS van de oplossing: $TCO = CAPEX + OPEX$. Het gaat hier om de globale kostprijs van het systeem, bestaande uit de initiële investering voor het ontwikkelen, testen en implementeren van het systeem (CAPEX), evenals de operationele kosten over meerdere jaren (OPEX).

Architectuurprincipes:

- GEBRUIKSVRIENDELIJKHEID: De oplossing moet bruikbaar zijn voor burgers die geen specifieke opleiding hebben genoten.
- INTEROPERABILITEIT: De oplossing moet verbinding kunnen maken met andere systemen om gegevens uit te wisselen (kiezerslijsten, partijlijsten, kandidatenlijsten, enz.).
- OVERDRAAGBAARHEID: *Vendor Locking* en *Technology Locking* moeten vermeden worden. De oplossing, de software, moet op verschillende platformen en machines kunnen draaien.
- MODULARITEIT & HERBRUIKBAARHEID: De oplossing moet bestaan uit specifieke functionele modules die onafhankelijk van elkaar kunnen evolueren, terwijl de soepele werking van de oplossing als geheel gewaarborgd blijft. Het systeem moet kunnen worden hergebruikt in:
 - o Een versie-upgrade van de oplossing (identiek functioneel bereik)
 - o Een functionele upgrade van de oplossing
- CONTROLEERBAARHEID: Het systeem moet betrouwbaar zijn (in termen van beveiligingsbeheer en correcte afhandeling van operationele problemen) en deze betrouwbaarheid moet worden beoordeeld.
- INTEGRITEIT: De oplossing moet zeer veilig zijn, met een sterke controle over de toegang tot functies en gegevens.
- HANDHAAFBAARHEID: Het moet mogelijk zijn om de oplossing te corrigeren en aan te passen als onderdeel van een continu verbeteringsproces. Dit principe garandeert een zekere mate van efficiëntie in de kostenbeheersing.

10.2 Bedrijfsarchitectuur (Business Layer)



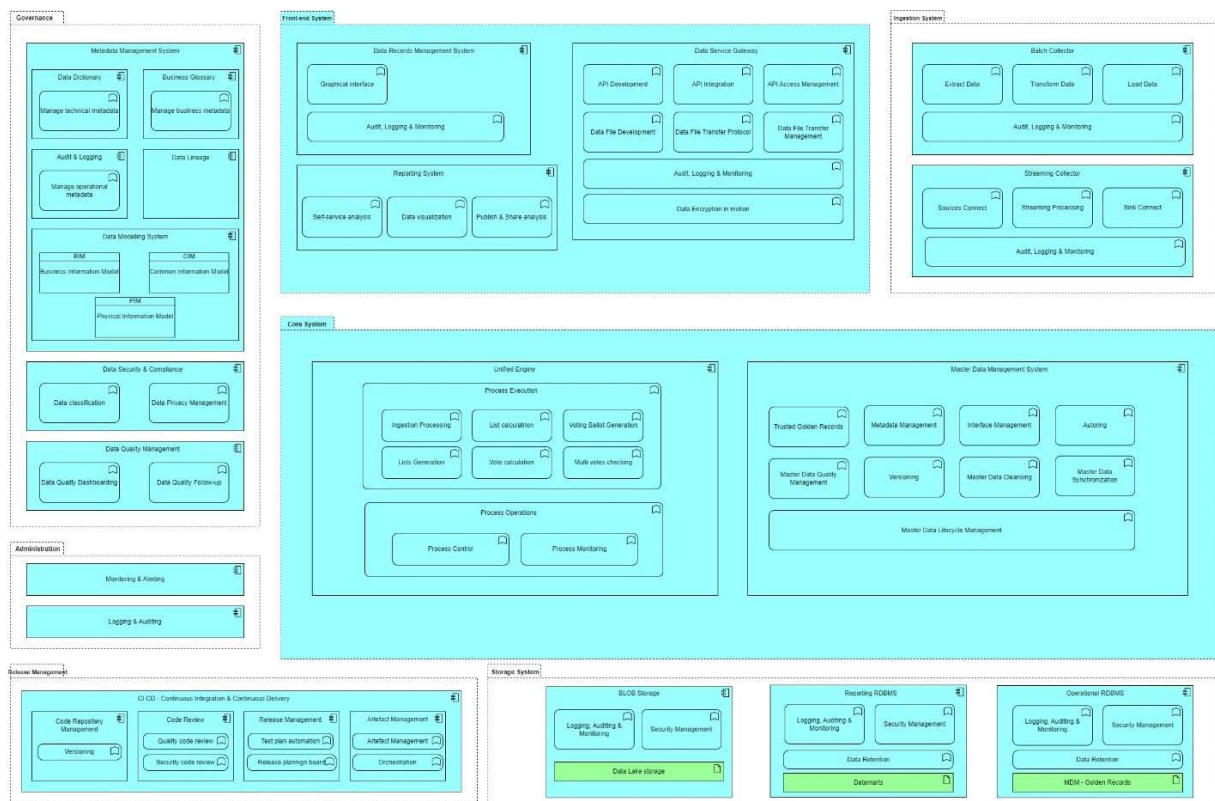
Echanges avec les autorités	Uitwisselingen met de autoriteiten
Suivi avec le pouvoir exécutif	Opvolging met de uitvoerende macht
Suivi avec les postes consulaires de carrières/postes diplomatiques	Opvolging met de beroepsconsulaire posten/diplomatieke posten
Suivi avec le pouvoir législatif	Opvolging met de wetgevende macht
Suivi avec le pouvoir judiciaire	Opvolging met de rechterlijke macht
Listes électorales	Kieslijsten
Concevoir les listes électorales	Opstellen van de kieslijsten
Lier aux registres nationaux	Koppelen aan de rijksregisters
Gérer les listes électorales	Beheren van de kieslijsten
Gestion des documents	Beheer van de documenten
Archiver les documents	Archiveren van de documenten
Imprimer les documents	Afdrukken van de documenten
Scanner les documents	Scannen van de documenten
Gérer & consulter les documents	Beheren en raadplegen van de documenten
Gestion des canaux	Beheer van de kanalen
Gérer la communication interne	Beheren van de interne communicatie
Gérer la communication externe	Beheren van de externe communicatie
Rédiger et diffuser les contenus	Opstellen en verspreiden van de inhoud
Convocations	Oproepingsbrieven
Gérer l'administratif	Beheren van de administratie
Rédiger les convocations	Opstellen van de oproepingsbrieven
Imprimer les convocations	Afdrukken van de oproepingsbrieven
Gérer les doubles enveloppes	Beheren van de dubbele omslagen
Envoyer les convocations	Versturen van de oproepingsbrieven
Gestion des données	Gegevensbeheer
Gérer les données électorales	Beheren van de verkiezingsgegevens
Gérer la confidentialité des données	Beheren van de vertrouwelijkheid van de gegevens
Assurer le reporting	Verzekeren van de rapportering
Crypter les données	Versleutelen van de gegevens
Intégrer base de données centralisée	Integreren van de gecentraliseerde gegevens
Services externes	Externe diensten
Etre partenaire avec itsme	Samenwerken met itsme
Système authentification faible	Zwak verificatiesysteem
Etre compatible avec eID	Compatibel zijn met eID
Etre partenaire avec Bpost	Samenwerken met bpost
Système de vote	Stemsysteem
Gérer les différentes interfaces de vote	Beheren van de verschillende steminterfaces
Effectuer des maintenances du système	Uitvoeren van het systeemonderhoud
Gérer les procurations	Beheren van de volmachten
Gérer les sessions des électeurs	Beheren van de kiezerssessies
Tester le système	Testen van het systeem
Gérer les inscriptions des électeurs	Beheren van de kiezersregistraties
Planifier la période d'ouverture des votes	Plannen van de periode van openstelling van de stemming
Légal	Wettelijk

Vérifier la conformité	Controleren van de conformiteit
Respecter la législation	Naleven van de wetgeving
Gestion des risques	Risicobeheer
Anticiper les risques	Anticiperen op risico's
Gérer les risques (opérationnels, légaux, cyber-sécurité, ...)	Beheren van de risico's (operationeel, juridisch, cybersecurity, enz.)
Gestion des bâtiments	Beheer van de gebouwen
Gérer la signalétique	Beheren van de bewegwijzering
Gérer le matériel	Beheren van het materieel
Gérer l'agencement des postes consulaires de carrières/postes	Beheren van de indeling van de beroepsconsulaire posten/posten
Gestion politique	Politiek beheer
Gérer la société d'agrément	Beheren van de accreditatieorganisatie
Centre de cybercriminalité & de défense	Cybercriminaliteits- en defensiecentrum
Gérer les témoins & les partis	Beheren van de getuigen en de partijen
Gérer le collège des experts	Beheren van het College van Deskundigen
Gérer les assemblées	Beheren van de parlementen
Vérification du vote	Verificatie van de stemming
Gérer les doubles-votes	Beheren van de dubbele stemmen
Gérer les URL's	Beheren van de URL's
Générer les codes de vérification "K"	Genereren van de 'K'-verificatiecodes
Calcul des résultats	Berekening van de resultaten
Valider les résultats	Valideren van de resultaten
Intégration système de totalisation	Integratie totaliseringssysteem
Réceptionner les bulletins	Ontvangen van de stembiljetten
Encoder les résultats	Invoeren van de resultaten
Répertorier les votes (pointages)	Inventariseren van de stemmen (aanstippen)
Coordonner les bureaux de réception/dépouillement	Coördineren van de ontvangst-/stemopnemingsbureaus
Helpdesk/support	Helpdesk/support
Gérer la FAQ	Beheren van de FAQ's
Gérer la hotline	Beheren van de hotline
Gestion de l'IT	Beheer van de IT
Assurer le support	Verzekeren van de ondersteuning
Gérer l'infrastructure	Beheren van de infrastructuur
Coder	Invoeren
Gérer l'environnement	Beheren van de omgeving
Acquérir & implémenter	Verwerven en implementeren
Planifier & organiser	Plannen en organiseren
Sécurité	Veiligheid
Sécuriser l'authentification	Beveiligen van de authenticatie
Effectuer les tests de sécurité	Uitvoeren van de veiligheidstests
Sécuriser le contrôle d'accès	Beveiligen van de toegangscontrole
Effectuer des tests statiques & dynamiques	Uitvoeren van de statische en dynamische tests
Réaliser des tests d'intrusion	Uitvoeren van de inbraaktests
Sécuriser la gestion des sessions	Beveiligen van het beheer van de sessies
Effectuer des tests de pénétration	Uitvoeren van de penetratietests

10.3 Functionele toepassingsarchitectuur (Application Layer)

De bedrijfsarchitectuur wordt gedefinieerd en de functionele vereisten worden gevalideerd. De toepassingsmodellen moeten worden geïdentificeerd door de referentiearchitectuur voor de applicatie te selecteren. Deze toepassingsmodellen moeten voldoen aan de vereisten en de bedrijfsarchitectuur ondersteunen.

De toepassingsarchitectuur is gebaseerd op de elementen van de Archimate-applicatie, een gemeenschappelijke taal die door architecten wordt gebruikt om de verschillende visies op de architectuur weer te geven. De volledige lijst en een korte uitleg van elk Archimate-applicatie-element werd toegevoegd als bijlage.



Sommige applicaties zullen absoluut geïmplementeerd moeten worden in de oplossing.

- **MUST** = De oplossing kan niet functioneel zijn zonder dat de toepassing is geïmplementeerd. MVP (Minimum Viable Product).
- **SHOULD** = De oplossing kan functioneel zijn in een eerste versie zonder dat de toepassing wordt geïmplementeerd, zolang de toepassing wordt opgenomen in een toekomstige versie.
- **COULD** = Dit is een "nice to have", het niet implementeren van deze toepassing is geen blokkerend punt voor de aanvaarding.

Governance

Voor het governance-gedeelte hebben we applicaties nodig om het volgende te handhaven:

- Gegevenswoordenboek
 - **MUST**
 - Aangezien het systeem gegevens moet beheren met een specifieke classificatie (bijv. vertrouwelijkheid) en ook informatie moet produceren voor belanghebbenden, is het essentieel om een middel te hebben om deze gegevens op een optimale manier te verzamelen en te onderhouden. Het gegevenswoordenboek wordt gebruikt om de structuur en inhoud van de gegevens te catalogiseren en te communiceren, en biedt zinvolle beschrijvingen voor afzonderlijk benoemde gegevensobjecten.
- Bedrijfswoordenlijst
 - **MUST**
 - Naast het gegevenswoordenboek kan het beheer van bedrijfstermen worden vergemakkelijkt door een bedrijfswoordenlijst. Ter herinnering: het gegevenswoordenboek beschrijft technische metadata en de bedrijfswoordenlijst beheert bedrijfsmetadata. Dus, om hetzelfde zakelijke begrip van de gegevens te hebben en de link te leggen tussen het bedrijfsconcept en de verschillende representaties ervan in de technische gegevens, kan de bedrijfswoordenlijst deze leemte opvullen. In een perfecte wereld komt de semantische laag die wordt toegepast op de belanghebbenden van de gegevens uit de bedrijfswoordenlijst.
- Data Lineage
 - **MUST**
 - Het is verplicht om het door de gegevens afgelegde traject te kennen, van het punt van binnenkomst tot de verschillende toepassingen ervan. Dit maakt het ook mogelijk om impactanalyses uit te voeren in het geval van een verandering in de gegevensbron.
- Audit & Logging
 - **MUST**
 - Nodig om te voldoen aan de beveiligingsvereisten in verband met de stemming.
- Systeem voor gegevensmodellering
 - **MUST**
 - Dit moet de functionele en technische analyse ondersteunen door conceptuele, logische en fysieke datamodellen op één plaats te creëren en gemakkelijk met iedereen te delen.

- Beheer van de gegevenskwaliteit
 - **MUST**
 - De kwaliteit van de gegevens moet beheerd worden op bronniveau. Maar als we betrouwbare informatie voor processen en rapporten willen hebben, moeten kwaliteitsindicatoren beschikbaar zijn voor zakelijke eindgebruikers.

Frontendsystemen

Voor het frontendsysteem dat we uiteenzetten aan de eindgebruikers, hebben we voornamelijk de volgende elementen nodig:

- Rapportagesysteem
 - **MUST**
 - De 'Business Intelligence'-platformen (BI) bieden mogelijkheden in drie categorieën:
 - Analyse, zoals online analytische verwerking (OLAP) en de zelfbedieningselementen;
 - Informatieverspreiding, zoals rapporten en dashboards;
 - Visualisatie van gegevens.

Invoersysteem

Hoe worden gegevens vanuit externe bronnen in het systeem ingevoerd? Het invoersysteem komt hieraan tegemoet door het volgende mogelijk te maken:

- Batchverzamelaar
 - **MUST**
 - Het invoermechanisme zal gedeeltelijk batchgeoriënteerd zijn, waarbij de batchverzamelaar over het algemeen snapshots of delta's vanuit bronsystemen verzamelt. Dit zal de rol zijn van de ETL-applicatie.
- Berichtenverzamelaar
 - **MUST**
 - Het invoermechanisme zal gedeeltelijk berichtgeoriënteerd zijn, waarbij de 'event'-verzamelaar over het algemeen onmiddellijke acties verzamelt (keuzes van de kiezers) wanneer deze worden uitgevoerd.

Opslagsysteem

De gegevens (bronnen en doelen) zullen voornamelijk worden opgeslagen in de vorm van:

- Operational RDBMS en BLOB-opslag
 - **MUST**
 - Deze opslagelementen wordt voornamelijk gebruikt om 'RAW' gegevens op te slaan (gestructureerd in een operationeel RDBMS en semi-/ongestructureerd in BLOB) die door de verzamelaars uit de bronsystemen worden opgenomen en opgeslagen voor latere verwerking en transformatie.

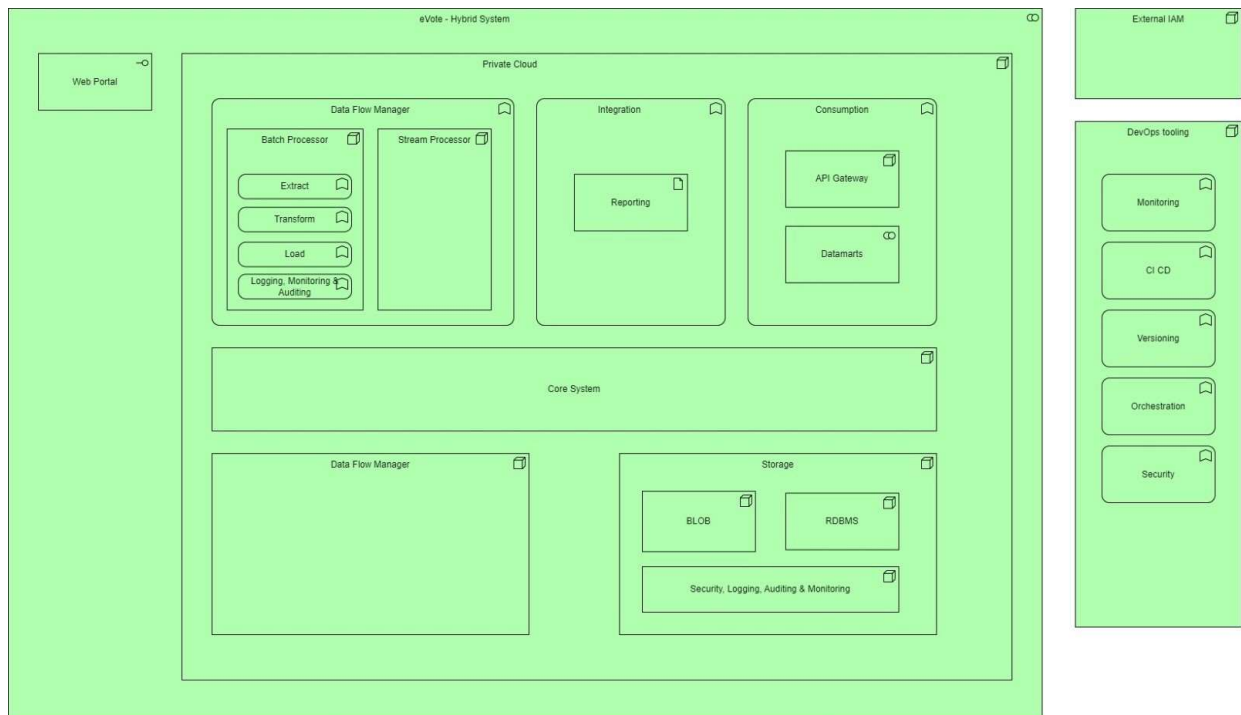
- Reporting RDBMS
 - **MUST**
 - Noodzaak van een gedistribueerd datawarehousesysteem dat fouttolerant is en het verrichten van analyses mogelijk maakt. Ter herinnering: een datawarehouse biedt een centrale opslagplaats van informatie die eenvoudig kan worden geanalyseerd om rapporten en dashboards te creëren.

Release Management

Dit onderdeel gaat voornamelijk over de manier waarop we de 'continue integratie'- en 'continue levering'-functionaliteiten gaan implementeren, ook wel bekend als het DEVOPS-gedeelte.

- Code Repository Management
 - **MUST**
 - Dit onderdeel betreft de continue integratie van nieuwe stukken code die gegevensverwerking en transformaties vertegenwoordigen. Het beheert de verschillende versies van de code en de manier waarop deze worden geïntegreerd in het programma als geheel.
- Artefact Repository
 - **MUST**
 - Met een Artefact Repository kan je Release Pipeline geversioneerde artefacten en hun afhankelijkheden publiceren en ophalen met behulp van centrale referentiekaders die toegankelijk zijn vanuit andere omgevingen. Het artefact kan bestaan uit project broncode, afhankelijkheden, binaries of resources, en kan in verschillende vormen worden weergegeven afhankelijk van de technologie.
- Release Management
 - **MUST**
 - We hebben een applicatie nodig voor Release Management. Met toegang tot de Artefact Repository consumeert een Release Pipeline de artefacten en voert vervolgcacties uit binnen een multi-environment platform.

10.4 Technische architectuur (Technology Layer)



10.5 SWOT



Au lancement d'un produit ou d'un service, une analyse **SWOT** (**strenghts**, **weaknesses**, **opportunities**, **threats**) permet de mettre en évidence les forces et opportunités sur lesquelles s'appuyer, mais également les menaces et faiblesses dont il faudra tenir compte.

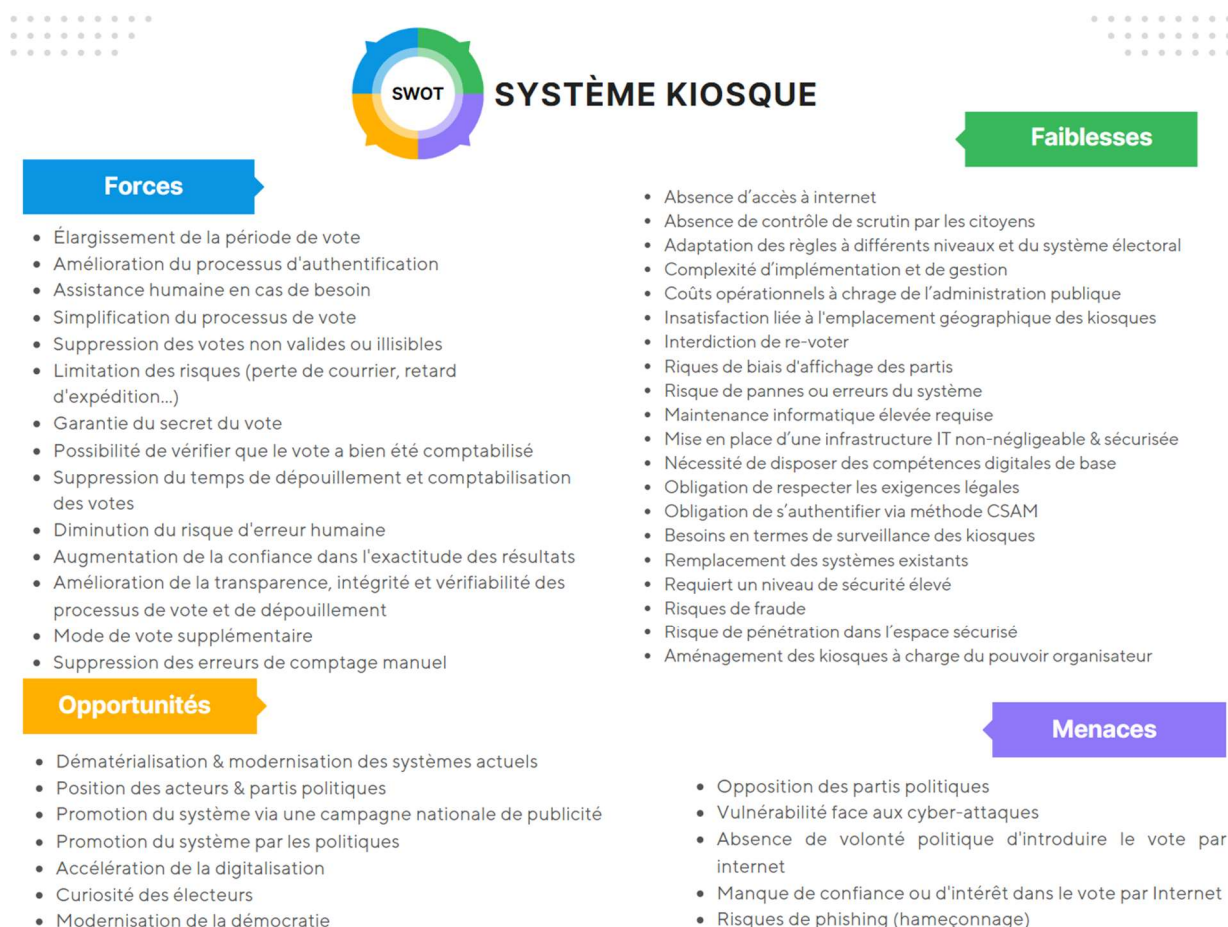
Dans notre cas, cette analyse nous permet de comparer les trois systèmes et de les analyser avec plus de recul.



SWOT	SWOT
Au lancement d'un produit ou d'un service, une analyse SWOT (strenghts , weaknesses , opportunities , threats) permet de mettre en évidence les forces et opportunités sur lesquelles s'appuyer, mais également les menaces et faiblesses dont il faudra tenir compte.	Wanneer een product of een dienst gelanceerd wordt, geeft een SWOT -analyse (' Strenghts ' (sterktes), ' Weaknesses ' (zwaktes), ' Opportunities ' (kansen), ' Threats ' (bedreigingen)) aan op welke sterktes en kansen kan worden voortgebouwd, maar ook met welke bedreigingen en zwaktes rekening moet worden gehouden.
Dans notre cas, cette analyse nous permet de comparer les trois systèmes et de les analyser avec plus de recul.	In ons geval stelt deze analyse ons in staat om de drie systemen te vergelijken en vanuit een breder perspectief te analyseren.
S	S
Forces	Sterktes
W	W
Faiblesses	Zwaktes
O	O
Opportunités	Kansen
T	T

Menaces	Bedreigingen
Les forces & faiblesses sont des choses internes à l'organisation et sur lesquelles celle-ci a une marge de manoeuvre.	Sterktes en zwaktes zijn zaken die binnen de organisatie liggen en waarover de organisatie manoeuvreerruimte heeft.
Kansen en bedreigingen zijn zaken die buiten de organisatie liggen en waarover ze geen manoeuvreerruimte heeft.	Kansen en bedreigingen zijn zaken die buiten de organisatie liggen en waarover ze geen manoeuvreerruimte heeft.

10.5.1 SWOT Business



10.5.2 Technische SWOT



SWOT TECHNIQUE



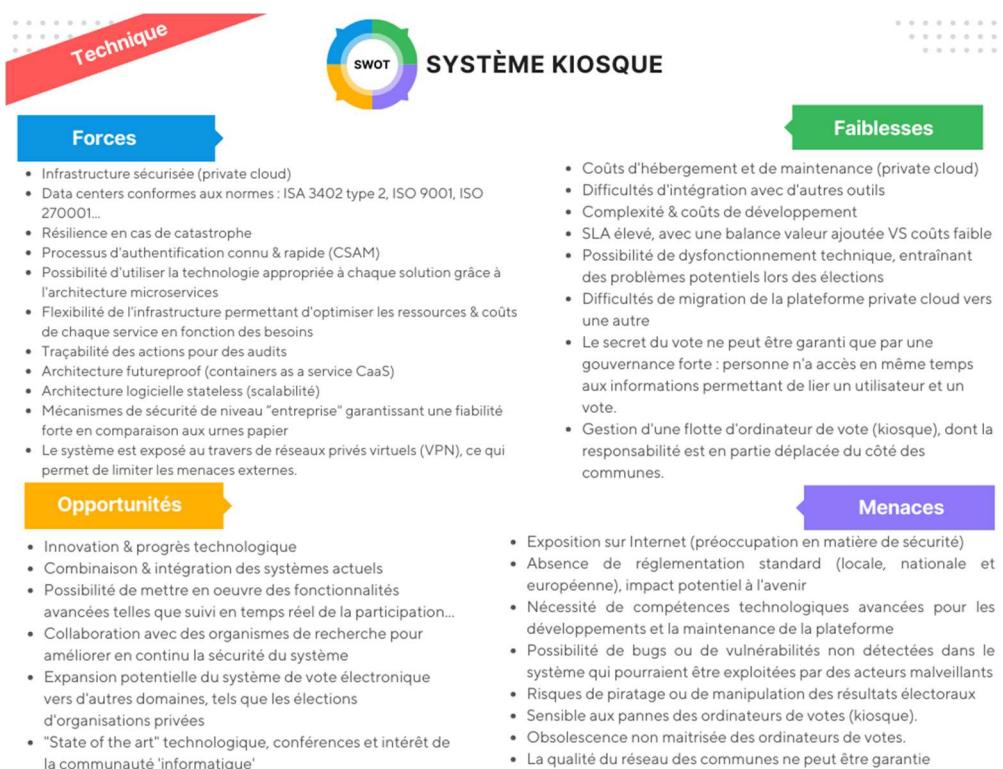
Au lancement d'un produit ou d'un service, une analyse **SWOT** (**strengths**, **weaknesses**, **opportunities**, **threats**) permet de mettre en évidence les forces et opportunités sur lesquelles s'appuyer, mais également les menaces et faiblesses dont il faudra tenir compte.

Dans notre cas, cette analyse nous permet de comparer les trois systèmes et de les analyser avec plus de recul.



SWOT	SWOT
SWOT TECHNIQUE	TECHNISCHE SWOT
Au lancement d'un produit ou d'un service, une analyse SWOT (strengths , weaknesses , opportunities , threats) permet de mettre en évidence les forces et opportunités sur lesquelles s'appuyer, mais également les menaces et faiblesses dont il faudra tenir compte.	Wanneer een product of een dienst gelanceerd wordt, geeft een SWOT -analyse (' Strengths ' (sterktes), ' Weaknesses ' (zwaktes), ' Opportunities ' (kansen), ' Threats ' (bedreigingen)) aan op welke sterktes en kansen kan worden voortgebouwd, maar ook met welke bedreigingen en zwaktes rekening moet worden gehouden.
Les opportunités & menaces sont des choses externes à l'organisation et sur lesquelles celle-ci n'a pas de marge de manoeuvre.	Kansen & bedreigingen zijn zaken die buiten de organisatie liggen en waarover ze geen manoeuvreerruimte heeft.

Les forces & faiblesses sont des choses internes à l'organisation et sur lesquelles celle-ci a une marge de manœuvre.	Sterktes & zwaktes zijn zaken die binnen de organisatie liggen en waarover de organisatie manoeuvreerruimte heeft.
Forces	Sterktes
Opportunités	Kansen
Faiblesses	Zwaktes
Menaces	Bedreigingen



Technique	Technisch
SWOT	SWOT
SYSTÈME KIOSQUE	KIOSKSYSTEEM
Forces	Sterktes
Infrastructure sécurisée (private cloud)	Beveiligde infrastructuur (private cloud)
Data centers conformes aux normes: ISA 3402 type 2, ISO 9001, ISO 270001...	Datacenters die voldoen aan normen: ISA 3402 type 2, ISO 9001, ISO 270001, enz.
Résilience en cas de catastrophe	Veerkracht in geval van een ramp
Processus d'authentification connu & rapide (CSAM)	Bekend en snel authenticatieproces (CSAM)
Possibilité d'utiliser la technologie appropriée à chaque solution grâce à l'architecture microservices	Mogelijkheid om voor elke oplossing de juiste technologie te gebruiken dankzij de microservices-architectuur

Flexibilité de l'infrastructure permettant d'optimiser les ressources & coûts de chaque service en fonction des besoins	Flexibiliteit van de infrastructuur om de middelen en kosten van elke dienst te optimaliseren in functie van de behoeften
Traçabilité des actions pour des audits	Traceerbaarheid van de acties voor audits
Architecture futureproof (containers as a service CaaS)	Toekomstbestendige architectuur (containers als service CaaS)
Architecture logicielle stateless (scalabilité)	Stateless softwarearchitectuur (schaalbaarheid)
Mécanismes de sécurité de niveau "entreprise" garantissant une fiabilité forte en comparaison aux urnes papier	Beveiligingsmechanismen op "ondernemingsniveau" die een hoge mate van betrouwbaarheid garanderen in vergelijking met papieren stembussen
Le système est exposé via des réseaux privés virtuels (VPN), ce qui permet de limiter les menaces externes.	Het systeem is blootgesteld via virtuele privénetwerken (VPN), wat de bedreigingen van buitenaf beperkt.
Opportunités	Kansen
Innovation & progrès technologique	Innovatie en technologische vooruitgang
Combinaison & intégration des systèmes actuels	Combinatie en integratie van de huidige systemen
Possibilité de mettre en œuvre des fonctionnalités avancées telles que suivi en temps réel de la participation...	Mogelijkheid om geavanceerde functionaliteiten te implementeren zoals real-time monitoring van de opkomst, ...
Collaboration avec des organismes de recherche pour améliorer en continu la sécurité du système	Samenwerking met onderzoeksinstituten om de veiligheid van het systeem continu te verbeteren
Expansion potentielle du système de vote électronique vers d'autres domaines, tels que les élections internes des grandes entreprises	Potentiële uitbreiding van het e-votingsysteem naar andere domeinen, zoals interne verkiezingen voor grote ondernemingen
"State of the art" technologique, conférences et intérêt de la communauté internationale.	"State of the art" technologie, conferenties en belangstelling van de internationale gemeenschap
Faiblesses	Zwaktes
Coûts d'hébergement et de maintenance (private cloud)	Hosting- en onderhoudskosten (private cloud)
Difficultés d'intégration avec d'autres outils	Moeilijkheden met integratie met andere tools
Complexité & coûts de développement	Complexiteit en ontwikkelingskosten
SLA élevé, avec une balance valeur ajoutée VS coût faible	Hoge SLA, met een geringe toegevoegde waarde in vergelijking met de kosten
Possibilité de dysfonctionnement technique, entraînant des problèmes potentiels lors des élections	Mogelijkheid van technische storing, wat tot potentiële problemen tijdens de verkiezingen kan leiden
Difficulté de migration de la plateforme private cloud vers une autre	Moeilijkheid om van een 'private cloud'-platform naar een ander te migreren
Le secret du vote ne peut être garanti que par une gouvernance forte : personne n'a accès en même temps aux informations permettant de lier un utilisateur et un vote.	Het stemgeheim kan alleen worden gegarandeerd door een sterke governance: niemand heeft gelijktijdig toegang tot de informatie die een gebruiker en een stem met elkaar verbindt.

Gestion d'une flotte d'ordinateur de vote (kiosque), dont la responsabilité est en partie déplacée du côté des communes.	Beheer van een vloot stemcomputers (kiosken), waarvoor de verantwoordelijkheid gedeeltelijk is overgedragen aan de gemeenten.
Menaces	Bedreigingen
Exposition sur Internet (préoccupation en matière de sécurité)	Blootstelling aan het internet (veiligheidsrisico's)
Absence de réglementation standard (locale, nationale et européenne), impact potentiel à l'avenir	Geen standaard regelgeving (lokaal, nationaal en Europees), potentiële impact in de toekomst
Nécessité de compétences technologiques avancées pour les développements et la maintenance de la plateforme	Behoeftte aan geavanceerde technologische competenties om het platform te ontwikkelen en te onderhouden
Possibilité de bugs ou de vulnérabilités non détectées dans le système qui pourraient être exploitées par des acteurs malveillants	Mogelijkheid van bugs of onopgemerkte kwetsbaarheden in het systeem die kunnen worden uitgebuit door kwaadwillenden
Risques de piratage ou de manipulation des résultats électoraux (sensible aux pannes des ordinateurs de vote kiosque)	Risico op hacking of manipulatie van verkiezingsresultaten (gevoelig voor storingen in stemcomputers (kiosken))
Obsolescence non maîtrisée des ordinateurs de vote	Ongecontroleerde veroudering van stemcomputers
La qualité des résultats peut être affectée par la vieillesse du matériel.	De kwaliteit van de resultaten kan worden beïnvloed door verouderde apparatuur

11 Bijlagen




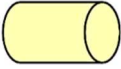
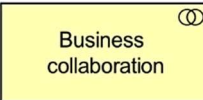



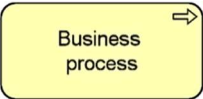
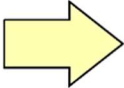



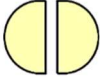
11.1 Glossarium





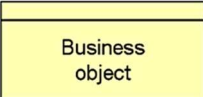
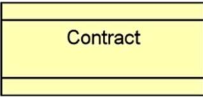
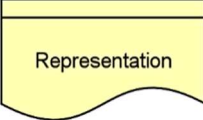
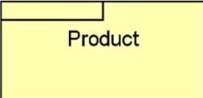
ID	Termijn	Definitie

11.2 Archimate-elementen

11.2.1 Business Architecture



Tabel 1: Elementen van de 'Business'-laag








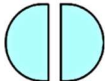

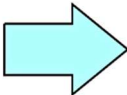




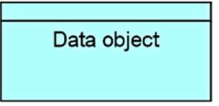
Item	Beschrijving	Notatie
Business Actor	Een businessentiteit die een gedrag kan uitvoeren.	 
Business Role	De verantwoordelijkheid voor het uitvoeren van een specifiek gedrag waaraan een actor kan worden toegewezen, of de rol die een actor speelt in een bepaalde actie of gebeurtenis.	 
Business Collaboration	Een samenvoeging van twee of meer elementen van de interne actieve structuur van de onderneming die samenwerken om een collectief gedrag uit te voeren.	 
Business Interface	Een toegangspunt waar een businessservice beschikbaar wordt gemaakt voor de omgeving.	 
Business Process	Een opeenvolging van businessgedragingen om een specifiek resultaat te bereiken, zoals een gedefinieerde reeks producten of diensten.	 
Business Function	Een reeks zakelijke gedragingen gebaseerd op een gekozen reeks criteria (meestal de vereiste middelen en/of professionele vaardigheden), nauw afgestemd op, maar niet noodzakelijk expliciet bestuurd door een organisatie.	 
Business Interaction	Een eenheid van collectief zakelijk gedrag uitgevoerd door (een samenwerking van) twee of meer zakelijke actoren, rollen of samenwerkingsverbanden.	 

Item	Beschrijving	Notatie
Business Event	Een verandering in de toestand van de organisatie.	 
Business Service	Het expliciet gedefinieerde gedrag dat een businessrol, businessactor of businesssamenwerking vertoont aan zijn omgeving.	 
Business Object	Een concept dat in een bepaald activiteitsdomein wordt gebruikt.	
Contract	Een formele of informele specificatie van een overeenkomst tussen een leverancier en een consument die de rechten en plichten specificeert die verbonden zijn aan een product en die functionele en niet-functionele parameters voor interactie vastlegt.	
Representation	Een waarneembare vorm van de informatie die door een bedrijfsobject wordt overgebracht.	
Product	Een samenhangend geheel van diensten en/of passieve structurele elementen, vergezeld van een contract/set van overeenkomsten, dat als geheel wordt aangeboden aan klanten (intern of extern).	

11.2.2 Architecture Application

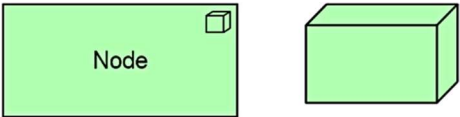
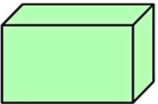
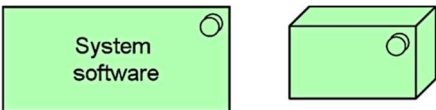

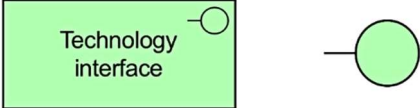
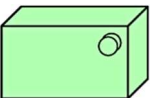

Tabel 2: Elementen van de 'Application'-laag




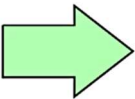

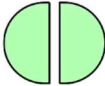



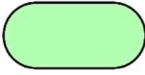
Item	Definitie	Notatie
Application Component	Een inkapseling van de applicatiefunctie afgesteld op de implementatiestructuur, die modulair en vervangbaar is.	 

Item	Definitie	Notatie
Application Collaboration	Een aggregaat van twee of meer elementen van de interne actieve structuur van de applicatie die samenwerken om collectief applicatiegedrag te bereiken.	 
Application Interface	Een toegangspunt waar applicatieservices beschikbaar worden gemaakt voor een gebruiker, een andere applicatiecomponent of een knooppunt.	 
Application Function	Het geautomatiseerde gedrag dat kan worden uitgevoerd door een applicatiecomponent.	 
Application Interaction	Een eenheid van collectief applicatiegedrag uitgevoerd door (een samenwerking van) twee of meer applicatiecomponenten.	 
Application Process	Een opeenvolging van applicatiegedragingen waarmee een specifiek resultaat wordt bereikt.	 
Application Event	Een toestandsverandering in de applicatie.	 
Application Service	Een expliciet gedefinieerd blootgesteld applicatiegedrag.	 
Data Object	Gestructureerde gegevens voor een geautomatiseerde verwerking.	

11.2.3 Architecture Technology

Tabel 3: Elementen van de 'Technology'-laag

Item	Definitie	Notatie
Node	Een computer of fysieke bron die andere computers of fysieke bronnen host, manipuleert of ermee interageert.	
Device	Een fysieke computerbron waarop systeemsoftware en artefacten kunnen worden opgeslagen of ingezet voor uitvoering.	
System Software	Doelt op software die voorziet in of bijdraagt tot een omgeving voor de opslag, uitvoering en het gebruik van software of gegevens die in die omgeving worden ingezet.	
Technology Collaboration	Een aggregaat van twee of meer elementen van de interne actieve structuur van de technologie die samenwerken om een collectief technologisch gedrag te bereiken.	
Technology Interface	Een toegangspunt tot de technologiediensten die door een knooppunt worden aangeboden.	
Path	Een verbinding tussen twee of meer knooppunten, waardoor deze knooppunten gegevens, energie of hardware kunnen uitwisselen.	
Communication Network	Een verzameling structuren die knooppunten verbinden	

Item	Definitie	Notatie
	voor de transmissie, routing en ontvangst van gegevens.	
Technology Function	Een reeks technologische gedragingen die door een knooppunt kunnen worden uitgevoerd.	 
Technology Process	Een opeenvolging van technologische gedragingen die kunnen worden gebruikt om een specifiek resultaat te behalen.	 
Technology Interaction	Een eenheid van collectief technologisch gedrag uitgevoerd door (een samenwerking van) twee of meer knooppunten.	 
Technology Event	Een verandering van technologische toestand.	 
Technology Service	Een expliciet gedefinieerd blootgesteld technologiegedrag.	 
Artifact	Een gegevenselement dat wordt gebruikt of geproduceerd in een softwareontwikkelingsproces, of door de inzet en werking van een computersysteem.	