BeVoting II
Studie over de evolutie van de elektronische stemming met papieren bewijsstuk in België

Olivier Pereira – Cyprien Delpech de Saint Guilhem – Bart Preneel
Katholieke Universiteit Leuven – Université catholique de Louvain
18 februari 2024

Samenvatting van de studie

Context van de studie

Deze studie is een antwoord op vragen van de Directie Verkiezingen van de FOD Binnenlandse Zaken over de evolutie van de elektronische stemming met papieren bewijsstuk in België, zowel op het vlak van de stemapparatuur als op het vlak van de mogelijkheden om de verkiezingsresultaten te verifiëren.

Deze vragen rijzen nu de overheidsopdracht met de leverancier van het huidige elektronische stemsysteem afloopt in 2027. Dat systeem is gebaseerd op een studie uit 2007. De Directie Verkiezingen heeft deze studie opgebouwd rond drie centrale vragen. We presenteren ze hier en vatten de centrale elementen van ons antwoord samen.

Vraag 1: Beoordeling van het huidige elektronische stemsysteem

Deze eerste vraag betreft de beoordeling van het huidige elektronische stemsysteem en of het in overeenstemming is met de huidige kwaliteits- en veiligheidseisen.

We hebben een reeks ontwikkelingen geïdentificeerd die nodig zouden zijn om het Belgische elektronische stemsysteem in overeenstemming te brengen met de internationale aanbevelingen over elektronisch stemmen, in het bijzonder met die van de Raad van Europa van 2017, en om een oplossing te bieden voor terugkerende problemen die werden vastgesteld bij het gebruik van het huidige systeem. Deze ontwikkelingen worden in vijf categorieën onderverdeeld:

1. *Het beheer en de implementatie van het stemsysteem vereenvoudigen.* Het doel hiervan is om het gemakkelijker te maken om het stemsysteem te installeren en op te starten in de stembureaus, maar ook om het onderhoud ervan in de loop van de tijd te vereenvoudigen, evenals de controle op de conformiteit ervan.

2. *De toegankelijkheid verbeteren.* Er zullen inspanningen worden geleverd om de toegang tot het stemsysteem voor een zo groot mogelijk deel van de bevolking te vergemakkelijken, door te profiteren van de mogelijkheden voor toegankelijkheid die elektronisch stemmen biedt.

3. *Transparantie.* We raden hier aan om het stemsysteem transparanter te maken en maatregelen te nemen om de voordelen van deze transparantie te benutten. België had dan wel een voortrekkersrol in het publiceren van zijn stemsoftware, maar de huidige aanbevelingen en praktijken in andere landen gaan nu veel verder, met duidelijke positieve effecten.

4. *Controleerbaarheid.* We stellen hier twee belangrijke ontwikkelingen voor om een doeltreffende en onafhankelijke verificatie van de verkiezingsresultaten mogelijk te maken, met inachtneming van het stemgeheim. Deze ontwikkelingen maken het mogelijk om eventuele fouten of inbraken in het systeem op te sporen en het bewijs te leveren dat de verkiezingsresultaten correct zijn.

5. *Rapportage.* Het doel hier is om mechanismen te implementeren voor het doeltreffend verzamelen van de incidenten die zijn waargenomen tijdens de uitrol van het stemsysteem, om het gemakkelijker te maken hun mogelijke gevolgen te meten.

Vraag 2: Voorgesteld concept van een nieuw stemsysteem

Vervolgens stellen we BeVoting II voor, een nieuw concept van een elektronisch stemsysteem, gebaseerd op het huidige systeem.

BeVoting II handhaaft het principe dat aan het huidige systeem ten grondslag ligt, namelijk het gebruik van stemmachines die papieren stembiljetten produceren en de stemmen niet tellen. Dit principe lijkt grotendeels te zijn bevestigd door de ontwikkelingen in de afgelopen jaren, waarbij veel landen zijn afgestapt van systemen zonder papieren stembiljetten.

Vergeleken met het huidige systeem stelt BeVoting II een aantal belangrijke veranderingen voor, in het bijzonder:

1. Het afstappen van de huidige elektronische stembus, die de belangrijkste niet-standaardcomponent van het systeem vormt, de uitrol van de stembureaus complexer maakt en het stemgeheim kan verzwakken. Die elektronische stembus wordt vervangen door traditionele stembussen, zoals de bussen die worden gebruikt voor de stemming op papier.

2. De introductie van een applicatie waarmee kiezers hun stembiljet van tevoren kunnen voorbereiden en in het stemhokje een QR-code kunnen scannen, zodat de stemmachine de vooraf gemaakte keuzes weergeeft en de kiezers hun keuzes kunnen bevestigen (of wijzigen). Deze optie zou het stemproces voor iedereen versnellen en de personen die dat wensen, de kans bieden om hun eigen toegankelijkheidssystemen te gebruiken op hun eigen toestel om het stembiljet voor te bereiden. Dit vormt een aanvulling op de aanbeveling om door te gaan met de pilots uit 2019, die gericht zijn op het verbeteren van de toegankelijkheid van de stemmachines in de stemhokjes.

3. De invoering van scanbureaus, waar de stembiljetten die in de stembussen worden gestopt, worden gescand. De organisatie van deze bureaus is vergelijkbaar met die van de telbureaus,

maar de uitvoering ervan zal veel minder inspanningen vergen dankzij de ontwikkelingen op het gebied van hogesnelheidsscanners.

4. De invoering van audits om het risico te beperken dat een fout resultaat wordt gevalideerd, georganiseerd op het niveau van de kieskringen. Deze audit, die in een groeiend aantal Amerikaanse staten verplicht is geworden, zorgt ervoor dat de stemmen die elektronisch worden geteld via scanning, een accurate weergave zijn van de papieren stembiljetten.

5. De invoering van een end-to-endverificatieprocedure waarmee de kiezers, door in te loggen op een website, zich ervan kunnen vergewissen dat het stembiljet dat ze in het stemhokje hebben ingevuld, wel degelijk is meegeteld bij het tellen van de stemmen, zonder dat het is gewijzigd.

6. De invoering van een applicatie voor het rapporteren van eventuele incidenten in de stem- en scanbureaus, waarmee de incidenten snel kunnen worden beschreven en de gegevens efficiënt kunnen worden verzameld, voor gebruik door de organisatoren van de verkiezing en het College van Deskundigen.

Vraag 3: Keuze van de hardware voor het voorgestelde nieuwe stemsysteem

De keuze van de hardware en de software voor elektronisch stemmen moet voldoen aan zeer specifieke randvoorwaarden. De apparatuur moet onder meer een aanzienlijk langere levensduur van het systeem mogelijk maken dan de klassieke levensduur van IT-apparatuur; ze moet een snelle, ongeplande uitrol mogelijk maken, met name om te voldoen aan de noodzaak om binnen 40 dagen verkiezingen te organiseren in het geval van ontbinding van de Kamer; ze moet voldoende gestandaardiseerd en getest zijn om een eerlijke en kwaliteitsvolle toegang voor de kiezers te garanderen; ze moet een snelle ondersteuning mogelijk maken in het geval van functionele gebrekkigheden tijdens de verkiezingen; en ze moet voldoen aan belangrijke beveiligings- en integriteitseisen, en dit alles terwijl de kosten zo laag mogelijk worden gehouden.

De keuze van de uitrusting kan ook worden bemoeilijkt door de kleine omvang van de Europese markt voor stemmachines voor nationale verkiezingen.

Het ontwerp van het BeVoting II-systeem, in combinatie met de ontwikkelingen van de hardware in de afgelopen vijftien jaar, betekent dat de volgende keuzes kunnen worden gemaakt:

1. Een systeem dat volledig is opgebouwd uit een klein aantal standaardonderdelen. Dit betekent dat onderdelen die kapot gaan, tegen lage kosten kunnen worden vervangen door nieuwe, goedkope onderdelen, waardoor het niet nodig is om op zoek te gaan naar originele onderdelen die mogelijk niet meer bestaan of om opnieuw specifieke hardware te maken.

2. Hardware waarmee het mogelijk wordt dat het besturingssysteem en de software meer dan tien jaar lang aan de veiligheidsnormen blijven voldoen.

De vereisten van integriteit, betrouwbaarheid en beschikbaarheid maken het onwaarschijnlijk dat het mogelijk zal zijn om de computers of laptops die in het stemsysteem zouden worden opgenomen, gedeeld te gebruiken.

Conclusies

Het ontwerp van het BeVoting II-stemsysteem dat in deze studie wordt beschreven, biedt een antwoord op de tekortkomingen van het elektronische stemsysteem dat momenteel in België wordt gebruikt ten opzichte van de aanbevelingen van de Raad van Europa van 2017, en pakt ook de moeilijkheden aan die door de Colleges van Deskundigen konden worden vastgesteld tijdens de uitrol van datzelfde stemsysteem.

BeVoting II bevat in het bijzonder de technieken voor het controleren van verkiezingen die beantwoorden aan de huidige stand van de techniek. Deze technieken bieden een fundamenteel antwoord op het klimaat van desinformatie dat zich heeft weten te ontwikkelen rond verkiezingen in tal van landen over de hele wereld, en op de aanzienlijke toename in de afgelopen vijftien jaar van het risico op internationale inmenging in de Belgische verkiezingen.

De hardware die nodig is om BeVoting II te implementeren, is volledig gestandaardiseerd, waardoor het systeem gemakkelijk is in onderhoud en duurzaam is. Er wordt voorgesteld om de stemsoftware ruim vóór het begin van de verkiezingsperiodes te onderwerpen aan een uitgebreid, onafhankelijk en publiek toegankelijk evaluatieproces, onder auspiciën van de Directie Verkiezingen van de FOD Binnenlandse Zaken.

1 INLEIDING

Deze studie werd uitgevoerd op vraag van de Directie Verkiezingen van de Federale Overheidsdienst Binnenlandse Zaken en heeft als doel te bepalen hoe de elektronische stemming met papieren bewijsstuk die momenteel in België wordt gebruikt, kan evolueren op het vlak van hardware, software en ook op het vlak van verifieerbaarheid.

1.1 ACHTERGROND VAN DE STUDIE

Het huidige elektronische stemsysteem wordt sinds de verkiezingen van 2012 gebruikt (na een proefproject in 2011). Het gaat om een stemsysteem dat in klassieke stemlokalen wordt gebruikt. De kiezers gaan naar een stemhokje, waar ze hun stem uitbrengen op een stemmachine die een papieren stembiljet uitprint. De kiezers controleren of het papieren stembiljet wel degelijk hun stemintentie leesbaar weergeeft en gaan vervolgens naar een elektronische stembus, waar ze een QR-code op het papieren stembiljet scannen. De QR-code bevat de stemintentie, die versleuteld wordt opgeslagen op de machine van de voorzitter van het stembureau. Als de scan gelukt is, gaat er een klep open op de stembus, zodat het stembiljet erin kan worden gestopt. In de kantonhoofdbureaus worden de stemmen getotaliseerd op basis van de registraties op de machines van de voorzitter in de verschillende stembureaus. De papieren stembiljetten worden bewaard voor controledoeleinden en maken het mogelijk om, indien nodig, een telling op papier uit te voeren.

De Directie Verkiezingen structureert de onderzoeksvragen rond twee centrale thema's: de ontwikkeling van de stemapparatuur en de controleerbaarheid van de verkiezingsuitslag. Ze wijst ook een aantal voor- en nadelen van het huidige systeem. Wat de voordelen betreft, haalt ze de aanwezigheid van het papieren stembiljet aan, dat de kiezers in staat stelt ervoor te zorgen dat er

een bewijs van hun stemintentie bestaat en dat een telling op papier mogelijk maakt bij problemen met het elektronische systeem. Ze merkt ook op dat de stemmachines geen harde schijf en geen netwerkconnectiviteit hebben, waardoor het oppervlak dat blootgesteld wordt aan cyberaanvallen, beperkt is. Wat de nadelen betreft, wijst ze op de noodzaak om te investeren in specifieke hardware, wat, in totaal, aanzienlijke kosten met zich meebrengt: vandaag zijn er meer dan 20.000 stemmachines in gebruik. Ze wijst ook op de snelle veroudering van de hardware, de onmogelijkheid om reserveonderdelen te vinden om storingen te herstellen en de beperkingen die ontstaan bij het uitvoeren van beveiligingsupdates vanwege de toenemende eisen op het gebied van evolutie van de software, eisen waaraan de bestaande hardware mogelijk niet meer kan voldoen. Ten slotte merkt zij op dat de kiezers geen enkele mogelijkheid hebben om te controleren of hun stem correct is geregistreerd en getotaliseerd, ondanks het feit dat het aanbieden van deze mogelijkheid een van de aanbevelingen van de Raad van Europa inzake elektronisch stemmen is.

Het huidige systeem wordt geleverd door het bedrijf Smartmatic, waarmee België een contract heeft dat in 2027 afloopt. Het doel van deze studie is om te onderzoeken hoe de Belgen ook na 2027 elektronisch kunnen blijven stemmen, met het huidige systeem als uitgangspunt. Als gevolg hiervan strekt deze studie er niet toe om de voordelen van elektronisch stemmen ten opzichte van stemmen op papier, of de voordelen van stemmen op afstand ten opzichte van stemmen in persoon te beoordelen: het gegeven kader is wel degelijk dat van een elektronisch stemsysteem met papieren bewijsstuk dat wordt ingezet in stembureaus.

1.2 STAND VAN ZAKEN

Het eerste deel van de studie beoordeelt het elektronische stemsysteem dat momenteel in België in gebruik is. De beoordeling gebeurt volgens drie hoofdlijnen.

De eerste hoofdlijn is een beoordeling van de manier waarop het huidige elektronische systeem heeft voldaan aan de behoeften tijdens de verkiezingen die sinds 2012 hebben plaatsgevonden. We baseren ons hierbij op de verslagen die de Colleges van Deskundigen na elke verkiezing opstellen. Hierin beschrijven de Colleges van Deskundigen hun controlewerkzaamheden inzake de voorbereiding, het gebruik en de goede werking van alle stem-, registratie- en telsystemen voor elektronisch stemmen. De Colleges doen ook een aantal aanbevelingen om het elektronische stemsysteem te verbeteren, aanbevelingen die de afgelopen jaren hebben geleid tot een aantal wijzigingen in het systeem.

In de tweede hoofdlijn beoordelen we of het huidige elektronische stemsysteem in overeenstemming is met de huidige internationale aanbevelingen. Die aanbevelingen zijn aanzienlijk geëvolueerd sinds het ontwerp van het elektronische stemsysteem dat momenteel in gebruik is, en weerspiegelen met name de vooruitgang in wetenschappelijk onderzoek die de afgelopen vijftien jaar heeft plaatsgevonden – vergeet niet dat het huidige systeem is ontworpen op basis van een BeVoting-studie die in 2007 is verricht [29].

De derde hoofdlijn bestaat in een beoordeling van het huidige elektronische stemsysteem vanuit het oogpunt van de beheerder, die de kosten in de hand moet houden en het onderhoud moet verzorgen gedurende een lange levensduur – het huidige contract met Smartmatic heeft een levensduur van vijftien jaar, wat veel langer is dan de gebruikelijke levensduur van IT-apparatuur.

Dit deel van de studie wordt afgesloten met negen hoofddoelstellingen voor het verbeteren van het huidige systeem, onderverdeeld in vijf categorieën: *(1)* Beheer van de hardware en de software, *(2)* Toegankelijkheid van het systeem, *(3)* Transparantie, *(4)* Controleerbaarheid, *(5)* Rapportage.

1.3 CONTROLEERBAARHEID

Het tweede deel van de studie gaat over controleerbaarheidstechnologieën, die de belangrijkste technologische vooruitgang in elektronisch stemmen in de afgelopen vijftien jaar vormen, en waarvan de studie is aangevraagd door de Directie Verkiezingen, in overeenstemming met de aanbevelingen van de Raad van Europa over elektronisch stemmen.

Het eerste voordeel van deze technologieën is dat ze het mogelijk maken om de goede werking van het systeem te verifiëren met middelen die niet afhangen van het stemsysteem. Dit is uiteraard belangrijk in de context van een elektronisch stemsysteem, waar gebruik wordt gemaakt van computers waarvan de werking altijd moeilijk te observeren is. Dit is des te belangrijker omdat de risico's verbonden aan internationale inmenging in de Belgische verkiezingen de laatste vijftien jaar alleen maar zijn toegenomen en omdat de steminfrastructuur zonder dit proces duidelijk een kritieke infrastructuur vormt.

Een tweede voordeel is dat de organisatoren van verkiezingen kunnen bewijzen dat de aangekondigde uitslag correct is. De beschikbaarheid van een dergelijk bewijs is met name belangrijk geworden in een context waarin de verkiezingsuitslag in meerdere landen steeds openlijker wordt betwist, wat soms leidt tot aanvallen op overheidsinstellingen, en waarin degenen die betrokken zijn bij de organisatie en ondersteuning van de verkiezingen, steeds vaker worden blootgesteld aan beschuldigingen, bedreigingen en openbaarmaking van persoonsgegevens[1]. De mogelijkheid om te bewijzen dat de resultaten van een verkiezing juist zijn, in tegenstelling tot de afwezigheid van bewijs dat ze onjuist zijn, wordt gezien als een middel om de verspreiding van misleidende informatie tegen te gaan.

We bespreken de twee belangrijkste bestaande benaderingen met hun vereisten: audits die het risico beperken dat een onjuist resultaat wordt gevalideerd, hoofdzakelijk met gebruik van statistische verificatietechnieken, en end-to-endcontroleerbaarheid, hoofdzakelijk met gebruik van technieken uit de cryptografie.

Deze twee benaderingen vullen elkaar aan en vereisen dat de stemsystemen worden ontworpen om ze te kunnen implementeren: al in de ontwerpfase van het systeem moet ervoor worden gezorgd dat de gegevens die nodig zijn voor de audit en de controleerbaarheid, worden geproduceerd en toegankelijk zijn en dat er doeltreffende audits en controles mee kunnen worden uitgevoerd. Deze technieken zijn in verschillende mate van maturiteit geïmplementeerd in andere landen. We baseren ons op de ervaring die elders is opgedaan en verkennen de mogelijkheden om deze

[1] Dit fenomeen is in de Verenigde Staten zo wijdverspreid dat sinds 2020 veertien staten nieuwe wetten hebben aangenomen om de personen die verantwoordelijk zijn voor het organiseren van verkiezingen en die in de stembureaus werken, te beschermen. *https://www.ncsl.org/elections-and-campaigns/state-laws-providing-protection-for-election-officials-and-staff*

technieken aan te passen aan de Belgische context en zijn belangrijke specifieke kenmerken: stembiljetten met soms een zeer groot aantal kandidaten, specifieke telmethodes, enz.

We zullen concrete methodes voorstellen voor het organiseren van de uitrol van deze methodes in een Belgische context, evenals een beoordeling van de complexiteit van een dergelijke uitrol op basis van gegevens die zijn gepubliceerd tijdens vorige Belgische verkiezingen en audit- en verificatietechnieken die overeenkomen met de stand van de techniek van de methodes die vandaag worden gebruikt.

1.4 BESCHRIJVING VAN EEN NIEUW ELEKTRONISCH STEMSYSTEEM

Het derde en laatste deel van de studie behandelt het ontwerp van een nieuw elektronisch stemsysteem, BeVoting II, dat na 2027 in België zou kunnen worden ingevoerd. Dit ontwerp biedt een antwoord op de negen hoofddoelstellingen die uit de huidige stand van zaken naar voren zijn gekomen, en beschrijft in het bijzonder hoe controleerbaarheidstechnieken kunnen worden geïmplementeerd.

We onderzoeken de hardware- en softwarevereisten van het BeVoting II-systeem en bestuderen de methodologieën voor het beoordelen, onderhouden en upgraden van deze hard- en software. Hierbij stellen wij ons tot doel om de haalbaarheid van de implementatie van het voorgestelde ontwerp aan te tonen, waarbij we vermijden om voorschrijvend te zijn wanneer dit niet nodig is: in een bepaald aantal contexten overwegen we verschillende opties die ons stuk voor stuk technisch geldig lijken, en we vinden het dan beter om te beslissen op basis van wat de beste oplossingsleveranciers kunnen voorstellen en kunnen beloven te handhaven op het moment waarop er een offerteaanvraag wordt uitgeschreven, en waarop de beschikbare hardware- en softwareomgevingen verder zullen zijn geëvolueerd.

We zien ook dat België een baanbreker was in de keuze van dit systeem, en in het bijzonder in de keuze om gebruik te maken van stemmachines die een papieren stembiljet met de keuzes van de kiezers afdrukken, en om de stemmen te tellen op basis van het papieren stembiljet, en niet op basis van een registratie van de stemmen in de stemmachine. Dit kan in perspectief worden geplaatst ten opzichte van de veranderende praktijken in de Verenigde Staten, een van de grootste markten voor stemmachines: in 2008 stemde meer dan 34% van de geregistreerde kiezers op machines die ook de stemmen telden, en meer dan 21% van de kiezers stemde op machines die geen papieren stembiljetten produceerden[2]. Deze aantallen zullen 3% en 1,7% zijn voor de verkiezingen van 2024. Bovendien zullen in 2024 de stembiljetten van meer dan 90% van de kiezers worden geteld op basis van papieren stembiljetten die met de hand zijn ingevuld of door stemmachines zijn afgedrukt[3]. We zien hierin een duidelijke erkenning van het belang van het bestaan van een papieren stembiljet en van een telling uitgevoerd op basis van papieren stembiljetten.

Los van dit voordeel zijn er een aantal beperkingen en zwakke punten in het huidige stemsysteem en de manier waarop het wordt geïmplementeerd. Vele daarvan kunnen in verband worden

[2] *https://verifiedvoting.org/verifier/#mode/visualization/year/2006*

[3] *https://verifiedvoting.org/verifier/#mode/visualization/year/2024*

gebracht met technologieën en internationale aanbevelingen voor elektronisch stemmen die nog niet bestonden toen het systeem werd ontworpen, en die vandaag zouden kunnen worden geïmplementeerd. Andere weerspiegelen structurele problemen op het gebied van stemmachines, waarvan het misschien goed zou zijn om ze vandaag opnieuw op tafel te leggen om te bepalen of er andere oplossingen kunnen worden gevonden.

2 STAND VAN ZAKEN

2.1 INLEIDING

We beoordelen het elektronische stemsysteem dat momenteel in België wordt gebruikt op basis van twee belangrijke bronnen:

1. De verslagen van de Colleges van Deskundigen die na elke verkiezing zijn ingediend.
2. De recente internationale aanbevelingen over elektronisch stemmen en de academische literatuur ter zake.

Aan de hand van verslagen van de Colleges zullen we de moeilijkheden in het gebruik van het huidige systeem kunnen identificeren. Misschien bestaat de wens om die problemen te verhelpen, zelfs als er geen vooruitgang wordt geboekt in de ontwikkeling van stemtechnologieën.

De recente internationale aanbevelingen, aangevuld met de academische literatuur, zullen ons in staat stellen om de meest bruikbare technologieën te identificeren die de afgelopen vijftien jaar zijn ontwikkeld en die een dusdanig niveau van maturiteit en belang hebben bereikt dat er nu een duidelijke consensus bestaat over het aanbevelen van de toepassing ervan.

Deze bronnen werden aangevuld met interviews van verschillende actoren uit het werkveld.

2.2 DE VERSLAGEN VAN DE COLLEGES VAN DESKUNDIGEN

De opdracht van het College van Deskundigen is vastgelegd in artikel 25 van de wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstuk:

1. […] zien deze deskundigen toe op de voorbereiding, het gebruik en de goede werking van alle elektronische stemsystemen, registratiesystemen, ontsleutelingssystemen en totaliseringssystemen, alsook de procedures betreffende de aanmaak, de verspreiding en het gebruik van de apparatuur, programmatuur en de elektronische gegevensdragers. Het College van deskundigen controleert eveneens de voorbereiding, het gebruik en de goede werking van de hardware, software en procedures voor de digitale transmissie en het digitaal verspreiden van de resultaten alsook alle software die gebruikt wordt in het kader van de verkiezingen, zelfs wanneer de stemming volgens andere modaliteiten verloopt dan die welke door deze wet voorzien zijn. […]
2. Uiterlijk vijftien dagen na de sluiting van de stemming en in ieder geval voor de geldigverklaring van de verkiezingen voor wat de Kamer van volksvertegenwoordigers, de Gewest- en Gemeenschapsparlementen en het Europees Parlement betreft, bezorgen de deskundigen een verslag aan de minister van Binnenlandse Zaken, alsook aan de federale wetgevende assemblees en de Gewest- en Gemeenschapsparlementen.

De verslagen waarnaar in de tweede paragraaf wordt verwezen, zijn een uitstekende bron van informatie over de kwaliteiten, moeilijkheden en verbeterpunten van het stemsysteem. Ze

beschrijven, vaak in detail, de verrichtingen inzake het toezicht op en de beoordeling van de stemsoftware, de waarnemingen door middel van steekproefsgewijze bezoeken aan stembureaus en hoofdbureaus, en de auditverrichtingen die na de verkiezingen worden uitgevoerd.

We zullen hier niet in detail de beschrijvende aspecten van de uitgevoerde procedures weergeven, maar we spitsen ons toe op de audits en aanbevelingen met betrekking tot het elektronische stemsysteem dat momenteel in België wordt gebruikt (het 'Smartmatic'-systeem), die zijn voortgekomen uit de elektronische verkiezingen van 2012 [15, 17, 19], 2014 [16], 2018 [13, 18, 20] en 2019 [14] (we laten de uitrol van 2011 buiten beschouwing, omdat het ging om een proefproject met slechts 6.000 kiezers).

Omwille van de duidelijkheid zijn de beschrijvende delen gebaseerd op de procedure die in 2019 is uitgevoerd [14]: we hebben kunnen vaststellen dat ze verschillende ontwikkelingen en verbeteringen sinds 2012 weerspiegelt. We lichten hier een aantal aspecten uit die volgens ons opvallend zijn en die afkomstig zijn uit de verslagen van de vorige verkiezingen.

2.2.1 Algemene opmerkingen

2.2.1.1 De ervaring van de kiezers

Een eerste observatie is dat er geen meldingen waren van moeilijkheden bij het gebruik van het elektronische stemsysteem: de kiezers lijken erin te zijn geslaagd hun stem uit te brengen en hun stembiljetten in de urne te steken zonder bijzondere moeilijkheden te ondervinden. In de eerste generaties van het systeem werden enkele 'kinderziektes' genoemd (traagheid van de interface waardoor kiezers meerdere keren moesten 'klikken' en onbedoelde selecties moesten maken, geluidsalarmen die in te veel omstandigheden afgingen en verwarring veroorzaakten, verwarring over het feit of de gescande stembiljetten wel of niet werden geregistreerd op de machine van de voorzitter, enz.), maar deze zijn duidelijk geleidelijk opgelost [16][14].

De belangrijkste resterende bekommernissen lijken te maken te hebben met machinestoringen (machines die niet starten, niet afdrukken, enz.), hoewel de verslagen geen duidelijk beeld geven van de impact van de ondervonden moeilijkheden. Die impact was echter beperkt, gezien hij nooit heeft geleid tot een annulering van verkiezingen.

2.2.1.2 De ervaring van de stembureaus

In de stembureaus deden zich wel een aantal problemen voor bij het initialiseren van de machines, in het bijzonder:

- bij het hanteren van de USB-sticks: niet-conform beheer van het openen en bewaren van de verzegelde enveloppen, niet-beveiliging van de toegang tot de USB-poorten van de stemmachines, onjuiste inbrenging van de USB-sticks in de machines, niet-werkende USB-sticks, enz. Uit de verslagen kan de omvang van deze problemen niet worden gekwantificeerd: ze worden vermeld, soms zonder informatie over de bureaus waar ze werden vastgesteld [14], maar ze zijn voldoende aanwezig om herhaaldelijk te worden opgemerkt in de verschillende verslagen – we denken bijvoorbeeld aan het incident in Sint-Joost-ten-Node in 2018 [13], waarbij een probleem werd vastgesteld dat verband hield met het vroegtijdig verwijderen van USB-sticks, een probleem dat zich in verschillende andere kieskringen voordeed en dat in 2019 werd opgelost [14].

De moeilijkheden tijdens de stemming betroffen vooral:

- behandeling van smartcards die worden gebruikt om stemmen te initialiseren: defecte chipkaarten, initialisatie voor onjuiste stemmingen, risico van verwarring tussen testkaarten en 'normale' kaarten. Dit probleem duikt op in alle verslagen [15][19][16][13], behalve in het verslag van 2019;
- problemen met afdrukken: in het bijzonder stembiljetten die vast komen te zitten in de stemmachines [20] [14]
- problemen met het lezen van stembiljetten door de stembussen [14]

De verslagen maken het niet mogelijk om de omvang en de impact van de ondervonden moeilijkheden precies te meten, en dit lijkt onvermijdelijk gezien het huidige proces, waarbij de deskundigen steekproefsgewijs stembureaus bezoeken[4]: we telden 100 bezoeken in 2012, 88 in 2018 en 133 in 2019 voor ongeveer 4.000 stembureaus die zijn uitgerust met Smartmatic-machines – in 2014 werd er geen lijst van bezochte stembureaus verstrekt.

Zoals de zaken er nu voorstaan, is het moeilijk om de werkelijke omvang van de vastgestelde problemen in te schatten: voor het hele land: welk percentage van de machines ondervond opstartproblemen, welk percentage van de USB-sticks werkte niet, hoeveel problemen met stembussen en afdrukken deden zich voor? Wat was de impact van deze problemen: konden ze in een paar minuten worden opgelost of hebben ze de stemverrichtingen aanzienlijk vertraagd of verhinderd?

2.2.1.3 Conclusies

In het algemeen lijkt het huidige elektronische stemsysteem het mogelijk te hebben gemaakt om aan de behoeften van de recente verkiezingen te voldoen: we kunnen vaststellen dat de verkiezingen systematisch geldig werden verklaard en dat de belangrijkste problemen die zich voordeden tijdens de recente verkiezingen, geen betrekking hadden op het 'Smartmatic'-stemsysteem. Zo betrof de

- befaamde 'verkiezingsbug van 2014' het Jites/Digivote-stemsysteem, dat door het Smartmatic-stemsysteem moest worden vervangen.
- De moeilijkheden bij het doorgeven van de resultaten van 2019 waren te wijten aan een probleem met de toegang tot het Martine-systeem voor de gegevensinvoer van de resultaten, dat ook onafhankelijk is van het Smartmatic-systeem.

Desalniettemin, en zoals te verwachten is wanneer op één dag 20.000 stemmachines en ongeveer 4.000 elektronische stembussen worden ingezet, maken de verslagen van de Colleges melding van een aantal technische problemen die zich tijdens de verkiezingsdagen voordeden. Hieruit kunnen volgens ons twee conclusies worden getrokken:

[4] Gezien het aantal leden van het College en het aantal stembureaus kunnen zij uiteraard niet anders te werk gaan.

1. Elke vereenvoudiging van het proces voor het beheer van de stembureaus is welkom: ze zal het risico op fouten en storingen verkleinen.

2. Een procedure voor systematische rapportering van de ondervonden moeilijkheden in de stembureaus en de hoofdbureaus, die een eenvoudige compilatie van de resultaten mogelijk maakt, zou nuttig zijn om de ondervonden moeilijkheden verder te kunnen kwantificeren.

2.2.2 Controles van de software

Een centraal onderdeel van de rol van het College van Deskundigen is de verificatie van de software die tijdens de verkiezing wordt gebruikt. De verificatie van de software behelst twee afzonderlijke elementen:

1. De inspectie van de software die bedoeld is voor gebruik in de stemmachines en de machines van de bureauvoorzitters.

2. Het onderzoek van de procedures om ervoor te zorgen dat de geïnspecteerde software daadwerkelijk de software is die tijdens de verkiezing is gebruikt.

2.2.2.1 Inspectie van de software

Enkele maanden voor de verkiezingen[5] wordt de broncode van de software overhandigd aan de FOD Binnenlandse Zaken. Deze code weerspiegelt de laatste verbeteringen aan het systeem, inclusief de verbeteringen die voortvloeien uit de aanbevelingen van het College van Deskundigen en het Centrum voor Cybersecurity België (CCB).

Deze broncode wordt gecompileerd om de uitvoerbare versie te produceren die op de verkiezingsdag op de stem- en voorzittersmachines wordt geïnstalleerd. Kopieën van de broncode en gecompileerde code worden aan verschillende instanties bezorgd voor archiverings- en inspectiedoeleinden.

De code wordt ook naar een gespecialiseerd IT-bedrijf gestuurd, in casu PricewaterhouseCoopers, dat, in het kader van een overeenkomst met Smartmatic, controleert of de software adequaat is. Dit bedrijf brengt een advies uit op basis waarvan de FOD Binnenlandse Zaken het systeem conform verklaart.[6]

Het College van Deskundigen wijst op een aantal problemen met betrekking tot de software. Zo heerst er bezorgdheid over de veiligheid van het softwareontwikkelingsproces en de leesbaarheid en documentatie ervan: aanbevelingen [2019-BE.12], [2019-BE.13], [2019-BE.17], [2019-BE.32] in 2019, die de aanbevelingen [2018-BXL.10] [2014-BE.42] en [2012-BXL.22] herhalen en ook de opmerkingen van PricewaterhouseCoopers [16] weerspiegelen.

De computercode voor een stemsysteem is complex en bestaat meestal uit enkele honderdduizenden regels. Bovendien is de review van de code een uiterst complexe en tijdrovende

---

[5] Bijvoorbeeld op 27 februari 2019 voor de verkiezingen van 26 mei 2019 [14].

[6] Dit advies is bijvoorbeeld ingediend op 12 april 2019 voor de verkiezingen van 26 mei 2019 [14], en op 3 en 4 oktober voor de verkiezingen van 14 oktober 2018 [13] [20].

taak. Het corrigeren van een bug in een kritiek IT-systeem is ook een uiterst gevoelige taak als je een correcte oplossing wilt bieden en tegelijkertijd wilt voorkomen dat er nieuwe problemen ontstaan.

Dit is zorgwekkend omdat in een aantal gevallen systemen die waren onderzocht en gevalideerd onder omstandigheden die vergelijkbaar zijn met wat er momenteel in België gebeurt, en die vervolgens werden onderworpen aan evaluatieprocedures door een breder publiek, hebben geleid tot de identificatie van grote gebreken, die zelfs hebben geresulteerd in het verlies van erkenning van systemen.[7][8][9]

Dit zet ons ertoe aan bijzondere aandacht te besteden aan de aanbeveling [2019-BE.30] van het College van Deskundigen, die als volgt luidt:

Het College van Deskundigen beveelt aan dat elk bestand dat door de organiserende autoriteit openbaar wordt gemaakt met betrekking tot de verkiezingen (resultaten, broncode, enz.), [...] permanent beschikbaar [wordt gesteld] op een site met een zoekfunctie.

De publicatie van de broncode van het stemsysteem is altijd al toegepast in België, en dit is een sterk punt dat benadrukt moet worden. We merken echter op dat een aantal beperkingen de voordelen beperken die van deze aanpak verwacht kunnen worden. In het bijzonder bepaalt artikel 17 van de wet tot organisatie van de elektronische stemming met papieren bewijsstuk [69] dat de stemsoftware wordt gepubliceerd in de week volgend op de dag van de verkiezing, zonder de veiligheidskenmerken, voor een periode van zes maanden na de verkiezing.

Deze publicatie maakt het op geen enkele manier mogelijk om eventuele fouten in deze code te corrigeren, temeer omdat deze waarschijnlijk lang na de definitieve geldigverklaring van de verkiezingsuitslag worden ontdekt, waardoor elke observatie in wezen ineffectief is.

Deze praktijkervaring inzake de publicatie van de code, zoals beschreven in de wet tot organisatie van de elektronische stemming, liggen ver onder wat wordt aanbevolen door de Raad van Europa, en zullen worden besproken in het volgende deel.

Bovendien lijken de redenen voor het niet-publiceren van de veiligheidselementen van de code ons in de gegeven omstandigheden niet duidelijk. De publicatie van deze elementen maakt het daarentegen mogelijk om te controleren of de beveiliging doeltreffend is en vormt een praktijk die sterk wordt aangemoedigd op het gebied van IT-beveiliging, zo ze al niet wordt opgelegd.

2.2.2.2 Authenticiteit van de gebruikte software

De stemsoftware (stemmachines en voorzitter) wordt op gecentraliseerde wijze opgeladen door de FOD Binnenlandse Zaken op USB-sticks die bestemd zijn voor alle stembureaus en waarvan de toegang beveiligd is met wachtwoorden.

---

[7] *https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review*

[8] *https://estoniaevoting.org/*

[9] *https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-74508.html*

De USB-sticks worden in verzegelde enveloppen naar de voorzitters van de stembureaus gestuurd, samen met een unieke stembureaucode en een wachtwoord. Twee USB-sticks worden in de elektronische stembus gestoken, waarna de computer van de voorzitter wordt opgestart en de code van het stembureau en het wachtwoord worden ingevoerd. Na het opstarten worden de USB-sticks uit de stembus gehaald en in de stemmachines gestoken om die op te starten. Na het opstarten van de stemmachines worden de USB-sticks opnieuw weggehaald en opnieuw in de urne gestoken[10].

De belangrijkste moeilijkheden die gepaard gaan met deze procedure, bestaan erin te zorgen voor het volgende:

1. De stemmachines en de machine van de bureauvoorzitter worden opgestart met USB-sticks die de software bevatten die door de FOD Binnenlandse Zaken conform is verklaard.
2. De stemmachines en de machine van de bureauvoorzitter werden niet zodanig gewijzigd dat ze de software op de USB-sticks geheel of gedeeltelijk kunnen negeren en in plaats daarvan op basis van corrupte software kunnen werken.

Moeilijkheden met betrekking tot het eerste punt worden opgemerkt door het College van Deskundigen, dat met name aanbeveelt om de USB-sticks en de wachtwoorden via verschillende kanalen aan de voorzitters van de stembureaus te leveren [2019-BE.24], wat zou voorkomen dat een persoon die instaat voor de overhandiging van de USB-sleutels, door het omzeilen van de beveiliging van de verzegelde envelop toegang zou kunnen krijgen tot een reeks geheime gegevens die op de USB-stick zijn opgeslagen.

We stellen ook vast dat het College van Deskundigen in sommige gevallen USB-sticks kon inspecteren na de sluiting van de verkiezingen om te controleren of de juiste software erop stond [16]. Dit wordt echter niet systematisch gerapporteerd.

We hebben in de verslagen van de deskundigen geen informatie gevonden over het risico dat is besproken in ons tweede punt (conformiteit van de machines). Aanpassingen aan de machines, waardoor het eventueel mogelijk zou worden om ze anders te doen werken dan de software op de USB-sticks voorschrijft, worden zowel bemoeilijkt als vergemakkelijkt door verschillende specifieke kenmerken van het Belgische systeem en het onderhoud ervan.

Een belangrijk sterk punt van het Belgische systeem is de afwezigheid van een niet-vluchtig opslagmedium (harde schijf, enz.) dat de stemsoftware bevat, waardoor vermeden wordt dat iemand met slechte bedoelingen die toegang heeft tot een stemmachine, de stemsoftware op de machine rechtstreeks zou kunnen wijzigen.

Een aandachtspunt is de opslag van de stemmachines, die wordt uitgevoerd onder voorwaarden die per gemeente kunnen variëren. Een fout in de toegangscontrolemechanismen van de machines zou actoren in staat kunnen stellen om de bootloader, die het opstarten van de machines regelt, aan te passen om zo de controle over de machines over te nemen, of zelfs om meer ingrijpende aanpassingen te doen die een niet-vluchtig geheugen en een compleet stemsysteem eraan zouden toevoegen, dat zich zichtbaar zou gedragen als het normale systeem, maar dat zou proberen om

[10] *https://verkiezingen.fgov.be/sites/default/files/inline-files/Clevo_VIU-805-SAES3370_A4-517BE_President_Manual-NL.pdf*

stemmen te wijzigen. Er zijn al dergelijke aanvallen uitgevoerd, soms met aanzienlijke juridische en media-impact [67].

We onthouden hier de moeilijkheid om te garanderen dat er authentieke software wordt gebruikt, die het belang van de papieren stembiljetten en de verificatie ervan nog verder vergroot.

2.2.3 Audits na de verkiezingen

De Colleges van Deskundigen verzamelen tijdens en vlak na de verkiezingen een aantal gegevens om audits uit te voeren. We merken in het bijzonder het volgende op:

- In elk gecontroleerd stembureau werden teststemmen uitgebracht door de deskundigen van het College, ter controle en analyse in een omgeving die specifiek is voor het College [16] [14].
- Het College heeft een volledige hertotalisering uitgevoerd van de stemmen op de USB-sticks die in de stembureaus werden gebruikt, om de officiële resultaten te vergelijken met de resultaten die het College via zijn eigen software heeft verkregen [14].
- In 2014 voerde het College een handmatige stembustelling uit in twee willekeurig gekozen stembureaus om de resultaten te vergelijken met die van de geautomatiseerde telling [16].

Ook worden sommige audits uitgevoerd in hoofdbureaus. [11]Artikel 80 van de ordonnantie van 20 juli 2023 houdende het Nieuw Brussels Gemeentelijk Kieswetboek bepaalt als volgt:

De voorzitter van het hoofdbureau kan eveneens beslissen om steekproefsgewijs over te gaan tot een manuele hertelling van de stemcijfers van de lijststemmen. Deze hertelling gebeurt hoe dan ook voor één kiesbureau per gemeente.

Deze audits brengen soms kleine discrepanties aan het licht, met name tussen het aantal stembiljetten dat daadwerkelijk in de stembussen aanwezig is en het aantal stembiljetten dat daadwerkelijk op de elektronische media is geregistreerd.

Het uitvoeren van die audits is uiterst nuttig en belangrijk. We hebben immers al eerder gezien hoe belangrijk papieren stembiljetten zijn als bescherming tegen defecte of gewijzigde software, en deze tests zijn vandaag de enige manier die we hebben om dit soort problemen op te sporen.

Het is echter opnieuw moeilijk om duidelijke conclusies te trekken uit die audits, hoewel ze grotendeels positief lijken te zijn. Op basis van de uitgevoerde audits is het immers niet mogelijk om een bruikbare grens af te leiden voor de waarschijnlijkheid dat een onjuist resultaat wordt gevalideerd ondanks de audits. Deze onmogelijkheid houdt met name verband met aspecten van het huidige systeem die het onmogelijk maken om audits met een redelijke doeltreffendheid uit te voeren.

Het verbeteren van de procedures voor het verifiëren en controleren van de verkiezingsresultaten is het doel van de controleerbaarheidstechnieken waarop we ingaan in hoofdstuk 3 van deze studie.

[11] *https://www.ejustice.just.fgov.be/cgi/article.pl?language=nl&sum_date=2023-08-14&lg_txt=n&pd_search=2023-08-14&s_editie=&numac_search=2023044127&caller=&2023044127=&view_numac=2023044127f*

2.3 De aanbevelingen van de Raad van Europa over elektronisch stemmen

De belangrijkste bron voor internationale aanbevelingen die van toepassing zijn op elektronisch stemmen, is Aanbeveling CM/Rec(2017)5 van het Comité van Ministers aan de lidstaten inzake normen voor e-voting, aangenomen door het Comité van Ministers op 14 juni 2017 [23], en in het bijzonder de bijlage B, die richtlijnen geeft voor de uitvoering van deze aanbevelingen [22]. De Raad van Europa blijft de enige organisatie die intergouvernementele normen heeft gedefinieerd voor elektronisch stemmen in Europa.

We zullen ook verwijzen, met name in punt *4.3*, naar de volgende documenten:

- "Securing the Vote: Protecting American Democracy" gepubliceerd in 2018 door de "National Academies of Sciences, Engineering, and Medicine" van de Verenigde Staten [45]. Dit document biedt soms een andere benadering van kwesties die ook in de aanbevelingen van de Raad van Europa worden behandeld.
- De "Voluntary Voting System Guidelines" (VVSG), gepubliceerd in 2022 door de "United States Election Assistance Commission" [62], die praktische aanbevelingen bevatten voor het ontwerp, de uitrol en het onderhoud van elektronische stemsystemen. In sommige staten van de VS is naleving van de VVSG verplicht.
- Ordonnantie 161.116 van de Zwitserse Bondskanselarij over elektronisch stemmen uit 2022 [11], die vandaag vooroploopt wat betreft transparantievereisten voor elektronisch stemmen.

Andere documenten, zoals het "Compendium on Cyber Security of Election Technology" van de Europese "NIS Cooperation Group", zijn zeker nuttig in de context van verkiezingen, maar zijn minder direct gericht op elektronische stemsystemen.

Het huidige elektronische stemsysteem in België is ontworpen op basis van de versie van 2004 van de Aanbevelingen van de Raad van Europa en voldoet nog steeds aan veel van de Aanbevelingen in de versie van 2017. We citeren hier de aanbevelingen ten opzichte waarvan het huidige Belgische elektronische stemsysteem ons nog aanzienlijke mogelijkheden tot verbetering lijkt te bieden.

2.3.1 Toegankelijkheid

2. Het elektronische stemsysteem wordt, voor zover mogelijk, zo ontworpen dat personen met een handicap en personen met bijzondere behoeften zelfstandig kunnen stemmen.

Het gebruik van stemmachines heeft het grote voordeel, vooral in België, waar de stembiljetten bijzonder groot en ingewikkeld zijn om in te vullen, dat het invullen van stembiljetten gemakkelijker wordt en dat het onbedoeld tot stand komen van een ongeldig stembiljet wordt voorkomen.

Het Belgische elektronische stemsysteem maakt echter geen gebruik van een aantal ondersteunende technologieën die een groter aantal mensen in staat zouden stellen om zelfstandig te stemmen. Tot op heden is er slechts één proefproject georganiseerd in 2019 in Aalst en Mechelen, met de installatie van technologieën om het stemmen voor slechtziende of blinde kiezers te vergemakkelijken [14].

We willen echter wijzen op een belangrijk voordeel van het elektronische stemsysteem dat momenteel in België wordt gebruikt, namelijk de vereenvoudiging van het invullen van de stembiljetten voor veel mensen. Door de grootte van de papieren stembiljetten in België, het grote aantal kandidaten op de lijsten en de regels voor het invullen van de stembiljetten, die het panacheren verbieden, wordt een aanzienlijk aantal met de hand ingevulde stembiljetten onbedoeld ongeldig gemaakt door de kiezers zelf. Dit werd met name bestudeerd door Jean-Benoit Pilet en zijn medeauteurs [51], die toegang kregen tot de stembiljetten die door kiezers met de hand waren ingevuld tijdens de Waalse gemeenteraadsverkiezingen van 2018: zo werd vastgesteld dat gemiddeld 65,4% van de stembiljetten die in de verkiezingsuitslag als 'blanco of ongeldig' werden gerapporteerd, ongeldige stembiljetten waren en dat daarvan gemiddeld 43% werd geïdentificeerd als onopzettelijk ongeldig, d.w.z. 28% van de 'blanco of ongeldige' stembiljetten. Op basis van de waarneming van gemiddeld 6,7% 'blanco of ongeldige' stembiljetten onder alle stembiljetten, komen we uit op 1,9% van alle stembiljetten die onbedoeld ongeldig zouden zijn bij het stemmen op papier. Dit percentage is veel hoger dan de gebruikelijke verkiezingsmarge in België, die het aandeel van de stemmen meet dat moet worden veranderd om de verkiezingsuitslag te wijzigen – we beschrijven dergelijke marges uitgebreider in punt *3.2.3*. Elektronisch stemmen voorkomt dat deze 1,9% van de uitgebrachte stemmen onbedoeld ongeldig worden gemaakt door de kiezers.

2.3.2 Controleerbaarheid

10. De intentie van de kiezer mag niet worden beïnvloed door het stemsysteem en wordt beschermd tegen ongepaste beïnvloeding.

15. Kiezers moeten kunnen controleren of hun intentie nauwkeurig wordt weergegeven in de uitgebrachte stem en of de verzegelde stem ongewijzigd de elektronische stembus heeft bereikt. Elke ongepaste beïnvloeding die de stemming heeft veranderd, kan worden opgespoord.

17. Het elektronische stemsysteem levert tastbaar bewijs van het feit dat elke authentieke stem correct is opgenomen in de respectieve verkiezingsuitslag. De bewijselementen moeten kunnen worden geverifieerd met middelen die onafhankelijk zijn van het elektronische stemsysteem.

Kiezers kunnen vandaag controleren of hun intentie correct is weergegeven op het papieren stembiljet, maar het is voor hen niet makkelijk om zich ervan te vergewissen dat de elektronische registratie hun stemintentie weergeeft:

- De mogelijkheden om de op het stembiljet afgedrukte QR-code te verifiëren zijn beperkt tot het gebruik van dezelfde software die de QR-code heeft geproduceerd, en die dus mogelijk op dezelfde manier corrupt is en daarom geen onafhankelijk verificatiemiddel vormt.
- Kiezers kunnen niet controleren of de scanner in de urne hun stem correct interpreteert en of de elektronische registratie van hun stem correct is.
- Aan de hand van de audits die momenteel worden verricht, kan niet worden vastgesteld in hoeverre er daadwerkelijk rekening wordt gehouden met de intenties van de kiezers, zoals vermeld in punt *2.2.3*.

De richtlijnen voor het implementeren van de aanbevelingen suggereren het gebruik van individuele en universele controleerbaarheidstechnieken, evenals statistisch significante technieken voor het controleren van papieren stembiljetten.

Een centraal aspect van deze technieken is dat ze verificaties mogelijk maken die onafhankelijk zijn van het elektronische stemsysteem zelf, zoals vereist door aanbeveling 17.

2.3.2.1 In verband met de papieren bewijsstukken

De keuze voor het gebruik van stemmachines in plaats van manueel ingevulde papieren stembiljetten is zeker een controversiële kwestie, zowel in België als in de rest van de wereld.

Terwijl er in de literatuur consensus bestaat over de noodzaak om te beschikken over papieren stembiljetten, is er met name een aanzienlijke controverse geweest in de Verenigde Staten, met de publicatie van een reeks studies en tegenstudies gericht op het aantonen van de mogelijkheid of praktische onmogelijkheid van het detecteren van corrupte stemmachines door middel van de papieren stembiljetten die ze afdrukken [5, 39, 59, 66]. Enerzijds zijn er mensen die beweren dat de enige haalbare optie is om de kiezers (althans zij die dat kunnen) te verplichten om hun stembiljetten manueel in te vullen, en anderzijds mensen die beweren dat het gebruik van stemmachines serieuze voordelen biedt, met name door te voorkomen dat kiezers fouten maken bij het naleven van de regels voor het invullen van stembiljetten.

Veel van deze controverse is gebaseerd op tegenstrijdige studies over het praktische vermogen of onvermogen van kiezers om op te merken dat hun stemmachine een stembiljet afdrukt met een andere stemintentie dan die welke ze hebben uitgedrukt. Dit vermogen hangt natuurlijk af van de instructies die aan de kiezers worden gegeven (herinnering om het papieren stembiljet te controleren), het formaat van het stembiljet (aantal vragen waarover gestemd kan worden, aantal kandidaten dat geselecteerd kan worden) en de overzichtelijkheid van het geproduceerde papieren stembiljet.

Het is duidelijk dat als de kiezers het papieren stembiljet dat door de stemmachine wordt geproduceerd, niet herlezen, of als de kiezers niet oplettend genoeg zijn om fouten te detecteren, de garanties van controleerbaarheid op basis van het papieren stembiljet sterk worden afgezwakt (zonder evenwel te verdwijnen: papier maakt het bijvoorbeeld nog steeds mogelijk om fouten te detecteren tijdens het telproces).

Dit herlezen is des te belangrijker omdat met een zeer klein aantal fouten dat door kiezers wordt gemeld, corrupte machines waarschijnlijk niet kunnen worden geïdentificeerd wanneer ze willekeurig vals spelen: één of twee fouten die door kiezers worden gemeld en die niet meer voorkomen wanneer deze kiezers opnieuw stemmen, kunnen zeer waarschijnlijk worden toegeschreven aan fouten die de kiezers hebben gemaakt bij het uitbrengen van hun eerste stem en niet aan een abnormale werking van de stemmachine.

Dit debat leidt ons tot drie vaststellingen:

1. Het is belangrijk om de kiezers aan te moedigen hun papieren stembiljet te herlezen en eventuele fouten in het stembiljet die ze toeschrijven aan hun stemmachine, te melden. Dit is ook richtinggevend voor de audits.
2. Het is belangrijk om deze verificatie in de praktijk zoveel mogelijk te vergemakkelijken. In deze context lijkt de huidige afdruk op een papier met het formaat van een kassabon niet aangewezen.

3. De Belgische stembiljetten hebben een heel andere vorm dan de Amerikaanse stembiljetten, die soms meerdere tientallen vragen bevatten. Hoewel het denkbaar is dat een kiezer die ongeveer twintig kandidaten van een lijst heeft geselecteerd, niet merkt dat de machine een kandidaat aan deze selectie heeft toegevoegd of eruit heeft verwijderd, lijkt het twijfelachtiger dat de kiezer meer significante manipulaties niet opmerkt, zoals een stemmachine die een stem afdrukt voor een andere lijst dan de lijst die de kiezer heeft geselecteerd. Het lijkt daarom veilig om aan te nemen dat de Belgische kiezers beter dan de Amerikaanse kiezers in staat zullen zijn om fouten op te sporen – een veronderstelling die kan worden geverifieerd aan de hand van tests in reële omstandigheden.

2.3.3 Vertrouwelijkheid van de stemming

19. De elektronische stemming wordt zo georganiseerd dat het geheime karakter van de stemming in alle fasen van de procedure wordt gerespecteerd.

26. De elektronische stemprocedure, in het bijzonder op het moment dat de stemmen worden geteld, wordt zo georganiseerd dat er geen verband kan worden gelegd tussen de niet-verzegelde stem en de kiezer. De stemmen zijn en blijven anoniem.

Het scannen van de stembiljetten op het moment dat ze in de urne worden gedeponeerd, kan aanleiding geven tot ongerustheid over de vertrouwelijkheid van de stemmen. Terwijl bij een conventionele stembus de stembiljetten gemengd kunnen worden voordat ze worden geopend, zien we hier dat de stembiljetten op de machine van de voorzitter worden geregistreerd in de volgorde waarin ze in de urne worden gedeponeerd. Iemand die de identiteit van kiezers noteert en de volgorde waarin ze hun stembiljetten in de stembus doen, zou dan kunnen achterhalen welke (versleutelde) geregistreerde stem bij welke kiezer hoort. De ontsleuteling van de stemmen is vandaag mogelijk met behulp van één enkele sleutel. Deze procedure is voor verbetering vatbaar, zoals ook het College van Deskundigen heeft opgemerkt in zijn aanbevelingen om de stembiljetten niet te scannen wanneer de stembiljetten in de stembussen worden gedeponeerd, maar om dit te doen na de sluiting van de stemming, met name om de bescherming van het stemgeheim te verbeteren [15] [16].

2.3.4 Transparantie

31. De lidstaten moeten transparantie aan de dag leggen bij alle aspecten van het elektronisch stemmen.

Dit artikel versterkt hier de verzoeken om transparantie die door het College van Deskundigen zijn gedaan en die zijn vermeld in punt *2.2.2.1*, betreffende de publicatie van de stemsoftware. In feite gaan deze verzoeken in dezelfde richting als de Raad van Europa in zijn richtlijnen voor de tenuitvoerlegging van artikel 31:

b. De toegang van het publiek tot de verschillende elementen van het elektronische stemsysteem en tot de informatie ter zake, in het bijzonder de documenten, de broncode en de vertrouwelijkheidsovereenkomsten, moet ruim voor het begin van de verkiezingsperiode worden meegedeeld.

2.3.5 Rapportage

39. Het elektronische stemsysteem kan onderworpen worden aan een audit. Het auditsysteem moet open en allesomvattend zijn en de bedreigingen en de mogelijke problemen doeltreffend signaleren.

We hebben hierboven gezien dat de gegevens over de bedreigingen en problemen bij de invoering van het stemsysteem die door de Colleges van Deskundigen zijn geïdentificeerd, afkomstig zijn van de steekproeven die zij in de stembureaus en hoofdbureaus hebben uitgevoerd. Deze gegevens worden niet verrijkt door auditinformatie die systematisch zou worden doorgestuurd vanuit elk stembureau of kantonbureau, in formaten die het gemakkelijk zouden maken om statistieken samen te stellen over deze bedreigingen, problemen en hun impact.

De richtlijnen voor de tenuitvoerlegging van artikel 39 specificeren het volgende:

a. De data, tijdstippen, gebeurtenissen en acties moeten worden vastgelegd in het auditsysteem, meer in het bijzonder: [...]

- elke aanval op het elektronische stemsysteem en de communicatie-infrastructuur ervan;
- de storingen, functionele gebrekkigheden en andere bedreigingen voor het systeem.

De geautomatiseerde tools en procedures van het systeem moeten een snelle en nauwkeurige gegevensanalyse en opstelling van verslagen in dat verband mogelijk maken, zodat er onmiddellijk corrigerende maatregelen kunnen worden genomen.

2.4 BEHEER VAN DE HARDWARE VOOR DE STEMMING

Voordat we de hierboven aangehaalde punten samenvatten, gaan we dieper in op twee aspecten die deel uitmaken van de doelstellingen van deze studie, maar die grotendeels losstaan van de bekommernissen van het College van Deskundigen en de Raad van Europa: de moeilijkheid om de software en de hardware van het elektronisch stemsysteem te onderhouden, die op haar beurt in sommige gevallen gekoppeld is aan het gebruik van systeemspecifieke apparatuur, die moeilijker te onderhouden is.

2.4.1 Moeilijkheden in verband met het onderhoud van de software en de hardware

De beslissing om stemmachines te gebruiken betekent een grote investering en we stellen vast dat de praktische gebruiksperiode van een machine vaak rond vijftien jaar ligt. Dit is een zeer lange periode voor computerapparatuur: het is moeilijk om een garantie van meer dan vijf jaar te krijgen bij de aankoop van professionele laptops. Op het gebied van besturingssystemen bieden de meest genereuze Linux-distributies (inclusief Ubuntu, dat wordt gebruikt in het Smartmatic-systeem) momenteel een uitgebreide ondersteuning, beperkt tot veiligheidslekken, van tien jaar.[12] Dezelfde limiet geldt voor de besturingssystemen 'server' bij Microsoft Windows.[13] Versies voor persoonlijke apparaten, voor zowel Windows als MacOS, werken volgens een strakker rotatieschema – doorgaans drie jaar.[14]

Dit brengt grote problemen met zich mee. Gezien de beperkte levensduur van de besturingssystemen is het noodzakelijk om nieuwe versies van besturingssystemen te installeren op stemmachines als men wil beschikken over een up-to-date systeem vanuit beveiligingsoogpunt.

---

[12] *https://ubuntu.com/security/esm*

[13] *https://learn.microsoft.com/en-us/lifecycle/faq/windows*

[14] *https://endoflife.date/*

De nieuwe versies van de besturingssystemen komen echter regelmatig met nieuwe hardwarevereisten (behoefte aan meer geheugen, enz.), die incompatibel kunnen worden met de hardware die aanwezig is op de stemmachines.

Dezelfde problemen kunnen zich voordoen met de randapparatuur. Door het gebrek aan reserveonderdelen is het moeilijk om apparaten na een paar jaar te repareren. Wanneer een goedkoop randapparaat (printer, enz.) kapot gaat, is vervanging de natuurlijke oplossing. Als de stemmachine echter beperkt blijft tot een ouder besturingssysteem, kan deze vervanging moeilijk worden door het gebrek aan ondersteuning voor recente randapparatuur door het oudere besturingssysteem.

De stemmachines die voor het eerst werden ingezet in 2012, zijn nu bijvoorbeeld extreem moeilijk te repareren en bij te werken, gezien de wijzigingen in de vereisten voor de besturingssystemen die sindsdien hebben plaatsgevonden.

Dit betekent dat deze machines werken op software met bekende, en vaak openbare, beveiligingslekken die niet worden aangepakt. De machines kunnen bijgevolg in wezen willekeurig gedrag vertonen, zelfs als ze geïnstalleerd zijn met authentieke software. Gelukkig zijn de risico's beperkt door de fysieke beveiliging van de machines, die nooit verbonden zijn met een netwerk, geen niet-vluchtig geheugen hebben en niet vrij toegankelijk zijn, noch tijdens de opslag tussen de verkiezingen, noch tijdens de verkiezingen dankzij de behuizing die de toegang tot de meeste toegangspunten van de machine verhindert. We zijn echter nog ver verwijderd van de aanbevolen en goed begrepen praktijken voor IT-risicobeheer.

2.4.2 Gebruik van specifieke hardware

In samenhang met het vorige punt is het huidige systeem deels gebaseerd op specifieke hardware, met name op het niveau van de stembussen die de stembiljetten scannen, maar ook op het niveau van de vaste behuizingen waarin de (standaard)onderdelen van het systeem zijn gemonteerd, die het niet mogelijk maken om het ene onderdeel te vervangen door het andere.

Het gebruik van specifieke hardware verhoogt uiteraard de kostprijs van het systeem en bemoeilijkt reparaties. Specifieke hardware is ook meer dan standaardhardware vatbaar voor kinderziekten. We merkten hierboven op dat de verslagen van het College van Deskundigen melding maken van verschillende moeilijkheden, wijzigingen en verbeteringen aan het systeem voor het scannen, openen en sluiten van de stembussen, om problemen op te lossen die tijdens de eerste implementaties werden vastgesteld.

De stemmachines die in gesloten behuizingen zijn geïntegreerd, hebben zeker het voordeel dat ze gemakkelijk kunnen worden ingezet: er hoeven geen kabels te worden aangesloten tussen de machine, de printer en de kaartlezer wanneer de stembureaus worden ingericht, kabels die altijd het gevaar lopen verloren te gaan of door kiezers te worden losgetrokken. Die vaste behuizingen kunnen de verrichtingen om de in het systeem geïntegreerde hardware up te daten, ook bemoeilijken of verveelvoudigen: het is eenvoudiger om een externe printer te vervangen door een andere die misschien een iets ander formaat heeft, dan om een printer te vervangen die geïntegreerd is in een behuizing en die dus precies voor de voorziene openingen geplaatst moet worden. In de praktijk betekent dit dat er niet moet worden voorzien in generieke printers of scanners uit voorraad, maar dat er een extra voorraad aan stemmachines moet worden aangekocht.

2.5 OVERZICHT VAN DE EVALUATIE VAN HET HUIDIGE STEMSYSTEEM

In het algemeen lijkt het huidige elektronische stemsysteem te voldoen aan de behoeften van de recente verkiezingen: de verkiezingen konden worden gevalideerd en de belangrijkste problemen die bij de verkiezingen van de afgelopen tien jaar werden vastgesteld, waren niet te wijten aan het elektronische stemsysteem Smartmatic.

Toch zijn er een aantal beperkingen en zwakke punten in het huidige elektronische stemsysteem en de manier waarop het wordt geïmplementeerd. Veel daarvan kunnen in verband worden gebracht met technologieën en internationale aanbevelingen voor elektronisch stemmen die nog niet bestonden toen het systeem werd ontworpen en die vandaag bestaan. Andere weerspiegelen structurele problemen op het gebied van stemmachines, waarvan het misschien goed zou zijn om ze vandaag opnieuw op tafel te leggen om te bepalen of er andere oplossingen kunnen worden gevonden.

We benadrukken vijf hoofdlijnen:

1. Beheer van de hard- en de software;
2. Toegankelijkheid van het stemsysteem;
3. Transparantie en veiligheid van de software;
4. Controleerbaarheid en audits van de verkiezing;
5. Rapportage over de werking van het systeem tijdens de verkiezingen.

2.5.1 Beheer van de hard- en de software

Hierbij wordt gestreefd naar het volgende:

1. De uitrol van de stembureaus vereenvoudigen om de in punt *2.2.1.2* genoemde problemen aan te pakken.
2. Vertrekken van hardware die eenvoudig te repareren, te vervangen en te upgraden is, gezien de algemeen waargenomen levensduur van een stemsysteem, zoals besproken in de punten *2.4.1* en *2.4.2*.
3. Hardware kiezen om besturingssystemen en software te laten draaien die voldoen aan de veiligheidsnormen gedurende de levensduur van het systeem, zoals besproken in punt *2.4.1*.
4. De verificatie van de conformiteit van de implementatie van de stemsoftware vergemakkelijken, zoals besproken in punt *2.2.2.2*.

2.5.2 Toegankelijkheid

Hierbij wordt gestreefd naar het volgende:

1. Het stemsysteem toegankelijker maken dan het nu is voor slechtzienden of minder behendige personen die moeite hebben met het selecteren van kandidaten op een scherm, zoals besproken in punt *2.3.1*.

2.5.3 Transparantie

Hierbij wordt gestreefd naar het volgende:

1. Een methodologie voorstellen om de technische elementen van het elektronisch stemsysteem bekend te maken, waardoor het mogelijk wordt om zowel de transparantie als de kwaliteit van het systeem te verbeteren, zoals besproken in de punten *2.2.2.1* en *2.3.4*.

2.5.4 Controleerbaarheid

Hierbij wordt gestreefd naar het volgende:

1. De kiezers in staat stellen om te controleren of hun stemintentie correct is geregistreerd en of hun stem wordt meegenomen, zonder te zijn gewijzigd, tijdens de telverrichtingen, zoals besproken in de punten *2.2.3* en *2.3.2*.
2. Het mogelijk maken deze controles uit te voeren zonder het stemgeheim in gevaar te brengen – het voorgestelde proces moet met name tegemoetkomen aan de bekommernissen die in punt *2.3.3.* worden aangekaart.

2.5.5 Rapportage

Hierbij wordt gestreefd naar het volgende:

1. Eenvoudige rapportagemechanismen opzetten die het mogelijk maken om de ontvangen gegevens efficiënt te compileren, zodat er een duidelijke meting is van het aantal incidenten en hun gevolgen, zoals besproken in de punten *2.2.1.2* en *2.3.5*.

3 TECHNOLOGISCHE ONTWIKKELINGEN

3.1 INLEIDING

Het landschap van de stemtechnologieën is aanzienlijk geëvolueerd sinds de BeVoting-studie uit 2007, die aan de basis ligt van het elektronische stemsysteem dat momenteel in België wordt gebruikt [29].

De ontwikkelingen op het gebied van stemtechnologie zijn vooral gericht op de ontwikkeling en verbetering van technieken waarmee kan worden gecontroleerd of de aangekondigde verkiezingsuitslag wel degelijk juist is. Deze technologische ontwikkelingen beantwoorden aan duidelijke behoeften en de toepassing ervan is een van de internationale aanbevelingen op dit gebied.

Deze controleerbaarheidstechnologieën volgen twee hoofdlijnen die elkaar in ruime mate aanvullen en die we in de volgende punten bespreken.

1. Risicobeperkende audits of *risk limiting audits* (RLA's), die bestaan uit een statistische verificatie dat de aangekondigde verkiezingsuitslag consistent is met het geheel van de papieren stembiljetten die door de stemmachines zijn geproduceerd, door de kiezers zijn geïnspecteerd en in de stembussen aanwezig zijn.

2. Controleerbaarheid van begin tot eind, of *end-to-end verifiability*, die een reeks technieken omvat, over het algemeen gebaseerd op versleuteling, die het mogelijk maken om te controleren of de stembiljetten die door het stemsysteem zijn geproduceerd, niet zijn gewijzigd en of ze correct zijn geteld tijdens het telproces.

Een van de voordelen van het gebruik van een elektronisch stemsysteem is dat het niet nodig is om alle stembiljetten te tellen die door de kiezers worden geproduceerd, dankzij de elektronische registratie en totalisering van de stembiljetten.

Terwijl de handmatige telling haar eigen risico's met zich meebrengt in verband met menselijke fouten en het hanteren van stembiljetten door een groot aantal mensen, brengt de elektronische telling ook risico's met zich mee. Zo kunnen vraagtekens worden geplaatst bij de volgende aspecten van het systeem dat momenteel in België wordt gebruikt:

1. De papieren stembiljetten bevatten twee delen: een samenvatting van de keuzes die leesbaar is voor de kiezer, en een QR-code die deze keuzes codeert en gescand wordt voor de elektronische gegevensinvoer. Een stemmachine die corrupt is, zou een leesbare samenvatting kunnen afdrukken die correct is voor de kiezer, maar een QR-code kunnen produceren die andere keuzes invoert. De kiezer kan deze QR-code niet zelfstandig controleren, maar het is die code die wordt gescand om het stembiljet te tellen.
2. Zelfs als de QR-code correct is, kan de machine van de voorzitter van het stembureau op dezelfde manier corrupt zijn en andere stemmen registreren dan de gescande stemmen.

Natuurlijk worden er maatregelen genomen om deze bekommernissen weg te nemen: de machines worden getest, kiezers kunnen een andere machine gebruiken om te controleren of de QR-code op hun stembiljet wel degelijk overeenkomt met hun stemintentie en er zijn een veilige architectuur en een veilige implementatiemethode ontworpen voor de machines om ervoor te zorgen dat ze niet corrupt raken.

Deze controlemechanismen zijn echter hoofdzakelijk intern aan het systeem, terwijl de Raad van Europa onafhankelijke controlemiddelen aanbeveelt om te voorkomen dat een interne actor het systeem en de verificatiemechanismen zou kunnen beïnvloeden. Hier werken we een voorstel uit voor de integratie in de Belgische verkiezingen van de twee belangrijkste technieken die hiervoor werden ontwikkeld en die al in andere landen worden gebruikt.

3.1.1 Risicobeperkende audit

Zowel de Raad van Europa als de Amerikaanse National Academies (zie onderstaande bespreking) zijn van mening dat het essentieel is om een auditprocedure te implementeren die onafhankelijk is van het elektronische stemsysteem zelf, gebaseerd op de papieren stembiljetten die de kiezers hebben kunnen controleren. Dit is wat een risk limiting audit biedt: door een statistisch significante steekproef van papieren stembiljetten te inspecteren, biedt een risk limiting audit de garantie dat de bekendgemaakte verkiezingsuitslag wel degelijk consistent is met alle beschikbare papieren stembiljetten.

Het feit dat de risk limiting audit vertrekt van de papieren stembiljetten, verleent die audit een grote kracht: er wordt uitgegaan van een tastbaar object dat de kiezers hebben kunnen inspecteren

om zich ervan te vergewissen dat het hun stemintentie goed weergeeft – er is hier geen ruimte voor een machine om vals te spelen zonder dat dit onopgemerkt blijft.[15]

Deze kracht is meteen ook de bron van de belangrijkste zwakte van deze audits: de kwaliteit van de audit hangt volledig af van de kwaliteit van de opvolging van de papieren stembiljetten: als een audit wordt uitgevoerd op basis van papieren stembiljetten die niet authentiek zijn, heeft het resultaat van de audit natuurlijk geen bewijskracht. Erger nog, een dergelijke audit zou zelfs een correcte uitslag ongeldig kunnen maken als de vervalsing van de stembiljetten heeft plaatsgevonden na het tellen.

Het is echter vaak moeilijk om de veiligheid van de opvolging van de papieren stembiljetten te garanderen. In België worden de stembiljetten vervoerd naar de telbureaus en vervolgens naar de kantonhoofdkantoren. Deze transporten worden doorgaans uitgevoerd in privévoertuigen en de urnen zijn normaal verzegeld, maar net als computers zijn zegels niet onschendbaar. De urnen worden ook opgeslagen in afgesloten lokalen voordat ze worden gecontroleerd. Nogmaals, het is moeilijk om te garanderen dat onbevoegden zich geen toegang verschaffen tot deze lokalen.[16]

3.1.2 Controleerbaarheid van begin tot eind

Dit is waar de tweede hoofdlijn van technologische ontwikkeling op het vlak van controleerbaarheid om de hoek komt kijken, namelijk de controleerbaarheid van begin tot eind, die ook wordt aanbevolen door zowel de Raad van Europa als de Amerikaanse National Academies.

Een van de gebruikelijke vormen van deze aanpak van de controleerbaarheid is om elke stemmachine te vragen om, tegelijk met het papieren stembiljet, een trackingnummer te produceren dat een soort vingerafdruk van dit stembiljet vormt. Dit trackingnummer wordt door de kiezer bewaard voor toekomstige controles.

Praktisch gezien heeft dit trackingnummer de vorm van een schijnbaar willekeurige reeks letters en cijfers en/of een QR-code: op basis van cryptografische versleutelingsmechanismen maakt het feit dat men over het trackingnummer van een stembiljet beschikt, het helemaal niet mogelijk om de inhoud van het stembiljet te bepalen. In het bijzonder zou dit trackingnummer kiezers niet in staat stellen om een bewijs te hebben van de inhoud van hun stembiljet, dat gebruikt zou kunnen worden om hun stem te verkopen, of om te reageren op druk die op hen zou kunnen worden uitgeoefend. De cryptografische mechanismen zorgen er echter voor dat het trackingnummer eigenschappen heeft die vergelijkbaar zijn met de eigenschappen die van vingerafdrukken worden

---

[15] Dit kon onlangs worden uitgetest: na een fout in de configuratie van de stemmachines die niet werd opgemerkt tijdens de verschillende tests, drukten de stemmachines die werden gebruikt bij de verkiezingen van november 2023 in Northampton County, PA, VS, verkeerde stembiljetten af voor bepaalde stemkeuzes. Deze fouten werden binnen enkele minuten na de opening van de stemverrichtingen door de kiezers ontdekt. Hier vindt u een nauwkeurig verslag met een beschrijving van dit probleem: *https://securiosa.com/posts/northampton_problems_2023.html.*

[16] Paul Burke heeft bijvoorbeeld een webpagina samengesteld waarin verschillende manieren worden gedocumenteerd om veel van de traditionele fysieke beveiligingsmaatregelen die bij verkiezingen gebruikt, te omzeilen: *http://www.votewell.net/locks.html*.

verwacht: het is technisch onmogelijk om twee stembiljetten met hetzelfde trackingnummer te produceren. In dit opzicht doet dit trackingnummer veel meer dan bijvoorbeeld een trackingnummer van een postpakje, dat op geen enkele manier de inhoud van het pakje garandeert. Het trackingnummer garandeert de kiezers dus dat hun stembiljet geregistreerd en intact is, maar stelt hen niet in staat om aan een derde te laten zien op wie ze gestemd hebben.

Het bestaan van deze trackingnummers maakt het mogelijk om een verkiezingsverslag te publiceren met de lijst van de trackingnummers van alle stembiljetten die zijn opgenomen in de elektronische telling van de verkiezing, zonder de inhoud van de stembiljetten te onthullen. Die lijst kan worden geraadpleegd door alle kiezers die dat willen, zodat ze zich ervan kunnen vergewissen dat hun stembiljet correct is geteld. Andere cryptografische technieken maken het bovendien mogelijk om te controleren of de aangekondigde verkiezingsuitslag een accurate weergave is van alle gepubliceerde trackingnummers – zonder ooit ook maar de minste informatie te onthullen over de inhoud van de stembiljetten die bij deze trackingnummers horen.

Omdat deze controleerbaarheidstechnieken hoofdzakelijk digitaal zijn, dekken ze slechts in beperkte mate de vraag of het trackingnummer dat aan kiezers wordt verstrekt, hun stemintentie correct weerspiegelt. Zoals in het geval van de bovengenoemde QR-code zou de stemmachine een trackingnummer kunnen produceren dat overeenkomt met een andere stemintentie. Omdat dit trackingnummer zo ontworpen moet zijn dat het de inhoud van de stem niet onthult, heeft de kiezer dan geen directe manier om erachter te komen – er bestaan technieken om kiezers in staat te stellen dit type fraude te detecteren, maar het is moeilijker om ze met succes in te zetten. We gaan er hierna dieper op in.

We zien hier echter de complementariteit tussen de risk limiting audit en de controleerbaarheid van begin tot eind opduiken: de risk limiting audit maakt het mogelijk om ervoor te zorgen dat een set papieren stembiljetten die de kiezers konden inspecteren, consistent is met de verkiezingsuitslag, in de veronderstelling dat de stembiljetten die in de audit worden gebruikt, inderdaad de stembiljetten zijn die de kiezers hebben geïnspecteerd. End-to-end controle zorgt ervoor dat de digitale stembiljetten die zijn gegenereerd op het moment van stemmen, maar waarvan de inhoud niet rechtstreeks kon worden geïnspecteerd door de kiezers, wel degelijk zijn meegenomen in de telling die tot de verkiezingsuitslag heeft geleid.

Geen van beide benaderingen is vandaag in de praktijk onfeilbaar. Om echter ongemerkt een vals verkiezingsresultaat te produceren, moet men, wanneer deze benaderingen worden ingezet, *consistent* kunnen valsspelen, zowel bij het traceren van de papieren stembiljetten als bij het genereren van de elektronische stembiljetten, zodat beide vormen van valsspelen leiden tot hetzelfde valse resultaat, in ieder geval met een zeer hoge waarschijnlijkheid. Dit is aanzienlijk moeilijker dan valsspelen op slechts één van die twee wegen, elektronisch of op papier.

Deze twee benaderingen zullen zeker ook de veiligheid van de huidige systemen verbeteren. In het elektronische stemsysteem dat momenteel in België wordt gebruikt, zal het bij gebrek aan een statistisch significante controle van de papieren stembiljetten moeilijk zijn om een corrupt computersysteem op te sporen: we verlaten ons sterk op het vertrouwen dat we hebben in de veiligheid van de procedures voor de implementatie van het systeem. En in het op systeem van stemmen op papier zal het, zonder de mogelijkheid om de stembiljetten van begin tot eind te traceren, erg moeilijk zijn om een vervanging van stembiljetten in een stembus, bijvoorbeeld tijdens het transport of het tellen, te detecteren: we baseren ons sterk op het vertrouwen dat we hebben in

de veiligheid van de procedures voor het traceren van stembiljetten. We suggereren uiteraard niet dat dit vertrouwen in een van beide gevallen misplaatst zou zijn. Gezien de belangen die op het spel staat, lijkt het wel aangewezen om mechanismen in te voeren om te controleren of dit vertrouwen inderdaad gewettigd is.

3.2 RISICOBEPERKENDE AUDIT

3.2.1 Inleiding

3.2.1.1 Wat houdt een risicobeperkende audit in?

Een risicobeperkende audit, ook bekend als '*risk limiting audit*' of RLA in het Engels, is een auditprocedure met als doel te garanderen dat de aangekondigde uitslag van een verkiezing correct is. Elke procedure voor het tellen van een groot aantal stembiljetten is complex en er kunnen fouten optreden, zowel in een telproces, een scanproces of een proces voor de invoer van totalen in een computer. De gebruikte softwareprogramma's kunnen fouten bevatten en een IT-infrastructuur kan worden gecorrumpeerd door kwaadwillende actoren.

De implementatie van een RLA voldoet aldus aan de aanbevelingen van de Raad van Europa. De "Lignes directrices pour la mise en œuvre des dispositions de la recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique" vermelden immers in artikel 15.b [22] [vrij vertaald]:

Er moet een verplichte telling van de stemmen worden uitgevoerd op basis van deze tweede drager [d.w.z. papier] in een statistisch significant aantal willekeurig gekozen stembureaus, met name voor de stemmachines en de apparaten voor het optisch lezen van de stembiljetten.

Criteria zoals het percentage betrokken stemmen of het aantal stembureaus waar de telling zal plaatsvinden, hun aanwijzing, enz. moeten op nationaal niveau worden vastgesteld. De criteria moeten ervoor zorgen dat het algemene doel van vrije verkiezingen wordt bereikt.

Door een rigoureus vastgestelde statistische garantie te bieden, wordt de uitvoering van een RLA vaak voorgesteld als een 'gold standard' om vast te stellen dat het resultaat dat aan het einde van een telprocedure wordt bekendgemaakt, overeenstemt met het geheel van beschikbare papieren stembiljetten.

De garantie die een RLA biedt, is niet absoluut: ze is probabilistisch, waardoor er een zeker risico bestaat dat de audit het niet mogelijk maakt een onjuist resultaat te corrigeren – en dat is wel degelijk het soort garantie dat de Raad van Europa voor ogen heeft. Een RLA zal echter nooit een correct resultaat als onjuist bestempelen. De limiet voor het risico op de bevestiging van een onjuist resultaat kan vooraf worden gekozen: bijvoorbeeld 10%, 1% of 0,1%. Hoe lager het aanvaarde risico, hoe groter de inspanning die nodig is om de auditprocedure uit te voeren. Het accepteren van een probabilistische garantie betekent dat de implementatie van een RLA meestal erg efficiënt is: in de meeste gevallen hoeven er maar enkele tientallen of enkele honderden stembiljetten gecontroleerd te worden tijdens het auditproces, zelfs als er miljoenen mensen hebben gestemd. Omgekeerd zou de enige manier om een absolute, niet-probabilistische garantie voor een correcte uitslag te hebben, een hertelling van alle stembiljetten zijn, ervan uitgaande dat het mogelijk is om dit foutloos te doen, zelfs als het aantal stembiljetten enorm is.

3.2.1.2 Hoe verloopt een RLA?

Het uitgangspunt voor een RLA is een set papieren stembiljetten, waarvan gecertificeerd is dat ze de intenties van de kiezers correct weergeven, en een uitslag die bekend wordt gemaakt op basis van een procedure voor het tellen van deze stembiljetten.

Het is natuurlijk van cruciaal belang om ervoor te zorgen dat de stembiljetten die voor de RLA worden gebruikt, authentiek zijn: als ermee geknoeid is, kan de audit een onjuist resultaat bevestigen of zelfs een juist resultaat ongeldig maken als er tussen de telling en de audit met de stembussen geknoeid is. Het verrichten van een RLA doet dus niets af aan de noodzaak om strenge maatregelen ter controle van de stembussen te handhaven, om te voorkomen dat de inhoud ervan wordt gewijzigd. Deze vereiste is natuurlijk al aanwezig bij de verkiezingen die geen gebruik maken van RLA's.

Deze stembiljetten moeten op een gestructureerde manier worden georganiseerd. Daarom moet er een verkiezingsmanifest zijn, waarin is vermeld hoeveel stembussen of enveloppen met stembiljetten uit elk stembureau afkomstig zijn en hoeveel stembiljetten er in elke stembus of envelop zitten. Het opstellen van dergelijke documenten is gebruikelijk bij de Belgische verkiezingen. Deze organisatie van de stembiljetten maakt het mogelijk om bijvoorbeeld het 21e stembiljet uit de 4e stembus van stembureau nummer 8 te halen, als de auditprocedure dat vereist. De audit kan nog veel efficiënter verlopen als er aanvullende informatie beschikbaar is, zoals een manifest dat de vermoedelijke inhoud van elk stembiljet aangeeft (bijvoorbeeld: volgens het manifest bevat het 21e stembiljet in de 4e stembus van het 8e stembureau een stem voor partij *A*).

Het doel van een RLA is om te bevestigen dat de aangekondigde verkiezingsuitslag correct is. Een RLA zal echter niet proberen het exacte aantal stemmen te bevestigen dat een partij of een kandidaat heeft gekregen: de RLA probeert te bevestigen dat het aantal zetels dat aan een partij is toegewezen, correct is, of dat een bepaalde kandidaat daadwerkelijk meer stemmen heeft gekregen dan een andere kandidaat. Het bevestigen van het exacte aantal ontvangen stemmen zou de audit immers extreem inefficiënt maken.

De efficiëntie van de audit hangt af van meerdere factoren. Ze hangt in de eerste plaats af van de gekozen risicolimiet. Sommige rechtsgebieden accepteren een risico van ongeveer 10%, terwijl andere het risico voor bepaalde verkiezingen hebben verlaagd tot 0,1%. De efficiëntie van de audit hangt dan af van de verkiezingsmarge, die een maat is van het aantal stembiljetten dat bij een verkiezing zou moeten worden gewijzigd om de uitslag te veranderen (bijvoorbeeld het aantal zetels dat aan een partij wordt toegewezen). Als het aanvaarde risico en de verkiezingsmarge hoog zijn, kan de uitslag worden bevestigd door een belachelijk klein aantal stembiljetten te inspecteren: vaak slechts enkele tientallen stembiljetten, zelfs voor een verkiezing met miljoenen kiezers. Als het aanvaarde risico gering is en/of de verkiezingsmarge (zeer) gering, is het in extreme gevallen mogelijk dat de RLA leidt tot een volledige handmatige hertelling van de stembiljetten.

Zodra het verkiezingsmanifest is vastgesteld, het risico is gekozen en de verkiezingsmarge is berekend, kan de RLA beginnen. Er wordt meestal gebruikgemaakt van een IT-tool (waarvan er steeds meer zijn, in open source) om te bepalen welke stembiljetten moeten worden gecontroleerd. Die tool zal op een controleerbare en transparante manier het aantal en de locatie aangeven, volgens het verkiezingsmanifest, van de stembiljetten die gecontroleerd moeten worden. Zo kan het gebeuren dat bijvoorbeeld stembiljet 21 van de 4e urne van stembureau 8, stembiljet 43 van de 6e

urne van stembureau 14 enz. moeten worden gecontroleerd. Deze inspectie kan verschillende vormen aannemen, afhankelijk van de beschikbare informatie: ofwel wordt eenvoudigweg de inhoud van het aangeduide stembiljet in het systeem ingevoerd (dan hebben we het over een *ballot-polling audit*) ofwel, als het systeem al de vermoedelijke inhoud van elk stembiljet bevat, wordt nagegaan of die conform is (dan hebben we het over een *ballot-comparison audit*). In het geval van non-conformiteit past het systeem het aantal eruit te pikken stembiljetten aan om te bepalen of deze non-conformiteit een op zichzelf staand geval is, of deel uitmaakt van een geheel van non-conformiteiten van voldoende belang om het resultaat van de verkiezing te wijzigen. Als er een groot aantal non-conformiteiten wordt gedetecteerd, zal het aantal eruit te halen stembiljetten het totale aantal stembiljetten benaderen en zal een volledige hertelling efficiënter zijn. Met die hertelling zal het correcte resultaat kunnen worden vastgesteld. Een RLA eindigt daarom op een van de volgende twee manieren: ofwel, en in de meeste gevallen, wordt de uitslag van de verkiezing bevestigd, doorgaans na controle van een klein aantal stembiljetten, ofwel er is een volledige hertelling van de stembiljetten nodig, die de aanvankelijk bekendgemaakte uitslag bevestigt of ongeldig maakt.

3.2.1.3 Over welke resources beschikken we op het vlak van RLA's?

Academische literatuur

RLA's zijn een relatief recente technologie: de eerste beschrijving van een RLA vinden we in een artikel van Philip B. Stark, gepubliceerd in 2008 [57]. Sindsdien wordt er elk jaar een groot aantal wetenschappelijke artikelen gepubliceerd, met als doel om steeds meer uiteenlopende scenario's te kunnen beheren (verkiezingen waarbij verschillende stemmethoden worden gebruikt, waarbij de methoden voor het tellen en opslaan van de stembiljetten per district verschillen, enz.) en om de nodige inspanningen tijdens de audit om een gegeven risicolimiet te bereiken, zo klein mogelijk te houden.

Gezien het snelle tempo waarin de literatuur evolueert, zullen we in dit document geen specifieke methode aanbevelen om in België te gebruiken. In plaats daarvan stellen wij ons tot doel om de haalbaarheid van RLA's in de Belgische context te bepalen, door de resultaten te beoordelen die zouden kunnen worden verkregen met de beste huidige methoden. Dit zal een bovengrens stellen aan de te leveren inspanningen, en we verwachten dat de vooruitgang in het onderzoek het snel mogelijk zal maken om het nog beter te doen, wanneer de beslissing over de te gebruiken methode concreet aan de orde is, hetzij ten vroegste voor de verkiezingen van 2029.

Uitrol

Het hoge tempo waarin de academische literatuur zich ontwikkelt, neemt niet weg dat tal van vormen van RLA's reeds een hoge maturiteitsgraad hebben bereikt en dat het gebruik ervan in de Verenigde Staten algemeen wordt aanbevolen. Zo lezen we in het verslag "Securing the Vote: Protecting American Democracy" van de Amerikaanse National Academies dat in 2018 is gepubliceerd [45]:

States should mandate risk-limiting audits prior to the certification of election results. With current technology, this requires the use of paper ballots.

States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.

State and local jurisdictions purchasing election systems should ensure that the systems will support cost-effective risk-limiting audits.

De strategie die we voorstellen, sluit aan bij deze aanbevelingen.

In de praktijk vonden de eerste RLA-proeftests plaats vanaf 2008 in drie county's in de staat Californië [36]. Talrijke andere pilots volgden, met name in de staat Colorado vanaf 2010 [60], waar RLA's sinds 2017 verplicht zijn. Andere staten hebben dit voorbeeld inmiddels gevolgd: RLA's zullen wettelijk verplicht zijn voor de presidentsverkiezingen van november 2024 in de staten Colorado, Georgia, Nevada, Pennsylvania, Rhode Island en West Virginia [65]. Hierbij komen uiteraard nog een paar andere staten waar RLA's worden uitgevoerd op initiatief van de county's (Californië, Michigan, Washington, enz.). Op die manier konden de resultaten van honderden verkiezingen worden bevestigd. In Europa is dit type audit echter nog niet wijdverbreid, hoewel er sinds 2015 een proefproject plaatsvond tijdens verkiezingen in Denemarken [54].

Om een idee te krijgen van de omvang van de taak die een RLA kan vertegenwoordigen, kunnen we het "Audit Center" van de staat Colorado [21] raadplegen, dat de audits die sinds 2017 in deze pioniersstaat zijn uitgevoerd, documenteert. Als we kijken naar de verkiezingen van 2023, zien we dat in de 63 county's die RLA's hebben verricht, het verwachte aantal te inspecteren stembiljetten varieert tussen 17 en 346 voor een risicolimiet van 3%, vastgesteld door de staat (voor de eerste pilots in deze staat was gekozen voor een limiet van 9%), en worden verkregen als onderdeel van "ballot-comparison audits", die bijzonder efficiënt zijn. Andere staten maken andere keuzes: Californië legt bijvoorbeeld een limiet van 5% op aan de county's die ervoor kiezen om een RLA te verrichten. Dezelfde limiet van 5% geldt in de staat Georgia. De verwachting is wel dat in België vaak een veel groter aantal stembiljetten zal moeten worden onderzocht, vanwege de zeer geringe marges die regelmatig worden geobserveerd.

Zo deden zich in de Verenigde Staten extreme gevallen voor, waar de marges zo klein waren dat de papieren stembiljetten volledig moesten worden geteld. Een opvallend voorbeeld is dat van de staat Georgia, waar een volledige hertelling van 5 miljoen stembiljetten nodig was voor de presidentsverkiezingen van 2020 [34]. De audit van de verkiezingen van 2022 verliep zonder problemen. (In België zijn de verkiezingen verdeeld in kieskringen, zodat een volledige hertelling alleen zou worden georganiseerd op het niveau van de kieskring, en niet op gewestelijk of landelijk niveau.)

Informaticatools

De hierboven beschreven audits worden uitgevoerd met behulp van software waarmee, op basis van manifesten, het genomen risico en de reeds uitgevoerde inspecties, wordt bepaald welke stembiljetten nog moeten worden geïnspecteerd of dat de audit kan worden afgesloten. Deze tools zijn meestal van het type 'open source' en worden geïmplementeerd door de personen die instaan voor het organiseren van de verkiezing, vaak met de hulp van deskundige ondernemingen die ondersteuning bieden bij het implementeren van die tools.

Op vandaag is de meest gebruikte tool Arlo, een open source tool die is geïmplementeerd in elf Amerikaanse staten en is ontwikkeld door VotingWorks, een non-profitorganisatie (501(c)(3) in Amerikaanse termen):

https://www.voting.works/risk-limiting-audits

Arlo lijkt geleidelijk in de plaats te komen van de oudere tools, zoals ColoradoRLA, dat tot 2018 werd gebruikt voor de RLA's van Colorado.

Philip Stark stelt ook een aantal open source tools, ontwikkeld in een academische context, beschikbaar via zijn GitHub-account:

https://github.com/pbstark/

Veel van die tools zijn in het verleden gebruikt in proefprojecten, en Arlo is grotendeels gebaseerd op methoden die zijn ontworpen door Philip Stark. Andere tools zijn recenter en bieden meer geavanceerde functies en prestaties. We denken hier in het bijzonder aan de SHANGRLA-tool, die kan worden aangepast aan een zeer groot aantal telmethoden, waaronder de D'Hondt-methode, die in België wordt gebruikt [58]. Deze tool wordt sinds 2019 getest, met name door de stad San Francisco, die bij bepaalde verkiezingen alternatief stemmen toepast (een stemmethode waarbij kiezers een rangorde van kandidaten, vaak gedeeltelijk, voorstellen op hun stembiljet) [6].

Wettelijk kader

Het wettelijke kader voor audits verschilt sterk van staat tot staat. Een 'Audit Law Database' is beschikbaar op de website van Verified Voting op het volgende adres:

https://verifiedvoting.org/auditlaws/

3.2.1.4 Nog een stapje verder ...

De invoering van RLA's ging gepaard met de publicatie van tal van handleidingen, ervaringsverslagen, video's, enz. We halen hier in het bijzonder de volgende bronnen aan.

- De Amerikaanse National Association of Election Officials heeft tussen 2019 en 2021 een reeks van vier "Knowing It's Right"-gidsen gepubliceerd om de implementatie van RLA's te ondersteunen [41-44].
- Het Brennan Center for Justice heeft in 2019 een verslag gepubliceerd met als titel "Pilot Implementation Study of Risk-Limiting Audit Methods in the State of Rhode Island" [52].
- Het Carter Center, dat sinds 2020 de RLA's in Georgia heeft geobserveerd, heeft in 2022 ook een handleiding gepubliceerd met de titel "Risk-Limiting Audits: A Guide for Election Observation Efforts" [10].

3.2.2 Een RLA-strategie voor België

Het implementeren van RLA's voor de verkiezingen in België is een proces dat geleidelijk moet worden uitgevoerd en waarbij een brede waaier aan actoren moet worden betrokken, anders lopen we het risico dat we de beoogde doelstellingen missen: op een efficiënte manier meer vertrouwen in verkiezingsuitslagen bereiken.

3.2.2.1 Voortbouwen op elders opgedane ervaring

De ervaring van het groeiende aantal Amerikaanse staten dat RLA's heeft ingezet – en nog steeds inzet – biedt een strategische basis voor de implementatie van dit type audits. De Belgische verkiezingen verschillen evenwel op een aantal belangrijke punten van de Amerikaanse verkiezingen. Twee aspecten lijken bijzonder belangrijk:

1. De verkiezingen worden in België veel minder frequent georganiseerd dan in de Verenigde Staten: wij houden (normaal gezien) gecombineerde verkiezingen in cycli van vijf of zes jaar, terwijl veel Amerikaanse staten twee of drie keer per jaar verkiezingen houden. Zo kenden we tussen 2000 en 2023 elf verkiezingsdagen in België.
2. De vorm van onze stembiljetten is heel anders: wij kiezen een groot aantal vertegenwoordigers voor een klein aantal assemblees, terwijl de stembiljetten die de Amerikaanse kiezers voorgelegd krijgen, vaak enkele tientallen vragen bevatten, afhankelijk van de woonplaats van de kiezers, met over het algemeen een klein aantal mogelijke keuzes bij elke vraag.

De frequentie van de verkiezingen heeft uiteraard een grote invloed. Enerzijds vereisen minder frequente verkiezingen minder frequente auditinspanningen, wat de totale last van het organiseren van verkiezingen in een land als België beperkt. Het nadeel is dat een zeldzamere organisatie minder mogelijkheden biedt om ervaringen op te doen met verkiezingen. Dit houdt in dat er minder mogelijkheden zijn om pilots van nieuwe processen onder reële omstandigheden te testen en dat er een grotere rotatie is in de actoren die betrokken zijn bij de verkiezingspraktijk. Het belang van een goede documentatie van de procedures zal des te groter zijn.

De vorm van onze stembiljetten heeft op zijn beurt ook voor- en nadelen. Elk van onze stembiljetten heeft betrekking op één enkele verkiezing. Elke verkiezing kan dus afzonderlijk worden geauditeerd. Op deze manier kan België de complexiteit vermijden die gepaard gaat met de Amerikaanse stembiljetten, die op een en hetzelfde stembiljet de keuzes van de kiezers voor verschillende afzonderlijke verkiezingen bevatten, wat de complexiteit van de audits aanzienlijk vergroot. Het grote aantal te verkiezen personen en de telmethodes die we gebruiken, betekenen echter dat de foutmarges binnen elk van onze verkiezingen doorgaans kleiner zijn, waardoor er minder ruimte is voor fouten en de audits mogelijk veeleisender zijn wat betreft het aantal te controleren stembiljetten.

Deze aspecten zijn belangrijk, maar het blijft een feit dat de bestaande praktijk zeker een leidraad kan vormen voor België wat zijn uitrolstrategie betreft.

3.2.2.2 Tijdlijn

Een werkgroep opzetten

Een belangrijke eerste stap is het samenbrengen van mensen met competenties in het organiseren van verkiezingen op alle niveaus om samenwerking op te bouwen rond de implementatie van RLA's.

Deze werkgroep moet actoren samenbrengen met ervaring in de verschillende fasen van het proces inzake de telling, de totalisering van de verkiezingsresultaten en het beheer van de stembiljetten. We denken in het bijzonder aan personen:

- van de directie Verkiezingen van de FOD Binnenlandse Zaken,
- van de diensten die instaan voor de verkiezingen op gewestelijk niveau,
- met ervaring in hoofdkantoren van kieskringen,
- met ervaring in kantonhoofdkantoren,
- met ervaring in telkantoren.

Deze actoren, en wellicht nog andere die nog moeten worden geïdentificeerd, zijn van essentieel belang om de RLA in elke fase efficiënt te organiseren.

Die groep moet zeker ook de volgende leden bevatten:

- een of meer personen met de nodige juridische deskundigheid om de wijzigingen te identificeren die in de wetgeving moeten worden aangebracht om de geplande audits te kunnen uitvoeren,
- een of meer mensen met ervaring op het vlak van RLA's, inclusief de informaticatools die zullen worden ontwikkeld en gebruikt ter ondersteuning van die audits,
- een of meer personen die verantwoordelijk zijn voor de communicatie over de activiteiten van de groep,
- een persoon die de leverancier van de te auditeren stemmachines vertegenwoordigt, of die de contacten met die leverancier kan verzorgen.

Het doel van deze werkgroep is om concreet een procedure op te stellen voor de implementatie van RLA's, eerst in de vorm van een proefproject, daarna in algemene vorm, en om de communicatiestrategie te bepalen die moet worden gevolgd ten aanzien van de politieke actoren en het grote publiek, evenals de organisatie van de opleiding van de actoren uit het werkveld.

Hieronder stellen we een traject voor naar een veralgemeende invoering van RLA's in België. We beginnen met het voorstellen van verschillende stappen op dat traject. Vervolgens stellen we een ruwe schets voor van de manier waarop de RLA's georganiseerd zouden kunnen worden.

Het proces simuleren op beperkte schaal

De zeldzaamheid van de verkiezingen in België betekent dat er weinig mogelijkheden zijn om te experimenteren met nieuwe procedures op het terrein. Om het auditproces een eerste mate van maturiteit te verlenen tijdens tests op het terrein, is het nuttig om dit auditproces op beperkte schaal te testen op basis van fictieve stembiljetten. Een mogelijke schaal zou ongetwijfeld het werken met 5.000 tot 10.000 stembiljetten zijn: een dergelijk formaat zou een goed gevoel geven van de complexiteit van het vinden en inspecteren van stembiljetten onder reële omstandigheden, zonder dat daarvoor een buitensporige logistiek nodig is.

Die tests zouden kunnen worden uitgevoerd door actoren van buiten de werkgroep. De werkgroep zelf zou aanwezig zijn als waarnemer. Het is zinvol om de aanwezigheid van externe waarnemers te beperken, zodat de aanwezigen zich volledig vrij voelen om eventuele misverstanden, kritiek of complimenten te uiten en om aan te zetten tot een eerlijk debat dat leidt tot een verbetering van de procedures.

Ze kunnen ook een eerste idee geven van de tijd die nodig is om een audit in een reële situatie uit te voeren.

Eerste pilot

Zodra er voldoende vertrouwen is in de organisatie van het RLA-proces door middel van simulaties, kan een eerste pilot op reële schaal worden georganiseerd. Ons doel hier is om de pilot uit te voeren op de schaal van een middelgrote kieskring.

Deze eerste pilot zou kunnen plaatsvinden net nadat de resultaten van een verkiezing zijn gevalideerd: zo vermijden we dat de stembiljetten te lang moeten worden bewaard, en kan de dynamiek van de ten einde lopende verkiezing worden bewaard. Bovendien zorgt het uitvoeren van de pilot na de validatie ervoor dat deze eerste pilot, waarbij authentieke stembiljetten worden verwerkt, het normale validatieproces van de verkiezingen niet kan verstoren.

De overgang naar een pilot op reële schaal stelt ons in staat om de documentatie en het opleidingsproces van de actoren te testen: de audit van enkele honderdduizenden stembiljetten vereist de deelname van een groter aantal personen, die een opleiding moeten krijgen. De pilot zal ook worden benut om de logistiek te testen die komt kijken bij het traceren en beheren van honderdduizenden stembiljetten.

Ook op dat vlak verdient het aanbeveling om die pilot uit te voeren in een omgeving die de vrije en constructieve meningsuiting van de verschillende deelnemers aanmoedigt.

De verschillende processen zullen worden aangepast aan de hand van de lessen die tijdens de pilot worden geleerd.

Tweede pilot

Een tweede pilot zal hoogstwaarschijnlijk nuttig blijken om het proces te verfijnen. In dit stadium kan worden overwogen om de audit onder reële omstandigheden uit te voeren, voordat de resultaten worden gecertificeerd. Het niveau van vertrouwen in het proces moet dan al erg hoog zijn: er moet aanvaard zijn dat de stembiljetten gemanipuleerd worden in het kader van een audit voorafgaand aan de certificering, en men moet voorbereid zijn op het feit dat de audit de verwachte resultaten mogelijk niet valideert. De aanpassingen aan de wetgeving zullen bijgevolg wellicht nog groter zijn.

In dit stadium, en vooral als deze pilot plaatsvindt voordat de resultaten zijn gecertificeerd, is het belangrijk om waarnemers in te zetten, volgens criteria die vergelijkbaar zijn met de criteria die in de telbureaus worden gebruikt.

Veralgemening

Op basis van succesvolle pilots zouden RLA's veralgemeend kunnen worden ingezet. Ze kunnen plaatsvinden in aanwezigheid van waarnemers, onder dezelfde omstandigheden als in een traditioneel telbureau.

3.2.2.3 Organisatorische aspecten

Targeting van de audits

Een eerste praktische beslissing is de targeting van de audit: welke verkiezing willen we auditeren en voor welke gedetailleerdheid van resultaten?

De eerste keuze is welke verkiezingen als eerste worden geauditeerd. Wij bevelen aan te beginnen met de **federale verkiezingen**:

- deze keuze betekent dat de RLA-strategie kan worden op één plaats die alle Belgen bereikt en vervolgens kan doorsijpelen naar de andere verkiezingen, op basis van de opgedane ervaring.
- Deze verkiezingen worden georganiseerd rond 11 kieskringen, tegenover 4 voor de Europese verkiezingen, die ook heel België beslaan, waardoor we te maken hebben met kleinere kieskringen, wat de controle vergemakkelijkt.

Het organiseren van pilots in het kader van gewestelijke, provinciale of gemeenteraadsverkiezingen zou het niet mogelijk maken om op een even directe manier nuttige ervaring op te doen voor alle Belgen. De gemeenteraadsverkiezingen zouden het voordeel kunnen hebben dat er per verkiezing een klein aantal stembiljetten moet worden beheerd, wat de logistiek vereenvoudigt. Het kleinere aantal kiezers dat bij elke verkiezing betrokken is, betekent echter dat de kennis die wordt opgedaan in pilots voor deze verkiezingen, veel vragen open zou laten voor een audit op het niveau van een volledige kieskring. Bovendien betekenen de kleine kiesmarges in deze stemmingen in combinatie met het kleine aantal kiezers dat volledige hertellingen waarschijnlijk regelmatig nodig zullen zijn, waardoor de voordelen van RLA's in deze context beperkt zijn.[17]

Wat de mate van detail betreft, stellen we voor om te focussen op de **zetelverdeling tussen de partijen**. Het zou natuurlijk ook interessant zijn om de zetelverdeling tussen de kandidaten te controleren, maar hier zien we twee problemen:

1. De marges waarmee de kandidaten worden verkozen, zijn ook erg klein, en rekening houden met de zetelverdeling leidt tot een gevoelige toename van het risico dat de audit moet worden afgesloten met een volledige hertelling van de stembiljetten. Dit lijkt niet wenselijk, vooral niet voor de proefprojecten.
2. In de context van traditioneel stemmen op papier, dat zal moeten worden geïntegreerd in de RLA in alle kieskringen waar zowel elektronisch als op papier wordt gestemd, worden de getelde stembiljetten vaak gerangschikt en gearchiveerd per partij. Deze indeling levert een aanzienlijke efficiëntiewinst op voor de auditprocedure, in zoverre de telprocedure op die

[17] Na de verkiezingen van 2019 zijn er kiesmarges berekend voor alle Waalse gemeenten: *https://decryptage.be/communes_wallonnes.html.*

manier een verbintenis creëert over de inhoud van de stembiljetten (in ieder geval op partijniveau), die het mogelijk maakt om efficiënte technieken van een ballot-comparison audit toe te passen. De verificatie van de inhoud van de stembiljetten wordt ook sterk vereenvoudigd als het gewoon een kwestie is van controleren of een stembiljet een geldige stem voor een bepaalde partij bevat.

Dit tweede punt zal in de komende jaren waarschijnlijk veranderen: de PATSY-software, die vanaf 2024 in Wallonië wordt geïmplementeerd, zorgt voor een elektronische registratie van de inhoud van elk individueel stembiljet. Een kieskring die gebruikmaakt van PATSY, zou in feite kunnen beschikken over een directe link tussen de papieren stembiljetten en hun elektronische invoer, op voorwaarde dat die kring ervoor zorgt dat de link tussen de papieren stembiljetten en hun elektronische registratie behouden blijft (door een nummer aan te brengen op elk stembiljet, of gewoon door de stembiljetten op te slaan in de volgorde waarin ze ingevoerd werden, in enveloppen van bescheiden omvang (een vijftig- of honderdtal stembiljetten)). Een veralgemeend gebruik van PATSY of andere gelijkwaardige software, samen met passende maatregelen voor de bewaring van de stembiljetten, zou het dus mogelijk kunnen maken om een ballot-comparison audit van de stembiljetten uit te voeren, ook wat betreft de zetelverdeling op het niveau van de kandidaten. (Dit verandert natuurlijk niets aan de kleine marges tussen de verkozenen.)

Auditmethode

Zoals hierboven vermeld, zijn er verschillende families van RLA's:

1. de audits via vergelijking van stembiljetten: *ballot-comparison audits*, waarbij papieren stembiljetten eruit worden gepikt om te controleren of ze correct zijn geïnterpreteerd in de elektronische verslagen van de telling;
2. audit door monsterneming van de stembiljetten: *ballot-polling audits*, waarbij papieren stembiljetten eruit worden gepikt en er een nieuwe telling wordt verricht op basis van die biljetten, waarbij ervoor wordt gezorgd dat de trend die in de steekproef wordt waargenomen, overeenkomt met de uitslag die voor alle stembiljetten is bekendgemaakt;
3. audits door vergelijking van batches van stembiljetten: *batch-comparison audits*, waarbij alle stembiljetten in een bepaald aantal enveloppen opnieuw worden geteld (elke envelop bevat naar verwachting maximaal een paar honderd stembiljetten) en waarbij wordt gecontroleerd of het opnieuw getelde resultaat voor elke envelop overeenkomt met wat werd verwacht.

We bevelen aan dat alles in het werk wordt gesteld voor de uitvoering van **ballot-comparison audits in België**. Dit is immers de methode waarbij, vaak verreweg, het kleinste aantal papieren stembiljetten moet worden gehanteerd. Gezien de vaak lage marges in België is het cruciaal om over efficiënte auditmethodes te beschikken.

De efficiëntie van ballot-comparison audits hangt af van een belangrijke logistieke vereiste: het moet mogelijk zijn om het papieren stembiljet terug te vinden dat bij elke elektronische registratie hoort. Dit lijkt echter een haalbaar doel in België:

- voor papieren stembiljetten maken zowel het gebruik van PATSY als de praktijk van het sorteren van stembiljetten in afzonderlijke enveloppen met stembiljetten die bij dezelfde

partij horen (art. 159 van de Kieswet [68]) het mogelijk om een manifest zo op te stellen dat we weten hoe elk stembiljet tijdens de telling werd geïnterpreteerd,

- voor de elektronisch stemming wordt de inhoud van elk papieren stembiljet vandaag al elektronisch geregistreerd, en de procedures voor het afdrukken en scannen van de stembiljetten, die hierna worden beschreven, zullen het ook mogelijk maken om een band te handhaven tussen het papier en de elektronische registratie ervan.

Traceerbaarheid van de stembiljetten

De geldigheid en het gemak van de uitvoering van een RLA hangen grotendeels af van de kwaliteit van de logistiek van de stembiljetten.

Enerzijds moet er een garantie zijn dat de papieren biljetten op basis waarvan de audit wordt verricht, authentiek zijn. Het doel van een RLA is om te bevestigen dat een aangekondigde verkiezingsuitslag een correcte weerspiegeling biedt van een geheel van stembiljetten. Als deze stembiljetten vervalst zijn, heeft de audit uiteraard geen zin.

Het is daarom essentieel om een strategie van onberispelijke traceerbaarheid van de stembiljetten te handhaven, van de handen van de kiezers tot de plaats waar de RLA plaatsvindt. Deze traceerbaarheidseis is zeker niet nieuw in de context van een RLA: hij is sowieso al nodig om te garanderen dat eventuele hertellingen geldig zijn.

De invoering van RLA's benadrukt dit belang echter: terwijl de hertellingen vandaag vrij zeldzaam zijn, en over het algemeen zeer gedeeltelijk gebeuren, kan het gebruik van RLA's onregelmatigheden aan het licht brengen die eventueel hebben plaatsgevonden tussen het moment waarop de stemmen worden geteld en het moment van de audit. En als de stembiljetten authentiek waren op het moment van de telling, maar dat niet meer zijn op het moment van de audit, kan de audit een telling ongeldig maken die misschien correct was. De invoering van RLA's vereist daarom een herziening van alle huidige traceerbaarheidsprocedures en een verbetering ervan wanneer dat mogelijk is.

Omgekeerd, als er vóór de telling is geknoeid met de stembiljetten (door biljetten te wijzigen, toe te voegen of weg te nemen), zal de audit waarschijnlijk de uitslag bevestigen die na de telling is bekendgemaakt, ook al klopt die niet, en geen fraude kunnen opsporen die het gevolg is van een inbreuk op de traceerbaarheid van de stembiljetten.

De verificatie van deze traceerbaarheid kan echter sterk worden verbeterd dankzij de 'end-to-end controleerbaarheid' van de verkiezing, gebaseerd op cryptografische technieken die worden beschreven in punt *3.3*. Kiezers kunnen zo controleren of hun stembiljet correct is meegenomen in de telling.

Verkiezingsmanifest

Naast de traceerbaarheid van de stembiljetten is het voor een efficiënte RLA ook essentieel om te beschikken over een classificatie van alle stembiljetten, vastgelegd in een manifest.

Voordat de audit wordt opgestart, moesten documenten beschikbaar zijn waarin minstens het volgende is opgesomd:

- de genummerde (of anderszins geïdentificeerde) houders (dozen, enz.) waarin de stembiljetten worden bewaard,
- het aantal stembiljetten in elke houder,
- de manier waarop van deze stembiljetten werd geïnterpreteerd.

Het is ook nuttig om de herkomst van elke houder bij te houden, evenals het traject dat ze hebben afgelegd: wie ze heeft verzegeld, waar en wanneer, en wie ze vervolgens heeft ontvangen en behandeld, waar en wanneer, tot het moment van opslag na de audit.

Dergelijke documenten worden al op grote schaal opgesteld in de context van het stemmen op papier via de processen-verbaal van de stembureaus en de telbureaus, die worden gecompileerd op het niveau van de hoofdkantoren van de kantons en van de arrondissementen. Zelfs als er geen specifiek register is waarin specifiek wordt vermeld hoe elk stembiljet is geïnterpreteerd, biedt de rangschikking van de stembiljetten voor elke partij in afzonderlijke enveloppen dezelfde functionaliteit: voordat je een envelop opent, weet je aan welke partij alle stembiljetten in die envelop zijn toegewezen (of dat het stembiljet als blanco of ongeldig is geïnterpreteerd).

Dit is momenteel echter niet het geval voor elektronisch stemmen: de papieren stembiljetten worden niet systematisch gesorteerd voor deze verkiezingen, aangezien de telling is gebaseerd op de gegevens op de USB-sticks van de voorzitters van de stembureaus. Het zou mogelijk zijn om deze situatie aan te pakken door 'batch-comparison audits' uit te voeren, maar die zouden de auditprocedure veel omslachtiger maken, aangezien elke te hertellen 'batch' overeenkomt met een stembus die 800 of meer stembiljetten kan bevatten. Daarbij moeten we in gedachten houden dat het aantal te tellen batches niet aanzienlijk geringer is dan het aantal te vergelijken stembiljetten in het kader van een 'ballot-comparison audit'.

Voor elektronisch stemmen zijn een aantal opties denkbaar. De optie die wij aanbevelen (andere opties worden hieronder besproken) is om bij het scannen van de papieren stembiljetten een uniek trackingnummer op het biljet af te drukken. Dat trackingnummer moet vervolgens worden samen met de elektronische registratie van het stembiljet worden bewaard.

Dit betekent dat de papieren stembiljetten moeten worden afgedrukt op papier waarop gemakkelijk een merkteken kan worden geprint bij het scannen. Hier lijkt het gebruik van papier van standaardformaat (A4 bijvoorbeeld) de meest aantrekkelijke en meest gebruikte oplossing. Dit type papier kan gemakkelijk in conventionele scanners worden geplaatst die zijn uitgerust met een printmodule waarmee doorgaans een serienummer van de scanner, de datum en het tijdstip van het scannen kan worden afgedrukt, en met een teller van het aantal gescande pagina's. Deze printmodules, die in het Frans soms 'endosseur' of 'imprimeuse' worden genoemd en 'imprinter' in het Engels, worden courant gebruikt in archiveringsoplossingen en bieden, wat de instapmodellen betreft, de mogelijkheid om ongeveer 70 tot 80 pagina's per minuut te scannen. Een stembus met ongeveer 800 stembiljetten zou den in ongeveer tien minuten kunnen worden gescand. De werklast van een telbureau, ongeveer 2.400 stembiljetten, zou kunnen worden verwerkt in een half uur scannen (exclusief de tijd die nodig is voor de behandeling van het papier).

Scannen met printen zou op verschillende locaties en op verschillende manieren kunnen plaatsvinden. We zullen ze in het volgende hoofdstuk bespreken, in samenhang met de structuur van het stemsysteem.

De aanpak die we hier hebben beschreven, legt de link tussen papieren stembiljetten en hun elektronische versie door een serienummer af te drukken op het moment van scannen. Andere opties zijn uiteraard mogelijk en we bespreken er hier verschillende.

1. Bewaren van de gescande stembiljetten in scanvolgorde. Het idee is hier om de stembiljetten in pakken van een honderdtal biljetten te scannen en de volgorde van de gescande stembiljetten intact te houden in enveloppen of mappen. Op voorwaarde dat de scansoftware ook de scanvolgorde bewaart (via logboeken, bestandsnamen, een volgorde van regels in tabellen die de interpretaties van de bulletins bevatten, enz.). Deze volgorde is enkel voldoende om een audit te kunnen uitvoeren die zou aangeven om de elektronische registratie en de papieren versie van bijvoorbeeld het 83e stembiljet van het 8e pak van de 17e doos met stembiljetten met elkaar te vergelijken. Een dergelijke oplossing, die op sommige plaatsen in de VS wordt gebruikt, is echter erg kwetsbaar: het 83e stembiljet in een stapel vinden kan lastig zijn, veel inspanningen kosten en een bron van fouten zijn bij de audit (fouten die ertoe kunnen leiden dat een groter aantal stembiljetten moet worden gecontroleerd om de audit te voltooien). Bovendien hoeft een stapel stembiljetten maar uit de handen van de behandelaar te glippen om de volgorde kwijt te raken, waardoor het onmogelijk wordt om het gekozen stembiljet te controleren tijdens het auditproces. Deze onmogelijkheid om te verifiëren zal bij de audit waarschijnlijk moeten worden geïnterpreteerd als een onjuist geteld stembiljet (om het risico te vermijden dat de controle wordt vervalst door een persoon die onjuiste stembiljetten zou verhullen door de stapel stembiljetten opzettelijk te laten vallen), wat tot gevolg kan hebben dat een bepaald aantal extra stembiljetten moet worden geverifieerd.

2. Afdrukken van een uniek serienummer op het stembiljet door de stemmachine, tegelijkertijd met het afdrukken van het stembiljet. Dit serienummer zou tegelijk met het stembiljet worden gescand en samen met de interpretatie van het stembiljet in elektronisch formaat worden bewaard. Deze oplossing heeft het voordeel dat er geen scanner met printmodule nodig is. Ze kan het auditproces echter aanzienlijk vertragen in vergelijking met de oplossing met een printmodule. Dit komt doordat de ingebouwde printmodule van de scanner de gescande stembiljetten gemakkelijk in oplopende volgorde kan nummeren: deze stembiljetten zijn door de stembus gegaan en gemengd voordat ze werden gescand, om bezorgdheden over de vertrouwelijkheid van de stemmen te vermijden. En deze oplopende nummering maakt het veel gemakkelijker om stembiljetten te vinden in een stapel: een stembiljet met een bepaald nummer kan binair worden gezocht, zoals in een woordenboek. Aan de andere kant geeft het nummeren van de stembiljetten in oplopende volgorde op het niveau van de stemmachine grote problemen: iemand die de volgorde waarin de kiezers een stemmachine gebruiken, observeert, zou vervolgens ieders stembiljetten in een stembus kunnen terugvinden, zelfs nadat ze intensief dooreen zijn gehusseld. Een alternatief zou zijn om willekeurige serienummers op de stembiljetten af te drukken, waardoor de risico's van vertrouwelijkheid die gepaard gaan met sequentiële nummering, worden vermeden. Het wordt echter veel lastiger om een stembiljet met een willekeurig nummer te vinden in een stapel gescande stembiljetten: gemiddeld moet je de helft van de stembiljetten doornemen voordat je het juiste stembiljet vindt. Deze oplossing zou echter robuuster zijn dan de vorige, in die zin dat het laten vallen van een stapel stembiljetten geen bijzonder probleem zou opleveren.

In contexten waar de gescande stembiljetten op volgorde worden bewaard en waar het erop aankomt om een stembiljet op een specifieke positie in de stapel te vinden, zijn meer exotische

methoden getest. Het zoeken naar een stembiljet kan bijvoorbeeld worden vergemakkelijkt door het gebruik van een zeer nauwkeurige weegschaal: er kan worden berekend dat het 83e stembiljet op een stapel kan worden gevonden door de eerste 82 stembiljetten te verwijderen, die (bijvoorbeeld) 408 gram zouden wegen. Stembiljetten worden dan van de stapel gehaald en gewogen tot ze het vereiste gewicht hebben. Deze methode blijkt echter vaak te willekeurig te zijn, vanwege de lichte variabiliteit in het gewicht van het papier, die vooral samenhangt met de aanwezige vochtigheid.

Een andere methode, met opeenvolgende afnames, werd voorgesteld voor het selecteren van een willekeurig stembiljet uit een stapel biljetten, ter vervanging van de vereiste om een stembiljet te selecteren dat zich in een bepaalde positie in een stapel bevindt [56]. Dit houdt in dat de stapel stembiljetten een bepaald aantal keren handmatig wordt 'afgenomen', door een bundel stembiljetten van de bovenkant van de stapel te pakken en onderaan weer terug te leggen (een stapel van vijf ABCDE-stembiljetten kan bijvoorbeeld worden getransformeerd in een DEABC-stapel na een dergelijke afname). In de praktijk blijkt dat de herhaling van zes opeenvolgende afnames voldoende is om een stembiljet min of meer uniform gekozen bovenaan de stapel stembiljetten te laten verschijnen, en dit voor stapels stembiljetten die tot 1.000 stembiljetten bevatten.

Deze strategie kan met name interessant zijn in de context van het selecteren van een papieren stembiljet in een envelop die verondersteld wordt stembiljetten te bevatten die naar één partij gaan: in dit geval zijn alle stembiljetten in wezen gelijkwaardig. Ze zou lastiger te gebruiken zijn in een context waar de stembiljetten verschillen en waar de link tussen papier en elektronisch gebaseerd is op een endossement: het willekeurig uitnemen van een papieren stembiljet in plaats van op basis van het elektronische manifest zou de deur open kunnen zetten voor fraude waarbij meerdere papieren stembiljetten met identieke stemmen ook gemarkeerd zouden worden met een identiek endossement, wat het mogelijk zou kunnen maken om stembiljetten toe te voegen aan het elektronische manifest, die geen papieren overeenstemming zouden hebben en daarom nooit onderzocht zouden worden.

Auditsoftware

Het verloop van een audit wordt veel eenvoudiger door het gebruik van specifiek daarvoor bedoelde software.

De software wordt allereerst voorzien van een kopie van het verkiezingsmanifest, meestal in de vorm van een spreadsheetbestand dat de essentiële elementen van het verkiezingsmanifest bevat: een lijst met de houders van de stembiljetten en hun inhoud, stembiljet per stembiljet, en het aangekondigde resultaat van de telling van de stemmen.

De audit wordt dan opgestart door de te tolereren risicomarge aan te geven en een willekeurig getal te selecteren waaruit de lijst met tijdens de audit te controleren stembiljetten wordt afgeleid. Het gebruik van een willekeurig getal dat aan de software wordt geleverd, zorgt ervoor dat de keuzes die tijdens de audit worden gemaakt, niet vertekend zijn en maakt het mogelijk om de hele audit te reproduceren als dat nodig is – wat niet mogelijk zou zijn als elke nieuwe uitvoering van de audit aanleiding zou geven tot een nieuwe willekeurige reeks bulletins.

In de praktijk wordt dit willekeurige getal vaak geproduceerd door een reeks dobbelstenen te gooien in aanwezigheid van een aantal waarnemers. In sommige rechtsgebieden wordt de worp met de dobbelstenen gefilmd en opgenomen in de openbare auditgegevens. Een voorbeeld van een dobbelceremonie in het kader van de RLA voor de verkiezing van de huidige Secretary of State van de staat Georgia is te zien op het volgende adres:

https://www.youtube.com/watch?v=1nhdtkryKtc

Op basis van deze informatie bepaalt de auditsoftware welke papieren stembiljetten moeten worden geïnspecteerd ter vergelijking met hun elektronische interpretatie, om het aangekondigde resultaat te kunnen valideren, met het gekozen risiconiveau. De software kan haar gedrag tijdens de controle aanpassen: als er bijvoorbeeld onjuist geïnterpreteerde of ontbrekende stembiljetten worden ontdekt, zal een groter aantal stembiljetten moeten worden gecontroleerd om te bepalen of deze fout anekdotisch is of een telprobleem weerspiegelt dat de verkiezingsuitslag kan veranderen. In het ergste geval kan de software concluderen dat een volledige hertelling nodig is.

Organisatie van het auditlokaal

Het is uiteraard belangrijk om de eigenlijke audit onder zodanige omstandigheden te organiseren dat degenen die bij de verkiezing betrokken zijn, ervan overtuigd kunnen zijn dat het getelde resultaat inderdaad juist is. De audit moet ook plaatsvinden in een ruimte die zo is ingericht dat de handelingen efficiënt kunnen worden uitgevoerd zonder de veiligheid van de stembiljetten in gevaar te brengen.

Over het algemeen is het een goed idee om de audit zo zichtbaar mogelijk te maken, in ieder geval voor de waarnemers. De dobbelceremonie om het willekeurige nummer te genereren dat de audit initieert, moet voor iedereen zichtbaar worden uitgevoerd. De laptop met de auditsoftware wordt aangesloten op een projector, zodat iedereen het verloop van de audit kan volgen, de ontwikkeling van de geschatte marges kan zien en de lijst met de te inspecteren of reeds geïnspecteerde stembiljetten kan bekijken.

Het lokaal moet het mogelijk maken dat er pauzes kunnen plaatsvinden zonder gevaar voor de veiligheid van de audit, en dat stroomafsluitingen of brandalarmen met een mogelijke evacuatie tot gevolg, kunnen worden beheerd. Het is belangrijk om te beschikken over een lokaal dat gemakkelijk af te sluiten en waaruit een vlotte evacuatie mogelijk is.

Ten slotte moet er rekening mee worden gehouden dat de audit kan leiden tot een volledig handmatige telling van de stembiljetten. Dit vereist een grotere ruimte, een spreiding over meerdere dagen en vereist een veel groter aantal personen dan een normale audit. Aangezien de voltooiing van de audit noodzakelijk is voor de definitieve validatie van de resultaten, moeten de procedure en de lijst van personen die nodig zijn voor een hertelling ruim van tevoren worden opgesteld.

Tot slot kan een proces-verbaal van de audit worden opgesteld, normaal gezien door de auditsoftware, gevalideerd door de aanwezige waarnemers en opgestuurd naar het bureau van de kieskring en naar de FOD Binnenlandse Zaken. Dit proces-verbaal kan samen met de verkiezingsuitslag worden gepubliceerd.

3.2.3 Beoordeling op basis van eerdere verkiezingen

Met behulp van de CSV-bestanden die beschikbaar zijn op de website van de federale dienst,[18] hebben we de marges berekend voor de federale verkiezingen van 2014 en 2019 in België, voor elke kieskring. Elke kieskring wordt beschouwd als een onafhankelijke verkiezing, aangezien elke kieskring beschikt over een eigen aantal toe te wijzen zetels.

Om de marges te berekenen, gingen we na het extraheren van de gegevens uit de CSV-bestanden als volgt te werk. Voor elk paar (A, B) partijen dat vertegenwoordigd is in elke kieskring, kijken we naar de volgende voorwaarden:

1. Heeft partij A genoeg stemmen behaald om de kiesdrempel te halen?
   - Zo ja, hoeveel stemmen zou ze minder moeten hebben gekregen om de drempel niet langer te behalen?
   - Zo niet, hoeveel stemmen zou ze nodig hebben om de drempel te halen en heeft partij B genoeg stemmen om er genoeg aan partij A te geven?
2. Als partij A een zetel heeft verkregen na de toewijzing volgens de methode-d'Hondt, hoeveel stemmen zou ze dan moeten verliezen ten gunste van partij B opdat de laatste zetel die aan partij A was toegewezen, in plaats daarvan aan partij B zou worden toegewezen?

Elke potentiële marge die volgens deze voorwaarden is vastgesteld, wordt eerst getest om na te gaan of de overdracht van stemmen van partij A ten gunste van partij B een ander resultaat zou opleveren (d.w.z. een andere zetelverdeling tussen de lijsten). Vervolgens wordt voor elk paar (A, B) de kleinste van de gevalideerde marges in aanmerking genomen. Tot slot wordt het paar met de kleinste marge van alle andere paren in aanmerking genomen: dit geeft de marge van de verkiezing aan, d.w.z. het kleinste aantal stemmen dat de uitslag van de verkiezing kan veranderen.

Marges van de federale verkiezingen van 2014 en 2019.

Kieskring	Jaar	Absolute marge	Relatieve marge
	2014	783	0,125%
	2019	919	0,148%
	2014	1.173	0,159%
	2019	743	0,102%
	2014	511	0,213%
	2019	5.261	2,128%
	2014	1.155	0,101%
	2019	453	0,039%

[18] *https://verkiezingsresultaten.belgium.be/nl*

2014	693	0,231%
2019	3.579	1,174%
2014	7.679	4,525%
2019	4.812	2,817%
2014	2.165	0,268%
2019	2.748	0,341%
2014	225	0,041%
2019	2.710	0,488%
2014	6.359	0,936%
2019	1.782	0,258%
2014	338	0,034%
2019	2.369	0,237%
2014	305	0,061%
2019	965	0,192%

De tabel *[tab:marges]* toont de aldus verkregen marges voor elke kieskring bij de federale verkiezingen van 2014 en 2019. Zoals te verwachten is, levert het systeem-d'Hondt soms zeer kleine marges op, vaak in de grootteorde van een paar honderd stemmen.

Op basis hiervan, en gezien de resultaten in andere landen, kunnen we verwachten dat de implementatie van RLA's in de context van deze verkiezingen de audit van een aantal stembiljetten zal vereisen dat kan variëren tussen een honderdtal stembiljetten (wanneer de marges hoog zijn, zoals het geval was in de kieskring Luxemburg) en een paar duizend stembiljetten. In bepaalde extreme gevallen is het echter mogelijk dat een volledige hertelling nodig is (zoals in het geval van Oost-Vlaanderen in 2014).

3.3 CONTROLEERBAARHEID VAN BEGIN TOT EIND

3.3.1 Inleiding

3.3.1.1 Wat is een van begin tot eind controleerbare verkiezing?

Een verkiezing is van begin tot eind controleerbaar, of '*end-to-end verifiable*' of '*E2E verifiable*' in het Engels, als ze de kans biedt om te verifiëren dat de aangekondigde verkiezingsuitslag correct is, onafhankelijk van enig vertrouwen dat moet worden gesteld in specifieke apparatuur, specifieke procedures of specifieke personen.

De uitgevoerde controles richten zich doorgaans op twee hoofdelementen:

1. *individuele controleerbaarheid*: zit mijn stembiljet ongewijzigd in de (eventueel elektronische) stembus die wordt geteld?

2. *universele controleerbaarheid*: zijn de stembiljetten in de stembus correct geteld?

Sommige auteurs voegen daar nog een vereiste aan toe, namelijk de *controleerbaarheid van de stemgerechtigdheid*: zijn de stembiljetten in de stembus alleen afkomstig van gemachtigde kiezers?

Individuele controleerbaarheid en universele controleerbaarheid worden aanbevolen door de Raad van Europa als middelen om zich te vergewissen van de vrije uitdrukking van de stem. De "Lignes directrices pour la mise en œuvre des dispositions de la recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique" vermelden inderdaad in artikel 10.c [22] [vrij vertaald]:

> In het elektronische stemsysteem zouden alle denkbare maatregelen moeten worden genomen om invloeden te voorkomen die bedoeld zijn om te knoeien met de stem na de registratie ervan, evenals systemen om zich ervan te vergewissen dat er geen dergelijke invloed werd uitgeoefend. [...]
>
> Deze bepaling is bedoeld ter verhindering van ongeoorloofde wijzigingen in de stem nadat die is geregistreerd. Ze beschermt het systeem tegen aanvallen van buitenaf, maar ook tegen interne bedreigingen. Individuele controleerbaarheid en universele controleerbaarheid [...] maken het mogelijk om elke ongeoorloofde interventie van dit type op te sporen.

De controleerbaarheid van de stemgerechtigdheid, hoewel op het eerste gezicht een vrij vanzelfsprekende vereiste, wordt in de praktijk vaak over het hoofd gezien: procedures voor de controleerbaarheid van de stemgerechtigdheid vereisen dat er een lijst met kiezers wordt gepubliceerd – het is moeilijk om te controleren of een lijst met kiezers correct is zonder die te publiceren – en het is over het algemeen problematisch, zo niet onwettig, om lijsten met kiezers en/of personen die hebben gestemd, te publiceren. In België wordt, in de stembureaus, de stemgerechtigdheid gecontroleerd in aanwezigheid van de stembureauleden en waarnemers. Deze controleprocedure lijkt ons veel sterkere garanties voor transparantie te bieden dan de procedure die kan worden uitgevoerd op stembussen die naar de telbureaus en de kantonhoofdbureaus worden verplaatst. Het is hierbij niet onze bedoelding om externe verificatiemiddelen van die controle voor te stellen. (De situatie is anders voor Belgen die in het buitenland wonen en per post stemmen: de verificatie van de identiteit van de kiezer is in die context natuurlijk veel moeilijker, en technieken om deze verificatie te verbeteren zijn elders voorgesteld [50].)

De technieken voor universele controleerbaarheid moeten systematisch worden toegepast en brengen weinig knelpunten met zich mee. Het komt er in wezen op aan dat er verificatiesoftware wordt uitgevoerd op een geheel van gegevens die beschikbaar zijn gemaakt na het tellen van de stemmen: deze software controleert of de aangekondigde uitslag wel degelijk overeenkomt met de inhoud van de stembussen met stemmen waarvan de vertrouwelijkheid wordt beschermd door cryptografische mechanismen. Het is wenselijk dat er verschillende onafhankelijk geproduceerde verificatiesoftwareprogramma's bestaan: ze kunnen worden geproduceerd door personen die ermee zijn belast om het goede verloop van de elektronische verkiezingen te verifiëren (denk bijvoorbeeld aan het College van Deskundigen), door partijen die de uitslag van de verkiezingen willen verifiëren, door actoren uit het maatschappelijk middenveld, door internationale waarnemers, enz. Hoewel deze controle het gebruik van computers en software vereist, is een centraal aspect van universele controleerbaarheid dat niemand wordt gevraagd zijn vertrouwen te stellen in een specifieke persoon, een specifiek softwareprogramma of een specifieke computer. De

controle kan potentieel door iedereen worden uitgevoerd, met behulp van om het even welke verificatiesoftware (inclusief software die door de controleur zelf is gemaakt als hij dat wenst) en met behulp van om het even welke computer. Uiteraard vereist het maken van verificatiesoftware specifieke competenties, maar deze zijn beperkt: er zijn verificatiesoftwareprogramma's voor verkiezingen ontwikkeld in het kader van programmeerprojecten door eerstejaarsstudenten informatica aan de universiteit. Deze onafhankelijkheid van personen, software en machines staat centraal: ze maakt het mogelijk om fouten te ontdekken zodra één enkele eerlijke persoon (of belanghebbende omdat hij stemmen is kwijtgespeeld door die fouten) in staat is om correcte software en een niet door malware gecorrumpeerde computer te vinden.

Individuele controleerbaarheidstechnieken vereisen de actieve (maar optionele) deelname van de kiezer. Aangezien het doel is om kiezers te garanderen dat hun stembiljet wel degelijk is geteld, is het natuurlijk noodzakelijk dat de kiezers het geleverde bewijs wensen te verifiëren. Het feit dat sommige kiezers, en zelfs een aanzienlijk deel van hen, beslissen om geen controles uit te voeren, is geen punt van zorg. Een systeem dat individuele controleerbaarheid biedt, zal zijn bewijsstukken moeten aanbieden aan de kiezers zonder te weten of ze die zullen verifiëren. Dit beperkt de kans op succesvolle fraude waarbij het systeem alleen de stembiljetten zou wijzigen van de kiezers die de aanwezigheid van hun stembiljet niet hebben gecontroleerd. Stel bijvoorbeeld dat iemand 1% van de stembiljetten bij een verkiezing wil veranderen, in de hoop dat dit genoeg zou zijn om een nuttig effect te hebben, zonder de aandacht te trekken. Dit betekent dat 1% van de bewijsstukken die aan de kiezers worden geleverd, vervalst moet zijn. Maar als een honderdtal personen hun stembiljetten controleren, zelfs in een verkiezing met miljoenen kiezers, is de kans groot dat minstens één persoon ontdekt dat zijn stembiljet vervalst is. Kiezers die geen verificatie willen uitvoeren, zijn ook vrij om die verificatie te delegeren aan personen die ze vertrouwen.

3.3.1.2 Hoe wordt een verkiezing gecontroleerd?

Het is eenvoudig om verkiezingen voor te stellen die individueel en universeel controleerbaar zijn als we de beperking van de vertrouwelijkheid van stemmen wegnemen.

Een eenvoudig voorbeeld bestaat erin om de kiezers in een zaal te verzamelen, ze allemaal te vragen hun stem bekend te maken, die vervolgens naast hun naam op een groot bord wordt geschreven dat voor iedereen zichtbaar is, en vervolgens de stemmen te totaliseren. Een dergelijk systeem heeft de vereiste kwaliteiten:

- *Individuele controleerbaarheid:* de kiezers kunnen controleren of hun stem wel degelijk naast hun naam op het bord staat.
- *Universele controleerbaarheid:* om het even wie kan de stemmen die op het bord worden weergegeven, bij elkaar optellen en controleren of het aangekondigde totaal klopt.

Dit systeem kan zelfs worden gebruikt om de stemgerechtigdheid te controleren: elke kiezer heeft kunnen controleren of alle stemmen die op het bord zijn genoteerd, ook daadwerkelijk overeenkomen met kiezers.

Dit systeem brengt twee problemen met zich mee in de context van politieke verkiezingen: het biedt geen garantie voor het stemgeheim, dat vereist is om een vrije stemming mogelijk te maken, en het stelt miljoenen personen niet in staat om te stemmen en de verkiezingsuitslag te controleren.

Het probleem van het aantal stemmers kan worden opgelost met behulp van het internet: de tabel waarop de stemmen worden genoteerd, kan worden vervangen door een webpagina (deze oplossing roept de vraag op of de server die deze webpagina weergeeft, dezelfde pagina aan iedereen laat zien, maar daar komen we later op terug). Om soortgelijke redenen worden verkiezingsresultaten nu ingevoerd in de Martine-software (ook voor de papieren stembiljetten), die wordt gebruikt om de resultaten van stemmentellingen in het hele land door te sturen en te consolideren.

Het probleem van het stemgeheim is hardnekkiger. De meest gebruikte oplossing is het gebruik van cryptografie om de stemintenties te versleutelen.[19] In plaats van een lijst met namen en stemmen te publiceren, wordt een lijst met namen en versleutelde stemmen gepubliceerd, of gewoon een lijst met versleutelde stemmen. Als de kiezers een kopie van hun versleutelde stem ontvangen wanneer ze stemmen, kunnen ze controleren of deze wel degelijk is gepubliceerd om opgenomen te worden in de berekening. Vervolgens worden verschillende cryptografische technieken gebruikt om aan te tonen dat de afgekondigde verkiezingsuitslag consistent is met alle gepubliceerde versleutelde stemmen. Deze laatste controle kan door om het even wie worden uitgevoerd.

Hier zien we echter de hierboven vermelde moeilijkheid opduiken: de kiezers zijn nu niet langer in staat om hun stem in een leesbare staat te traceren, wat wel degelijk nodig is om het stemgeheim te waarborgen, maar kunnen een versleutelde versie van hun stem traceren. De kiezers kunnen zich dus afvragen of die versleutelde versie een echte weergave is van hun stemintentie of dat de machine die de versleutelde stem heeft berekend, vals heeft gespeeld door ze vervangen door de versleutelde versie van een andere stem. Er zijn verschillende methodes om deze vraag te beantwoorden en hier beschrijven we de twee meest gebruikelijke, die ook gecombineerd kunnen worden gebruikt.

De eerste optie is om alle kiezers de mogelijkheid te bieden, zoals nu al het geval is in België, om hun stembiljet ongeldig te maken voordat ze het in de stembus doen. Wanneer kiezers het stemhokje verlaten, hebben ze zowel hun papieren stembiljet, dat leesbaar is en waarvan ze de inhoud kunnen controleren en bevestigen, als de versleutelde versie van het stembiljet, waarvan ze de aanwezigheid later kunnen controleren op het internet. Als kiezers twijfels koesteren over de eerlijkheid van de stemmachine die de versleutelde stem heeft berekend, kunnen ze beslissen om het stembiljet ongeldig te maken en te vragen om de versleutelde versie te ontsleutelen, waarbij een bewijs van de nauwkeurigheid van de ontsleuteling wordt geleverd. Er kan dan worden gecontroleerd of de ontsleutelde stem wel degelijk overeenkomt met wat er op het stembiljet staat. Een machine die vals speelt op het moment van de versleuteling, zou dus op heterdaad betrapt worden. Natuurlijk kan het ontsleutelde stembiljet niet meer in de stembussen worden gedaan: dit

---

[19] Een alternatieve oplossing is om de stemmen niet te versleutelen, maar om de namen van de kiezers te vervangen door pseudoniemen, zodat elke kiezer de enige is die zijn of haar pseudoniem kent [53]. Deze aanpak brengt in de Belgische context echter aanzienlijke problemen met zich mee, omdat zoiets de verkoop van stemmen sterk kan vergemakkelijken: de mogelijkheid om zoveel kandidaten als gewenst goed te keuren uit een lange lijst van kandidaten die door een partij wordt verstrekt, maakt het namelijk bijzonder gemakkelijk om een geldig stembiljet te produceren waarvan men vrijwel zeker kan zijn dat het uniek is, en dit unieke karakter kan dan worden gebruikt om een verkoop te verzekeren of een stem af te dwingen.

zou de vertrouwelijkheid van de stemming schenden. Aan de andere kant zal een tevredengestelde kiezer een nieuw stembiljet aanmaken en beslissen om dat stembiljet in de stembus te doen (of het opnieuw ongeldig te maken en een derde in te vullen).

Merk op dat deze testoperatie niet specifiek door kiezers hoeft te worden uitgevoerd: waarnemers, deskundigen of anderen kunnen net zo goed een stemmachine die op een bepaald moment niet in gebruik is, gebruiken om een stembiljet in te vullen en het vervolgens ongeldig maken om te controleren of het correct is. De handeling van het stemmen is wel degelijk het in de urne steken van een stembiljet, niet het produceren van een stembiljet op een stemmachine.

De tweede optie is vergelijkbaar met het proces van de risk limiting audit: een aantal papieren stembiljetten zou uit de stembussen gehaald kunnen worden, zonder te weten wie de eigenaar is, omdat de stembus al dooreen werd gehusseld, en de bijbehorende versleutelde stemmen zouden verifieerbaar ontsleuteld kunnen worden. Deze methode heeft het voordeel dat er minder getest hoeft te worden tijdens de stemverrichtingen. Ze heeft wel het nadeel dat ze zwakker is wat betreft de vertrouwelijkheid van de stemming: als een kiezer besluit om zijn of haar versleutelde stembiljet op sociale netwerken te publiceren, bijvoorbeeld om aan te tonen dat hij of zij de aanwezigheid van zijn of haar stem heeft geverifieerd, en als hetzelfde stembiljet wordt uitgekozen in het kader van de audit, kan deze persoon de vertrouwelijkheid van zijn of haar stem verliezen. Dit zijn echter tamelijk extreme omstandigheden: slechts een uiterst klein deel van de stembiljetten zal worden ontsleuteld en verwacht kan worden dat de overgrote meerderheid van de kiezers hun versleutelde stembiljetten niet openbaar zullen maken.

In beide gevallen beschikken we over de volgende traceerbaarheidsketen van de stembiljetten:

1. De kiezers bewaren een versleutelde kopie van hun stembiljet en hebben er alle vertrouwen in dat deze versleutelde kopie hun stem weergeeft, omdat ze de gebruikte stemmachine hebben kunnen testen, net als alle kiezers die voor en na hen dezelfde machine gebruiken.

2. De kiezers kunnen nagaan dat hun versleutelde stembiljet wel degelijk is opgenomen in de lijst van stembiljetten die in de telling zijn weergegeven. Ze kunnen ook controleren of het aantal stembiljetten dat wordt weergegeven, overeenkomt met het aantal mensen waarvan is aangegeven dat ze hebben gestemd.

3. De kiezers kunnen nagaan dat de verkiezingsuitslag inderdaad consistent is met alle gepubliceerde versleutelde stembiljetten.

Een probleem met deze aanpak is de noodzaak om voor bepaalde stappen gebruik te maken van cryptografie, wat geen bijzonder inclusieve technologie is.

We kunnen echter een vergelijkbaar onderscheid zien als in andere gebieden van het dagelijkse leven waar cryptografie wordt gebruikt: e-maildiensten, bankverrichtingen, het openen van een auto zonder sleutel, enz. Voor de gebruiker is het gebruik van cryptografie in feite transparant en de gebruiker heeft vaak niet eens de behoefte om te weten dat ze bestaat, laat staan hoe ze werkt. Aan de andere kant verhindert dit niet dat het gebruik van cryptografie efficiënt is: de gebruikte mechanismen, vooral hier, zijn stuk voor stuk openbaar gedefinieerd en onderzocht door gemeenschappen van deskundigen van alle kanten.

Praktisch gezien komen we tot een stemprocedure die de volgende vorm aanneemt:

1. Er wordt een groep sleutelbeheerders gevormd. In de context van politieke verkiezingen zijn het er vaak vijf. Deze beheerders beheren en bewaren de cryptografische sleutels die nodig zijn om het bewijs te produceren dat alle stembiljetten die door de kiezers zijn ingeleverd, overeenkomen met de aangekondigde verkiezingsuitslag. Daarnaast publiceren de beheerders de openbare sleutel die wordt gebruikt om de stemmen van alle kiezers te versleutelen. Deze openbare sleutel wordt gedistribueerd naar alle stemmachines.

2. De stemmachines gebruiken de openbare sleutel om alle stembiljetten te versleutelen en de kiezers een kopie van de versleutelde versie van hun stembiljet te bezorgen, of, in de praktijk, een trackingnummer dat een hashcode is van deze versleutelde versie en dat een korte vingerafdruk van deze versleutelde versie vormt.

3. De kiezers beslissen of ze het trackingnummer dat ze van de stemmachine ontvangen, accepteren als een afspiegeling van hun stem, of dat ze dit willen verifiëren en een nieuw stembiljet willen aanmaken.

4. Kiezers die tevreden zijn met het stembiljet en het trackingnummer dat ze hebben ontvangen, doen hun stembiljet in de stembus en verlaten het stembureau met hun trackingnummer van het stembiljet.

5. Aan het einde van de stemverrichtingen worden alle trackingnummers van de stembiljetten die in de stembussen zijn gedaan, openbaar gemaakt en geauthenticeerd via een website. Elke kiezer kan controleren of zijn of haar trackingnummer wel degelijk is vermeld en de waarnemers kunnen zich ervan vergewissen (bijvoorbeeld door vergelijking) dat ze wel degelijk toegang hebben tot dezelfde lijst met stembiljetten en dat het aantal stembiljetten op de lijst overeenkomt met de opkomstcijfers voor de verkiezing.

6. De sleutelbeheerders komen samen om over te gaan tot het produceren en het publiceren van de gegevens die aantonen dat de aangekondigde verkiezingsuitslag inderdaad consistent is met alle gepubliceerde trackingnummers van stembiljetten. Ze doen dit zonder ook maar één stembiljet in de stembussen te ontsleutelen, waardoor het stemgeheim behouden blijft.

7. De beheerders ontsleutelen ook alle stembiljetten die niet in de stembussen zijn gedaan en waarvan de kiezers een controle hebben gevraagd, om de ontsleutelde versie te vergelijken met wat op het papieren stembiljet staat. Die gegevens worden ook openbaar gemaakt, zodat de kiezers kunnen controleren of het stembiljet of de stembiljetten die ze hebben laten controleren, ook daadwerkelijk gecontroleerd zijn.

8. Elke belanghebbende (partijleden, verkiezingswaarnemers, leden van het maatschappelijk middenveld, belanghebbende particulieren, enz.) controleert of de gegevens die door de beheerders zijn gepubliceerd, daadwerkelijk bevestigen dat de aangekondigde verkiezingsuitslag correct is.

Stappen 3, 5 en 7 bieden individuele controleerbaarheid van de verkiezing. Stap 8 biedt universele controleerbaarheid van de verkiezing.

We merken op dat kiezers die daar geen belangstelling voor hebben, de controlestappen gewoon kunnen negeren en kunnen stemmen zoals ze zouden doen in een niet-controleerbaar stemsysteem. Geïnteresseerde kiezers kunnen zeer eenvoudige taken uitvoeren: beslissen om een stembiljet ongeldig te maken en opnieuw te stemmen, en controleren of een trackingnummer wel

degelijk aanwezig is in een lijst met gepubliceerde stemmen. De eerste taak is niet moeilijker dan stemmen, en de tweede is gelijk aan het traceren van een postpakket via een website of een applicatie van de postdiensten.

De taken van de beheerders zijn veeleisender: ze moeten aanwezig zijn bij het begin en het einde van de verkiezing en software doen werken die cryptografische bewerkingen uitvoert. Er is niets geheims aan de software in kwestie: in bestaande systemen is een reeks softwareprogramma's onafhankelijk van elkaar tot stand gebracht door geïnteresseerden. De softwareprogramma's die de beheerders gebruiken, genereren echter cryptografische sleutels die geheim moeten blijven. Het is daarom belangrijk dat de gebruikte softwareprogramma's correct zijn en worden gebruikt op machines die niet zijn besmet met malware. Het systeem is echter robuust ontworpen: zelfs als alle beheerders corrupt zijn, zijn ze nog niet in staat om de verkiezingsuitslag te vervalsen. De vertrouwelijkheid van de stemming zou daarentegen wel in gevaar kunnen komen: als een kiezer het trackingnummer van zijn of haar stembiljet publiceert, zou het bezit van een voldoende groot aantal sleutels van de beheerders het mogelijk kunnen maken om de inhoud van de overeenstemmende stem te achterhalen – dit 'voldoende grote' aantal wordt vooraf gekozen, wanneer de sleutels worden gegenereerd.

De taak van universele controle van de verkiezing is minder gevoelig, omdat er geen geheime sleutels of andere vertrouwelijke informatie bij komen kijken. Voor die taak kunnen wel aanzienlijke IT-middelen nodig zijn, als we een volledige controle willen uitvoeren binnen een beperkte tijdspanne.

3.3.1.3 Over welke resources beschikken we op het vlak van controleerbaarheid van begin tot eind?

Academische literatuur

De eerste end-to-end controleerbare stemsystemen stammen uit het midden van de jaren 1980, en in het bijzonder uit de doctoraatsthesis van Josh Benaloh [3]. De eerste technieken waren echter complex om toe te passen en peperduur wat betreft de benodigde rekenkracht.

Een tweede grote stap werd gezet met de publicatie van het 'optimale' protocol door Cramer, Gennaro en Schoenmakers in 1997 [27]: dit protocol bracht alle hulpmiddelen samen die nodig zijn voor een controleerbare verkiezing, terwijl de rekenkundige vereisten tot een minimum werden beperkt, althans asymptotisch.

Het onderzoek wordt intensief voortgezet en sinds het begin van de jaren 2000 is de gemeenschap van onderzoekers die actief zijn op dit gebied, zodanig gegroeid dat er jaarlijks conferenties worden gewijd aan deze stemtechnologieën – naast de traditionele publicaties in de grote beveiligings- en cryptografieconferenties.

Er is een vrij duidelijke convergentie ontstaan in termen van technieken voor het versleutelen van stembiljetten en het bereiken van universele controleerbaarheid. Hoewel er bijvoorbeeld tussen de jaren 1980 en begin 2000 een aantal mechanismen voor stemversleuteling werd voorgesteld, kwamen vrijwel alle geïmplementeerde systemen op hetzelfde mechanisme uit: ElGamal-versleuteling.

Er wordt nog steeds intensief onderzoek verricht in tal van richtingen. Stemmen op afstand, en stemmen via het internet in het bijzonder, roepen vragen op die moeilijk te beantwoorden blijven.

De verificatie van het feit dat het verstuurde stembiljet de intentie van de kiezer weergeeft, het stemgeheim en het verzet tegen gedwongen stemmen en de verkoop van stemmen zijn stuk voor stuk problemen waarvoor bevredigende oplossingen worden gezocht. Stemmen per brief krijgt ook steeds meer aandacht, gezien het groeiende belang ervan in de praktijk en dankzij de garantie die het biedt dat het papieren stembiljet dat de kiezers opsturen, hun stemintentie wel degelijk weergeeft. Veel inspanningen zijn ook gericht op het verkrijgen van end-to-end controleerbare stemoplossingen die het stemgeheim bewaren in contexten waar de stem- en telprocessen bijzonder complex zijn – bijvoorbeeld bij stemmingen met één enkele overdraagbare stem.

Uitrol

Na de publicatie van het protocol van Cramer, Gennaro en Schoenmakers duurde het nog ongeveer tien jaar voordat de technieken verder werden verfijnd en voordat algemeen beschikbare IT-middelen het mogelijk maakten om end-to-end verifieerbare verkiezingen op te zetten in reële omstandigheden. De eerste toepassing in een reële verkiezing met enkele duizenden kiezers dateert van 2009, met de verkiezing van de rector van de UCLouvain [2]. Sindsdien is het gebruik wijdverspreid, in ieder geval in de privésector waar stemmen via het internet gebruikelijk is en plaatsvindt in een minder gevaarlijke context wat betreft cyberbeveiliging: duizenden verkiezingen zijn gehouden met dezelfde protocollen of met behulp van variaties daarop. In België in het bijzonder kondigen sommige van de voorgestelde systemen voor het stemmen via het internet voor de sociale verkiezingen aan dat ze controleerbaar zijn en een zekere mate van individuele controleerbaarheid bieden [55].

Op het gebied van de politieke verkiezingen zijn systemen die bepaalde gedeeltelijke vormen van controleerbaarheid bieden, ingezet in de context van verkiezingen via het internet in bijvoorbeeld Noorwegen [35], Zwitserland [61], Estland [37] en Frankrijk [25]. End-to-end controleerbare systemen (individuele en universele controleerbaarheid) zijn ook ingezet in de context van pilots, in 2009 en 2011 in Takoma Park in Maryland [9] en voor de Australische verkiezingen in de staat Victoria van 2015 [8]. In deze systemen wordt persoonlijk gestemd (niet op afstand) en staan de papieren stembiljetten centraal. Dit is in overeenstemming met het verslag "Securing the Vote" van de National Academies [45], dat in aansluiting op een studie getiteld "The future of voting" van de Amerikaanse Vote Foundation [63] benadrukt dat er eerst significante ervaring moet worden opgedaan met end-to-end controleerbare verkiezingen in de context van face-to-face verkiezingen voordat stemmen via het internet wordt overwogen in de context van politieke verkiezingen.

Deze pilots waren succesvol, maar werden niet permanent nagevolgd, waarschijnlijk deels omdat het projecten waren onder leiding van academische teams, en geen testimplementaties onder leiding van de systeemleveranciers die in de positie waren om het initiatief voort te zetten. De zeer technische aard van al deze controleerbare oplossingen, in combinatie met een gebrek aan standaarden, vormt ongetwijfeld ook een belemmering.

Deze situatie lijkt de laatste jaren een positieve wending te hebben genomen met de introductie van de software development kit ElectionGuard [31], een opensourceproject dat een set van gedocumenteerde en gratis cryptografische bouwstenen biedt die ontworpen zijn voor integratie in systemen die op de markt worden gebracht door leveranciers van stemoplossingen. ElectionGuard is sinds 2020 geïntegreerd in de oplossingen van ten minste twee afzonderlijke leveranciers en met succes ingezet bij de verkiezingen van ten minste vier county's.

Informaticatools

De implementatie van end-to-end controleerbare verkiezingen vereist doorgaans de implementatie van specifieke cryptografische protocollen, die behoorlijk verschillen van de protocollen die we in internetstandaarden terugvinden.

Een aantal 'library's' (bibliotheken) wordt echter bij steeds meer verkiezingen gebruikt. We vermelden hier een paar van de open source library's die bij ons weten het vaakst worden toegepast en vandaag nog steeds in gebruik zijn.

- Het Helios-systeem biedt een van de oudste en vandaag nog gebruikte implementaties van de tools die nodig zijn om end-to-end controleerbare verkiezingen uit te voeren. Het wordt sinds 2010 elk jaar gebruikt voor de verkiezingen van de IACR, de International Association for Cryptographic Research.

  https://github.com/benadida/helios-server/

- Verificatum biedt library's voor end-to-end controleerbare versleuteling en anonimisering van stembiljetten (mix-net), die worden gebruikt bij (gemeentelijke en nationale) verkiezingen in Noorwegen, Estland en Spanje.

  https://www.verificatum.org

- Het Belenios-systeem bevat cryptografische library's die zijn gebruikt in talrijke private verkiezingen en, meer recent, in bepaalde delen van het systeem voor stemmen via het internet dat werd gebruikt om Franse burgers vanuit het buitenland te laten stemmen voor de parlementsverkiezingen van 2022.

  https://gitlab.inria.fr/belenios/

- De SDK ElectionGuard bevat library's die zijn geïntegreerd in de oplossingen van verschillende leveranciers en die met name zijn ingezet bij verkiezingen in Fulton (Wisconsin), Preston (Idaho), Inyo County (Californië) en College Park (Maryland).

  https://www.electionguard.vote/

- De Zwitserse post heeft de cryptografische library's die gebruikt worden in haar systeem voor stemmen via het internet openbaar gemaakt en als open source uitgegeven. Dit systeem wordt ingezet in verkiezingspilots in de kantons Basel-Stadt, Sankt Gallen en Thurgau.

  https://gitlab.com/swisspost-evoting

Merk op dat, hoewel deze library's de cryptografische ingrediënten bevatten voor het organiseren van end-to-end controleerbare verkiezingen, ze niet noodzakelijkerwijs worden ingezet in systemen die deze vorm van controleerbaarheid bieden.

Wettelijk kader

We haalden hierboven de expliciete verwijzing aan naar individuele en universele controleerbaarheid in de aanbevelingen van de Raad van Europa over elektronisch stemmen [22].

Wat de nationale wetgeving betreft, is het meest geavanceerde project en het project dat bij ons de meeste interesse heeft gewekt, dat van Zwitserland, en meer bepaald Ordonnantie 161.116 van de

Bondskanselarij over elektronisch stemmen [11], die met name in artikel 5 de vormen van individuele en universele controleerbaarheid definieert die vereist zijn voor de goedkeuring van elektronische stemsystemen in Zwitserland – binnen de grenzen die verbonden zijn aan het stemmen via het internet. Volgens ons vormt de structuur van deze ordonnantie een belangrijke basis die in andere landen, waaronder België, gebruikt zou kunnen worden voor het stemmen met papieren bewijs.

3.3.1.4 Nog een stapje verder ...

Het begrip end-to-end controleerbaarheid wordt beschreven en besproken in een essay gericht op een lezerspubliek zonder technische deskundigheid ter zake: "End-to-end verifiability" door Josh Benaloh en zijn co-auteurs [4].

De opname van een tweedaagse workshop over ElectionGuard en de integratie ervan in de 'Verity Scanner' van het bedrijf Hart Intercivic is beschikbaar op het volgende adres:

https://www.electionguard.vote/events/eg_usability_aug_2022/

3.3.2 Een end-to-end controleerbaarheidsstrategie voor België

End-to-end controleerbaarheid en risk limiting audits zijn zeer complementaire technologieën. Het is bijgevolg niet verwonderlijk dat hun implementatiemethoden erg verschillen.

Het eerste belangrijke verschil betreft de actoren die betrokken zijn bij deze twee controlestrategieën.

- In de context van RLA's zijn de centrale actoren degenen die betrokken zijn bij het tellen en scannen van de papieren stembiljetten, die de manifesten produceren die nodig zijn voor de RLA, de personen die instaan voor de tracking en de authenticiteit van de stembiljetten, en de personen die de eigenlijke RLA uitvoeren op basis van de manifesten. Hier zijn doorgaans een paar honderd personen per kieskring bij betrokken, die opgeleid moeten worden inzake vrij technische procedures (zoals nu het geval is in de telbureaus).
- In de context van end-to-end controleerbaarheid zijn de actoren alle kiezers, die gevraagd zullen worden om de correctie en de telling van hun stembiljetten na te gaan, en een klein aantal personen, doorgaans minder dan een tiental, die betrokken worden bij het beheer van de cryptografische sleutels, bijgestaan door operators van het computersysteem dat de nodige berekeningen uitvoert en de resultaten publiceert, en die bijstand bieden aan de personen die deze resultaten willen controleren.

We stellen ook vast dat het type taak heel verschillend is:

- In de context van RLA's is de grootste inspanning het uitvoeren van een nauwkeurige tracking van de papieren stembiljetten, het produceren van uitvoerige manifesten en het inspecteren van de papieren stembiljetten.
- In de context van end-to-end controleerbaarheid is de grootste inspanning het informeren van alle kiezers over de mogelijkheden van verificatie, het aanmoedigen van externe actoren en kandidaten om betrokken te raken bij de onafhankelijke verificatie van de tellingen, en het

doen werken van een IT-infrastructuur die de verkiezingsgegevens publiceert met de hulp van een klein tiental personen die instaan voor het beheer van cryptografische sleutels.

De implementatie van de end-to-end controleerbaarheid zal ook pilots omvatten, maar die zullen beduidend andere doelstellingen nastreven dan de RLA's. Het testen en dimensioneren van de procedures zal waarschijnlijk veel eenvoudiger verlopen: afgezien van de behoefte aan krachtigere computers, zal de overgang van een test met 1.000 kiezers naar een uitrol voor 1 miljoen kiezers niet zoveel veranderen (terwijl er wel fundamentele verschillen zijn in het geval van een RLA). Toch zullen er veel grotere inspanningen nodig zijn om de communicatie rond het auditproces vorm te geven, gericht op kiezers en op verenigingen, kandidaten of partijen die onafhankelijke verificatietools kunnen leveren.

3.3.2.1 Voortbouwen op elders opgedane ervaring

Net als bij RLA's zijn er een aantal ervaringen op basis waarvan verkiezingen die van begin tot eind controleerbaar zijn, kunnen worden opgebouwd. In tegenstelling tot de RLA's is de openbare documentatie van deze ervaringen echter veel beperkter. We hebben geen gedetailleerde "handleiding voor de uitrol van end-to-end controleerbare verkiezingen" gevonden.

Hoewel er in België geen ervaring lijkt te zijn met het gebruik van RLA's, is er wel ervaring opgedaan door een groot Belgisch publiek in de context van private verkiezingen: verschillende Belgische universiteiten hebben sinds 2009 systematisch hun rectoren verkozen door middel van algemene verkiezingen met behulp van end-to-end controleerbare systemen, waarbij honderdduizenden studenten werden blootgesteld aan de procedure van controle van de publicatie van hun versleutelde stembiljetten. Een aantal werknemers van Belgische ondernemingen heeft ook een dergelijke ervaring opgedaan in het kader van sociale verkiezingen of verkiezingen van beroepsorganisaties. Op die manier maakten deze verkiezingen het mogelijk om in België nuttige ervaring op te doen inzake het organiseren van de taak van de sleutelbeheerders bij het genereren van cryptografische sleutels en het produceren van bewijzen van correctie van het verkiezingsresultaat.

We mogen echter niet voorbijgaan aan de verschillen tussen het ecosysteem dat verbonden is aan het organiseren van een verkiezing met behulp van een private IT-infrastructuur, gericht op een publiek dat verbonden is aan een specifieke instelling, en het ecosysteem van politieke verkiezingen, gebaseerd op een publieke infrastructuur en gericht op een veel breder en heterogener publiek.

De omvang van de verkiezing en van de stembiljetten die aanwezig zijn bij de Belgische politieke verkiezingen, doet ook vragen rijzen over de IT-middelen die nodig zijn om de verkiezingsgegevens te hosten en de correctiebewijzen van de resultaten te berekenen. We behandelen deze kwesties hieronder.

3.3.2.2 Tijdlijn

Een werkgroep opzetten

Als eerste stap bevelen we aan een werkgroep op te zetten die instaat voor het organiseren van de end-to-end controleerbaarheid van de verkiezingen.

De rol van deze werkgroep omvat ook het definiëren van een aantal belangrijke elementen.

- De strategie voor het selecteren van de sleutelbeheerders: dit omvat het bepalen van het aantal sleutelbeheerders en de manier waarop ze worden gekozen. De belangrijkste eis is ervoor te zorgen dat ze er geen belang bij hebben zich aan te sluiten met de bedoeling de vertrouwelijkheid van de stemmen te schenden en dat ze op betrouwbare wijze aanwezig kunnen zijn voor het genereren van de sleutels vóór de verkiezing en voor het produceren van de bewijzen aan het einde van de verkiezing.
- De strategie voor het ontwerpen van de IT-infrastructuur die nodig is voor de controleerbaarheid: hosting en publicatie van de verkiezingsgegevens, rekenresources die nodig zijn om de vereiste cryptografische verrichtingen uit te voeren.
- De strategie voor het ontwikkelen van de software van de beheerders en van de verificatie van de verkiezingsgegevens. Idealiter worden verschillende actoren gevonden die onafhankelijk van elkaar softwareprogramma's produceren op basis van een duidelijk vastgestelde specificatie. De productie van opensource-referentiesoftware is zeker ook nuttig.
- De communicatiestrategie ten opzichte van de kiezers om hen uit te nodigen bij te dragen aan de individuele controleerbaarheid van de verkiezing.
- De inhoud van de communicatie en de communicatiestrategie ten aanzien van de verkiezingswaarnemers die waarschijnlijk de controles in verband met de universele controleerbaarheid zullen uitvoeren.
- De strategie voor de evaluatie door derden van de procedure voor de verkiezingscontrole, om ervoor te zorgen dat de voorgestelde taken, indien correct uitgevoerd, daadwerkelijk de correctie van de verkiezingsuitslag garanderen.

Het proces simuleren op beperkte schaal

Parallel met de activiteiten van de werkgroep en in samenwerking met die werkgroep kan het nuttig zijn om het end-to-end controleproces op beperkte schaal te simuleren.

Dit zal ons in staat stellen om te begrijpen hoe we het beste de ceremonies waarbij de sleutelbeheerders betrokken zijn, kunnen organiseren, de procedures voor het publiceren van auditgegevens kunnen uittesten en belanghebbende actoren kunnen uitnodigen om controles uit te voeren.

Deze tests zullen ons ook in staat stellen om de behoeften op het gebied van rekenresources, opslaginfrastructuur en netwerkcapaciteit beter te meten.

Het kan nuttig zijn om in ieder geval de eerste simulaties met een klein aantal deelnemers uit te voeren, zodat ze makkelijker kunnen aangeven wat ze niet begrijpen en een luisterend oor vinden, er makkelijker oplossingen worden gevonden voor eventuele vergissingen en een eerlijk debat wordt aangemoedigd dat tot betere procedures leidt.

Eerste pilot

Zodra er voldoende vertrouwen is in de organisatie van het proces voor een end-to-end controle door middel van simulaties, kan een eerste pilot onder reële omstandigheden worden georganiseerd.

De procedure voor de beheerders en de universele controleerbaarheid zou niet significant mogen veranderen in vergelijking met de simulaties. De grootste nieuwigheid is echter de betrokkenheid van kiezers onder reële omstandigheden.

We streven hier naar de uitvoering van die eerste pilot in een klein aantal (1 tot 3) stembureaus. Het komt er vooral op aan om de mechanismen te testen om kiezers te informeren en uit te nodigen om deel te nemen aan de individuele controle, waarbij ze de kans krijgen om feedback te geven over het proces.

De verschillende processen zullen worden aangepast aan de hand van de lessen die tijdens de pilot worden geleerd.

Een van de voordelen van end-to-end controleerbaarheid is dat ze bijna volledig parallel loopt met het normale stemproces en het bijgevolg niet verstoort, in tegenstelling tot RLA's, die, door het hanteren van de papieren stembiljetten, zouden kunnen leiden tot een eventuele hertelling van stembiljetten die vereist zou zijn naar aanleiding van een klacht.

Tweede pilot

Een tweede pilot zal hoogstwaarschijnlijk nuttig blijken om het proces te verfijnen. Afhankelijk van de maturiteit van het systeem kunnen nog tests worden uitgevoerd in een klein aantal gemeenten, of meteen in alle elektronische stembureaus van een volledige kieskring.

Het voordeel van het mikken op een breed publiek is dat het zo mogelijk wordt om kiezers via verschillende communicatiekanalen van informatie te voorzien: televisiefilmpjes, radioreclames en persartikelen behoren allemaal tot de mogelijkheden.

In dit stadium, en vooral als deze pilot plaatsvindt voordat de resultaten zijn gecertificeerd, is het belangrijk om waarnemers in te zetten voor de door de beheerders uitgevoerde ceremonieën, volgens criteria die vergelijkbaar zijn met de criteria die in de telbureaus worden gebruikt.

Veralgemening

Op basis van succesvolle pilots zouden end-to-end controleerbare verkiezingen veralgemeend kunnen worden ingevoerd.

3.3.2.3 Organisatorische aspecten

Hier bespreken we een aantal generieke technische elementen voor de implementatie van end-to-end controleerbare verkiezingen, die kunnen worden gebruikt als input voor de denkoefeningen van de werkgroep die instaat voor het organiseren van de implementatie van het proces. Deze elementen zullen uiteraard worden verfijnd en herzien op basis van de keuzes die de werkgroep maakt en de voorstellen van de partner(s) en leveranciers die betrokken worden bij de implementatie van de oplossing.

Publicatie van de gegevens van de verkiezingen

Een centraal ingrediënt in de uitrol van end-to-end controleerbare verkiezingen is de publicatie van de te controleren gegevens. Die publicatie vereist bijzondere zorg als we een daadwerkelijke controle van de verkiezingsgegevens mogelijk willen maken.

Het eenvoudigweg publiceren van de gegevens op een website is weliswaar nuttig voor archiveringsdoeleinden, maar kan de website in staat stellen om aanzienlijk vals te spelen: een corrupte website (bijvoorbeeld als gevolg van hacking) kan een correcte set stembiljetten tonen aan de kiezers, en een andere set stemmen doorgeven aan de beheerders, waardoor de beheerders een resultaat valideren op basis van stembiljetten die anders zijn dan de stembiljetten die door de kiezers zijn gecontroleerd. Bovendien, zelfs als een beheerder op een bepaald moment een afwijking opmerkt, zal het waarschijnlijk erg moeilijk zijn om ook maar iets te bewijzen, omdat er geen manier zal zijn om een liegende beheerder te onderscheiden van een valsspelende websitebeheerder.

Een voor de hand liggende aanpak om dit probleem op te lossen zou erin bestaan om een digitale handtekening van de verkiezingsgegevens te produceren. Dit betekent dat we, als twee afzonderlijke gegevensreeksen worden ondertekend en gepubliceerd, en als dit wordt ontdekt, kunnen bewijzen dat het publicatieproces van die gegevens corrupt is. We krijgen echter te kampen met twee moeilijkheden:

1. Hoe kan een kiezer zeker zijn van de authenticiteit van de verstrekte handtekening? Hiervoor is een authentieke versie van de verificatiesleutel nodig. Als de kiezer echter de verificatiesleutel verkrijgt via de corrupte website, zal de corrupte website een valse verificatiesleutel verstrekken, die de onjuiste verkiezingsgegevens zal valideren, maar niet als bewijs kan worden gebruikt. Bovendien, als we verificatie vanaf een website mogelijk willen maken, wordt de verificatiecode van de handtekening ook door de website geleverd en zal die code om het even welke handtekening geldig verklaren, ongeacht de werkelijke geldigheid. Helaas hebben beschikken browsers momenteel niet over een mechanisme om onafhankelijk een handtekening te verifiëren op gegevens die door een website worden aangeleverd. Het gebruik van een specifieke app die gedistribueerd wordt via een app store voor smartphones of tablets kan een gedeeltelijke oplossing bieden voor dit probleem. In de praktijk beperkt dit echter de toegankelijkheid van de oplossing en betekent het dat er vertrouwen moet worden gesteld in de beheerders van de app store wat betreft de authenticiteit van de app die ze gaan distribueren.
2. Als we ervan uitgaan dat de handtekeningen geldig zijn en correct geverifieerd zijn, hoe detecteren we dan een website die afzonderlijke verkiezingsgegevens distribueert naar verschillende personen? De enige manier om dit soort manipulatie te ontdekken, is door de ondertekende gegevens te vergelijken. Dit is zeker een mogelijke verrichting, maar gezien het gebrek aan faciliteiten om dergelijke vergelijkingen te maken, is het twijfelachtig of zoiets in de praktijk op grote schaal zal worden uitgevoerd.

Een gedeeltelijke oplossing voor het tweede probleem is om over te stappen van een eenvoudige handtekening van de verkiezingsgegevens naar handtekeningen door een groep waarnemers, of naar een gedistribueerd handtekeningprotocol dat alleen door een groep waarnemers kan worden berekend. Deze benadering is zeker interessant in de praktijk [28, 38], al was het maar omdat ze

voorkomt dat een aanvaller die een unieke handtekeningsleutel steelt, de veiligheid van de verkiezing in gevaar brengt, maar ze laat het vertrouwen afhangen van de groep gekozen waarnemers.

Een manier om de kring van waarnemers te openen is het aanmoedigen van de publicatie van kopieën van de verkiezingsgegevens die zijn ondertekend door waarnemers afkomstig van internationale instanties die verkiezingswaarnemingen uitvoeren, door partijen of door andere actoren uit het maatschappelijk middenveld. De taak van deze actoren zou zijn om de authenticiteit van de door hen ontvangen ondertekende verkiezingsgegevens te verifiëren en openbaar te maken – aan deze actoren zou kunnen worden gevraagd om de authenticiteit van de verificatiesleutel voor handtekeningen op verschillende onafhankelijke manieren te verifiëren. Enerzijds stelt deze benadering de kiezers in staat om te controleren of hun stem op een lijst staat die is gepubliceerd door de actor van hun keuze: kiezers kunnen gerustgesteld zijn als hun stem op een lijst staat die is gepubliceerd door de politieke partij van hun keuze, of door een internationale instantie die ze vertrouwen. Dit stelt die waarnemers ook in staat om de autoriteit die de verkiezingsgegevens ondertekent, te controleren, door hun respectieve gegevens te vergelijken om er zeker van te zijn dat ze identiek zijn. Elk verschil tussen versies met geldige handtekeningen zou bewijs zijn van corruptie door de autoriteit die de verkiezingsgegevens publiceert.

Natuurlijk is het denkbaar dat kwaadwillende actoren mogelijk ook valse verkiezingsgegevens willen publiceren. Dit kan gebeuren ongeacht of we de publicatie van kopieën aanmoedigen of niet, net zoals iedereen luidkeels de overwinning van om het even welke kandidaat in een verkiezing kan verkondigen. Het blijft echter makkelijk te bewijzen dat deze actoren kwaadwillend zijn, aangezien ze niet in staat zullen zijn om een versie voor te leggen van de door hen gepubliceerde gegevens die is ondertekend door de autoriteit die instaat voor het publiceren van de verkiezingsgegevens.

De grootste praktische uitdaging van deze benadering bestaat er ongetwijfeld in om verschillende onafhankelijke actoren te identificeren en hen ervan te overtuigen de verkiezingsgegevens te publiceren.

Over blockchains Sommigen hebben voorgesteld om verkiezingsgegevens op een blockchain te publiceren. Volgens ons is dit in het algemeen een te vermijden benadering in de context van politieke verkiezingen.

De aantrekkingskracht van de blockchaintechnologie ligt in het feit dat ze is opgebouwd als een register waarin we informatie publiceren die we beschikbaar en onvervreemdbaar willen houden, wat op het eerste gezicht overeen kan komen met de wensen die we hebben voor auditgegevens van een verkiezing.

Deze onvervreemdbaarheid houdt echter verband met het proces van het bouwen van de blokken. In open blockchains (permissionless), zoals die welke gebruikt worden voor cryptomunten zoals de bitcoin, is het fundamentele idee om te beschikken over een mechanisme zonder een centrale autoriteit en om een proces van afstemming, of consensus, op te zetten tussen actoren die een verschillende kijk hebben op de gegevens die op de keten geregistreerd staan (in vereenvoudigde termen: de persoon met de 'grootste' keten die bepaalde regels respecteert, 'wint').

Een politieke verkiezing is een heel ander proces: er is een autoriteit belast met het organiseren van de verkiezing, volgens duidelijk vastgestelde wetten. Deze autoriteit bepaalt de lijst van kandidaten die op de stembiljetten staan, de tijdstippen waarop mensen kunnen stemmen, publiceert de

resultaten van de verkiezingen, enz. En deze autoriteit is gehouden aan een zekere transparantie: ze moet met name waarnemers de kans bieden om te controleren of ze zich aan de geldende regels houdt. Deze autoriteit neemt dus een centrale plaats in en het is de bedoeling dat alle aandacht van de waarnemers op haar is gericht om zich ervan te vergewissen dat de verkiezing wel degelijk volgens de geldende regels is verlopen.

Het gebruik van een blockchain om verkiezingsgegevens te publiceren doet precies het tegenovergestelde: de publicatieverantwoordelijkheden van een duidelijk geïdentificeerde autoriteit worden verwaterd naar een reeks computers die worden gecontroleerd door doorgaans anonieme personen die zich overal ter wereld kunnen bevinden, wier belangen mogelijk heel anders zijn dan die van de burgers van het land waar de verkiezingen plaatsvinden, en die over het algemeen geen verantwoording hoeven af te leggen voor hun handelingen in het land dat de verkiezingen organiseert.

De kwestie is uiteraard heel anders bij een gesloten (permissioned) blockchain die beheerd wordt door actoren die duidelijk geïdentificeerd zijn door de verkiezingsautoriteit. In bepaalde contexten kan dit type blockchain een optie zijn die meer weerstand biedt tegen binnendringing. Maar het is zeker niet de enige optie.[20]

Ceremonie rond het genereren van de sleutels

Zoals hierboven vermeld, is de eerste stap in het end-to-end controleerbare verkiezingsproces het genereren van cryptografische sleutels door een groep beheerders.

Deze beheerders worden gekozen als betrouwbare personen die er weinig belang bij hebben om met elkaar samen te spannen teneinde de vertrouwelijkheid van de stemming te schenden. We kunnen denken aan magistraten, notarissen of zelfs partijvertegenwoordigers die veel te verliezen zouden hebben als hun kiezers te horen zouden krijgen dat ze een zo fundamentele voorwaarde als het stemgeheim bij verkiezingen niet hebben gerespecteerd.

Er kan een willekeurig aantal beheerders worden gekozen en er kan een quorum van beheerders worden vastgesteld om het proces voor de productie van controleerbaarheidsgegevens te voltooien. Een mogelijke keuze is om vijf beheerders aan te stellen en te bepalen dat er minimaal drie van hen nodig zijn om de vereiste gegevens te produceren.

Dit quorum van drie van de vijf personen impliceert het volgende:

- zelfs als twee beheerders verdwijnen, hun sleutel verliezen, weigeren deel te nemen aan het proces, het slachtoffer worden van een ongeval of om een andere reden niet beschikbaar zijn, is het nog steeds mogelijk om het volledige gegevensproductieproces uit te voeren;
- als drie beheerders samenspannen en beslissen vals te spelen, kunnen ze de stemmen bepalen van de kiezers van wie ze een kopie hebben van de trackingnummers van het stembiljet.

---

[20] Er is veel geschreven over de potentiële rol van blockchains bij verkiezingen. Een voorbeeld van een bespreking van deze rol is te vinden in Scientific American: *https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/.*

Andere opties die soms worden voorgesteld zijn om een quorum van twee van de drie, of vier of vijf van de zes of zeven personen te eisen. We wijzen erop dat dit quorum alleen betrekking heeft op de vertrouwelijkheid van de stemmen: zelfs een coalitie van alle beheerders zal niet in staat zijn om de correctiebewijzen van de verkiezingsresultaten te vervalsen.

De eerste handeling van die beheerders is het genereren van de sleutels. Hiervoor hebben ze elk een laptop of tablet nodig die is uitgerust met de juiste software. De laptop en de software kunnen door de organisatoren van de verkiezing worden geleverd, maar het kan de voorkeur hebben dat de beheerder die op onafhankelijke wijze aanschaft. Aangezien het stemgeheim afhankelijk is van de laptop en de software, kan het een voordeel zijn om onafhankelijke toestellen en software te gebruiken om het risico te beperken dat eenzelfde kwetsbaarheid aanwezig is in alle gebruikte laptops of softwareprogramma's. Dit vereist natuurlijk dat de beheerder toegang heeft tot een redelijk veilige laptop en software van goede kwaliteit.

De toestellen van de beheerders communiceren vervolgens onderling, doorgaans gedurende een paar seconden, om de sleutels te genereren en het noodzakelijke niveau van redundantie te creëren, zodat de stemverrichtingen kunnen worden uitgevoerd door het gekozen quorum. Deze communicatie vindt doorgaans plaats via een geïsoleerd lokaal netwerk, met de hulp van een verkiezingsgegevensbeheerder die de door elke beheerder meegedeelde openbare informatie verzamelt. Aan het einde van de procedure voor het genereren van de sleutels moeten de beheerders ervoor zorgen dat de verzamelde openbare gegevens wel degelijk coherent zijn met de gegevens die ze hebben geproduceerd en gebruikt, om zich te verdedigen tegen een beheerder die zich zou voordoen als een of meerdere beheerders, of die andere systeemparameters zou wijzigen.

De openbare gegevens worden een eerste maal gepubliceerd en naar alle stemmachines gestuurd. De beheerders van hun kant bewaren hun laptops en geheime sleutels, die eventueel worden opgeslagen op beveiligde draagbare opslagapparaten (beveiligde USB-sticks, enz.).

Productie van de elektronische stembiljetten en trackingnummers

De productie van de elektronische stembiljetten en de trackingnummers van de stembiljetten is een vrij directe handeling: de stemmachine produceert, op basis van de openbare sleutel die door de beheerders is geproduceerd en de stemintentie die door de kiezer is aangegeven, een versleutelde versie van het stembiljet. Deze versleutelde versie wordt beschikbaar gesteld aan de beheerders en de personen die de correctie van de telling controleren, in de context van de universele controleerbaarheid van het systeem.

De kiezers ontvangen ook een trackingnummer van hun elektronische stembiljet. Dit trackingnummer zou de versleutelde versie zelf kunnen zijn, maar die versleutelde versie is vrij omvangrijk, waardoor ze moeilijk te gebruiken is als trackingnummer. Om deze reden wordt het trackingnummer van het stembiljet berekend als een hashcode van die versleutelde versie, d.w.z. als een unieke vingerafdruk van die versleutelde versie berekend met behulp van een cryptografische hashfunctie, wat het mogelijk maakt om een veel korter resultaat te verkrijgen, ook al blijft de lengte aanzienlijk: doorgaans een vijftigtal letters en cijfers, die op een gemakkelijk leesbare manier moeten worden gepresenteerd.

Dit trackingnummer wordt door de stemmachine afgedrukt en aan de kiezers doorgegeven, zodat ze kunnen controleren of hun stembiljet wel degelijk is meegenomen in de telling.

Het kan ook gebeuren dat kiezers willen controleren of het trackingnummer overeenkomt met hun stemintentie. Daartoe moeten de kiezers, in plaats van hun werkelijke stemintentie in te voeren en het geprinte stembiljet in de stembus te doen, om het even welke stemintentie registreren op de stemmachine, controleren of het geprinte stembiljet wel degelijk de uitgedrukte stem weergeeft, het trackingnummer nemen en aan de voorzitter van het stembureau hun wens kenbaar maken om te controleren of de stemmachine geldige trackingnummers aanmaakt. Het stembiljet en het trackingnummer worden dan gemarkeerd, eventueel met een stempel, als overeenkomend met een teststem. De kiezers bewaren de originele documenten, terwijl een kopie of foto ervan in het stemlokaal wordt bewaard. Op het moment van de telling wordt aan de beheerders gevraagd om een verifieerbaar bewijs te leveren dat het afgedrukte trackingnummer wel degelijk overeenkwam met de ongecodeerd afgedrukte stem. Deze bewijzen worden samen met de verkiezingsgegevens openbaar gemaakt en de kiezers kunnen het ontvangen trackingnummer gebruiken om ze te controleren.

Dit proces verklaart waarom het geteste stembiljet niet eveneens in de stembus mag worden gedeponeerd: het proces om de geldigheid van het trackingnummer te verifiëren vereist de publicatie, zichtbaar voor iedereen, van de inhoud van het stembiljet in kwestie, wat uiteraard niet aanvaardbaar is voor een stembiljet dat in de stembus wordt gedeponeerd. We merken wel op, en dit is een centraal element van het protocol, dat de stemmachine het stembiljet en het trackingnummer moet afdrukken *voordat* bekend is of het stembiljet in de stembus zal worden gedeponeerd, of zal worden gecontroleerd. Op deze manier kan de stemmachine haar strategie niet aanpassen door te proberen alleen vals te spelen met stembiljetten die in de stembussen worden gedaan.

Het spreekt voor zich dat een kiezer ook tot de vaststelling kan komen dat het door de stemmachine afgedrukte stembiljet niet overeenstemt met de stemintentie die hij of zij meent te hebben uitgedrukt. In dat geval wordt dezelfde procedure voor het ongeldig maken van het stembiljet gevolgd en wordt de kiezer uitgenodigd om opnieuw te stemmen. Het is belangrijk dat het stembureau kennis neemt van deze twijfel aan de eerlijkheid van de stemmachine, en dat deze informatie deel uitmaakt van de rapportage over de werking van het systeem, om te bepalen of het nodig is om een grondige audit van bepaalde stemmachines uit te voeren.

Audit van de stembiljetten

Aan het einde van de stemverrichtingen worden de gegevens die overeenstemmen met de versleutelde en geverifieerde stembiljetten gepubliceerd. Alle kiezers kunnen op die manier controleren of het trackingnummer dat overeenkomt met het stembiljet dat in de stembussen is gestopt, daadwerkelijk voorkomt in de lijst van stembiljetten die zullen worden geteld, en of het volgnummer of de volgnummers van het stembiljet of de stembiljetten waarvoor ze om een controle hebben gevraagd, wel degelijk zijn opgenomen in de lijst van stembiljetten die moeten worden gecontroleerd.

In de praktijk zullen websites die de kiezers deze verificatiemogelijkheden bieden, de kiezers kunnen uitnodigen om de eerste vijf tekens van het trackingnummer van hun stembiljet in te voeren, en de website zal daarop reageren door alle trackingnummers te verstrekken die ze heeft en die beginnen met deze vijf tekens. De kiezers kunnen dan nagaan of hun trackingnummer wel degelijk is vermeld.

Het bedrijf Enhanced Voting stelt een voorbeeld voor van een website die dit soort verificatie mogelijk maakt. De afbeelding *[fig:bb-example]* toont een voorbeeld van gegevenspublicaties die zijn geproduceerd met ElectionGuard voor de algemene verkiezingen van november 2023 in College Park, Maryland. Het is thans mogelijk om de aanwezigheid van je stembiljet te verifiëren op het adres:

https://app.enhancedvoting.com/results/public/cc/CollegePark/nov23

Als je bijvoorbeeld de reeksen *ØD1C*, *2E3E* of *6AC7* invoert, krijg je de volledige trackingnummers te zien, die de kiezers kunnen controleren op basis van de kopie die ze hebben ontvangen op het moment dat ze hun stem uitbrachten. Sommige stembiljetten werden in de stembus gedaan, in welk geval de inhoud niet zichtbaar is. Andere stembiljetten zijn ongeldig verklaard met het oog op verificatie en de inhoud van het stembiljet verschijnt dan wel. Merk op dat de trackingnummers als één enkele lange reeks worden weergegeven, wat de kiezers meteen niet helpt om te controleren of die reeks correct is. De reeks maakt ook gebruik van de hexadecimale weergave, wat niet de meest compacte is en ertoe kan leiden dat kiezers het cijfer nul verwarren met de letter O. Er zijn talloze variaties mogelijk, waaronder: het gebruik van een alfabet en getallen waarvan potentieel onduidelijke symbolen worden uitgesloten, het weergeven van symbolen in blokjes van vijf, eventueel op twee regels, of omgeven door genummerde kaders om de vergelijkingen te vergemakkelijken, enz.

In het geval van een probleem worden de kiezers uitgenodigd om contact op te nemen met een bevoegde autoriteit, waarschijnlijk op het niveau van de kieskring, waar personen zijn opgeleid om de communicatie te registreren van kiezers die denken dat hun trackingnummer ontbreekt. Die personen zullen de sporen daarvan bijhouden in het pv van de verkiezing.

Het zal belangrijk zijn om absurde klachten te kunnen detecteren: het komt erop aan te controleren of de kiezers op de juiste manier hebben geprobeerd om de aanwezigheid van hun trackingnummer te controleren en, indien nodig, hen te verzoeken de originele documenten te tonen die door de stemmachine zijn geproduceerd, en die op specifiek papier zullen worden afgedrukt om het moeilijker te maken voor wie valse trackingnummers zou willen produceren, en die ook een stempel kunnen dragen die in het stemlokaal is aangebracht.

Zoals bij elk incident in een verkiezing, zal het ook een kwestie zijn van het meten van de omvang van het incident om te bepalen of het invloed zou kunnen hebben op de uitkomst van de verkiezing. In geval van twijfel kan aan de kiezers worden gevraagd om te bevestigen dat ze de aanwezigheid van hun stembiljet wel degelijk hebben kunnen controleren, wat erop zou kunnen wijzen dat de klacht over een ontbrekend stembiljet een op zichzelf staand probleem is. Een controle van de in de stembureaus toegepaste procedures kan ook helpen om de oorsprong van het ontbrekende stembiljet te begrijpen en de omvang van een eventueel probleem vast te stellen.

Vertoon van de bewijzen van correctie van de verkiezingsuitslag

Zodra er voldoende vertrouwen is dat de juiste trackingnummers zijn gepubliceerd, zowel voor de stembiljetten die moeten worden geteld als voor de stembiljetten die moeten worden getest, worden de beheerders verzameld voor de tweede fase van hun taak: het leveren van bewijzen van de correctie van de verkiezingsuitslag.

Dit houdt in dat de geldigheid van alle gepubliceerde verkiezingsgegevens wordt bevestigd en dat elke aanwezige beheerder wordt verzocht om zijn laptop en geheime sleutel te gebruiken om het protocol te starten voor het produceren van bewijzen van de correctie van de verkiezingsuitslag, evenals bewijzen van de geldigheid van de trackingnummers die zijn geproduceerd voor de stembiljetten waarvan de verificatie is aangevraagd.

De verificatie van alle verkiezingsgegevens is waarschijnlijk een te lastige taak om in een paar minuten uit te voeren op een standaardlaptop. Deze verificatie vereist echter geen gebruik van geheime sleutels en kan door iedereen worden uitgevoerd. De beheerders kunnen daarom een beroep doen op derden van hun keuze om deze controles uit te voeren. Het produceren van de bewijzen zelf is daarentegen een zeer eenvoudige taak en kan eenvoudig worden uitgevoerd op de laptops van de beheerders.

Deze bewijzen worden toegevoegd aan de verkiezingsgegevens en gepubliceerd, zodat derden ze ook kunnen controleren, waardoor de verkiezing universeel controleerbaar wordt.

Zodra de verkiezingsresultaten definitief gevalideerd zijn, kunnen alle geheime sleutels van de beheerders vernietigd worden, om het risico verder te beperken dat deze sleutels op een dag in verkeerde handen vallen.

3.3.3 Beoordeling van de complexiteit van de berekening

Terwijl een RLA een inspanning vergt om de papieren stembiljetten te verwerken, vergen end-to-end technieken vooral een inspanning op het gebied van rekenkracht, die in bepaalde contexten prohibitief kan worden.

Hier beoordelen we een mogelijke aanpak voor het uitvoeren van de cryptografische verrichtingen die in de vorige delen zijn besproken. Dit is zeker niet de enige mogelijke benadering en er zijn tal van andere oplossingen, waarvan sommige niet zo veeleisend zijn.

We hebben ervoor gekozen om ons te baseren op de bekendste technieken, die tot nu toe het meest zijn toegepast. Als ze voldoende efficiënt blijken te zijn voor de Belgische context, lijken ze ons een geschikte keuze. Aan het gebruik van rekenkundig efficiëntere technieken zijn vaak ook bepaalde nadelen verbonden:

- complexere technieken leiden bij hun implementatie vaker tot fouten,
- complexere technieken resulteren in code die voor derden moeilijker te auditeren is,
- complexere technieken zijn over het algemeen gebaseerd op sterkere aannames, waardoor de kans groter is dat ze onjuist blijken,
- complexere technieken maken het moeilijker om code te produceren waarmee de auditgegevens die tijdens een verkiezing worden gepubliceerd, kunnen worden geverifieerd.

Het blijft wel zo dat de uitrol van de technieken die we hier bespreken, op zijn vroegst over vijf jaar zal plaatsvinden. Tegen die tijd zal de maturiteit van verschillende technieken zeker geëvolueerd zijn, net als de bibliotheken van beschikbare cryptografische tools.

Praktisch gezien volgen we zo dicht mogelijk de cryptografische protocollen die momenteel worden gebruikt in ElectionGuard, waarvan versie 2.0 afgelopen augustus is gepubliceerd [31] en die de

afgelopen drie jaar is gebruikt bij verschillende politieke verkiezingen in de VS. De protocollen in ElectionGuard zijn een evolutie van de protocollen die al aanwezig waren in het systeem van Cramer, Gennaro en Schoenmakers [27] uit 1997 en die worden gebruikt in systemen als Helios [2] en Belenios [24]. De ElectionGuard-specificatie is openbaar en referentie-implementaties zijn gepubliceerd in open source onder de MIT-licentie.

We zullen de details van het systeem hier niet reproduceren, maar we vermelden de belangrijkste kenmerken ervan, waarbij we die kenmerken toelichten die het meest nuttig zijn voor het hier beoogde systeem. We staan ook stil bij de weinige elementen die verband houden met de Belgische specifieke kenmerken en die momenteel nog niet beschikbaar zijn in ElectionGuard.

3.3.3.1 Basisbouwstenen en keuze van de parameters

ElectionGuard bouwt zijn cryptografie op rond twee basiselementen:

- Een cyclische groep $\mathbb{G}$ waarin het Diffie-Hellman-beslissingsprobleem [7] verondersteld wordt moeilijk op te lossen te zijn. ElectionGuard gebruikt een subgroep van orde q van een multiplicatieve groep $\mathbb{Z}_p^*$, waarbij p een priemgetal van 4096-bits is en q een priemgetal van 256-bits is.
- De hashfunctie met HMAC-sleutel zoals gedefinieerd in de standaard FIPS 198-1 en geïmplementeerd op basis van de SHA-256-functie zoals gedefinieerd in de standaard FIPS 180-4.

Het is mogelijk om ElectionGuard met andere groepen te gebruiken, en het gebruik van een eerste p van 3072 bits zal de werking van de protocollen versnellen, waarschijnlijk zonder hun veiligheid significant te verminderen[21].

3.3.3.2 Gebruikte protocollen

Versleuteling

De groep $\mathbb{G}$ wordt gebruikt om de keuzes van de kiezers te versleutelen met het ElGamal-versleutelingssysteem [32]. Op basis van een generator g van $\mathbb{G}$ wordt een geheime sleutel x gegenereerd op een gedistribueerde manier door de beheerders, en wordt een openbare sleutel $y = g^x$ berekend, met behulp van een protocol dat lijkt op het protocol dat is voorgesteld door Pedersen [48]. Voor elke kandidaat op het stembiljet berekenen we een versleuteling $(c, d) = (g^r, y^{r+v})$ van de keuze van de kiezer v, verborgen met behulp van een willekeurig getal r, uniform gekozen uit $\mathbb{Z}_q$. De keuze v is 1 als de kiezer de kandidaat heeft gekozen die overeenkomt met de versleutelde versie en is 0 als de kiezer de kandidaat niet heeft gekozen (de vakjes bovenaan de lijst worden gewoon behandeld als een extra kandidaat die op 1 wordt gezet zodra een kandidaat van de lijst wordt gekozen). Elke sleutel die door ElectionGuard wordt geproduceerd, telt dus 8192 bits.

Een belangrijke eigenschap van de ElGamal-versleuteling zoals hier gebruikt, is zijn additieve homomorfisme: als ik term voor term de versleutelingen van twee keuzes v_0 en v_1, die respectievelijk zijn versleuteld met de willekeurige getallen r_0 en r_1, vermenigvuldig, verkrijg ik een

[21] Zie bijvoorbeeld *https://www.keylength.com/*.

versleuteling van $v_0 + v_1$ met behulp van $r_0 + r_1$. Dit maakt het mogelijk de stemmen te totaliseren zonder dat ze ontsleuteld hoeven te worden: als ik wil weten hoeveel stemmen een kandidaat heeft behaald, kan ik alle door de kiezers geproduceerde versleutelingen voor deze kandidaat met elkaar vermenigvuldigen. Dit levert een unieke versleutelde versie op van het aantal verkregen stemmen, die ik dan kan ontsleutelen zonder het stemgeheim te schenden.

Het feit dat de individuele stembiljetten, die bestaan uit het geheel van de versleutelingen die voor elk van de kandidaten op het stembiljet zijn geproduceerd, niet worden ontsleuteld, vormt echter een probleem: een kwaadwillende machine zou bijvoorbeeld $v = 1000$ kunnen versleutelen om 1000 stemmen aan een kandidaat te geven via één enkel stembiljet.

Zero-knowledge-proofs

Dit wordt verhinderd door voor elke versleuteling een zero-knowledge-proof te leveren dat die versleuteling daadwerkelijk 0 of 1 versleutelt, en geen andere waarde. De zero-knowlegde-proof garandeert dat het bewijs niet onthult of de versleutelde waarde 0 of 1 is: het bewijst alleen dat het om een van deze twee waarden gaat.

ElectionGuard gebruikt een bewijs gebaseerd op het Chaum-Pedersen-protocol [12], gebruikt in disjunctieve vorm volgens de techniek van Cramer, Damgård en Schoenmakers [26], en niet-interactief gemaakt volgens de Fiat-Shamir-heuristiek [33].

Concreet worden op basis van een versleuteling $(c, d) = (g^r, y^{r+v})$ of $v \in \{0,1\}$ de volgende elementen berekend:

$(a_0, b_0) = (g^{s_0}, y^{s_0+vt_0})$ $(a_1, b_1) = (g^{s_1}, y^{s_1+(v-1)t_1})$
$e = \text{HMAC}(K; 0\text{x}21, c, d, a_0, b_0, a_1, b_1)$
$e_0 = (e - t_1)(1 - v) + t_0 v$ $e_1 = t_1(1 - v) + (e - t_0)v$
$f_0 = s_0 - e_0 r$ $f_1 = s_1 - e_1 r$

waarbij s_0, s_1, t_0, t_1 willekeurige elementen zijn, gekozen in $\mathbb{Z}_q$, K een hashcode is van de beschrijving en de openbare sleutels van de verkiezing, en $0\text{x}21$ een identificator van het bewijs is. Het bewijs zelf bestaat uit (e_0, e_1, f_0, f_1), dat 1024 bits lang is, en de manier om het te verifiëren is vermeld in de specificatie van ElectionGuard [31].

Deze bewijzen volstaan echter niet om aan te tonen dat een stembiljet geldig is: een Belgisch stembiljet is alleen geldig als de kiezer louter kandidaten van één partij heeft geselecteerd (of één lijststem heeft gegeven). Dit kan worden bereikt door een nieuw bewijs te bouwen dat, in dit stadium, niet is opgenomen in ElectionGuard, maar gebaseerd is op zeer vergelijkbare technieken.

Er kan in twee stappen te werk worden gegaan. Allereerst vermenigvuldigen we alle berekende versleutelingen, kieslijst per kieslijst. Als we m kieslijsten op het stembiljet hebben, krijgen we dus m versleutelingen $(c_1, d_1), \ldots, (c_m, d_m)$. Dankzij de bewijzen dat de versleutelingen die we met elkaar hebben vermenigvuldigd, allemaal 0 of 1 versleutelen, weten we dat, zodra een kandidaat (of de lijststem) uit de lijst i is geselecteerd, de versleuteling (c_i, d_i) de versleutelde versie van een niet-nulwaarde zal zijn. We hebben dus te maken met een geldig stembiljet als en alleen als maximaal één van de versleutelingen in de lijst $(c_1, d_1), \ldots, (c_m, d_m)$ een niet-nulwaarde versleutelt.

Als we ervan uitgaan dat $(c_i, d_i) = (g^{r_i}, y^{r_i+v_i})$ voor $i \in \{1, \dots m\}$, waarbij v_i alleen voor index ℓ niet nul is, kunnen we het bewijs als volgt berekenen.

$(a_i, b_i) = (g^{s_i}, y^{s_i+v_i t_i})$ voor $i \in \{1, \dots, m\}$
$e = \text{HMAC}(K; 0\text{x}51, c_1, d_1, \dots, c_m, d_m, a_1, b_1, \dots, a_m, b_m)$
$e_i = i(t_\ell - e)/\ell + e$ voor $i \in \{1, \dots, m\}$
$f_i = s_i - e_i r_i$ voor $i \in \{1, \dots, m\}$

waarbij de waarden s_i en t_i willekeurig worden geselecteerd in $\mathbb{Z}_q$ en K wordt gedefinieerd zoals voorheen. Het bewijs bestaat uit e_i en f_i, en zal daarom $512m$ bits lang zijn.

Om het te controleren, herberekenen we $(a_i', b_i') = (g^{f_i} c_i^{e_i}, y^{f_i} d_i^{e_i})$ voor elke $i \in \{1, \dots, m\}$, we berekenen

$$e = \text{HMAC}(K; 0\text{x}51, c_1, d_1, \dots, c_m, d_m, a'_1, b'_1, \dots, a'_m, b'_m)$$

en controleren dat $(0, e)$ en alle punten (i, e_i) zich wel degelijk op eenzelfde rechte bevinden in $\mathbb{Z}_q \times \mathbb{Z}_q$.

Vorming van de versleutelde stembiljetten

Een stembiljet zal daarom bestaan uit:

- evenveel ElGamal-versleutelingen als er kandidaten zijn op de stembiljetten, waarbij één versleuteling per kieslijst wordt toegevoegd (voor de lijststem),
- evenveel bewijzen van 0-1 als er versleutelingen op het stembiljet staan,
- een bewijs dat de kiezer niet meer dan één kieslijst heeft geselecteerd.

De omvang van een stembiljet met m lijsten en n kandidaten zal daarom $8192(m+n) + 1024(m+n) + 512m = 9216(m+n) + 512m$ bits zijn. Op grote Belgische stembiljetten kan m van de orde van 15 en n van de orde van 300 zijn, wat een lengte geeft van 2910720 bits,

dus ongeveer 355 kB. Voor 8 miljoen stembiljetten[22] is dat goed voor een volume van iets minder dan 3 TB, een volume dat tegenwoordig kan worden opgeslagen op een harde schijf van minder dan 100 euro.

Indien nodig kan deze omvang aanzienlijk worden verkleind door een ander type groep te kiezen: een overstap naar elliptische krommen van 256 bits zou de grootte van de stembiljetten bijvoorbeeld met een factor 5 tot 6 verkleinen. Het gebruik van andere types zero-knowledge-proofs kan deze grootte nog verder verlagen met een factor 2 tot 3 [30]. Het zou ook mogelijk zijn, in de hier beoogde context, om de ElGamal-versleutelingen te vervangen door multi-commitments van Pedersen [49], wat opnieuw zou leiden tot aanzienlijke winst in termen van datavolumes.

We gaan niet verder in op deze technieken: ons doel in dit verslag is om vast te stellen dat de voorgestelde aanpak realistisch is in termen van rekenkracht met behulp van grotendeels

[22] Er waren 7.989.802 geregistreerde kiezers en 7.218.633 ingediende stembiljetten bij de Belgische federale verkiezingen van 2019. *https://elections.fgov.be/sites/default/files/inline-files/CK_TauxParticip.xlsx*

standaardtechnieken, in plaats van de sterk aan verandering onderhevige grenzen vast te stellen van wat bereikt kan worden met de meest geavanceerde technieken.

Het trackingnummer voor het stembiljet van elke kiezer kan worden berekend als een hash van alle versleutelingen van het stembiljet (met een bepaalde hoeveelheid contextuele informatie), d.w.z. 256 bits met SHA-256, die kan worden afgedrukt in de vorm van ongeveer vijftig tekens. De opslag van 8 miljoen trackingnummers

vertegenwoordigt dan 250 MB, het equivalent van een paar tientallen foto's gemaakt door een recente smartphone.

Bewijs van de correctie van de uitslag

Als we een reeks stembiljetten hebben waarvan we de geldigheid kennen dankzij de hierboven beschreven zero-knowledge-proofs, wordt het eenvoudig om versleutelingen voor de verkiezingsuitslag te verkrijgen (één versleuteling voor elke kandidaat) door de versleutelingen op elk stembiljet te vermenigvuldigen, kandidaat per kandidaat.

Aan de beheerders kan dan worden gevraagd om een zero-knowledge-proof te leveren dat deze versleutelingen voor het resultaat van elke lijst en elke kandidaat wel degelijk consistent zijn met de verkiezingsuitslag. ElectionGuard doet dit eenvoudigweg met behulp van een Chaum-Pedersen-bewijs.

Publicatie van de auditgegevens

Voor de individuele controleerbaarheid is het essentieel om alle hashcodes van de stembiljetten te publiceren, zodat de kiezers kunnen controleren of hun stembiljet wel degelijk is geregistreerd, zonder wijzigingen, voor opname in de telling. Zelfs op de schaal van heel België blijft deze publicatie in de orde van grootte van een kleine website, zowel wat betreft de hoeveelheid gegevens die moeten worden opgeslagen als wat betreft het verkeer dat nodig is om de kiezers in staat te stellen de aanwezigheid van hun trackingnummer te controleren.

Deze lichtheid is bijzonder welkom om de replicatie van deze lijst met trackingnummers te vergemakkelijken voor verschillende partijen, officiële waarnemers of actoren uit het maatschappelijk middenveld die er een kopie van zouden willen hosten.

Aan de andere kant is de publicatie van alle versleutelde stembiljetten en de bewijzen, op de schaal van België, veeleisender en kan ze aanzienlijke kosten met zich meebrengen als velen toegang willen krijgen tot deze gegevens. Als we bijvoorbeeld uitgaan van de kosten voor het verzenden van gegevens naar het internet bij de belangrijkste cloudserviceproviders van vandaag, die momenteel ongeveer 0,08 euro per GB bedragen, komen we uit op 240 euro voor de aangegeven 3 TB. Deze kostprijs kan er natuurlijk toe aanzetten om het gebruik van minder gestandaardiseerde cryptografische protocollen, die ook minder veeleisend zijn in termen van datavolumes, te overwegen en/of de verspreiding van de volledige dataset te beperken.

Er kunnen verschillende andere redenen zijn om de verspreiding van deze volledige dataset te beperken:

- De verificatie van deze gegevens heeft vooral zin als we kunnen bevestigen dat die gegevens alleen de gegevens van de kiezers zijn en dat er bijvoorbeeld geen valse stembiljetten in de

urnes zijn gestopt. Aangezien de presentielijsten niet worden gepubliceerd, is het voor geen enkele burger mogelijk om alleen op basis hiervan te controleren of de verkiezingsuitslag correct is – wat natuurlijk niet verhindert dat deze controle zinvol is.

- De publicatie van de gegevens houdt een risico in voor de vertrouwelijkheid van bepaalde stemmen. Als kiezers hun trackingnummer openbaar maken (ervan uitgaande dat ze hun eigen nummer publiceren en niet dat van iemand anders) en als het door een bug of cryptoanalytische vooruitgang mogelijk wordt om het gebruikte versleutelingsmechanisme te breken, zou het immers mogelijk kunnen worden om de inhoud van bepaalde stemmen te weten te komen. Dit is zeker niet de enige manier om het stemgeheim te schenden in een stemsysteem (elektronisch of op papier) en waarschijnlijk ook niet de eenvoudigste, maar het is een mogelijke overdrager.

3.3.3.3 Rekenkracht

De berekeningskosten van de bewerkingen die door de beheerders worden uitgevoerd om de sleutels te genereren en de bewijzen van geldigheid van het resultaat te berekenen zijn onbeduidend: het duurt slechts een paar seconden op een standaardlaptop.

We stellen wel hogere kosten vast voor het maken van de stembiljetten en het controleren van de geldigheid ervan. De voorbereiding van de stembiljetten is zeker een cruciaal element: je wilt niet dat de cryptografische bewerkingen die nodig zijn om de stembiljetten te versleutelen en hun geldigheid te bewijzen, het hele proces vertragen.

We hebben dit getest door de hierboven besproken versleutelings- en bewijsmechanismen te implementeren. Onze Python-implementatie is geïnterpreteerd met Python 3.11 en berust op de gmpy2-bibliotheek (v. 2.2.0) voor de berekeningen op grote gehele getallen.

We hebben het getest op een enkele kern van een relatief oude laptop uitgerust met een i5-7300U-processor uit het eerste kwartaal van 2017, wat waarschijnlijk een redelijk idee geeft van de snelheid die we kunnen hopen te vinden op een processor, over het algemeen low-end, die we zullen aantreffen in een stemmachine die over een paar jaar gemaakt zal worden.

Onze tests werden uitgevoerd voor twee stembiljetten in de federale verkiezingen van 2019:[23]

- Het Luxemburgse stembiljet, met 11 lijsten met tussen 7 en 10 kandidaten voor in totaal 106 kandidaten, is het kleinste stembiljet van die verkiezingen.
- Het Henegouwse stembiljet, met 15 lijsten met tussen 7 en 28 kandidaten voor in totaal 348 kandidaten, is het grootste stembiljet van die verkiezingen.

[23] De grootte van de stembiljetten varieert aanzienlijk en kan bij andere verkiezingen groter of kleiner zijn. Het stembiljet voor het Vlaams Parlement voor het kiesdistrict Antwerpen in 2019 vermeldde bijvoorbeeld 447 kandidaten, en het stembiljet voor het Brussels Parlement in 2019 vermeldde er 771. Het stembiljet van 2019 voor het Waals Parlement van de kieskring Dinant-Philippeville bevatte 72 kandidaten.

De resultaten in de tabel *[tab:encrypt-ballot]* laten zien dat zelfs voor het grootste stembiljet bij die verkiezingen en de hoogste veiligheidsparameter met een priemgetal van 4.096 bits, de rekentijd voor versleuteling en bewijzen onder 300 ms blijft.

Wetende dat het grootste deel van die berekening kan gebeuren voordat de kiezer zijn voorkeuren selecteert op de stemmachine, is het duidelijk dat deze versleutelingsoperatie in wezen transparant zal zijn.

En als het de bedoeling is om de stembiljetten rechtstreeks te versleutelen naarmate ze worden gescand, dan zien we dat het versleutelingstempo overeenkomt met dat van de snelste hogesnelheidsscanners op de markt. Indien nodig kan de berekening zeer vlot worden geparallelliseerd.

Rekentijd voor de berekening van de versleuteling en het bewijs van geldigheid van een stembiljet voor de verkiezingen van 2019

Kieskring	$\|p\| = 3072$	$\|p\| = 4096$
Luxemburg	81 ms	96 ms
Henegouwen	209 ms	295 ms

Deze korte rekentijden zijn grotendeels te danken aan het feit dat alle hierboven beschreven protocollen alleen exponentiële berekeningen met twee vooraf vastgestelde basissen uitvoeren, waardoor we kunnen profiteren van voorcalculatie. Helaas is dit niet het geval voor de verificatie van de geldigheid van de stembiljetten, waar exponentiële berekeningen met een variabele basis nodig zijn. De verificatietijden die gemeten zijn voor een stembiljet met dezelfde beveiligingsparameters staan in tabel *[tab:verify-ballot]*. Hieruit blijkt dat de verificatietijd voor de grootste stembiljetten kan oplopen tot 3 seconden met de hoogste beveiligingsparameter, maar ook ruim onder een seconde kan blijven voor de kleinste kieskring en een standaardbeveiligingsparameter.

Rekentijd voor de verificatie van een stembiljet voor de verkiezingen van 2019

Kieskring	$\|p\| = 3072$	$\|p\| = 4096$
Luxemburg	0.66s	1.13s
Henegouwen	2.14s	3.33s

Als we 8 miljoen stembiljetten willen controleren, uitgaande van een gemiddelde verificatietijd van 2 seconden per stembiljet, hebben we 185 dagen nodig. Op de machine van de gemiddelde thuisgebruiker is dit waarschijnlijk een prohibitieve berekening. Maar omdat deze berekening in wezen repetitief is en parallel kan worden uitgevoerd, wordt het heel realistisch om ze snel uit te voeren op rekenmachines die zijn uitgerust met 128 tot 256 rekenkernen, die in elke professionele infrastructuur gebruikelijk zijn en kunnen worden gehuurd van leveranciers van clouddiensten tegen ongeveer 5 euro per uur voor machines die zijn uitgerust met 128 vCPU's.

Aangezien het niet hoogdringend is om de geldigheid van de stembiljetten te controleren, zijn deze resultaten volgens ons voldoende om de haalbaarheid van de benadering aan te tonen. Zoals hierboven vermeld, is het echter mogelijk om deze verificaties aanzienlijk te versnellen door andere technieken toe te passen: overschakelen naar groepen punten op elliptische krommen zal het hele

proces aanzienlijk versnellen, er zijn 'batching'-technieken om de verificatie van de bewijzen te versnellen, en het is uiteraard ook mogelijk om meer geavanceerde bewijstechnieken toe te passen, waardoor efficiëntere verificaties mogelijk zijn. Deze worden echter (nog) niet gebruikt in de tools die vandaag algemeen worden ingezet, daarom hebben we ze in dit stadium buiten beschouwing gelaten.

3.4 CONCLUSIE

In dit hoofdstuk hebben we de haalbaarheid onderzocht van het gebruik van de twee meest veelbelovende technieken voor de verificatie van de verkiezingsuitslagen, die de afgelopen vijftien jaar zijn opgedoken in het landschap van de politieke verkiezingen en waarvan de toepassing wordt aangemoedigd door de Raad van Europa.

Het is duidelijk dat de toepassing van deze technologieën extra kosten met zich meebrengt: deze kosten zijn zowel financieel als menselijk, op het vlak van het ontwerp van het systeem, het testen van de verificatieprocedures en de daadwerkelijke implementatie ervan.

Deze kosten moeten worden vergeleken met de potentiële kosten voor ons land van een daadwerkelijke manipulatie van de verkiezingsresultaten, die in een aantal gevallen extreem moeilijk te detecteren zou kunnen zijn in het huidige systeem, door het gebrek aan voldoende robuuste controle, en ertoe zou kunnen leiden dat de verkeerde personen worden verkozen. Er moet ook een afweging worden gemaakt van de kosten die beschuldigingen van manipulatie van resultaten voor ons land met zich zouden meebrengen, ongeacht of deze manipulatie daadwerkelijk heeft plaatsgevonden of niet: door de hier voorgestelde technieken toe te passen, zou het mogelijk worden om een duidelijk en gedocumenteerd antwoord op dergelijke aantijgingen te geven.

4 ONTWERP VAN BEVOTING II

4.1 INLEIDING

In dit hoofdstuk geven we toelichtingen bij het ontwerp van het BeVoting II-systeem, dat wordt voorgesteld als antwoord op het verzoek van de Directie Verkiezingen van de FOD Binnenlandse Zaken om:

"te definiëren hoe het huidige elektronische stemsysteem met papieren bewijsstuk kan evolueren qua hardware maar ook qua verifieerbaarheid".

De voorgestelde wijzigingen zijn daarom gebaseerd op de twee elementen die in de vorige hoofdstukken zijn ontwikkeld:

- een beoordeling van de kwaliteiten en zwakke punten van het huidige systeem, vergeleken met de ontwikkelingen op het gebied van beschikbare hardware in de afgelopen vijftien jaar,
- de technologische ontwikkelingen op het gebied van controleerbaarheid die hebben plaatsgevonden sinds de invoering van het huidige elektronische stemsysteem en die nu zijn opgenomen in internationale aanbevelingen over elektronische verkiezingen.

De voorgestelde ontwikkelingen zijn dan ook bedoeld om de negen hoofddoelstellingen uit deel *2.5* op te nemen. Die doelstellingen hebben betrekking op het beheer van hardware en software, de toegankelijkheid van het stemsysteem, de transparantie en beveiliging van de software, de controleerbaarheid en de audit van de verkiezingen en de rapportage over de werking van het systeem.

Wanneer verschillende technische keuzes aanvaardbaar lijken, zullen we proberen te vermijden dat opties onnodig worden tegengehouden, om de markt zo open mogelijk te houden.

4.2 SYSTEEMARCHITECTUUR VAN BEVOTING II

Bij onze beschrijving van het BeVoting II-systeem opteren we ervoor de kiezer centraal te stellen. We beginnen dan ook bij de kiezer, wiens stembiljet we volgen tijdens het telproces, en eindigen met kwesties in verband met het onderhoud en de audit.

4.2.1 De stemmachine

Kiezers beginnen met zich te identificeren bij de ingang van het stembureau, waar ze een 'token' ontvangen (momenteel een smartcard, maar op dit aspect komen we later nog terug) waarmee ze aan de stemmachine kunnen vertellen aan welke verkiezingen ze mogen deelnemen (voor de gemeente, de Kamer, Europa enz.). Vervolgens gaat ze naar een stemhokje, waar ze toegang krijgen tot een stemmachine.

4.2.1.1 Functies

Op die stemmachine krijgen de kiezers momenteel het volgende te zien:

- Een smartcardlezer waarin de kiezers de kaart invoeren waarmee ze de stemmachine kunnen activeren en de stembiljetten die hen betreffen, te zien krijgen.
- Een touchscreen dat groot genoeg is om in één oogopslag alle voorgestelde lijsten op het stembiljet en de kandidaten op een lijst weer te geven, zodat kiezers hun keuzes kunnen aangeven en zo nodig bevestigen.
- De uitvoerlade van de printer, die het stembiljet met de keuzes van de kiezer afdrukt.

Het geproduceerde papieren stembiljet heeft de vorm van een kassabon en bevat zowel een samenvatting van het stembiljet, die leesbaar is voor de kiezers en alle gemaakte keuzes vermeldt, als een QR-code om het stembiljet te scannen, die ook de stemintentie (naast andere informatie) bevat en zal worden gebruikt om de stem te tellen.

Geen van de controleerbaarheidstechnologieën vereist een fundamentele wijziging van die functies. Uit de verslagen van het College van Deskundigen en de ontwikkelingen op de markt komen wel een aantal verbeteringen naar voren.

1. Het papieren stembiljet zou kunnen worden afgedrukt op een groter papier, van standaardformaat, waardoor het gemakkelijker te lezen, te controleren en te hanteren is.
2. De toegang tot de machine voor personen met beperkt zicht of die minder mobiel zijn en het dus moeilijk hebben om hun keuzes via het aanraakscherm aan te geven, is complex.

3. De logistiek in verband met de smartcards voor de kiezers is een terugkerend probleem.

We zetten die punten hieronder uiteen.

Afdrukken van het papieren stembiljet

Belgische kiezers hebben regelmatig de mogelijkheid om voorkeuren uit te spreken voor enkele tientallen kandidaten: zo werden in het kiesdistrict Antwerpen op 7 lijsten 37 kandidaten voorgesteld op het stembiljet voor de Kamerverkiezingen van 2019, en een stembiljet zou dus potentieel 37 geselecteerde kandidaten kunnen vermelden. Dit aantal liep op tot 72 kandidaten op verschillende lijsten voor de verkiezingen van 2019 voor het Brussels Parlement.

Deze keuzes worden momenteel afgedrukt op thermisch papier in kassabonformaat (80 mm breed), wat het herlezen ervan niet gemakkelijk maakt, vooral wanneer kiezers hun keuzes voor drie verkiezingen die tegelijkertijd plaatsvinden, moeten herlezen. Een alternatief is om te kiezen voor papier van standaardformaat (A4). Figuur *[fig:la-ballot]* geeft bijvoorbeeld een idee van het formaat van een stembiljet zoals dat wordt gebruikt in het VSAP-systeem van de county Los Angeles[24]. Dit stembiljet verzamelt de antwoorden van de kiezer op 59 verschillende vragen. De structuur lijkt erg op die in België: het stembiljet bevat alleen de keuzes die de kiezer heeft gemaakt, in een formaat dat door de kiezer kan worden gelezen, en voegt ook twee QR-codes toe die worden gebruikt bij het scannen van het stembiljet.

Toegankelijkheid van de stemmachine

In 2019 werd een proefproject uitgevoerd in de gemeenten Aalst en Mechelen om slechtziende of blinde personen de kans te geven om te stemmen met behulp van speciale koptelefoons en selectieboxen. Deze test is uiteraard bemoedigend en de mogelijkheid om dergelijke hulpmiddelen te integreren is een groot voordeel van het gebruik van stemmachines.

[25] De county Los Angeles heeft een innovatieve aanpak geïmplementeerd in zijn VSAP-systeem – Voting Solution for All People – dat vanaf 2019 in gebruik is. Naast het stemsysteem is er ook een applicatie 'Interactive Sample Ballot' beschikbaar om stembiljetten voor te bereiden. De kiezers kunnen die app installeren, doorgaans op hun smartphone.

Met deze applicatie kunnen kiezers die dat wensen, vooraf op hun smartphone of computer toegang krijgen tot de stembiljetten en het stembiljet invullen. Aan het einde van het proces maakt de app een QR-code aan die de keuze van de kiezer weergeeft (die natuurlijk zoveel QR-codes kan maken als hij of zij wil). Met de applicatie kun je echter niet stemmen: het gaat niet om een stemming op afstand.

Als de kiezer echter met de QR-code in het stembureau aankomt, kan hij of zij de code aan een in de stemmachine ingebouwde lezer presenteren, die vervolgens een stembiljet maakt dat overeenkomt met de code. De kiezer blijft volledig vrij om het stembiljet op de stemmachine te controleren en te wijzigen zoveel hij of zij wil, voordat het afdrukproces wordt opgestart.

---

[24] Bron: *https://vsap.lavote.net/wp-content/uploads/2017/09/BMD-Ballot-Specification-Deck-for-RFI-Response.pdf*

[25] *https://vsap.lavote.gov/*

Deze benadering heeft volgens ons meerdere voordelen:

- Ze stelt kiezers die te maken krijgen met grote stembiljetten, in staat om goed na te denken over de stem die ze willen uitbrengen, zonder dat het een vorm van stemmen op afstand wordt die problemen zou opleveren op het gebied van vertrouwelijkheid of het verkopen van stemmen.
- Ze stelt kiezers die moeite hebben met het gebruik van stemmachines, in staat om hun eigen toegankelijkheidstools te gebruiken, aangepast aan hun specifieke behoeften en meestal beschikbaar op hun smartphone of computer, teneinde hun stembiljet voor te bereiden. Dit is zeker eenvoudiger dan zich te moeten aanpassen aan de toegankelijkheidstools op de stemmachine, die de kiezers moeten ontdekken op het stemmoment zelf.
- Ze zou de wachtrijen bij de stembureaus misschien kunnen verminderen: kiezers die hun stembiljet van tevoren hebben voorbereid, kunnen op de verkiezingsdag sneller hun stem uitbrengen.

Natuurlijk kunnen we bezorgd zijn over het risico dat zo'n applicatie mensen aanmoedigt om op een bepaalde manier te stemmen, en over het gebruik van een smartphone in een stemhokje. Wij zijn van mening dat er hier sprake is van een interessant risico-evenwicht tussen een grotere toegankelijkheid en risico's die waarschijnlijk hoe dan ook aanwezig zijn zolang kiezers met een smartphone een stemhokje mogen binnengaan. Deze evenwichtsoefening kan worden beoordeeld in de geest van de bespreking van artikel 40 van de aanbevelingen van de Raad van Europa [22] [vrij vertaald]:

f. [...] De aard en de omvang van de toe te passen beschermingsmaatregelen moeten per geval worden vastgesteld en er moet een billijk evenwicht worden gevonden tussen bepaalde verschillende, maar even belangrijke aspecten, bijvoorbeeld tussen de noodzakelijke veiligheidsmaatregelen en de wens te beschikken over een systeem dat de kiezers gemakkelijk kunnen gebruiken. In een dergelijk geval mag het streven naar gebruiksgemak geen voorrang krijgen boven de noodzaak om een hoog veiligheidsniveau te garanderen, maar kan het wel een rol spelen bij de keuze van de te nemen veiligheidsmaatregelen. Dezelfde overwegingen kunnen gelden in een situatie waar een minimale verbetering van de veiligheid de voorkeur zou krijgen ten koste van de bruikbaarheid.

Merk ook op dat het afdrukken van het stembiljet op een standaardpapierformaat ook voordelen kan bieden voor kiezers die een leeshulpmiddel gebruiken: het is waarschijnlijk gemakkelijker om een app op een smartphone te gebruiken om een standaardpagina te lezen dan om een ticket te lezen.

Keuze van het 'token' dat de kiezer gebruikt om de stemmachine te activeren

De noodzaak om een QR-code op de stemmachine te scannen om een stembiljet vooraf in te vullen, voegt een nieuwe complexiteit toe aan de stemmachine, die dan moet worden uitgerust met een QR-codescanner.

Die nieuwe scanner zou echter de smartcard kunnen vervangen die momenteel wordt gebruikt om de stemmachines te activeren. Een alternatieve oplossing zou zijn om de stemmachines te activeren met behulp van een andere QR-code, die dan zou worden gegenereerd bij de identificatie van de kiezer. In plaats van de kiezer een smartcard te geven, die gevoelig is voor storingen of slechte contacten in de lezers, en waarvan moeilijk te zien is tot welke stembiljetten hij toegang verleent, zou de kiezer kunnen worden voorzien van een gedrukt papier waarop leesbaar de opschriften

staan van de verkiezingen waaraan hij kan deelnemen, evenals een QR-code die door de stemmachine kan worden gescand.

Deze oplossing zou niet alleen het beheer van smartcards en hun lezers overbodig maken, maar ook de verwarring en technische problemen verminderen die regelmatig naar voren komen in de verslagen van de Colleges van Deskundigen [19], [16], [13].

4.2.1.2 Materiaalkeuze

De stemmachines vertegenwoordigen een aanzienlijk deel van de kostprijs van een stemsysteem, en Smartmatic zegt er ongeveer 22.850 te hebben geleverd aan België voor de verkiezingen van 2019[26]. Met de prijs van de stembussen en de machines van de bureauvoorzitters komen we op een kostprijs van ongeveer 50 miljoen euro, gebaseerd op de prijzen van 2016 voor de 4.338 aangegeven stembureaus [47].

Centrale eenheid

De stemmachines in het huidige elektronische stemsysteem worden gevormd op basis van een traditionele mini-pc waarop een aangepaste Ubuntu-distributie draait. Deze pc bevat geen opslagonderdeel (harde schijf, enz.) voor het installeren van een besturingssysteem: het besturingssysteem wordt in het geheugen geladen vanaf een USB-stick wanneer de machine wordt opgestart. Deze pc heeft ook geen netwerkverbinding. Deze specifieke kenmerken zijn bedoeld om het aanvalsoppervlak zo klein mogelijk te houden voor iemand die het systeem in gevaar wil brengen. De pc is wel uitgerust met interfaces voor het aansluiten van een scherm, een kaartlezer en een printer. Hij wordt ook in een gesloten behuizing gestopt, waardoor de verschillende elementen van het systeem met elkaar verbonden blijven, de machines makkelijker te verplaatsen en op te bergen zijn en de toegang wordt bemoeilijkt voor iemand die de machine corrupt zou willen maken.

Sinds de aanbesteding voor de huidige machines, nu bijna vijftien jaar geleden, hebben tal van ontwikkelingen plaatsgevonden op het vlak van IT-apparatuur. Om er maar een paar te noemen:

- De Chromebooks, een assortiment van laptops en tablets dat in 2011 werd geïntroduceerd op basis van een Linux-distributie en dat een toenemende ontwikkeling heeft doorgemaakt, in het bijzonder in de onderwijssector, voornamelijk dankzij de lagere aankoopprijzen[27].
- Er is een tabletmarkt voor het ruime publiek tot stand gekomen, met name met de introductie van de iPad in 2010.
- Er ontstond ook een markt van singleboardcomputers voor het ruime publiek, met de Raspberry Pi[28] die in 2012 op de markt kwam, vaak aangeboden voor enkele tientallen euro's

---

[26] *https://www.smartmatic.com/us/case-studies/belgium-custom-voting-solution-enables-seamless-election-experiences-for-all/*

[27] *https://en.wikipedia.org/wiki/Chromebook*

[28] *https://en.wikipedia.org/wiki/Raspberry_Pi*

en uitgerust met HDMI-aansluitingen voor een scherm en USB-aansluitingen voor een printer, kaartlezer of scanner.

Al deze nieuwe mogelijkheden zijn aantrekkelijk: ze bieden uitzicht op lagere toestelkosten, zowel voor de aankoop als voor de opslag ervan.

Ze vertonen echter ook een aantal obstakels. In een markt die zich nog steeds snel ontwikkelt, blijft het moeilijk om vast te stellen of deze obstakels echt een blokkerende belemmering zullen vormen in de huidige staat van de markt wanneer een aankoop wordt gedaan. Deze bespreking is bedoeld om verschillende criteria naar voren te brengen voor het beantwoorden van deze vraag, die uiteindelijk zal moeten worden opgelost met de leveranciers die zich ertoe zullen verbinden de vereiste ergonomische en veiligheidskenmerken te bieden en het systeem te onderhouden.

1. Noodzaak van een scherm dat groot genoeg is. Alle kandidaten op een lijst – dus tot 72 kandidaten voor het Brusselse Parlement in 2019 – moeten duidelijk leesbaar kunnen worden weergegeven, met voldoende ruimte om de namen foutloos te kunnen selecteren. Dit criterium lijkt veel 'goedkope' tablets en een aantal laptops uit te sluiten. Ter referentie: de stemmachines die momenteel in gebruik zijn, hebben een scherm met een diagonaal van 17 inch, even groot als de grootste laptopschermen die momenteel standaard worden aangeboden.

2. Onderhoud van het besturingssysteem. Veel toestellen worden geleverd met een eigen besturingssysteem, waardoor de mogelijkheden voor systeembeveiligingsupdates beperkt zijn tot wat de fabrikant zal leveren. In 2022 kondigde Samsung bijvoorbeeld een verlenging van de periode voor beveiligingsupdates aan voor de meeste van zijn high-end tablets (S-serie) tot vijf jaar [29], wat duidelijk nog te kort is. Google heeft op zijn beurt in 2023 een verlenging tot tien jaar aangekondigd van de updates voor de Chromebooks[30]. De situatie kan anders zijn in de wereld van de singleboardcomputers: zo blijft de Raspberry Pi 2, die op de markt werd gebracht in 2015, gecertificeerd onder Ubuntu Core 2022, dat gepaard gaat met beveiligingsupdates tot in 2032, wat neerkomt op een supportduur voor het besturingssysteem van minstens 17 jaar[31].

3. Robuustheid bij een faillissement van een fabrikant. Vertrouwen op een zeer specifiek fysiek platform (exotische processor, enz.) stelt je mogelijk bloot aan grotere problemen in het geval dat de fabrikant failliet gaat, in zoverre dat overschakelen naar een nieuw platform grotere veranderingen aan de systeemsoftware vereist. Kiezen voor een toestel waarvoor tientallen nauwe equivalenten bestaan, biedt sowieso meer robuustheid.

4. Flexibiliteit van de hardware. De USB-poorten en de bluetooth- en wifiverbindingen zijn de beste manieren om een computersysteem binnen te dringen. Idealiter zouden we willen dat de machine niet is uitgerust met bluetooth en wifi, maar deze verbindingsmodi zijn vaak in het systeem vastgesoldeerd. Als ze er niet mee zijn uitgerust, zouden we ze willen uitschakelen in

---

[29] *https://news.samsung.com/global/samsung-sets-the-new-standard-with-four-generations-of-os-upgrades-to-ensure-the-most-up-to-date-and-more-secure-galaxy-experience*

[30] *https://blog.google/outreach-initiatives/education/automatic-update-extension-chromebook/*

[31] *https://ubuntu.com/download/raspberry-pi*

de firmware van de machine, wat een probleem kan vormen bij sommige systemen waar de fabrikant de toegang tot dit configuratietype beperkt. We zullen er zeker ook naar streven dat de stuurprogramma's die het besturingssysteem in staat stellen om deze communicatiemiddelen te gebruiken, zich niet op de machine bevinden. Ook nu weer zal dat in een bedrijfseigen systeem niet noodzakelijkerwijs mogelijk zijn. De USB-poorten zijn op hun beurt over het algemeen nodig om de stemmachine te configureren en om de benodigde randapparatuur (printer, kaart- of codelezer, enz.) aan te sluiten. Naast fysieke beveiligingen (die helaas vaak eenvoudig te omzeilen zijn), zal een strikte configuratie van het besturingssysteem het mogelijk maken de apparaten die op deze poorten kunnen worden aangesloten, te beperken.

5. Mogelijkheid tot beveiligd opstarten. Het is van vitaal belang om ervoor te zorgen dat de stemmachines goed werken met de stemsoftware die vooraf is gecertificeerd, en niet met software die door een kwaadwillende zou zijn gewijzigd. De huidige machines beschermen zichzelf tegen dit type aanval door niet te beschikken over een niet-vluchtig geheugen (geen harde schijf, geen SD-kaart) waarmee een aanvaller een klassiek besturingssysteem zou kunnen installeren dat het gecertificeerde besturingssysteem zou imiteren en vervangen. De machines werken dan vanaf USB-sleutels die zijn geïnitialiseerd in een beveiligde infrastructuur. Dit is niet noodzakelijk mogelijk op alle hardwareplatforms, waar niet-vluchtige geheugens vaak door de fabrikant worden vastgesoldeerd. Een gedeeltelijk alternatief, dat vijftien jaar geleden nog niet beschikbaar was, maar dat sindsdien matuur is geworden en ondertussen geleidelijk wordt toegepast, onder andere in stemmachines, als vervanging voor of aanvulling op het ontbreken van niet-vluchtig geheugen, is de mogelijkheid van een beveiligde opstart die wordt gecontroleerd door een TPM ('Trusted Platform Module'), die elke wijziging in de software moet detecteren.

Uiteindelijk denken we dat, in de context van de huidige markt, de meest plausibele oplossingen gebaseerd zijn op micro-pc's, laptops of singleboardcomputers, zijnde de oplossingen die systeemintegrators de meeste vrijheid geven op het gebied van configuratie en beveiliging.

Het is ook niet uitgesloten dat tablet-equivalenten van de door Fairphone geproduceerde smartphones op de markt zullen verschijnen: deze telefoons zijn ontworpen om gemakkelijk te kunnen worden gerepareerd, ze kunnen draaien op opensourcesoftware[32] en worden momenteel geleverd met een beveiligingsondersteuning voor ten minste acht jaar[33]. Een dergelijk platform zou van enorm belang kunnen zijn in de context van stemmachines.

Op dezelfde manier zou een oplossing die gebruik maakt van hardware gebaseerd op een Risc-V-architectuur[34], die steeds meer wordt ontwikkeld door tal van fabrikanten, aanzienlijke voordelen kunnen opleveren in termen van transparantie en weerstand tegen binnendringing door internationale actoren.

---

[32] *https://shop.fairphone.com/fairphone-4-e-operating-system*

[33] *https://support.fairphone.com/hc/en-us/articles/9979180437393-Fairphone-OS*

[34] *https://riscv.org/*

Gedeeld gebruik van de hardware voor de stemming

Een andere mogelijkheid voor het beheer van de hardware komt voort uit de observatie dat de stemmachines slechts bij een zeer klein aantal gelegenheden worden gebruikt, in de huidige staat van de wetgeving alleen op zondag. Dit zeer beperkte gebruik, evenals de problemen in verband met de levensduur van de machines, zou het gedeelde gebruik van toestellen die normaal gesproken doordeweeks in administraties of scholen worden gebruikt en die ook op verkiezingszondagen kunnen worden gebruikt, kunnen aanmoedigen. Het onderhoud en de vernieuwing van de toestellen in het kader van de verkiezingen zouden dan profiteren van wat er hoe dan ook al wordt verricht in de scholen en administraties.

Er kunnen twee benaderingen worden overwogen:

1. De aankoop van stemmachines, gebaseerd op een gestandaardiseerd model dat is getest op de verkiezingsvereisten, waaruit de computers (laptops of pc's en schermen) worden weggehaald voor gebruik buiten de verkiezingen, en weer in elkaar worden gezet voor verkiezingsdoeleinden.
2. De aankoop van toestellen (laptops of pc's en schermen) volgens de gebruikelijke aankoopmethoden van administraties en scholen, waarna die toestellen zouden worden ontleend voor verkiezingsdoeleinden.

Voor deze benaderingen zijn er een aantal obstakels, die ertoe zouden kunnen leiden dat de besparingen op aankoop- en onderhoudskosten kunnen omslaan in organisatorische en operationele kosten en dat het risico op ernstige problemen tijdens verkiezingsdagen toeneemt.

Het overnemen van een van beide benaderingen zou dan afhankelijk zijn van het oplossen van de volgende moeilijkheden.

- *Integriteit van de machines.* Iemand zou de machines die voor de stemming worden gebruikt, kunnen corrumperen door de fysieke onderdelen die ze bevatten of de firmware van deze machines (een niet-vluchtig geheugen dat niet kan worden verwijderd en dat met name het opstarten van het besturingssysteem ondersteunt) te wijzigen. Dit zou kunnen gebeuren tijdens routineonderhoudsbeurten. Het beschermen van de fysieke toegang tot de machines wordt gezien als een belangrijke factor in de veiligheid van een elektronisch stemsysteem. De figuur *[fig:eac-machines-access]* toont, bij wijze van voorbeeld, de voorschriften van de Election Assistance Commission op dit gebied, waaruit de strikte beperkingen blijken die vereist zijn voor de toegang tot de stemsystemen[35]. Zonder een dergelijke bescherming zal het nodig zijn om overtuigende argumenten te vinden om aan te tonen dat de machines niet buiten de

[35] In een voorbeeld dat breed werd uitgemeten in de pers, werd een Indiase onderzoeker die had meegewerkt aan een analyse van de veiligheid van stemmachines die worden gebruikt in India [67], gearresteerd, blijkbaar om informatie te verkrijgen over hoe hij toegang had gekregen tot de stemmachine die hij en zijn collega's hadden gebruikt voor hun analyse *https://freedom-to-tinker.com/2010/08/22/electronic-voting-researcher-arrested-over-anonymous-source/.* Denk ook aan de hevige debatten en juridische procedures die sinds 2020 hebben plaatsgevonden rond (pogingen tot) illegale toegang tot stemmachines in de VS.

verkiezingen om zijn aangepast. We hebben geen weet van een standaardprocedure voor het uitvoeren van dit type verificatie.

De verificatie van de verkiezingen, zowel via RLA's als via end-to-end controleerbaarheid, biedt zeker antwoorden ter beperking van de risico's die gepaard gaan met de corruptie van stemmachines. We wijzen wel op het volgende: *(i)* de verificatie maakt het mogelijk om onjuiste resultaten te detecteren, maar kan niet garanderen dat de juiste resultaten kunnen worden berekend, en het zou een echte ramp zijn om een verkiezing te moeten annuleren, en *(ii)* de verificatie betreft de correctie van de resultaten, niet de vertrouwelijkheid van de stemmen, en machines zouden 'enkel' kunnen worden aangepast om systematisch de stemmen van de kiezers die ze gebruiken te onthullen, wat zeker ook rampzalig zou zijn.

- *Specifieke materiële configuratie van de stemmachines.* Zoals hierboven besproken, moet ervoor worden gezorgd dat de gecertificeerde stemsoftware daadwerkelijk wordt gebruikt op de stemmachines door middel van allerlei beveiligingen, waaronder het ontbreken van netwerkverbindingsmogelijkheden, het ontbreken van niet-vluchtig geheugen en/of de aanwezigheid van systemen voor beveiligd opstarten. Machines die voor andere functies zijn aangeschaft, voldoen niet noodzakelijkerwijs aan deze vereisten, en, in gevallen waarin de machines specifiek zijn aangeschaft om aan de behoeften van de verkiezingen te voldoen, zal een specifieke logistiek nodig zijn voor het ombouwen van de machines, die tijdens hun dagelijkse gebruik waarschijnlijk op verschillende netwerken en verschillende randapparatuur moeten kunnen worden aangesloten. We denken hierbij bijvoorbeeld aan een vervanging of een schrapping van de niet-vluchtige geheugens die buiten de verkiezingen worden gebruikt, en van alle interfaces voor netwerkcommunicatie, in elk geval draadloze.
- *Beschikbaarheid van de hardware voor de verkiezingen.* Er moet altijd voldoende hardware beschikbaar blijven om aan eventuele verkiezingsbehoeften te voldoen, in de praktijk dus continu. Artikel 46 van de Grondwet bepaalt immers dat er binnen veertig dagen vervroegde verkiezingen moeten worden gehouden in geval van een ontbinding van de Kamer[36]. Een dergelijk tijdsbestek is extreem kort en vereist in de praktijk dat ten minste alle apparatuur die nodig is voor elektronisch stemmen, op voorraad is: het aanbesteden, aankopen, configureren en testen van nieuwe machines in een dergelijk tijdsbestek lijkt onrealistisch. De staat van de machines die buiten de verkiezingen worden gebruikt, moet daarom onder toezicht blijven en worden getest. (Dit geldt natuurlijk ook voor de specifiek voor de verkiezingen bestemde stemmachines. Maar testoperaties zijn gemakkelijker uit te voeren als de machines worden opgeslagen op bekende locaties en als ze continu beschikbaar zijn.)
- *Beschikbaarheid van de hardware voor andere gebruiksvormen.* In de aanloop naar de verkiezingen zullen de intensieve controles van de machines, de herconfiguratie ervan voor de verkiezingen en de organisatie van hun uitrol de machines onbruikbaar maken voor andere gebruiksvormen. De machines moeten ook na de verkiezingen beschikbaar blijven, in afwachting van de validatie van die verkiezingen, om gevolg te kunnen geven aan eventuele onderzoekvereisten. Tijdens deze perioden zijn ze dus niet beschikbaar voor ander gebruik.

[36] *https://www.senate.be/doc/const_nl.html#art46*

Alle andere gebruikers van deze apparatuur zullen er zich dus moeten in schikken dat ze gedurende enkele weken rond de verkiezingen niet kunnen beschikken over de apparatuur.

De aanpak om apparatuur te gebruiken die is aangeschaft volgens aankoopprocedures en tijdschema's die losstaan van de verkiezingen, brengt extra uitdagingen met zich mee.

- *Compatibiliteit van de hardware.* De stemsystemen worden ontworpen op basis van een specifiek besturingssysteem, dat in de meeste gevallen een aangepaste Linux-distributie is. Het zal moeilijk zijn om ervoor te zorgen dat dit besturingssysteem zal kunnen opstarten op standaardmachines, die mogelijk fysieke componenten bevatten die niet compatibel zijn. Het is natuurlijk mogelijk om dit soort compatibiliteit te garanderen door er een criterium van te maken bij de aankoop van de apparatuur. De extra kosten die aan dit criterium verbonden zijn, zijn echter moeilijk te voorspellen en tests vóór de aankoop zullen waarschijnlijk elke keer nodig zijn. De diversificatie van de hardware betekent ook dat er verschillende versies van de stemsoftware moeten worden gemaakt, aangepast aan elk type hardware dat wordt gebruikt, met telkens nieuwe risico's op fouten, en dus testvereisten.
- *Variabiliteit in kiezerservaringen.* Apparatuur die in verschillende contexten wordt aangeschaft, zal moeilijker te standaardiseren zijn en vooral de schermformaten zullen waarschijnlijk van plaats tot plaats verschillen qua grootte en resolutie. Dit kan leiden tot een problematische variabiliteit in de weergave van stembiljetten, of zelfs tot situaties waarin het scherm niet alle kandidaten toont. Dit soort problemen kan worden beperkt door systematisch te testen, maar we zullen nooit dezelfde uniformiteit bereiken als met specifieke apparaten. Nogmaals, het zou mogelijk zijn om vereisten op te leggen bij de aankoop om specifieke schermformaten enz. te garanderen.
- *Complexiteit van het installeren van stemhokjes.* De gedeelde apparatuur moet worden verplaatst en geïnstalleerd in de stemhokjes, verbonden met een printer en een QR-codelezer. Gebruikmaken van apparatuur die in andere contexten wordt gebruikt, zal extra organisatorische vereisten met zich meebrengen voor de personen die de stembureaus inrichten, terwijl de aanbevelingen van de Raad van Deskundigen gericht zijn op vereenvoudiging, gezien de moeilijkheden waarmee men vandaag wordt geconfronteerd.

We zijn niet op de hoogte van enig land dat is overgegaan tot een gedeeld gebruik van zijn stemmachines, we kunnen dan ook niet putten uit ervaringen die elders zijn opgedaan.

Het probleem dat het moeilijkst te overwinnen lijkt, is het controleren van de integriteit van de apparaten, een probleem dat momenteel elders wordt opgelost door strikte controle op de toegang tot de machines op te leggen.

De andere moeilijkheden zijn in wezen randvoorwaarden, die niet onoplosbaar zijn, maar die de kosten als gevolg van het gedeeld gebruik zullen doen oplopen. Het is dan ook geen evidentie dat er op het einde van de rit besparingen zouden worden gerealiseerd – ook al is dat uiteraard sterk afhankelijk van de context.

Printer

Het tweede belangrijke onderdeel van de stemmachine is de printer, die het stembiljet van de kiezer afdrukt. De huidige oplossing is het gebruik van een thermische printer met een rol papier van het type kassabon.

Dit levert ergonomische problemen op voor grote formulieren en is niet compatibel met het in batches scannen van de stembiljetten. De flexibiliteit van de stembiljetten die op dit soort papier zijn gedrukt, kan het ook moeilijk maken om ze bij de stembus te scannen.

Het voorstel van BeVoting II is om printers in het klassieke A4-formaat te gebruiken, die:

- het voor kiezers makkelijker maken om de stembiljetten te controleren,
- het voor kiezer makkelijker maken om de stembiljetten te hanteren en te scannen,
- zich gemakkelijker lenen voor het gebruik van leeshulptechnieken voor slechtziende of blinde personen.

Een gevoeliger punt is het type printer dat wordt gebruikt. De momenteel gebruikte technologie van thermisch afdrukken heeft een aantal grote voordelen, waaronder:

- hoge robuustheid en weinig onderhoud dankzij de afwezigheid van inkt en poeder in het systeem,
- beperkte afmetingen,
- geen inktkosten, en
- beperkt energieverbruik.

Thermische kassabonprinters (rollen papier van ongeveer 8 cm breed) zijn heel gebruikelijk, maar het is veel minder gebruikelijk om thermische printers te vinden met een invoerlade die honderden vellen A4-papier bevat, waarmee een vlotte scanning mogelijk is, en met stuurprogramma's voor opensourcebesturingssystemen.

Een alternatief dat gemeengoed is geworden, met name in de Verenigde Staten, is het gebruik van laserprinters. De voordelen van deze printers zijn dat ze zeer gangbaar zijn, bekend bij veel mensen, niet erg duur, robuust en dat ze afdrukken op standaardpapier dat gemakkelijk te scannen is. Ze worden ook breed ondersteund door opensourcebesturingssystemen, wat hun implementatie en eventuele vervanging vereenvoudigt. Ze vereisen echter het gebruik van poedertoners om het afdrukken te ondersteunen en zijn niet zo robuust als thermische printers. Laserprinters werden soms ook uitgesloten omdat ze veel stroom verbruiken wanneer ze aanstaan en/of afdrukken, uit vrees dat ze het elektriciteitsnetwerk in de stembureaus zouden overbelasten. De ontwikkeling van deze printers en hun huidige wijdverspreide toepassing bieden een geruststellend antwoord op deze vrees. Tot slot neemt een laserprinter meer ruimte in beslag dan een thermische printer die in de stemmachine is geïntegreerd: de laserprinter wordt niet in de behuizing van de stemmachine geïntegreerd, maar wordt ernaast geplaatst.

Inkjetprinters, die erg goedkoop zijn, zijn in de praktijk uitgesloten van dit soort toepassingen vanwege hun beperkte betrouwbaarheid en problemen met het drogen van de inkt.

De keuze voor laserprinters lijkt hier het meest plausibel, hoewel het niet uitgesloten is dat er oplossingen op basis van thermische printers kunnen worden gevonden.

Papier

Het gebruikte papier moet gemakkelijk te scannen zijn. Het is ook belangrijk om ervoor te zorgen dat er heel specifiek papier wordt gebruikt, met een watermerk, gemaakt van specifieke vezels, enz. Dit is nuttig als informatiebron voor het onderzoek naar stembussen waarvan de inhoud mogelijk gemanipuleerd is, maar ook voor het opsporen van ongegronde klachten van kiezers, die bijvoorbeeld aangeven dat een vervalst stembiljettrackingnummer ontbreekt in de lijst van stembiljetten die in de telling zijn opgenomen.

Smartcardlezer of scanner

Het laatste onderdeel van de stemmachines in België is de lezer van de smartcards. Deze vereisen logistiek in termen van initialisaties en lezers, en zijn een bron van verwarring geweest tussen verschillende soorten kaarten (de initialisatie van een kaart is niet zichtbaar op de kaart, wat uitstekende sorteerprocedures of een discipline voor het annoteren van de kaarten vereist).

Het voorstel van BeVoting II is om deze kaartlezers te vervangen door QR-codelezers, om de redenen die zijn beschreven in punt *4.2.*

Assemblage

Het beschikken over van een stemmachine die alle onderdelen in één behuizing integreert, zoals nu het geval is, heeft zeker grote voordelen: het maakt het gemakkelijker om de machines te vervoeren en ze in de stemhokjes te installeren, en het vermijdt de problemen van het aansluiten en losmaken van kabels die verschillende componenten verbinden.

Aan de andere kant verhoogt dit de kosten van de oplossing en bemoeilijkt het eventuele hardware-aanpassingen die na een paar jaar nodig kunnen blijken. Het zou de moeite waard kunnen zijn om te kijken naar oplossingen om onderdelen van stemmachines op te nemen in standaardtransportkisten, meestal gemaakt van harde kunststof, die meer flexibiliteit bieden als het gaat om het aanpassen van de apparatuur. De verschillende systeemonderdelen en kabels kunnen bijvoorbeeld worden bevestigd met blokken uit hardschuim, die gemakkelijk kunnen worden vervangen als er nieuwe apparatuur moet worden geïnstalleerd.

Verschillen met de huidige stemmachines

Een voor de hand liggende vraag in dit stadium is om het hier voorgestelde stemmachineconcept BeVoting II op het vlak van hardware te vergelijken met de machines die momenteel in België in gebruik zijn. Het is daarbij de bedoeling duidelijk te maken welke vooruitgang wordt voorgesteld en waar aanpassingen eventueel mogelijk zijn.

- Wat de centrale eenheid betreft, is het aannemelijk dat de micro-pc die momenteel aanwezig is in stemmachines van de tweede generatie, nog steeds toereikend zal zijn om de nieuwe noodzakelijke cryptografische bewerkingen uit te voeren.
- BeVoting II stelt voor om de printers van tickets van 8 cm te vervangen door A4-printers. Er zijn meerdere nadelen verbonden aan het behoud van de huidige printers:

- De validatie van de biljetten op het moment van het scannen zou aanzienlijk complexer zijn. Deze validatie, of een sortering van de papieren stembiljetten per lijst, is nodig voor een efficiënte risk limiting audit.
- De verificatie van de inhoud van de stembiljetten door de kiezers zou minder makkelijk verlopen. In verschillende onderzoeken is gewezen op het belang van het vergemakkelijken van deze verificatie.

Een mogelijke denkpiste zou kunnen zijn om de ticketprinter die nu in de machines zit, uit te schakelen en te vervangen door een aparte printer.

- Het voorstel van BeVoting II is om de smartcardlezer te vervangen door een QR-codelezer. Het behoud van de smartcardlezer zou een aantal nadelen hebben:
  - De huidige problemen met het beheer van de smartcards zouden aanhouden.
  - Bij gebrek aan een QR-codelezer is er geen eenvoudige manier voor de kiezers om hun stembiljetten van tevoren in te vullen en ze in het stemhokje te scannen. Dit vermindert de toegankelijkheid voor mensen die moeite hebben met het gebruik van de machines, en vermindert de verwachte tijdsbesparing als mensen vooraf ingevulde formulieren kunnen gebruiken.

4.2.2 Indienen van het stembiljet en tellen van stemmen

4.2.2.1 Functies

In het huidige elektronische stemsysteem worden de geprinte stembiljetten naar een elektronische stembus gebracht. Hier scant de kiezer de QR-code op het stembiljet, waardoor de stem wordt opgeslagen op de machine van de voorzitter en de stembus wordt geopend. Deze sluit zodra het stembiljet in de stembus is gestopt.

Van alle onderdelen van het huidige elektronische stemsysteem is dit deel wellicht het minst gestandaardiseerd. Het heeft aanleiding gegeven tot een aantal problemen die in de verslagen van het College van Deskundigen aan de orde zijn gesteld, en is in de loop der jaren ook ingrijpend herzien en verbeterd.

Een ander nadeel van dit proces is dat het beperkt is tot het scannen van een QR-code die niet of niet goed is geverifieerd door de kiezer, in plaats van het scannen van de stemintentie zoals herlezen door de kiezer. Overschakelen op stembiljetten die op klassieke A4-vellen zijn gedrukt, zou het mogelijk maken om de hele pagina te scannen (wat moeilijk is voor een smalle, langwerpige kassabon), waardoor het mogelijk zou worden om de stem van de kiezer af te lezen van de door de kiezer in plaats van door de scanner herlezen afdruk. Dit zou het systeem robuuster maken, omdat het dan onmogelijk is voor een stemmachine om met de QR-code te 'sjoemelen'. Dit legt echter vereisten op aan het scan- en tekenherkenningsproces, en de haalbaarheid van deze aanpak wordt waarschijnlijk bepaald door de keuze van de scanapparatuur. Tot op heden hebben we geen weet van enig rechtsgebied dat daadwerkelijk gebruikmaakt van tekenherkenning om gescande stembiljetten te lezen (ofwel worden er QR-codes geïdentificeerd, ofwel de aan- of afwezigheid van markeringen op plaatsen die overeenkomen met het keuzevak van de kandidaat, wat op zich risico's met zich meebrengt). Bovendien kan het sjoemelen met stemmachines ook worden

geïdentificeerd via een risk limiting audit, waardoor de noodzaak om het volledige stembiljet te lezen, wordt beperkt.

Het implementeren van een doeltreffende RLA door 'ballot comparison' legt ook nieuwe vereisten op aan het scanproces: de noodzaak om elk gescand stembiljet te endosseren, met andere woorden van extra informatie te voorzien door er een serienummer op af te drukken in de vorm van een teller (naast informatie zoals een identificatiecode van de scanner of het scanbureau, een scantijdstip, enz.). Voor een RLA is deze bekrachtiging niet nodig. Het maakt het echter wel mogelijk om RLA's te organiseren waarbij een aanzienlijk kleiner aantal stembiljetten moet worden gecontroleerd, of om een volledige telling van de papieren stembiljetten te vermijden.

Praktisch gezien betekent dit het gebruik van een scanner die het papier inslikt en het onderweg bekrachtigt, in plaats van simpelweg een QR-codescanner te gebruiken zoals in het huidige systeem. Het scannen kan gebeuren in pakketten van ongeveer honderd pagina's, en elk pakket gescande stembiljetten wordt in een envelop gedaan, waarop het serienummer van het eerste en laatste gescande stembiljet in het pakket, zoals afgedrukt door de printmodule, wordt vermeld, evenals het aantal stembiljetten in de envelop. Diezelfde nummers zullen worden vastgelegd in een manifest, waarschijnlijk in de vorm van een spreadsheet op een laptop, met het oog op de voorbereiding van de RLA. De enveloppen worden in dozen gedaan die veilig kunnen worden afgesloten voor transport naar locatie waar de risk limiting audit zal worden verricht.

Het scanproces zorgt ook voor een individuele interpretatie van elk gescand stembiljet, in relatie tot het serienummer dat op het moment van bekrachtiging is geproduceerd. Dit maakt het mogelijk om de tijdens de verkiezing uitgebrachte stemmen bij elkaar op te tellen en de uitslag te berekenen, maar ook om de risk limiting audit efficiënt uit te voeren: voor een bepaald aantal willekeurig gekozen serienummers van stembiljetten moet het corresponderende papieren stembiljet zo efficiënt mogelijk kunnen worden teruggevonden en moet een aflezing van het papieren stembiljet kunnen worden vergeleken met de verrichte elektronische registratie. Tot slot zal het scanproces voor elk stembiljet ook een nummer opleveren dat is ontleend aan de QR-code die op het stembiljet is gedrukt, en dat zal worden gebruikt voor de end-to-end controleerbaarheid van de verkiezing. We zullen dit nummer bespreken in het onderdeel over end-to-end controleerbaarheid hieronder.

Scanproces

Concreet zien we zes tijden en plaatsen waar de scanning zou kunnen plaatsvinden:

1. op de stemmachine, die ook zou worden uitgerust met een stembus,
2. bij het deponeren in de stembus,
3. aan het einde van het stemmen, in het stembureau,
4. in de telbureaus op het niveau van het kanton,
5. in een scanbureau op het niveau van het hoofdkantonbureau,
6. in een gecentraliseerd scanbureau op het niveau van het kiesarrondissement.

Op het niveau van de stemmachine

Naar onze mening zijn er verschillende problemen met deze aanpak:

- De QR-codelezer die al op de stemmachine aanwezig is, zou kunnen worden gebruikt om de kiezers uit te nodigen om hun stembiljet in een stembus in het stemhokje te deponeren. Dit maakt het erg moeilijk om te controleren of de kiezers daadwerkelijk hun stembiljet in de urne hebben gedeponeerd (kiezers kunnen het bijhouden, door onoplettendheid, onbekendheid met het systeem of kwaadwilligheid). Dit vereist ook dat de stembiljetten worden opgeslagen op de stemmachine, ook al proberen we op deze plaats binnen het systeem de aanwezigheid van niet-vluchtig geheugen te vermijden.
- We zouden kunnen kiezen voor een systeem voor de inname van het stembiljet, dat het stembiljet tegelijkertijd zou inslikken en scannen en het in een stembus zou deponeren die aan de stemmachine is gekoppeld, zodat de kiezers een gescand stembiljet niet kunnen terugnemen. Het is duidelijk dat dit extra kosten met zich meebrengt voor de stemmachine, evenals niet-standaardonderdelen die moeten worden toegevoegd. Dit levert grote problemen op: de gescande stembiljetten zullen over het algemeen in de stembus worden gestapeld in de volgorde waarin ze zijn gescand, wat bekommernissen oproept over de geheimhouding van de stemming ten aanzien van de personen die de stembus openen. Bovendien, als het afdruksysteem ook wordt gebruikt om het papier in te slikken, om redenen van besparingen en ergonomie, kunnen we ook vraagtekens plaatsen bij het risico dat er extra inscripties op het stembiljet worden gemaakt, waardoor het wordt gewijzigd zonder dat de kiezer dit kan zien[37].
- Deze benadering is niet echt compatibel met de oplossingen voor het endosseren van de stembiljetten, dat nodig is voor efficiënte risk limiting audits: sequentiële aantekeningen op stemmachineniveau zouden duidelijk problematisch zijn wat het stemgeheim betreft.

Bij het deponeren in de stembus

De huidige oplossing, die gebaseerd is op het scannen van een QR-code in kassabonformaat, brengt een aantal hardwareproblemen met zich mee die regelmatig naar voren komen in de verslagen van het College van Deskundigen. Bovendien, met slechts één stembus per bureau, legt elk probleem het stembureau snel lam. Er kunnen ook vraagtekens worden geplaatst bij het geheim van de stemming wanneer zich een scanprobleem voordoet: een kiezer die zijn of haar stembiljet met de hand heeft gemarkeerd, zal een beroep doen op een medewerker van het stembureau die de kiezer te hulp zal snellen bij het scannen van het stembiljet of die een storing in het systeem zal vaststellen – we kunnen ons voorstellen hoe moeilijk het is om het stembiljet, zelfs als het opgevouwen is, in dergelijke omstandigheden geheim te houden.

Een alternatief, dat vaak wordt gebruikt in heel wat elektronische stembussen in de Verenigde Staten, is om de stembus uit te rusten met een scanner die het stembiljet inneemt en leest vooraleer het in de stembus te deponeren.

Deze oplossing, die wordt vergemakkelijkt door het gebruik van papier dat groter en steviger is dan een kassabon, is zeer voordelig voor het scannen van met de hand gemarkeerde stembiljetten: rechtstreeks scannen stelt de machine in staat om een ongeldig of onleesbaar ingevuld stembiljet

---

[37] Zie bijvoorbeeld de bespreking van dit probleem in het VSAP-systeem dat wordt gebruikt in Los Angeles *https://www.politico.com/news/2020/03/03/los-angeles-county-voting-experiment-119157.*

terug te bezorgen aan de kiezer. Dit is hier echter niet het geval, aangezien de stembiljetten worden afgedrukt door de stemmachines, die de geldigheid ervan moeten garanderen.

Een ander voordeel van deze oplossing is dat de stembussen kunnen worden gesloten zodra het stemmen is afgelopen: tegen de tijd dat de laatste kiezer het stemlokaal verlaat, zijn alle stembiljetten gescand.

Deze oplossing is echter nog steeds kwetsbaar voor defecten of vastlopende scanners, die de werking van het stembureau kunnen blokkeren. Ze is ook relatief duur, omdat voor elke stembus nog steeds een scanner nodig is met een gleuf die één A4-stembiljet kan inslikken.

Gezien de beperkte voordelen, de kwetsbaarheid en de ermee verbonden kosten raden we deze aanpak niet aan in België.

Aan het einde van het stemmen, in het stembureau

Deze aanpak houdt het gebruik in van een stembus die volledig standaard is, zoals die welke wordt gebruikt bij de papieren verkiezingen. Die stembus wordt dan geopend zodra de laatste kiezer het stemlokaal heeft verlaten, waarbij de stembiljetten goed worden gemengd voordat ze worden gescand.

De scanners van tegenwoordig nemen met gemak zo'n 70 pagina's per minuut in. Het scannen zelf zou dan ongeveer 34 minuten kunnen duren voor de 2.400 pagina's die zouden overeenkomen met de drie stembiljetten die in een gecombineerde verkiezing worden uitgebracht door de 800 kiezers die een volledig stembureau bezoeken, wat een redelijke hoeveelheid tijd lijkt, zelfs als er enige tijd moet worden toegevoegd om de stembussen te openen, de stembiljetten te mengen en ze in pakketten samen te voegen om ze in de scanner in te voeren.

Deze aanpak heeft het voordeel dat het scannen in een zeer vroeg stadium van het telproces wordt verzorgd, en in het bijzonder voordat de stembiljetten naar een tel- of controlebureau worden vervoerd, zodat het risico van manipulatie tijdens het vervoer wordt vermeden. Als het systeem van end-to-end controleerbaar is, zouden dergelijke manipulaties toch worden ontdekt, wat het belang van dit type fraude beperkt.

Los van vragen over de authenticiteit zullen sommigen het ongetwijfeld ook op prijs stellen om de resultaten van de stemming zo snel mogelijk te ontvangen: door in het stembureau te scannen, bespaar je de tijd die nodig is om de stembussen naar een telbureau te vervoeren.

Aan de andere kant zal deze aanpak zwakker zijn in termen van de vertrouwelijkheid van de stemming: het hanteren van de stembiljetten in kleine stembureaus (de geplande grootte is ten minste 150 kiezers) door personen die aanwezig waren op het moment van de stemming, zou het gemakkelijker kunnen maken om kleine markeringen op de stembiljetten te herkennen, bijvoorbeeld met het oog op het verkopen van stemmen. Dit probleem wordt vermeden bij het stemmen op papier, dankzij de oprichting van telbureaus die onafhankelijk van de stembureaus worden beheerd.

Bovendien is het scannen in het stemlokaal kwetsbaarder, vooral als het stemlokaal afgezonderd ligt: in geval van technische problemen zal het verkrijgen van technische ondersteuning waarschijnlijk trager verlopen dan in meer centrale scanbureaus, en een defect aan een scanner zal het proces volledig blokkeren omdat het stembureau waarschijnlijk maar één scanner heeft. Door

het scannen in elk stembureau te organiseren in plaats van op een meer gecentraliseerde manier, zal ongetwijfeld ook de omvang van de opleiding die nodig is voor de voorzitters van de stembureaus, toenemen, evenals het aantal personen dat moet worden opgeleid in scanverrichtingen.

Dit risico kan anders worden ingeschat in dichtbevolkte gebieden waar bijvoorbeeld vaak meerdere stembureaus in dezelfde school zijn gegroepeerd: een scanner die wordt gebruikt in een stembureau waar het scannen al voltooid is, kan waarschijnlijk gemakkelijk worden ingezet om een defect te compenseren. Het kan ook een goed idee zijn om te beschikken over reservescanners voor meerdere gezamenlijke stembureaus.

Daarnaast zouden er ook noodscanners beschikbaar kunnen worden gesteld in een of meer kantonbureaus, waar de voorzitters van een stembureau de stembiljetten naartoe kunnen brengen in geval van een defect.

In de telbureaus op het niveau van het kanton

Het idee hier is om te werk te gaan naar analogie van de traditionele papieren stembusgang, waarbij de stembussen naar de telbureaus in de kantons worden gestuurd. Deze bureaus bestaan al in kantons die zowel werken met elektronisch stemmen als met stemmen op papier.

Op dezelfde manier te werk gaan voor het scannen biedt een aantal voordelen:

- Er zouden scanbureaus op grotere schaal kunnen worden georganiseerd, uitgerust met een aantal scanners, wat de impact van storingen zou beperken.
- Als het scannen geconcentreerd is op een klein aantal plaatsen, zou het mogelijk zijn om dit te doen in de aanwezigheid, of in de nabijheid, van personen die veel ervaring hebben met het hanteren van scanners en die nuttige hulp of begeleiding kunnen bieden tijdens het proces.
- Scannen op grotere schaal zou het aantal op te leiden personen beperken, en zou ook de behoefte aan opleiding kunnen beperken als er technische ondersteuning ter plaatse beschikbaar is.
- Dit voorkomt de mogelijke risico's voor het stemgeheim en de verkoop van stemmen die gepaard gaan met het tellen van de stemmen in de stembureaus.

Wat de nadelen betreft, wijzen we op het volgende:

- het scannen vindt plaats nadat de stembussen zijn vervoerd, wat het risico vergroot dat de inhoud van de stembussen wordt gewijzigd voorafgaand aan het scannen – ook al zouden deze wijzigingen worden gedetecteerd dankzij de end-to-end controleerbaarheid,
- deze oplossing kan vereisen dat scanbureaus worden opgezet in kantons die geen telbureaus meer hebben, wat een uitgebreidere logistiek zou vereisen.

Merk wel op dat deze scanbureaus veel minder medewerkers nodig zullen hebben dan een telbureau, omdat scannen veel sneller gaat dan handmatig tellen.

In een scanbureau op het niveau van het kanton

Deze oplossing is identiek aan de vorige. Ze zou de voorkeur kunnen hebben in kantons waar volledig elektronisch wordt gestemd: één enkel scanbureau zou zeer efficiënt kunnen zijn.

Ze zou ook zinvol zijn in kleine kantons: bij de federale verkiezingen van 2019 kregen de kantons Voeren en Fauvillers in totaal stemmen van respectievelijk 1.510 en 1.514 kiezers. Dit staat in schril contrast met het kanton Antwerpen, waar de stemmen van 293.377 kiezers werden geteld.

In een gecentraliseerd scanbureau op het niveau van het arrondissement

Deze oplossing voert de vorige oplossing tot het uiterste door en zou interessant kunnen zijn in geografisch dichtbevolkte gemeenten.

Ze zou het voordeel hebben dat de logistiek voor de risk limiting audit die op gemeentelijk niveau plaatsvindt, wordt vergemakkelijkt: de stembiljetten zouden direct op de auditlocatie kunnen worden verzameld.

Conclusie

De laatste drie opties hebben onze voorkeur, om reden van de vereenvoudiging van de stembureaus die zij bieden, de beperking van de risico's voor het stemgeheim, de beperking van de technische risico's in het geval van een defect aan de stembus en de behoeften aan opleiding in het scannen.

Ons voorstel sluit aan bij de aanbevelingen van het College van Deskundigen, dat ook aanbeveelt om het scannen bij de elektronische stembus af te schaffen en die stembus-scanner te vervangen door het gebruik een klassieke stembus gevolgd door een scanproces na het sluiten van de stemverrichtingen, om de organisatie van de stembureaus te vereenvoudigen en de transparantie van het systeem en het stemgeheim te verbeteren [15][16].

We vinden het niet gepast om een definitieve keuze te maken tussen de drie in aanmerking genomen opties, en het lijkt ons plausibel dat de optie die de voorkeur heeft voor het ene kanton, niet de voorkeur heeft voor het aangrenzende kanton, vanwege verschillen in het percentage elektronische stemmen, de bevolkingsdichtheid, de grootte van het kanton, enz.

4.2.2.2 Hardware

De oplossing om te scannen op het niveau van de stembus zou vereisen dat er weinig courante hardware wordt gebruikt, en wordt hier niet aanbevolen.

We concentreren ons hier op een stembus, die ondoorzichtig moet zijn om niet het risico te lopen dat de inhoud van de stembiljetten die erin worden gedeponeerd, zichtbaar wordt.

Voor de andere benaderingen worden over het algemeen twee soorten scanners gebruikt:

1. bedrijfsscanners, uitgerust met een papierinvoer voor een honderdtal pagina's, die ongeveer zeventig pagina's per minuut scannen en net zo groot zijn als een kleine printer,

2. hogesnelheidsscanners, ontworpen voor intensief gebruik in bijvoorbeeld archiveringsdiensten, die snelheden van meer dan tweehonderd pagina's per minuut kunnen halen en de omvang hebben van een meubelstuk.

Voorbeelden van beide soorten scanners die bij verkiezingen worden gebruikt, zijn bijvoorbeeld te vinden in de lijst van stemtechnologieën die op 30 oktober 2023 in de staat Californië zijn goedgekeurd[38].

Veel van deze bedrijfsscanners kunnen per stuk worden gekocht, voor een particulier, tegen een prijs van ongeveer 1.000 euro, exclusief de validatiemodule, die vaak wordt aangeboden tegen een meerprijs van ongeveer 500 euro. Prijzen voor hogesnelheidsscanners worden niet gepubliceerd.

Validatiemodules zijn over het algemeen mini-inkjetprinters die zo zijn geïnstalleerd dat ze slechts op een beperkte strook van het vel papier kunnen afdrukken, wat ook nodig is om compatibel te zijn met hoge scansnelheden (veel hoger dan die van conventionele inkjetprinters die zijn ontworpen om over de hele breedte van de pagina af te drukken).

Gezien de gewoonte in België om de verkiezingsuitslag zeer snel te verkrijgen, lijkt het ons aannemelijk dat een oplossing op basis van een groot aantal bedrijfsscanners efficiënter en goedkoper zal zijn dan het gebruik van hogesnelheidsscanners, tenzij deze laatste kunnen worden gehuurd voor de verkiezingsdag – sommige ondernemingen bieden inderdaad diensten aan voor het huren van hogesnelheidsscanners, die vooral gericht lijken te zijn op ondernemingen, verenigingen of overheidsdiensten met een grote specifieke archiveringsbehoefte.

Wat de hoeveelheid betreft, kunnen we een raming maken op basis van het volgende: uitgaande van bedrijfsscanners die 70 pagina's per minuut scannen en anderhalf uur lang ononderbroken worden gebruikt (exclusief de tijd die nodig is om de stapels te scannen stembiljetten in te voeren, de gescande stembiljetten eruit te halen, eventuele vastgelopen stembiljetten te beheren, enz.) menen we dat een scanner kan worden gebruikt om 6.300 stembiljetten te scannen. Dit betekent dat er ongeveer 160 scanners nodig zullen zijn voor elk miljoen stembiljetten (reservescanners in geval van defect niet meegerekend).

4.2.3 Controleerbaarheid

Hier beschrijven we de verschillende elementen die moeten worden geïmplementeerd voor het uitvoeren van de audit die het risico op onjuiste resultaten beperkt en voor de controleerbaarheid van begin tot eind.

4.2.3.1 Risicobeperkende audit

De ingrediënten die nodig zijn om RLA voor te bereiden, zijn hierboven besproken. Zodra de stembiljetten zijn gescand, worden de volgende elementen verzameld op één locatie voor elk arrondissement:

---

[38] Zie *https://votingsystems.cdn.sos.ca.gov/cert-and-approval/vote-sys-appr-in-ca-10-30-23.pdf*. Dezelfde types scanners zijn terug te vinden op de lijst van de andere staten waarvan we de lijsten met gecertificeerde hardware hebben geraadpleegd, soms met variaties in merken.

- een verkiezingsmanifest in het arrondissement dat minimaal het volgende bevat:
  - voor elektronisch stemmen: een lijst van de dozen met stembiljettenenveloppen voor de verkiezing, met vermelding van welke envelop zich in welke doos bevindt, en een lijst van de serienummers van de stembiljetten in elke envelop,
  - voor elektronisch stemmen: een lijst van alle stembiljetten met, voor elk serienummer van het stembiljet, de manier waarop het stembiljet werd geïnterpreteerd op het moment van het scannen,
  - voor stemmen op papier: een lijst van de dozen met stembiljettenenveloppen die voor het stemmen op papier zijn geproduceerd, met vermelding van welke envelop zich in welke doos bevindt, hoeveel stembiljetten elke envelop bevat en aan welke partij de stemmen in elke envelop zijn toegewezen,
  - verkiezingstotalen en -uitslagen, zoals die zijn berekend,
- alle kisten met alle papieren stembiljetten voor de verkiezingen in het desbetreffende arrondissement.

In het vorige hoofdstuk (punt *3.2*) hebben we een auditprocedure voorgesteld op basis van gesprekken met personen die audits hebben verricht, op basis van gepubliceerde handleidingen en op basis van de specifieke kenmerken van België.

4.2.3.2 Controleerbaarheid van begin tot eind

We hebben in het vorige hoofdstuk (punt *3.3*) ook het geheel van cryptografische operaties beschreven die nodig zijn voor de end-to-end controleerbaarheid, maar we lieten open waar en wanneer deze berekeningen plaatsvinden, waarvoor een meer algemene beschrijving van het systeem nodig was. We zullen deze punten hier in meer detail uitleggen.

Het gaat om een precisering van:

1. de manier waarop elke kiezer zijn of haar stembiljettrackingnummer krijgt,
2. de manier waarop de gecodeerde stembiljetten worden berekend en opgeslagen in het stemsysteem, voor auditdoeleinden.

Productie van het trackingnummer van het stembiljet voor de kiezer

We zagen in punt *3.3* dat het trackingnummer van het stembiljet van een kiezer een hashcode is, weergegeven in de vorm van ongeveer vijftig tekens, van het cijfer van zijn stembiljet.

Het doel is om de kiezers dit trackingnummer te geven voordat ze hun stembiljet in de stembus stoppen, zodat ze eventueel kunnen vragen om hun stembiljet ongeldig te verklaren om na te gaan of het trackingnummer inderdaad hun stemintentie weergeeft. De natuurlijke oplossing is dan om dit trackingnummer (of deze trackingnummers, als er meerdere stembiljetten zijn bij een gecombineerde verkiezing) af te drukken op een extra pagina die wordt afgedrukt door de stemmachine, op hetzelfde moment als de stembiljetten.

Deze pagina met de trackingnummers wordt bewaard door de kiezers. Het zal belangrijk zijn om heel duidelijk met de kiezers te communiceren om ervoor te zorgen dat de pagina's die door de

stemmachine worden afgedrukt, correct worden gebruikt. Kiezers moeten ervan bewust zijn dat hun stembiljetten aan niemand mogen worden getoond en in de stembus moeten worden gedaan. De pagina met de trackingnummers moet echter door de kiezers worden bewaard en mag niet in de stembus worden gestopt. Dit kan van tevoren worden verduidelijkt, tijdens de gebruikelijke voorlichting in de media voor de kiezers voorafgaand aan de verkiezingen. Aan de kiezers zouden ook middelen kunnen worden verstrekt waarmee ze documenten gemakkelijk kunnen scheiden voordat ze het stemhokje verlaten: hiervoor zouden kartonnen mappen van verschillende kleuren en met duidelijke etiketten kunnen worden gebruikt (de kiezers zouden ze krijgen voordat ze het stemhokje binnengaan en zouden ze teruggeven bij het verlaten van het stemhokje, nadat ze hun stembiljetten in de stembussen hebben gestopt).

Een technisch probleem is het communiceren van de door de stemmachine berekende sleutel naar het centrale systeem dat de auditgegevens zal publiceren: er is geen enkel digitaal communicatiemiddel tussen deze twee systemen.

De wens zou kunnen bestaan om de sleutel af te drukken op het stembiljet van de kiezer, eventueel ingebed in de QR-code, maar dit is technisch niet haalbaar: zoals we hebben gezien is de versleuteling meestal enkele tientallen of enkele honderden kilobytes lang, terwijl de grootste QR-codes slechts enkele kilobytes kunnen weergeven.

ElectionGuard bevat een oplossing voor dit probleem: voor elk stembiljet selecteert de stemmachine een unieke waarde van 256 bits, die bekend staat als de 'ballot nonce'. Alle willekeurige waarden die gebruikt worden om de ElGamal-sleutels van de keuzes van de kiezer te berekenen, worden dan afgeleid van die ballot nonce, met behulp van de HMAC als een (dubbele) pseudo-willekeurige functie.

Die ballot nonce van 256 bits kan dan worden verzonden naar de rest van het stemsysteem via de QR-code die op het stembiljet is afgedrukt, en die wordt opgehaald op het moment van het scannen.

Herberekening van de versleutelde stembiljetten voor de universele controleerbaarheid

We moeten ons wel rekenschap geven van de gevoeligheid van die ballot once: iemand die bijvoorbeeld zou weten van welke kiezer een ballot nonce was, zou kunnen nagaan voor wie de kiezer in kwestie heeft gestemd. Om deze reden lijkt het niet gepast om de ballot nonce ongecodeerd af te drukken op de QR-code van het stembiljet. Het verdient de voorkeur om die voorafgaand aan de doorgifte te versleutelen. Dit betekent dat we op het moment van het scannen niet de ballot nonce ophalen, maar een versleutelde versie ervan. Na de ontcijfering is het mogelijk om de sleutel van het stembiljet zoals berekend door de stemmachine opnieuw te berekenen, de bijbehorende niet openbaar te maken bewijzen te berekenen (die niet berekend hoeven te zijn door de stemmachine en die berekend kunnen worden op basis van nieuwe willekeurige getallen) en dit resultaat te publiceren als onderdeel van de verrichtingen inzake individuele en universele controleerbaarheid.

Er moet nog worden bepaald hoe de versleuteling wordt verwezenlijkt, en hiervoor zijn er ten minste drie opties:

1. Sleutels voor een symmetrisch versleutelingssysteem worden gegenereerd tijdens de stap van het genereren van de USB-sticks voor het initialiseren van de stemmachines in de FOD Binnenlandse Zaken, en worden op deze sticks ingevoegd. Wanneer de scangegevens de FOD

Binnenlandse Zaken bereiken, ontcijfert hij alle ballot nonces en berekent hij aan de hand van de overeenkomstige ongecodeerde stemmen de auditgegevens.

2. Een sleutelpaar voor een encryptiesysteem van het type hashed-ElGamal of DHIES [1] wordt gegenereerd door de FOD Binnenlandse Zaken wanneer de USB-sticks voor het initialiseren van de stemmachines worden gegenereerd. De openbare sleutel wordt geïntegreerd in de USB-sticks. De FOD Binnenlandse Zaken decodeert de gegevens op dezelfde manier als voorheen.

3. Wanneer de sleutels van de beheerders worden gegenereerd, produceren ze een tweede paar van een openbare sleutel en een geheime sleutel, zoals in het vorige punt. De openbare sleutel wordt geïntegreerd in de USB-sticks voor de initialisatie van de machines, en de decodering wordt deze keer uitgevoerd door meerdere beheerders op basis van de gegevens die zijn verkregen na de scanning.

De tweede oplossing lijkt ons a priori de meest geschikte: de verdeling van symmetrische sleutels, zoals in de eerste optie, is altijd een zeer gevoelige operatie, en de betrokkenheid van de beheerders zoals vereist in de derde optie vertegenwoordigt een aanzienlijke behoefte aan rekenkracht, die we willen vermijden van de kant van de beheerders.

Deze tweede oplossing is echter van fundamenteel belang voor de veiligheid van de infrastructuur van de FOD Binnenlandse Zaken: een lek van de 'ballot nonces' zou de vertrouwelijkheid van de stemmen aanzienlijk kunnen verzwakken als deze 'ballot nonces' met andere informatie zouden worden gecombineerd. De vertrouwelijkheid van de stemmen is echter nog steeds veel beter beschermd dan onder het systeem dat momenteel in België wordt gebruikt.

Behoeften aan rekenkracht

We hebben gezien dat de rekenkracht die nodig is voor end-to-end controleerbaarheid op de meeste plaatsen verwaarloosbaar is:

- Voor de taken van de beheerders vergen niet meer dan enkele rekenseconden op een laptop.
- De berekeningen op de stemmachine duren minder dan een halve seconde, zelfs voor de grootste stembiljetten. Bovendien is meer dan 90% van deze berekening onafhankelijk van de keuzes van de kiezers en kan ze daarom worden uitgevoerd terwijl de stemming plaatsvindt.
- Kiezers kunnen controleren of hun stembiljet correct is geregistreerd door eenvoudigweg de trackingnummers te vergelijken.

Er zijn twee plaatsen waar aanzienlijke rekenkracht nodig is:

1. de her-encryptie en de berekening van de geldigheid van de stembiljetbewijzen, op basis van de informatie die is verkregen van de gescande stembiljetten,

2. de universele controle van de geldigheid van de stembiljetten en de totalisering ervan.

Conceptueel gezien hoeft alleen de eerste taak door de organisatoren van de verkiezingen te worden uitgevoerd: het controleren van hun eigen werk in de tweede fase is niet bedoeld om fraude op te sporen. Aan de andere kant lijkt het natuurlijk verstandig dat de organisatoren van de

verkiezingen hun berekeningen daadwerkelijk controleren voordat ze overgaan tot het publiceren van de gegevens waarmee de verkiezing kan worden gecontroleerd.

Hier evalueren we een bovengrens voor de vereiste rekentijd. Die is gebaseerd op de hierboven beschreven protocollen, die zijn gebaseerd op ElectionGuard. Zoals ook aangegeven, is het heel duidelijk dat veel betere prestaties (we kunnen een factor van ongeveer 10 qua rekentijd verwachten) kunnen worden bereikt met technologieën die vandaag bestaan, maar nog niet op grote schaal worden toegepast. Verschillende hiervan zullen waarschijnlijk gebruikelijk zijn geworden tegen de tijd dat het systeem wordt geïmplementeerd. Onze beoordeling van de rekentijd houdt echter geen rekening met andere factoren die enorm variëren afhankelijk van de context, zoals de tijd die nodig is om gegevens op te slaan en over te dragen tussen verschillende machines.

Onze beoordeling is gebaseerd op een uitvoering van de code beschreven in punt *3.3*, op een werkstation uitgerust met een AMD Ryzen 3990X-processor uit 2020, en met 64 threads die parallel de versleuteling en de geldigheidsbewijzen berekenen van 10.000 stembiljetten met elk 200 kandidaten. De gemeten tijden zijn vermeld in tabel *[tab:compute-many-ballots]*. Als we uitgaan van een beveiligingsniveau met een priemgetal p van 3072 bits, zien we dat het versleutelen van een miljoen stembiljetten 35 minuten zou duren op één enkele machine (dat is 100 keer de 21,1 seconden die in tabel *[tab:compute-many-ballots]* worden weergegeven). Het controleren van de geldigheid van de stembiljetten, zoals vereist voor de universele controleerbaarheid, is langzamer: nu duurt het 4 uur 28 minuten, opnieuw voor één miljoen stembiljetten. Aangezien er geen vertrouwelijke gegevens bij deze bewerking betrokken zijn, kan ze eenvoudig worden gedelegeerd naar minder veilige infrastructuren van het cloudtype.

Tijd om de bewijzen van geldigheid van stembiljetten met 200 kandidaten verspreid over 10 partijen te versleutelen en te berekenen, en tijd om de geldigheid van deze stembiljetten te controleren, met gebruik van 64 threads op een werkstation.

	$\|p\| = 3072$	$\|p\| = 4096$
Berekening van een stembiljet	0,083 s	0,118 s
Berekening van 10.000 stembiljetten	21,1 s	29,1 s
Verificatie van een stembiljet	0,85 s	1,44 s
Verificatie van 10.000 stembiljetten	161 s	272 s

Wij geloven dat de hier aangegeven ordes van grootte laten zien dat het heel goed mogelijk is om de gegevens die nodig zijn voor de individuele en de universele controleerbaarheid in korte tijd te verkrijgen, met behulp van louter standaardtools en zonder te hoeven te investeren in een zware infrastructuur.

4.2.4 Logistiek voorafgaand aan de verkiezingen

De stemmachines worden momenteel onder verschillende omstandigheden opgeslagen: sommige gemeenten beheren hun eigen opslag, terwijl andere gebruikmaken van de opslagdiensten van Smartmatic.

Wanneer de stembureaus opengaan, moeten de machines, die al op voorhand geïnstalleerd en getest zijn, worden geïnitialiseerd en opgestart met behulp van USB-sticks. Momenteel worden ongeveer 10.000 USB-sticks (twee sticks per stembureau) geïnitialiseerd in de infrastructuur van de FOD Binnenlandse Zaken en doorgegeven aan de voorzitters van de kantonhoofdbureaus, die ze

de dag vóór de verkiezingen doorgeven aan de voorzitters van de stembureaus. Deze USB-sticks bevatten het besturingssysteem dat nodig is om de machines op te starten, een set cryptografische sleutels en de stemgegevens, waaronder een beschrijving van de stembiljetten die de machine aan de kiezers kan presenteren.

Aan deze aanpak zijn grote voordelen verbonden: hierdoor krijgen personen met toegang tot de stemmachines tijdens de opslagperiode tussen verkiezingen niet de mogelijkheid om de software die op deze machines draait, te wijzigen, aangezien er geen software staat op die machines. De integriteit van de software is ook afhankelijk van het opvolgen van USB-sticks, wat makkelijker is dan het opvolgen van volumineuze machines – zonder het belang van het goed opvolgen van de USB-sticks te veronachtzamen.

Toegang tot de stemmachines die niet zijn uitgerust met software lost het probleem van de vertrouwelijkheid van de stemmen echter niet op. Toegang tot de stemmachines zou bijvoorbeeld gebruikt kunnen worden om een elektronische spionagecomponent toe te voegen die alle op de machine uitgebrachte stemmen registreert, in de volgorde waarin ze zijn uitgebracht. Iemand die in het stemlokaal aanwezig is, zou de lijst kunnen bijhouden van de mensen die op elke machine hebben gestemd en zo de inhoud van ieders stem kunnen traceren. Hoewel dit type aanval niet eenvoudig is, zijn er demonstraties uitgevoerd van de haalbaarheid ervan op bepaalde stemmachines [67]. Deze bezorgdheid bevestigt het belang van het veilig opslaan van de stemmachines, zelfs als ze niet zijn uitgerust met een niet-vluchtig geheugen.

De aanpak op basis van de USB-sticks levert in de praktijk ook problemen op, die regelmatig door het College van Deskundigen werden opgemerkt en die te maken hebben met de betrouwbaarheid en de zorgvuldigheid die vereist is bij het hanteren van deze USB-sticks.

Een alternatief, dat wordt gebruikt in verschillende jurisdicties in de Verenigde Staten, bestaat uit het organiseren van een veel meer gecentraliseerde opslag van stemmachines, met strenge beveiliging, waarbij de stemmachines worden uitgerust met niet-vluchtige opslag (harde schijven) en de mogelijkheid om ze aan te sluiten op een bekabeld netwerk. De machines kunnen worden opgeslagen in kisten in racks, wat betekent dat ze kunnen worden voorzien van elektriciteit en aangesloten worden op het netwerk. Software voor verkiezingsbeheer maakt het dan mogelijk om tegelijk een diagnose te stellen van de machines en ze te configureren voor elke verkiezing. De machines worden dan vanuit de opslagplaatsen naar de stembureaus vervoerd, waar ze alleen nog maar opgestart hoeven te worden. Er zijn ook beveiligingen om ongecontroleerd opstarten van de machines te voorkomen.

Deze aanpak heeft als voordeel dat er geen USB-sticks gebruikt hoeven te worden op de verkiezingsdag en dat de problemen met deze sleutels vermeden worden. Ze stelt de machines echter bloot aan veel grotere risico's, omdat ze nu moeten worden uitgerust met geheugen en mogelijkheden voor netwerkconnectiviteit. Deze extra risico's moeten daarom worden gecompenseerd door een infrastructuur voor opslag van de machines met een uitermate versterkte veiligheid. De kosten voor de opslagruimte zullen ook toenemen door de behoefte aan opslagracks die zijn uitgerust met stroomvoorzieningen en netwerkaansluitkabels voor elke machine. Het belang van het implementeren van technologieën voor beveiligd opstarten zal in deze context ook toenemen.

Voor zover het gebruik van de USB-sticks de bron van terugkerende problemen lijkt te zijn, lijkt het ons mogelijk interessant om de wens en haalbaarheid, inclusief de financiële haalbaarheid, te meten van het opzetten van beveiligde ruimten voor de opslag, het onderhoud en de configuratie van de stemmachines.

Het veiligheidsbeheer zal zeker van groot belang zijn en de inschatting ervan zal ingewikkeld zijn. In het ideale geval zou het wenselijk zijn de machines op honderden locaties op te slaan, stuk voor stuk zeer goed beveiligd. We weten dat er niet zoiets bestaat als perfecte beveiliging en het feit dat de machines verspreid staan, betekent dat een inbreuk op één plaats een beperkte impact zal hebben (zelfs als de impact nog steeds volledig kan zijn als het gedrag van de machines in een gemeente wordt veranderd in het kader van lokale verkiezingen, bijvoorbeeld). Het beschikken over honderden hoogbeveiligde opslaginfrastructuren is echter niet realistisch, gezien de kosten die ermee gemoeid zijn, en we staan dan voor een reeks keuzes, van het opslaan van machines op een enorm aantal locaties, maar ongetwijfeld ook onder wisselende veiligheidsomstandigheden, tot het opzetten van een minimaal aantal opslaglocaties (slechts één, in het uiterste geval) waarin we echt kunnen investeren in beveiliging.

De gecentraliseerde strategie komt overeen met die van veel IT-systemen vandaag de dag, waar het beheer van e-mails, bestanden enz. wordt gedelegeerd aan cloudserviceproviders. Zij kunnen beveiligingsstandaarden implementeren die doorgaans te duur zijn voor kleine en middelgrote bedrijven. Maar hoe meer we centraliseren, hoe meer we onszelf blootstellen aan het risico van grote inbreuken met een veel grotere impact: aankondigingen van beveiligingsinbreuken in grote cloudinfrastructuren zijn nog steeds aan de orde van de dag. Het vooruitzicht van een grote impact vergroot natuurlijk ook de interesse om zulke aanvallen uit te voeren.

Onze suggestie hier zou zijn om inspiratie te halen uit het vaststellen van een minimaal aanvaardbaar beveiligingsniveau, eventueel geïnspireerd door de EAC-aanbevelingen (samengevat in afbeelding *[fig:eac-machines-access]*), en om de opslag te verdelen over zoveel mogelijk locaties die dit beveiligingsniveau kunnen garanderen.

4.2.5 Logistiek na de verkiezingen

Naast de hierboven beschreven tel- en auditwerkzaamheden is het verslag van het College van Deskundigen een centraal element in de certificering van de verkiezingsuitslag.

Wat de analyse van de werking van het elektronische stemsysteem tijdens de verkiezingsdagen betreft, zijn deze verslagen grotendeels gebaseerd op de bezoeken aan de verschillende stembureaus en de kantonhoofdbureaus die op de verkiezingsdag zijn uitgevoerd, maar gezien het aantal stembureaus waar elektronisch stemmen van toepassing is en het aantal leden van het College, kan in de praktijk slechts een klein deel van de bureaus worden bezocht: de 16 leden van het College melden bijvoorbeeld 132 stembureaus te hebben bezocht tijdens de verkiezingen van 2019, op meer dan 4.000 bureaus, wat neerkomt op ongeveer 3% van de bureaus [14].

Het zou nuttig kunnen zijn om over systematische en gestructureerde rapportagetools te beschikken voor elk stembureau, die de deskundigen in staat zouden stellen om elk van de vastgestelde problemen exact te meten. Een smartphone-app die ter beschikking wordt gesteld van de voorzitters van de bureaus en waarmee snel kan worden gerapporteerd op basis van de geselecteerde opties, zou in deze context een zeer nuttig hulpmiddel kunnen zijn.

4.3 PROCEDURE VOOR DE BEOORDELING VAN DE KWALITEIT VAN HET SYSTEEM

De stemsystemen zijn cruciaal voor de bescherming van onze democratieën. In België wordt dit algemeen erkend: naast de beoordeling door het College van Deskundigen is het stemsysteem beoordeeld door het Centre for Cyber Security Belgium (CCB) en door het Nationaal Crisiscentrum. De broncodes van bepaalde software, zonder hun veiligheidselementen, worden ook gepubliceerd na de verkiezingen, voor een beperkte periode.[39]

Op Europees niveau publiceerde de Raad van Europa in 2004 zijn eerste aanbevelingen over elektronisch stemmen, die in 2017 werden bijgewerkt, samen met richtlijnen voor de implementatie ervan [22].[40] Deze aanbevelingen vormden een belangrijke inspiratiebron voor deze studie. De NIS-groep, die is opgericht in het kader van de Europese NIS-richtlijn, heeft in 2018 ook een cyberbeveiligingscompendium gepubliceerd van de technologieën die worden gebruikt tijdens de verkiezingen [46]. Dit compendium richt zich echter voornamelijk op de 'online' onderdelen van de systemen, zoals het beheer van kiezersdatabases en de systemen voor de compilatie van de resultaten, die grotendeels losstaan van deze studie.

In de Verenigde Staten is de stemuitrusting door het Department of Homeland Security geclassificeerd als onderdeel van de kritieke infrastructuur van het land en moet ze als zodanig worden beschermd.[41] De Election Assistance Commission (EAC),[42] opgericht onder de Help America Vote Act van 2002, bundelt en publiceert verschillende verkiezingshandleidingen, in het bijzonder de 'voluntary voting system guidelines' (VVSG), die een reeks specificaties en vereisten voor stemsystemen definiëren [62]. Het opvolgen van de VVSG is vrijwillig, behalve in de staten waar dit verplicht is. De nieuwste versie van de VVSG (2.0), die in 2021 is gepubliceerd, spitst zich in het bijzonder toe op de kwesties van beveiliging, interoperabiliteit en systeemtoegankelijkheid.

Zwitserland, met zijn recente ontwikkelingen in zijn experimentele internetstemsysteem, loopt nu voorop wat betreft goede praktijken op het gebied van transparantie en het evaluatieproces voor zijn elektronische stemsysteem, in het bijzonder door zijn Ordonnantie 161.116 van de Bondskanselarij over elektronisch stemmen (OVotE), gepubliceerd in 2022 [11]. Deze ordonnantie legt de voorwaarden vast voor de toekenning van de erkenning voor het laten uitvoeren van tests met elektronisch stemmen door de kantons.

Artikel 3, dat we hier weergeven, bevat de voorwaarden voor het verkrijgen van de erkenning:

1. het systeem wordt ontworpen en geëxploiteerd om een verifieerbare, veilige en betrouwbare elektronische stemming te garanderen;
2. het systeem is gemakkelijk te gebruiken door de kiezers; het houdt zoveel mogelijk rekening met ieders individuele behoeften;

---

[39] *https://verkiezingen.fgov.be/algemeen/veiligheid-en-transparantie*

[40] *https://www.coe.int/en/web/electoral-assistance/e-voting*

[41] *https://www.cisa.gov/topics/election-security*

[42] *https://www.eac.gov/*

3. het systeem en de operationele processen zijn zodanig ontworpen en gedocumenteerd dat het mogelijk is om de technische en organisatorische aspecten ervan in detail te controleren en te begrijpen;
4. het publiek heeft toegang tot aangepaste informatie over de werking van het systeem en de operationele processen, en er worden maatregelen genomen om personen met de nodige kennis aan te moedigen mee te werken aan de verbetering van het systeem.

We willen graag een aantal andere aspecten van deze ordonnantie onder de aandacht brengen die volgens ons van bijzonder belang zijn voor de beoordeling van de kwaliteit van het systeem.

- Onafhankelijke audits. Artikel 10 bepaalt dat de Bondskanselarij onafhankelijke organen aanwijst die belast worden met het controleren van de compliance van de cryptografische protocollen, de software, de veiligheid van de infrastructuur en het gebruik, en de bescherming tegen pogingen tot binnendringing in de infrastructuur.
- Publicatie. Artikel 11 stelt dat, om erkend te kunnen worden, het volgende moet worden gepubliceerd: de broncode (inclusief de parameterbestanden); de documenten die aantonen dat deze code daadwerkelijk de code is die wordt gebruikt in de machines; de softwaredocumentatie; handleidingen die laten zien hoe geïnteresseerden het systeem kunnen compileren, laten werken en analyseren in hun eigen infrastructuur met behulp van de broncode; de technische specificaties van de belangrijkste onderdelen van het systeem; de documentatie van de exploitatie-, onderhouds- en beveiligingsprocessen van het systeem; de informatie over en de beschrijvingen van de vastgestelde gebreken. Artikel 12 bepaalt dat deze publicaties zo moeten gebeuren dat ze zo gemakkelijk mogelijk te lezen en te analyseren zijn, wat ook betekent dat de toegang gratis moet zijn en dat er geen registratie voor vereist is. Artikel 13 bepaalt dat de kantons een dienst aanwijzen waar het publiek suggesties kan doen voor verbeteringen aan het systeem, en voorzien in een billijke vergoeding voor suggesties die van invloed zijn op de veiligheid van het systeem.

Hier merken we de centrale rol van de Bondskanselarij in de beoordeling, die niet aanwezig was in de eerste versies van de ordonnantie. In het bijzonder betekent deze positie dat de personen die instaan voor de beoordeling, worden aangeworven door de instantie die belast is met de beoordeling van de kwaliteit van het systeem en niet, zoals voorheen, door de leverancier van het stemsysteem, wiens commerciële belang vanzelfsprekend de validatie van het systeem is. Alle evaluatieverslagen worden gepubliceerd door de Kanselarij.[43]

We merken ook op dat aan het publiek een belangrijke rol wordt toebedeeld bij de beoordeling van het systeem, ruim *vóór* de verkiezingen, dat de publicaties zeer uitgebreid zijn (inclusief de documentatie waarmee geïnteresseerden het systeem in hun eigen IT-omgeving kunnen gebruiken) en dat de infrastructuur wordt beschreven, en dat er aandacht wordt besteed aan het stimuleren van het publiek om het systeem te onderzoeken (met name door gebreken bekend te maken en mensen die gebreken ontdekken, te vergoeden).

Elementen die ons ook belangrijk lijken, zijn de afwezigheid van vereisten betreffende het gebruik van specifieke technologieën (programmeertalen, specifieke standaarden, enz.), evenals de continuïteit van het beoordelingsproces, ook door het publiek. Dit weerspiegelt de in wezen

[43] *https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html*

veranderlijke aard van de technologieën en het feit dat een stemsysteem nooit geïsoleerd werkt: het is afhankelijk van talloze externe componenten, waaronder besturingssystemen en bibliotheken, maar ook fysieke beschermingsmiddelen zoals sloten, beveiligde enveloppen of verzegelingen. Deze elementen veranderen voortdurend, met name om fouten te corrigeren en te reageren op nieuwe aanvalstechnieken, en een stemsysteem moet zich, net als elk ander IT-systeem, dienovereenkomstig aanpassen. Het is niet mogelijk om op een dag een goedkeuringsstempel op een stemsysteem te drukken en te hopen dat dit stempel geldig blijft zolang het systeem niet gewijzigd wordt. De validatie van een stemsysteem zal eerder aangeven dat, na een voldoende breed beoordelingsproces en gezien de stand van de kennis op een bepaald moment, het redelijk lijkt om een stemsysteem te gebruiken in de context van een specifieke verkiezing.

Op basis van de huidige kennis zijn onze aanbevelingen als volgt:

- Een werkgroep oprichten binnen de Directie van de verkiezingen om de procedure voor de beoordeling van het stemsysteem uit te breiden, op basis van de Zwitserse ervaring. Wij zijn van mening dat de nadere regels voor het publiceren en documenteren van het stemsysteem die in Zwitserland worden gebruikt, geschikt zijn voor België. Het doel is om te bepalen hoe ervoor kan worden gezorgd dat de gepubliceerde informatie daadwerkelijk wordt beoordeeld (een publicatie die wordt genegeerd, is nutteloos) en om te bepalen wat er op het niveau van de Directie van de verkiezingen nodig is om de beoordeling te kunnen uitvoeren in interactie met de verschillende actoren (leveranciers van het systeem, instellingen of deskundigen die het systeem moeten onderzoeken, en het publiek).
- Bij het uitvoeren van de beoordeling inspiratie putten uit aanbevelingen en geleerde lessen uit andere landen. Zoals de zaken er nu voorstaan, bevelen we aan om bijzondere aandacht te besteden aan de aanbevelingen van de Raad van Europa [22], de VVSG [62] en de lessen die nog steeds geleerd worden in de Zwitserse context.[44]

De ontwikkeling van een systeem dat zoveel mogelijk is gebaseerd op standaardelementen die al elders zijn beoordeeld en op standaardgegevensformaten die de inspectie en de tests vergemakkelijken, moet worden aangemoedigd. Dit was een van de centrale uitgangspunten bij het ontwerp van BeVoting II, en we hopen dat het de beoordeling van dit systeem, dat aanzienlijk meer gestandaardiseerd is dan de oplossing die in Zwitserland is ontwikkeld en die aan heel andere specificaties moet voldoen, aanzienlijk zal vereenvoudigen. Het gebruik van standaardcomponenten beperkt niet alleen het risico op fouten en kinderziekten in het systeem, maar maakt de beoordeling ook veel eenvoudiger. De stemsystemen zijn systemen met veel vrij unieke beperkingen en er zijn maar weinig mensen met specifieke expertise op dit gebied.

4.4 SYNTHESE VAN HET BEVOTING II-SYSTEEM

De eerdere beschrijving van het BeVoting II-systeem werd opgenomen in de motivatie voor elk element, evenals in de bespreking van verschillende varianten. Hier zetten we de verschillende elementen van het systeem op een rijtje en benadrukken we de verschillen met het huidige

[44] *https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html*

elektronische stemsysteem – als er geen vermelding is, gaan we ervan uit dat BeVoting II zich net zo gedraagt als het huidige systeem. De nummers in de rechterkolom verwijzen naar de hoofdstukken van de studie waar deze stappen worden besproken.

4.4.1 Ervaring van de kiezers

De kiezers voeren enkele of alle van de volgende stappen uit.

Als ze dat willen, kunnen kiezers hun stembiljet of stembiljetten op voorhand invullen op een smartphone-app. De applicatie maakt een QR-code aan die gescand zal kunnen worden door de stemmachine en die de ingevoerde keuzes zal weergeven. Deze kunnen nog steeds worden gewijzigd naar goeddunken van de kiezers.	*4.2.1.1.2*
De kiezers identificeren zich bij de ingang van het stembureau en ontvangen een papier met een lijst van de stemmingen waaraan ze mogen deelnemen, in leesbare vorm en in de vorm van een QR-code.	*4.2.1.1.3* *4.2.1.2.5*
De kiezers gaan het stemhokje binnen en scannen de QR-code die ze bij de ingang van het stembureau hebben ontvangen, op de stemmachine.	*4.2.1.1.3*
De kiezers geven hun keuzes aan via het touchscreen op de stemmachine of door de QR-code te scannen die ze op voorhand hebben voorbereid en die hun keuzes vooraf codeert.	*4.2.1.1.2*
De kiezers kunnen ook besluiten om een willekeurige stem uit te brengen als ze willen controleren of de stemmachine goed werkt. In dit geval zullen ze, na het afdrukken en controleren van het afgedrukte stembiljet, het stembiljet ongeldig laten maken door de voorzitter en een nieuwe QR-code ontvangen waarmee ze kunnen stemmen.	*3.3.2.3.3*
De kiezers controleren hun keuzes op het eindscherm van de stemmachine. Ze kunnen die nog naar believen wijzigen.	*4.2.1.1.2*
Als de kiezers tevreden zijn, starten ze het afdrukken van hun stembiljet(ten) af op papier in A4-formaat. Ze ontvangen hun stembiljetten, waarop hun keuzes leesbaar worden weergegeven en die ook een QR-code bevatten. Er wordt ook een extra pagina afgedrukt met het trackingnummer van het biljet, om individuele controleerbaarheid mogelijk te maken.	*4.2.1.1.1* *4.2.1.2.3*
Als de kiezers tevreden zijn met het afdrukken, doen ze hun stembiljetten in een map en bewaren ze hun trackingnummer buiten de map. Ze overhandigen de pagina met hun trackingnummer aan de leden van het stembureau zodat die de pagina afstempelen om de authenticiteit ervan aan te geven en zodat die zich ervan vergewissen dat deze pagina niet in de stembus wordt gestopt. De kiezers doen hun stembiljet(ten) in de stembus (dit is een conventionele stembus, zonder scanner of elektronische klep).	*4.2.2.1* *4.2.3.2.1*
Als de kiezers niet tevreden zijn over de afdruk, melden ze dit aan de voorzitter van het stembureau, die het afgedrukte stembiljet annuleert en de kiezer toestaat opnieuw te stemmen. Als de kiezers denken dat de machine valsspeelt, wordt het incident genoteerd voor eventueel onderzoek.	*4.2.3.2.1*
Zodra de voorlopige verkiezingsuitslagen zijn gepubliceerd, kunnen alle kiezers die dat willen, controleren of hun trackingnummer is opgenomen in de lijst met trackingnummers van de getelde stembiljetten. Ze kunnen ook de aanwezigheid van	*3.3.2.3.1* *3.3.3.2.3*

trackingnummers voor stembiljetten die ze ongeldig hebben gemaakt, controleren in een lijst van ongeldig verklaarde stembiljetten. In geval van een probleem nemen ze contact op met de dienst die hiervoor instaat.

4.4.2 Ervaring van het stembureau

De leden van de stembureaus voeren hun verrichtingen als volgt uit.

De voorzitter van het stembureau ontvangt in een beveiligde envelop de activeringscodes voor de stemmachines en, indien van toepassing, de USB-sticks die nodig zijn om ze op te starten. De stemmachines worden opgestart wanneer de stemming begint. *4.2.4*

De leden van het stembureau identificeren de kiezers, geven hen de QR-codes waarmee ze kunnen stemmen en informeren hen over de werking van het stemsysteem en de verificatiemogelijkheden die het systeem biedt. *4.2.1.1.3*

De leden van de stembureaus verlenen bijstand aan de kiezers die aangemaakte stembiljetten ongeldig willen maken. Ze markeren deze stembiljetten als ongeldig en geven een nieuwe QR-code waarmee de personen een nieuw stembiljet kunnen aanmaken. *3.3.2.3.3* *4.2.3.2.1*

De leden van het stembureau stempelen de pagina's met de trackingnummers af om ze te markeren als authentiek. *4.2.2.1* *4.2.3.2.1*

Na afloop van de stemverrichtingen stelt de voorzitter het proces-verbaal van het stembureau op, waarin voor elke stemming het aantal opgekomen kiezers wordt vermeld. *3.2.1.2*

De voorzitter doet alle stembiljetten in enveloppen, die worden verzegeld en door verschillende personen worden vervoerd naar de plaats waar de stembiljetten worden gescand om te worden geteld. De enveloppen worden doorgegeven tegen ontvangstbewijs. *3.2.2.3.4* *4.2.2.1*

De voorzitter van het stembureau registreert de lijst van de incidenten, of de afwezigheid van incidenten, in een app die ontworpen is om een snelle invoer te vergemakkelijken, en stuurt het resultaat naar de hoofdbureaus, het College van Deskundigen en de FOD Binnenlandse Zaken. *4.2.5*

4.4.3 Ervaring van het scanbureau

De verrichtingen in de scanbureaus verlopen als volgt.

Elke envelop van de stembureaus wordt geopend, de ontvangen stembiljetten worden gemengd en de stembiljetten worden gebundeld in stapels van ongeveer honderd stembiljetten. *4.2.2.1*

De stembiljetten worden gescand en geldig verklaard door de scanner. Elke stapel gescande stembiljetten wordt in een nieuwe envelop gedaan, zonder de volgorde te veranderen. Deze envelop wordt gemarkeerd met de nummers van het eerste en van het laatste stembiljet in de stapel, en met het aantal stembiljetten dat door de scanner is geteld. *3.2.2.3.4* *4.2.2.2*

De enveloppen met gescande stembiljetten worden verzameld in dozen. Van de inhoud van elke doos wordt een manifest bijgehouden met ten minste het nummer van de doos, de lijst van de enveloppen die de doos bevat en de nummers van het eerste en het laatste stembiljet die op het moment van de geldigverklaring in elke envelop zijn gestoken. *3.2.2.3.4*

De scanningtool levert een bestand met de lijst van de gescande stembiljetten, met hun geldigverklaringsnummer, de inhoud van de stem en de versleuteling die wordt gebruikt voor de end-to-end controleerbaarheid van het stembiljet en de telling. *4.2.2.1*

De totalen worden berekend op basis van dit bestand, dat wordt doorgestuurd naar het betrokken hoofdbureau, de FOD Binnenlandse Zaken en het bureau dat zal instaan voor het uitvoeren van de risk limiting audit. *4.2.2.1*

Alle dozen met de stembiljetten, zowel voor elektronisch stemmen als voor stemmen op papier, worden naar de plaats gebracht waar de risk limiting audit zal plaatsvinden. *3.2.2.3.4*

De voorzitter van het scanbureau registreert de lijst van de incidenten, of de afwezigheid van incidenten, in een app die ontworpen is om een snelle invoer te vergemakkelijken, en stuurt het resultaat naar de hoofdbureaus, het College van Deskundigen en de FOD Binnenlandse Zaken. *4.2.5*

4.4.4 Ervaring van het telbureau voor de stemming op papier

Wanneer in dezelfde kieskring zowel elektronische verkiezingen als verkiezingen op papier worden gehouden, worden de handelingen ter voorbereiding van de risk limiting audit als volgt uitgevoerd in de telbureaus voor de stemming op papier.

De enveloppen met de stembiljetten, die zo zijn ingedeeld dat elke envelop slechts stemmen voor één partij bevat, worden genummerd, in genummerde dozen gestopt en naar het bureau gebracht waar de risk limiting audit zal plaatsvinden. *3.2.2.3.1*

Een manifest met de inhoud van elke doos wordt op dezelfde manier verzonden. Dit manifest bevat minstens de lijst met de enveloppen in elke doos en de aangegeven inhoud van elke envelop (aantal stembiljetten en de partij waaraan deze stembiljetten zijn toegewezen). *3.2.2.3.1*

4.4.5 Risicobeperkende audit

De verrichtingen in verband met de risk limiting audit verlopen als volgt.

De manifesten met de lijsten van stembiljetten, hun getelde inhoud en de locatie van deze stembiljetten (nummer van de doos en envelop, met ook het bevestigingsnummer in het geval van elektronische stembiljetten) worden opgeladen in de software die de risicobeperkende audit organiseert. De verkiezingsresultaten worden ook ingevoerd (enkel het aantal behaalde stemmen voor elke lijst). *3.2.2.3.5*

De dobbelstenen worden gegooid in aanwezigheid van waarnemers om het selectieproces van de stembiljetten op te starten. *3.2.2.3.5*

De auditsoftware toont de lijst met te controleren stembiljetten op een projectiescherm dat voor iedereen zichtbaar is. *3.2.2.3.6*

Het auditbureau vindt de vermelde stembiljetten in de kisten, geeft de leesbare inhoud ervan aan en vergelijkt ze met de elektronische interpretatie die werd geregistreerd. *3.2.2.3.5*

De software bevestigt dat het risico van een onjuiste toewijzing van de zetels aan de lijsten onder de gekozen drempel ligt, of geeft aan dat de selectie van extra stembiljetten nodig is (omdat er bijvoorbeeld fouten zijn gedetecteerd), of geeft aan dat een volledige handmatige hertelling nodig is omdat de verkiezingsmarge te klein is en/of het aantal fouten te hoog is. *3.2.2.3.5*

Het resultaat van de risicobeperkende audit wordt naar het arrondissementsbureau, de FOD Binnenlandse Zaken en het College van Deskundigen gestuurd. *3.2.2.3.6*

4.4.6 Controle van begin tot eind

De verrichtingen in verband met de controle van begin tot eind verlopen als volgt.

Voordat de verkiezing begint, genereren de beheerders en de FOD hun publieke sleutels en bewaren ze hun geheime sleutels. *3.3.1.2 4.2.3.2.2*

De FOD produceert de initialisatiemedia voor alle stemmachines, die de publieke sleutels bevatten die in de vorige stap zijn gegenereerd. *4.2.4*

Op basis van de bestanden die aan het einde van het scanproces worden verkregen, herberekent de FOD Binnenlandse Zaken de versleutelde versie en het trackingnummer van elk van de vermelde stembiljetten en maakt de trackingnummers openbaar, waarbij wordt aangegeven of ze overeenstemmen met getelde stembiljetten of met stembiljetten die op verzoek van de kiezer ongeldig zijn gemaakt. *3.3.2.3.1 4.2.3.2.2 4.2.3.2.3*

Op basis van diezelfde bestanden berekent de FOD Binnenlandse Zaken een zero-knowledge-proof van de geldigheid van elk van de versleutelde stembiljetten en van het feit dat de aangekondigde verkiezingsresultaten wel degelijk overeenstemmen met deze versleutelde stembiljetten. *4.2.3.2.3*

Kiezers die dat willen, kunnen controleren of het trackingnummer van hun stembiljet wel degelijk is vermeld in de lijst van stembiljetten die worden meegeteld, via de website van de FOD of via andere websites die door waarnemers of partijen worden gehost. *3.3.2.3.1*

Kiezers die hebben verzocht om een stembiljet ongeldig te maken en te controleren, kunnen desgewenst controleren of dit stembiljet wel degelijk is vermeld in de stembiljetten die niet worden meegenomen in de telling. *3.3.1.2*

Verkiezingswaarnemers die dat willen, hebben toegang tot alle versleutelde stembiljetten en zero-knowledge-proofs, controleren of deze versleutelde stembiljetten overeenkomen met de lijst met trackingnummers die is gepubliceerd, met het aantal stembiljetten dat in elk stembureau is geregistreerd en met de aangekondigde verkiezingsuitslag. De resultaten van al die controles worden doorgegeven aan de FOD Binnenlandse Zaken en het College van Deskundigen. *3.3.1.1 3.3.1.2 3.3.2.3.4 3.3.2.3.5 3.3.3.2.5*

4.5 HOE MOET BEVOTING II WORDEN ONTWIKKELD?

De keuze van een leverancier of leveranciers die een elektronisch stemsysteem zullen ontwikkelen, helpen te implementeren en upgraden is een grote uitdaging: ze verbindt België voor lange tijd (vaak tien tot vijftien jaar of meer) tot het gebruik van een systeem dat bedoeld is voor gebruik in kritieke omstandigheden en in een grotendeels nichemarkt, waarvoor vaak zeer specifieke expertise vereist is.

4.5.1 Groepen actoren op de markt van het elektronisch stemmen

Het feit dat de markt van stemmachines een nichemarkt is, betekent dat er slechts een klein aantal actoren is met ervaring in het organiseren van politieke verkiezingen met stemmachines.

In de Europese Unie merkt het International Institute for Democracy and Electoral Assistance (International IDEA) op dat alleen België, Bulgarije en Frankrijk stemmachines gebruiken.[45] Meer nog, in Frankrijk geldt sinds 2008 een moratorium dat alle nieuwe gemeenten verbiedt stemmachines in te zetten.[46] En Smartmatic, de huidige leverancier van de Belgische oplossing, is ook leverancier voor Bulgarije.[47]

Naast gespecialiseerde marktactoren kiezen een aantal landen ervoor om elektronisch stemmen te ontwikkelen via lokale ondernemingen, die vaak al erg actief zijn op andere markten. In Frankrijk wordt het stemmen via het internet, dat bij bepaalde verkiezingen wordt aangeboden aan Franse burgers die in het buitenland wonen, ontwikkeld door Voxaly, een merk van Docaposte, een bedrijf van de groep La Poste.[48] In Zwitserland worden ook tests inzake elektronisch stemmen gedaan met een systeem dat is ontwikkeld door La Poste.[49] In Brazilië worden de stemmachines ontwikkeld door Positivo Tecnologia, een Braziliaans bedrijf dat actief is in een brede waaier van IT-activiteiten, zowel hardware als software.[50] In India worden de stemmachines ontwikkeld door Electronics Corporation of India Limited, een overheidsbedrijf dat elektronische en IT-systemen levert.[51]

De markt van de privéverkiezingen is heel anders, met een groot aantal actoren die voornamelijk oplossingen voor stemmingen via het internet aanbieden. Verschillende Belgische oplossingen worden vermeld op de website van de sociale verkiezingen 2024 [55]. Deze actoren zijn wellicht in staat om competenties in te brengen op het vlak van verkiezingen, ook al zijn de kwesties van infrastructuur, veiligheid en onderhoud heel anders in een context van de politieke verkiezingen.

---

[45] *https://www.idea.int/data-tools/data/question?question_id=9349&database_theme=327*

[46] *https://www.legifrance.gouv.fr/download/pdf/circ?id=45311*

[47] *https://www.smartmatic.com/case-studies/bulgaria-first-binding-e-vote-is-100-accurate/*

[48] *https://www.voxaly.com/vote-par-internet-pour-les-francais-de-letranger-dans-le-cadre-des-elections-legislatives-2022/*

[49] *https://digital-solutions.post.ch/fr/e-government/solutions-numerisation/vote-electronique/*

[50] *https://www.reuters.com/world/americas/brazils-positivo-wins-207-million-voting-machines-tender-2021-12-27/*

[51] Deze machines worden onder meer beschreven in *https://thewire.in/government/the-anatomy-of-an-electronic-voting-machine-what-we-know-and-what-we-dont*

4.5.2 De kostprijs van de elektronische stemming

Het beoordelen van de totale kosten van een stemoplossing is helaas een zeer complexe en slecht gedocumenteerde aangelegenheid. Krimmer en zijn medeauteurs [40] wijzen op een aantal systematische problemen. De drie belangrijkste bronnen van moeilijkheden die worden genoemd, en die wij ook hebben ondervonden, zijn: *(i)* de moeilijkheid om toegang te krijgen tot de kosten, die niet systematisch openbaar worden gemaakt, *(ii)* de moeilijkheid om te weten wat wordt gedekt door de kosten die openbaar worden gemaakt, en wat wordt opgenomen in andere begrotingen (omvat een begroting voor de aankoop van machines de kosten voor ontwikkeling, onderhoud, updates, opslag, opleiding in het gebruik van de machines, ondersteuning tijdens de verkiezingen, enz.?), *(iii)* de moeilijkheid om de kosten te evalueren die verband houden met de bij de verkiezingen betrokken ambtenaren en openbare infrastructuren.

In het specifieke geval van stemmachines heeft een extra moeilijkheid bij het beoordelen van de kosten te maken met het zeer kleine aantal actoren op de Europese markt (tot nu toe lijkt alleen Smartmatic actief te zijn op de overheidsmarkt in Europa), wat vergelijkingen en mededinging bemoeilijkt en het moeilijk maakt om te anticiperen op de prijzen.

In België werden de kosten voor de aankoop van een stembureau met 5 stemmachines, een voorzittersmachine, een stembus, een scanner en bijbehorende kleine onderdelen (smartcards) in 2015 geschat op 11.585 euro exclusief btw. Dezelfde apparatuur, gehuurd voor één dag, wordt aangeboden tegen 1.975 euro [47]. Deze kosten houden geen rekening met een hele reeks andere kosten: de kosten voor technische ondersteuning tijdens de verkiezingen, de kosten voor de opleiding van de verschillende systeembedieners, de kosten voor de opslag, het onderhoud en de herstelling van de aangekochte stemsystemen, de kosten voor de totaliseringsbureaus, de kosten voor IT en de aanmaak van USB-sticks bij de FOD Binnenlandse Zaken, de kosten voor systeemaudits, enz.

Het inzicht in de kosten op één enkele markt, de Belgische, blijft zelf één enkel gegeven, op basis waarvan het uiterst riskant is om de kosten van een toekomstig systeem in te schatten. We stellen vast dat zelfs over één enkele periode de kosten voor vergelijkbare apparatuur enorm kunnen variëren.

Het is leerzaam om hier te verwijzen naar de Amerikaanse markt, die veel gediversifieerder is. VerifiedVoting geeft aan dat, voor de verkiezingen van 2024, ES&S en Dominion meer dan 70% van de markt in handen hebben, gevolgd door Hart InterCivic, Clear Ballot en Smartmatic, die de volgende 21% van het marktaandeel in handen hebben (de percentages worden geteld in termen van het aantal geregistreerde kiezers). Elektronisch tellen is alomtegenwoordig in de VS: slechts 0,2% van de stembiljetten wordt met de hand geteld.[52] Hoewel de totale kosten van elektronisch stemmen nog steeds zeer slecht bekend zijn, licht een studie uit 2021, gepubliceerd door VerifiedVoting, een tipje van de sluier op over de prijspraktijken voor een aantal apparaten [64]. Hieruit blijkt een grote variabiliteit: zo werd een van de best verkochte scanners voor stembiljetten, uitgerust met een stembus (de DS200 van ES S), in 110 verschillende rechtsgebieden aangekocht tegen prijzen die varieerden van 4.270 tot 6.975 USD. De variaties zijn met name het gevolg van de keuze van verschillende materialen voor de stembus, de beschikbaarheid van transportboxen of het

[52] *https://verifiedvoting.org/verifier/#mode/visualization/year/2024*

feit of de leveringskosten al dan niet zijn inbegrepen. Allianties van rechtsgebieden, die dus een grotere markt aanbieden, lijken ook betere prijzen te krijgen. De studie toont ook aan dat de aankoopprijs van de machines slechts een klein stukje van de puzzel is: we stellen vast dat de onderhoudskosten van de machines over een periode van tien jaar, van contract tot contract, variëren tussen 40% en 90% van de aankoopprijs van de machines – prijzen die ongetwijfeld een onderschatting zijn van de werkelijke prijzen, waarop de leveranciers een indexering toepassen.

VotingWorks lijkt de enige leverancier van stemapparatuur te zijn die zijn prijzen toont[53], met bijvoorbeeld een stemmachine uitgerust met een printer, ondersteunende apparaten, geïntegreerd in een vaste transportkist en ondersteund door een garantie van 5 jaar voor 1.750 USD.

4.5.3 De machines aanpassen of vernieuwen?

Een voor de hand liggende vraag in dit stadium is of de huidige stemmachines, eventueel aangepast, verder gebruikt kunnen worden of dat nieuwe aankopen nodig zijn.

De tweede generatie machines, geïntroduceerd in 2018, kan waarschijnlijk nog steeds worden gebruikt na 2027, met updates – zie de vergelijking en de compatibiliteit tussen de huidige machines en het BeVoting II-voorstel in punt *4.2.1.2.7.*

Aan de andere kant is de eerste generatie, geïntroduceerd in 2012, wellicht verouderd (de hardware is te beperkt om de huidige besturingssystemen te laten draaien en reserveonderdelen zijn waarschijnlijk onvindbaar geworden) en gemeenten die met deze machines zijn uitgerust en ook na 2027 elektronisch willen blijven stemmen, zullen worden geconfronteerd met de vraag om nieuwe apparatuur aan te schaffen, al was het maar om defecte machines te vervangen. Hetzelfde geldt voor nieuwe gemeenten die na 2027 willen overgaan op elektronisch stemmen.

Welke beslissing ook wordt genomen voor machines van de tweede generatie, het lijkt belangrijk om ertoe te komen de markt open te stellen voor nieuwe aankopen, zodat België de kosten en mogelijkheden van verschillende opties echt kan beoordelen, rekening houdend met de belemmeringen die België biedt voor toegang tot de markt, met name vanwege het relatief kleine aantal kiezers[54] en de versnippering van de Belgische markt. In dit opzicht lijkt het essentieel om één enkel aanspreekpunt aan te bieden voor ondernemingen die zich op de Belgische markt begeven.

Gezien de belangen die op het spel staan en de specifieke kenmerken van de aankoop van een elektronisch stemsysteem, vereist het ontwerp van een offerteaanvraag uiteraard veel expertise: op commercieel vlak, op juridisch vlak, inzake IT-infrastructuur en technieken met betrekking tot stemtechnologieën – er moeten grote inspanningen worden geleverd.

Het beoordelen van de reacties op de offerteaanvragen vereist zeker veel expertise. De procedure voor de beoordeling van de kwaliteit van het systeem, besproken in punt *4.3*, vergt ook veel

---

[53] *https://www.voting.works/voting-system/*

[54] Om enig idee te krijgen: de county Los Angeles alleen al heeft bijna 20.000 stemmachines ingezet voor de verkiezingen van 2020, ongeveer evenveel als België voor de verkiezingen van 2019. *https://www.smartmatic.com/us/case-studies/los-angeles-county-building-deploying-vsap-a-model-for-21st-century-elections/*

expertise, vooral dan op technisch vlak. De aanbeveling om de Directie van de verkiezingen van de FOD in het middelpunt van het beoordelingsproces te plaatsen en de beoordeling door deskundigen met verschillende achtergronden en door het publiek sterk uit te breiden, evenals de stimulansen voor deze beoordelingen, zijn elementen die aan de taken van de FOD worden toegevoegd. Interacties met de Zwitserse Bondskanselarij, die deze rol op zich heeft genomen in een land van vergelijkbare grootte als het onze, zouden zeker kunnen helpen om het beoordelingsproces in België vorm te geven.

4.5.4 Tijdschalen

De aanschaf van een nieuw stemsysteem kost tijd. De in 2007 gepubliceerde BeVoting-studie heeft geleid tot de aanschaf van stemmachines die werden ingezet voor de verkiezingen van 2012. Deze tijdschaal lijkt ons redelijk in de context van BeVoting II, aangezien het volgende moet gebeuren:

1. De wensen inzake de aanschaf van nieuwe machines en het onderhoud en de update van de bestaande machines in de verschillende gewesten objectief vastleggen.
2. Een eerste oproep tot informatie publiceren en verwerken, waarbij zoveel mogelijk actoren warm moeten worden gemaakt, om de interesses en capaciteiten van potentiële leveranciers te identificeren en om te vermijden dat er onbedoeld beperkingen in het formele aanbestedingsproces worden ingevoerd die bepaalde actoren onnodig zouden ontmoedigen of uitsluiten.
3. Een formele aanbesteding publiceren en de resultaten ervan beoordelen.
4. De ontwikkeling van de nieuwe generatie machines volgen en ervoor zorgen dat ze voldoen aan de internationale normen en aanbevelingen die van kracht zullen zijn.
5. Het proces van risicobeperkende audits uitwerken met de gekozen actoren.
6. Het ecosysteem ontwikkelen voor het publiceren en verifiëren van de geproduceerde gegevens voor end-to-end verificatie (individuele en universele controleerbaarheid).
7. Het proces voor de beoordeling van het systeem door deskundigen en het publiek ten uitvoer leggen.
8. De resultaten van de beoordelingen verwerken in het te implementeren systeem.

5 CONCLUSIES

5.1 INLEIDING

In deze studie hebben we een voorstel geformuleerd voor de ontwikkeling van het elektronisch stemsysteem met papieren bewijsstuk, aangepast aan de context van de Belgische verkiezingen, waarbij hardware- en softwareaspecten aan bod kwamen en specifieke aandacht werd besteed aan de vereisten inzake controleerbaarheid.

In een eerste fase hebben we een stand van zaken geschetst van het elektronische stemsysteem dat momenteel in België in gebruik is, op basis van de verslagen van de Colleges van Deskundigen en de

aanbevelingen van de Raad van Europa over elektronisch stemmen. Dit heeft ons ertoe gebracht negen hoofddoelstellingen te definiëren voor de verdere ontwikkeling van het huidige systeem, verdeeld over vijf krachtlijnen, waarop we hieronder zullen terugkomen.

Vervolgens hebben we meer specifiek gekeken naar de controleerbaarheidstechnieken die vandaag de stand van de techniek vormen en het product zijn van onderzoek dat grotendeels tot hun maturiteit heeft geleid in de afgelopen vijftien jaar, d.w.z. in de periode sinds het eerste BeVoting-onderzoek in 2007 [29].

Tot slot hebben we het concept van een nieuw stemsysteem voorgesteld, BeVoting II genaamd, dat beantwoordt aan de negen doelstellingen voor de verdere ontwikkeling van het huidige systeem en dat in het bijzonder de aspecten van controleerbaarheid integreert die vereist zijn door de recente internationale aanbevelingen, met name in Europa en de Verenigde Staten.

5.2 De doelstellingen van de verdere ontwikkeling van het huidige systeem bereiken

Hier vermelden we de doelstellingen die we aan het einde van onze stand van zaken (punt *2.5*) hebben geformuleerd en beoordelen we in hoeverre het BeVoting II-ontwerp het mogelijk maakt om deze doelstellingen te verwezenlijken.

5.2.1 Beheer van de hard- en de software

1. [goal-1] De uitrol van de stembureaus vereenvoudigen om de in punt *2.2.1.2* genoemde problemen aan te pakken.

De BeVoting II-stembureaus zijn aanzienlijk vereenvoudigd door het verdwijnen van de elektronische stembus en de machine van de voorzitter, die worden vervangen door een standaardstembus. Hier gaan meerdere belangrijke voordelen mee gepaard:

- Schrapping van een niet-standaardelement van het huidige systeem, waarvan de mogelijke defecten de normale indiening van de stembiljetten voor een volledig stembureau blokkeert.
- Schrapping van de opstartprocedure van het systeem op basis van een voorzittersmachine, die moet worden opgestart met behulp van USB-sticks voordat diezelfde USB-sticks kunnen worden gebruikt om de stemmachines op te starten en voordat de USB-sticks kunnen worden teruggeplaatst in de elektronische stembus.
- Vervanging van de smartcards door QR-codes op papier met, in een voor mensen leesbare vorm, de lijst van verkiezingen waaraan men kan deelnemen op basis van de QR-code.

Vervanging van de ticketprinter door een printer voor A4-papier lijkt ons ook praktische voordelen te bieden:

- We verwachten dat de leden van stembureaus meer gewend zullen zijn aan het laden van A4-papier in een printer, een handeling die voor veel mensen nog steeds heel gewoon is, dan aan het laden van een rol thermisch papier.
- Als de printer zich buiten de stemmachine bevindt, worden de risico's van papierstoringen in de stemmachine die gepaard gaan met de huidige ad-hocmontage, verminderd door een standaardprinter te gebruiken in de huidige gebruiksmodus.

Een nadeel van het gebruik van een externe printer is dat je een voedingskabel en een USB-kabel moet aansluiten. Maar nogmaals, deze handelingen zijn voor veel burgers heel gewoon.

1. Vertrekken van hardware die eenvoudig te repareren, te vervangen en te upgraden is, gezien de algemeen waargenomen levensduur van een stemsysteem, zoals besproken in de punten *2.4.1* en *2.4.2*.

De BeVoting II-stemmachine is nog steeds een geheel van volledig gestandaardiseerde componenten. De optie om deze componenten niet langer te assembleren in een stevige doos, die geen gemakkelijke wijzigingen/vervangingen toelaat, werd besproken: we vestigden de aandacht op het bestaan van nieuwe leveranciers die flexibelere assemblagemethodes aanbieden.

De elektronische stembus, het belangrijkste niet-standaardkenmerk van het huidige systeem, is geëlimineerd.

Het scannen van de stembiljetten kan worden uitgevoerd met een groot gamma aan standaardscanners.

Voor de verrichtingen inzake controleerbaarheid is geen speciale hardware nodig: een laptop en een projector voor de RLA, en de beschikbaarheid van rekenstations en een website voor de end-to-end controleerbaarheid.

1. Hardware kiezen om besturingssystemen en software te laten draaien die voldoen aan de veiligheidsnormen gedurende de levensduur van het systeem, zoals besproken in punt *2.4.1*.

Het streven naar een zeer lange levensduur voor een stemsysteem is een ingewikkelde en ongebruikelijke eis voor een IT-systeem.

Dit zijn onze belangrijkste antwoordelementen:

- Keuze voor volledig gestandaardiseerde hardware die gemakkelijk te vervangen is in geval van een defect, om opgewassen te zijn tegen problemen inzake reparatie en toegang tot reserveonderdelen.
- Een microcomputer of stemlaptop kiezen die in het begin robuust genoeg is om het besturingssysteem gedurende ongeveer vijf jaar te kunnen upgraden, voordat een supportfase voor het geïnstalleerde besturingssysteem ingaat, die volgens de huidige normen tot tien jaar kan duren.
- Alternatieve keuze voor een goedkope singleboardmicrocomputer, die tegen lage kosten vervangen kan worden en ook compatibel kan zijn met wijzigingen in het besturingssysteem over een lange periode. De keuze voor een van de laatste twee alternatieven hangt waarschijnlijk af van wat de verkopers kunnen bieden.

Het hergebruik voor het stemmen van standaardapparatuur die in andere contexten wordt gebruikt, is aantrekkelijk, maar lijkt ons bij nader inzien een moeilijk te implementeren optie onder voorwaarden die een uniforme ervaring voor de kiezers, een eenvoudige uitrol van de stembureaus (in lijn met de doelstelling *[goal-1]*), een eenvoudige uitrollogistiek en een veilig stemproces garanderen.

1. De verificatie van de conformiteit van de implementatie van de stemsoftware vergemakkelijken, zoals besproken in punt *2.2.2.2*.

Hier stellen we het volgende voor:

- Optimaal gebruikmaken van de veilige opstarttechnologieën en 'trusted platform modules' die op de meeste hedendaagse machines aanwezig zijn.
- Ervoor zorgen dat de stemmachines worden opgeslagen in goede omstandigheden voor toegangscontrole, waarbij sleutels van verschillende medewerkers nodig zijn om toegang te krijgen tot de machines, en met mechanismen om de toegang te controleren en te loggen.
- De nauwkeurigheid en traceerbaarheid van de logistieke distributieketen van de USB-sticks verhogen, inclusief een gescheiden distributie van de USB-sticks en de wachtwoorden.
- Als alternatief, en met behulp van beveiligde opstarttechnologieën, de stemsoftware en de bestanden voor de configuratie van de verkiezingen (semi)gecentraliseerd vooraf installeren op de stemmachines, zodat USB-sticks niet langer nodig zijn en een wachtwoord volstaat om de machines op te starten.

5.2.2 Toegankelijkheid

1. Het stemsysteem toegankelijker maken dan het nu is voor slechtzienden of minder behendige personen die moeite hebben met het selecteren van kandidaten op een scherm, zoals besproken in punt *2.3.1*.

Hier stellen we de volgende opties voor:

- De smartcardlezer op de huidige stemmachines vervangen door QR-codelezers en alle kiezers een externe app aanbieden waarmee stembiljetten vooraf kunnen worden ingevuld en waarmee een QR-code wordt weergegeven die door de stemmachine kan worden gescand, zodat deze een vooraf ingevuld stembiljet weergeeft dat de kiezer uiteraard nog kan wijzigen voordat het definitief wordt gevalideerd.
- Voortzetting van het proefproject voor de inzet van ondersteunende technologieën dat in 2019 plaatsvond in Aalst en Mechelen.

Aan de ene kant zou de hierboven voorgestelde app de kiezers in staat stellen om hun stembiljet voor te bereiden met behulp van hun eigen ondersteunende technologieën, aangepast aan hun behoeften, maar de app zou waarschijnlijk ook het stemproces voor iedereen versnellen, aangezien deze app een tijdbesparing voor iedereen zou betekenen in het stemhokje.

5.2.3 Transparantie

Hierbij wordt gestreefd naar het volgende:

1. Een methodologie voorstellen om de technische elementen van het elektronisch stemsysteem bekend te maken, waardoor het mogelijk wordt om zowel de transparantie als de kwaliteit van het systeem te verbeteren, zoals besproken in de punten *2.2.2.1* en *2.3.4*.

Hier worden de volgende voorstellen gedaan:

- De Directie van de verkiezingen van de FOD Binnenlandse Zaken centraal stellen in het beoordelingsproces, met inbegrip van de financiering ervan: de Directie van de verkiezingen selecteert de auditors.
- De broncode, de architectuur en de documentatie van het stemsysteem permanent publiceren, en niet slechts een paar maanden na de verkiezingen.
- De huidige auditprocedures door het CCB, een adviesorgaan en het College van Deskundigen handhaven.
- Geïnteresseerde partijen voorzien van de omgevingen die ze nodig hebben om het systeem te testen op hun eigen IT-infrastructuur.
- Een programma opzetten om zoveel mogelijk mensen te betrekken bij het daadwerkelijk onderzoeken van het stemsysteem en bij het formuleren van mogelijke verbeteringen aan het stemsysteem.

Hier lijkt het bijzonder interessant om gebruik te maken van de ervaring die in Zwitserland is opgedaan met een soortgelijk proces.

5.2.4 Controleerbaarheid

1. De kiezers in staat stellen om te controleren of hun stemintentie correct is geregistreerd en of hun stem wordt meegenomen, zonder te zijn gewijzigd, tijdens de telverrichtingen, zoals besproken in de punten *2.2.3* en *2.3.2*.

Het voorstel dat hier wordt gedaan is om de twee complementaire controleerbaarheidstechnieken te implementeren waarvan de toepassing de laatste vijftien jaar steeds meer standaard is geworden:

- de audits die het risico beperken dat een fout resultaat wordt gevalideerd (RLA),
- de end-to-end controleerbaarheid.

Dankzij de RLA's zal de garantie kunnen worden verkregen dat de elektronisch geproduceerde telling wel degelijk consistent is met alle papieren stembiljetten die door de kiezers zijn ingeleverd. Het succes van een RLA hangt af van de beschikbaarheid van authentieke papieren stembiljetten, of deze nu afkomstig zijn van elektronisch stemmen of van traditioneel stemmen op papier. De implementatie van een RLA zou plaatsvinden op het niveau van de kieskringen, en zou een zeer variabele menselijke inspanning vereisen, sterk afhankelijk van de verkiezingsmarge: een RLA zou een kleine inspanning kunnen betekenen bij verkiezingen waar het nodig zou zijn om een groot deel van de stemmen te wijzigen om de verkiezingsuitslag te veranderen, maar de RLA-procedure zou kunnen leiden tot een volledige telling van papieren stembiljetten in gevallen met uitzonderlijk lage marges.

End-to-end controleerbaarheid van haar kant maakt het mogelijk om effectief te controleren of de stembiljetten die door de stemmachines zijn voorbereid, correct zijn geïntegreerd in de elektronische telling, zonder verloren te zijn gegaan of te zijn gewijzigd. Deze techniek biedt dus aanvullende garanties bij die van de RLA's, die ervan uitgaan dat de beschikbare stembiljetten op geen enkele manier zijn gewijzigd tussen de indiening en het moment van de audit. Aan de andere kant is ze veel minder efficiënt in het identificeren van een stemmachine die valsspeelt en een

stembiljet produceert met een onjuiste QR-code, wat de RLA efficiënt zal kunnen detecteren. Wat de implementatie betreft, vereist end-to-end controleerbaarheid het opzetten van een IT-infrastructuur om de verificatiegegevens voor te bereiden en te hosten op het niveau van de Directie van de verkiezingen, en het ontwikkelen van een ecosysteem van software en personen die geïnteresseerd zijn in het verifiëren van deze gegevens. In tegenstelling tot RLA's hangt de complexiteit van de processen die gepaard gaan met end-to-end controleerbaarheid, niet af van de verkiezingsmarges.

1. Het mogelijk maken deze controles uit te voeren zonder het stemgeheim in gevaar te brengen – het voorgestelde proces moet met name tegemoetkomen aan de bekommernissen die in punt *2.3.3.* worden aangekaart.

BeVoting II volgt hier de voorstellen van de Colleges van Deskundigen om de stembiljetten niet langer te scannen en te registreren wanneer ze in de stembussen worden gedeponeerd. Het voorstel is om scanbureaus in te richten, vergelijkbaar met bureaus voor het tellen van de papieren stembiljetten, maar in veel kleinere aantallen, om een consistent niveau van stemgeheim te bieden tussen de verschillende stemmethoden en om robuuste scanbureaus te kunnen inrichten met gemakkelijke toegang tot de ondersteunende diensten, waardoor de risico's die gepaard gaan met het scannen in de stembureaus worden vermeden.

5.2.5 Rapportage

1. Eenvoudige rapportagemechanismen opzetten die het mogelijk maken om de ontvangen gegevens efficiënt te compileren, zodat er een duidelijke meting is van het aantal incidenten en hun gevolgen, zoals besproken in de punten *2.2.1.2* en *2.3.5*.

Hier is het voorstel om een efficiënt instrument voor rapportage en compilatie van rapporten op te zetten voor alle stem- en telbureaus, dat de vorm zou kunnen aannemen van een mobiele applicatie of een webpagina waarop de leden van de bureaus eventuele problemen met slechts een paar klikken kunnen aangeven.

Dit zal een systematischer inzicht geven in de werking van het systeem dan wat momenteel kan worden verkregen via de huidige steekproeven, en zal helpen om moeilijk waarneembare aanvallen te identificeren die in verschillende stembureaus zouden kunnen plaatsvinden.

5.3 DANKWOORD

De auteurs willen graag de vele mensen bedanken met wie ze van gedachten hebben kunnen wisselen in het kader van deze studie, en die een grote bijdrage hebben geleverd aan de informatie, in het bijzonder: Josh Benaloh, Henri Devillez, Alex Halderman, Thomas Peters, Philip Stark, Vanessa Teague en Emmanuel Willems. We hadden ook veel baat bij enkele zeer verhelderende interacties met leden van de Directie van de verkiezingen van de FOD Binnenlandse Zaken, bpost, Smartmatic en VotingWorks. Eventuele vergissingen in deze studie blijven evenwel onze verantwoordelijkheid.

[1] Abdalla, M., Bellare, M. and Rogaway, P. 2001. The oracle diffie-hellman assumptions and an analysis of DHIES. *Topics in cryptology - CT-RSA 2001* (2001), 143-158.

[2] Adida, B., Marneffe, O. de, Pereira, O. and Quisquater, J. 2009. Electing a university president using open-audit voting: Analysis of real-world use of helios. *2009 electronic voting technology workshop / workshop on trustworthy elections, EVT/WOTE '09* (2009).

[3] Benaloh, J. 1987. Verifiable secret-ballot elections. PhD Thesis - Yale University.

[4] Benaloh, J., Rivest, R., Ryan, P.Y.A., Stark, P., Teague, V. and Vora, P. 2015. End-to-end verifiability.

[5] Bernhard, M., McDonald, A., Meng, H., Hwa, J., Bajaj, N., Chang, K. and Halderman, J.A. 2020. Can voters detect malicious manipulation of ballot marking devices? *2020 IEEE symposium on security and privacy, SP 2020, San Francisco, CA, USA, 18-21 may 2020* (2020), 679–694.

[6] Blom, M.L., Conway, A., King, D., Sandrolini, L., Stark, P.B., Stuckey, P.J. and Teague, V. 2020. You can do RLAs for IRV. *CoRR*. abs/2004.00235, (2020).

[7] Boneh, D. 1998. The Decision Diffie-Hellman problem. *Algorithmic number theory, third international symposium, ants-iii* (1998), 48-63.

[8] Burton, C., Culnane, C. and Schneider, S.A. 2016. VVote: Verifiable electronic voting in practice. *IEEE Secur. Priv.* 14, 4 (2016), 64-73. DOI:*https://doi.org/10.1109/MSP.2016.69*.

[9] Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T. and Vora, P.L. 2010. Scantegrity II municipal election at takoma park: The first E2E binding governmental election with ballot privacy. *19th USENIX security symposium* (2010), 291-306.

[10] Carter Center 2022. Risk-limiting audits: A guide for election observation efforts. *https://www.cartercenter.org/resources/pdfs/peace/democracy/risk-limiting-audits-guide.pdf*.

[11] Chancellerie fédérale de la Confédération suisse 2022. Ordonnance de la chfsur le vote électronique 161.116. *https://www.fedlex.admin.ch/eli/cc/2022/336/fr*.

[12] Chaum, D. and Pedersen, T.P. 1992. Wallet databases with observers. *Advances in cryptology - CRYPTO '92, 12th annual international cryptology conference* (1992), 89-105.

[13] Collège des experts 2018. Rapport du collège d'experts chargés du contrôle des systèmes de vote électronique pour les élections communales de la région de bruxelles-capitale. Parlement bruxellois. A-748-1 - 2018/2019.

[14] Collège des experts 2019. Rapport du Collège d'experts chargés du contrôle des systèmes électroniques de vote, de dépouillement et de collecte des résultats. Élections simultanées du 26 mai 2019 pour le Parlement européen, la Chambre des représentants et les Parlements de région et communauté. Chambre des représentants de Belgique. DOC 55 0014/001.

[15] Collège des experts 2012. Rapport du collège d'experts chargés du contrôle du système de vote et de dépouillement automatisés pour les élections communales de la région de bruxelles-capitale. Parlement bruxellois. A-323/1 - 2012/2013.

[16] Collège des experts 2014. Rapport du collège d'experts chargés du contrôle dy système de vote et de dépouillement automatisés. Élections simultanées du 25 mai 2014. Chambre des représentants de Belgique. DOC 54 0014/001.

[17] Collège d'experts chargés du contrôle des systèmes de vote automatisés 2012. Rapport concernant les élections communales et provinciales du 14 octobre 2012 en wallonie.

[18] Collège d'experts chargés du contrôle des systèmes de vote automatisés 2018. Rapport concernant les élections communales et provinciales du 14 octobre 2018 en wallonie. Parlement wallon. 1316 (2018/2019) – No 1.

[19] College van deskundigen 2012. College van deskundigen belast met de controle op de geautomatiseerde stemmingen – verslag van de verkiezingen van 14 oktober 2012. Vlaams Parlement.

[20] College van deskundigen 2018. Verslag van het college van deskundigen belast met de controle op de geautomatiseerde stemmingen en opnemingen over de provincie-, gemeente- en districtsraadverkiezingen van 14 oktober 2018. Vlaams Parlement – 1715 (2018-2019) - Nr. 1.

[21] Colorado Secretary of State Audit Center. *https://www.sos.state.co.us/pubs/elections/auditCenter.html*.

[22] Conseil de l'Europe 2017. Lignes directrices pour la mise en œuvre des dispositions de la recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique. *https://www.coe.int/fr/web/electoral-assistance/e-voting*.

[23] Conseil de l'Europe 2017. Recommandation CM/Rec(2017)5 du Comité des Ministres aux Etats membres sur les normes relatives au vote électronique. *https://www.coe.int/fr/web/electoral-assistance/e-voting*.

[24] Cortier, V., Gaudry, P. and Glondu, S. 2019. Belenios: A simple private and verifiable electronic voting system. *Foundations of security, protocols, and equational reasoning - essays dedicated to Catherine A. Meadows* (2019), 214–238.

[25] Cortier, V., Gaudry, P. and Glondu, S. 2023. Vérifiabilité des élections législatives partielles 2023, réalisées par voie électronique. *https://verifiabilite-legislatives2023.fr/*.

[26] Cramer, R., Damgård, I. and Schoenmakers, B. 1994. Proofs of partial knowledge and simplified design of witness hiding protocols. *Advances in cryptology - CRYPTO '94, 14th annual international cryptology conference* (1994), 174–187.

[27] Cramer, R., Gennaro, R. and Schoenmakers, B. 1997. A secure and optimally efficient multi-authority election scheme. *Advances in cryptology - EUROCRYPT '97* (1997), 103-118.

[28] Culnane, C. and Schneider, S.A. 2014. A peered bulletin board for robust use in verifiable voting systems. *IEEE 27th computer security foundations symposium, CSF 2014* (2014), 169-183.

[29] De Cock, D., Bosselaers, A., Milgrom, E., Rijmen, V., Coudert, F., Engelen, J., Marneffe, O. de, Koeune, F., Lobelle, M., Pereira, O., Preneel, B., Quisquater, J.-J. and Vercauteren, F. 2007. BeVoting – Etude des systèmes de vote électronique. http://hdl.handle.net/2078.1/281976.

[30] Devillez, H., Pereira, O. and Peters, T. 2022. How to verifiably encrypt many bits for an election? *Computer security - ESORICS 2022 - 27th european symposium on research in computer security* (2022), 653–671.

[31] ElectionGuard 2023. *https://www.electionguard.vote/*.

[32] ElGamal, T. 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*. 31, 4 (1985), 469-472.

[33] Fiat, A. and Shamir, A. 1986. How to prove yourself: Practical solutions to identification and signature problems. *Advances in cryptology - CRYPTO '86* (1986), 186-194.

[34] Georgia Secretary of State 2020. 2020 General Election Risk-Limiting Audit. *https://sos.ga.gov/page/2020-general-election-risk-limiting-audit*.

[35] Gjøsteen, K. 2013. The Norwegian Internet Voting Protocol. Cryptology ePrint Archive, Paper 2013/473.

[36] Hall, J.L., Stark, P.B., Miratrix, L., Briones, M., Ginnold, E., Oakley, F., Peaden, M., Pellerin, G., Stanionis, T. and Webber, T. 2009. Implementing risk-limiting post-election audits in california. *2009 electronic voting technology workshop / workshop on trustworthy elections, EVT/WOTE '09* (2009).

[37] Heiberg, S., Martens, T., Vinkel, P. and Willemson, J. 2016. Improving the Verifiability of the Estonian Internet Voting Scheme. *Electronic voting - first international joint conference, e-vote-id 2016* (2016), 92–107.

[38] Hirschi, L., Schmid, L. and Basin, D.A. 2021. Fixing the Achilles Heel of E-Voting: The Bulletin Board. *34th IEEE computer security foundations symposium, CSF 2021* (2021), 1–17.

[39] Kortum, P.T., Byrne, M.D., Azubike, C.O. and Roty, L.E. 2022. Can voters detect errors on their printed ballots? Absolutely. *CoRR*. abs/2204.09780, (2022).

[40] Krimmer, R., Duenas-Cid, D., Krivonosova, I., Vinkel, P. and Koitmae, A. 2018. How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. *Electronic voting - third international joint conference, e-vote-id 2018* (2018), 117-131.

[41] Morrell, J. 2019. Knowing it's right, part one: A practical guide to risk-limiting audits. *https://electionline.org/resources/rla-practical-guide/*.

[42] Morrell, J. 2021. Knowing it's right part four: Ballot accounting audits best practices guide. *https://electionline.org/resources/knowing-its-right-part-four-ballot-accounting-audits-best-practices-guide/*.

[43] Morrell, J. 2020. Knowing it's right part three: Planning and conducting a risk limiting audit pilot. *https://electionline.org/resources/knowing-its-right-part-3-planning-and-conducting-a-risk-limiting-audit-pilot/*.

[44] Morrell, J. 2019. Knowing it's right part two: Risk-limiting audit implementation workbook. *https://electionline.org/resources/rla-implementation-workbook/*.

[45] National Academies of Sciences, Engineering, and Medicine. 2018. Securing the Vote: Protecting American Democracy. The National Academies Press.

[46] NIS Cooperation Group Compendium on Cyber Security of ElectionTechnology – CG Publication 03/2018. *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645*.

[47] Parlement de la Région de Bruxelles-Capitale 2015. VI. Annexe – Rapport relatif aux auditions sur les systèmes de vote, approuvé par MM. Emmanuel De Bock et Julien Uyttendaele, rapporteurs. *http://www.weblex.irisnet.be/data/crb/doc/2015-16/129202/images.pdf*.

[48] Pedersen, T.P. 1991. A threshold cryptosystem without a trusted party (extended abstract). *Advances in cryptology - EUROCRYPT '91* (1991), 522-526.

[49] Pedersen, T.P. 1991. Non-interactive and information-theoretic secure verifiable secret sharing. *Advances in cryptology - CRYPTO '91* (1991), 129-140.

[50] Pilet, J.-B., Preneel, P.B., Erzeel, S., Pereira, O., Sbaraglia, F., Tibbaut, A., Carpent, X. and Dandoy, R. 2021. Projet NETVOTING.BE – Etude sur la possibilité d'introduire le vote Internet en Belgique – Volet 2. *https://elections.fgov.be/informations-generales/etude-sur-la-possibilite-dintroduire-le-vote-internet-en-belgique*.

[51] Pilet, J.-B., Sanhuza, M.J., Talukder, D., Dodeigne, J. and Brennan, A.E. 2019. Opening the opaque blank box. *Politics of the Low Countries*. 1, 3 (Nov. 2019), 182-204. DOI:*https://doi.org/10.5553/plc/258999292019001003003*.

[52] Rhode Island RLA Working Group 2019. Pilot Implementation Study of Risk-Limiting Audit Methods in the State of Rhode Island. *https://www.brennancenter.org/our-work/research-reports/pilot-implementation-study-risk-limiting-audit-methods-state-rhode-island*.

[53] Ryan, P.Y.A., Rønne, P.B. and Iovino, V. 2016. Selene: Voting with transparent verifiability and coercion-mitigation. *Financial cryptography and data security - FC 2016 international workshops* (2016), 176-192.

[54] Schürmann, C. 2016. A Risk-Limiting Audit in Denmark: A Pilot. *Electronic voting - first international joint conference, e-vote-id 2016* (2016), 192-202.

[55] Federale Overheidsdienst Werkgelegenheid, Arbeid en Sociaal Overleg 2023. Elektronisch stemmen. *https://emploi.belgique.be/fr/themes/concertation-sociale/elections-sociales-2024/vote-electronique*.

[56] Sridhar, M. and Rivest, R.L. 2019. K-cut: A simple approximately-uniform method for sampling ballots in post-election audits. *Financial cryptography and data security - FC 2019 international workshops, VOTING and wtsc* (2019), 242-256.

[57] Stark, P.B. 2008. Conservative statistical post-election audits. *The Annals of Applied Statistics*. 2, 2 (2008), 550-581.

[58] Stark, P.B. 2020. Sets of half-average nulls generate risk-limiting audits: SHANGRLA. *Financial cryptography and data security - FC 2020 international workshops* (2020), 319-336.

[59] Stark, P.B. 2019. There is no reliable way to detect hacked ballot-marking devices. *CoRR*. abs/1908.08144, (2019).

[60] State of Colorado Risk-Limiting Audit – Final Report – Post-Election Audit Initiative – Grant No. EAC110150E. *https://www.eac.gov/sites/default/files/eac_assets/1/28/Risk-Limiting%20Audit%20Report%20-%20Final%20.CO.pdf*.

[61] Swiss Post 2023. The Swiss Post e-voting system. *https://gitlab.com/swisspost-evoting/*.

[62] Technical Guidelines Development Committee 2021. Voluntary VotingSystem Guidelines – VVSG 2.0. *https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines*.

[63] U.S. Vote Foundation 2015. The Future of Internet Voting – End-to-end verfiable Internet voting – Specification and assessment study. *https://www.usvotefoundation.org/E2E-VIV*.

[64] Verified Voting 2021. The price of voting. *https://verifiedvoting.org/wp-content/uploads/2021/03/Price-of-Voting-FINAL2.pdf*.

[65] Verified Voting The Verifier — Post-Election Audits — November 2024. *https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/audit/year/2024*.

[66] Wallach, D.S. 2019. On the security of ballot marking devices. *CoRR*. abs/1908.01897, (2019).

[67] Wolchok, S., Wustrow, E., Halderman, J.A., Prasad, H.K., Kankipati, A., Sakhamuri, S.K., Yagati, V. and Gonggrijp, R. 2010. Security analysis of India's electronic voting machines. *Proceedings of the 17th ACM conference on computer and communications security, CCS 2010* (2010), 1-14.

[68] 2023. Kieswetboek. Beschikbaar via *https://verkiezingen.fgov.be/wetgeving/wetten*. Originele versie op *https://www.ejustice.just.fgov.be/eli/wet/1894/04/12/1894041255/justel*.

[69] 2023. Wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstuk – bijgewerkt op 14 april 2023. Beschikbaar via *https://verkiezingen.fgov.be/wetgeving/wetten*. Originele versie op *https://www.ejustice.just.fgov.be/eli/wet/2014/02/07/2014000108/justel*.