BeVoting II

Étude sur l'évolution du vote électronique avec preuve papier en Belgique

Olivier Pereira – Cyprien Delpech de Saint Guilhem – Bart Preneel

Université catholique de Louvain – Katholieke Universiteit Leuven

18 février 2024

Synthèse de l'étude

Cadre de l'étude La présente étude répond à des interrogations de la Direction Élections du SPF Intérieur portant sur l'évolution du vote électronique avec preuve papier en Belgique, tant en terme de matériel de vote qu'en terme de possibilités de vérifier les résultats des élections.

Ces interrogations se placent dans la cadre de la fin du marché avec le fournisseur du système de vote électronique actuellement utilisé à l'horizon de 2027, système qui est basé sur une étude qui date de 2007. La Direction des Élections a structuré cette étude autour de trois questions centrales. Nous les présentons ici, et résumons les éléments centraux de réponse que nous apportons.

Question 1 : Évaluation du système de vote électronique actuel Cette première question porte sur l'évaluation du système de vote électronique actuel et sur sa conformité aux exigences actuelles de qualité et de sécurité.

Nous avons identifié un ensemble d'évolutions qui seraient nécessaires pour que le système de vote électronique belge réponde aux recommandations internationales en matière de vote électronique, en particulier celles du Conseil de l'Europe de 2017, ainsi que pour résoudre des difficultés récurrentes observées lors de l'usage du système actuel. Ces évolutions sont regroupées en cinq catégories :

1. *Simplifier la gestion et le déploiement du système de vote.* On cherche ici à faciliter l'installation et le démarrage du système de vote dans les bureaux de vote, mais aussi à simplifier sa maintenance dans la durée, ainsi que la vérification de sa conformité.
2. *Améliorer l'accessibilité.* On cherchera à faciliter l'accès au système de vote par la plus grande part de la population, en tirant parti des opportunités d'accessibilité offertes par le vote électronique.
3. *Transparence.* On recommande ici une transparence accrue sur le système de vote, ainsi que la mise en œuvre de mesures permettant de tirer les bénéfices de cette transparence. Si la Belgique a été pionnière en matière de publication de ses logiciels de vote, les recommandations actuelles et les pratiques d'autres pays vont aujourd'hui beaucoup plus loin, avec des effets positifs observés.

4. *Vérifiabilité.* On propose ici deux évolutions majeures en vue de permettre la vérification efficace et indépendante des résultats des élections, dans le respect du secret des votes. Ces évolutions permettent de détecter d'éventuelles erreurs ou intrusions dans le système, et d'offrir des preuves que les résultats des élections sont corrects.
5. *Reporting.* On vise ici la mise en œuvre de mécanismes permettant de compiler de manière efficace les incidents observés lors du déploiement du système de vote, afin de faciliter la mesure de leurs éventuelles conséquences.

Question 2 : Proposition du concept d'un nouveau système de vote

Nous proposons ensuite BeVoting II, un nouveau concepte de système de vote électronique basé sur le système actuel.

BeVoting II maintient le principe, à la base du système actuel, d'utiliser des machines de vote qui produisent des bulletins de vote papier et ne comptabilisent pas les votes. Ce principe apparaît comme largement confirmé par les évolutions des dernières années, avec un abandon des systèmes sans bulletin papier dans de nombreux états.

Par rapport au système actuel, BeVoting II propose plusieurs changements importants, et en particulier :

1. L'abandon de l'urne électronique actuelle, qui est le principal composant non-standard du système, complexifie le déploiement des bureaux de vote, et peut affaiblir le secret du vote. Celle-ci est remplacée par des urnes classiques, comme celles utilisées pour le vote papier.
2. L'introduction d'une application permettant de préparer son bulletin de vote à l'avance et de scanner un code QR dans l'isoloir, permettant à la machine de vote d'afficher les pré-selections et à l'électeur de confirmer (ou de modifier) ses choix. Cette option permettrait d'accélérer le processus de vote pour tous, et aux personnes qui le souhaitent d'employer leur propres dispositifs d'accessibilité sur leur propre appareil pour préparer le bulletin. Ceci vient en complément d'une recommandation de poursuivre les pilotes de 2019 visant à améliorer l'accessibilité des machines de vote dans les isoloirs.
3. L'introduction de bureaux de scanning, dans lesquels les bulletins déposés dans les urnes sont scannés. L'organisation de ces bureaux est similaire à celle des bureaux de dépouillement, mais leur mise en œuvre demandera des efforts bien plus limités grâce aux évolutions des scanners à grande vitesse.

4. L'introduction d'audits limitant le risque de valider un résultat erroné, organisé au niveau des circonscriptions électorales. Cet audit, qui est devenu une obligation dans un nombre croissant d'états américains, permet de s'assurer que le dépouillement effectué électroniquement via scanning reflète bien les bulletins papier.
5. L'introduction d'une procédure de vérifiabilité de bout en bout qui permet aux électeurs, en se connectant à un site web, de s'assurer que le bulletin de vote qu'ils ont produit dans l'isoloir a bien été comptabilisé dans le dépouillement, sans avoir fait l'objet de modifications.
6. Le déploiement d'une application de reporting des éventuels incidents dans les bureaux de vote et de scanning, permettant une description rapide des incidents et une compilation efficace des données, à destination des organisateurs de l'élection et du Collège des experts.

Question 3 : Choix du matériel pour le nouveau système de vote proposé Le choix du matériel et du logiciel pour le vote électronique doit permettre de répondre à des contraintes très spécifiques. Il doit notamment permettre une durée de vie du système sensiblement plus longue que la durée de vie classique du matériel informatique ; il doit permettre un déploiement rapide et non planifié, notamment pour répondre à la nécessité d'organiser une élection dans un délai de 40 jours en cas de dissolution de la Chambre ; il doit être suffisamment standardisé et testé que pour garantir un accès équitable et de qualité aux électeurs ; il doit permettre un support rapide en cas de dysfonctionnement durant les élections ; il doit aussi répondre à d'importantes exigences de sécurité et d'intégrité, le tout en limitant les coûts autant que possible.

Le choix d'équipement peut aussi être compliqué par la petite taille du marché européen en matière de machines de vote pour des élections nationales.

La conception du système BeVoting II, couplée avec les évolution du matériel au cours des 15 dernières années, permet de réaliser les choix suivants :

1. Un système entièrement réalisé par l'assemblage d'un petit nombre de composants standard. Ceci permet une substitution peu coûteuse de composants qui tomberaient en panne, par de nouveaux composants bon marché, et évite la contrainte de retrouver des pièces d'origine qui n'existeraient plus ou de devoir recréer du matériel spécifique.
2. Un matériel permettant de conserver un système d'exploitation et des logiciels aux normes de sécurité pendant plus de 10 ans.

Les contraintes d'intégrité, de fiabilité et de disponibilité rendent peu probable de parvenir à mutualiser les ordinateurs ou laptops qui seraient inclus dans le système de vote.

Conclusions Le concept du système de vote BeVoting II décrit dans cette étude apporte une réponse aux manquements du système de vote électronique actuellement utilisé en Belgique par rapport aux recommandations du Conseil de l'Europe de 2017, et répond aussi aux difficultés qui ont pu être relevées par les Collèges des experts lors du déploiement de ce même système de vote.

En particulier, BeVoting II intègre les techniques de vérifiabilité d'élections qui correspondent à l'état de l'art. Ces techniques constituent un élément de réponse fondamental dans le climat de désinformation qui a pu se développer autour des élections dans bon nombre de pays du monde, ainsi que face à l'accroissement considérable, au cours des quinze dernières années, des risques d'ingérences internationales dans les élections belges.

La matériel requis pour la mise en œuvre de BeVoting II est entièrement standard, facilitant la maintenance et la durabilité du système. Il est proposé que le logiciel de vote fasse l'objet d'un large processus de review indépendant et accessible au public, sous la houlette de la Direction des Élections du SPF Intérieur, et ce bien avant le début des périodes électorales.

Table des matières

Partie 1
Introduction

La présente étude a été réalisée en réponse à une interrogation de la Direction des Élections du Service public fédéral Intérieur et a pour objectif de définir comment le système de vote électronique avec preuve papier actuellement utilisé en Belgique peut évoluer en termes de matériel, logiciel et également en terme de vérifiabilité.

1.1 Contexte de l'étude

Le système de vote électronique actuel est déployé depuis les élections de 2012 (suite à un projet pilote qui avait eu lieu en 2011). C'est un système de vote déployé dans des bureaux de vote classiques. Les électeurs se rendent dans un isoloir, où ils expriment leur vote sur une machine de vote qui imprime un bulletin de vote papier. Les électeurs vérifient que le bulletin de vote papier reprend bien leur intention de vote de manière lisible, puis se rendent auprès d'une urne électronique, où ils scannent un code QR présent sur le bulletin papier. Le code QR contient l'intention de vote qui est stockée, chiffrée, sur la machine du Président du Bureau de vote. Quand le scan est réussi, un clapet s'ouvre sur l'urne et permet le dépôt du bulletin de vote. Les votes sont totalisés dans les Bureaux principaux de canton sur base des enregistrements réalisés sur les machines de Président dans les différents Bureaux de vote. Les bulletins papier sont conservés à des fins d'audit et permettent, si besoin, de réaliser un dépouillement papier.

La Direction des Élections structure les questionnements de l'étude autour de deux thématiques centrales : l'évolution des équipements de vote et la vérifiabilité des résultats des élections. Elle relève ainsi certains avantages et inconvénients du système actuel. En termes d'avantage, elle relève la pré-

sence du bulletin de vote papier qui permet aux électeurs de s'assurer qu'une preuve de leur intention de vote existe et permet un dépouillement papier en cas de problème avec le système électronique. Elle relève aussi l'absence de disque dur et de connectivité réseau sur les machines de vote, qui limitent la surface exposée à des attaques informatiques. En termes d'inconvénients, elle relève le besoin d'investissement dans du matériel spécifique qui, au total, représente un coût important : plus de 20 000 machines de vote sont utilisées aujourd'hui. Elle relève aussi l'obsolescence rapide du matériel, l'impossibilité de trouver des pièces de rechange pour réparer les pannes, et les restrictions qui surviennent lors de mises à jour de sécurité en raison des exigences croissantes en termes d'évolution du logiciel, exigences qui peuvent cesser d'être remplies par le matériel existant. Enfin, elle relève l'absence de possibilité pour l'électeur de vérifier que son vote a été correctement enregistré et totalisé, alors que l'offre de cette possibilité fait partie des Recommandations du Conseil de l'Europe en matière de vote électronique.

Le système actuel est fourni par la société Smartmatic, avec qui la Belgique a un contrat qui prend fin en 2027. La présente étude a pour objectif d'examiner de quelle manière les Belges pourraient continuer à voter électroniquement après 2027 en se donnant le système actuel comme point de départ. En corollaire, il n'est pas dans les objectifs de cette étude d'évaluer les mérites du vote électronique par rapport au vote papier ou ceux du vote à distance par rapport au vote en personne : le cadre donné est bien celui d'un système de vote électronique avec preuve papier déployé dans des bureaux de vote.

1.2 État des lieux

La première partie de l'étude évalue le système de vote électronique actuellement utilisé en Belgique. Cette évaluation est effectuée en suivant trois axes.

Dans le premier axe, nous évaluons la manière dont le système électronique actuel a pu répondre aux besoins durant les élections qui ont eu lieu depuis 2012. Nous nous basons pour cela sur les rapports que les Collèges des experts produisent après chaque élection. Les Collèges des experts y décrivent leurs opérations de contrôle sur la préparation, l'utilisation, et le bon fonctionnement de l'ensemble des systèmes de vote, d'enregistrement et de dépouillement pour le vote électronique. Les Collèges émettent aussi un certain nombre de recommandations visant à améliorer le système de vote électronique, recommandations qui ont mené à un certain nombre d'évolu-

tions du système au cours des dernières années.

Dans le second axe, nous évaluons l'adéquation du système de vote électronique actuel aux recommandations internationales en vigueur. Celles-ci ont évolué de manière importante depuis la conception du système de vote électronique actuellement utilisé, reflétant notamment les avancées de la recherche scientifique qui ont eu lieu au cours des 15 dernières années – on se souviendra que le système actuel a été conçu sur base d'une étude BeVoting réalisée en 2007 [30].

Dans le troisième axe, nous évaluons le système de vote électronique actuel du point de vue de son gestionnaire, qui doit en assurer les coûts et la maintenance sur une longue durée de vie – le contrat actuel avec Smartmatic porte sur une durée de vie de 15 ans, ce qui est largement supérieur à la durée de vie habituelle de matériel informatique.

Cette partie de l'étude se conclut par neuf objectifs principaux d'améliorations du système actuel, répartis en cinq catégories : *(1)* Gestion du matériel et du logiciel, *(2)* Accessibilité du système, *(3)* Transparence, *(4)* Vérifiabilité, *(5)* Reporting.

1.3 Vérifiabilité

La deuxième partie de l'étude s'intéresse aux technologies de vérifiabilité, qui sont la principale avancée technologique en matière de vote électronique au cours des 15 dernières années, et dont l'étude est demandée par la Direction des élections, en accord avec les Recommandations du Conseil de l'Europe sur le vote électronique.

Ces technologies offrent comme premier bénéfice de permettre, par des moyens indépendants du système de vote, de vérifier le bon fonctionnement de celui-ci. Ceci est évidemment important dans le cadre d'un système de vote électronique, où l'on se sert d'ordinateurs dont le fonctionnement est toujours difficile à observer. Ceci est d'autant plus important que les risques associés à l'ingérence internationale dans les élections belges n'ont fait que croître au cours des 15 dernières années, et où les infrastructures de vote sont clairement des infrastructures critques sans ce processus.

Un second bénéfice est de permettre aux organisateurs d'élections de fournir des preuves que les résultats annoncés sont corrects. La disponibilité de telles preuves est rendue particulièrement importante dans un contexte où les résultats sont contestés de plus en plus ouvertement dans différents pays, menant parfois à des attaques contre les institutions publiques, et où les personnes impliquées de l'organisation et le support aux élections sont de

plus en plus exposées à des accusations, menaces et divulgation de données personnelles[1]. La possibilité de démontrer que les résultats d'une élection sont corrects, par opposition à l'absence de preuve qu'ils sont incorrects, est vue comme un moyen de lutter contre la prolifétation d'informations fallacieuses.

Nous abordons les deux grandes approches existantes qui nécessitent : les audits limitant le risque qu'un résultat incorrect soit validé, qui mettent essentiellement en œuvre des techniques de vérification statistiques, et la vérifiabilité de bout en bout, qui mettent essentiellement en œuvre des techniques issues de la cryptographie.

Ces deux approches sont complémentaires, et nécessitent que les systèmes de vote soient conçus pour permettre leur mise en œuvre : dès la conception du système, il est nécessaire de s'assurer que les données nécessaires à l'audit et à la vérifiabilité soient produites, accessibles, et permettent des audits et des vérifications efficaces. Ces techniques ont été mises en œuvre, avec divers niveaux de maturité, dans d'autres pays. Nous nous basons sur l'expérience acquise ailleurs, et explorons les possibilités d'adapter ces techniques au contexte belge et à ses importantes spécificités : bulletins de vote listant parfois un très grand nombre de candidats, méthodes de dépouillement spécifiques, etc.

Nous proposerons des méthodes concrètes pour organiser un déploiement de ces méthodes dans un contexte belge, ainsi qu'une évaluation de la complexité d'un tel déploiement sur base des données publiées lors d'élections belges précédentes et de techniques d'audit et de vérification qui correspondent à l'état de l'art des méthodes déployées aujourd'hui.

1.4 Description d'un nouveau système de vote électronique

La troisième et dernière partie de l'étude s'intéresse à la description du concept d'un nouveau système de vote électronique, BeVoting II, qui pourrait être déployé en Belgique après 2027. Ce concept apporte une réponse aux neuf objectifs principaux qui ont émergé de l'état des lieux actuel, et décrit

1. Ce phénomène a notamment pris une telle ampleur aux États-Unis que, depuis 2020, 14 états ont voté de nouvelles lois visant à protéger les personnes en charge de l'organisation d'élection et travaillant dans les bureaux de vote. https://www.ncsl.org/elections-and-campaigns/state-laws-providing-protection-for-election-officials-and-staff

en particulier comment les techniques de vérifiabilité peuvent être mises en œuvre.

Nous examinons les besoins matériels et logiciels associés au système Be-Voting II, et étudions les méthodologies visant à évaluer, maintenir, et faire évoluer ce matériel et ce logiciel. Notre objectif ici est de démontrer la faisabilité de la mise en œuvre du concept proposé, tout en évitant d'être prescriptifs quand ce n'est pas nécessaire : dans un certain nombre de contextes, nous envisageons différentes options qui nous semblent toutes techniquement valables, et il nous semble alors préférable de trancher sur base de ce que les meilleurs fournisseurs de solution pourront proposer et s'engager à maintenir au moment où un appel d'offre sera réalisé, et où le matériel et les environnements logiciels disponibles auront encore évolué.

On constate aussi que la Belgique a été assez pionnière dans le choix de ce système, et en particulier dans le choix d'utiliser des machines de vote qui impriment un bulletin papier reprenant le choix des électeurs, et d'un dépouillement qui se réalise sur base du bulletin papier, et non sur base d'un enregistrement des votes réalisé sur la machine de vote. On peut mettre cela en perspective par rapport à l'évolution des pratiques aux États-Unis qui sont l'un des plus grands marchés de machines de vote : en 2008, plus de 34% des électeurs inscrits votaient sur des machines qui comptaient aussi les votes, et plus de 21% des électeurs votaient sur des machines qui ne produisaient pas de bulletins papier [2]. Ces nombres seront à 3% et 1.7% pour les élections de 2024. Qui plus est, en 2024, les bulletins de vote de plus de 90% des électeurs seront comptabilisés à partir de bulletins de vote papier complétés à la main ou imprimés par des machines de vote [3]. On voit là une claire reconnaissance de l'importance de l'existence d'un bulletin de vote papier et d'un dépouillement effectué à partir des bulletins de vote papier.

Indépendamment de ce bénéfice, on peut relever un certain nombre de limitations et de faiblesses dans le système de vote actuel et dans la manière dont il est mis en œuvre. Bon nombre d'entre elles peuvent être associées à des technologies et à des recommandations internationales en matière de vote électronique qui n'existaient pas quand le système a été conçu, et que l'on pourrait mettre en œuvre aujourd'hui. D'autres reflètent des difficultés structurelles dans le domaine des machines de vote, que l'on peut souhaiter remettre sur la table aujourd'hui afin de déterminer si d'autres solutions pourraient être trouvées.

2. https://verifiedvoting.org/verifier/#mode/visualization/year/2006
3. https://verifiedvoting.org/verifier/#mode/visualization/year/2024

Partie 2

État des lieux

2.1 Introduction

Nous évaluons le système de vote électronique actuellement déployé en Belgique sur base de deux sources principales :

1. Les rapports des Collèges des experts qui ont été remis après chaque élection.
2. Les recommandations internationales récentes en matière de vote électronique et la littérature académique à ce sujet.

Les rapports des Collèges nous permettront d'identifier des difficultés dans l'usage du système actuel, auxquelles on pourrait souhaiter remédier même en l'absence de progrès dans le développement des technologies de votes.

Les recommandations internationales récentes, complétées par la littérature académique, nous permettront d'identifier les technologies les plus utiles qui ont été développées au cours de quinze dernières années et ont atteint un niveau de maturité et d'intérêt tel que la recommandation de leur adoption fait aujourd'hui l'objet d'un consensus clair.

Ces sources ont été complétées par des interviews de différents acteurs de terrains.

2.2 Les rapports des Collèges des experts

La mission du Collège des experts est définie à l'Article 25 de la loi du 7 février 2014 organisant le vote électronique avec preuve papier :

> *1. [...] [L]es experts contrôlent la préparation, l'utilisation et le bon fonctionnement de l'ensemble de systèmes de vote, de décryptage, d'enregistrement et de totalisation électroniques ainsi que les procédures concernant la confection, la distribution et l'utilisation des appareils, des logiciels et des supports d'information électroniques. Le Collège d'Experts contrôle également la préparation, l'utilisation et le bon fonctionnement des matériels, logiciels et procédures de transmission et de diffusion digitale des résultats ainsi que tout logiciel utilisé dans le cadre des élections même lorsque le vote se déroule selon d'autres modalités que celles prévues par la présente loi. [...]*
> *2. Au plus tard quinze jours après la clôture des scrutins et en tout état de cause avant la validation des élections pour ce qui concerne la Chambre des représentants, les Parlements de communauté et de région et le Parlement européen, les experts remettent un rapport au ministre de l'Intérieur ainsi qu'aux assemblées législatives fédérales, régionales et communautaires.*

Les rapports visés au deuxième paragraphe sont une très bonne source d'informations concernant les qualités, difficultés et points d'amélioration concernant le système de vote. Ils décrivent, souvent en détail, les opérations de suivi et d'évaluation du logiciel de vote, les observations réalisées via des visites en coup de sonde dans des bureaux de vote et dans des bureaux principaux, et les opérations d'audit effectuées après les élections.

Nous ne reproduirons pas ici en détail les aspects descriptifs des procédures réalisées, mais nous concentrerons sur les audits et recommandations liées au système de vote électronique actuellement utilisé en Belgique (le système "Smartmatic"), issues des élections électroniques de 2012 [14, 16, 20], 2014 [17], 2018 [18, 15, 21] et 2019 [19] (nous n'incluons pas le déploiement de 2011 qui était un projet pilote qui n'a concerné que 6000 électeurs).

Par souci de clarté, les parties descriptives qui sont présentes se basent sur la procédure réalisée en 2019 [19] : nous avons pu constater qu'elle est le reflet de différentes évolutions et améliorations depuis 2012. Nous relevons ici différents aspects qui nous semblent marquants, en provenance des rapports des élections précédentes.

2.2.1 Remarques générales

2.2.1.1 L'expérience des électeurs

Une première observation est l'absence de remarque faisant état d'une difficulté d'usage du système de vote électronique : les électeurs semblent parvenir à exprimer leur vote et à déposer leur bulletin dans l'urne sans éprouver de difficulté particulière. Des "maladies d'enfance" ont été mentionnées dans les premières générations du système (lenteur de l'interface amenant des électeurs à "cliquer" plusieurs fois et à réaliser des sélections involontaires, alarmes sonores de déclenchant en trop de circonstances et amenant de la confusion, confusion quant à l'enregistrement ou non des bulletins scannés sur la machine du président, ...) mais celles-ci ont manifestement été progressivement réglées [17, Sec. 3.2.3 et 4.3.5][19, Sec. 2.1 et 4.1.1.1].

Les principaux soucis restants semblent liés aux pannes de machines (machines qui ne démarrent pas, qui n'impriment pas, etc.) sans que les rapports ne permettent de se faire une idée claire de l'impact des difficultés rencontrées. Cet impact a cependant dû rester limité, étant donné qu'il n'a jamais donné lieu à des annulations d'élections.

2.2.1.2 L'expérience des Bureaux de vote

On relève cependant un certain nombre de difficultés éprouvées dans les Bureaux de vote pour l'initialisation des machines, et en particularité :

— dans la manipulation des clés USB : gestion non conforme de l'ouverture et du stockage des enveloppes scellées, non protection de l'accès aux ports USB des machines de vote, insertion incorrecte des clés USB dans les machines, clés USB non fonctionnelles, etc. Les rapports ne permettent pas de quantifier l'importance de ces problèmes : ils sont cités, parfois sans information concernant les bureaux où ils ont été identifiés [19, Sec. 4.2.2.1], mais ils sont suffisamment présents que pour être relevés de manière répétitive dans les différents rapports – on pourra notamment noter l'incident de Saint-Josse-ten-Noode en 2018 [18, Sec. 4.3.5], qui a permis d'identifier un problème lié à un retrait précoce de clés USB, problème qui était présent dans plusieurs autres circonscriptions et qui a été résolu en 2019 [19, Sec. 4.1.1.1].

Durant les scrutins, les difficultés relevées concernent essentiellement :

— la manipulation des cartes à puce d'initialisation des votes : pannes de cartes à puce, initialisation pour des scrutins incorrects, risques de confusion entre cartes de test et cartes "normales". Ceci apparaît dans tous les rapports [16, Sec. 5.2.2.3][14, Sec. 3][17, Sec. 4.2.1.3][18, Sec.4.2.2.7] sauf dans celui de 2019 ;

— des problèmes d'impression : et notamment des bulletins qui restent bloqués dans les machines à voter [15, Sec. 6.1] [19, Sec. 4.2.2.2]

— des problèmes de lecture des bulletins papier par les urnes [19, Sec. 4.2.2.2]

Les rapports ne permettent pas de mesurer précisément l'ampleur et l'impact des difficultés rencontrées, et ceci semble inévitable au vu du processus actuel, dans lequel les experts visitent des bureaux en coup de sonde [1] : nous avons dénombré 100 visites en 2012, 88 en 2018 et 133 en 2019 pour environ 4 000 bureaux de vote équipés des machines Smartmatic – il n'y avait pas de liste des bureaux visités fournie en 2014.

En l'état, il est difficile de se rendre compte de l'importance réelle des problèmes identifiés : à l'échelle du pays, quelle proportion des machines ont éprouvé des problèmes de démarrage, quelle proportion des clés USB étaient non fonctionnelles, combien de problèmes d'urnes et d'impression ont eu lieu ? Quel était l'impact de ces problèmes : ont-ils pu être résolu en quelques minutes, ou ont-ils significativement retardé ou empêché les opérations de vote ?

2.2.1.3 Conclusions

Globalement, le système de vote électronique actuel semble avoir permis de répondre aux besoins des élections récentes : on peut constater que les élections ont pu être systématiquement validées et que les problèmes les plus importants qui ont été rencontrés lors des récentes élections ne concernaient pas le système de vote "Smartmatic". En particulier,

— Le fameux "bug des élections de 2014" concernait le système de vote Jites/Digivote, que le système Smartmatic visait à remplacer.

— Les difficultés de transmission des résultats de 2019 étaient un problème d'accès au système Martine d'encodage des résultats, lui aussi indépendant du système Smartmatic.

Néanmoins, et comme on peut s'y attendre lorsqu'on déploie 20 000 machines de vote et de l'ordre de 4 000 urnes électroniques en une journée, les rapports des Collèges des experts font état qu'un certain nombre de difficultés techniques rencontrées durant les jours d'élection. Deux conclusions nous semblent pouvoir être tirées de ceci :

1. Toute simplification du processus de gestion des bureaux de vote est bienvenue : elle limitera les risques d'erreurs et de pannes.

1. Il est évidemment impossible pour eux de faire autrement compte tenu du nombre de membres du Collège et du nombre de bureaux de vote.

2. Un processus de reporting systématique des difficultés éprouvées dans les bureaux de vote et dans les bureaux principaux, permettant une compilation simple des résultats, serait utile pour être en mesure de davantage quantifier les difficultés rencontrées.

2.2.2 Vérifications des logiciels

Un élément central du rôle du Collège des experts est la vérification des logiciels utilisés durant l'élection. La vérification des logiciels comporte deux éléments bien distincts :

1. L'inspection des logiciels destinés à être utilisés, notamment dans les machines de vote et les machines de présidents de bureaux.
2. L'examen des procédures qui permettent de s'assurer que le logiciel qui a été inspecté est réellement celui qui est utilisé durant l'élection.

2.2.2.1 Inspection des logiciels

Quelques mois avant les élections,[2] le code source du logiciel est remis au SPF Intérieur. Ce code reflète les dernières améliorations du système, en ce compris celles qui résultent des recommandations du Collège des experts et du Centre pour la Cybersécurité Belgique (CCB).

Ce code source est compilé en vue de produire la version exécutable qui sera installée sur les machines de vote et des présidents le jour de l'élection. Des copies du code source et du code compilé sont remises à différents organes, à des fins d'archivage et d'inspection.

Le code est aussi transmis à une société spécialisée en informatique, en l'occurrence PricewaterhouseCoopers qui, dans le cadre d'un accord avec Smartmatic, vérifie l'adéquation du logiciel. Cette société remet un avis, sur base duquel le SPF intérieur constate la conformité du système.[3]

Le collège des experts relève un certain nombre de difficultés concernant les logiciels. On trouve ainsi des préoccupations quant à la sécurité du processus de développement du logiciel, ainsi qu'à sa lisibilité et à sa documentation : recommandations [2019-BE.12], [2019-BE.13], [2019-BE.17], [2019-BE.32] en 2019, qui répètent les recommandations [2018-BXL.10] [2014-BE.42] et [2012-BXL.22] et font aussi écho à des remarques émises par PricewaterhouseCoopers [17, Sec. 4.1.1.4.2].

2. Le 27 février 2019 pour les élections du 26 mai 2019, par exemple [19, Sec. 4.1.1.1].
3. Cet avis a par exemple été remis le 12 avril 2019 pour les élections du 26 mai 2019 [19, Sec. 4.1.1.2], et présenté les 3 et 4 octobre pour les élections du 14 octobre 2018 [18] [15].

Le code informatique d'un système de vote est un code complexe, comptant typiquement plusieurs centaines de milliers de lignes. Qui plus est, la relecture de code est une tâche extrêmement complexe et consommatrice de temps. Par ailleurs, la correction d'un bug dans un système informatique critique est aussi une tâche extrêmement sensible si l'on veut apporter une solution correcte tout en évitant de créer de nouveaux problèmes.

Ceci est préoccupant, dans la mesure où, à différentes reprises, des systèmes qui avaient été examinés et validés dans des conditions similaires à ce qui est fait actuellement en Belgique, et qui ont ensuite fait l'objet de procédures d'évaluation par un public plus large, ont mené à l'identification de failles importantes, allant jusqu'à la perte d'agrément de systèmes. [4] [5] [6]

Ceci nous incite à porter une attention particulière à la recommandation [2019-BE.30] du Collège des experts, qui indique :

> *Le Collège d'experts recommande que chaque fichier rendu public par le pouvoir organisateur concernant les élections (résultats, code source, etc.) [. . .] [soit rendu] disponible[s] de manière permanente sur un site avec fonction de recherche.*

La publication du code source du système de vote est pratiquée en Belgique depuis toujours, et c'est une force à souligner. Nous constatons cependant qu'un certain nombre de restrictions limitent les bénéfices que l'on peut espérer de cette démarche. En particulier, la loi organisant le vote électronique avec preuve papier [42] indique en son Article 17 que le logiciel de vote est publié dans la semaine qui suit le jour des élections, sans les éléments de sécurité, et ce pour une période de 6 mois après l'élection.

Cette publication ne permet en rien de corriger des éventuelles erreurs qui seraient détectées dans ce code, d'autant plus qu'elles seront vraisemblablement identifiées bien après la validation définitive des résultats de l'élection, ce qui rend toute observation essentiellement inefficace.

Ces pratiques de publication du code, telles que décrites dans la loi organisant le vote électronique, sont bien inférieures à ce que recommande le Conseil de l'Europe, et qui seront discutées dans la prochaine section.

Par ailleurs, en l'état, les raisons motivant la non-publication des éléments de sécurité du code ne nous semblent pas claires. La publication de ces éléments permet au contraire de vérifier que la sécurité est effective, et

4. https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review
5. https://estoniaevoting.org/
6. https://www.bk.admin.ch/bk/fr/home/documentation/communiques.msg-id-74508.html

est une pratique fortement encouragée dans le domaine de la sécurité informatique, quand elle n'est pas imposée.

2.2.2.2 Authenticité du logiciel utilisé

Le logiciel de vote (machines de vote et président) est chargé, de manière centralisée au niveau du SPF Intérieur, sur des clés USB destinées à tous les bureaux de vote, et dont l'accès est protégé par des mots de passe.

Les clés USB sont transmises aux Présidents de bureau de vote dans des enveloppes scellées, avec un code unique de bureau de vote et un mot de passe. Deux clés USB sont insérées dans l'urne électronique, à la suite de quoi l'ordinateur du Président est démarré, et les code de bureau de vote et le mot de passe sont introduits. Après démarrage, les clés USB sont retirées de l'urne et introduites dans les machines de vote, pour démarrer celles-ci. Lorsque les machines de vote ont démarré, les clés USB sont à nouveau retirées, et réintroduites dans l'urne [7].

Les principales difficultés de cette procédure sont de s'assurer que :

1. Les machines de vote et de président de bureau sont démarrées avec des clés USB qui contiennent le logiciel qui a été déclaré conforme par le SPF Intérieur.
2. Les machines de vote et de président de bureau n'ont pas été modifiées de manière à pouvoir ignorer tout ou partie du logiciel présent sur les clés USB et à fonctionner sur base d'un logiciel corrompu à la place.

Des difficultés liées au premier point sont relevées par le Collège des experts, qui recommande notamment que les clefs USB et les mots de passe soient délivrés aux présidents de bureau de vote via des canaux différents [2019-BE.24], ce qui éviterait qu'une personne assurant l'acheminement des clés USB soit en mesure, en contournant la sécurité associée à l'enveloppe scellée, d'accéder à un ensemble de données secrètes stockées sur la clé USB.

On observe aussi que, en certaines occurrences, le Collège des experts a pu procéder à une inspection de clés USB après la clôture des élections, afin de vérifier que le logiciel correct s'y retrouvait [17, Sec. 4.3.4]. Ceci n'est cependant pas rapporté systématiquement.

Nous n'avons pas trouvé d'information liées au risque discuté dans notre second point (conformité des machines) dans les rapports des experts. Les modifications des machines, qui permettrait éventuellement de les faire fonctionner de manière différente de ce que le logiciel présent sur les clés USB

7. https://elections.fgov.be/sites/default/files/inline-files/President%20Manual-FR-V1.0.pdf

prescrit, est à la fois compliqué et facilité par différentes spécificités du système belge et de sa maintenance.

Une force importante du système belge est l'absence de support de stockage non-volatile (disque dur, ...) contenant le logiciel de vote, qui évite qu'une personne mal intentionnée ayant accès à une machine de vote puisse directement modifier le logiciel de vote qui serait présent sur la machine.

Un point d'attention est celui du stockage des machines de vote, effectué selon des conditions variables selon les communes. Une faille des mécanismes de contrôle d'accès aux machines pourrait permettre à des acteurs de modifier le boot-loader, qui contrôle le démarrage des machines, afin de prendre contrôle des machines, voire d'effectuer des modifications plus importantes qui ajouteraient une mémoire non-volatile et un système de vote complet, qui se comporterait de manière visible comme le système normal, mais chercherait à modifier des votes. Des démonstrations de telles attaques ont déjà été réalisées, parfois avec un fort impact judiciaire et médiatique [69].

Nous retenons ici la difficulté de garantir que du logiciel authentique est utilisé, qui augmente d'autant l'importance des bulletins de vote papier et de la vérification de ceux-ci.

2.2.3 Audits post-électoraux

Les Collèges des experts rassemblent un certain nombre de données durant et juste après les élections afin de réaliser des audits. On relève notamment que :

— Dans chaque bureau de vote contrôlé, des votes de test ont été émis par les experts du collège, à des fins de contrôle et d'analyse dans un environnement propre au Collège [17, 4.3.1.2] [19, Sec. 4.2.1.1].

— Le Collège a réalisé une retotalisation complète des votes contenus sur les clés USB utilisées dans les bureaux de vote, afin de comparer les résultats officiels avec ceux que le Collège a obtenu via ses propres logiciels [19, Sec. 4.3.1].

— Le collège a réalisé en 2014 le dépouillement manuel des urnes de 2 bureaux de votes choisis au hasard, afin de comparer le résultat à celui du dépouillement automatisé [17, Sec. 4.3.2].

De la même manière certains audits sont réalisés dans des Bureaux principaux. L'article 80 de l'ordonnance du 20 juillet 2023 portant sur le Nouveau Code électoral communal bruxellois reprend ainsi [8] :

8. https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=23-08-14&numac=2023044127

Le président du bureau principal peut également décider d'opérer un recomptage manuel des chiffres électoraux des votes de listes par coups de sonde. Il procède à un tel recomptage au minimum pour un bureau de vote par commune.

Ces audits mettent parfois à jour des petites disparités, notamment entre le nombre de bulletins effectivement présents dans les urnes et le nombre de bulletins effectivement enregistrés sur les supports électroniques.

La réalisation de ces audits est extrêmement utile et importante. On a notamment vu précédemment à quel point les bulletins papier sont importants comme protection contre un logiciel défectueux ou modifié, et ces tests sont aujourd'hui le seul moyen dont nous disposons pour détecter ce type de problème.

Il est cependant à nouveau difficile de tirer des conclusions claires de ces audits, bien qu'ils semblent largement positifs. En effet, sur base des audits réalisés, il n'est pas possible de dériver une borne utile sur la probabilité qu'un résultat incorrect soit validé malgré les audits. Cette impossibilité est notamment liée à des aspects du système actuel qui ne permettent pas de réaliser des audits avec une efficacité raisonnable.

L'amélioration des procédures de vérification et d'audit des résultats de l'élection est l'objet des techniques de vérifiabilité qui seront développées dans le chapitre 3 de la présente étude.

2.3 Les recommandations du Conseil de l'Europe relatives au vote électronique

La principale source en matière de recommandations internationales s'appliquant au vote électronique est la Recommandation CM/Rec(2017)5 du Comité des Ministres aux États membres sur les normes relatives au vote électronique, adoptée par le Comité des Ministres le 14 juin 2017 [24], et en particulier son Annexe B qui donne des lignes directrices pour la mise en œuvre de ces recommandations [23]. Le Conseil de l'Europe reste la seule organisation à avoir défini des normes intergouvernementales dans le domaine du vote électronique en Europe.

Nous nous référerons aussi, en particulier dans la section 4.3, aux documents suivants :

— "Securing the Vote : Protecting American Democracy" publié en 2018 par les "National Academies of Sciences, Engineering, and Medicine" des États-Unis [47]. Ce document offre parfois une approche différente

sur des questions par ailleurs abordées dans les Recommandations du Conseil de l'Europe.

— les "Voluntary Voting System Guidelines" (VVSG) publiées en 2022 par la "United States Election Assistance Commission" [64], qui offrent des recommandations pratiques concernant la conception, le déploiement et la maintenance de systèmes de vote électronique. Dans certains états américains, la conformité aux VVSG est obligatoire.

— L'Ordonnance 161.116 de la Chancellerie fédérale suisse sur le vote électronique de 2022 [11] qui est aujourd'hui à l'avant-garde en matière d'exigences de transparence dans le vote électronique.

D'autres documents, comme le "Compendium on Cyber Security of Election Technology" du "NIS Cooperation Group" européen sont certainement utiles dans le contexte d'élections mais ciblent moins directement les systèmes de vote électronique.

Le système de vote électronique en place en Belgique a été conçu en fonction des Recommandations du Conseil de l'Europe dans leur version de 2004 et remplit encore bon nombre des Recommandations de la version de 2017. Nous citons ici les Recommandations par rapport auxquelles le système de vote électronique belge actuel nous semble offrir des marges importantes d'amélioration.

2.3.1 Accessibilité

> *2. Le système de vote électronique sera, dans la mesure du possible, conçu de manière à permettre aux personnes handicapées et aux personnes ayant des besoins spéciaux de voter de façon autonome.*

L'usage de machines de vote présente le grand avantage, en particulier en Belgique où les bulletins de vote sont particulièrement grands et complexes à remplir, de faciliter le remplissage des bulletins tout en empêchant de produire involontairement un bulletin de vote invalide.

Le système de vote électronique belge ne met cependant pas en œuvre un certain nombre de technologies d'assistance qui permettraient à un plus grand nombre de personnes de voter de manière autonome. À ce jour, seul un pilote a été organisé en 2019 à Alost et Malines, avec l'installation de technologies visant à faciliter le vote des électeurs malvoyants ou aveugles [19, Sec. 2.1].

Nous voudrions néanmoins relever ici un bénéfice important du système de vote électronique actuellement utilisé en Belgique, qui est de faciliter

la complétion des bulletins de vote pour un grand nombre de personnes. La dimension des bulletins de vote papier en Belgique, le grand nombre de candidats listés, ainsi que les règles de complétion des bulletins qui interdisent notamment le panachage entre listes, font qu'un nombre significatif de bulletins de vote remplis à la main sont rendus involontairement invalides par les électeurs. Ceci a notamment été étudié par Jean-Benoit Pilet et ses co-auteurs [53] qui ont obtenu un accès aux bulletins de vote remplis à la main par les électeurs lors des élections communales wallonnes de 2018 : il a ainsi été observé que, en moyenne, 65.4% des bulletins rapportés comme "blancs ou nuls" dans les résultats des élections sont des bulletins nuls et que, parmi ceux-ci, en moyenne, 43% sont identifiés comme non-intentionnellement nuls, soit 28% des bulletins "blanc ou nuls". Sur base de l'observation d'une moyenne de 6.7% des bulletins "blancs ou nuls" parmi tous les bulletins de vote, on arrive ainsi à 1.9% de l'ensemble des bulletins qui seraient involontairement nuls dans du vote papier. Cette proportion est très largement supérieure à la marge habituelle des élections en Belgique, qui mesure la proportion de votes qu'il est nécessaire de modifier pour changer les résultats de l'élection – nous détaillons de telles marges en section 3.2.3. Le vote électronique permet d'éviter à ces 1.9% de votes exprimés d'être rendus involontairement invalides par les électeurs.

2.3.2 Vérifiabilité

> *10. L'intention de l'électeur ne sera pas affectée par le système de vote et sera à l'abri de toute influence indue.*
>
> *15. L'électeur devra pouvoir vérifier que son intention est représentée avec exactitude dans le suffrage exprimé et que le vote scellé est parvenu à l'urne électronique sans avoir été modifié. Toute influence indue ayant modifié le suffrage pourra être détecté.*
>
> *17. Le système de vote électronique produira des preuves tangibles que chaque suffrage authentique est inclus correctement dans les résultats électoraux respectifs. Les éléments de preuve devraient pouvoir être vérifiés par des moyens indépendants du système de vote électronique.*

L'électeur peut aujourd'hui vérifier que son intention est représentée avec exactitude sur le bulletin papier, mais il lui est difficile de s'assurer que l'enregistrement électronique reflète son intention de vote :

— Les possibilités de vérification du QR code imprimé sur le bulletin de

vote sont limitées à l'usage du même logiciel qui a produit le code QR, et qui est donc potentiellement corrompu de la même manière et ne constitue donc pas un moyen de vérification indépendant.

— L'électeur n'a aucun moyen de vérifier que le scanner de l'urne interprète son vote correctement, et que l'enregistrement électronique de son vote est correct.

— Les audits réalisés actuellement ne permettent pas d'établir la mesure dans laquelle l'intention des électeurs est réellement prise en compte, comme mentionné dans la section 2.2.3.

Les lignes directrices de mise en œuvre des Recommandations suggèrent ici d'avoir recours aux techniques de vérifiabilité individuelles et universelles, ainsi qu'à des techniques statistiquement significatives d'audit des bulletins papier.

Un aspect central de ces techniques est qu'elles permettent des vérifications qui sont indépendantes du système de vote électronique lui-même comme requis dans la Recommandation 17.

2.3.2.1 À propos des preuves papier

Le choix d'employer des machines de vote plutôt que des bulletins papier marqués à la main est certainement une question controversée, tant en Belgique que dans le reste du monde.

En particulier, si la nécessité de disposer de bulletin papiers fait consensus dans la littérature, on a assisté à une importante controverse aux États-Unis, avec la publication d'une série d'études et de contre-études visant à démontrer la possibilité ou l'impossibilité pratique de détecter des machines de vote corrompues grâce aux bulletins papier qu'elles impriment [60, 68, 5, 40], avec d'un côté des personnes soutenant que la seule option viable est d'imposer aux électeurs (au moins tous ceux qui le peuvent) de compléter leurs bulletins de vote à la main, et de l'autre des personnes argumentant que l'usage de machines de vote offre de sérieux bénéfices, notamment en évitant aux électeurs de commettre des erreurs dans le respect des règles de complétion des bulletins de vote.

Cette controverse a été en bonne partie soutenue par des études contradictoires sur la capacité ou l'incapacité pratique d'un électeur à s'apercevoir que sa machine de vote imprime un bulletin reprenant une intention de vote différente de celle qu'il a exprimée. Cette capacité dépend naturellement des instructions données aux électeurs (rappel de vérifier le bulletin papier), du format du bulletin de vote (nombre de questions sur lesquelles on vote,

nombre de candidats que l'on peut sélectionner) et de la lisibilité du bulletin papier produit.

Il est évident que, si l'électeur ne relit pas le bulletin papier produit par sa machine de vote, ou si l'électeur n'est pas assez attentif pour détecter des erreurs, alors les garanties de vérifiabilité reposant sur ce bulletin papier sont largement affaiblies (sans disparaître pour autant : le papier permet toujours de détecter des erreurs dans le processus de dépouillement par exemple).

Cette relecture est d'autant plus importante qu'un très petit nombre d'erreurs rapportées par les électeurs ne permettra probablement pas d'identifier des machines corrompues quand elles trichent de manière aléatoire : une ou deux erreurs rapportées par des électeurs, et qui n'apparaissent plus lorsque ces électeurs votent à nouveau, risquent fort d'être attribuées à des erreurs des électeurs lors de l'expression de leur premier vote plutôt que comme un fonctionnement anormal de la machine de vote.

Ce débat nous amène à trois observations :

1. Il est important d'encourager les électeurs à relire leur bulletin papier et à rapporter toute erreur dans le bulletin qu'ils attribueraient à leur machine de vote. Ceci permettra de guider des audits.
2. Il est important de faciliter cette vérification autant que possible en pratique. L'impression actuelle sur un papier au format ticket de caisse ne semble pas recommandée dans ce contexte.
3. Les bulletins de vote belge ont une forme très différente des bulletins de vote américains, qui contiennent parfois plusieurs dizaines de questions. Si on peut imaginer qu'un électeur qui a sélectionné une vingtaine de candidats dans une liste ne s'apercevra peut-être pas que la machine a ajouté ou retiré un candidat à cette sélection, il semble plus douteux que l'électeur ne s'apercevra pas de manipulations plus importantes, comme une machine de vote qui imprimerait un vote pour une liste différente de celle sélectionnée par l'électeur. Il semble donc permis de faire l'hypothèse que les électeurs belges seront dans une meilleure situation que les électeurs américains pour détecter des erreurs – cette hypothèse pourra être vérifiée à l'aide de tests en conditions réelles.

2.3.3 Confidentialité du vote

19. Le vote électronique sera organisé de manière à garantir à toutes les étapes de la procédure que le secret du scrutin est respecté.

> *26. La procédure de vote électronique, en particulier au moment du décompte des voix, sera organisée de sorte qu'il ne soit pas possible d'établir un lien entre le suffrage non scellé et l'électeur. Les suffrages sont, et restent, anonymes.*

Le scanning des bulletins au moment du dépôt dans l'urne peut soulever des inquiétudes en matière de confidentialité des votes. Alors qu'une urne classique permet un mélange des bulletins avant ouverture, on voit ici que les bulletins sont enregistrés sur la machine du Président dans l'ordre de leur dépôt dans l'urne. Une personne qui prendrait note de l'identité des électeurs et de l'ordre dans lequel ils déposent leurs bulletins de vote dans l'urne pourrait ainsi trouver quel vote (chiffré) enregistré appartient à quel électeur. Le déchiffrement des votes est aujourd'hui possible à l'aide d'une seule clé. Cette procédure laisse de la marge d'amélioration, relevée aussi par le Collège des experts dans ses recommandations de ne pas procéder au scanning des bulletins au moment du dépôt des bulletins dans les urnes, mais après la clôture des votes, notamment à des fins d'amélioration de la préservation du secret des votes [16, 2012-Bxl.6] [17, Sec. 6.1].

2.3.4 Transparence

> 31. Les États membres feront preuve de transparence pour tous les aspects du vote électronique.

Cet article vient ici renforcer les demandes de transparence émises par le Collège des experts et relevées en section 2.2.2.1, concernant la publication des logiciels de vote. Ces demandes vont en effet dans la même direction que le Conseil de l'Europe dans ses lignes directrices pour la mise en œuvre de l'Article 31 :

> *b. L'accès du public aux différents éléments du système de vote électronique et aux informations sur le sujet, en particulier les documents, le code source et les accords de confidentialité, devrait être communiqué bien avant le début de la période électorale.*

2.3.5 Reporting

> *39. Le système de vote électronique pourra faire l'objet d'un audit. Le système d'audit sera ouvert et complet, et signalera effectivement les menaces et les problèmes potentiels.*

On a constaté plus haut que les données concernant les menaces et problèmes rencontrés dans le déploiement du système de vote et identifiées par les Collèges des experts proviennent des coups de sonde réalisés par ceux-ci dans les Bureaux de vote et Bureaux principaux. Ces données ne sont pas nourries par des informations d'audit qui seraient systématiquement remontées au départ de chaque bureau de vote ou bureau de canton, sous des formats qui permettraient l'établissement aisé de statistiques concernant ces menaces, problèmes et leur impact.

Les lignes directrices pour la mise en œuvre de l'Article 39 précisent notamment :

> *a. Il conviendrait d'enregistrer dans le système d'audit les dates et heures et les événements et actions, notamment : [...]*
>
> — *toute attaque contre le système de vote électronique et ses infrastructures de communication ;*
>
> — *les pannes, dysfonctionnements et autres menaces contre le système.*
>
> *Les outils automatisés et les procédures du système devraient permettre une procédure rapide et précise d'analyse des données et d'élaboration des rapports y relatifs, afin que les mesures correctives puissent être prises sans tarder.*

2.4 Gestion du matériel de vote

Avant de synthétiser les points soulevés précédemment, nous abordons deux aspects repris dans les objectifs de la présente étude, mais largement indépendants des préoccupations du Collège des experts et du Conseil de l'Europe : les questions de difficulté de maintenance du logiciel et du matériel du système de vote électronique, qui sont elles-mêmes liées, dans certains cas, à l'usage de matériel spécifique au système, plus difficile à entretenir.

2.4.1 Difficultés de maintenance du logiciel et du matériel

La décision d'employer des machines de vote représente un investissement important, et on observe que la durée de déploiement pratique d'une machine tourne souvent autour de 15 ans. Il s'agit là d'une très longue durée pour du matériel informatique : il est difficile d'obtenir une garantie de plus de 5

ans lors de l'achat de laptops professionnels. En termes de système d'exploitation, les distributions linux les plus généreuses (y compris Ubuntu, qui est déployé dans le système Smartmatic) offrent aujourd'hui un support étendu, limité aux failles de sécurité, de 10 ans.[9] Cette même limite s'applique aux systèmes d'exploitation "serveur" chez Microsoft Windows.[10] Les versions destinées aux machines personnelles, tant pour Windows que pour MacOS, fonctionnent selon un rythme de roulement plus serré – habituellement 3 ans.[11]

Ceci soulève des difficultés importantes. Étant donné la durée de support limitée des systèmes d'exploitation, il est nécessaire, si on souhaite disposer d'un système à jour du point de vue de la sécurité, d'installer sur les machines de vote de nouvelles versions des systèmes d'exploitation. Cependant, les nouvelles versions des systèmes d'exploitation viennent régulièrement avec de nouvelles exigences au niveau du matériel (exigence de davantage de mémoire, etc.), qui peuvent devenir incompatible avec le matériel présent sur les machines de vote.

Les mêmes difficultés peuvent se présenter au niveau des périphériques. Faute de disponibilité de pièces de rechange, il est difficile de réparer des appareils après quelques années. Quand un périphérique peu coûteux (imprimante, ...) est en panne, son remplacement sera alors la solution naturelle. Mais, si la machine de vote est restée limitée à un système d'exploitation ancien, ce remplacement pourra devenir difficile, faute de support pour les périphériques récents par le système d'exploitation ancien.

Ainsi, les machines de vote déployées pour la première fois en 2012 sont aujourd'hui extrêmement difficiles à réparer et à mettre à jour, vu les évolutions qui ont eu lieu depuis lors dans les exigences des systèmes d'exploitation.

Ceci veut dire que ces machines vont fonctionner avec des logiciels dans lesquelles des failles de sécurité sont connues, souvent publiques, et restent non corrigées. Les machines peuvent dès lors exhiber des comportements essentiellement arbitraires, même si elles sont installées avec du logiciel authentique. Les risques sont heureusement limités par la sécurité physique des machines, qui ne sont jamais connectées à un réseau, ne disposent pas de mémoire non-volatile, et ne sont pas en libre accès, que ce soit durant le stockage entre les élections, ou durant les élections grâce aux boîtiers qui empêchent l'accès à la plupart des points d'entrée de la machine. On reste

9. https://ubuntu.com/security/esm
10. https://learn.microsoft.com/en-us/lifecycle/faq/windows
11. https://endoflife.date/

cependant loin des pratiques recommandées et bien comprises en matière de gestion des risques informatiques.

2.4.2 Usage de matériel spécifique

Lié au point précédent, le système actuel est en partie basé sur du matériel spécifique, en particulier au niveau des urnes qui scannent les bulletins de vote, mais aussi au niveau des boîtiers de vote rigides dans lesquels les composants (standard) du système sont assemblés, qui ne facilitent pas l'échange d'un composant par un autre.

L'usage de matériel spécifique tend naturellement à augmenter le coût du système et complique ses réparations. Il est aussi susceptible, plus que du matériel standard, de faire des "maladies d'enfance". Nous avons ainsi relevé plus haut que les rapports du Collège des experts font état de diverses difficultés, modifications et améliorations du dispositif de scanning, d'ouverture et de fermeture des urnes, afin de résoudre des problèmes identifiés lors de premiers déploiements.

Les machines de vote intégrées dans des boîtiers fermés ont certainement des avantages de simplicité de déploiement : il n'y a pas de câbles à raccorder entre la machine, l'imprimante et le lecteur de cartes au moment de l'installation des bureaux de vote, câbles qui risquent toujours de se perdre ou d'être arrachés par les électeurs. Néanmoins, ces boîtiers rigides sont aussi susceptibles de compliquer ou d'augmenter les opérations de mise à niveau du matériel intégré dans le système : il est plus simple de remplacer une imprimante externe par une autre imprimante qui aurait éventuellement une taille un peu différente, qu'un composé intégré à un boîtier, qui doit venir se positionner exactement en face d'ouvertures prévues. En pratique, cela implique que, au lieu de prévoir des imprimantes ou des scanners génériques de stock, il faut prévoir d'acheter un stock supplémentaire de machines de votes.

2.5 Bilan de l'évaluation du système de vote actuel

Globalement, le système de vote électronique actuel semble avoir permis de répondre aux besoins des élections récentes : les élections ont pu être validées, et les difficultés les plus importantes qui ont pu être identifiées lors des élections des 10 dernières années ne provenaient pas du système de vote

électronique Smartmatic.

Néanmoins, on peut relever un certain nombre de limitations et de faiblesses dans le système de vote électronique actuel et dans la manière dont il est mis en œuvre. Bon nombre d'entre elles peuvent être associées à des technologies et à des recommandations internationales en matière de vote électronique qui n'existaient pas quand le système a été conçu et qui existent aujourd'hui. D'autres reflètent des difficultés structurelles dans le domaine des machines de vote, que l'on peut souhaiter remettre sur la table aujourd'hui afin de déterminer si d'autres solutions pourraient être trouvées.

Nous relevons ainsi 5 axes :

1. Gestion du matériel et du logiciel ;
2. Accessibilité du système de vote ;
3. Transparence et sécurité du logiciel ;
4. Vérifiabilité et audits de l'élection ;
5. Reporting sur le fonctionnement du système durant les élections.

2.5.1 Gestion du matériel et du logiciel

On cherchera ici à :

(G1) Simplifier le déploiement des bureaux de vote, afin de répondre aux difficultés mentionnées en section 2.2.1.2.

(G2) Se baser sur du matériel facile à réparer, remplacer et faire évoluer, compte tenu de la durée de vie généralement observée pour un système de vote, comme discuté en sections 2.4.1 et 2.4.2.

(G3) Choisir du matériel permettant de faire fonctionner des systèmes d'exploitation et du logiciel conforme aux normes de sécurité durant la durée de vie du système, comme discuté en section 2.4.1.

(G4) Faciliter la vérification de la conformité du déploiement des logiciels de vote, comme discuté en section 2.2.2.2.

2.5.2 Accessibilité

On cherchera ici à :

(G5) Aller plus loin qu'actuellement en matière d'accessibilité du système de vote pour des personnes malvoyantes ou des personnes dont la dextérité ne permet pas de sélectionner facilement des candidats sur un écran, comme discuté en section 2.3.1.

2.5.3 Transparence

On cherchera ici à :

(G6) Proposer une méthodologie de publicité autour des éléments techniques du système de vote électronique, permettant d'améliorer à la fois la transparence et la qualité du système, comme discuté dans les sections 2.2.2.1 et 2.3.4.

2.5.4 Vérifiabilité

On cherchera ici à :

(G7) Permettre aux électeurs de vérifier que leur intention de vote est correctement enregistrée et que leur vote est bien pris en compte, sans avoir été modifié, lors des opérations de dépouillement, comme discuté dans les sections 2.2.3 et 2.3.2.

(G8) Permettre que ces vérifications puissent s'opérer sans compromettre le secret des votes – le processus proposé veillera notamment à lever les préoccupations soulevées en section 2.3.3.

2.5.5 Reporting

On cherchera ici à :

(G9) Mettre en place des mécanismes de reporting simples et permettant une compilation efficace des données reçues, afin d'avoir une mesure claire du nombre d'incidents et de leurs conséquences, comme discuté dans les sections 2.2.1.2 et 2.3.5.

Partie 3
Avancées technologiques

3.1 Introduction

Le paysage des technologies de votes a considérablement évolué depuis l'étude BeVoting de 2007 à la source du système de vote électronique actuellement utilisé en Belgique [30].

L'axe principal d'évolution des technologies de vote porte sur le développement et l'amélioration des techniques permettant de vérifier que le résultat des élections qui est annoncé est effectivement correct. Ces évolutions technologiques répondent à des besoins clairs, et leur adoption fait partie des recommandations internationales en la matière.

Ces technologies de vérifiabilité suivent deux axes largement complémentaires, que nous abordons dans les sections qui suivent.

1. Les audits limitant le risque, ou *risk limiting audits* – RLAs, qui consistent en une vérification statistique que le résultat annoncé d'une élection est conforme à l'ensemble des bulletins de vote papier produits par les machines de vote, inspectés par les électeurs et qui sont présents dans les urnes.
2. La vérifiabilité de bout en bout, ou *end-to-end verifiability*, qui inclut un ensemble de techniques, généralement basées sur de la cryptographie, qui permettent de vérifier que les bulletins de vote produits par le système de vote n'ont pas été modifiés et ont été correctement comptabilisés lors du dépouillement.

L'un des attraits du déploiement d'un système de vote électronique est d'éviter de devoir dépouiller l'ensemble des bulletins de vote produits par les

électeurs, grâce à un enregistrement et à une totalisation électronique des bulletins de vote.

Si le dépouillement manuel amène ses propres risques liés aux erreurs humaines et à la manipulation des bulletins de vote par un nombre important de personnes, le dépouillement électronique pose des risques, lui aussi. On peut par exemple s'interroger sur les aspects suivants du système actuellement déployé en Belgique :

1. Les bulletins de vote papier contiennent deux parties : un résumé des choix lisible par l'électeur, et un code QR qui encode ces choix et est scanné pour l'encodage électronique. Une machine de vote qui aurait été corrompue pourrait imprimer un résumé lisible correct pour l'électeur, mais produire un QR code encodant des choix différents. L'électeur n'est pas en mesure de vérifier ce code QR de manière indépendante, mais c'est lui qui est scanné pour la comptabilisation du bulletin de vote.
2. Même si le code QR est correct, la machine du président du bureau de vote pourrait, de la même manière, être corrompue, et enregistrer des votes différents de ceux qui sont scannés.

Bien évidemment, des mesures sont prises pour répondre à ces interrogations : les machines sont testées, les électeurs peuvent vérifier, à l'aide d'une autre machine, que le code QR imprimé sur leur bulletin reflète bien leur intention de vote, et une architecture et un mode de déploiement sécurisé des machines visent à garantir que ces machines ne sont pas corrompues.

Il n'en reste pas moins que ces mécanismes de contrôle sont essentiellement internes au système, là où le Conseil de l'Europe recommande des moyens de contrôle indépendants pour éviter qu'un acteur interne ne puisse biaiser le système et les mécanismes de vérification. Nous développons ici une proposition d'intégration dans les élections belges des deux plus importantes techniques qui ont été développées à cet effet, et qui sont déjà déployées dans d'autres pays.

3.1.1 Audit limitant le risque

Tant le Conseil de l'Europe que les National Academies américaines (voir discussions plus bas) estiment qu'il est central de mettre en œuvre une procédure d'audit indépendante du système de vote électronique lui-même, basée sur les bulletins de vote papier que les électeurs ont pu inspecter. C'est ce qu'un risk limiting audit fournit : par l'inspection d'un échantillon statistiquement significatif des bulletins papier, un risk limiting audit offre une

garantie que le résultat de l'élection annoncé est bien en accord avec l'ensemble des bulletins papier disponibles.

Le fait de se baser sur le papier donne une grande force au risk limiting audit : on part d'un objet tangible que l'électeur a pu inspecter de manière à s'assurer qu'il représente bien son intention de vote – il n'y pas de place ici pour qu'une machine triche sans que cela ne puisse être détecté. [1]

Cette force est aussi la source de la principale faiblesse de ces audits : la qualité de l'audit repose tout entière sur la qualité du suivi des bulletins de vote papier : si l'on réalise un audit à partir de bulletins papier qui ne sont pas authentiques, le résultat de l'audit n'aura bien sûr force probante. Pire, un tel audit pourrait même mener à invalider un résultat correct si la falsification des bulletins de vote a eu lieu après le dépouillement.

Or, il est souvent difficile de garantir la sécurité du suivi des bulletins papier. En Belgique, les bulletins de vote sont transportés vers des bureaux de dépouillement puis vers des bureaux principaux de canton. Ces transports se font habituellement dans des véhicules privés et les urnes sont normalement scellées mais, comme les ordinateurs, les scellés ne sont pas inviolables. Les urnes sont aussi stockées, avant audit, dans des locaux fermés. À nouveau, il est difficile de garantir que des accès non-autorisés à ces locaux n'ont pas eu lieu. [2]

3.1.2 Vérifiabilité de bout en bout

C'est ici qu'intervient le second axe de développement technologique en matière de vérifiabilité, la vérifiabilité de bout en bout, elle aussi recommandée tant par le Conseil de l'Europe que par les National Academies américaines.

L'une des formes courantes de cette approche de vérifiabilité consiste à demander à chaque machine de vote de produire, en même temps que le bulletin de vote papier, un numéro de suivi qui constitue une sorte d'empreinte

1. Ceci a pu être expérimenté récemment : à la suite d'une erreur de configuration des machines de vote qui est passée inaperçue lors des différents tests, les machines à voter utilisées lors des élections de novembre 2023 dans Northampton County, PA, USA, imprimaient, pour certains choix de votes, des bulletins de vote incorrects. Ces erreurs ont été détectées par les électeurs en quelques minutes après l'ouverture des opérations de vote. Un rapport détaillé décrivant ce problème est proposé ici : https://securiosa.com/posts/northampton_problems_2023.html.

2. Une page web documentant différentes manières de contourner bon nombre de mesures classiques de sécurité physique utilisée dans le cadre des élections est par exemple proposée par Paul Burke à l'adresse : http://www.votewell.net/locks.html.

digitale de ce bulletin de vote. Ce numéro de suivi est conservé par l'électeur, pour vérifications futures.

Concrètement, ce numéro de suivi se présente comme une séquence de lettres et de chiffres d'apparence aléatoire et/ou comme un QR code : basé sur des mécanismes cryptographiques de chiffrement, le fait de disposer du numéro de suivi d'un bulletin ne permet en rien de déterminer le contenu du bulletin. En particulier, ce numéro de suivi ne permettrait pas à un électeur d'avoir une preuve du contenu de son bulletin de vote qui pourrait être utilisée pour vendre son vote, ou pour répondre à des pressions qui seraient opérées sur lui. Cependant, les mécanismes cryptographiques garantissent que le numéro de suivi présente des propriétés similaires à celles qu'on attend d'empreintes digitales : il n'est techniquement pas réalisable de produire deux bulletins de vote qui présentent le même numéro de suivi. En cela, ce numéro de suivi accomplit bien plus qu'un numéro de suivi associé à un colis postal, par exemple, qui ne garantit en rien le contenu du colis. Le numéro de suivi garantit ainsi à l'électeur que son bulletin de vote est enregistré et intact, mais ne permet pas à l'électeur de montrer pour qui il a voté à une tierce personne.

L'existence de ces numéros de suivi rend alors possible de publier un rapport d'élection qui reprend la liste des numéros de suivi de tous les bulletins inclus dans le dépouillement électronique de l'élection, et ce sans révéler le contenu des bulletins de vote. Cette liste peut être consultée par tous les électeurs qui le souhaitent, leur permettant ainsi de s'assurer que leur bulletin de vote a été correctement dépouillé. D'autres techniques cryptographiques permettent par ailleurs de vérifier que le résultat annoncé de l'élection reflète exactement l'ensemble des numéros de suivi publiés – et ce sans jamais révéler la moindre information sur le contenu des bulletins associés à ces numéros de suivi.

Ces techniques de vérifiabilité étant essentiellement digitales, elles ne couvrent que de manière limitée la question de savoir si le numéro de suivi fourni à un électeur reflète bien son intention de vote. Comme dans le cas du QR code mentionné plus haut, la machine de vote pourrait produire un numéro de suivi correspondant à une autre intention de vote et, comme ce numéro de suivi doit être conçu pour ne pas révéler le contenu du vote, l'électeur n'a pas de moyen direct de s'en apercevoir – des techniques existent pour permettre aux électeurs de détecter ce type de fraude, mais elles sont plus exigeantes à déployer de manière efficace, et seront discutées plus bas.

On voit cependant apparaître ici la complémentarité entre le risk limiting audit et la vérifiabilité de bout en bout : le risk limiting audit permet de s'assurer qu'un ensemble de bulletins papier que les électeurs ont pu ins-

pecter sont consistants avec le résultat de l'élection, sous l'hypothèse que les bulletins utilisés dans l'audit sont bien ceux que les électeurs ont inspectés. La vérification de bout en bout permet de s'assurer que les bulletins de vote digitaux générés au moment du vote, mais dont le contenu n'a pas pu être inspecté par les électeurs directement, ont bien été pris en compte dans le dépouillement menant au résultat de l'élection.

Aucune des deux approches n'est à ce jour infaillible en pratique. Cependant, produire un résultat d'élection erroné sans que cela soit détecté demande, quand ces approches sont déployées, d'être capable de tricher *de manière cohérente* à la fois dans le suivi des bulletins papier et dans la génération des bulletins de vote électroniques, de manière que les deux triches mènent au même faux résultat, en tous cas avec une très grande probabilité. Ceci est sensiblement plus difficile que de tricher sur un seul de ces deux axes, électronique ou papier.

Ces deux approches renforcent certainement aussi la sécurité des systèmes actuels. Dans le système de vote électronique employé actuellement en Belgique, faute d'audit statistiquement significatif des bulletins papier, il sera malaisé de détecter un système informatique corrompu : on se repose largement sur la confiance que l'on a dans la sécurité des procédures de déploiement du système. Et dans le système de vote papier, faute de possibilité de suivi des bulletins de bout en bout, il sera fort malaisé de détecter une substitution de bulletins de vote dans une urne, durant un transport ou un dépouillement par exemple : on se repose largement sur la confiance que l'on a dans la sécurité des procédures de suivi des bulletins de vote. Nous ne suggérons évidemment pas que cette confiance est mal placée, dans un cas comme dans l'autre. Mais, au vu des enjeux, il semble approprié de mettre en œuvre des mécanismes permettant de vérifier que cette confiance est effectivement bien placée.

3.2 Audit limitant le risque

3.2.1 Introduction

3.2.1.1 Qu'est-ce qu'un audit limitant le risque ?

Un audit limitant le risque, aussi appelé "*risk-limiting audit*" ou RLA en anglais, est une procédure d'audit visant à garantir que le résultat annoncé d'une élection est correct. Toute procédure de décompte d'un grand nombre de bulletins de vote est complexe, et des erreurs peuvent se produire, que ce

soit dans un processus de comptage, dans un processus de scanning, ou dans un processus d'encodage de totaux dans un ordinateur. Les logiciels utilisés peuvent contenir des erreurs, et une infrastructure informatique peut être compromise par des acteurs malveillants.

La mise en œuvre d'un RLA répond ainsi aux recommandations du Conseil de l'Europe. Les "Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique" indiquent en effet en leur article 15.b [23] :

> Il conviendrait de procéder à un décompte obligatoire des voix à partir de ce deuxième support [c'est-à-dire le support papier] dans un nombre statistiquement significatif de bureaux de vote sélectionnés de façon aléatoire, notamment pour les machines à voter et les dispositifs de lecture optique des bulletins de vote.
>
> Les critères tels que le pourcentage de votes concernés ou le nombre de bureaux de vote dans lesquels ce décompte aura lieu, leur désignation, etc. seront établis au niveau national. Ils devraient veiller à ce que le but général d'assurer des élections libres soit atteint.

En offrant une garantie statistique établie de manière rigoureuse, l'exécution d'un RLA est souvent présentée comme un "gold standard" pour établir que le résultat annoncé à la fin d'une procédure de dépouillement est conforme à l'ensemble de bulletins de vote papier dont on dispose.

La garantie offerte par un RLA n'est pas absolue : elle est probabiliste, laissant la place à un certain risque que l'audit ne permette pas de corriger un résultat incorrect – ce qui est bien le type de garantie visée par le Conseil de l'Europe. Un RLA ne déclarera cependant jamais qu'un résultat correct est incorrect. La borne sur le risque de confirmer un résultat incorrect peut être choisie à l'avance : 10%, 1% ou 0.1% par exemple. Au plus le risque accepté est faible, au plus l'effort requis pour réaliser la procédure d'audit sera important. Accepter une garantie probabiliste permet que la mise en œuvre d'un RLA soit la plupart du temps très efficace : dans la plupart des cas, seuls quelques dizaines ou centaines de bulletins de vote doivent être inspectés durant le processus d'audit, même si des millions de personnes ont voté. Inversement, le seul moyen d'avoir une garantie absolue, non probabiliste, d'un résultat correct serait de réaliser un recompte de tous les bulletins de vote, en supposant qu'il soit possible de réaliser celui-ci sans erreur même si le nombre de bulletins est énorme.

3.2.1.2 Comment se déroule un RLA ?

Le point de départ d'un RLA est un ensemble de bulletins de vote papier, dont on a certifié qu'ils reflètent bien les intentions des électeurs, ainsi qu'un résultat annoncé sur base d'une procédure de décompte de ces bulletins.

Il est évidemment primordial de s'assurer que les bulletins utilisés pour le RLA sont authentiques : s'ils ont été manipulés, l'audit pourrait confirmer un résultat erroné, voire invalider un résultat correct si la manipulation des urnes a eu lieu entre le décompte et l'audit. La mise en œuvre d'un RLA ne dispense donc en rien de conserver de fortes mesures de suivi des urnes, visant à empêcher toute modification de leur contenu. Cette exigence est naturellement déjà présente dans les élections qui n'ont pas recours à des RLAs.

Ces bulletins de vote doivent être organisés de manière structurée. Il est ainsi nécessaire de disposer d'un manifeste de l'élection, indiquant combien d'urnes ou d'enveloppes de bulletins de vote proviennent de chaque bureau de vote, ainsi que le nombre de bulletins contenus dans chaque urne ou enveloppe. La production de tels documents est habituelle dans les élections en Belgique. Cette organisation des bulletins permettra par exemple de piocher le 21ème bulletin de la 4ème urne provenant du bureau de vote numéro 8, si c'est ce que la procédure d'audit requiert. L'audit peut être rendu bien plus efficace si l'on dispose d'informations supplémentaires, comme un manifeste indiquant le contenu présumé de chaque bulletin de vote (par exemple : selon le manifeste, le 21ème bulletin de la 4ème urne du 8ème bureau de vote contient un vote pour le parti A).

Le but d'un RLA est de confirmer que les résultats annoncés pour l'élection sont corrects. Un RLA ne cherchera cependant pas à confirmer le nombre de voix exact reçu par un parti ou un candidat : il cherchera à confirmer que le nombre de sièges attribués à un parti est correct, ou que tel candidat a effectivement obtenu plus de voix que tel autre candidat. Confirmer un nombre exact de voix reçues rendrait en effet l'audit extrêmement inefficace.

L'efficacité de l'audit dépendra alors de plusieurs facteurs. Elle dépendra tout d'abord de la limite de risque que l'on choisit. Certaines juridictions acceptent un risque de l'ordre de 10%, alors que d'autres sont descendues pour certaines élections à un risque de 0.1%. L'efficacité de l'audit dépendra ensuite de la marge de l'élection, qui est une mesure du nombre de bulletins de vote qu'il faudrait modifier dans une élection pour changer son résultat (c'est-à-dire, changer le nombre de sièges attribués à un parti par exemple). Si le risque accepté et la marge de l'élection sont élevés, le résultat pourra être confirmé en inspectant un nombre de bulletins dérisoirement faible :

souvent quelques dizaines de bulletins, même pour une élection comptant des millions de votants. Si le risque accepté est faible et/ou si la marge de l'élection est (très) faible, il est possible, dans des cas extrêmes, que le RLA mène à un recompte manuel complet des bulletins.

Une fois le manifeste de l'élection établi, le risque choisi, et la marge de l'élection calculée, le RLA peut commencer. On se servira habituellement d'un outil informatique (il en existe un nombre croissant, open source) qui déterminera les bulletins de vote à inspecter. Cet outil indiquera, de manière vérifiable et transparente, le nombre et la localisation, selon le manifeste de l'élection, des bulletins de vote qui doivent être inspectés. On verra ainsi qu'il faut par exemple inspecter le bulletin 21 de la 4ème urne du bureau de vote 8, le bulletin 43 de la 6ème urne du bureau de vote 14, et ainsi de suite. Cette inspection pourra prendre plusieurs formes selon les informations disponibles : soit on encodera simplement le contenu du bulletin indiqué dans le système (on parle alors de *ballot-polling audit*) soit, si le système contient déjà un contenu présumé de chaque bulletin, on vérifiera que celui-ci est conforme (on parle alors de *ballot-comparison audit*). En cas de non-conformité, le système ajustera le nombre de bulletins à piocher, afin de déterminer si cette non-conformité est un cas isolé, ou fait partie d'un ensemble de non-conformités suffisamment importantes que pour modifier le résultat de l'élection. Si un nombre important de non-conformités est détecté, le nombre de bulletins à piocher s'approchera du nombre total de bulletins, et un recompte complet sera plus efficace. Ce recompte permettra d'établir le résultat correct. Un RLA se termine donc de deux manières possibles : soit, et dans la plupart des cas, le résultat de l'élection est confirmé, généralement après l'inspection d'un petit nombre de bulletins, soit un recompte complet des bulletins est requis et confirme ou infirme le résultat initialement annoncé.

3.2.1.3 De quelles ressources dispose-t-on en matière de RLAs ?

3.2.1.3.1 Littérature académique Les RLAs sont une technologie relativement récente : on peut trouver la première description d'un RLA dans un article de Philip B. Stark publié en 2008 [59]. Depuis lors, de nombreux articles scientifiques sont publiés chaque année, qui visent à pouvoir gérer des cas de figure de plus en plus diversifiés (élections dans lesquelles différentes méthodes de vote sont utilisées, dans lesquelles les méthodes de décompte et de stockage des bulletins diffèrent d'un comté à l'autre, ...) et à réduire le

plus possible les efforts nécessaires durant l'audit pour atteindre une limite de risque donnée.

Le rythme rapide d'évolution de la littérature fait que, dans le présent document, nous ne recommanderons pas l'usage d'une méthode spécifique en Belgique. Notre objectif sera plutôt de déterminer la faisabilité de RLAs dans le contexte belge, en évaluant les résultats qui pourraient être obtenus en employant les meilleures méthodes actuelles. Ceci donnera une limite supérieure sur les efforts à réaliser, et nous nous attendons à ce que les avancées de la recherche permettent rapidement de faire mieux, quand la décision de la méthode à utiliser se posera concrètement, soit pour les élections de 2029 au plus tôt.

3.2.1.3.2 Déploiements Le rythme d'évolution rapide de la littérature académique n'empêche pas que de nombreuses formes de RLAs ont déjà atteint une maturité importante et que leur usage est largement recommandé aux États-Unis. On peut ainsi trouver dans le rapport "Securing the Vote : Protecting American Democracy" des National Academies américaines publié en 2018 [47, p. 101] :

> 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.

La stratégie que nous proposons est alignée sur ces recommandations.

Concrètement, de premiers tests pilote de RLA ont eu lieu dès 2008 dans trois comtés de l'état de Californie [37]. De nombreux autres pilotes ont suivi, en particulier dans l'état du Colorado à partir de 2010 [62], état où les RLAs sont devenus obligatoires depuis 2017. D'autres états ont suivi depuis lors : des RLAs seront légalement requis pour les élections présidentielles de novembre 2024 dans les états du Colorado, Georgia, Nevada, Pennsylvania, Rhode Island et West-Virginia [66]. À ceux-ci s'ajoutent bien sûr un certain nombre d'autres états où des RLAs sont pratiqués à l'initiative des comtés (California, Michigan, Washington, ...). Les résultats de centaines d'élections

ont ainsi pu être confirmés. En Europe cependant, ce type d'audit n'est pas encore répandu, même si un projet pilote a eu lieu lors d'élections au Danemark dès 2015 [56].

Pour se faire une idée de l'ampleur de la tâche que peut représenter un RLA, on peut consulter le "Audit Center" de l'état du Colorado [22] qui documente les audits réalisés depuis 2017 dans cet état pionnier. Si l'on regarde les élections de 2023, on peut y lire que, dans les 63 comtés qui ont réalisé des RLAs, le nombre prévu de bulletins à inspecter oscille entre 17 et 346 pour une limite de risque de 3%, fixée par l'état (une limite de 9% avait été choisie pour les premiers pilotes dans cet état), et sont obtenu dans le cadre de "ballot-comparison audits", particulièrement efficaces. D'autres états font d'autres choix : la Californie par exemple, impose une limite de 5% aux comtés qui choisissent de réaliser un RLA. Cette même limite de 5% est d'application dans l'état de Georgia. On s'attend néanmoins à ce qu'un nombre nettement plus grand de bulletins doivent souvent être examinés en Belgique, en raison des très faibles marges qui sont régulièrement observées.

Des cas extrêmes ont ainsi pu se présenter aux États-Unis où les marges étaient tellement faibles qu'un dépouillement complet des bulletins papier a dû être réalisé. Un exemple marquant a ainsi été celui de l'état de Georgia où, pour les élections présidentielles de 2020, un recomptage complet de 5 millions de bulletins de vote a été nécessaire [35]. L'audit des élections de 2022 s'est déroulé sans difficulté. (En Belgique, les élections étant découpées par circonscriptions électorales, un recompte complet ne serait organisé qu'au niveau de la circonscription, et non au niveau de la région ou du pays.)

3.2.1.3.3 Outils informatiques Les audits décrits ci-dessus sont réalisés avec le support de logiciels qui permettent de déterminer, sur base de manifestes, du risque assumé et des inspections déjà réalisées, quels bulletins doivent encore être inspectés, ou si l'audit peut être clôturé. Ces outils sont le plus souvent open source et mis en œuvre par les personnes en charge de l'organisation de l'élection, souvent avec l'aide d'entreprises expertes qui apportent leur support à la mise en œuvre de ces outils.

À ce jour, l'outil le plus largement utilisé est Arlo, un outil open source qui a été déployé dans 11 états des États-Unis et est développé par VotingWorks, une organisation sans but lucratif (501(c)(3) en termes américains) :

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

Arlo semble progressivement remplacer les outils plus anciens, comme ColoradoRLA, qui a été utilisé pour les RLAs du Colorado jusqu'en 2018.

Philip Stark met par ailleurs à disposition un certain nombre d'outils open source développés dans un contexte académique, via son compte GitHub :

https://github.com/pbstark/

Bon nombre de ces outils ont été utilisés dans des déploiements pilote dans le passé, et Arlo est largement basé sur des méthodes conçues par Philip Stark. D'autres outils sont plus récents et offrent des fonctionnalités et des performances plus avancées. On pense ici en particulier à l'outil SHANGRLA qui peut s'adapter à un très grand nombre de méthodes de décompte, y compris la méthode D'Hondt utilisée en Belgique [61]. Cet outil est testé depuis 2019, notamment par la ville de San Francisco qui pratique le vote alternatif dans certaines élections (une méthode de vote dans laquelle les électeurs proposent un classement des candidats, souvent partiel, sur le bulletin de vote) [6].

3.2.1.3.4 Cadre légal Le cadre légal concernant les audits varie fort d'un état à l'autre. Une "Audit Law Database" est proposée par le site Verified Voting à l'adresse suivante :

https://verifiedvoting.org/auditlaws/

3.2.1.4 Pour aller plus loin...

Les déploiements de RLAs ont été accompagnés de la publication de bon nombre de guides, rapports d'expérience, vidéos, ... Nous pouvons notamment pointer les ressources suivantes.

— La National Association of Election Officials américaine a publié entre 2019 et 2021 une série de quatre guides "Knowing It's Right" en support de la mise en œuvre de RLAs [43, 44, 45, 46].

— Le Brennan Center for Justice a publié en 2019 un rapport détaillé "Pilot Implementation Study of Risk-Limiting Audit Methods in the State of Rhode Island"[54].

— Le Carter Center, qui a notamment observé les RLAs en Georgia depuis 2020, a lui aussi publié en 2022 un guide intitulé "Risk-Limiting Audits : A Guide for Election Observation Efforts" [10].

3.2.2 Une stratégie de RLA pour la Belgique

La mise en œuvre de RLAs pour les élections en Belgique est une procédure qui doit se faire de manière progressive et impliquer un large spectre

d'acteurs, faute de quoi on risque de passer à côté des objectifs visés : obtenir de manière efficace une confiance accrue dans les résultats des élections.

3.2.2.1 Se baser sur l'expérience acquise ailleurs

L'expérience du nombre croissant d'états américains qui ont déployé des RLAs – et continuent à le faire – permet de dégager les éléments stratégiques pour la mise en place de ce type d'audits. Les élections belges diffèrent cependant des élections américaines par un nombre important d'aspects. Deux aspects semblent particulièrement importants :

1. Les élections sont organisées en Belgique de manière beaucoup plus rares qu'aux États-Unis : nous organisons (en temps normal) des élections conjointes selon des cycles de 5 ou 6 ans, là où bon nombre d'états américains organisent des élections deux ou trois fois par an. Nous avons ainsi eu 11 jours d'élections entre 2000 et 2023 en Belgique.
2. La forme de nos bulletins de vote est très différente : nous élisons un grand nombre de représentants pour un petit nombre d'assemblées, là où les bulletins proposés aux électeurs américains contiennent souvent plusieurs dizaines de questions, variables selon le domicile des électeurs, avec généralement un petit nombre de choix possibles associés à chaque question.

La fréquence des élections a évidemment un impact important. D'une part, des élections moins fréquentes requièrent un travail d'audit moins fréquent, ce qui limite la charge globale de l'organisation des élections dans un pays comme la Belgique. L'inconvénient est qu'une organisation plus rare donne moins d'occasions de pratiquer les élections. Cela implique un plus petit nombre d'occasions d'organiser des pilotes de nouveaux processus dans des conditions réelles, ainsi qu'une plus grande rotation dans les acteurs impliqués dans la pratique des élections. L'importance d'une bonne documentation des procédures sera d'autant plus grande.

La forme de nos bulletins de vote présente elle aussi, des avantages et des inconvénients. Chacun de nos bulletins de vote porte sur une unique élection, et chaque élection peut donc être auditée de manière individuelle. La Belgique peut ainsi éviter toutes les complexités associées aux bulletins de vote américains qui, sur un même bulletin, vont contenir les choix des électeurs pour plusieurs élections distinctes, ce qui ajoute beaucoup à la complexité des audits. Cependant, le grand nombre de personnes que nous élisons, et les méthodes de décompte que nous utilisons, font que, au sein de chacune de nos élections, les marges d'erreur tendent à être plus réduites,

laissant moins de place aux erreurs et rendant les audits potentiellement plus exigeants en termes de nombre de bulletins à vérifier.

Ces aspects sont importants, mais il n'en reste pas moins que la pratique existante peut certainement guider la Belgique dans sa stratégie de déploiement.

3.2.2.2 Temporalité

3.2.2.2.1 Mettre en place un groupe de travail Une première étape importante est de rassembler des personnes ayant les compétences de l'organisation d'élections à tous les niveaux afin de construire une collaboration autour de la mise en place de RLAs.

Ce groupe de travail rassemblera des acteurs expérimentés des différentes étapes du processus de dépouillement, de totalisation des résultats des élections et de gestion des bulletins de vote. On pense notamment à des personnes :

- de la Direction des élections au SPF intérieur,
- des services en charge des élections au niveau des régions,
- ayant l'expérience de bureaux principaux de circonscription électorale,
- ayant l'expérience de bureaux principaux de canton,
- ayant l'expérience de bureaux de dépouillement.

Ces acteurs, et peut-être d'autres qui seront identifiés, seront essentiels pour que la procédure de RLA puisse être organisée de manière efficace à chacune des étapes.

Il sera aussi important d'inclure dans ce groupe :

- une ou plusieurs personnes avec l'expertise légale nécessaire pour identifier les adaptations qui seront nécessaires dans la législation afin de permettre de réaliser les audits envisagés,
- une ou plusieurs personnes ayant de l'expérience en matière de RLAs, y compris en terme d'outils informatiques qui seront développés et utilisés en support de ces audits,
- une ou plusieurs personnes en charge de la communication autour des activités du groupe,
- une personne représentant le fournisseur des machines de vote qui seront auditées, ou pouvant assurer les interactions avec celui-ci.

L'objectif de ce groupe de travail sera d'établir de manière concrète la procédure de mise en œuvre de RLAs, tout d'abord sous la forme de pilote,

puis sous une forme généralisée, ainsi que de déterminer la stratégie de communication vers les acteurs politiques et la population qui devra être mise en place, ainsi que l'organisation de la formation des acteurs de terrain.

Nous proposons ci-dessous un chemin menant vers un déploiement généralisé de RLAs en Belgique. Nous commençons par proposer différentes étapes sur ce chemin. Par la suite, nous proposerons une première esquisse de la manière dont des RLAs pourraient être organisés.

3.2.2.2.2 Simuler le processus en dimensions réduites La rareté des élections en Belgique donne peu d'occasions d'expérimenter de nouvelles procédures sur le terrain. Afin de garantir une première maturité au processus d'audit lors des essais de terrain, il sera utile de tester ce processus d'audit en dimension réduite, sur base de bulletins fictifs. Une dimension possible serait sans doute de travailler avec de l'ordre de 5000 à 10000 bulletins : une telle dimension permettrait de donner un bon sens de la complexité de retrouver et inspecter des bulletins de vote dans les conditions réelles, sans requérir une logistique démesurée.

Ces tests pourront être réalisés par des acteurs externes au groupe de travail qui, lui, serait présent en situation d'observation. Il sera utile de limiter la présence d'observateurs externes, afin que les personnes présentes se sentent pleinement libres d'exprimer leurs éventuelles incompréhensions, critiques, compliments, et de faciliter un débat sincère menant à une amélioration des procédures.

Ils pourront aussi donner un premier sens du temps nécessaire à l'accomplissement d'un audit dans une situation réelle.

3.2.2.2.3 Premier pilote Lorsqu'une confiance suffisante dans l'organisation du processus de RLA aura été acquise via des simulations, un premier pilote à dimension réelle pourra être organisé. Nous viserions ici de réaliser le pilote à l'échelle d'une circonscription électorale de taille moyenne.

Ce premier pilote pourrait avoir lieu juste après la validation des résultats d'une élection : cela évite de devoir conserver les bulletins de vote pour des périodes trop importantes, et permet de conserver la dynamique de l'élection qui se termine. Par ailleurs, réaliser le pilote après la validation permet que ce premier pilote, qui impliquera de manipuler des bulletins de vote authentiques, ne pourra pas interférer avec le processus normal de validation de l'élection.

Le passage à un pilote de dimension réelle permettra de tester la documentation et le processus de formation des acteurs : l'audit de plusieurs

centaines de milliers de bulletins de vote va nécessiter la participation d'un plus grand nombre de personnes, qui devront être formées. Il permettra aussi de tester la logistique associée au suivi et à la gestion de centaines de milliers de bulletins de vote.

Il sera à nouveau utile de réaliser ce pilote dans un cadre propice à l'expression libre et constructive des différents participants.

Les différents processus seront ajustés en fonction des leçons apprises durant le pilote.

3.2.2.2.4 Second Pilote Un second pilote sera très vraisemblablement utile afin d'affiner le processus. À ce stade, il pourra être envisagé de réaliser l'audit en conditions réelles, avant la certification des résultats. Le niveau de confiance dans le processus devra alors être déjà très élevé : il faudra avoir accepté que les bulletins de vote soient manipulés dans le cadre d'un audit avant certification, et être préparé à ce que l'audit puisse éventuellement ne pas valider les résultats escomptés. Les adaptations de la législation seront dès lors vraisemblablement plus importantes.

À ce stade, et en particulier si ce pilote se déroule avant la certification des résultats, il deviendra important d'inclure des observateurs, selon des critères similaires à celles utilisées dans les bureaux de dépouillement.

3.2.2.2.5 Généralisation Sur base de pilotes réussis, un déploiement généralisé des RLAs pourra être réalisé. Ceux-ci pourront avoir lieu en présence d'observateurs, dans les mêmes conditions que dans un bureau de dépouillement classique.

3.2.2.3 Éléments d'organisation

3.2.2.3.1 Cible des audits Une première décision pratique est la cible de l'audit : quelle élection souhaite-t-on auditer, et pour quelle granularité de résultats ?

Le premier choix porte sur les élections que l'on souhaite auditer en premier. Ici, notre recommandation porte sur les **élections fédérales** :

— ce choix permet d'élaborer la stratégie de RLA en un lieu unique qui touche tous les Belges et pourra par la suite percoler vers les autres élections, sur base de l'expérience acquise,

— ces élections sont organisées autour de 11 circonscriptions électorales, contre 4 pour les européennes, qui touchent aussi toute la Belgique, ce

qui permet de garder des circonscriptions de dimension plus limitée, facilitant l'audit.

Organiser des pilotes dans le cadre des élections régionales, provinciales ou communales ne permettrait pas d'acquérir de manière aussi directe une expérience utile pour tous les Belges. Les élections communales pourraient avoir l'attrait d'un petit nombre de bulletins à gérer par élection, simplifiant la logistique. Cependant, le plus petit nombre d'électeurs impliqués dans chaque élection fait que les connaissances acquises dans des pilotes pour ces scrutins laisseraient beaucoup de questions ouvertes avant un audit au niveau d'une circonscription électorale complète. Qui plus est, la petitesse des marges électorales de ces scrutins combinée au petit nombre d'électeurs risque de mener régulièrement à des recomptages complets, limitant les bénéfices des RLAs dans ce contexte. [3]

Au niveau de la granularité, notre proposition est de se concentrer sur la **répartition des sièges entre les partis**. Il serait bien évidemment intéressant aussi d'auditer la répartition des sièges entre les candidats, mais nous voyons deux difficultés à ce niveau :

1. Les marges avec lesquelles les candidats sont élus sont fort faibles aussi, et prendre en compte l'allocation des sièges risque dès lors d'augmenter sensiblement le risque de devoir conclure l'audit par un recomptage complet des bulletins. Ceci ne semble pas souhaitable, en particulier pour des pilotes.
2. Dans le contexte du vote papier classique, qui devra être intégré au RLA dans toutes les circonscriptions où l'on pratique à la fois le vote électronique et le vote papier, les bulletins dépouillés sont souvent classés et archivés par parti. Ce classement permet un gain d'efficacité considérable pour la procédure d'audit, dans la mesure où la procédure de dépouillement créée ainsi un engagement sur le contenu des bulletins (au niveau des partis en tous cas), ce qui permet d'appliquer des techniques efficaces de ballot-comparison audit. La vérification du contenu des bulletins est aussi fortement simplifiée s'il s'agit uniquement de s'assurer qu'un bulletin contient un vote valide pour un parti donné.

Ce second point est susceptible d'évoluer dans les années à venir : le logiciel PATSY, qui sera déployé en Wallonie dès 2024, fournit en effet un encodage électronique du contenu de chaque bulletin, pris individuellement.

3. Le calcul des marges électorales a été réalisé pour toutes les communes wallonnes après les élections de 2019 : https://decryptage.be/communes_wallonnes.html.

Une circonscription se servant de PATSY pourrait en effet disposer d'un lien direct entre les bulletins papier et leur encodage électronique, pour autant qu'elle veille à garder le lien entre les bulletins papier et leur encodage électronique (en apposant un numéro sur chaque bulletin, ou simplement en stockant les bulletins dans l'ordre de leur encodage, dans des enveloppes de taille modérée (une cinquantaine ou une centaine de bulletins). Un usage généralisé de PATSY ou d'un autre logiciel équivalent, assorti de mesure de conservation des bulletins appropriées, pourrait ainsi permettre de pratiquer un ballot-comparison audit, y compris au niveau de la répartition des sièges au niveau des candidats. (Ceci ne change évidemment rien aux faibles marges entre les élus.)

3.2.2.3.2 Méthode d'audit Comme indiqué plus haut, il existe plusieurs familles de RLAs :

1. les audits par comparaison de bulletins de vote : *ballot-comparison audits*, qui consistent à piocher des bulletins de vote papier et à vérifier qu'ils ont été correctement interprétés dans les rapports électroniques du décompte ;
2. les audits par échantillonnage des bulletins : *ballot-polling audits*, qui consistent à piocher des bulletins de vote papier et à réaliser un nouveau dépouillement sur base de ceux-ci, en s'assurant que la tendance observée sur l'échantillon correspond au résultat qui a été annoncé pour l'ensemble des bulletins ;
3. les audits par comparaison de bulletins par paquets : *batch-comparison audits*, qui consistent à recompter l'entièreté des bulletins qui se trouvent dans un certain nombre d'enveloppes (on s'attend à ce que chaque enveloppe contienne au maximum quelques centaines de bulletins), et à vérifier que le résultat recompté pour chaque enveloppe correspond à ce qui était prévu.

Nous recommandons de tout mettre en place pour pouvoir réaliser des **ballot comparison audits en Belgique**. En effet, cette méthode est celle qui permet, souvent de loin, de devoir manipuler le plus petit nombre de bulletins papier. Or, étant donné les marges souvent faibles que l'on trouve en Belgique, disposer de méthodes d'audit efficaces est primordial.

L'efficacité des ballot-comparison audits repose sur une exigence logistique importante : il faut être en mesure de retrouver le bulletin de vote papier associé à chaque encodage électronique. Ceci semble cependant être un objectif réalisable en Belgique :

— pour le vote papier, tant l'usage de PATSY que la pratique du tri des bulletins de vote en enveloppes séparées rassemblant les bulletins associés à un même parti (Art. 159 du Code électoral [13]), permettent de construire un manifeste tel que l'on sait comment a été interprété, lors du décompte, chacun des bulletins de vote,

— pour le vote électronique, le contenu de chaque bulletin papier est déjà enregistré de manière électronique aujourd'hui, et les procédures d'impression et de scanning des bulletins qui seront décrites ci-dessous permettront aussi de garder un lien entre le papier et son enregistrement électronique.

3.2.2.3.3 Traçabilité des bulletins de vote La validité et la facilité de mise en œuvre d'un RLA reposent largement sur la qualité de la logistique des bulletins de vote.

Il faut d'une part avoir la garantie que les bulletins papier sur base desquels on réalise l'audit sont authentiques. Le but d'un RLA est de confirmer qu'un résultat d'élection annoncé reflète bien un ensemble de bulletins de vote. Naturellement, si ces bulletins de vote ont été falsifiés, l'audit n'apporte rien.

Le maintien d'une stratégie de traçabilité irréprochable des bulletins, est donc primordiale, depuis les mains des électeurs jusqu'au lieu où se déroule le RLA. Cette exigence de traçabilité n'est certainement pas neuve dans le contexte d'un RLA : elle est déjà nécessaire afin de garantir que des éventuels recomptages de bulletins soient valides.

L'introduction de RLAs accentue cependant cette importance : alors que les recomptages sont relativement rares aujourd'hui, et généralement très partiels, l'usage de RLAs pourra mettre en lumière des irrégularités qui auraient lien entre le moment de dépouillement des votes et celui de l'audit. Et, si les bulletins de vote étaient authentiques au moment du décompte, mais ne le sont plus au moment de l'audit, il se pourrait que l'audit vienne invalider un dépouillement qui était peut-être correct. L'introduction de RLAs appelle donc à un passage en revue de toutes les procédures actuelles de traçabilité, et à une amélioration de celles-ci partout où ce serait possible.

Inversement, si les bulletins de vote sont manipulés avant le dépouillement (par modification, ajout ou suppression de bulletins), il est vraisemblable que l'audit confirme le résultat annoncé suite au dépouillement, bien que celui-ci soit incorrect, et ne permette pas de détecter une fraude qui résulterait d'une brèche dans la traçabilité des bulletins.

La vérification de cette traçabilité pourra cependant être largement amé-

liorée grâce à la "vérifiabilité de bout en bout" de l'élection, basée sur des techniques cryptographiques qui sont décrites en section 3.3. Un électeur pourra ainsi s'assurer que son bulletin de vote a été correctement pris en compte dans le dépouillement de l'élection.

3.2.2.3.4 Manifeste de l'élection Outre la traçabilité des bulletins de vote, il est aussi primordial, pour un RLA efficace, de disposer d'un classement de tous les bulletins, consigné dans un manifeste.

Il est en effet nécessaire, avant d'entamer l'audit, de disposer de documents listant au minimum :

— les conteneurs (boîtes, etc.) numérotés (ou autrement identifiés) dans lesquels les bulletins de vote sont stockés,

— le nombre de bulletins de vote présents dans chaque conteneur,

— la manière dont chacun de ces bulletins a été interprété.

Il sera aussi utile de garder une trace de l'origine de chacun des conteneurs, ainsi que de leur parcours : qui les a scellés, où et quand, et qui les a ensuite réceptionnés et manipulés, en quel lieux et à quels moments, et ce jusqu'au moment du stockage après l'audit.

De tels documents sont déjà largement produits dans le cadre du vote papier via les procès-verbaux des bureaux de vote et de dépouillement, qui sont compilés au niveau des bureaux principaux de canton, et d'arrondissement. En effet, même si on ne dispose pas d'un registre indiquant spécifiquement comment chaque bulletin a été interprété, le classement des bulletins pour chaque parti en enveloppes séparées offre la même fonctionnalité : l'on sait, avant d'ouvrir une enveloppe, à quel parti ont été attribués tous les bulletins contenus dans cette enveloppe (ou si le bulletin a été interprété comme blanc ou nul).

Ceci n'est cependant pas le cas aujourd'hui pour le vote électronique : les bulletins papier ne sont en effet pas systématiquement triés pour ces élections, le dépouillement se faisant sur base des données présentes sur les clés USB des présidents de bureaux de vote. Il serait possible de s'accommoder de cette situation en procédant à des "batch-comparison audits", mais ceux-ci alourdiraient considérablement la procédure d'audit, chaque "batch" qui doit être recompté correspondant à une urne pouvant contenir 800 bulletins de vote ou plus – sachant que le nombre de batches à dépouiller n'est pas sensiblement inférieur au nombre de bulletins à comparer dans le cadre d'un ballot-comparison audit.

Un certain nombre d'options sont envisageables ici, pour le vote électronique. Celle que nous recommandons (d'autres options sont discutées ci-

dessous) est de réaliser, au moment du scanning des bulletins papier, l'impression d'un numéro de suivi unique sur le bulletin, numéro de suivi qui serait conservé avec l'enregistrement électronique du bulletin.

Cette impression impose que les bulletins papier soient imprimés sur du papier permettant l'impression aisée d'une marque au moment du scanning. Ici, l'usage de papier au format standard (A4 par exemple) apparait comme la solution la plus attrayante et la plus couramment utilisée. Ce type de papier peut être facilement inséré dans des scanners classiques, équipés d'un module d'impression permettant généralement d'imprimer un numéro de série du scanner, la date et l'heure du scanning, ainsi qu'un compteur de pages scannées. Ces modules d'impression, parfois appelé "endosseur" ou "imprimeuse" en français et "imprinter" en anglais, sont courants dans les solutions d'archivage, et permettent, pour des modèles d'entrée de gamme, de scanner de l'ordre de 70 à 80 pages par minute. Une urne contenant de l'ordre de 800 bulletins de vote pourrait ainsi être scannée en une dizaine de minutes. La charge d'un bureau de dépouillement, qui tourne autour de 2400 bulletins de vote, pourrait être absorbée en une demi-heure de scanning (hors temps de manutention du papier).

Le scanning avec impression pourrait avoir lieu à différents endroits et selon différentes modalités. Nous les discuterons au chapitre suivant, en lien avec la structure du système de vote.

L'approche que nous avons décrite ici construit le lien entre les bulletins papier et leur version électronique via l'impression d'un numéro de série au moment du scanning. D'autres options sont évidemment possibles, et nous en discutons plusieurs ici.

1. Conservation des bulletins scannés en ordre de scanning. Ici, l'idée est de scanner les bulletins par paquets d'une centaine de bulletins, et de conserver intact, dans des enveloppes ou des fardes, l'ordre des bulletins scannés. Si le logiciel du scanner préserve lui aussi l'ordre de scanning (via des logs, des noms de fichiers, un ordre des lignes dans des tableaux contenant les interprétations des bulletins, etc.). Cet ordre est suffisant que pour permettre de réaliser un audit qui indiquerait de comparer l'enregistrement électronique et la version papier du 83ème bulletin de vote du paquet 8 de la boite de bulletins de vote 17 par exemple. Une telle solution, qui est utilisée dans certaines localités aux USA, est cependant très fragile : retrouver le 83ème bulletin dans une pile peut être malaisé, demander des efforts importants, et source d'erreurs dans l'audit (erreurs qui pourraient amener à devoir vérifier un plus grand nombre de bulletins pour achever l'audit). Qui plus est, il

suffit qu'une pile de bulletins échappe des mains de la personne qui la manipule pour que l'ordre soit perdu, rendant impossible la vérification du bulletin choisi dans le processus d'audit. Cette impossibilité de vérification devra vraisemblablement être interprétée dans l'audit comme un bulletin incorrectement dépouillé (pour éviter le risque que l'audit ne soit faussé par une personne qui camouflerait des bulletins incorrects en laissant tomber la pile de bulletins à dessein), ce qui risque d'avoir pour effet d'imposer la vérification d'un certain nombre de bulletins complémentaires.

2. Impression d'un numéro de série unique sur le bulletin par la machine de vote, en même temps que l'impression du bulletin. Ce numéro de série serait scanné en même temps que le bulletin, et conservé au format électronique avec l'interprétation du bulletin. Cette solution aurait l'avantage d'éviter le besoin d'utiliser un scanner équipé d'un endosseur. Elle risque cependant de ralentir sensiblement le processus d'audit par rapport à la solution basée sur un endosseur. En effet, l'endosseur intégré au scanner peut sans difficulté numéroter de manière croissante les bulletins qui sont scannés : ces bulletins sont passés par l'urne et ont été mélangés avant d'être scannés, ce qui évite les préoccupations liées à la confidentialité des votes. Et cette numérotation croissante facilite grandement la recherche des bulletins dans une pile : on peut rechercher par dichotomie un bulletin portant un numéro donné, comme dans un dictionnaire. Numéroter de manière croissante les bulletins de vote au niveau de la machine à voter pose en revanche des soucis importants : une personne qui observe l'ordre dans lequel les électeurs utilisent une machine à voter pourrait ensuite retrouver les bulletins de chacun dans une urne, même après un mélange intensif. Une alternative serait d'imprimer des numéros de série aléatoires sur les bulletins de vote, ce qui éviterait les risques de confidentialité associés à une numérotation séquentielle. Cependant, la recherche d'un bulletin de vote portant un numéro aléatoire dans une pile de bulletins scannés va devenir nettement plus ardue : il s'agira de passer en revue la moitié des bulletins en moyenne avant de trouver le bon. Cette solution serait cependant plus robuste que la précédente, dans la mesure où la chute d'une pile de bulletins de vote ne poserait pas de problème particulier.

Dans les contextes où les bulletins scannés sont conservés dans l'ordre et où il s'agit de retrouver un bulletin dans une position spécifique de la pile, des méthodes plus exotiques ont été testées. Par exemple, la recherche d'un bulletin peut être aidée par l'usage d'une balance très précise : il pourrait

être calculé que le 83ème bulletin d'une pile peut être retrouvé en retirant les 82 premiers bulletins qui pèseraient 408 grammes (par exemple). On soulève alors des bulletins de la pile et les pèse jusqu'à atteindre le poids recherché. Cependant, cette méthode s'avère souvent trop aléatoire, à cause de la légère variabilité dans le poids du papier, notamment liée à l'humidité présente.

Une autre méthode, par découpes successives, a été proposée pour la sélection d'un bulletin aléatoire dans une pile de bulletins, en remplacement de l'exigence de sélectionner un bulletin dans une position donnée dans une pile [58]. Il s'agit ici de "couper" manuellement la pile de bulletins un certain nombre de fois, en piochant un paquet de bulletins en haut de la pile et en la remplaçant au bas de la pile (par exemple, une pile de cinq bulletins ABCDE pourrait être transformée en une pile DEABC à la suite d'une coupe). En pratique, il semble que la répétition de 6 coupes successives suffit à faire apparaître un bulletin de vote à peu près uniformément choisi au sommet de la pile de bulletins, et ce pour des piles de bulletins pouvant contenir jusqu'à 1000 bulletins.

Cette stratégie pourrait notamment être intéressante dans le contexte de la sélection d'un bulletin papier dans une enveloppe supposée contenir des bulletins allant à un unique parti : dans ce cas, tous les bulletins de vote sont essentiellement équivalents. Elle serait plus délicate à utiliser dans un contexte où les bulletins diffèrent et où le lien entre le papier et l'électronique repose sur de l'endossement : piocher un bulletin papier au hasard plutôt qu'au départ du manifeste électronique pourrait ouvrir la porte à des fraudes dans lesquelles plusieurs bulletins de vote papier contenant des votes identiques seraient aussi marqués d'un endossement identique, ce qui pourrait permettre d'ajouter des bulletins de vote dans le manifeste électronique, qui n'auraient pas de correspondance papier, et ne seraient dès lors jamais examinés.

3.2.2.3.5 Logiciel d'audit Le déroulement d'un audit est grandement facilité par l'usage d'un logiciel dédié.

On fournit tout d'abord à ce logiciel une copie du manifeste de l'élection, généralement sous la forme d'un fichier tableur reprenant les éléments essentiels du manifeste de l'élection : liste des conteneurs de bulletins de vote, ainsi que de leur contenu, bulletin par bulletin, et résultat annoncé du dépouillement de l'élection.

On initialise ensuite l'audit en indiquant la marge de risque que l'on souhaite tolérer, ainsi qu'en sélectionnant un nombre aléatoire à partir duquel sera dérivée la liste des bulletins de vote à vérifier durant l'audit. Partir d'un

nombre aléatoire fourni au logiciel permet de s'assurer que les choix opérés durant l'audit ne sont pas biaisés, et permet de reproduire l'intégralité de l'audit si besoin – ce qui ne serait pas possible si chaque nouvelle exécution de l'audit donnait lieu à une nouvelle séquence aléatoire de bulletins.

Concrètement, ce nombre aléatoire est souvent produit en lançant une série de dés en présence d'un certain nombre d'observateurs. Dans certaines juridictions, le lancer de dés est filmé et inclus dans les données publiques de l'audit. Un exemple de cérémonie de lancer de dés dans le contexte du RLA de l'élection de l'actuel secrétaire d'État de l'état de Georgia peut être visualisé à l'adresse ci-dessous.

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

Sur base de ces informations, le logiciel d'audit détermine quels bulletins de vote papier doivent être inspectés pour comparaison avec leur interprétation électronique, et ce afin de pouvoir valider le résultat annoncé, avec le niveau de risque choisi. Le logiciel pourra adapter son comportement en cours d'audit : par exemple, si des bulletins incorrectement interprétés ou manquants sont découverts, la vérification d'un plus grand nombre de bulletins sera requise afin de déterminer si cette erreur est anecdotique ou reflète un problème de dépouillement susceptible de modifier le résultat de l'élection. Dans le pire des cas, le logiciel pourra conclure qu'un nouveau dépouillement complet est requis.

3.2.2.3.6 Organisation du local d'audit Il est naturellement important d'organiser l'audit lui-même dans des conditions qui permettront de convaincre les intervenants de l'élection que le résultat dépouillé est effectivement correct. L'audit doit aussi avoir lieu dans un local arrangé de sorte que les opérations puissent se dérouler de manière efficace, et sans compromettre la sécurité des bulletins de vote.

De manière générale, il est intéressant de rendre l'audit aussi visible que possible, au moins pour les observateurs. La cérémonie de lancer de dés pour la génération du nombre aléatoire initialisant l'audit sera réalisée aux yeux de tous. On connectera le laptop sur lequel fonctionne le logiciel d'audit à un projecteur, afin que tous puissent suivre le déroulement de l'audit, l'évolution des marges estimées, et avoir en vue la liste des bulletins de vote à inspecter ou déjà inspectés.

Le local devra permettre que des pauses aient lieu sans compromettre la sécurité de l'audit, ainsi que de gérer des coupures d'électricité ou déclenchements d'alarme incendie qui pourraient forcer à évacuer les lieux. Disposer d'un local facile à verrouiller et à évacuer est important.

Enfin, il devra être prévu que l'audit puisse mener à un dépouillement manuel complet des bulletins. Celui-ci nécessitera un espace plus important, devra s'étaler sur plusieurs jours et nécessitera un nombre de personnes bien plus important qu'un audit normal. La complétion de l'audit étant nécessaire pour la validation finale des résultats, la procédure et la liste des personnes requises pour un éventuel nouveau dépouillement devront être établis bien à l'avance.

Enfin, un procès-verbal de l'audit pourra être produit, normalement par le logiciel d'audit, validé par les observateurs présents, et transmis au Bureau de circonscription ainsi qu'au SPF intérieur. Ce procès-verbal pourra être publié avec les résultats de l'élection.

3.2.3 Évaluation sur base de précédentes élections

En partant des fichiers CSV disponibles sur le site du service fédéral,[4] nous avons calculé les marges des élections fédérales de 2014 et 2019 en Belgique, pour chaque circonscription. Chaque circonscription est considérée comme une élection indépendante des autres puisque chacune possède un nombre de sièges à allouer qui lui est propre.

Pour calculer les marges, après extraction des données à partir des fichiers CSV, nous avons procédé de la façon suivante. Pour chaque paire (A, B) de partis représentés dans chaque circonscription nous regardons les conditions suivantes :

1. Est-ce que le parti A a obtenu suffisamment de voix pour dépasser le seuil électoral ?
   - Si oui, combien de voix devrait-il ne pas avoir reçu pour ne plus dépasser le seuil ?
   - Si non, combien de voix lui faudrait-il pour dépasser le seuil et le parti B a-t-il suffisamment de voix pour en donner assez au parti A ?
2. Si le parti A a obtenu un siège après l'allocation selon la méthode d'Hondt, combien de votes faudrait-il qu'il perde au profit du parti B pour que le dernier siège alloué au parti A soit plutôt alloué au parti B ?

Chaque marge potentielle établie selon ces conditions est tout d'abord testée pour vérifier que le transfert de votes du parti A au profit du parti B donnerait un résultat différent (c'est à dire une répartition des sièges différentes

4. https://resultatselection.belgium.be

entre les listes). Ensuite, pour chaque paire (A, B), la plus petite des marges validées est retenue. Enfin, la paire avec la plus petite marge parmi toutes les autres paires est retenue : c'est elle qui indique la marge de l'élection, c'est-à-dire le plus petit nombre de votes susceptible de changer le résultat de l'élection.

La Table 3.1 présente les marges ainsi obtenues pour chaque circonscription lors des élections fédérales de 2014 et 2019. Comme on peut s'y attendre, le système d'Hondt donne lieu à des marges parfois très faibles, souvent de l'ordre de quelques centaines de votes.

Sur base de cela, et au vu des résultats obtenus dans d'autres pays, on peut s'attendre à ce que la mise en œuvre de RLAs dans le contexte de ces élections requière d'auditer un nombre de bulletins de vote pouvant osciller entre une centaine de bulletins (quand les marges sont élevées, comme cela a été le cas dans le circonscription du Luxembourg) et quelques milliers de bulletins. Dans certains cas extrêmes, il n'est cependant pas exclu qu'un recomptage complet soit nécessaire (on pense ici par exemple au cas de la Flandre orientale en 2014).

3.3 Vérifiabilité de bout en bout

3.3.1 Introduction

3.3.1.1 Qu'est-ce qu'une élection vérifiable de bout en bout ?

Une élection est vérifiable de bout en bout, aussi appelée "*end-to-end verifiable*" ou "*E2E verifiable*" si elle permet de vérifier que le résultat de l'élection annoncé est correct, indépendamment d'une confiance devant être placée dans un équipement spécifique, dans des procédures spécifiques, ou dans des personnes spécifiques.

Les vérifications effectuées portent habituellement sur deux éléments principaux :

1. la *vérifiabilité individuelle* : mon bulletin de vote est-il bien présent, sans modification, dans l'urne (éventuellement électronique) qui est dépouillée ?
2. la *vérifiabilité universelle* : les bulletins présents dans l'urne sont-ils dépouillés correctement ?

Circonscription	Année	Marge Absolue	Marge Relative
Liège	2014	783	0.125 %
	2019	919	0.148 %
Hainaut	2014	1 173	0.159 %
	2019	743	0.102 %
Brabant Wallon	2014	511	0.213 %
	2019	5 261	2.128 %
Anvers	2014	1 155	0.101 %
	2019	453	0.039 %
Namur	2014	693	0.231 %
	2019	3 579	1.174 %
Luxembourg	2014	7 679	4.525 %
	2019	4 812	2.817 %
Flandre Occidentale	2014	2 165	0.268 %
	2019	2 748	0.341 %
Limbourg	2014	225	0.041 %
	2019	2 710	0.488 %
Brabant Flamand	2014	6 359	0.936 %
	2019	1 782	0.258 %
Flandre Orientale	2014	338	0.034 %
	2019	2 369	0.237 %
Bruxelles-Capitale	2014	305	0.061 %
	2019	965	0.192 %

TABLE 3.1 – Marges des élections fédérales de 2014 et 2019.

Certains auteurs ajoutent une exigence supplémentaire, la *vérifiabilité d'éligibilité* : les bulletins présents dans l'urne proviennent-ils bien uniquement d'électeurs autorisés ?

La vérifiabilité individuelle et la vérifiabilité universelle sont recommandées comme des moyens permettant de s'assurer de la libre expression du vote par le Conseil de l'Europe. Les "Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique" indiquent en effet en leur article 10.c [23] :

> Toutes les mesures envisageables devraient être prises dans le système de vote électronique pour éviter les influences destinées à manipuler le vote après son enregistrement, et des dispositions permettant de s'assurer qu'aucune influence de ce type n'a été exercée. [...]
>
> Cette disposition vise à empêcher toute modification non autorisée du vote une fois qu'il a été enregistré. Elle assure la protection du système contre les attaques venant de l'extérieur, mais aussi contre les menaces internes. La vérifiabilité individuelle et la vérifiabilité universelle [...] permettent de détecter toute intervention non autorisée de ce type.

La vérifiabilité d'éligibilité, bien qu'étant une exigence assez naturelle de prime abord, est souvent laissée de côté en pratique : les procédures de vérifiabilité d'éligibilité requièrent de publier une liste des électeurs – il est difficile de vérifier qu'une liste d'électeurs est correcte sans publier celle-ci – et il est généralement problématique, voire illégal, de publier les listes d'électeurs et/ou de personnes ayant voté. En Belgique, dans les bureaux de vote, la vérification d'éligibilité se fait en présence des membres du bureau de vote et d'observateurs. Cette procédure de vérification nous semble offrir des garanties de transparence beaucoup plus fortes que celle que l'on peut réaliser sur des urnes que l'on déménage vers des bureaux de dépouillement et des bureaux principaux de canton. Nous ne chercherons pas ici à proposer des moyens externes de vérification de ce contrôle. (La situation est différente pour les Belges résidant à l'étranger qui votent par courrier : la vérification de l'identité de l'électeur est bien sûr bien plus malaisée dans ce contexte-là, et des techniques pour améliorer cette vérification ont été proposées ailleurs [52].)

Les techniques de vérifiabilité universelle sont systématiques à mettre en œuvre et amènent peu de contraintes. Il s'agit essentiellement de faire fonctionner un logiciel de vérification sur un ensemble de données mises à disposition après le dépouillement de l'élection : ce logiciel va vérifier que le résultat

annoncé est bien en accord avec le contenu d'urnes contenant des votes dont la confidentialité est protégée par des mécanismes cryptographiques. Il est souhaitable que plusieurs logiciels de vérification, produits indépendamment les uns des autres, existent : ils peuvent être produits par des personnes mandatées pour vérifier le bon déroulement des élections électroniques (on pense ici au Collège des experts par exemple), par des partis soucieux de vérifier le résultat des élections, par des acteurs de la société civile, par des observateurs internationaux, etc. Bien que cette vérification nécessite l'usage d'ordinateurs et de logiciels, un aspect central de la vérifiabilité universelle est qu'il n'est demandé à personne de placer sa confiance dans une personne, un logiciel ou un ordinateur spécifique. La vérification peut potentiellement être effectuée par n'importe qui, en se servant de n'importe quel logiciel de vérification (y compris un logiciel réalisé par le vérificateur lui-même s'il en a le souhait), et en se servant de n'importe quel ordinateur. La réalisation d'un logiciel de vérification demande naturellement des compétences spécifiques, mais celles-ci restent limitées : des logiciels de vérification d'élections ont été réalisés dans le cadre de projets de programmation d'étudiants de première année en informatique à l'université. Cette indépendance des personnes, logiciels et machines est centrale : elle permet de détecter des erreurs dès qu'une seule personne honnête (ou intéressée car ayant perdu des votes à cause de ces erreurs) a la possibilité de trouver un logiciel correct et un ordinateur non corrompu par des malwares.

Les techniques de vérifiabilité individuelle demandent la participation active (mais facultative) de l'électeur. Le but étant de garantir à un électeur que son bulletin de vote a bien été dépouillé, il est naturellement nécessaire que l'électeur souhaite vérifier la preuve qui lui est fournie. Le fait que certains électeurs, et même une proportion importante d'entre eux, décident de ne pas effectuer de vérification n'est pas un souci. Un système offrant une vérifiabilité individuelle devra offrir ses preuves aux électeurs sans savoir si ceux-ci les vérifieront. Ceci limite la probabilité de succès de fraudes dans lesquelles le système modifierait uniquement les bulletins de vote des électeurs qui n'ont pas vérifié la présence de leur bulletin. Supposons par exemple que quelqu'un souhaite modifier 1% des bulletins de vote d'une élection, espérant que cela soit suffisant pour avoir un effet utile sans attirer l'attention. Cela signifie que 1% des preuves fournies aux électeurs devront être falsifiées. Mais, dès lors qu'une centaine de personnes vérifient la présence de leur bulletin, même pour une élection comptant des millions d'électeurs, on aura une probabilité importante qu'au moins une personne découvre que son bulletin a été falsifié. Des électeurs qui ne souhaitent pas effectuer de vérification ont aussi la liberté de déléguer cette vérification à des personnes en qui elles ont

confiance.

3.3.1.2 Comment vérifie-t-on une élection ?

Il est aisé de proposer des élections individuellement et universellement vérifiables si on lève la contrainte de confidentialité des votes.

Un exemple simple consiste à rassembler les électeurs dans une salle, à demander à chacun d'annoncer son vote, qui est ensuite inscrit à côté de son nom sur un grand tableau visible de tous, et puis de totaliser les votes. Un tel système présente les qualités requises :

— *Vérifiabilité individuelle :* l'électeur peut vérifier que son vote est bien écrit à côté de son nom sur le tableau.

— *Vérifiabilité universelle :* n'importe qui peut additionner les votes affichés sur le tableau et vérifier que le total annoncé est correct.

Ce système permet même de vérifier l'éligibilité : chaque électeur a pu s'assurer que tous les votes inscrits sur le tableau correspondent bien à des électeurs.

Ce système pose deux difficultés dans un contexte d'élections gouvernementales : il ne garantit pas le secret du vote, qui est requis pour permettre un vote libre, et il ne permet pas à des millions de personnes de voter et de vérifier le résultat de l'élection.

Le problème du nombre d'électeurs peut se résoudre grâce à l'informatique internet : on peut remplacer le tableau sur lequel on inscrit les votes par une page web (cette solution pose la question de savoir si le serveur qui affiche cette page web montrera la même page à tous, mais nous y reviendrons plus tard). C'est pour des raisons similaires que les résultats des élections sont aujourd'hui encodés dans le logiciel Martine (y compris pour le vote papier), logiciel qui permet de transmettre et de consolider le résultat des dépouillements à l'échelle du pays.

Le problème du secret du vote est plus ardu. La solution la plus souvent retenue consiste à avoir recours à la cryptographie pour chiffrer les intentions de vote.[5] Au lieu de publier une liste de noms et de votes, on publie une

5. Une solution alternative consiste à ne pas chiffrer les votes mais à remplacer les noms des électeurs par des pseudonymes de manière telle que chaque électeur est le seul à connaître son pseudonyme [55]. Cette approche soulève cependant des difficultés importantes dans le contexte belge dans la mesure où elle peut sensiblement faciliter la vente de votes : en effet, la possibilité d'approuver autant de candidats qu'on le souhaite dans une longue liste de candidats fournie par un parti rend particulièrement simple de produire un bulletin de vote valide dont on peut être quasiment certain qu'il sera unique, et cette unicité peut alors être employée pour sécuriser une vente ou pour forcer un vote.

liste de noms et de votes chiffrés, ou simplement une liste de votes chiffrés. Si l'électeur reçoit, au moment de voter, une copie de son vote chiffré, il peut vérifier que ce vote est bien publié pour être intégré au décompte. Différentes techniques de cryptographie permettent ensuite de prouver que le résultat proclamé de l'élection est bien cohérent par rapport à l'ensemble des votes chiffrés publiés. Cette dernière vérification peut être effectuée par n'importe qui.

On voit cependant apparaître la difficulté indiquée précédemment : l'électeur n'est maintenant plus en mesure de tracer son vote dans un état lisible, ce qui est bien nécessaire pour garantir le secret du vote, mais est capable de tracer une version chiffrée de son vote. L'électeur peut donc se demander si ce chiffré reflète bien son intention de vote ou si la machine qui a calculé ce vote chiffré n'a pas triché de manière à le remplacer par le chiffré d'un vote différent. Il existe plusieurs méthodes pour répondre à cette interrogation, et nous décrivons ici les deux plus courantes, qui peuvent d'ailleurs être utilisées en combinaison.

La première option est de permettre à chaque électeur, comme c'est déjà le cas actuellement en Belgique, d'invalider son bulletin de vote avant de le mettre dans les urnes. Au moment où l'électeur sort de son isoloir, il dispose déjà à la fois de son bulletin de vote papier, lisible, dont il peut vérifier et confirmer le contenu, et de la version chiffrée de celui-ci, dont il pourra vérifier la présence plus tard sur internet. Si l'électeur a un doute quant à l'honnêteté de la machine de vote qui a calculé ce vote chiffré, il peut décider d'invalider le bulletin et demander que le vote chiffré soit déchiffré, tout en recevant des preuves de l'exactitude de l'opération de déchiffrement. On peut alors vérifier que le vote déchiffré correspond bien à ce qui est imprimé sur le bulletin de vote. Une machine qui aurait triché au moment du chiffrement serait ainsi prise sur le fait. Bien sûr, le bulletin déchiffré ne pourra plus être mis dans les urnes : cela violerait la confidentialité des votes. En revanche, l'électeur satisfait pourra produire un nouveau bulletin de vote et décider de déposer celui-là dans les urnes (ou de l'invalider à nouveau et d'en préparer un troisième).

On notera que cette opération de test ne doit pas spécifiquement être réalisée par des électeurs : des observateurs, experts, ou autres, pourraient tout aussi bien utiliser une machine de vote qui serait un moment inutilisée pour préparer un bulletin de vote et l'invalider ensuite pour vérifier qu'il est correct. L'acte de vote est bien le dépôt d'un bulletin dans les urnes, pas le fait de produire un bulletin sur une machine de vote.

La deuxième option est similaire au processus de risk limiting audit : on pourrait piocher un certain nombre de bulletins de vote papier dans les

urnes, sans savoir qui en est le propriétaire puisque l'urne a déjà été mélangée, et déchiffrer de manière vérifiable le vote chiffré lui correspondant. Cette méthode présente l'avantage de limiter le besoin de test durant les opérations de vote. Mais elle a l'inconvénient d'être plus faible au niveau de la confidentialité des votes : si un électeur décide de publier son bulletin de vote chiffré sur les réseaux sociaux, par exemple, pour démontrer qu'il a bien vérifier la présence de son vote, et si le même bulletin de vote est choisi pour audit, il est possible que cette personne perde le secret de son vote. Il s'agit cependant de circonstances assez extrêmes : on ne déchiffrera qu'une proportion infime des bulletins de vote, et on peut s'attendre à ce que l'immense majorité des électeurs ne fassent pas état de leur bulletin de vote chiffré publiquement.

Dans un cas comme dans l'autre, on dispose de la chaîne de traçabilité des bulletins suivante :

1. L'électeur garde une copie chiffrée de son bulletin de vote, et a confiance que cette copie chiffrée représente bien son vote parce qu'il a pu tester la machine de vote employée, tout comme tous les électeurs qui utilisent la même machine avant et après lui.
2. L'électeur peut vérifier que son bulletin de vote chiffré est bien affiché dans la liste des bulletins de vote qui sont indiqués dans le décompte. Il peut aussi éventuellement vérifier que le nombre de bulletins de vote affichés correspond au nombre de personnes dont on a indiqué qu'elles ont voté.
3. L'électeur peut vérifier que le résultat de l'élection est bien cohérent par rapport à l'ensemble des bulletins de votes chiffrés publiés.

Une difficulté de cette approche est le besoin d'utiliser de la cryptographie pour certaines étapes, qui n'est pas une technologie particulièrement inclusive.

On peut cependant observer des distinctions très similaires à celles que l'on opère dans d'autres domaines de la vie courante où la cryptographie est utilisée : services de messagerie électronique, opérations bancaires, ouverture de voiture sans clé, etc. Pour l'utilisateur, l'usage de la cryptographie est en effet transparent, et l'utilisateur n'a souvent même pas besoin de savoir qu'elle existe, et encore moins comment elle fonctionne. Par contre, cela n'empêche pas l'usage de la cryptographie d'être efficace : les mécanismes employés, en particulier ici, sont tous définis publiquement et examinés par des communautés d'experts de tous bords.

Concrètement, on arrive à une procédure de vote qui prend la forme suivante :

1. Un groupe de gardiens des clés est formé – ils sont souvent au nombre de 5 dans le contexte d'élections gouvernementales. Ces gardiens génèrent et conservent les clés cryptographiques qui sont nécessaires pour produire les preuves que l'ensemble des bulletins de vote soumis par les électeurs est consistant avec le résultat annoncé de l'élection. De plus, les gardiens publient la clé publique qui sera utilisée pour chiffrer les votes de tous les électeurs. Cette clé publique est distribuée dans toutes les machines de vote.
2. Les machines de vote se servent de la clé publique pour chiffrer tous les bulletins de vote produits et fournir aux électeurs une copie du chiffré de leur bulletin ou, en pratique, un numéro de suivi qui est un haché de ce chiffré et qui constitue une empreinte digitale courte de ce chiffré.
3. L'électeur décide s'il accepte le numéro de suivi qu'il reçoit de la machine de vote comme reflétant son vote, ou s'il souhaite vérifier cela et produire un nouveau bulletin de vote.
4. L'électeur qui est satisfait du bulletin de vote et du numéro de suivi qu'il a reçus dépose son bulletin de vote dans l'urne et quitte le bureau de vote avec son numéro de suivi de bulletin.
5. À la fin des opérations de vote, l'ensemble des numéros de suivi des bulletins déposés dans les urnes est rendu public et authentifié via un site web. Chaque électeur peut vérifier que son numéro de suivi est bien présent, et les observateurs peuvent s'assurer (par comparaison par exemple) qu'ils ont bien accès à la même liste de bulletins, et que le nombre de bulletins repris dans la liste est cohérent par rapport aux chiffres de participation à l'élection.
6. Les gardiens se rassemblent pour produire et publier les données qui démontrent que le résultat annoncé de l'élection est bien consistant par rapport à l'ensemble des numéros de suivi de bulletins publiés. Ils font cela sans jamais déchiffrer un seul bulletin de vote déposé dans les urnes, préservant ainsi le secret du vote.
7. Les gardiens déchiffrent aussi l'ensemble des bulletins de vote qui n'ont pas été déposés dans les urnes et dont les électeurs ont demandé la vérification, afin de comparer ce qui est déchiffré avec ce qui est imprimé sur le bulletin papier. Ces données sont aussi rendues publiques afin de permettre aux électeurs de vérifier que le ou les bulletin(s) de vote dont ils ont demandé la vérification ont bien été vérifiés.
8. Toute personne intéressée (membre de partis, observateurs d'élections, membres de la société civiles, personnes privées intéressées, ...) vérifie

que les données publiées par les gardiens confirment effectivement que le résultat annoncé de l'élection est correct.

Les étapes 3, 5 et 7 offrent la vérifiabilité individuelle de l'élection. L'étape 8 offre la vérifiabilité universelle de l'élection.

On observe que l'électeur qui n'est pas intéressé peut simplement ignorer les étapes de vérification et voter comme il le fait dans un système de vote non vérifiable. L'électeur intéressé peut réaliser des tâches qui restent fort simples : décider d'invalider un bulletin de vote et de voter à nouveau, et vérifier qu'un numéro de suivi est bien présent dans une liste de votes publiés. La première tâche n'est pas plus difficile que de voter, et la seconde est équivalente à celle requise pour tracer un colis postal via un site web ou une application de services postaux.

Les tâches des gardiens sont plus exigeantes : le gardien doit être présent au début et à la fin de l'élection et faire fonctionner un logiciel réalisant des opérations cryptographiques. Le logiciel en question n'a rien de secret : dans des systèmes existants, on a vu une série de logiciels produits indépendamment les uns des autres par des personnes intéressées. Néanmoins, les logiciels utilisés par les gardiens génèrent des clés cryptographiques qui doivent rester secrètes. Il importe donc que les logiciels employés soient corrects et soient utilisés sur des machines qui ne sont pas corrompues par des malwares. Le système est cependant conçu de manière à être robuste : même si tous les gardiens sont corrompus, ils restent incapables de falsifier le résultat de l'élection. Par contre, la confidentialité des votes pourrait être mise à mal : si un électeur publie son numéro de suivi de bulletin de vote, la possession d'un nombre suffisamment grand de clés des gardiens pourrait permettre de retrouver le contenu du vote correspondant – ce nombre "suffisamment grand" est choisi à l'avance, au moment de la génération des clés.

La tâche de vérification universelle de l'élection est moins sensible, dans la mesure où elle n'implique aucune clé secrète ou autre information confidentielle. Cependant, elle peut requérir des ressources informatiques non négligeables si l'on souhaite réaliser une vérification complète en un temps limité.

3.3.1.3 De quelles ressources dispose-t-on en matière de vérifiabilité de bout en bout ?

3.3.1.3.1 Littérature académique Les premiers systèmes de votes vérifiables de bout en bout datent du milieu des années 1980, et en particulier de la thèse de doctorat de Josh Benaloh [3]. Les premières techniques étaient

cependant complexes à mettre en œuvre et prohibitives au niveau des ressources de calcul nécessaires.

Une deuxième étape majeure a été passée avec la publication du protocole "optimal" de Cramer, Gennaro et Schoenmakers en 1997 [28] : ce protocole rassemblait tous les outils nécessaires à une élection vérifiable, tout en réduisant les exigences calculatoires au maximum, au moins asymptotiquement.

Les recherches se poursuivent de manière intensive et, depuis le début des années 2000, la communauté de chercheurs actifs sur cette thématique a atteint une taille suffisante que pour que des conférences annuelles soient dédiées à ces technologies de vote – outre les publications classiques dans les grandes conférences de sécurité et cryptographie.

Une convergence assez claire est apparue au niveau des techniques permettant de chiffrer les bulletins de vote et d'obtenir de la vérifiabilité universelle. Par exemple, alors qu'un certain nombre de mécanismes de chiffrement des votes ont été proposés entre les années 1980 et le début des années 2000, on voit que quasiment tous les systèmes déployés ont convergé sur le même mécanisme : le chiffrement d'ElGamal.

Les recherches restent intenses dans un grand nombre de directions. Le vote à distance, et en particulier le vote par internet, posent des questions qui restent difficiles. Les questions de la vérification du fait que le bulletin de vote envoyé reflète l'intention de l'électeur, du secret du vote et de la résistance à la coercition et à la vente de vote sont autant de problèmes en recherche de solutions satisfaisantes. Le vote par courrier attire des efforts de plus en plus intenses aussi, vu son importance croissante en pratique, et grâce à la garantie qu'il offre que le bulletin de vote papier envoyé par l'électeur reflète bien son intention de vote. Bon nombre d'efforts visent aussi à obtenir des solutions de vote vérifiables de bout en bout et préservant le secret du vote dans des contextes où les processus de vote et de dépouillement sont particulièrement complexes – on pense par exemple aux scrutins à vote unique transférable.

3.3.1.3.2 Déploiements Il aura fallu encore une dizaine d'années après la publication du protocole de Cramer, Gennaro et Schoenmakers pour que les techniques s'affinent encore et pour que les ressources informatiques communément accessibles permettent de déployer des élections vérifiables de bout en bout dans des circonstances réelles. Le premier déploiement dans une élection réelle avec plusieurs milliers d'électeurs remonte à 2009, avec l'élection du recteur de l'UCLouvain [2]. Depuis lors, les déploiements se sont généralisés, en tous cas dans le domaine privé où le vote par internet est courant et se réalise dans un contexte moins dangereux au niveau de la

cybersécurité : des milliers d'élections ont eu lieu avec ces mêmes protocoles ou à l'aide de variations de ceux-ci. En Belgique en particulier, certains des systèmes de vote par internet proposés pour les élections sociales annoncent être universellement vérifiables, et offrir un certain degré de vérifiabilité individuelle [57].

Dans le domaine des élections gouvernementales, des systèmes offrant certaines formes partielles de vérifiabilité ont été déployés dans le contexte d'élections par internet en Norvège [36], en Suisse [63], en Estonie [38] et en France [26] par exemple. Des systèmes vérifiables de bout en bout (vérifiabilité individuelle et universelle) ont aussi été déployés dans le contexte de pilotes, en 2009 et 2011 à Takoma Park dans le Maryland [9] et pour les élections dans l'état de Victoria de 2015 en Australie [8]. Dans ces systèmes, le vote se fait en personne (pas à distance) et les bulletins papier sont un ingrédient central. Ceci est cohérent par rapport au rapport "Securing the Vote" des National Academies [47, p. 105] qui suivant une étude intitulée "The future of voting" de la U.S. Vote Foundation [65] insiste sur le fait qu'une expérience importante en matière d'élections vérifiables de bout en bout doit être acquise dans le contexte d'élections en personne avant d'envisager du vote par Internet dans un contexte d'élections gouvernementales.

Ces pilotes ont été des succès mais n'ont pas mené à une adoption permanente, probablement en partie parce qu'ils correspondaient à des projets menés par des équipes académiques plutôt qu'à des déploiements test menés par les fournisseurs de système positionnés pour poursuivre. La technicité importante de toutes ces solutions vérifiables, combinée à une absence de standards, constitue certainement un frein aussi.

Cette situation semble prendre un tournant au cours des dernières années, avec l'introduction du kit de développement logiciel ElectionGuard [32], un projet open source offrant un ensemble de briques cryptographiques documentées et libres, conçues pour être intégrées dans les systèmes commercialisés par des vendeurs de solutions de vote. ElectionGuard a été intégré dans les solutions d'au moins deux vendeurs distincts depuis 2020, et déployé avec succès dans les élections d'au moins quatre comtés.

3.3.1.3.3 Outils informatiques Le déploiement d'élections vérifiables de bout en bout passe généralement par la mise en œuvre de protocoles cryptographiques spécifiques, et en particulier assez différents des protocoles que l'on peut trouver dans les standards internet.

Un certain nombre de librairies sont cependant utilisées dans un nombre croissant d'élections. Nous en mentionnons ici quelques-unes, parmi celles qui

sont open source et qui ont été le plus largement déployées à notre connaissance, et sont encore en usage aujourd'hui.

— Le système Helios propose l'une des plus anciennes implémentations encore en usage aujourd'hui des outils nécessaires à la réalisation d'élections vérifiables de bout en bout. Il est notamment utilisé chaque année depuis 2010 pour les élections de l'IACR, l'association internationale des chercheurs en cryptographie.

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

— Verificatum offre des librairies de chiffrement et d'anonymisation de bulletins de vote (mix-net) vérifiables de bout en bout, utilisées dans des élections (municipales et nationales) en Norvège, Estonie et Espagne.

https://www.verificatum.org

— Le système Belenios inclut des librairies cryptographiques qui ont été utilisées dans de nombreuses élections privées et, récemment, dans certaines parties du système de vote par internet utilisé pour le vote des Français depuis l'étranger lors des législatives de 2022.

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

— Le SDK ElectionGuard inclut des librairies qui ont été intégrées dans les solutions de plusieurs vendeurs et notamment déployées dans des élections à Fulton (Wisconsin), Preston (Idaho), Inyo County (Californie) et à College Park (Maryland).

https://www.electionguard.vote/

— La Poste suisse a rendu public et open source les librairies cryptographiques utilisées dans son système de vote par internet qui est déployé dans des programmes pilotes d'élections des cantons de Basel-Stadt, St. Gallen et Thurgau.

https://gitlab.com/swisspost-evoting

Il est à noter que, si ces librairies contiennent les ingrédients cryptographiques permettant de déployer des élections vérfiables de bout en bout, elles ne sont pas forcément déployées dans des systèmes offrant cette forme de vérifiabilité.

3.3.1.3.4 Cadre légal Nous avons mentionné plus haut la référence explicite à la vérifiabilité individuelle et universelle dans les recommandations en matière de vote électronique du Conseil de l'Europe [23].

Au niveau des législations nationales, le projet le plus avancé et celui qui a soulevé le plus d'intérêt de notre part est celui de la Suisse, et en particulier l'Ordonnance de la Chancellerie Fédérale 161.116 sur le vote électronique [11], qui définit, notamment en son Article 5, les formes de vérifiabilité individuelle et universelle requises pour l'homologation de systèmes de vote électronique en Suisse – dans les limites associées au vote par internet. Nous pensons que la structure de cette ordonnance offre une base importante qui pourrait être utilisée dans d'autres pays, dont la Belgique, dans le cadre du vote avec preuve papier.

3.3.1.4 Pour aller plus loin...

La notion de vérifiabilité de bout en bout est décrite et discutée dans un essai à destination d'un lectorat non expert technique dans l'essai : "End-to-end verifiability" par Josh Benaloh et ses co-auteurs [4].

L'enregistrement d'un workshop de deux jours décrivant ElectionGuard et son intégration dans le "Verity Scanner" de la société Hart Intercivic est disponible à l'adresse :

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

3.3.2 Une stratégie de vérifiabilité E2E pour la Belgique

La vérifiabilité de bout en bout et les risk limiting audits sont des technologies très complémentaires. Il n'est dès lors pas étonnant que leurs modes de déploiement soient très différents.

Une première différence centrale porte sur les acteurs impliqués dans ces deux stratégies de vérification.

— Dans le contexte des RLAs, les acteurs centraux sont ceux impliqués dans le dépouillement et le scanning des bulletins papier, qui produisent les manifestes nécessaires au RLA, les personnes qui assurent le suivi et l'authenticité des bulletins de vote, et les personnes qui réalisent le RLA proprement dit sur base des manifestes. Il s'agira typiquement de quelques centaines de personnes par circonscription, qui devront être formées à des procédures relativement techniques (comme c'est le cas dans les bureaux de dépouillement actuellement).

— Dans le contexte de la vérifiabilité E2E, les acteurs seront l'entièreté des votants, à qui l'on proposera de vérifier la correction et la comptabilisation de leurs bulletins de vote, ainsi qu'un petit nombre de personne, typiquement moins d'une dizaine, qui seront impliquées dans la gestion de clés cryptographiques, assistés par des opérateurs du système informatique qui réalise les calculs nécessaires et publie les résultats, et assistent les personnes souhaitant vérifier ces résultats.

On voit aussi que le type de tâche est très différent :

— Dans le contexte des RLAs, le principal effort consiste à réaliser un suivi précis des bulletins de vote papier, produire des manifestes détaillés, et inspecter des bulletins de vote papier.

— Dans le contexte de la vérifiabilité E2E, le principal effort consiste à informer l'ensemble des électeurs sur les possibilités de vérification, à encourager des acteurs externes et des candidats à s'impliquer dans la vérification indépendante des décomptes, et à faire fonctionner une infrastructure informatique publiant les données de l'élection avec l'aide d'une petite dizaine de personnes impliquées dans la gestion de clés cryptographiques.

La mise en œuvre de la vérifiabilité E2E passera elle aussi par des pilotes, mais qui viseront des objectifs sensiblement différents de ceux associés aux RLAs. Le test et le dimensionnement des procédures sera vraisemblablement nettement plus simple : à part un besoin d'ordinateurs plus puissants, le passage d'un test à 1000 électeurs vers un déploiement pour 1 million d'électeurs ne changera pas énormément de choses (alors qu'on aura des différences fondamentales dans le cas d'un RLA). Néanmoins, des efforts nettement plus importants seront nécessaires pour concevoir la communication autour du processus d'audit, adressée vers les votants et vers les associations, candidats ou partis susceptibles de fournir des outils de vérification indépendants.

3.3.2.1 Se baser sur l'expérience acquise ailleurs

Tout comme dans le cas des RLAs, un certain nombre d'expériences existent sur lesquelles se baser pour construire des élections vérifiables E2E. Cependant, contrairement aux RLAs, la documentation publique de ces expériences est nettement plus limitée, et nous n'avons pas trouvé de "guide du déploiement d'élections vérifiables E2E " détaillé.

Cependant, alors que l'expérience en matière de déploiement de RLAs semble inexistante en Belgique, une expérience a été acquise par un large public belge dans le cadre d'élections privées : plusieurs universités belges ont

systématiquement élu leurs recteurs au suffrage universel à l'aide de systèmes vérifiables de bout en bout, et ce depuis 2009, exposant des centaines de milliers d'étudiants à la procédure de vérification de la publication de leur bulletin de vote chiffré. Un certain nombre d'employés d'entreprises belges ont aussi acquis une expérience similaire dans le cadre des élections sociales, ou d'élections d'ordres professionnels. Ce faisant, ces élections ont permis la création, en Belgique, d'une expérience utile en matière d'organisation de la tâche des gardiens des clés pour la génération de clés cryptographiques et la production de preuves de correction du résultat d'élections.

Il ne faudra cependant pas négliger les différences entre l'écosystème associé à l'organisation d'une élection à l'aide d'une infrastructure informatique privée, dédiée à un public associé à une institution spécifique, et l'écosystème d'élections gouvernementales, basé sur une infrastructure publique et visant un public nettement plus large et hétérogène.

La dimension de l'élection et des bulletins de votes présents dans les élections gouvernementales belges pose aussi des questions en termes de ressources informatiques nécessaires pour l'hébergement des données de l'élection et le calcul des preuves de correction des résultats. Nous aborderons ces questions plus bas.

3.3.2.2 Temporalité

3.3.2.2.1 Mettre en place un groupe de travail La première étape que nous recommandons consiste à créer un groupe de travail en charge d'organiser la vérifiabilité E2E des élections.

Le rôle de ce groupe de travail inclura de définir un certain nombre d'éléments centraux.

— La stratégie de sélection des gardiens des clés : il s'agira de déterminer leur nombre et la manière dont on les choisira. La contrainte principale est de s'assurer qu'ils n'auront aucun intérêt à s'allier pour violer la confidentialité des votes, et qu'ils pourront être présents de manière fiable pour la génération des clés avant l'élection et pour la production des preuves en fin d'élection.

— La stratégie de conception de l'infrastructure informatique nécessaire à la vérifiabilité : hébergement et publication des données électorales, ressources de calcul nécessaires pour mener les opérations cryptographiques requises.

— La stratégie de développement du logiciel des gardiens et de vérification des données de l'élection. Idéalement, on souhaiterait trouver différents

acteurs produisant des logiciels de manière indépendante sur base d'une spécification bien établie. La production de logiciels de référence open source est certainement utile aussi.

— La stratégie de communication vis-à-vis des électeurs pour les inviter à contribuer à la vérifiabilité individuelle de l'élection.

— Le contenu et la stratégie de communication vis-à-vis des observateurs d'élections susceptible de réaliser les vérifications associées à la vérifiabilité universelle.

— La stratégie d'évaluation par des tiers de la procédure de vérification d'élections, afin de s'assurer que les tâches proposées, si elles sont correctement effectuées, garantissent réellement la correction du résultat de l'élection.

3.3.2.2.2 Simuler le processus en dimensions réduites En parallèle avec les activités du groupe de travail, et en collaboration avec celui-ci, il pourra être utile de simuler le processus de vérification E2E dans des dimensions réduites.

Cela permettra de comprendre comment organiser au mieux les cérémonies impliquant les gardiens des clés, de tester les procédures de publication des données d'audit, et d'inviter des acteurs intéressés à réaliser des démarches de vérification.

Ces tests permettront aussi de mieux mesurer les besoins en termes de ressources de calcul, infrastructure de stockage et de capacités de réseau.

Il pourra être utile d'effectuer au moins les premières simulations avec un petit nombre de participants, et ce afin de faciliter l'expression et l'écoute d'éventuelles incompréhensions, la recherche de solution à des erreurs qui auraient lieu et de faciliter un débat sincère menant à une amélioration des procédures.

3.3.2.2.3 Premier pilote Lorsqu'une confiance suffisante dans l'organisation du processus de vérification E2E aura été acquise via des simulations, un premier pilote en conditions réelles pourra être organisé.

La procédure au niveau des gardiens et de la vérifiabilité universelle ne devrait pas sensiblement changer par rapport aux simulations. Par contre, la nouveauté importante sera l'implication d'électeurs dans des conditions réelles.

Nous viserions ici la réalisation de réaliser ce premier pilote dans un petit nombre (1 à 3) de bureaux de vote. Il s'agira principalement de tester les mécanismes d'information aux électeurs et de les inviter à participer à la

vérification individuelle, en leur donnant l'occasion d'exprimer des retours sur le processus.

Les différents processus seront ajustés en fonction des leçons apprises durant le pilote.

Une facilité offerte par la vérifiabilité E2E est qu'elle s'insère presque entièrement en parallèle du processus de vote normal, et n'interfère donc pas avec celui-ci, contrairement aux RLAs qui, en manipulant les bulletins papier, pourraient avoir un impact sur un éventuel re-dépouillement de bulletins de vote qui serait requis à la suite d'une plainte.

3.3.2.2.4 Second Pilote Un second pilote sera très vraisemblablement utile afin d'affiner le processus. En fonction de la maturité du système, on testera encore sur un petit nombre de localités, ou visera tous les bureaux de vote électroniques d'une circonscription complète.

L'avantage de viser un large public sera de pouvoir ouvrir l'information des électeurs à des canaux de communication différents : on pourra envisager d'utiliser des clips télévisés, des annonces radio ou des articles de presse.

À ce stade, et en particulier si ce pilote se déroule avant la certification des résultats, il sera important d'inclure des observateurs pour les cérémonies opérées par les gardiens, selon des critères similaires à ceux utilisés dans les bureaux de dépouillement.

3.3.2.2.5 Généralisation Sur base de pilotes réussis, un déploiement généralisé des élections vérifiables E2E pourra être réalisé.

3.3.2.3 Éléments d'organisation

Nous discutons ici un certain nombre d'éléments techniques génériques pour la mise en œuvre d'élections vérifiables de bout en bout, qui pourront servir à alimenter les réflexions du groupe de travail chargé d'organiser la mise en œuvre du processus. Ces éléments seront naturellement affinés et révisés en fonction des choix du groupe de travail et des propositions du ou des partenaires et vendeurs impliqués dans la mise en œuvre de la solution.

3.3.2.3.1 Publication des données des élections Un ingrédient central dans le déploiement d'élections vérifiables de bout en bout est la publication des données à vérifier. Celle-ci requiert un soin spécifique si l'on souhaite permettre une vérification effective des données de l'élection.

La simple publication des données sur un site web, si elle peut être utile pour de l'archivage, peut permettre au site web de tricher significativement : un site web corrompu (parce qu'il aurait été piraté par exemple) pourrait afficher un ensemble de bulletins de vote correct aux électeurs, et communiquer un ensemble de votes différents aux gardiens, amenant les gardiens à valider un résultat basé sur des bulletins différents de ceux qui ont été vérifiés par les électeurs. Qui plus est, même si un gardien s'aperçoit d'une différence à un moment donné, il sera vraisemblablement très difficile de prouver quoique ce soit, dans la mesure où il n'y aura pas moyen de différentier un gardien qui ment d'un opérateur de site web qui triche.

Une approche naturelle pour résoudre cette difficulté serait de produire une signature digitale des données de l'élection. Ceci permet, si deux séries de données distinctes sont signées et publiées, et si cela est découvert, d'être en mesure de prouver que le processus de publication de ces données est corrompu. On se heurte cependant à deux difficultés :

1. Comment permettre à un électeur de s'assurer de l'authenticité de la signature fournie ? Cela demande de disposer d'une version authentique de la clé de vérification. Mais, si l'électeur obtient la clé de vérification depuis le site web corrompu, le site corrompu fournira une fausse clé de vérification, qui validera les données d'élection incorrectes mais ne pourra pas servir de preuve. Qui plus est, si l'on souhaite permettre une vérification depuis un site web, le code de vérification de la signature sera fourni par le site web aussi, et déclarera valide n'importe quelle signature, indépendamment de la validité réelle. À ce jour, les navigateurs ne disposent malheureusement d'aucun mécanisme permettant de vérifier indépendamment une signature sur des données fournies par un site web. Passer par une app spécifique distribuée via un app store pour smartphone ou tablette peut fournir une solution partielle à ce problème. Mais cela limite en pratique l'accessibilité de la solution et impose de faire confiance aux gestionnaires de l'app store quant à l'authenticité de l'app qu'il va distribuer.
2. Si l'on suppose que les signatures sont valides et correctement vérifiées, comment détecter un site web qui distribue des données d'élections distinctes à différentes personnes ? Le seul moyen de découvrir ce type de manipulation est de réaliser la comparaison des données signées. C'est certainement une opération possible mais, en l'absence de facilité pour réaliser de telles comparaisons, on peut douter qu'elle sera réalisée à une échelle importante en pratique.

Une solution partielle au second problème est de passer d'une simple

signature des données de l'élection à des signatures par un ensemble d'observateurs, ou à un protocole de signature distribuée ne pouvant être calculée que par un ensemble d'observateurs. Cette approche est certainement intéressante en pratique [29, 39], ne serait-ce que parce qu'elle évite qu'un attaquant qui vole une unique clé de signature puisse mettre à mal la sécurité de l'élection, mais fait reposer la confiance sur le groupe d'observateurs choisis.

Une manière d'ouvrir le cercle des observateurs consiste à encourager la publication de copies des données d'élection signées par des observateurs provenant d'organismes internationaux effectuant des observations d'élections, par des partis, ou par d'autres acteurs de la société civile. Ces acteurs auraient pour tâche de vérifier l'authenticité des données d'élection signées qu'ils reçoivent et de les rendre publiques – on peut demander à de tels acteurs de vérifier l'authenticité de la clé de vérification de signature par plusieurs moyens indépendants. Une telle approche permet d'une part aux électeurs de vérifier la présence de leur vote dans une liste publiée par l'acteur de leur choix : un électeur pourra se sentir en confiance en vérifiant la présence de son vote dans une liste publiée par le parti politique de son choix, ou auprès d'un organisme international en qui il a confiance. Cela permet aussi à ces observateurs de surveiller l'autorité qui signe les données de l'élection, en comparant leurs données respectives pour s'assurer qu'elles sont identiques. Toute différence entre des versions portant des signatures valides fournirait une preuve de la corruption de l'autorité publiant les données de l'élection.

Bien sûr, on peut imaginer que des acteurs malicieux pourraient aussi vouloir publier de fausses données d'élection. Ceci peut arriver que l'on encourage la publication de copies ou non, tout comme n'importe qui peut annoncer haut et fort la victoire de n'importe quel candidat d'une élection. Il restera cependant facile de démontrer que ces acteurs sont malicieux, dans la mesure où ils ne seront pas en mesure de fournir une version des données qu'ils publient qui serait signée par l'autorité en charge de la publication des données de l'élection.

Le principal défi pratique de cette approche sera sans doute d'identifier et de convaincre différents acteurs indépendants de publier les données d'élections.

À propos des blockchains Un certain nombre de personnes ont proposé de publier des données d'élection sur une blockchain. Nous pensons qu'il s'agit globalement d'une approche à éviter dans un contexte d'élections gouvernementales.

L'attrait pour la blockchain vient du fait qu'elle est construite comme un registre dans lequel on publie des informations dont on souhaite qu'elles restent disponibles et inaliénables ce qui, à première vue, peut correspondre aux souhaits que l'on a pour des données d'audit d'une élection.

Cette inaliénabilité tient cependant au processus de construction des blocs. Dans les blockchains ouvertes (permisionless), comme celles utilisées pour les crypto-monnaies comme le Bitcoin, l'idée fondamentale est d'avoir un mécanisme sans autorité centrale, et d'établir un processus de réconciliation, ou de consensus, entre des acteurs qui auraient des vues distinctes sur les données enregistrées sur la chaîne (de manière simplifiée : la personne possédant la plus "grande" chaîne respectant certaines règles "gagne").

Une élection gouvernementale est un processus totalement différent : on a une autorité en charge d'organiser l'élection, selon des lois bien établies. Cette autorité définit la liste des candidats qui apparaissent sur les bulletins de vote, les moments où l'on peut voter, publie les résultats de l'élection, etc. Et cette autorité est tenue à une certaine transparence : elle doit notamment permettre à des observateurs de vérifier qu'elle se comporte conformément aux règles en vigueur. Cette autorité occupe donc une position centrale, et l'on souhaite diriger toute l'attention des observateurs vers elle, pour s'assurer que l'élection s'est bien déroulée selon les règles en vigueur.

Utiliser une blockchain pour publier les données d'une élection fait exactement le contraire : on dilue les responsabilités de publication qui incombent à une autorité bien identifiée vers un ensemble d'ordinateurs contrôlés par des personnes généralement anonymes et situées n'importe où dans le monde, qui ont des intérêts potentiellement très différents de ceux des citoyens du pays où l'élection a lieu, et qui n'ont généralement pas à répondre de leurs actes dans le pays qui organise les élections.

La question se pose évidemment différemment pour une blockchain fermée (permissioned) gérée par des acteurs bien identifiés par l'autorité de l'élection. Une telle blockchain peut être, dans certains contextes, un choix permettant d'offrir une résistance accrue à des intrusions. Mais ce n'est certainement pas la seule option. [6]

3.3.2.3.2 Cérémonie de génération des clés Comme indiqué plus haut, la première étape du processus d'élection vérifiable de bout en bout consiste en la génération de clés cryptographiques par un groupe de gardiens.

6. Le rôle potentiel des blockchains dans les élections a fait couler beaucoup d'encre. Un exemple de discussion de ce rôle se trouve dans Scientific American : https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/.

Ces gardiens seront choisis comme des personnes fiables et ayant peu d'intérêt à collaborer entre elles pour violer la confidentialité des votes. On peut penser à des magistrats, des notaires, ou même à des représentants de partis qui auraient beaucoup à perdre si leurs électeurs apprenaient qu'ils n'ont pas respecté une condition aussi fondamentale que le secret des votes dans des élections.

On peut en choisir un nombre quelconque, et définir un quorum de gardiens devant être présents pour compléter le processus de production des données de vérifiabilité. Un choix possible est de nommer cinq gardiens et de déterminer qu'un minimum de trois d'entre eux sont nécessaires pour produire les données requises.

Ce quorum de trois personnes parmi cinq veut dire que :

— même si deux gardiens disparaissent, perdent leur clé, refusent de participer au processus, sont victimes d'un accident ou sont indisponibles pour une autre raison, il restera possible de réaliser le processus de production des données en entier ;

— si trois gardiens se coalisent et décident de tricher ensemble, ils pourront déterminer les votes des électeurs dont ils auraient copie des numéros de suivi de bulletin.

D'autres choix qui sont parfois proposés sont de demander un quorum de 2 parmi 3, ou de 4 ou 5 parmi 6 ou 7 personnes. On précisera que ce quorum ne concerne que la confidentialité des votes : même une coalition de tous les gardiens restera incapable de falsifier les preuves de correction des résultats d'élections.

Le premier acte de ces gardiens est de générer des clés. Pour cela, ils auront chacun besoin d'un laptop ou d'une tablette munie d'un logiciel adéquat. Le laptop et le logiciel pourront être fournis par les organisateurs de l'élection, mais il pourrait être préférable que le gardien se les procure de manière indépendante. En effet, dans la mesure où le secret des votes dépend de ce laptop et de ce logiciel, il peut être avantageux d'utiliser des appareils et des logiciels indépendants pour limiter les risques qu'une même vulnérabilité soit présente dans tous les laptops ou dans tous les logiciels utilisés. Bien sûr, cela implique que le gardien soit en mesure d'accéder à un laptop raisonnablement sécurisé et à un logiciel de bonne qualité.

Les appareils des gardiens communiqueront ensuite entre eux, typiquement pendant quelques secondes, pour générer les clés et créer le niveau de redondance nécessaire pour que les opérations de vote puissent être réalisées par le quorum choisi. Ces communications se feront typiquement via un réseau local isolé, avec l'aide d'un gestionnaire des données de l'élection qui

collectera les informations publiques communiquées par chaque gardien. Les gardiens veilleront, à la fin de la procédure de génération des clés, à ce que les données publiques rassemblées soient bien cohérentes avec celles qu'ils ont produites et utilisées, et ce afin de se défendre contre un gestionnaire qui se ferait passer pour un ou plusieurs gardiens, ou modifierait d'autres paramètres du système.

Les données publiques font l'objet d'une première publication, et seront acheminées vers toutes les machines de vote. Les gardiens, pour leur part, conservent leur laptop et leurs clés secrètes, éventuellement stockées sur des appareils de stockage portable sécurisés (clés USB sécurisées, ou autres).

3.3.2.3.3 Production des bulletins électroniques et numéros de suivi La production des bulletins de vote électroniques et des numéros de suivi des bulletins est une opération assez directe : la machine de vote, sur base de la clé publique produite par les gardiens et de l'intention de vote indiquée par l'électeur, produit une version chiffrée du bulletin de vote. Ce chiffré sera mis à disposition des gardiens et des personnes qui vérifient la correction du dépouillement, dans le contexte de la vérifiabilité universelle du système.

Les électeurs reçoivent aussi un numéro de suivi de leur bulletin électronique. Ce numéro de suivi pourrait être le chiffré lui-même mais ce chiffré est assez volumineux, ce qui le rend peu utilisable comme un numéro de suivi. Pour cette raison, le numéro de suivi du bulletin sera plutôt calculé comme un haché de ce chiffré, c'est-à-dire comme une empreinte unique de ce chiffré calculé à l'aide d'une fonction cryptographique de hachage, ce qui permet d'obtenir un résultat beaucoup plus court, même si sa longueur reste non négligeable : typiquement une cinquantaine de lettres et chiffres, qu'il importera de présenter de manière à faciliter la lecture.

Ce numéro de suivi sera imprimé par la machine de vote et transmis à l'électeur afin de lui permettre de vérifier que son bulletin de vote est bien inclus dans le dépouillement.

L'électeur peut aussi souhaiter vérifier le fait que ce numéro de suivi correspond bien à son intention de vote. Pour ce faire, plutôt que d'introduire son intention de vote réelle et de déposer le bulletin de vote imprimé dans l'urne, l'électeur introduira une intention de vote quelconque sur la machine à voter, vérifiera que le bulletin imprimé reflète bien le vote exprimé, prend le numéro de suivi, et signifie au Président du bureau de vote son souhait de vérifier que la machine de vote produit des numéros de suivi valides. Le bulletin de vote et le numéro de suivi sont alors marqués, éventuellement

à l'aide d'un cachet, comme correspondant à un vote de test. L'électeur garde les documents originaux, tandis qu'une copie ou une photo de ceux-ci est conservée dans le bureau de vote. Au moment du dépouillement, il sera demandé aux gardiens de démontrer, de manière vérifiable, que le numéro de suivi qui a été imprimé était bien consistant avec le vote imprimé en clair. Ces preuves seront rendues publiques avec les données de l'élection, et l'électeur pourra se servir du numéro de suivi reçu pour les vérifier.

Ce processus explique pourquoi le bulletin de vote testé ne peut pas être aussi déposé dans les urnes : le processus de vérification de la validité du numéro de suivi passe par la publication, visible pour tous, du contenu du bulletin de vote en question, ce qui n'est évidemment pas acceptable pour un bulletin de vote déposé dans les urnes. On observe cependant, et c'est un élément central du protocole, que la machine à voter doit imprimer le bulletin et le numéro de suivi *avant* de savoir si le bulletin sera déposé dans les urnes ou vérifié. De la sorte, elle ne pourra pas adapter sa stratégie en essayant de ne tricher que pour des bulletins qui seront déposés dans les urnes.

Bien évidemment, un électeur peut aussi découvrir que le bulletin de vote papier qui a été imprimé par la machine de vote ne correspond pas à l'intention de vote qu'il pense avoir exprimée. Dans ce cas, le même processus d'invalidation du bulletin de vote est suivi, et l'électeur est invité à voter à nouveau. Il est important que le Bureau de vote prenne acte de ce doute dans l'honnêteté de la machine de vote, et que cette information face partie du reporting du fonctionnement du système, afin de déterminer s'il y a lieu de réaliser un audit approfondi de certaines machines de vote.

3.3.2.3.4 Audit des bulletins de vote À la fin des opérations de vote, les données correspondant aux bulletins de vote chiffrés et vérifiés sont publiées. Chaque électeur peut ainsi vérifier que le numéro de suivi correspondant au bulletin qui a été déposé dans les urnes se trouve bien dans la liste des bulletins qui seront comptabilisés, et que le ou les numéro(s) de suivi du ou des bulletin(s) dont il a demandé la vérification est/sont bien repris dans la liste des bulletins à vérifier.

Concrètement, les sites offrant aux électeurs ses possibilités de vérification pourront inviter les électeurs à introduire les 5 premiers caractères du numéro de suivi de leur bulletin, et le site web répondra en fournissant l'ensemble des numéros de suivi qu'il possède et qui commencent par ces 5 caractères. L'électeur vérifiera ensuite que son numéro de suivi est bien listé.

Un exemple de site web offrant ce type de vérification est proposé par la

société Enhanced Voting. La figure 3.1 montre un exemple de publications de données produites à l'aide d'ElectionGuard pour l'élection générale de novembre 2023 à College Park, Maryland. Il est actuellement possible de vérifier la présence de son bulletin de vote à l'adresse :

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

On peut, à titre d'exemple, introduire les séquences `ØD1C`, `2E3E` ou `6AC7` pour voir s'afficher les numéros de suivi complets, que l'électeur peut vérifier sur base de la copie qu'il a reçue au moment de son vote. Certains des bulletins ont été déposés dans l'urne, auquel cas on ne voit pas leur contenu. D'autres ont été invalidés en vue de vérification, et on voit alors apparaître le contenu du bulletin. On notera que les numéros de suivi sont affichés comme une unique longue séquence, ce qui n'aide pas l'électeur à vérifier que cette séquence est correcte. La séquence utilise aussi la représentation hexadécimale, qui n'est pas la plus compacte, et qui peut mener les électeurs à confondre le chiffre zéro et la lettre "O". De nombreuses variations sont possibles, notamment : utiliser un alphabet et des chiffres dont on exclut les symboles potentiellement ambigus, afficher les symboles par paquets de 5, éventuellement sur deux lignes, éventuellement entourés de cadres numérotés pour aider les comparaisons, ...

En cas de problème, l'électeur est invité à contacter une autorité compétente, vraisemblablement au niveau de la circonscription où des personnes auront été formées pour enregistrer la communication d'électeurs qui pensent que leur numéro de suivi est manquant, et conserveront des traces dans le PV de l'élection.

Il importera d'être en mesure de détecter des plaintes frivoles : il s'agira de s'assurer que l'électeur a correctement essayé de vérifier la présence de son numéro de suivi et, au besoin, de lui demander de produire les documents originaux produits par la machine à voter, qui seront imprimés sur du papier spécifique afin de compliquer la tâche de personnes qui essaieraient de produire de faux numéros de suivi, et pourront aussi porter un cachet apposé dans le bureau de vote.

Comme pour tout incident dans une élection, il s'agira aussi d'en mesurer la portée pour déterminer si un impact sur le résultat de l'élection est possible. En cas de doute, on pourra notamment inviter les électeurs à confirmer qu'ils ont bien pu vérifier la présence de leur bulletin de vote, ce qui pourrait indiquer que la plainte d'un bulletin manquant correspond à un problème isolé. Une vérification des procédures appliquées dans les bureaux de vote peut aussi aider à comprendre l'origine du bulletin de vote manquant, et à déterminer l'importance d'un éventuel problème.

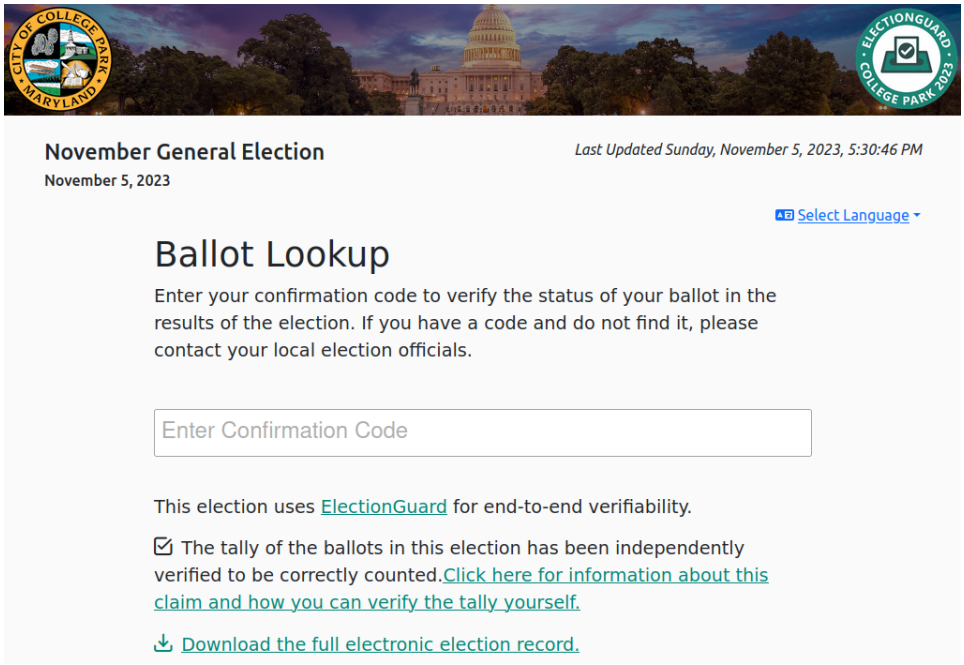

FIGURE 3.1 – Publication des données de vérification produites à l'aide d'ElectionGuard pour l'élection générale de novembre 2023 à College Park, Maryland

3.3.2.3.5 Production des preuves de correction du résultat de l'élection Dès lors qu'une confiance satisfaisante a été acquise sur le fait que les bons numéros de suivi ont bien été publiés, tant pour les bulletins de vote à dépouiller que pour ceux à tester, on rassemble les gardiens pour la deuxième étape de leur tâche : la production des preuves de correction des résultats de l'élection.

Il s'agira pour cela de confirmer la validité de l'ensemble des données de l'élection qui ont été publiées, et d'inviter chaque gardien présent à se servir de son laptop et de sa clé secrète pour lancer le protocole de production des preuves de correction du résultat de l'élection, ainsi que des preuves de la validité des numéros de suivi produits pour les bulletins dont la vérification a été demandée.

La vérification de l'ensemble des données de l'élection sera vraisemblablement une tâche trop ardue que pour être réalisée en quelques minutes sur un laptop standard. Cette vérification ne nécessite cependant pas d'employer de clés secrètes, et peut être réalisée par n'importe qui. Les gardiens peuvent

ainsi se reposer sur des tiers de leur choix pour effectuer ces vérifications. La production des preuves proprement dite est en revanche une tâche très simple, et elle pourra sans difficulté être réalisée sur les laptops des gardiens.

Ces preuves sont ajoutées aux données de l'élection, et publiées afin de permettre à des tiers de les vérifier aussi, réalisant ainsi la vérifiabilité universelle de l'élection.

Une fois que les résultats de l'élection ont été définitivement validés, toutes les clés secrètes des gardiens pourront être détruites, afin de limiter encore les risques que ces clés arrivent un jour dans de mauvaises mains.

3.3.3 Évaluation de la complexité calculatoire

Là où un RLA requiert un effort de manipulation de bulletins papier, les techniques E2E requièrent surtout un effort en termes de ressources de calcul, qui peuvent devenir prohibitives dans certains contextes.

Nous évaluons ici une approche possible pour réaliser les opérations cryptographiques discutées dans les sections précédentes. Ce n'est certainement pas la seule approche possible, et bon nombre d'autres solutions, parfois nettement moins gourmandes, existent.

Notre choix est de nous baser sur les techniques les mieux connues, et qui ont été le plus largement déployées à ce jour. Si elles s'avèrent être suffisamment efficaces pour le contexte belge, elles nous semblent donner un choix approprié. L'usage de techniques calculatoirement plus efficace vient en effet souvent avec certains inconvénients aussi :

— des techniques plus complexes sont davantage source d'erreurs lors de leur mise en œuvre,

— des techniques plus complexes résultent en code plus difficile à auditer pour des tiers,

— des techniques plus complexes reposent généralement sur des hypothèses plus fortes, qui risquent donc davantage de s'avérer erronées,

— des techniques plus complexes rendent plus ardue la réalisation de code permettant de vérifier les données d'audit publiées lors d'une élection.

Il n'en reste pas moins que le déploiement des techniques que nous envisageons ici aura lieu au plus tôt dans 5 ans. D'ici là, la maturité de différentes techniques aura certainement évolué, de même que les librairies d'outils cryptographiques disponibles.

Concrètement, nous suivons au maximum les protocoles cryptographiques qui sont aujourd'hui présents dans ElectionGuard, dont la version 2.0 a été

publiée en août dernier [32], et qui a été utilisé dans plusieurs élections gouvernementales aux USA au cours des 3 dernières années. Les protocoles présents dans ElectionGuard sont une évolution de ceux qui étaient déjà présents dans le système de Cramer, Gennaro et Schoenmakers de 1997 [28], et qui sont utilisés dans des systèmes comme Helios [2] et Belenios [25]. La spécification d'ElectionGuard est publique, et les implémentations de référence sont publiées sous licence open source MIT.

Nous ne reproduisons pas ici les détails du système, mais reprenons ses principales caractéristiques, en développant celles qui sont les plus utiles au système envisagé ici. Nous développons aussi les quelques éléments liés à des spécificités belges qui ne sont actuellement pas disponibles dans ElectionGuard.

3.3.3.1 Briques de base et choix des paramètres

ElectionGuard construit sa cryptographie autour de deux éléments de base :

— Un groupe cyclique $\mathbb{G}$ dans lequel le problème décisionnel de Diffie-Hellman [7] est supposé difficile à résoudre. ElectionGuard utilise un sous-groupe d'ordre q d'un groupe multiplicatif $\mathbb{Z}_p^*$, où p est un nombre premier de 4096 bits et q est un nombre premier de 256 bits.

— La fonction de hachage à clé HMAC telle que définie dans le standard FIPS 198-1 et réalisée sur base de la fonction SHA-256 définie dans le standard FIPS 180-4.

Il est possible d'utiliser ElectionGuard avec d'autres groupes, et l'usage d'un premier p de 3072 bits accélérera le fonctionnement des protocoles, probablement sans baisse significative de leur sécurité [7].

3.3.3.2 Protocoles utilisés

3.3.3.2.1 Chiffrement Le groupe $\mathbb{G}$ est utilisé pour chiffrer les choix des électeurs à l'aide du système de chiffrement d'ElGamal [33]. Sur base d'un générateur g de $\mathbb{G}$, une clé secrète x est générée de manière distribuée par les gardiens, et une clé publique $y = g^x$ est calculée, suivant un protocole proche de celui proposé par Pedersen [51]. Pour chaque candidat présent sur le bulletin, on calculera un chiffré $(c, d) = (g^r, y^{r+v})$ du choix de l'électeur v, caché à l'aide du nombre aléatoire r choisi uniformément dans $\mathbb{Z}_q$. Le

7. Voir https://www.keylength.com/ par exemple.

choix v vaudra 1 si l'électeur a choisi le candidat correspondant au chiffré et 0 si l'électeur n'a pas choisi le candidat (les cases de tête de liste sont simplement traitées comme un candidat supplémentaire que l'on met à 1 dès qu'un candidat de la liste est sélectionné). Chaque chiffré produit par ElectionGuard compte donc 8192 bits.

Une caractéristique importante du chiffrement d'ElGamal tel qu'employé ici est son homomorphisme additif : si je multiplie terme à terme les chiffrés de deux choix v_0 et v_1 chiffrés respectivement avec les nombres aléatoires r_0 et r_1, j'obtiens un chiffré de $v_0 + v_1$ à l'aide de $r_0 + r_1$. Ceci permet de totaliser les votes sans devoir les déchiffrer : si je veux savoir combien de voix un candidat a obtenu, je peux multiplier entre eux tous les chiffrés produits par les électeurs pour ce candidat, et j'obtiens un unique chiffré du nombre de voix obtenues, que je peux alors déchiffrer sans risque de violer le secret des votes.

Le fait de ne pas déchiffrer les bulletins de vote individuels, formés de l'ensemble des chiffrés produits pour chacun des candidats présents sur le bulletin, pose cependant une difficulté : une machine malveillante pourrait par exemple chiffrer $v = 1000$ pour donner 1000 voix à un candidat via un unique bulletin.

3.3.3.2.2 Preuves à divulgation nulle

Ceci est empêché en produisant, pour chaque chiffré, une preuve à divulgation nulle que ce chiffré chiffre réellement 0 ou 1 et pas une autre valeur. La divulgation nulle garantit que la preuve ne révèle en rien si la valeur chiffrée est 0 ou est 1 : elle prouve uniquement qu'il s'agit de l'une de ces deux valeurs.

ElectionGuard utilise pour cela une preuve basée sur le protocole de Chaum-Pedersen [12] utilisée sous une forme disjonctive suivant la technique de Cramer, Damgård et Schoenmakers [27], et rendue non-interactive en suivant l'heuristique de Fiat-Shamir [34].

Concrètement, sur base d'un chiffré $(c, d) = (g^r, y^{r+v})$ où $v \in \{0, 1\}$, on calcule les éléments suivants :

$$\begin{gathered}
(a_0, b_0) = (g^{s_0}, y^{s_0 + v t_0}) \qquad (a_1, b_1) = (g^{s_1}, y^{s_1 + (v-1) t_1}) \\
e = \mathrm{HMAC}(K; \texttt{0x21}, c, d, a_0, b_0, a_1, b_1) \\
e_0 = (e - t_1)(1 - v) + t_0 v \qquad e_1 = t_1(1 - v) + (e - t_0)v \\
f_0 = s_0 - e_0 r \qquad f_1 = s_1 - e_1 r
\end{gathered}$$

où s_0, s_1, t_0, t_1 sont des éléments aléatoires choisis dans $\mathbb{Z}_q$, K est un haché de la description et des clés publiques de l'élection, et `0x21` est un identifiant de preuve. La preuve elle-même est formée de (e_0, e_1, f_0, f_1), soit une longueur

de 1024 bits, et la manière de la vérifier est reprise dans la spécification d'ElectionGuard [32, p. 32].

Ces preuves ne suffisent cependant pas à démontrer qu'un bulletin de vote est valide : un bulletin belge n'est valide que si l'électeur n'a sélectionné des candidats (ou la case de tête) qu'au sein d'un unique parti. Ceci peut être réalisé en construisant une nouvelle preuve qui, à ce stade, n'est pas incluse dans ElectionGuard, mais est basée sur des techniques très similaires.

On peut procéder en 2 étapes. Tout d'abord, on multiplie entre eux tous les chiffrés qui ont été calculés, liste électorale par liste électorale. Si on a m listes électorales sur le bulletin, on obtiendra donc m chiffrés $(c_1, d_1), \ldots, (c_m, d_m)$. Grâce aux preuves que les chiffrés que l'on a multiplié entre eux chiffrent tous 0 ou 1, on sait que, dès lors qu'un candidat (ou la case de tête) a été sélectionné dans la liste i, le chiffré (c_i, d_i) sera le chiffré d'une valeur non nulle. On aura donc un bulletin valide si et seulement si au maximum l'un des chiffrés de la liste $(c_1, d_1), \ldots, (c_m, d_m)$ chiffre une valeur non nulle.

Si l'on suppose que $(c_i, d_i) = (g^{r_i}, y^{r_i+v_i})$ pour $i \in \{1, \ldots m\}$, avec v_i non nul uniquement pour l'index ℓ, on peut calculer la preuve de la manière suivante.

$$
\begin{gathered}
(a_i, b_i) = (g^{s_i}, y^{s_i+v_i t_i}) \text{ pour } i \in \{1, \ldots, m\} \\
e = \mathrm{HMAC}(K; \texttt{0x51}, c_1, d_1, \ldots, c_m, d_m, a_1, b_1, \ldots, a_m, b_m) \\
e_i = i(t_\ell - e)/\ell + e \text{ pour } i \in \{1, \ldots, m\} \\
f_i = s_i - e_i r_i \text{ pour } i \in \{1, \ldots, m\}
\end{gathered}
$$

où les valeurs s_i et t_i sont sélectionnées aléatoirement dans $\mathbb{Z}_q$ et K est défini comme précédemment. La preuve est formée des e_i et f_i, et aura donc une longueur de $512m$ bits.

Pour la vérifier, on recalculera $(a'_i, b'_i) = (g^{f_i} c_i^{e_i}, y^{f_i} d_i^{e_i})$ pour tout $i \in \{1, \ldots, m\}$, on calculera

$$
e = \mathrm{HMAC}(K; \texttt{0x51}, c_1, d_1, \ldots, c_m, d_m, a'_1, b'_1, \ldots, a'_m, b'_m)
$$

et on vérifiera que $(0, e)$ et tous les points (i, e_i) se trouvent bien sur une même droite dans $\mathbb{Z}_q \times \mathbb{Z}_q$.

3.3.3.2.3 Formation des bulletins chiffrés Un bulletin de vote sera donc formé de :

— autant de chiffrés ElGamal qu'il y a des candidats sur les bulletins, auxquels on ajoute un chiffré par liste électorale (pour la case de tête),

— autant de preuves 0-1 qu'il y a de chiffrés sur le bulletin

— une preuve qu'une seule liste électorale, au maximum, a été sélectionnée par l'électeur.

La taille d'un bulletin comptant m listes et n candidats sera donc de $8192(m+n) + 1024(m+n) + 512m = 9216(m+n) + 512m$ bits. Sur de grands bulletins belges, on verra que m pourra être de l'ordre de 15 et n de l'ordre de 300, ce qui donne une taille de 2910720 bits,

soit environ 355 kB. Pour 8 millions de bulletins de vote, [8] cela représente un volume légèrement inférieur à 3 TB, un volume qui peut aujourd'hui être stocké sur un disque dur d'une valeur de moins de 100 euros.

Si besoin, cette taille pourra être considérablement réduite en choisissant un autre type de groupe : un passage à des courbes elliptiques sur 256 bits réduirait par exemple la taille des bulletins d'un facteur entre 5 et 6. L'usage d'autres types de preuves à divulgation nulle peut encore réduire cette taille d'un facteur 2 à 3 [31]. Il serait aussi possible, dans le contexte envisagé ici, de remplacer les chiffrés ElGamal par des multi-engagements de Pedersen [50], ce qui amènerait encore des gains sensibles en termes de volumes de données.

Nous n'élaborons pas davantage sur ces techniques : notre objectif dans ce rapport est d'établir que l'approche proposée est réaliste en termes de ressources informatiques en employant des techniques largement standard, plutôt que d'établir les limites fort mouvantes de ce qu'il est possible de réaliser avec les techniques les plus avancées.

Le numéro de suivi du bulletin de chaque électeur pourra quant à lui être calculé comme un haché de l'ensemble des chiffrés du bulletin (avec un certain nombre d'informations de contexte), soit 256 bits avec SHA-256 que l'on peut imprimer sous la forme d'une cinquantaine de caractères. Le stockage de 8 millions de numéros de suivi

représente alors 250 MB, soit l'équivalent de quelques dizaines de photos prises par un smartphone récent.

3.3.3.2.4 Preuve de la correction du résultat

Si l'on dispose d'un ensemble de bulletins de vote dont on connaît la validité grâce aux preuves à divulgation nulle décrites précédemment, il devient simple d'obtenir des chiffrés du résultat des élections (un chiffré par candidat) en multipliant entre eux, candidat par candidat, les chiffrés présents sur chaque bulletin.

8. Il y avait 7,989,802 électeurs inscrits et 7,218,633 bulletins déposés aux élections fédérales belges de 2019. https://elections.fgov.be/sites/default/files/inline-files/CK_TauxParticip.xlsx

On peut alors demander aux gardiens de produire une preuve à divulgation nulle que ces chiffrés du résultat de chaque liste et de chaque candidat est bien consistant avec le résultat de l'élection. ElectionGuard fait cela simplement à l'aide d'une preuve de Chaum-Pedersen.

3.3.3.2.5 Publication des données d'audit Il sera essentiel, pour la vérifiabilité individuelle, de publier l'ensemble des hachés des bulletins de vote, afin que les électeurs puissent vérifier que leur bulletin est bien enregistré, sans avoir été modifié, pour être inclus dans le dépouillement. Même à l'échelle de toute la Belgique, cette publication reste de l'ordre d'un petit site web, tant en termes de volume de données à stocker qu'en termes de trafic pour permettre aux électeurs de vérifier la présence de leur numéro de suivi.

Cette légèreté est particulièrement bienvenue pour faciliter la réplication de cette liste de numéros de suivis vers différents partis, observateurs officiels, ou acteurs de la société civile, qui voudraient en héberger une copie.

La publication de l'ensemble des bulletins chiffrés et des preuves, à l'échelle de la Belgique, est par contre plus exigeante et pourrait générer des coûts importants si un engouement pour l'accès à ces données survient. Par exemple, si l'on prend le coût d'envoi de données vers internet chez les principaux fournisseurs de service cloud actuels, qui tournent aujourd'hui autour de 0.08 euro par GB, on arrive à un coût de 240 euros pour les 3 TB indiqués. Ce coût peut naturellement inviter à envisager l'usage de protocoles cryptographiques moins standard mais moins exigeants en volumes de données et/ou restreindre la diffusion du jeu de données complètes.

Il peut y avoir plusieurs autres raisons de restreindre la diffusion de ce jeu de données complètes :

— La vérification de ces données a surtout du sens si l'on peut confirmer qu'elles sont uniquement celles des électeurs et qu'il n'y a pas eu de bourrage d'urnes par exemple. Les listes d'émargement n'étant pas publiées, il n'est pas possible, pour n'importe quel citoyen, de vérifier que le résultat de l'élection est correct sur base de cela uniquement – ce qui n'empêche pas, bien sûr, que cette vérification a du sens.

— La publication des données présente un risque pour la confidentialité de certains votes. En effet, si des électeurs rendent public leur numéro de suivi (en supposant qu'ils publient bien le leur et pas celui de quelqu'un autre) et si, en raison d'un bug ou d'avancées cryptanalytiques, il devient possible de casser le mécanisme de chiffrement utilisé, il pourrait devenir possible d'apprendre le contenu de certains

votes. Cela n'est certainement pas la seule manière de violer le secret du vote dans un système de vote (qu'il soit électronique ou papier), ni vraisemblablement la plus simple, mais c'est un vecteur possible.

3.3.3.3 Ressources calculatoires

Le coût calculatoire des opérations de calcul réalisées par les gardiens pour la génération des clés et pour le calcul des preuves de validité du résultat est dérisoire : on parle de quelques secondes sur un laptop standard.

On observe cependant des coûts plus importants pour la préparation des bulletins de vote et pour la vérification de la validité de ceux-ci. La préparation des bulletins de vote est certainement un élément critique : on ne souhaite pas que les opérations cryptographiques nécessaires pour chiffrer les bulletins de vote et prouver leur validité vienne ralentir l'ensemble du processus.

Nous avons testé cela en réalisant une implémentation des mécanismes de chiffrement et de preuves discutés plus haut. Notre implémentation Python a été interprétée avec Python 3.11 et se repose sur la librairie gmpy2 (v. 2.2.0) pour les calculs sur les grands entiers.

Nous l'avons testée sur un unique cœur d'un laptop relativement ancien équipé d'un processeur i5-7300U datant de Q1 2017, qui donne probablement une idée raisonnable de la vitesse que l'on pourra espérer trouver sur un processeur, généralement bas de gamme, que l'on trouvera dans une machine de vote qui sera réalisée dans quelques années.

Nos tests ont été effectués pour deux bulletins de l'élection fédérale de 2019 :[9]

— Le bulletin du Luxembourg, qui compte 11 listes avec entre 7 et 10 candidats pour un total de 106 candidats, qui est le plus petit bulletin de ces élections,

— Le bulletin du Hainaut, qui compte 15 listes avec entre 7 et 28 candidats pour un total de 348 candidats, qui est le plus grand bulletin de ces élections.

Les résultats de la table 3.2 montrent que, même pour le plus grand bulletin présent lors de ces élections et le paramètre de sécurité le plus élevé

9. Les dimensions des bulletins varient sensiblement et peuvent être plus grands ou plus petits dans d'autres élections. Ainsi, le bulletin de vote au parlement flamand pour la circonscription d'Anvers en 2019 listait 447 candidats, et le bulletin de vote au parlement bruxellois de 2019 en comptait 771. Le bulletin de vote au parlement wallon de la circonscription de Dinant-Philippeville de 2019 en comptait 72.

Circonscription	$\|p\| = 3072$	$\|p\| = 4096$
Luxembourg	81 ms	96 ms
Hainaut	209 ms	295 ms

TABLE 3.2 – Temps de calcul pour le calcul du chiffré et des preuves de validité d'un bulletin de vote des élections de 2019

Circonscription	$\|p\| = 3072$	$\|p\| = 4096$
Luxembourg	0.66s	1.13s
Hainaut	2.14s	3.33s

TABLE 3.3 – Temps de calcul pour la vérification de la validité d'un bulletin de vote des élections de 2019

avec un premier de 4 096 bits, le temps de calcul du chiffrement et des preuves reste intérieur à 300 ms.

Sachant que la majeure partie de ce calcul peut être fait avant que l'électeur ne sélectionne ses préférences sur sa machine de vote, il est clair que cette opération de chiffrement sera essentiellement transparente.

Et si le souhait est de chiffrer les bulletins en direct au fur et à mesure qu'ils sont scannés, on voit que le rythme de chiffrement est en ligne avec celui des plus rapides scanners à haute vitesse du marché. En cas de besoin, le calcul est très aisément parallélisable.

Ces faibles temps de calcul viennent en bonne partie du fait que tous les protocoles décrits plus haut ne calculent des exponentiations que dans deux bases fixées à l'avance, ce qui permet de tirer avantage de précalcul. Ce n'est malheureusement pas le cas pour la vérification de la validité des bulletins de vote, où des exponentiations en base variable sont nécessaires. Les temps de vérification mesuré pour un bulletin produit avec les mêmes paramètres de sécurité sont repris dans la table 3.3. On y voit que le temps de vérification des plus gros bulletins peut monter jusqu'à 3 secondes avec le paramètre de sécurité le plus élevé, mais peut aussi rester largement sous la seconde pour la plus petite circonscription et un paramètre de sécurité standard.

Si l'on souhaite vérifier 8 millions de bulletins de vote en comptant un temps de vérification moyen de 2 secondes par bulletin, on arrive à 185 jours de calcul. Sur la machine d'un utilisateur privé moyen, il s'agit probablement

d'un calcul prohibitif. Cependant, ce calcul étant essentiellement répétitif et parallélisable, il devient tout à fait réaliste de le réaliser rapidement sur des machines de calcul équipées de 128 à 256 cœurs de calcul qui sont courantes dans n'importe quelle infrastructure professionnelle et qui se louent chez des fournisseurs de services cloud autour de 5 euros/heure pour des machines équipées de 128 vCPU.

Étant donné qu'il n'y a pas d'urgence majeure à réaliser la vérification de la validité des bulletins, ces résultats nous semblent suffisants que pour démontrer la faisabilité de l'approche. Néanmoins, comme indiqué précédemment, il est possible d'accélérer ces vérifications considérablement en adoptant d'autres techniques : le passage à des groupes de points sur courbes elliptiques accélérera considérablement tout le processus, il existe des techniques de "batching" pour accélérer la vérification des preuves, et il est bien sûr aussi possible d'adopter des techniques de preuves plus avancées, permettant des vérifications plus efficaces. Celles-ci ne sont cependant pas (encore) employées dans les outils couramment déployés aujourd'hui, raison pour laquelle nous les avons exclues à ce stade.

3.4 Conclusion

Nous avons étudié dans ce chapitre la faisabilité de déployer les deux techniques de vérification des résultats d'élections les plus prometteuses, techniques qui ont émergé dans le paysage des élections gouvernementales au cours des 15 dernières années, et dont l'adoption est encouragée par le Conseil de l'Europe.

Il est évident que l'adoption de ces technologies amène un coût supplémentaire : ce coût est tant financier qu'humain, dans la conception du système, dans le test des procédures de vérification et dans leur mise en œuvre concrète.

Ce coût doit être comparé à celui que pourrait avoir pour notre pays une manipulation effective des résultats de l'élection, qui pourrait dans un certain nombre de cas être extrêmement difficile à détecter dans le système actuel, faute d'audit suffisamment robuste, et mener à élire les mauvaises personnes. Il y a aussi lieu de mettre dans la balance le coût qu'auraient pour notre pays des allégations de manipulations de résultats, que ces manipulations aient réellement eu lieu ou non : la mise en œuvre des techniques proposées ici permettraient d'offrir une réponse claire et documentée à ces allégations.

Partie 4
Conception de BeVoting II

4.1 Introduction

Ce chapitre développe le concept du système BeVoting II, proposé en réponse à la demande de la Direction des élections du SPF intérieur de :

> "définir comment l'actuel système de vote électronique avec preuve papier peut évoluer en terme de hardware mais également en terme de vérifiabilité."

Les évolutions proposées sont ainsi guidées par les deux éléments développés dans les chapitres précédents :

— le bilan des qualités et faiblesses identifiées dans le système actuel, mises en regard des évolutions en terme de matériel disponible au cours des 15 dernières années,

— les évolutions technologiques en matière de vérifiabilité qui ont eu lieu depuis l'introduction du système de vote électronique actuel, et qui sont à présent intégrées dans les recommandations internationales en matière d'élections électroniques.

Les évolutions proposées visent ainsi à intégrer les neuf objectifs principaux relevés en section 2.5, associés à la gestion du matériel et de logiciel, l'accessibilité du système de vote, la transparence et la sécurité du logiciel, la vérifiabilité et l'audit des élections, et le reporting sur le fonctionnement du système.

Quand différents choix techniques semblent acceptables, nous chercherons à ne pas fermer des options inutilement, afin de garder le marché le plus ouvert possible.

4.2 Architecture du système BeVoting II

Plaçant l'électeur au centre du système, nous décrivons le système BeVoting II en partant de l'électeur, dont nous suivons le bulletin au travers du processus de décompte, pour terminer par les questions liées à la maintenance et à l'audit.

4.2.1 La machine de vote

L'électeur commence par s'identifier à l'entrée du bureau de vote, où il reçoit un "token" (actuellement une carte à puce, mais nous reviendrons plus cet aspect plus bas) lui permettant d'indiquer à la machine de vote à quelles élections il peut participer (communales, chambre, Europe, etc.). Il se rend ensuite dans un isoloir où il accède à une machine de vote.

4.2.1.1 Fonctionnalités

Cette machine de vote expose actuellement à l'électeur :

— Un lecteur de carte à puce dans lequel l'électeur introduit la carte lui permettant d'activer la machine de vote et d'afficher les bulletins de vote qui le concernent.

— Un écran tactile suffisamment grand que pour afficher, en une seule fois, l'ensemble des listes proposées sur le bulletin et les candidats d'une liste, afin de permettre à l'électeur d'indiquer ses choix et, le cas échéant, de les confirmer.

— La sortie de l'imprimante qui imprime le bulletin de vote reprenant les choix de l'électeur.

Le bulletin papier produit a la forme d'un ticket de caisse, et contient d'une part un résumé du bulletin de vote lisible par l'électeur et reprenant l'ensemble des choix effectués, et d'autre part un code QR facilitant le scanning du bulletin, qui contient lui-aussi l'intention de vote (entre autres informations), et sera utilisé pour comptabiliser le vote.

Aucune des technologies de vérifiabilité n'impose un changement fondamental dans ces fonctionnalités. Plusieurs améliorations possibles ressortent cependant des rapports du Collège des experts ainsi que des évolutions constatées sur le marché.

1. L'impression du bulletin papier pourrait être réalisée sur un papier plus grand, de format standard, ce qui le rendrait plus facile à lire, à vérifier et à manipuler.

2. L'accès à la machine pour des personnes à visibilité limitée, ou dont la mobilité permet difficilement d'indiquer leurs choix via l'écran tactile, est complexe.
3. La logistique associée aux cartes à puce des électeurs est une difficulté récurrente.

Nous élaborons ces différents points ci-dessous.

4.2.1.1.1 Impression du bulletin papier Un électeur belge a régulièrement la possibilité d'exprimer des préférences pour plusieurs dizaines de candidats : à titre d'exemple, dans la circonscription d'Anvers, 7 listes proposaient 37 candidats sur le bulletin de vote des élections à la chambre en 2019, et un bulletin de vote pouvait donc potentiellement lister 37 candidats sélectionnés. Ce chiffre montait à 72 candidats présents sur plusieurs listes lors des élections de 2019 au Parlement bruxellois.

Ces choix sont actuellement imprimés sur un papier thermique au format ticket de caisse (80mm de large), ce qui ne facilite pas la relecture, d'autant plus quand l'électeur doit relire ses choix pour trois élections ayant lieu simultanément. Une alternative serait d'imprimer sur du papier de format standard (A4). À titre d'exemple la figure 4.1 donne une idée du format d'un bulletin de vote tel qu'utilisé dans le système VSAP du comté de Los Angeles [1]. Ce bulletin rassemble les réponses données par l'électeur à 59 questions différentes. On observe une structure très similaire à ce que l'on a en Belgique : le bulletin de vote reprend uniquement les choix effectués par l'électeur, sous un format lisible par celui-ci, et ajoute par ailleurs deux codes QR qui sont utilisés dans le scanning du bulletin.

4.2.1.1.2 Accessibilité de la machine de vote Un pilote a eu lieu en 2019 dans les communes d'Alost et de Malines afin d'offrir la possibilité de voter à des personnes malvoyantes ou aveugles, au moyen d'écouteurs et de boîtiers de sélection spécifiques. Ce test est évidemment encourageant, et la possibilité d'intégrer de tels outils est un avantage important de l'usage de machines de vote.

Le comté de Los Angeles a mis en place une approche novatrice dans son système VSAP [2] – Voting Solution for All People – déployé depuis 2019. En marge du système de vote, une application "Interactive Sample Ballot"

1. Source : https://vsap.lavote.net/wp-content/uploads/2017/09/BMD-Ballot-Specification-Deck-for-RFI-Response.pdf
2. https://vsap.lavote.gov/

Ballot Style
1234 Abc
Serial Number
12345
Precinct Number
12345678

2018
Nov. 6

Los Angeles County

OFFICIAL
General Election Ballot

Governor
Roy D. Bernard AC

Lieutenant Governor
Rita A. Ruggeri 3D

Secretary of State
Corin Sams 3H

Controller
Tania Rose Kimball 3K

Assoc. Justice-Supreme Ct: Harper Samuel
Yes 3M

Assoc. Justice, Ct of Appeal, 2nd Appellate Dist., Div 1: Harry Alfred Till
No 3N

Assoc. Justice, Ct of Appeal, 2nd Appellate Dist., Div 2: Wynn Brandon
No 3Q

Superior Ct Judge, Office No. 61
Nicky Van Daal B4

State Measure 1
Yes BO

State Measure 2
No BP

State Measure 45
No BS

State Measure 46
Yes B3

State Measure 47
Yes BW

State Measure 48
Yes C1

County Measure P
No DO

County Measure O
No C9

County Measure A
No CC

County Measure J
No PO

County Measure N
No CI

Central Basin Municipal Water Dist.
Nowell Townsend CK
Bunny Berger AK

Water Replenishment Dist. of Southern California
Chen Huang CK
Clara Rosales AK
Len Pemberton R4

Governor
Roy D. Bernard AC

Lieutenant Governor
Rita A. Ruggeri 3D

Secretary of State
Corin Sams 3H

Controller
Tania Rose Kimball 3K

Assoc. Justice-Supreme Ct: Harper Samuel
Yes 3M

Assoc. Justice, Ct of Appeal, 2nd Appellate Dist., Div 1: Harry Alfred Till
No 3N

Assoc. Justice, Ct of Appeal, 2nd Appellate Dist., Div 2: Wynn Brandon
No 3Q

Superior Ct Judge, Office No. 61
Nicky Van Daal B4

State Measure 1
Yes BO

State Measure 2
No BP

State Measure 45
No BS

State Measure 46
Yes B3

State Measure 47
Yes BW

State Measure 48
Yes C1

County Measure P
No DO

County Measure O
No C9

County Measure A
No CC

County Measure J
No PO

County Measure N
No CI

Central Basin Municipal Water Dist.
Nowell Townsend CK
Bunny Berger AK

FIGURE 4.1 – Bulletin de vote fictif du comté de Los Angeles

de préparation de bulletins de vote est proposée, que les électeurs peuvent installer, généralement sur leur smartphone.

Cette application permet à l'électeur qui le souhaite d'accéder aux bulletins de vote à l'avance sur leur téléphone ou leur ordinateur, et de compléter ce bulletin de vote. À la fin du processus, l'application prépare un code QR reprenant la sélection réalisée par l'électeur (celui-ci peut bien sûr produire autant de codes QR qu'il le souhaite). L'application ne permet par contre pas de voter : il ne s'agit pas de vote à distance.

Cependant, si l'électeur arrive muni de ce code QR dans son bureau de vote, il peut présenter ce code à un lecteur intégré à la machine de vote, qui va alors préparer un bulletin conforme au contenu de ce code. L'électeur reste entièrement libre de vérifier et de modifier le bulletin autant qu'il le souhaite sur la machine de vote, avant de lancer l'impression.

Nous voyons plusieurs bénéfices importants à cette approche :

— Elle permet à l'électeur exposé à de grands bulletins de vote de réfléchir posément au vote qu'il souhaite transmettre, sans pour autant devenir une forme de vote à distance qui poserait des problèmes de confidentialité ou de vente de votes.

— Elle permet à l'électeur qui éprouve des difficultés à se servir de machines de vote d'utiliser ses propres outils d'accessibilité, adaptés à ses besoins spécifiques, et généralement présents sur son smartphone ou son ordinateur, pour préparer son bulletin. Ceci est certainement plus simple que de devoir s'adapter aux outils d'accessibilité présents sur la machine de vote, que l'électeur doit découvrir au moment de voter.

— Elle permet potentiellement de réduire les files aux bureaux de vote : les électeurs qui ont préparé leur bulletin de vote à l'avance pourront voter plus rapidement le jour de l'élection.

On peut bien sûr être préoccupé par les risques d'incitation à voter dans un sens particulier qu'une telle application amène, ainsi que par l'usage d'un smartphone dans un isoloir. Nous pensons qu'il y a ici une balance des risques intéressante entre une accessibilité accrue et des risques qui sont probablement présents de toute manière aussi longtemps que l'on laisse l'électeur muni d'un smartphone entrer dans un isoloir. L'équilibre de cette balance peut être évalué dans l'esprit de la discussion de l'Article 40 des recommandations du Conseil de l'Europe [23] :

> f. [...] Il convient de déterminer dans chaque cas la nature et l'étendue des mesures de protection à appliquer, et d'établir un juste équilibre entre certains aspects différents, mais de même importance, par exemple entre l'impératif sécuritaire et la volonté

de disposer d'un système facile à utiliser par les électeurs. En pareil cas, le souci d'assurer la commodité d'utilisation ne doit pas l'emporter sur la nécessité de garantir un haut niveau de sécurité, mais peut constituer un élément dans le choix des mesures de sécurité à adopter. Les mêmes considérations peuvent s'appliquer dans une situation où l'on privilégierait une amélioration minime de la sécurité au détriment de l'utilisabilité.

On notera par ailleurs que l'impression du bulletin de vote sur un papier de format standard peut aussi offrir des bénéfices pour des électeurs qui se servent d'une assistance pour la lecture : il sera vraisemblablement plus facile de se servir d'une application présente sur un smartphone pour lire une page standard que pour lire un ticket.

4.2.1.1.3 Choix du "token" utilisé par l'électeur pour activer la machine de vote Le besoin de scanner un code QR sur la machine de vote pour préremplir un bulletin de vote apporte une nouvelle complexité à la machine de vote, qui devrait alors être munie d'un scanner de codes QR.

Ce nouveau scanner pourrait cependant arriver en remplacement de la carte à puce actuellement utilisée pour activer les machines de vote. Une solution alternative serait d'activer les machines de vote à l'aide d'un autre code QR, qui serait produit lors de l'identification de l'électeur. Plutôt que de fournir une carte à puce à l'électeur, susceptible de pannes ou de faux contacts dans les lecteurs, et dont il est difficile de dire, par simple inspection, à quels bulletins de vote elle donne accès, on pourrait fournir à l'électeur un papier imprimé contenant de manière lisible les intitulés des élections auxquelles il permet de participer, ainsi qu'un code QR qui pourra être scanné par la machine de vote.

Outre le fait de dispenser de la gestion des cartes à puce et de leurs lecteurs, cette solution permettrait de réduire les confusions et problèmes techniques qui sont régulièrement relevés dans les rapports des collèges des experts [14, Sec. 3], [17, Sec. 6.1], [18, Sec. 4.2.2.7].

4.2.1.2 Choix du matériel

Les machines de vote représentent une part importante du coût d'un système de vote, et Smartmatic indique en avoir fourni approximativement 22850 à la Belgique pour les élections de 2019 [3]. Avec le prix des urnes et

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

des machines de Président de Bureau, on arrive à un coût de l'ordre de 50 millions d'euros, en suivant les prix de 2016 pour les 4338 bureaux de vote indiqués [49].

4.2.1.2.1 Unité centrale Les machines de vote du système de vote électronique actuel sont formées à partir d'un mini-PC classique, sur lequel fonctionne une distribution Ubuntu adaptée aux besoins. Ce PC ne contient pas de composant de stockage (disque dur, etc.) permettant d'installer un système d'exploitation : le système d'exploitation est chargé en mémoire depuis une clé USB au moment du démarrage de la machine. Ce PC ne dispose d'aucune connexion réseau non plus. Ces spécificités visent à réduire le plus possible la surface d'attaque pour une personne souhaitant compromettre le système. Il dispose par contre d'interfaces permettant de connecter un écran, un lecteur de carte et une imprimante. Il est aussi inséré dans un boîtier fermé, ce qui permet de garder les différents éléments du système raccordés entre eux, de faciliter le déplacement et le stockage des machines, et de compliquer l'accès à une personne qui souhaiterait corrompre la machine.

Depuis l'appel d'offre pour les machines actuelles il y a près de 15 ans, bon nombre de d'évolutions ont eu lieu au niveau du matériel informatique. Pour en citer quelques-unes :

— Les Chromebooks, une gamme de laptops et tablettes introduite en 2011 basée sur une distribution linux et qui a trouvé un développement croissant, en particulier dans le secteur éducatif, en raison notamment de prix d'achat réduits [4].

— Le marché des tablettes "grand public" est apparu, avec notamment l'introduction de l'iPad en 2010.

— Le marché des ordinateurs à carte unique "grand public" est aussi apparu, avec notamment la mise sur le marché du Raspberry Pi [5] en 2012, souvent commercialisé pour quelques dizaines d'euros et équipé de connexions HDMI pour un écran et USB pour une imprimante, un lecteur de cartes ou un scanner.

Toutes ces nouvelles opportunités sont attrayantes : elles offrent des perspectives de réductions de coûts des machines, tant pour l'achat que pour le stockage de celles-ci.

Elles présentent cependant un certain nombre d'obstacles aussi. Sur un marché qui reste en forte évolution, il reste difficile d'établir si ces obstacles

4. https://en.wikipedia.org/wiki/Chromebook
5. https://en.wikipedia.org/wiki/Raspberry_Pi

seront réellement bloquants en l'état du marché au moment où une acquisition sera réalisée. La présente discussion a pour objectif de mettre en avant différents critères qui permettront de répondre à cette question, qui devra in fine être tranchée avec les fournisseurs qui s'engageront à offrir les caractéristiques ergonomiques et de sécurité requises, ainsi qu'à assurer la maintenance du système.

1. Nécessité d'un écran de taille suffisante. Il est nécessaire de pouvoir afficher l'ensemble des candidats présents sur une liste – soit jusqu'à 72 candidats pour le parlement bruxellois en 2019 – et ce de manière bien lisible et en laissant un espace suffisant pour qu'on puisse sélectionner les noms sans erreur. Ce critère semble exclure bon nombre de tablettes "bon marché" et un certain nombre de laptops. À titre de point de repère, les machines de vote utilisées actuellement proposent un écran de 17 pouces de diagonale, ce qui correspond à la taille des plus grands écrans de laptops proposés de manière standard aujourd'hui.
2. Maintenance du système d'exploitation. Bon nombre d'appareils sont fournis avec un système d'exploitation propriétaire, ce qui limite les possibilités de mises à jour de la sécurité du système à ce que le fabriquant fournira. À titre d'exemple, Samsung a annoncé en 2022 une extension à 5 ans de la durée des mises à jour de sécurité de la plupart de ses tablettes haut de gamme (série S) [6] ce qui reste clairement trop court. Google a pour sa part annoncé en 2023 une extension à 10 ans des mises à jour pour les Chromebooks [7]. La situation peut se présenter différemment dans le monde des ordinateurs à carte unique : on observe par exemple que le Raspberry Pi 2, qui a été mis sur le marché en 2015, reste certifié sous Ubuntu Core 2022 qui vient avec des mises à jour de sécurité jusqu'en 2032, soit une durée de support du système d'exploitation d'au moins 17 ans [8].
3. Robustesse face aux faillites des fabricants. Se baser sur une plate-forme physique très spécifique (processeur exotique, etc.) expose potentiellement à de plus grandes difficultés en cas de faillite du fabriquant, dans la mesure où le passage à une nouvelle plate-forme imposera de plus grands changements dans les logiciels du système. Le choix d'une

6. 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
7. https://blog.google/outreach-initiatives/education/automatic-update-extension-chromebook/
8. https://ubuntu.com/download/raspberry-pi

machine dont il existe des dizaines d'équivalents proches offre certainement plus de robustesse.

4. Flexibilité du hardware. Les ports USB et les connexions Bluetooth et Wifi sont des vecteurs de choix pour l'intrusion dans un système informatique. Idéalement, on souhaiterait que la machine ne soit pas équipée de Bluetooth et Wifi, mais ces modes de connexion sont souvent soudés au système. À défaut, on souhaitera les désactiver au niveau du firmware de la machine, ce qui pourra poser un problème sur certains systèmes où l'accès à ce type de configuration est restreint par le fabriquant. On visera certainement aussi à ce que les pilotes permettant au système d'exploitation de faire fonctionner ces moyens de communications ne se trouvent pas sur la machine. À nouveau, dans un système propriétaire, ce ne sera pas forcément possible. Concernant les ports USB, ils sont généralement nécessaires pour configurer la machine de vote et pour connecter les périphériques requis (imprimante, lecteur de cartes ou de codes.) Outre des protections physiques (qu'il est malheureusement souvent aisé de contourner), une configuration stricte du système d'exploitation permettra de restreindre les appareils qui pourront être raccordés sur ces ports.
5. Possibilité de démarrage sécurisé. Il est central de veiller à ce que les machines de vote fonctionnent bien avec le logiciel de vote qui a été préalablement certifié, et pas avec un logiciel qui aurait été modifié par une personne malveillante. Les machines actuelles se protègent contre ce type d'attaque en ne disposant pas de mémoire non volatile qui permettraient à un attaquant d'installer un système d'exploitation classique (pas de disque dur, pas de carte SD) qui imiterait et remplacerait celui qui a été certifié. Les machines fonctionnent alors au départ de clés USB initialisées dans une infrastructure sécurisée. Ceci n'est pas forcément possible sur toutes les plate-formes matérielles, où des mémoires non-volatiles sont souvent soudées par le fabriquant. Une alternative partielle, qui n'était pas disponible il y a 15 ans mais qui a acquis une maturité depuis lors et commence à être déployée, y compris dans des machines de vote, en remplacement ou en complément de l'absence de mémoire non-volatile, est la possibilité de démarrage sécurisé contrôlé depuis un TPM ("Trusted Platform Module"), qui vise à détecter toute modification dans le software.

In fine, les solutions les plus plausibles au vu du marché actuel nous semblent basées sur des micro-PCs, des laptops, ou sur des ordinateurs à carte unique, qui sont les solutions laissant le plus de liberté de configuration

et de sécurisation aux intégrateurs du système.

Il n'est pas exclu non plus qu'apparaissent sur le marché des équivalents tablettes des smartphones produits par Fairphone : ces téléphones sont conçus pour être facilement réparables, peuvent fonctionner sur base de logiciel open source [9] et sont actuellement fournis avec un support de sécurité d'au moins 8 ans [10]. Une telle plate-forme pourrait avoir énormément d'intérêt dans le contexte des machines de vote.

De la même manière, une solution qui utiliserait du matériel basé sur une architecture Risc-V [11], dont le développement va croissant chez de nombreux fabriquants, pourrait apporter d'importants gains en matière de transparence et de résistance à des intrusions par des acteurs internationaux.

4.2.1.2.2 Mutualisation du matériel de vote

Une autre piste pour la gestion du matériel vient de l'observation que les machines de vote ne sont utilisées qu'en un très petit nombre d'occasions et uniquement les dimanches en l'état actuel de la législation. Cet usage très limité, ainsi que les difficultés liées à la durée de vie des machines, pourraient inciter à mutualiser des machines qui sont normalement utilisées en semaine dans des administrations ou des écoles et qui pourraient aussi être utilisées les dimanches d'élection. La maintenance et le renouvellement des machines dans le contexte des élections bénéficieraient alors de ce qui est de toute manière déjà réalisé dans les écoles et administrations.

Deux approches peuvent être considérées :

1. L'achat de machines de vote, selon un modèle standardisé et testé pour les contraintes des élections, dont on extrairait les ordinateurs (laptops, ou PC et écran) pour un usage hors élections, et qu'on ré-assemblerait pour les besoins des élections.
2. L'achat de machines (laptops ou PC et écran) selon les modes d'acquisition habituels des administrations et écoles, machines qui seraient empreintées pour les besoins des élections.

Un certain nombre d'obstacles se présentent face ces approches, obstacles qui pourraient transformer les économies de coûts d'acquisition et de maintenance en des coûts organisationnels et opérationnels, et augmenter les risques de problèmes majeurs durant les jours d'élections.

9. https://shop.fairphone.com/fairphone-4-e-operating-system
10. https://support.fairphone.com/hc/en-us/articles/9979180437393-Fairphone-OS
11. https://riscv.org/

Adopter l'une des deux approches serait conditionné à la résultion des difficultés suivantes.

— *Intégrité des machines.* Une personne pourrait compromettre les machines utilisées pour le vote en modifiant les composants physiques qu'elle contient, ou le firmware de ces machines (une mémoire non-volatile qui ne peut être retirée et qui supporte notamment le démarrage du système d'exploitation). Ceci pourrait notamment avoir lieu lors d'opérations de maintenance de routine. La protection de l'accès physique aux machines est perçue comme un élément majeur de la sécurité d'un système de vote électronique. La figure 4.2 reprend, à titre d'exemple, les prescriptions de l'Election Assistance Commission en la matière, qui montrent les contraintes strictes requises pour l'accès aux systèmes de vote [12]. En l'absence de telles protection, il y aura lieu de trouver des arguments convainquants pour démontrer que les machines n'ont pas été modifiées en dehors des élections. Nous n'avons pas connaissance de procédure standard permettant de réaliser ce type de vérification. La vérification des élections, tant via des RLAs que via de la vérifiabilité E2E, apporte certainement des réponses qui limitent les risques associés à la corruption de machines de vote. Néanmoins, *(i)* la vérification permet de détecter des résultats incorrects, mais ne peut garantir que les résultats corrects peuvent être calculés, et le fait de devoir annuler une élection serait certainement désastreux, *(ii)* la vérification porte sur la correction des résultats, pas sur la confidentialité des votes, et des machines pourraient être "seulement" modifiées pour systématiquement révéler les votes des électeurs qui les emploient, ce qui serait certainement désastreux aussi.

— *Configuration matérielle spécifique des machines de vote.* Comme discuté plus haut, on veille à s'assurer que le logiciel de vote certifié est effectivement employé sur les machines de vote au moyen de toutes sortes de protections, dont l'absence de possibilités de connexion réseau, l'absence de mémoire non-volatile et/ou les démarrages sécurisés. Ces contraintes ne pourront pas forcément être satisfaites par des ma-

12. Dans un exemple largement documenté dans la presse, un chercheur indien ayant contribué à une analyse de la sécurité des machines de vote utilisées en Inde [69] a été arrêté, apparemment en vue d'obtenir des informations sur la manière dont il avait pu accéder à la machine de vote dont lui et ses collègues s'étaient servi pour leur analyse https://freedom-to-tinker.com/2010/08/22/electronic-voting-researcher-arrested-over-anonymous-source/. On peut aussi penser aux intenses débats et poursuites judiciaires qui ont eu lieu autour (de tentatives) d'accès illégaux à des machines de vote aux USA depuis 2020.

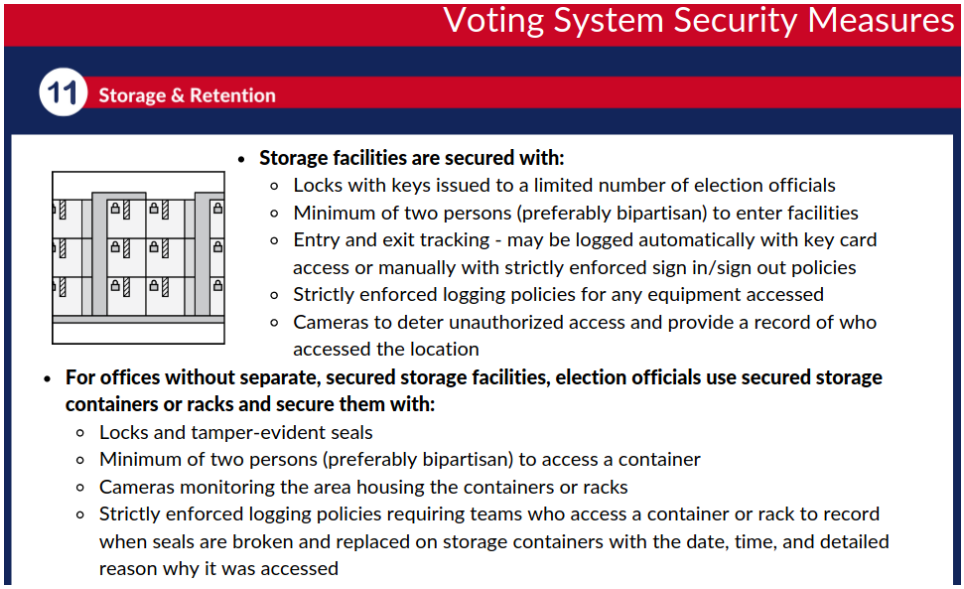

FIGURE 4.2 – Mesures de sécurité pour l'accès aux systèmes de vote indiquées par l'Election Assistance Commission américaine. Source : https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf

chines achetées pour d'autres fonctions et, dans le cas où les machines ont été spécifiquement achetées en réponse aux besoins des élections, imposera une logistique spécifique de reconversion des machines, qui devront vraisemblablement pouvoir être connectées sur différents réseaux et à différents périphériques dans leur usage quotidien. On pense ici par exemple à un remplacement ou à une suppression des mémoires non-volatiles utilisées en-dehors des élections, ainsi que de toutes les interfaces de communication réseau, au moins sans fil.

— *Disponibilité du matériel pour les élections.* Le matériel devra rester disponible en quantités suffisantes pour les éventuels besoins d'élection, et ce en pratique en permanence. En effet, l'Article 46 de la Constitution prévoit l'organisation d'élections anticipées dans un délai de 40 jours en cas de dissolution de la Chambre [13]. Un tel délai est extrêmement court, et impose dans les faits d'avoir au moins, de stock, tout le matériel nécessaire pour la conduite du vote électronique : réaliser l'appel d'offre, l'achat, la configuration et le test de nouvelles machines dans

13. https://www.senate.be/doc/const_fr.html#art46

un tel délai semble irréaliste. L'état des machines utilisées en-dehors des élections devra donc rester sous surveillance, et faire l'objet de tests. (Tout ceci s'applique évidemment aussi dans le cas des machines de vote dédiées. Mais les opérations de test sont plus faciles à réaliser quand les machines sont entreposées dans des endroits bien connus et disponibles en permanence.)

— *Disponibilité du matériel pour d'autres usages.* À l'approche d'élections, les contrôles intensifs des machines, leur reconfiguration pour les élections et l'organisation de leur déploiement rendront ces machines indisponibles pour d'autres usages. Les machines devront aussi rester disponibles après les élections en attente de la validation de celles-ci, pour pouvoir répondre à des éventuels besoin d'enquête. Durant ces périodes, elles ne pourront dès lors pas être disponibles pour d'autres usages. Tout autre utilisateur de ces machines devra donc pouvoir s'accomoder d'être privé d'accès à la machine pendant plusieurs semaines autour des élections.

L'approche qui consiste à employer du matériel acquis selon des procédures d'achat et selon des calendriers indépendants des élections pose des défis supplémentaires.

— *Compatibilité du matériel.* Les systèmes de vote sont conçus sur base d'un système d'exploitation spécifique, qui est dans la plupart des cas une distribution linux modifiée. Il sera difficile de garantir que ce système d'exploitation pourra démarrer sur des machines standard, qui pourront contenir des composants physiques non compatibles. Il est bien sûr possible de veiller à ce type de compatibilité en en faisant un critère au moment de l'achat du matériel. Le coût supplémentaire associé à ce critère est cependant difficile à prévoir, et des tests avant achat seront vraisemblablement chaque fois nécessaires. La diversification du matériel va aussi d'imposer de créer différentes versions du logiciel de vote, adaptées à chaque type de matériel utilisé, avec à chaque fois de nouveaux risques d'erreurs, et donc des contraintes de testing.

— *Variabilité d'expérience des électeurs.* Du matériel acheté dans différents contextes sera plus difficilement uniforme et, en particulier, les formats d'écran risquent de varier d'un endroit à l'autre, en taille et en résolution. Ceci est susceptible de créer une variabilité problématique dans l'affichage des bulletins de vote, voire des situations dans lesquelles l'écran ne montrerait pas l'entièreté des candidats qu'il doit montrer. Ce type de problème peut être limité à l'aide de tests systématiques, mais on ne parviendra pas à la même uniformité que celle

dont on dispose quand on a des machines dédiées. À nouveau, il serait possible de contraindre les achats de manière à garantir des formats d'écrans spécifiques, etc.

— *Complexité d'installation des isoloirs.* Le matériel mutualisé devra être déménagé et installé dans les isoloirs, raccordé à une imprimante et à un lecteur de codes QR. Se baser sur du matériel utilisé dans d'autres contextes imposera des contraintes organisationnelles supplémentaires pour les personnes qui déploient les bureaux de vote, là où les recommandations du Conseil des experts vont vers la simplification, au vu des difficultés actuellement rencontrées.

Nous n'avons connaissance d'aucun pays qui mutualise l'usage de ses machines de vote, et ne pouvons donc pas nous baser sur l'expérience acquise ailleurs.

La difficulté qui semble la plus difficile à surmonter est le contrôle de l'intégrité des machines, problème qui est actuellement résolu ailleurs en imposant un strict contrôle d'accès aux machines.

Les autres difficultés sont essentiellement des contraintes, qui ne sont pas insolubles, mais qui vont augmenter les coûts résultant de la mutualisation. Il n'est pas évident que, in fine, des économies seraient réalisées – bien que ce soit évidemment extrêmement dépendent du contexte.

4.2.1.2.3 Imprimante Le second composant important de la machine de vote est l'imprimante qui imprime le bulletin de vote de l'électeur. La solution actuelle consiste à utiliser une imprimante thermique avec un rouleau de papier de type ticket de caisse.

Ceci pose des soucis d'ergonomie pour de grands bulletins, et n'est pas compatible avec du scanning de bulletins par batch. La flexibilité des bulletins imprimés sur ce type de papier peut aussi compliquer leur scanning à l'urne.

La proposition de BeVoting II est d'adopter des imprimantes au format classique A4, qui :

— faciliteront le contrôle des bulletins par les électeurs,

— faciliteront la manipulation et le scanning des bulletins par les électeurs,

— se prêteront plus facilement à l'usage de techniques de lecture assistée pour des personnes malvoyantes ou aveugles.

Une question plus délicate est celle du type d'imprimante utilisée. La technologie d'impression thermique utilisée actuellement présente des avantages importants, notamment :

— grande robustesse et maintenance limitée par l'absence d'encre et de poudre dans le système,

— encombrement limité,

— pas de coût d'encre, et

— consommation électrique limitée.

Si les imprimantes thermiques à tickets de caisse (rouleaux de papier d'une largeur autour de 8cm) sont très courantes, il est nettement moins ordinaire de trouver des imprimantes thermiques munies d'un bac d'alimentation contenant plusieurs centaines de feuilles de papier au format A4, permettant un scanning aisé, et disposant de pilotes pour des systèmes d'exploitation open source.

Une alternative qui est devenue courante, notamment aux États-Unis, est l'usage d'imprimantes laser. Ces imprimantes ont l'avantage d'être extrêmement courantes, d'un usage familier pour beaucoup de personnes, peu coûteuses, robustes et d'imprimer sur du papier standard facile à scanner. Elles sont aussi largement supportées par les systèmes d'exploitation open source, ce qui simplifie leur mise en œuvre et leur éventuel remplacement. Elles nécessitent cependant l'usage de toners de poudre pour supporter l'impression et ne sont pas aussi robustes que les imprimantes thermiques. Les imprimantes laser ont aussi parfois été exclues en raison de leur importante consommation électrique au moment de leur allumage et/ou d'impressions, la crainte étant qu'elles déclenchent des surcharges sur le réseau électrique dans les bureaux de vote. Les évolutions de ces imprimantes et leurs larges déploiements actuels donnent une réponse rassurante à ces craintes. L'encombrement généré par une imprimante laser est enfin plus important que celui d'une imprimante thermique intégrée à la machine de vote : l'imprimante laser ne sera pas intérgée au boîtier de la machine de vote mais restera posée à côté de celle-ci.

Les imprimantes à jet d'encre, très bon marché, sont en pratique exclues de ce type d'application en raison de leur fiabilité limitée et des problèmes de séchage de l'encre.

Le choix d'adopter des imprimantes laser semble le plus plausible ici, même si il n'est pas exclu que des solutions à base d'imprimantes thermiques puissent être trouvées.

4.2.1.2.4 Papier Le papier utilisé devra permettre un scanning facile. Il sera aussi important de veiller à utiliser un papier très spécifique, portant un filigrane, constitué de fibres spécifiques, etc. Ceci est utile à la fois pour informer des enquêtes sur des urnes dont le contenu pourrait avoir été altéré,

mais aussi pour détecter des plaintes frivoles que des électeurs soumettraient, indiquant par exemple qu'un numéro de suivi de bulletin de vote falsifié serait manquant dans la liste des bulletins repris dans le décompte.

4.2.1.2.5 Lecteur de carte à puce ou scanner Le dernier composant des machines de vote en place en Belgique est le lecteur de cartes à puce. Celles-ci demandent une logistique en termes d'initialisations et de lecteurs et ont été sources de confusions entre différents types de cartes (l'initialisation d'une carte n'est pas visible sur la carte, ce qui impose d'excellentes procédures de tri ou une discipline d'annotation des cartes).

La proposition de BeVoting II est de remplacer ces lecteurs de carte par des lecteurs de codes QR, pour les raisons décrites en section 4.2.

4.2.1.2.6 Assemblage Disposer d'une machine de vote intégrant tous les composants dans un unique boîtier, comme c'est le cas actuellement, présente certainement des attraits importants : cela facilite le transport des machines et leur installation dans les isoloirs, et cela évite les problèmes de connexion et d'arrachage de câbles reliant différents composants.

Cela augmente par contre les coûts de la solution et complique sensiblement toute modification du matériel qui serait nécessaire après quelques années. Il pourrait être intéressant d'explorer des solutions d'inclusion des composants des machines de vote dans des boîtes de transport standard, généralement en plastique rigide, qui offriraient davantage de flexibilité dans les modifications des équipements. Les différents composants du système et les câbles pourraient par exemple être fixés à l'aide de blocs en mousse rigide, qui pourraient facilement être remplacés si un nouvel équipement doit être mis en place

4.2.1.2.7 Différences avec les machines de vote actuellement utilisées Une question naturelle à ce stade est de comparer, au niveau matériel, le concept de machines de vote BeVoting II proposé ici avec les machines actuellement utilisées en Belgique. Ceci en vue de clarifier les avancées proposées, et les endroits où des adaptations seraient éventuellement possibles.

— Au niveau de l'unité centrale, il est plausible que le micro-PC actuellement présent dans les machines de vote de seconde génération reste suffisant pour réaliser les nouvelles opérations cryptographiques requises.

— BeVoting II propose de remplacer les imprimantes de tickets de 8 cm par de l'impression au format A4. Conserver les imprimantes actuelles présenterait plusieurs inconvénients :

  - L'endossement de tickets au moment du scanning serait sensiblement plus complexe. Cet endossement, ou un tri des bulletins papier par liste, sont nécessaires pour obtenir un audit à limitation de risque efficace.
  - La vérification du contenu des bulletins par les électeurs resterait moins aisée. L'importance de faciliter cette vérification a été soulevée dans différentes études.

  On pourrait probablement imaginer de désactiver l'imprimante à ticket actuellement présente dans les machines et de la remplacer par une imprimante séparée.
- BeVoting II propose le remplacement du lecteur de cartes à puce par un lecteur de code QR. Conserver le lecteur de cartes à puce présenterait plusieurs inconvénients :
  - Maintien des difficultés actuelles avec la gestion des cartes à puce.
  - En l'absence de lecteur de code QR, pas de possibilité simple pour des électeurs de préremplir leurs bulletins à l'avance et de les scanner dans l'isoloir. Ceci fait perdre de l'accessibilité pour les personnes éprouvant des difficultés à se servir des machines, et fait perdre les gains de temps escomptés si les personnes peuvent utiliser des bulletins préremplis.

4.2.2 Dépôt du bulletin de vote et dépouillement

4.2.2.1 Fonctionnalités

Dans le système de vote électronique actuel, les bulletins de vote imprimés sont amenés à une urne électronique. Là, l'électeur scanne le code QR imprimé sur son bulletin, ce qui permet de stocker le vote sur la machine du Président du bureau et déclenche l'ouverture de l'urne. Celle-ci se referme une fois le bulletin déposé dans l'urne.

Cette partie de la solution est vraisemblablement la partie la moins standard du système de vote électronique actuel. Elle a suscité bon nombre de difficultés soulignées dans les rapports du Collège des experts, et a aussi fait l'objet d'importantes révisions et améliorations au cours des années.

Un autre inconvénient de ce processus est la limitation au scanning d'un code QR, non ou mal vérifié par l'électeur, plutôt qu'un scanning de l'intention de vote telle que relue par l'électeur. Le passage à des bulletins de vote imprimés sur des feuilles A4 classiques permet d'envisager un scan de la page entière (difficile pour un ticket de caisse étroit et allongé), ce qui

offrirait une possibilité de lire le vote de l'électeur à partir de l'impression relue par celui-ci plutôt que par le scanner. Ceci ajouterait de la robustesse au système, dans la mesure où la "triche" d'une machine de vote sur le code QR deviendrait inopérante. Ceci impose cependant des contraintes sur le processus de scanning et de reconnaissances de caractère, et la faisabilité de cette approche sera vraisemblablement dictée par le choix de l'équipement de scan. Nous n'avons pas connaissance, à ce jour, de juridiction pratiquant réellement de la lecture avec reconnaissance de caractères sur des bulletins scannés (ce sont soit des codes QR qui sont identifiés, soit la présence ou l'absence de marques aux endroits qui correspondent à la case de sélection de candidats, ce qui comporte des risques en soi). Qui plus est, la triche des machines à voter peut aussi être identifiée via le Risk Limiting Audit, ce qui limite la nécessité de lire le bulletin en entier.

La mise en œuvre d'un RLA efficace par "ballot comparison" impose aussi de nouvelles contraintes sur le processus de scanning : le besoin d'endosser chaque bulletin scanné, en imprimant dessus un numéro de série sous la forme d'un compteur (en plus d'informations comme un identifiant du scanner ou du bureau de scanning, une heure de scanning, etc.) Cet endossement n'est pas nécessaire pour réaliser un RLA. Il permet cependant d'organiser des RLAs nécessitant la vérification d'un nombre considérablement plus faible de bulletins, ou d'échapper à un dépouillement complet des bulletins papier.

Ceci impose concrètement d'utiliser un scanner qui avale le papier, l'endossant au passage, et exclut de s'en tenir à un simple scanner de code QR comme dans le système actuel. Le scanning pourra se faire par paquets d'une centaine de pages, et chaque paquet de bulletins scannés sera placé dans une enveloppe, sur laquelle on indiquera les numéros de série du premier et du dernier bulletins scannés du paquet, tels qu'imprimés par l'endosseur, ainsi que le nombre de bulletins de vote placés dans l'enveloppe. Ces mêmes numéros seront consignés dans un manifeste, probablement sous la forme d'un tableur sur un laptop, en vue de la préparation du RLA. On placera les enveloppes dans des boîtes que l'on peut solidement fermer en vue d'un transport vers le lieu où se déroulera le Risk Limiting Audit.

Le processus de scanning fournira aussi une interprétation individuelle de chaque bulletin scanné, en vis-à-vis de son numéro de série produit à l'endossement. Ceci permettra de totaliser les votes exprimés durant l'élection et de calculer les résultats, mais aussi d'être en mesure de réaliser le risk limiting audit de manière efficace : il s'agira, pour un certain nombre de numéros de série de bulletins piochés de manière aléatoire, d'être en mesure de retrouver le plus efficacement possible le bulletin papier correspondant, et de comparer une lecture du bulletin papier avec l'enregistrement électronique qui a été

fait. Pour finir, le processus de scanning fournira aussi, pour chaque bulletin, un nombre extrait du code QR imprimé sur le bulletin, nombre qui servira pour la vérifiabilité de bout en bout de l'élection. Nous discuterons de ce nombre dans la section consacrée à la vérifiabilité E2E ci-dessous.

4.2.2.1.1 Processus de scanning

Concrètement, nous voyons six moments et lieux où le scanning pourrait avoir lieu :

1. au niveau de la machine de vote, qui serait alors aussi munie d'une urne,
2. au moment du dépôt dans l'urne,
3. dès la fin des votes, dans le bureau de vote,
4. dans des bureaux de dépouillement au niveau du canton,
5. dans un bureau de scanning au niveau du bureau de canton principal,
6. dans un bureau de scanning centralisé au niveau de l'arrondissement électoral.

4.2.2.1.2 Au niveau de la machine de vote

Cette approche nous semble poser plusieurs problèmes :

— On pourrait se servir du lecteur de code QR déjà présent sur la machine de vote et inviter l'électeur à déposer son bulletin dans une urne présente dans l'isoloir. Il devient alors très difficile de contrôler si l'électeur a effectivement déposé son bulletin de vote (des électeurs pourraient le conserver, par inadvertance, méconnaissance du système, ou malice). Cela impose aussi de stocker les bulletins de vote sur la machine de vote, alors qu'on essaie d'éviter d'avoir toute mémoire non-volatile à cet endroit du système.

— On pourrait avoir un dispositif de saisie du bulletin papier qui avalerait et scannerait le bulletin en même temps, le déposant dans une urne attachée à la machine de vote, empêchant l'électeur de récupérer un bulletin scanné. On se rend compte du coût supplémentaire que cela placera sur la machine de vote, ainsi que des composants non standard qui devront être ajoutés. Ceci pose des difficultés importantes : les bulletins de vote scannés s'empileront généralement dans l'urne dans l'ordre de leur scanning, ce qui pose des soucis de secret du vote vis-à-vis des personnes qui ouvrent l'urne. Qui plus est, si le dispositif d'impression est aussi utilisé pour avaler le papier, à des fins d'économie et d'ergonomie, on peut aussi s'interroger sur le risque que des

inscriptions supplémentaires soient réalisées sur le bulletin, le modifiant sans que l'électeur puisse le voir [14].

— Elle est difficilement compatible avec les solutions d'endossage des bulletins de vote, qui est requis pour des risk limiting audits efficaces : un endossage séquentiel au niveau de la machine de vote serait clairement problématique au niveau du secret du vote.

4.2.2.1.3 Au moment du dépôt dans l'urne La solution actuelle, basée sur un scanning de QR code au format ticket de caisse, pose des difficultés matérielles régulièrement rapportées dans les rapports du Collège des experts. Par ailleurs, étant donné la présence d'une unique urne par bureau, toute difficulté paralyse rapidement le bureau de vote. On peut aussi mentionner des interrogations par rapport au secret du vote dès lors qu'une difficulté de scanning se pose : un électeur, son bulletin de vote marqué à la main, fera appel à un membre du bureau de vote qui viendra l'aider à scanner le bulletin ou constatera une panne du système – même plié, on peut imaginer la difficulté de garder le bulletin secret dans de telles circonstances.

Une alternative, largement présente dans de nombreuses urnes électroniques utilisées aux États-Unis, consiste à équiper l'urne d'une avaleuse scanneuse qui saisit le bulletin et le lit avant de le déposer dans l'urne.

Cette solution, facilitée par l'usage de papier plus grand et rigide qu'un ticket de caisse, est très avantageuse pour le scanning de bulletins de vote marqués à la main : le scanning direct permet à la machine de retourner à l'électeur un bulletin de vote qui aurait été complété de manière invalide ou serait illisible. Ceci n'est cependant pas notre cas ici puisque les bulletins sont imprimés par les machines de vote, qui doivent garantir leur validité.

Un autre avantage de cette solution est de permettre de fermer les urnes sitôt la fin des opérations de vote : au moment où le dernier électeur quitte le bureau de vote, tous les bulletins ont été scannés.

Néanmoins, cette solution reste toujours fragile par rapport aux éventuels dysfonctionnements ou bourrages du scanner, qui bloquent le fonctionnement du bureau de vote. Elle est aussi relativement coûteuse, dans la mesure où un scanner muni d'une fente lui permettant d'avaler un unique bulletin A4 reste nécessaire pour chaque urne.

Au vu des avantages limités, de la fragilité et des coûts associés, nous ne recommandons pas cette approche en Belgique.

14. Voir par exemple la discussion de ce problème dans le système VSAP utilisé à Los Angeles https://www.politico.com/news/2020/03/03/los-angeles-county-voting-experiment-119157.

4.2.2.1.4 Dès la fin des votes, dans le bureau de vote

Cette approche consisterait à utiliser une urne parfaitement standard, telle que celle utilisée dans les élections papier, et à l'ouvrir dès la sortie du dernier électeur et à bien mélanger les bulletins de vote avant de les scanner.

Les scanners actuels avalent facilement de l'ordre de 70 pages par minute. L'opération de scanning proprement dite pourrait alors prendre de l'ordre de 34 minutes pour les 2400 pages qui correspondraient aux trois bulletins de vote déposés dans une élection conjointe par les 800 électeurs qui se rendent dans un bureau de vote complet, ce qui semble un temps raisonnable, même s'il faudra y additionner un peu de temps pour ouvrir les urnes, mélanger les bulletins, et les rassembler en paquets à introduire dans le scanner.

Cette approche a l'avantage de garantir un scanning très tôt dans le processus de dépouillement, et en particulier avant tout transport des bulletins vers un bureau de dépouillement ou d'audit, évitant les risques de manipulation durant le transport. Si le système est vérifiable de bout en bout, de telles manipulations seraient cependant détectées, ce qui limite l'intérêt de ce type de fraude.

Certains apprécieront sans doute aussi, indépendamment des questions d'authenticité, de recevoir les résultats des votes le plus rapidement possible : en scannant dans le bureau de vote : on gagne le temps nécessaire à l'acheminement des urnes vers un bureau de dépouillement.

Cette approche sera par contre plus faible au niveau de la confidentialité du vote : la manipulation des bulletins de vote dans de petits bureaux de vote (la taille prévue est de minimum 150 électeurs) par des personnes qui étaient présentes au moment du scrutin pourrait faciliter la reconnaissance de petites marques apposées sur les bulletins, en vue de vendre des votes par exemple. C'est quelque chose qui est évité dans le vote papier, grâce à la mise en place de bureaux de dépouillement gérés indépendamment des bureaux de vote.

De plus, le scanning dans le bureau de vote est plus fragile, surtout si le bureau de vote est isolé : en cas de difficulté technique, l'obtention de support technique sera probablement plus lente que dans des bureaux de scanning plus centraux, et une panne d'un scanner bloquera le processus complètement dans la mesure où le bureau de vote n'aura vraisemblablement qu'un unique scanner. Organiser le scanning dans chaque bureau de vote plutôt que de manière plus centralisée augmentera sans doute aussi le travail de formation des présidents de bureaux de vote et le nombre de personnes qu'il faudra former aux opérations de scanning.

Ce risque pourrait s'apprécier différemment dans des zones densément peuplées où l'on rassemble souvent plusieurs bureaux de vote dans une même

école par exemple : il sera vraisemblablement simple de récupérer un scanner utilisé dans un bureau de vote qui a terminé son scanning pour compenser une panne. Il peut aussi être raisonnable de disposer d'un équipement de scanning de rechange pour plusieurs bureaux de vote conjoints.

Par ailleurs, des équipements de scanning de secours pourraient aussi être disponibles dans un ou plusieurs bureaux de canton, où les Présidents de bureau de vote pourraient amener les bulletins de vote en cas de panne.

4.2.2.1.5 Dans des bureaux de dépouillement au niveau du canton L'idée ici serait de procéder par analogie à ce qui se fait au niveau du vote papier traditionnel, où les urnes sont acheminées vers des bureaux de dépouillement au niveau des cantons. Ces bureaux existent déjà dans les cantons qui utilisent à la fois le vote électronique et le vote papier.

Procéder de la même manière pour le scanning présente différents avantages :

— On pourrait organiser des bureaux de scanning à plus grande échelle, munis d'un certain nombre de scanners, ce qui limite l'impact de pannes.

— Si le scanning est concentré dans un petit nombre d'endroits, il serait possible de le faire en présence, ou à proximité de personnes qui auraient une bonne expérience dans la manipulation des scanners et pourraient offrir une assistance utile, voire une guidance, dans le processus.

— Avoir du scanning organisé à plus grande échelle permettrait de limiter le nombre de personnes à former, et pourrait limiter le besoin de formation aussi si du support technique est disponible sur place.

— On évite les éventuels risques pour le secret du vote et la vente de vote qui sont associés à un dépouillement dans les bureaux de vote.

Au niveau des inconvénients, nous observons que :

— le scanning a lieu après le transport des urnes, ce qui augmente les risques que le contenu des urnes soit modifié avant scanning – même si ces modifications seraient détectées grâce à la vérifiabilité de bout en bout,

— cette solution peut imposer de créer des bureaux de scanning dans des cantons qui n'ont plus de bureaux de dépouillement, ce qui demanderait une logistique plus importante.

On notera tout de même que ces bureaux de scanning demanderont nettement moins de monde qu'un bureau de dépouillement, le scanning étant bien plus rapide que le dépouillement manuel.

4.2.2.1.6 Dans un bureau de scanning au niveau du canton

Cette solution est identique à la précédente. Elle pourrait être privilégiée dans des cantons où le vote est entièrement électronique : un unique bureau de scanning pourra être très efficace.

Elle aurait aussi son sens dans des petits cantons : on observe que, lors des élections fédérales de 2019, les cantons des Fourons et de Fauvillers ont totalisé les votes de 1510 et 1514 électeurs respectivement. Ceci est très différent du canton d'Anvers où les votes de 293377 électeurs ont été totalisés.

4.2.2.1.7 Dans un bureau de scanning au niveau de l'arrondissement

Cette solution pousse la solution précédente à son extrême et pourrait être intéressante dans des arrondissements géographiquement denses.

Elle présenterait l'avantage de faciliter la logistique en vue du risk limiting audit qui a lieu au niveau de l'arrondissement : les bulletins de vote pourraient être directement rassemblés sur le lieu de l'audit.

4.2.2.1.8 Conclusion

Les trois dernières options listées ici ont notre préférence, en raison de la simplification des bureaux de vote qu'elles apportent, de la limitation des risques pour le secret du vote, de la limitation des risques techniques en cas de panne d'urne, et des besoins de formation au scanning.

Notre proposition va dans le sens de recommandations du Collège des experts, qui recommandent eux aussi d'éliminer le scanning au niveau de l'urne électronique et de remplacer cette urne-scanneuse par l'usage d'une urne classique suivi d'un processus de scanning après la clôture des opérations de vote, et ce pour simplifier l'organisation des bureaux de vote et améliorer la transparence du système et le secret du vote [16, 2012-Bxl.6][17, Sec. 6.1].

Nous ne pensons pas approprié de trancher entre les trois options retenues, et il nous semble plausible que l'option qui est préférable pour un canton ne le soit pas pour le canton voisin, en raison de différences dans la proportion d'usage du vote électronique, dans la densité de population, dans la taille du canton, etc.

4.2.2.2 Matériel

La solution de scanner au niveau de l'urne imposerait l'usage de matériel peu courant, et n'est pas recommandée ici.

Nous nous concentrons ici sur une urne, qui sera opaque pour ne pas risquer de rendre visible le contenu des bulletins de vote qui y sont déposés.

Pour les autres approches, deux types de scanners sont généralement utilisés :

1. des scanners d'entreprise, munis d'une avaleuse d'une centaine de pages, et qui scannent de l'ordre de 70 pages par minute, et ont la taille d'une petite imprimante,
2. des scanners à haute vitesse, conçus pour un usage intense dans des services d'archivage par exemple, qui peuvent atteindre des vitesses de plus de 200 pages par minute, et qui sont de véritables meubles.

Des exemples de scanners de ces deux types utilisés dans des élections peuvent par exemple être trouvés dans la liste des technologies de vote approuvées dans l'état de Californie du 30 octobre 2023 [15].

Plusieurs de ces scanners d'entreprise peuvent s'acheter à la pièce, pour un particulier, pour un prix autour de 1000 euros, hors module d'endossement, souvent proposé en supplément pour une somme autour de 500 euros. Les prix des scanners à haute vitesse ne sont pas publiés.

Les modules d'endossement sont généralement une mini imprimante jet d'encre, installée de manière à ne pouvoir imprimer que sur une bande limitée sur la feuille de papier, ce qui est aussi nécessaire pour être compatible avec les rythmes de scanning élevés (bien supérieurs à ceux d'imprimantes jet d'encre classiques conçues pour imprimer sur la largeur de la page).

Vu l'habitude en Belgique d'obtenir les résultats d'élection très rapidement, il nous semble plausible qu'une solution basée sur un grand nombre de scanners d'entreprise sera plus efficace et moins coûteuse que l'usage de scanners à haute vitesse, sauf si ceux-ci peuvent être loués pour le jour de l'élection – des entreprises proposent effectivement des services de location de scanners à haute vitesse, qui semblent principalement destinés à des entreprises, associations ou administrations qui ont un gros besoin d'archivage ponctuel.

Au niveau du dimensionnement, nous pouvons réaliser une estimation sur les bases suivantes : en se basant sur de scanners d'entreprise qui scannent 70 pages par minute et sont employés pour 1h30 en continu (en excluant le temps nécessaire pour introduire les piles de bulletins à scanner, sortir les bulletins scannés, gérer les éventuels bourrages, etc.), nous voyons qu'un scanner pourra être utilisé pour scanner 6300 bulletins. Il faudra donc comp-

15. Voir https://votingsystems.cdn.sos.ca.gov/cert-and-approval/vote-sys-appr-in-ca-10-30-23.pdf. On retrouve les mêmes types de scanners listés par les autres états dont nous avons consulté les listes de matériel certifié, avec parfois des variantes de marques.

ter environ 160 scanners par million de bulletins (sans compter des scanners de réserve en cas de panne).

4.2.3 Vérifiabilité

Nous élaborons ici les différents éléments à mettre en œuvre pour réaliser l'audit limitant le risque de résultat incorrect et la vérifiabilité de bout en bout.

4.2.3.1 Audit limitant le risque

Les ingrédients nécessaires à la préparation du RLA ont été discutés plus haut. À la suite du scanning des bulletins, on rassemble en un unique lieu par arrondissement les éléments suivants :

- un manifeste de l'élection dans l'arrondissement qui reprend, au minimum :
  - pour le vote électronique : une liste des boites d'enveloppes de bulletins de vote de l'élection, indiquant quelle enveloppe se trouve dans quelle boîte, et la liste des numéros de série des bulletins présents dans chaque enveloppe,
  - pour le vote électronique : une liste de tous les bulletins de vote donnant, pour chaque numéro de série de bulletin, la manière dont ce bulletin a été interprété au moment du scanning,
  - pour le vote papier : une liste des boîtes d'enveloppes de bulletin produits dans le cadre du vote papier, indiquant quelle enveloppe se trouve dans quelle boîte, combien de bulletins chaque enveloppe contient, et le parti auquel ont été attribué les votes de chaque enveloppe,
  - les totaux et résultats de l'élection, tels qu'ils ont été calculés.
- l'ensemble des caisses contenant tous les bulletins de vote papier de l'élection dans l'arrondissement concerné.

Nous avons détaillé au chapitre précédent (section 3.2) une proposition de déroulement de l'audit, basée sur les échanges que nous avons pu avoir avec des personnes qui en ont pratiqué, sur des guides publiés, et sur les spécificités belges.

4.2.3.2 Vérifiabilité de bout en bout

Nous avons aussi décrit au chapitre précédent (section 3.3) l'ensemble des opération cryptographiques nécessaires pour la vérifiabilité de bout en bout, mais avons laissé en suspens les lieux et moments où ces calculs ont lieu, qui nécessitaient une description plus générale du système. Nous précisons ces éléments ici.

Il s'agit de préciser :

1. la manière dont on fournit à chaque électeur son numéro de suivi de bulletin,
2. la manière dont les bulletins de vote chiffrés sont calculés et stockés dans le système de vote, pour audit.

4.2.3.2.1 Production du numéro de suivi de bulletin pour l'électeur On a vu, en section 3.3, que le numéro de suivi du bulletin de vote d'un l'électeur est un haché, représenté sous la forme d'une cinquantaine de caractères, du chiffré de son bulletin de vote.

On souhaite fournir ce numéro de suivi à l'électeur avant qu'il dépose son bulletin dans l'urne, afin qu'il puisse éventuellement demander d'invalider son bulletin de vote pour vérifier que le numéro de suivi reflète bien son intention de vote. La solution naturelle est alors de faire imprimer ce numéro de suivi (ou ces numéros de suivi, s'il y a plusieurs bulletins lors d'élection conjointes) sur une page supplémentaire imprimée par la machine de vote, en même temps que les bulletins de vote.

Cette page avec les numéros de suivi sera conservée par l'électeur. Il importera de communiquer très clairement avec les électeurs pour une manipulation correcte des pages imprimées par la machine de vote. L'électeur doit réaliser que son ou ses bulletins de vote ne doivent être montrés à personne et être déposés dans l'urne. La page portant les numéros de suivi doit par contre être conservée par l'électeur, et ne doit pas être déposée dans l'urne. Ceci pourra être clarifié à l'avance, lors de l'information habituelle que l'on fait dans les médias vis-à-vis des électeurs avant les élections. On pourra aussi fournir aux électeurs des moyens de séparer facilement les documents avant de sortir de l'isoloir : des fardes en carton de couleur différentes et portant des étiquettes claires pourraient être utilisées à cet effet (on les fournirait à l'électeur avant son entrée dans l'isoloir, il les restituerait à la sortie, après avoir déposé ses bulletins de vote dans les urnes).

Une difficulté technique est la communication du chiffré calculé par la machine de vote vers le système central qui publiera les données d'audit : il

n'y a aucun moyen de communication digitale entre ces deux systèmes.

On pourrait souhaiter imprimer le chiffré sur le bulletin de vote de l'électeur, éventuellement sous intégré dans le code QR, mais cela n'est techniquement pas faisable : on a vu que le chiffré avait typiquement une longueur de quelques dizaines ou centaines de kilobytes, alors que les plus grands codes QR ne permettent de représenter que quelques kilobytes.

Une solution à ce problème est intégrée dans ElectionGuard : pour chaque bulletin de vote, la machine de vote sélectionne une unique valeur de 256 bits, appelée le "ballot nonce". Toutes les valeurs aléatoires utilisées pour calculer les chiffrés ElGamal des choix de l'électeur sont alors dérivées de ce ballot nonce, à l'aide de HMAC employé comme fonction (doublement) pseudo-aléatoire.

Ce ballot nonce de 256 bits peut alors être transmis au reste du système de vote via le code QR imprimé sur le bulletin de vote, qui sera récupéré au moment du scanning.

4.2.3.2.2 Recalcul des bulletins chiffrés en vue de la vérifiabilité universelle On se rend cependant compte de la sensibilité de ce ballot nonce : par exemple, une personne qui saurait à quel électeur appartient un ballot nonce serait en mesure de vérifier pour qui l'électeur en question a voté. Pour cette raison, il ne semble pas approprié d'imprimer le ballot nonce en clair sur le code QR du bulletin. On préférera le chiffrer avant de le transmettre. Cela signifie que, au moment du scanning, on ne récupérera pas le ballot nonce mais une version chiffrée de celui-ci. Après déchiffrement, il sera possible de recalculer le chiffré du bulletin de vote tel qu'il a été calculé par la machine de vote, de calculer les preuves à divulgation nulle associées (qui ne doivent pas avoir été calculées par la machine de vote et qui peuvent être calculées à partir de nombres aléatoires frais) et de publier ce résultat dans le cadre des opérations de vérifiabilité individuelle et universelle.

Il reste à déterminer comment le chiffrement est réalisé, et au moins trois options se présentent ici :

1. Des clés pour un système de chiffrement symétrique sont générées durant l'étape de génération des clés USB d'initialisation des machines de vote au SPF intérieur, et sont insérées sur ces clés. Lorsque les données du scanning arrivent au SPF intérieur, celui-ci déchiffre tous les nonces de bulletin et, à l'aide des votes clairs correspondants, calcule les données d'audit.
2. Une paire de clés pour un système de chiffrement de type hashed-ElGamal ou DHIES [1] est générée par le SPF intérieur au moment de

la génération des clés USB d'initialisation des machines de vote. La clé publique est intégrée dans ces clés USB. Le SPF intérieur procède au déchiffrement comme précédemment.

3. Au moment de la génération des clés des gardiens, ceux-ci produisent une seconde paire clé-publique clé-secrète, comme au point précédent. La clé publique est intégrée dans les clés USB d'initialisation des machines, et le déchiffrement est cette fois effectué par plusieurs gardiens, sur base des données reçues après le scanning.

La seconde solution nous semble a priori la plus appropriée : la distribution de clés symétriques, comme dans la première option, est toujours une opération fort sensible, et l'implication des gardiens telle que requise dans la troisième option représente un besoin considérable de ressources calculatoires, que l'on souhaite éviter dans le chef des gardiens.

Cette seconde solution donne cependant une importance fondamentale à la sécurité de l'infrastructure du SPF intérieur : une fuite des ballot nonces pourrait sensiblement affaiblir la confidentialité des votes, si ces ballot nonces venaient à être combinés avec d'autres informations. On reste cependant dans une protection de la confidentialité des votes nettement supérieure à celle offerte par le système actuellement utilisé en Belgique.

4.2.3.2.3 Besoins en ressources de calcul

On a vu que les ressources de calcul nécessaires pour la vérifiabilité de bout en bout sont négligeables à la plupart des endroits :

— Les tâches des gardiens ne nécessitent pas plus de quelques secondes de calcul sur un laptop.

— Les calculs réalisés sur la machine de vote demanderont moins d'une demi seconde de calcul, même pour les plus grands bulletins de vote. Qui plus est, plus de 90% de ce calcul est indépendant des choix des électeurs et peut donc être réalisé pendant que le vote a lieu.

— La vérification par l'électeur de l'enregistrement correct de son bulletin requiert la simple comparaison de numéros de suivi.

Il existe deux endroits où des ressources de calcul importantes seront nécessaires :

1. Le re-chiffrement et le calcul de validité des preuves des bulletins de vote, sur base des informations obtenues grâce aux bulletins de vote scannés
2. la vérification universelle de la validité des bulletins de vote et de leur totalisation.

Conceptuellement, seule la première tâche doit être réalisée par les organisateurs de l'élection : la vérification de leur propre travail dans la seconde étape ne vise pas à détecter des fraudes. Par contre, il semble naturellement prudent que les organisateurs de l'élection vérifient réellement leurs calculs avant publier les données visant à permettre la vérification de l'élection.

Nous évaluons ici une borne supérieure sur les temps de calcul requis. Celle-ci est basée sur les protocoles décrits plus haut, basés sur ElectionGuard. Comme indiqué aussi, il est très clair que des performances bien meilleures (on peut espérer un facteur de l'ordre de 10 en temps de calcul) pourront être obtenues avec des technologies qui existent aujourd'hui mais qui ne sont pas encore couramment déployées. Plusieurs d'entre elles seront probablement devenue communes d'ici la mise en œuvre du système. Notre évaluation du temps de calcul ne prend par contre pas en compte d'autres facteurs extrêmement variables en fonction du contexte, comme le temps de stockage et de transferts de données entre différentes machines.

Notre évaluation est basée sur une exécution du code décrit en section 3.3, sur une workstation dotée d'un processeur AMD Ryzen 3990X datant de 2020, et en utilisant 64 threads calculant en parallèle le chiffrement et les preuves de validité de 10 000 bulletins de vote reprenant 200 candidats chacun. Les temps mesurés sont repris à la table 4.1. En prenant un niveau de sécurité avec un premier p de 3072 bits, on voit que le chiffrement d'un million de bulletins de vote prendrait, sur une seule machine, 35 minutes (soit 100 fois les 21.1 secondes reprises dans la table 4.1). La vérification de la validité des bulletins, telle que requise pour la vérifiabilité universelle, est plus lente : elle nécessite pour sa part 4h28, toujours pour un million de bulletins. Cette opération n'impliquant aucune donnée confidentielle, elle peut facilement être déléguée à des infrastructures moins sécurisées de type cloud.

Nous pensons que les ordres de grandeur indiqués ici montrent qu'il est tout à fait possible d'obtenir les données nécessaires à la vérifiabilité individuelle et à la vérifiabilité universelle dans des délais rapides, en se servant d'outils tout à fait standard, et sans avoir à investir dans une infrastructure lourde.

4.2.4 Logistique avant les élections

Les machines de vote sont actuellement entreposées dans des conditions variables : certaines communes se chargent elles-mêmes de gérer l'entreposage, tandis que d'autres ont recours à un entreposage par l'intermédiaire de Smartmatic.

	$\|p\| = 3072$	$\|p\| = 4096$
Calcul d'un bulletin	0.083s	0.118s
Calcul de 10 000 bulletins	21.1s	29.1s
Vérification d'un bulletin	0.85s	1.44s
Vérification de 10 000 bulletins	161s	272s

TABLE 4.1 – Temps de chiffrement, de calcul des preuves de validité de bulletins de vote avec 200 candidats répartis sur 10 partis, et temps de vérification de la validité de ces bulletins, en employant 64 threads sur une workstation.

À l'ouverture des bureaux de vote, les machines qui ont été préalablement installées et testées doivent être initialisées et démarrées à l'aide de clés USB. Actuellement, de l'ordre de 10 000 clés USB (deux clés par bureau) sont initialisées dans les infrastructures du SPF intérieur, sont transmises de manière sécurisée aux présidents de bureaux principaux de cantons, qui les transmettent aux présidents de bureau de vote la veille de l'élection. Ces clés USB contiennent le système d'exploitation nécessaire au démarrage des machines, un ensemble de clés cryptographiques, et les données du scrutin, y compris la description des bulletins de vote que la machine pourra présenter aux électeurs.

Cette approche a des avantages importants : elle ne permet pas à des personnes ayant accès aux machines de vote durant la période de stockage entre élections de modifier le logiciel qui fonctionne sur ces machines, étant donné qu'il n'y a pas de logiciel sur ces machines. L'intégrité du logiciel repose aussi sur le suivi de clés USB, plus facile à assurer que celui de machines volumineuses – ceci sans négliger l'importance des enjeux d'un bon suivi des clés USB.

L'accès aux machines de vote non équipées de logiciel ne résout cependant pas la question de la confidentialité des votes. À titre d'exemple, un accès aux machines de votes pourrait permettre de leur ajouter un composant électronique espion qui enregistrerait tous les votes effectués sur la machine, dans l'ordre dans lequel ils ont été effectués. Une personne présente dans le bureau de vote pourrait conserver la liste des personnes ayant voté sur chaque machine, et ainsi retrouver le contenu du vote de chacun. Si ce type d'attaque n'est pas simple, des démonstrations de leur faisabilité sur certaines machines de vote ont pu être réalisée [69]. Cette préoccupation confirme l'importance de conserver les machines de vote de manière sécurisée, même si elles sont

dépourvues de mémoire non volatile.

L'approche basée sur des clés USB pose par ailleurs des difficultés en pratique, régulièrement observées par le Collège des experts, liées à la fiabilité et au soin nécessaire à la manipulation de ces clés USB.

Une alternative, utilisée dans différentes juridictions aux États-Unis, consiste à organiser un entreposage nettement plus centralisé des machines de vote, avec une sécurité rigoureuse, de munir les machines de vote de stockage non-volatile (disques durs) et de possibilités de connexion à un réseau filaire. Les machines peuvent être stockées dans des caissons rassemblés dans des racks ce qui permet de les alimenter en électricité et de les raccorder au réseau. Un logiciel de gestion d'élection permet alors à la fois de réaliser des diagnostics des machines et de les configurer pour chaque élection. Les machines sont ensuite acheminées, depuis les entrepôts, vers les bureaux de vote où il n'y a plus qu'à les mettre en route. Des protections visant à empêcher un démarrage non contrôlé des machines sont mises en place par ailleurs.

Cette approche a le mérite d'éviter la manipulation de clés USB le jour de l'élection, et d'éviter les problèmes relevés avec ces clés. Elle expose cependant les machines à des risques bien plus importants, vu qu'il s'agit à présent de les équiper de mémoire et de possibilités de connexion à un réseau. Ces risques supplémentaires doivent dès lors être compensés par une infrastructure de stockage des machines dont la sécurité doit être fortement renforcée. Les coûts du local de stockage seront aussi augmentés étant donné la nécessité de disposer de racks de stockage des machines munis d'alimentation électrique et de câbles de raccordement au réseau pour chaque machine. L'importance de mettre en œuvre des technologies de démarrage sécurité sera aussi accrue dans ce contexte.

Dans la mesure où l'usage des clés USB semble être la source de difficultés récurrentes, il nous semble potentiellement intéressant de mesurer le désir et la faisabilité, y compris financière, de la mise en place de locaux sécurisés d'entreposage, maintenance et configuration des machines de vote.

La gestion de la sécurité sera certainement importante et complexe à apprécier. Idéalement, on souhaiterait que les machines soient stockées dans des centaines d'endroits tous très bien sécurisés. On sait que la sécurité parfaite n'existe pas, et éparpiller les machines permet qu'une brèche à un endroit garde un impact limité (même si l'impact peut rester complet si on modifie le comportement des machines d'une localité dans le cadre des élections locales par exemple). Disposer de centaines d'infrastructures d'entreposage à haute sécurité est cependant peu réaliste vu les coûts que cela occasionne, et on est alors confronté à une gamme de choix allant entre un stockage des machines

dans énormément d'endroits mais sans doute aussi dans des conditions de sécurité variables, et mettre en place un nombre minimal de lieux de stockages (un seul, à l'extrême) dans lesquels on pourra faire un réel investissement en sécurité.

La stratégie centralisée correspond à celle de beaucoup de systèmes informatiques aujourd'hui, où l'on délègue la gestion des emails, des fichiers, etc. à des fournisseurs de service "cloud" qui peuvent mettre en place des normes de sécurité qui sont généralement trop coûteuses pour de petites et moyennes entreprises. Mais, au plus on centralise, au plus on s'expose au risque de brèches majeures dont l'impact serait beaucoup plus important : les annonces de brèches de sécurité dans les grandes infrastructures "cloud" restent courantes. Et la perspective d'un impact important augmente naturellement aussi l'intérêt de monter de telles attaques.

Notre suggestion ici serait de s'inspirer de fixer un niveau de sécurité minimal acceptable, éventuellement inspiré des recommandations de l'EAC (résumées en Figure 4.2), et de répartir le stockage entre autant de lieux que possible qui permettent de garantir ce niveau de sécurité.

4.2.5 Logistique après les élections

Outre les opérations de dépouillement et d'audit décrites ci-dessus, un élément central pour la certification des résultats de l'élection est le rapport du Collège des experts.

Concernant l'analyse du fonctionnement du système de vote électronique durant les jours d'élection, ces rapports sont largement informés par les visites des différents bureaux de vote et bureaux principaux de cantons opérées le jour de l'élection mais, au vu du nombre de bureaux de vote concernés par le vote électronique et du nombre de membres du Collège, seule une petite proportion des bureaux peuvent faire l'objet d'une visite en pratique : les 16 membres du Collège rapportent par exemple avoir visité 132 bureaux de vote lors des élections de 2019, parmi plus de 4 000 bureaux, soit à peu près 3 % des bureaux [19].

Il pourrait être utile de disposer d'outils de reporting systématiques et structurés pour chaque bureau de vote, ce qui permettrait aux experts de prendre la mesure exacte de chacun des problèmes relevés. Une application pour smartphone mise à disposition des présidents de bureaux, permettant un reporting rapide basé sur la sélection d'options, pourrait être un outil fort utile dans ce contexte.

4.3 Processus d'évaluation de la qualité du système

Les systèmes de vote sont des éléments critiques dans la protection de nos démocraties. En Belgique, ceci est largement reconnu : outre l'évaluation réalisée par le Collège des experts, le système de vote a été évalué par le Centre for Cyber Security Belgium (CCB) et par le Centre de Crise national. Les codes sources de certains logiciels, dépourvus de leurs éléments de sécurité, sont aussi publiés après les élections, pour une durée limitée. [16]

Au niveau européen, le Conseil de l'Europe a publié en 2004 ses premières recommandations en matière de vote électronique, recommandations qui ont été mises à jour en 2017, accompagnées de lignes directrices concernant leur mise en œuvre [23]. [17] Ces recommandations ont été une source d'inspiration importante pour la présente étude. Le groupe NIS, mis en place dans le cadre de la directive européenne NIS, a aussi publié, en 2018, un compendium en matière de cybersécurité des technologies employées durant les élections [48]. Ce compendium vise cependant principalement les parties "en ligne" des systèmes, comme la gestion des bases de données d'électeurs et les systèmes de compilation des résultats, qui sont largement orthogonaux à la présente étude.

Aux États-Unis, les équipements de vote ont été classés par le Department of Homeland Security comme faisant partie des infrastructures critiques du pays, et devant être protégées comme telles. [18] L'Election Assistance Commission (EAC), [19] créée via le Help America Vote Act de 2002, rassemble et publie différents guides en matière d'élection, et en particulier les "voluntary voting system guidelines" qui définissent un ensemble des spécifications et d'exigences en matière de systèmes de vote [64]. L'adhésion aux VVSG est volontaire, sauf dans les états où elle est imposée. La dernière version des VVSGs (2.0), publiée en 2021, développe particulièrement les questions de sécurité, interopérabilité, et accessibilité des systèmes.

La Suisse, dans le cadre des développements récent de son système de vote par internet expérimental, se trouve aujourd'hui à l'avant-garde en matière de bonnes pratiques de transparence et de processus d'évaluation de son système de vote électronique, en particulier via son Ordonnance 161.116 de

16. https://elections.fgov.be/informations-generales/securite-et-transparence
17. https://www.coe.int/en/web/electoral-assistance/e-voting
18. https://www.cisa.gov/topics/election-security
19. https://www.eac.gov/

la Chancellerie fédérale sur le vote électronique (OVotE) publiée en 2022 [11]. Cette ordonnance conditionne l'octroi de l'agrément pour la réalisation d'essais de vote électronique par les cantons.

L'Article 3, que nous reproduisons ici, précise les conditions pour obtenir l'agrément :

> a. le système est conçu et exploité de façon à garantir un scrutin électronique vérifiable, sûr et fiable ;
>
> b. le système est facile à utiliser par les électeurs ; il tient compte autant que possible des besoins particuliers de chacun ;
>
> c. le système et les processus d'exploitation sont conçus et documentés de façon à ce qu'il soit possible de vérifier et de comprendre dans le détail leurs aspects techniques et organisationnels ;
>
> d. le public a accès à des informations adaptées sur le fonctionnement du système et sur ses processus d'exploitation, et des mesures sont prises pour inciter les personnes disposant des connaissances nécessaires à participer à l'amélioration du système.

Nous relevons ici un certain nombre d'autres éléments de cette ordonnance qui nous semblent particulièrement significatifs dans le cadre de l'évaluation de la qualité du système.

— Audits indépendants. L'article 10 indique que la Chancellerie fédérale mandate des organes indépendants en charge de vérifier la conformité des protocoles cryptographiques, du logiciel, de la sécurité de l'infrastructure et de l'exploitation, et de la protection contre les tentatives d'intrusion dans l'infrastructure.

— Publication. L'article 11 indique que doivent être publiés, pour l'agrément, le code source (y compris les fichiers de paramètres) ; les documents justifiant que ce code est réellement celui utilisé dans les machines ; la documentation du logiciel, des guides indiquant comment les personnes intéressées peuvent compiler, faire fonctionner et analyser le système dans leur propre infrastructure au moyen du code source ; les spécifications techniques des principaux composants du système ; la documentation des processus d'exploitation, de maintenance et de sécurité du système ; les informations et descriptifs concernant les failles identifiées. L'Article 12 précise que ces publications doivent être réalisées de manière à faciliter autant que possible leur lecture et leur

> analyse, ce qui inclut que l'accès doit être gratuit et ne pas requérir d'inscription. L'Article 13 indique que les cantons désignent un service auquel le public peut indiquer les propositions d'améliorations du système, et prévoient que les indications qui touchent à la sécurité du système soient rémunérées de manière équitable.

Nous observons ici le rôle central de la chancellerie fédérale dans l'évaluation, qui n'était pas présent dans les premières versions de l'ordonnance. Cette position permet notamment que les personnes en charge de l'évaluation soient engagées par l'organe en charge de l'évaluation de la qualité du système et non, comme précédemment, par le fournisseur du système de vote dont l'intérêt commercial est évidemment la validation du système. Tous les rapports d'évaluation sont publiés par la Chancellerie. [20]

Nous observons aussi le rôle important du public dans l'évaluation du système, largement *avant* les élections, la portée très large des publications (y compris la documentation permettant aux personnes intéressées de faire fonctionner le système dans leur propre environnement informatique) et la description des infrastructures, l'attention à placer des incitants pour que le public examine le système (notamment, via la publicité des failles et la rémunération des personnes identifiant des failles).

Des éléments qui nous semblent aussi important sont l'absence d'exigences concernant l'usage de technologies spécifiques (langages de programmation, normes spécifiques, etc.), ainsi que la continuité du processus d'évaluation, y compris par le public. Ceci permet de refléter le caractère essentiellement mouvant des technologies, et le fait qu'un système de vote ne fonctionne jamais en isolation : il dépend de nombreux composants externes, y compris des systèmes d'exploitation, des librairies, mais aussi des moyens de protection physique comme des serrures, des enveloppes sécurisées ou des scellés. Ces éléments évoluent en permanence, notamment pour corriger des erreurs, répondre à de nouvelles techniques d'attaque, et un système de vote, comme tout système informatique, doit s'adapter en fonction de cela. Il n'est pas possible de "mettre un cachet" validant un système de vote un jour, et d'espérer que ce cachet reste valable tant que le système n'est pas modifié. La validation d'un système de vote indiquera plutôt que, à la suite d'un processus d'évaluation suffisamment large, et en l'état des connaissances à un moment donné, il semble raisonnable d'utiliser un système de vote dans le contexte d'une élection spécifique.

Nos recommandations, en l'état des connaissances actuelles, sont de :

20. https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html

— Mettre en place un groupe de travail au niveau de la Direction des élections, visant à élargir la procédure d'évaluation du système de vote en se basant sur l'expérience suisse. Les modalités de publication et de documentation du système de vote utilisées en Suisse nous semblent appropriées en Belgique. Il s'agira de déterminer la manière de s'assurer que l'information publiée est réellement évaluée (une publication qui reste ignorée est inutile) et de déterminer les besoins au niveau de la Direction des élections pour être en mesure de mener l'évaluation en interaction avec les différents acteurs (fournisseurs du système, institutions ou experts mandatés pour son examen, et public).

— S'inspirer, lors de l'évaluation, des recommandations et leçons apprises d'autres pays. En l'état, nous recommandons une attention particulière pour les recommandations du Conseil de l'Europe [23], les VVSG [64] et les leçons qui continuent à être acquises dans le contexte suisse. [21]

On encouragera le développement d'un système basé, dans la plus large mesure possible, sur des éléments standard qui ont déjà été évalués par ailleurs, ainsi que sur des formats de données standard facilitant l'inspection et les tests. Ceci a été l'un des principes centraux dans la conception de BeVoting II, et nous espérons que cela simplifiera considérablement l'évaluation de ce système, qui est considérablement plus standard que la solution développée en Suisse, qui doit répondre à un cahier des charges fort différent. Outre le fait que l'usage de composants standard limite les risques d'erreurs et de maladies d'enfance du système, il facilitera aussi fortement l'évaluation. Les systèmes de vote sont des systèmes rassemblant beaucoup de contraintes relativement uniques, et les personnes ayant une expertise spécifique à ce domaine sont peu nombreuses.

4.4 Synthèse du système BeVoting II

La description du système BeVoting II réalisée précédemment était intégrée à la motivation de chaque élément, ainsi qu'à la discussion de différentes variantes. Nous assemblons ici les différents éléments du système, mettant en évidence les différences avec le système de vote électronique actuellement en place – sans indication, nous supposons que BeVoting II se comporte comme le système actuel. Les numéros dans la colonne de droite renvoient aux sections de l'étude où ces étapes sont discutées.

21. https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html

4.4.1 Expérience de l'électeur

L'électeur réalise tout ou partie des étapes suivantes.

E1. Si l'électeur le souhaite, il complète à l'avance son bulletin de vote, ou ses bulletins de vote, sur une application smartphone. L'application préparera un code QR qui pourra être scanné par la machine de vote et affichera les choix encodés. Ceux-ci pourront encore être modifiés à souhait par l'électeur. 4.2.1.1.2

E2. L'électeur s'identifie à l'entrée du bureau de vote et reçoit un papier reprenant, de manière lisible et sous la forme d'un code QR, la liste des scrutins auxquels il peut participer. 4.2.1.1.3 4.2.1.2.5

E3. L'électeur se rend dans l'isoloir et scanne, sur la machine de vote, le code QR qu'il a reçu à l'entrée du bureau de vote. 4.2.1.1.3

E4. L'électeur indique ses choix via l'écran tactile de la machine de vote ou en scannant le code QR qu'il a préparé à l'avance et qui pré-encode ses choix. 4.2.1.1.2

E5. L'électeur peut aussi décider d'exprimer un vote aléatoire s'il souhaite vérifier le bon fonctionnement de la machine de vote. Dans ce cas, après impression et vérification du bulletin imprimé, il fera invalider le bulletin par le président et obtiendra un nouveau code QR lui permettant de voter. 3.3.2.3.3

E6. L'électeur vérifie ses choix sur l'écran final de la machine de vote. Il peut encore modifier ceux-ci à volonté. 4.2.1.1.2

E7. Quand l'électeur est satisfait, il lance l'impression de son ou de ses bulletins de vote sur du papier au format A4. Il reçoit ses bulletins de vote, qui montrent ses choix de manière lisible et reprennent aussi un code QR. Une page supplémentaire contenant le numéro de suivi du bulletin est aussi imprimée, pour permettre la vérifiabilité individuelle. 4.2.1.1.1 4.2.1.2.3

E8. Si l'électeur est satisfait de l'impression, il place ses bulletins de vote dans une farde et garde son numéro de suivi hors de la farde. Il présente la page contenant son numéro de suivi aux membres du bureau de vote pour que ceux-ci marquent la page d'un cachet pour indiquer son authenticité et s'assurent que cette page ne sera pas placée dans l'urne. L'électeur dépose son ou ses bulletins de vote dans l'urne (il s'agit d'une urne classique, sans scanner ou clapet électronique). 4.2.2.1 4.2.3.2.1

E9. Si l'électeur n'est pas satisfait de l'impression, il le signale au président du bureau de vote qui annule le bulletin imprimé et permet à l'électeur de voter à nouveau. Si l'électeur pense que la machine triche, l'incident sera noté en vue d'une éventuelle investigation. — 4.2.3.2.1

E10. Après la publication des résultats temporaires de l'élection, l'électeur qui le souhaite peut vérifier la présence de son numéro de suivi dans la liste des numéros de suivi de bulletins décomptés. Il pourra éventuellement aussi vérifier la présence de numéros de suivi de bulletins qu'il a invalidés dans une liste de bulletins déclarés invalides. En cas de problème, il contacte le service prévu à cet effet. — 3.3.2.3.1, 3.3.3.2.3

4.4.2 Expérience du Bureau de vote

Les opérations effectuées par les membres des Bureaux de vote se déroulent ainsi.

P1. Le Président de bureau de vote reçoit, sous enveloppe sécurisée, les codes d'activation des machines de vote et, le cas échéant, les clés USB permettant de faire démarrer celles-ci. Il démarre les machines de vote à l'ouverture des scrutins. — 4.2.4

P2. Les membres du bureau de vote identifient les électeurs, leur fournissent les codes QR leur permettant de voter, et les informent du fonctionnement du système de vote ainsi que des possibilités de vérifiabilité offertes par le système. — 4.2.1.1.3

P3. Les membres du bureau de vote assistent les électeurs qui souhaitent invalider des bulletins de vote produits. Ils marquent ces bulletins comme invalides et fournissent un nouveau code QR pour permettre aux personnes de préparer un nouveau bulletin. — 3.3.2.3.3, 4.2.3.2.1

P4. Les membres du bureau de vote marquent les pages portant les numéros de suivi d'un cachet, afin d'offrir une marque de l'authenticité de ceux-ci. — 4.2.2.1, 4.2.3.2.1

P5. À la fin des opérations de vote, le Président rédige le procès-verbal du bureau de vote, spécifiant notamment le nombre d'électeurs qui se sont présentés pour chaque scrutin. — 3.2.1.2

P6. Le Président de vote place l'ensemble des bulletins de vote dans des enveloppes qui sont scellées et transportées, par plusieurs personnes, vers le lieu où aura lieu le scanning des bulletins en vue du dépouillement. Les enveloppes sont transmises contre reçu. — 3.2.2.3.4, 4.2.2.1

P7. Le Président du bureau de vote encode la liste des incidents, ou l'absence d'incidents, dans une application prévue pour faciliter un encodage rapide, et transmet le résultat vers les Bureaux principaux, le Collège des experts, et le SPF intérieur.	4.2.5

4.4.3 Expérience du Bureau de scanning

Les opérations dans les bureaux de scanning se déroulent ainsi.

S1. Chaque enveloppe provenant des bureaux de vote est ouverte, les bulletins de vote reçus sont mélangés, et les bulletins sont assemblés en piles d'une centaine de bulletins.	4.2.2.1
S2. Les bulletins sont scannés et endossés par le scanner. On place chaque pile de bulletins scannés, sans en changer l'ordre, dans une nouvelle enveloppe. On indique sur cette enveloppe le numéro du premier et du dernier bulletin de la pile, ainsi que le nombre de bulletins comptés par le scanner.	3.2.2.3.4 4.2.2.2
S3. Les enveloppes de bulletins scannés sont rassemblées dans des boîtes. On conserve un manifeste du contenu de chaque boîte, contenant au minimum le numéro de la boîte, la liste des enveloppes qu'elle contient, et les premiers et derniers numéros des bulletins placés dans chaque enveloppe au moment de l'endossement.	3.2.2.3.4
S4. L'outil de scanning fournit un fichier contenant la liste des bulletins scannés, avec leur numéro d'endossement, le contenu du vote, et le chiffré qui sera utilisé pour la vérifiabilité de bout en bout du bulletin et du dépouillement.	4.2.2.1
S5. Les totaux sont calculés sur base de ce fichier, qui est transmis au bureau principal concerné, au SPF intérieur et au bureau qui se chargera de la conduite de l'audit à limitation de risque.	4.2.2.1
S6. L'ensemble des boîtes contenant les bulletins de vote, tant pour le vote électronique que pour le vote papier, est acheminé vers le lieu où se déroulera l'audit à limitation de risque.	3.2.2.3.4
S7. Le Président du bureau de scanning encode la liste des incidents, ou l'absence d'incidents, dans une application prévue pour faciliter un encodage rapide, et transmet le résultat vers les Bureaux principaux, le Collège des experts, et le SPF intérieur.	4.2.5

4.4.4 Expérience du Bureau de dépouillement "papier"

Quand, dans une même circonscription, on organise à la fois des élections électroniques et des élections "papier", les opérations de préparation de l'audit limitant le risque dans les bureaux de dépouillement papier se déroulent ainsi.

D1. Les enveloppes contenant les bulletins de vote, classés de manière telle que chaque enveloppe ne contient des votes que pour un unique parti, sont numérotées, placées dans des boîtes numérotées elles-aussi, et acheminées vers le bureau où se déroulera l'audit à limitation de risque. 3.2.2.3.1

D2. Un manifeste reprenant le contenu de chaque boîte est acheminé de la même manière. Ce manifeste reprendra au minimum la liste des enveloppes contenues dans chaque boîte et le contenu affirmé de chaque enveloppe (nombre de bulletins et parti auquel sont attribués ces bulletins). 3.2.2.3.1

4.4.5 Audit limitant le risque

Les opérations liées à l'audit limitant le risque se déroulent ainsi.

A1. Les manifestes reprenant les listes de bulletins de vote, leur contenu tel que comptabilisé, et la localisation de ces bulletins de vote (numéro de boîte et d'enveloppe, avec aussi le numéro d'endossement dans le cas des bulletins électroniques), sont chargés dans le logiciel organisant l'audit limitant le risque. Les résultats de l'élection sont aussi encodés (uniquement le nombre de voix obtenu pour chaque liste). 3.2.2.3.5

A2. Les dés sont lancés en présence d'observateurs pour initialiser le processus de sélection des bulletins. 3.2.2.3.5

A3. Le logiciel d'audit indique, sur un écran de projection visible à tous, la liste des bulletins à vérifier. 3.2.2.3.6

A4. Le bureau d'audit retrouve les bulletins indiqués dans les caisses, en indique le contenu lisible, qui est comparé avec l'interprétation électronique qui avait été enregistrée. 3.2.2.3.5

A5. Le logiciel confirme que le risque d'une attribution incorrecte des sièges aux listes est inférieur au seuil choisi, ou indique que la sélection de bulletins supplémentaires est nécessaire (parce que des erreurs ont été détectées, par exemple), ou indique qu'un recomptage manuel complet est requis en raison d'une marge d'élection trop faible et/ou d'un nombre d'erreurs trop élevé.	3.2.2.3.5
A6. Le résultat de l'audit limitant le risque est transmis au Bureau d'arrondissement, au SPF intérieur et au Collège des experts.	3.2.2.3.6

4.4.6 Vérification du bout en bout

Les opérations liées à la vérification de bout en bout se déroulent comme suit.

V1. Avant le début de l'élection, les gardiens et le SPF génèrent leurs clés publiques et conservent leurs clés secrètes.	3.3.1.2 4.2.3.2.2
V2. Le SPF produit les supports d'initialisation de toutes les machines de vote, qui incluent les clés publiques générées à l'étape précédente.	4.2.4
V3. Sur base des fichiers obtenus à la fin du processus de scanning, le SPF intérieur recalcule la version chiffrée et le numéro de suivi de chacun des bulletins repris et rend les numéros de suivi publics, en indiquant s'ils correspondent à des bulletins dépouillés ou à des bulletins invalidés à la demande de l'électeur.	3.3.2.3.1 4.2.3.2.2 4.2.3.2.3
V4. Sur base de ces mêmes fichiers, le SPF intérieur calcule des preuves à divulgation nulle de la validité de chacun des bulletins chiffrés, ainsi que du fait que les résultats annoncés pour l'élection sont bien consistants par rapport à ces bulletins chiffrés.	4.2.3.2.3
V5. Les électeurs qui le souhaitent vérifient que le numéro de suivi de leur bulletin est bien présent dans la liste des bulletins inclus dans le dépouillement, via le site du SPF ou via d'autres sites web hébergés par des observateurs ou des partis.	3.3.2.3.1
V6. Les électeurs qui ont demandé d'invalider et de vérifier un bulletin de vote vérifient, s'ils le souhaite, que ce bulletin est bien repris dans les bulletins qui ne sont pas inclus dans le dépouillement.	3.3.1.2

V7. Les observateurs de l'élection qui le souhaitent accèdent à l'ensemble des bulletins chiffrés et preuves à divulgation nulle, vérifient que ces bulletins chiffrés sont cohérents par rapport à la liste des numéros de suivis qui a été publiée, par rapport au nombre de bulletins de vote enregistrés dans chaque bureau de vote, et par rapport aux résultats de l'élection annoncés. Les résultats de toutes ces vérifications sont transmis au SPF intérieur et au Collège des experts.	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 Comment développer BeVoting II ?

Le choix d'un fournisseur ou de fournisseurs qui développeront, assisteront le déploiement et feront évoluer un système de vote électronique est un défi majeur : il engage la Belgique pour une longue durée (souvent 10 à 15 ans, voire plus) dans l'usage d'un système destiné à être utilisé dans des conditions critiques, et sur un marché largement de niche, demandant des expertises souvent très spécifiques.

4.5.1 Les familles d'acteurs sur le marché du vote électronique

Le fait que le marché des machines de vote soit une niche fait qu'il n'existe qu'un petit nombre d'acteurs ayant de expérience dans l'organisation d'élections gouvernementales avec des machines de vote.

Au niveau de l'Union Européenne, l'International Institute for Democracy and Electoral Assistance (International IDEA) relève que seuls la Belgique, la Bulgarie et la France emploient des machines de vote.[22] Qui plus est en France, un moratoire existe depuis 2008 qui interdit à toute nouvelle commune de déployer des machines de vote.[23] Et la société Smartmatic, qui est le fournisseur actuel de la solution belge, est aussi fournisseur de la Bulgarie.[24]

Outre les acteurs spécialisés sur le marché, un certain nombre de pays choisissent de développer le vote électronique via des entreprises locales, souvent largement actives sur d'autres marchés. En France, le vote par internet

22. https://www.idea.int/data-tools/data/question?question_id=9349&database_theme=327
23. https://www.legifrance.gouv.fr/download/pdf/circ?id=45311
24. https://www.smartmatic.com/case-studies/bulgaria-first-binding-e-vote-is-100-accurate/

proposé dans certaines élections pour les Français résidant à l'étranger, est développé par Voxaly, une marque de Docaposte, une société du Groupe La Poste. [25] En Suisse, les essais de vote électronique sont aussi réalisés à l'aide d'un système développé par la Poste. [26] Au Brésil, les machines de vote sont développées par la société Positivo Tecnologia, une société brésilienne active sur un large spectre d'activités dans l'IT, tant du côté matériel que du côté logiciel. [27] En Inde, les machines de vote sont développées par Electronics Corporation of India Limited, une entreprise du secteur public fournissant des systèmes électroniques et IT. [28]

Le marché des élections privées se présente très différemment, avec une multitude d'acteurs offrant principalement des solutions de vote par internet. On retrouve ainsi plusieurs solutions belges listées sur le site des élections sociales de 2024 [57]. Ces acteurs sont susceptibles d'apporter des compétences en matière d'élections, même si les questions d'infrastructure, de sécurité et de maintenance se présentent très différemment dans un contexte d'élections gouvernementales.

4.5.2 Le coût du vote électronique

L'évaluation des coûts globaux d'une solution de vote est malheureusement une chose extrêmement complexe et mal documentée. Krimmer et ses coauteurs [41] pointent un certain nombre de difficultés systématiques. Les trois principales sources de difficultés évoquées, et que nous avons rencontrées aussi, sont : *(i)* la difficulté d'accéder aux coûts, qui ne sont pas systématiquement divulgués, *(ii)* la difficulté de savoir ce qui est couvert par les coûts qui sont divulgués, et ce qui va être repris dans d'autres budgets (dans un budget d'achat de machines, inclut-on un coût de développement, de maintenance, de mises à jour, de stockage, de formation à l'usage des machines, de support pendant les élections, etc. ?), *(iii)* la difficulté d'évaluer les coûts liés aux agents et infrastructures publiques impliqués dans les élections.

Dans le cas spécifique des machines de vote, une difficulté supplémentaire pour l'évaluation des coûts est liée au très petit nombre d'acteurs présents

25. https://www.voxaly.com/vote-par-internet-pour-les-francais-de-letranger-dans-le-cadre-des-elections-legislatives-2022/
26. https://digital-solutions.post.ch/fr/e-government/solutions-numerisation/vote-electronique/
27. https://www.reuters.com/world/americas/brazils-positivo-wins-207-million-voting-machines-tender-2021-12-27/
28. Ces machines ont été notamment décrites dans https://thewire.in/government/the-anatomy-of-an-electronic-voting-machine-what-we-know-and-what-we-dont

sur le marché européen (seul Smartmatic semble actif à ce jour sur le marché gouvernemental en Europe), qui complique les comparaisons, la mise en compétition et rend les prix difficiles à anticiper.

En Belgique, le prix d'acquisition d'un bureau de vote formé de 5 machines de vote, une machine de président, une urne, un scanner et le petit matériel associé (cartes à puce) était évalué à 11 585 euros HTVA en 2015. Le même équipement, loué pour une journée, est proposé à 1 975 euros [49]. Ces coûts ne prennent pas en compte toute une série d'autres coûts : les coûts de support technique durant l'élection, le coût des formations des différents opérateurs du système, les frais de stockage, de maintenance et de réparations des systèmes de vote achetés, le coût des bureaux de totalisation, le coût de l'IT et de la création des clés USB au niveau du SPF Intérieur, le coût des audits du système, etc.

La compréhension des coûts sur l'unique marché belge reste elle-même un unique point de donnée, sur base duquel il est extrêmement hasardeux de se baser pour l'évaluation de coûts d'un futur système. Même au cours d'une période unique, on observe que les coûts obtenus pour des équipements similaires peuvent varier énormément.

Il est instructif de se référer ici au marché américain, beaucoup plus diversifié. VerifiedVoting indique ainsi que, pour les élections de 2024, ES&S et Dominion couvrent plus de 70 % du marché, suivis de Hart InterCivic, Clear Ballot et Smartmatic qui couvrent les 21 % de parts du marché suivantes (les pourcentages sont comptés en termes de nombre d'électeurs inscrits). Le décompte électronique est omniprésent sur le marché américain : seuls 0.2 % des bulletins seront comptés à la main. [29] Si les coûts globaux du vote électronique restent très mal connus, une étude de 2021 publiée par VerifiedVoting lève le voile sur les pratiques de prix pour un certain nombre d'équipements [67] et met en évidence une grande variabilité : l'un des scanners de bulletins de vote muni d'une urne les plus vendus (le DS200 d'ES&S) a été ainsi acheté dans 110 juridictions différentes pour des prix oscillant entre 4 270 et 6 975 USD. Les variations sont notamment motivées par des choix de matériaux différents pour l'urne, la disponibilité de boîtes de transport, ou l'inclusion ou non des frais de livraison. Les alliances de juridictions offrant un marché plus important semblent aussi obtenir de meilleurs prix. L'étude montre aussi que les prix d'achat des machines ne sont qu'une petite pièce du puzzle : il est observé que les frais de maintenance des machines sur 10 ans oscillent, d'un contrat à l'autre, entre 40 % et 90 % du prix d'achat des machines – prix qui sous-estiment sans doute les prix réels que les fournisseurs

29. https://verifiedvoting.org/verifier/#mode/visualization/year/2024

se réservent le droit d'indexer.

VotingWorks semble être le seul fournisseur d'équipement de vote qui affiche ses prix,[30] annonçant par exemple une machine de vote munie d'une imprimante, de dispositifs d'assistance, intégrée dans une boîte de transport rigide et assortie d'une garantie de 5 ans pour 1 750 USD.

4.5.3 Adapter ou renouveler les machines ?

Une question naturelle à ce stade de décider si les machines de vote actuelles, éventuellement adaptées, peuvent continuer à être utilisées ou si de nouvelles acquisitions sont nécessaires.

La deuxième génération de machines introduite en 2018 pourra vraisemblablement être encore utilisée après 2027, avec des mises à jour – voir la comparaison et la compatibilité entre les machines actuelles et la proposition BeVoting II en section 4.2.1.2.7.

Par contre, la première génération, introduite en 2012, est vraisemblablement devenue obsolète (le matériel est trop limité pour permettre de faire fonctionner des systèmes d'exploitation actuels, et les pièces de rechange sont vraisemblablement devenues introuvables) et les communes équipées de ces machines qui souhaiteront continuer à voter de manière électronique au-delà de 2027 seront confrontées à la question de l'achat d'un nouvel équipement, ne serait-ce que pour remplacer les machines défaillantes. Il en sera de même pour de nouvelles communes qui souhaiteraient adopter le vote électronique au-delà de 2027.

Quelle que soit la décision prise pour les machines de deuxième génération, il semble important de parvenir à ouvrir le marché pour les nouvelles acquisitions, afin de permettra à la Belgique de réellement évaluer les coûts et opportunités de différentes options, tout en gardant en tête les barrières que la Belgique offre à l'entrée, notamment en raison de la relative petitesse de son nombre d'électeurs[31] et du morcellement de son marché. À ce titre, il semble essentiel d'offrir un interlocuteur unique aux entreprises qui viendraient sur le marché belge.

Au vu des enjeux et des spécificités de l'acquisition d'un système de vote électronique, la conception d'un appel d'offre nécessite naturellement

30. https://www.voting.works/voting-system/

31. Pour se faire une idée, le comté de Los Angeles a, à lui seul, déployé près de 20000 machines de vote lors des élections de 2020, soit à peu près le même nombre que la Belgique lors des élections de 2019. https://www.smartmatic.com/us/case-studies/los-angeles-county-building-deploying-vsap-a-model-for-21st-century-elections/

de nombreuses expertises : commerciales, légales, infrastructures IT, et techniques liées aux technologies de vote – il s'agit d'un effort majeur.

L'évaluation des réponses aux appels d'offre demande certainement une importante expertise. Le processus d'évaluation de la qualité du système, discuté en section 4.3, demandera aussi une expertise importante, en particulier au niveau technique. La recommandation de mettre la Direction des élections du SPF au centre du processus d'évaluation, et de fortement augmenter l'évaluation par des experts de différents horizons ainsi que par le public, ainsi que les incitants à ces évaluations, sont des éléments qui s'ajoutent aux tâches du SPF. Des interactions avec la Chancellerie fédérale suisse, qui assume ce rôle dans un pays d'une taille similaire au nôtre, pourraient certainement aider à construire le processus d'évaluation en Belgique.

4.5.4 Échelles de temps

Acquérir un nouveau système de vote demande du temps. L'étude BeVoting publiée en 2007 a permis l'acquisition de machines de vote qui ont été déployées pour les élections de 2012. Cette échelle de temps nous semble raisonnable dans le contexte de BeVoting II, dans la mesure où il s'agit de :

1. Objectiver les souhaits d'acquisition de nouvelles machines et de maintenance et mise à jour des machines actuelles dans les différentes régions.
2. Publier et traiter un premier appel à information, auquel on essaiera d'intéresser un maximum d'acteurs, afin d'identifier les intérêts et capacités de potentiels fournisseurs, et pour éviter d'introduire par inadvertance dans le processus d'appel formel des contraintes qui décourageraient ou éliminerait inutilement certains acteurs.
3. Publier un appel d'offre formel et en évaluer les résultats.
4. Suivre le développement de la nouvelle génération de machines, et assurer sa conformité aux normes et recommandations internationales qui seront en vigueur.
5. Développer le processus de risk limiting audits avec les acteurs choisis.
6. Développer l'écosystème de publication et vérification des données produites pour la vérification de bout en bout (vérifiabilité individuelle et universelle).
7. Mettre en œuvre le processus d'évaluation par des experts et par le public du système réalisé.

8. Incorporer les résultats des évaluations dans le système qui sera déployé.

Partie 5
Conclusions

5.1 Introduction

Dans cette étude, nous avons formulé une proposition d'évolution du système de vote électronique avec preuve papier adaptée au contexte des élections belges, abordant les aspects matériels, logiciels et portant une attention spécifique aux exigences de vérifiabilité.

Nous avons dans un premier temps réalisé un état des lieux du système de vote électronique actuellement utilisé en Belgique, sur base des rapports des Collèges des experts et des Recommandations du Conseil de l'Europe en matière de vote électronique. Ceci nous a amené à définir neuf objectifs principaux d'évolution du système actuel, répartis sur cinq axes, sur lesquels nous reviendrons ci-dessous.

Nous avons ensuite exploré plus spécifiquement les techniques de vérifiabilité qui constituent aujourd'hui l'état de l'art et sont le produit de recherches largement amenées à leur maturité au cours des quinze dernières années, soit dans la période qui a suivi la première étude BeVoting de 2007 [30].

Nous avons enfin proposé le concept d'un nouveau système de vote, appelé BeVoting II, qui répond aux neufs objectifs d'évolution du système actuel et intègre en particulier les aspects de vérifiabilité requis par les récentes recommandations internationales, en Europe et aux États-Unis notamment.

5.2 Réalisation des objectifs d'évolution du système actuel

Nous reprenons ici les objectifs présentés en conclusion de notre état des lieux (section 2.5), et évaluons dans quelle mesure le concept BeVoting II permet de les atteindre.

5.2.1 Gestion du matériel et du logiciel

(G1) Simplifier le déploiement des bureaux de vote, afin de répondre aux difficultés mentionnées en section 2.2.1.2.

Les Bureaux de vote de BeVoting II sont considérablement simplifiés par la disparition de l'urne électronique et de la machine du président, qui sont remplacés par une urne standard. Ceci amène plusieurs avantages importants :

- Suppression d'un élément non standard du système actuel, dont les éventuelles pannes bloquent le dépôt normal des bulletins de vote de tout un bureau de vote.
- Suppression de la procédure de démarrage du système basée sur une machine de président qui doit être démarrée sur des clés USB avant que ces mêmes clés ne soient utilisées pour le démarrage des machines à voter et que les clés USB puissent être ramenées à l'urne électronique.
- Remplacement des cartes à puce par des codes QR imprimés sur des papiers portant par ailleurs, de manière lisible par un être humain, la liste des élections auxquelles le code QR donne le droit de participer.

Le remplacement du l'imprimante à ticket par une imprimante de papier A4 nous semble offrir des avantages pratiques aussi :

- Nous nous attendons à ce que les membres de Bureaux de vote soient plus accoutumés à charger du papier A4 dans une imprimante, opération qui reste courante pour beaucoup de gens, qu'à charger un rouleau de papier thermique.
- Si l'imprimante est extérieure à la machine de vote, les risques de papier restant bloqués dans la machine de vote associés à l'assemblage adhoc actuel sont réduits par l'usage d'une imprimante standard dans son mode d'usage actuel.

Un inconvénient de l'usage d'une imprimante externe serait la nécessité de raccorder un câble d'alimentation électrique et un câble USB. Mais, à nouveau, ces opérations sont courantes pour beaucoup de citoyens.

(G2) Se baser sur du matériel facile à réparer, remplacer et faire évoluer, compte tenu de la durée de vie généralement observée pour un système de vote, comme discuté en sections 2.4.1 et 2.4.2.

La machine de vote BeVoting II reste un assemblage de composants tout à fait standard. L'option de ne plus assembler ces composants dans une boîte rigide, qui ne permet pas de modifications/remplacements aisés, a été discutée : nous avons attiré l'attention sur l'existence de nouveaux vendeurs proposant des modes d'assemblage plus flexibles.

L'urne électronique, qui est le principal élément non-standard du système actuel, est supprimée.

Les opérations de scanning des bulletins de vote peuvent être effectuées à l'aide d'une large gamme de scanners parfaitement standard.

Les opérations de vérifiabilité ne nécessitent rien de particulier au niveau matériel : un laptop et un projecteur pour le RLA, la disponibilité de stations de calcul et d'un site web pour la vérifiabilité de bout en bout.

(G3) Choisir du matériel permettant de faire fonctionner des systèmes d'exploitation et du logiciel conforme aux normes de sécurité durant la durée de vie du système, comme discuté en section 2.4.1.

La recherche d'une très longue durée de vie pour un système de vote est une exigence compliquée et inhabituelle pour un système informatique.

Nos principaux éléments de réponse sont ici :

— Choix de matériel complètement standard et facile à remplacer en cas de panne, permettant de faire face aux difficultés de réparation et d'accès à des pièces de rechange.

— Choix d'un micro-ordinateur ou laptop de vote suffisamment robuste au départ que pour permettre de l'ordre de 5 ans de mise à niveau du système d'exploitation, avant d'entrer dans une phase de support du système d'exploitation installé, qui pourra durer jusqu'à 10 ans selon les normes actuelles.

— Choix alternatif d'un micro-ordinateur à carte unique bon marché, qui pourrait être remplacé à bas coût et pourrait potentiellement aussi être compatible avec des évolutions du système d'exploitation sur une longue durée. La sélection d'une des deux dernières alternatives résultera vraisemblablement de ce que les vendeurs pourront proposer.

La réutilisation pour le vote de matériel standard déployé dans d'autres contextes par ailleurs est attrayante mais, après examen, nous semble être une option difficile à mettre en œuvre dans des conditions qui permettent de garantir une expérience uniforme aux électeurs, un déploiement facile des bureaux de vote (en accord avec l'objectif (G1)), une logistique de déploiement simple et un processus de vote sûr.

(G4) Faciliter la vérification de la conformité du déploiement des logiciels de vote, comme discuté en section 2.2.2.2.

Ici, les propositions sont de :

— Tirer parti des technologies de démarrage sécurisé et des "trusted platform modules" présents sur la plupart des machines actuelles.

— S'assurer que les machines de vote sont stockées dans de bonnes conditions de contrôle d'accès, nécessitant des clés de plusieurs intervenant pour accéder aux machines, et avec des mécanismes de surveillance et de journalisation des accès.

— Augmenter la rigueur et la traçabilité de la chaîne logistique de distribution des clés USB, avec notamment une distribution séparée des clés et des mots de passe.

— De manière alternative, et en se reposant sur les technologies de démarrage sécurisé, préinstaller de manière (semi-)centralisée les logiciels de vote et les fichiers de configuration des élections sur les machines de vote, de telle sorte que les clés USB ne soient plus nécessaires et qu'un mot de passe suffise à faire démarrer les machines.

5.2.2 Accessibilité

(G5) Aller plus loin qu'actuellement en matière d'accessibilité du système de vote pour des personnes malvoyantes ou des personnes dont la dextérité ne permet pas de sélectionner facilement des candidats sur un écran, comme discuté en section 2.3.1.

Ici, les options proposées sont :

— Remplacer le lecteur de carte à puce des machines de vote actuelles par des lecteurs de codes QR, et de proposer une application externe à tous les électeurs, application qui pourrait être utilisée pour préremplir des bulletins de vote à l'avance, et qui afficherait un code QR pouvant être scanné par la machine de vote, de telle sorte que celle-ci affiche un bulletin prérempli que l'électeur peut bien sûr encore modifier avant validation finale.

— Pousser plus avant le projet pilote de déploiement de technologies d'assistance qui a eu lieu à Alost et Malines en 2019.

L'application proposée ci-dessus permettrait d'une part à des électeurs de préparer leur bulletin de vote en se servant de leurs propres technologies d'assistance, adaptées à leurs besoins, mais permettrait vraisemblablement aussi d'accélérer le processus de vote pour tout le monde, vu que cette application permettait à tout le monde de gagner du temps dans l'isoloir.

5.2.3 Transparence

On cherchera ici à :

(G6) Proposer une méthodologie de publicité autour des éléments techniques du système de vote électronique, permettant d'améliorer à la fois la transparence et la qualité du système, comme discuté dans les sections 2.2.2.1 et 2.3.4.

Les propositions faites ici sont de :

— Mettre la Direction des élections du SPF intérieur au centre du processus d'évaluation, y compris du financement de celui-ci : la Direction des Élections sélectionne les auditeurs

— Publier le code source, l'architecture, et la documentation du système de vote en permanence, et pas uniquement pour quelques mois après les élections.

— Maintenir les procédures d'audit actuelles par le CCB, un organisme d'avis et le Collège des experts.

— Fournir aux personnes intéressées les environnements nécessaires pour qu'elles puissent tester le système dans leur propre infrastructure informatique.

— Organiser un programme visant à intéresser le plus de personnes possible à effectivement examiner et proposer des améliorations du système de vote.

Ici, il semble particulièrement intéressant de s'inspirer de l'expérience acquise en Suisse pour un processus similaire.

5.2.4 Vérifiabilité

(G7) Permettre aux électeurs de vérifier que leur intention de vote est correctement enregistrée et que leur vote est bien pris en compte, sans

avoir été modifié, lors des opérations de dépouillement, comme discuté dans les sections 2.2.3 et 2.3.2.

La proposition faite ici est de mettre en œuvre les deux techniques complémentaires de vérifiabilité dont le déploiement est devenu de plus en plus standard au cours des 15 dernières années :

— Les audits limitant le risque (RLA) de valider un résultat incorrect,

— La vérifiabilité de bout en bout.

Les RLAs permettront d'obtenir une garantie que le décompte réalisé électroniquement est bien consistant par rapport à l'ensemble des bulletins de vote papier qui ont été déposés par les électeurs. Le succès d'un RLA repose sur la disponibilité de bulletins de vote papier authentiques, qu'ils proviennent du vote électronique ou du vote papier classique. La mise en œuvre d'un RLA se ferait au niveau des circonscriptions électorales, et demandera un effort humain très variable, et fort dépendant de la marge de l'élection : un RLA pourra représenter un effort mineur dans des élections où il serait nécessaire de modifier une grande proportion des votes pour modifier le résultat des élections, mais la procédure de RLA pourrait mener à un comptage complet des bulletins papier dans des cas de marges exceptionnellement faibles.

La vérifiabilité de bout en bout permet pour sa part de vérifier efficacement que les bulletins de vote préparés par les machines de vote sont bien intégrés dans le décompte électronique, sans avoir été perdus ou modifiés. Cette technique apporte donc des garanties complémentaires à celles des RLAs qui partent de l'hypothèse que les bulletins de vote disponibles n'ont fait l'objet d'aucune modification entre leur dépôt et le moment de l'audit. Elle est par contre beaucoup moins efficace pour identifier une machine de vote qui triche et produirait un bulletin de vote contenant un code QR incorrect, ce que le RLA pourra détecter efficacement. Au niveau de la mise en œuvre, la vérifiabilité de bout en bout nécessitera la mise en place d'une infrastructure informatique pour préparer et héberger les données de vérification au niveau de la Direction des élections, et de développer un écosystème de logiciels et de personnes intéressées par la vérification de ces données. Contrairement aux RLAs, la complexité des processus associés à la vérifiabilité de bout en bout ne dépendent pas des marges de l'élection.

(G8) Permettre que ces vérifications puissent s'opérer sans compromettre le secret des votes – le processus proposé veillera notamment à lever les préoccupations soulevées en section 2.3.3.

BeVoting II suit ici les propositions des Collèges des experts de ne plus réaliser le scanning et l'enregistrement des bulletins de vote au moment où ceux-ci sont déposés dans les urnes. La proposition est de mettre en place des bureaux de scanning, à l'image des bureaux de dépouillement papier mais en nombre nettement plus petit, afin d'offrir un niveau consistant de secret du vote entre les différents modes de scrutin et d'être en mesure de mettre des bureaux de scanning robustes et avec un accès simple à des services de support, évitant ainsi les risques associés à un scanning dans les bureaux de vote.

5.2.5 Reporting

(G9) Mettre en place des mécanismes de reporting simples et permettant une compilation efficace des données reçues, afin d'avoir une mesure claire du nombre d'incidents et de leurs conséquences, comme discuté dans les sections 2.2.1.2 et 2.3.5.

Ici, la proposition et de mettre en place un outil de reporting et de compilation de rapports efficace dans tous les bureaux de vote et de dépouillement, outil qui pourrait prendre la forme d'une application mobile ou d'une page web sur laquelle les membres des Bureaux pourraient indiquer les difficultés rencontrées en quelques "clicks".

Ceci permettra d'avoir une vue du fonctionnement du système plus systématique que celle qui peut être obtenue via les coups de sonde actuels, et d'identifier des attaques peu visibles qui seraient montées au travers de différents bureaux de vote.

Remerciements

Les auteurs souhaitent remercier les nombreuses personnes avec qui ils ont pu interagir dans le contexte de cette étude, et qui ont largement contribué à l'informer, et en particulier : Josh Benaloh, Henri Devillez, Alex Halderman, Thomas Peters, Philip Stark, Vanessa Teague et Emmanuel Willems. Nous avons aussi pu bénéficier d'interactions fort éclairantes avec des membres de la Direction des élections du SPF intérieur, BPost, Smartmatic et VotingWorks. Toute erreur qui serait découverte dans la présente étude reste cependant de notre fait.

Bibliographie

[1] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The oracle diffie-hellman assumptions and an analysis of DHIES. In David Naccache, editor, *Topics in Cryptology - CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 143–158. Springer, 2001.

[2] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a university president using open-audit voting : Analysis of real-world use of helios. In *2009 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '09*. USENIX Association, 2009.

[3] Josh Benaloh. Verifiable secret-ballot elections. PhD Thesis - Yale Univesity, 1987.

[4] Josh Benaloh, Ronald Rivest, Peter Y. A. Ryan, Philip Stark, Vanessa Teague, and Poorvi Vora. End-to-end verifiability, 2015.

[5] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. Can voters detect malicious manipulation of ballot marking devices ? In *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*, pages 679–694. IEEE, 2020.

[6] Michelle L. Blom, Andrew Conway, Dan King, Laurent Sandrolini, Philip B. Stark, Peter J. Stuckey, and Vanessa Teague. You can do RLAs for IRV. *CoRR*, abs/2004.00235, 2020.

[7] Dan Boneh. The Decision Diffie-Hellman problem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer, 1998.

[8] Craig Burton, Chris Culnane, and Steve A. Schneider. vvote : Verifiable electronic voting in practice. *IEEE Secur. Priv.*, 14(4) :64–73, 2016.

[9] Richard Carback, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc,

Ronald L. Rivest, Emily Shen, Alan T. Sherman, and Poorvi L. Vora. Scantegrity II municipal election at takoma park : The first E2E binding governmental election with ballot privacy. In *19th USENIX Security Symposium*, pages 291–306. USENIX Association, 2010.

[10] Carter Center. Risk-limiting audits : A guide for election observation efforts. https://www.cartercenter.org/resources/pdfs/peace/democracy/risk-limiting-audits-guide.pdf, Juin 2022.

[11] Chancellerie fédérale de la Confédération suisse. Ordonnance de la chf-sur le vote électronique 161.116. https://www.fedlex.admin.ch/eli/cc/2022/336/fr, Mai 2022.

[12] David Chaum and Torben P. Pedersen. Wallet databases with observers. In *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 1992.

[13] Le code electoral. Disponible depuis https://elections.fgov.be/legislation/lois. Version originale à http://www.ejustice.just.fgov.be/eli/loi/1894/04/12/1894041255/justel., Octobre 2023.

[14] College van deskundigen. College van deskundigen belast met de controle op de geautomatiseerde stemmingen – verslag van de verkiesingen van 14 oktober 2012. Vlaams Parlement, Octobre 2012.

[15] College van deskundigen. 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, Octobre 2018.

[16] Collège des experts. 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, Octobre 2012.

[17] Collège des experts. 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, Juin 2014.

[18] Collège des experts. 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, Octobre 2018.

[19] Collège des experts. 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, Juin 2019.

[20] Collège d'experts chargés du contrôle des systèmes de vote automatisés. Rapport concernant les élections communales et provinciales du 14 octobre 2012 en wallonie, Octobre 2012.

[21] Collège d'experts chargés du contrôle des systèmes de vote automatisés. Rapport concernant les élections communales et provinciales du 14 octobre 2018 en wallonie. Parlement wallon. 1316 (2018/2019) – No 1, Octobre 2018.

[22] Colorado Secretary of State. Audit Center. https://www.sos.state.co.us/pubs/elections/auditCenter.html.

[23] Conseil de l'Europe. 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, Juin 2017.

[24] Conseil de l'Europe. 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, Juin 2017.

[25] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. Belenios : A simple private and verifiable electronic voting system. In *Foundations of Security, Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows*, volume 11565 of *Lecture Notes in Computer Science*, pages 214–238. Springer, 2019.

[26] Véronique Cortier, Pierrick Gaudry, and Stéphane Glondu. Vérifiabilité des élections législatives partielles 2023, réalisées par voie électronique. https://verifiabilite-legislatives2023.fr/, 2023.

[27] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference*, volume 839 of *Lecture Notes in Computer Science*, pages 174–187. Springer, 1994.

[28] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118. Springer, 1997.

[29] Chris Culnane and Steve A. Schneider. A peered bulletin board for robust use in verifiable voting systems. In *IEEE 27th Computer Security Foundations Symposium, CSF 2014*, pages 169–183. IEEE Computer Society, 2014.

[30] Danny De Cock, Antoon Bosselaers, Elie Milgrom, Vincent Rijmen, Fanny Coudert, Jan Engelen, Olivier de Marneffe, François Koeune, Marc Lobelle, Olivier Pereira, Bart Preneel, Jean-Jacques Quisquater, and Frederik Vercauteren. BeVoting – Etude des systèmes de vote électronique. http ://hdl.handle.net/2078.1/281976, Décembre 2007.

[31] Henri Devillez, Olivier Pereira, and Thomas Peters. How to verifiably encrypt many bits for an election ? In *Computer Security - ESORICS 2022 - 27th European Symposium on Research in Computer Security*, volume 13555 of *Lecture Notes in Computer Science*, pages 653–671. Springer, 2022.

[32] ElectionGuard. https://www.electionguard.vote/, 2023.

[33] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*, 31(4) :469–472, 1985.

[34] Amos Fiat and Adi Shamir. How to prove yourself : Practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[35] Georgia Secretary of State. 2020 General Election Risk-Limiting Audit. https://sos.ga.gov/page/2020-general-election-risk-limiting-audit, Novembre 2020.

[36] Kristian Gjøsteen. The Norwegian Internet Voting Protocol. Cryptology ePrint Archive, Paper 2013/473, 2013.

[37] Joseph Lorenzo Hall, Philip B. Stark, Luke Miratrix, Melvin Briones, Elaine Ginnold, Freddie Oakley, Martin Peaden, Gail Pellerin, Tom Stanionis, and Tricia Webber. Implementing risk-limiting post-election audits in california. In *2009 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '09*. USENIX Association, 2009.

[38] Sven Heiberg, Tarvi Martens, Priit Vinkel, and Jan Willemson. Improving the Verifiability of the Estonian Internet Voting Scheme. In *Electronic Voting - First International Joint Conference, E-Vote-ID 2016*, volume 10141 of *Lecture Notes in Computer Science*, pages 92–107. Springer, 2016.

[39] Lucca Hirschi, Lara Schmid, and David A. Basin. Fixing the Achilles Heel of E-Voting : The Bulletin Board. In *34th IEEE Computer Security Foundations Symposium, CSF 2021*, pages 1–17. IEEE, 2021.

[40] Philip T. Kortum, Michael D. Byrne, Chidera O. Azubike, and Laura E. Roty. Can voters detect errors on their printed ballots ? Absolutely. *CoRR*, abs/2204.09780, 2022.

[41] Robert Krimmer, David Duenas-Cid, Iuliia Krivonosova, Priit Vinkel, and Arne Koitmae. How Much Does an e-Vote Cost ? Cost Comparison per Vote in Multichannel Elections in Estonia. In *Electronic Voting - Third International Joint Conference, E-Vote-ID 2018*, volume 11143 of *Lecture Notes in Computer Science*, pages 117–131. Springer, 2018.

[42] Loi du 7 février 2014 organisant le vote électronique avec preuve papier – mise à jour au 14 avril 2023. Disponible depuis https://elections.fgov.be/legislation/lois. Version originale à http://www.ejustice.just.fgov.be/eli/loi/2014/02/07/2014000108/justel., Avril 2023.

[43] Jennifer Morrell. Knowing it's right, part one : A practical guide to risk-limiting audits. https://electionline.org/resources/rla-practical-guide/, Mai 2019.

[44] Jennifer Morrell. Knowing it's right part two : Risk-limiting audit implementation workbook. https://electionline.org/resources/rla-implementation-workbook/, Mai 2019.

[45] Jennifer Morrell. 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/, Juin 2020.

[46] Jennifer Morrell. 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/, Février 2021.

[47] National Academies of Sciences, Engineering, and Medicine. Securing the Vote : Protecting American Democracy. The National Academies Press, 2018.

[48] NIS Cooperation Group. Compendium on Cyber Security of ElectionTechnology – CG Publication 03/2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645.

[49] Parlement de la Région de Bruxelles-Capitale. 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, Octobre 2015.

[50] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Advances in Cryptology - CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140. Springer, 1991.

[51] Torben P. Pedersen. A threshold cryptosystem without a trusted party (extended abstract). In *Advances in Cryptology - EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 522–526. Springer, 1991.

[52] Jean-Benoit Pilet, Prof. Bart Preneel, Silvia Erzeel, Olivier Pereira, Fanny Sbaraglia, Aurélie Tibbaut, Xavier Carpent, and Régis Dandoy. 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, Mars 2021.

[53] Jean-Benoit Pilet, Maria Jimena Sanhuza, David Talukder, Jérémy Dodeigne, and Audrey E. Brennan. Opening the opaque blank box. *Politics of the Low Countries*, 1(3) :182–204, nov 2019.

[54] Rhode Island RLA Working Group. 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, Septembre 2019.

[55] Peter Y. A. Ryan, Peter B. Rønne, and Vincenzo Iovino. Selene : Voting with transparent verifiability and coercion-mitigation. In *Financial Cryptography and Data Security - FC 2016 International Workshops*, volume 9604 of *Lecture Notes in Computer Science*, pages 176–192. Springer, 2016.

[56] Carsten Schürmann. A Risk-Limiting Audit in Denmark : A Pilot. In *Electronic Voting - First International Joint Conference, E-Vote-ID 2016*, volume 10141 of *LNCS*, pages 192–202. Springer, 2016.

[57] Service Public Fédéral Emploi, Travail et Concertation sociale. Vote électronique. https://emploi.belgique.be/fr/

themes/concertation-sociale/elections-sociales-2024/vote-electronique, Novembre 2023.

[58] Mayuri Sridhar and Ronald L. Rivest. k-cut : A simple approximately-uniform method for sampling ballots in post-election audits. In *Financial Cryptography and Data Security - FC 2019 International Workshops, VOTING and WTSC*, volume 11599 of *Lecture Notes in Computer Science*, pages 242–256. Springer, 2019.

[59] Philip B. Stark. Conservative statistical post-election audits. *The Annals of Applied Statistics*, 2(2) :550–581, Juin 2008.

[60] Philip B. Stark. There is no reliable way to detect hacked ballot-marking devices. *CoRR*, abs/1908.08144, 2019.

[61] Philip B. Stark. Sets of half-average nulls generate risk-limiting audits : SHANGRLA. In *Financial Cryptography and Data Security - FC 2020 International Workshops*, volume 12063 of *LNCS*, pages 319–336. Springer, 2020.

[62] 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.

[63] Swiss Post. The Swiss Post e-voting system. https://gitlab.com/swisspost-evoting/, 2023.

[64] Technical Guidelines Development Committee. Voluntary VotingSystem Guidelines – VVSG 2.0. https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines, Février 2021.

[65] U.S. Vote Foundation. The Future of Internet Voting – End-to-end verfiable Internet voting – Specification and assessment study. https://www.usvotefoundation.org/E2E-VIV, Juillet 2015.

[66] Verified Voting. The Verifier — Post-Election Audits — November 2024. https://verifiedvoting.org/verifier/#mode/navigate/map/auditLaw/mapType/audit/year/2024.

[67] Verified Voting. The price of voting. https://verifiedvoting.org/wp-content/uploads/2021/03/Price-of-Voting-FINAL2.pdf, Mars 2021.

[68] Dan S. Wallach. On the security of ballot marking devices. *CoRR*, abs/1908.01897, 2019.

[69] Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp.

Security analysis of India's electronic voting machines. In *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010*, pages 1–14. ACM, 2010.